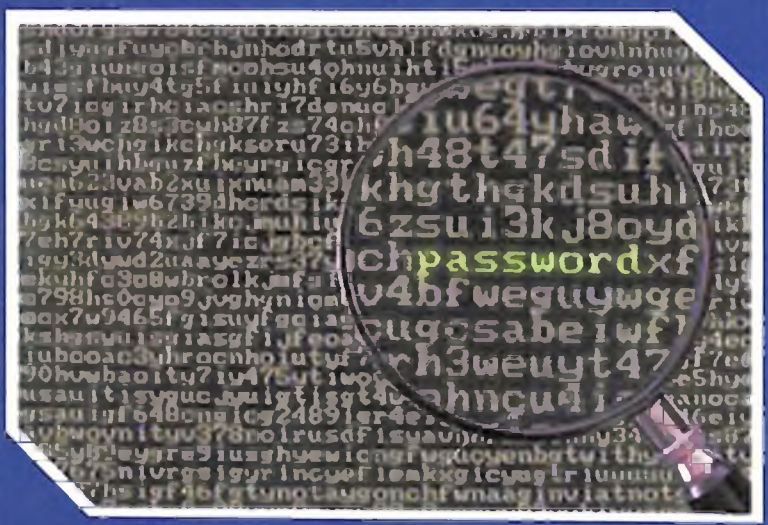
Д.М. КУРЬЯЗОВ, А.Б. САТТАРОВ, Б.Б. АХМЕДОВ.

БЛОКЛИ СИММЕТРИК ШИФРЛАШ АЛГОРИТМЛАРИ БАРДОШЛИЛИГИНИ ЗАМОНАВИЙ КРИПТОТАҲЛИЛ УСУЛЛАРИ БИЛАН БАҲОЛАШ



ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

РАДИОЭЛЕКТРОН ТИЗИМЛАР ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ МАРКАЗИ

Д.М. КУРЬЯЗОВ, А.Б. САТТАРОВ, Б.Б. АХМЕДОВ.

БЛОКЛИ СИММЕТРИК ШИФРЛАШ АЛГОРИТМЛАРИ БАРДОШЛИЛИГИНИ ЗАМОНАВИЙ КРИПТОТАҲЛИЛ УСУЛЛАРИ БИЛАН БАҲОЛАШ

ЎҚУВ ҚЎЛЛАНМА

ТОШКЕНТ – 2017

УЎК 004.056.550(075.8)
КБК 32.811.4я73
К 94

Курьязов Д.М., Саттаров А.Б., Ахмедов Б.Б. **Блокли симметрик шифрлаш алгоритмлари бардошлилигини замонавий криптотаҳлил усуллари билан баҳолаш.** Ўқув қўлланма. Т.: «Aloqachi». 2017, 228 бет.

ISBN 978–9943–5034 – 8 – 9

Ўқув қўлланмада блокли симметрик шифрлаш алгоритмларига қўлланувчи умумий криптографик талаблар, чизиқли, дифференциал, чизиқли-дифференциал, слайд, алгебраик, интеграл, аппарат хатоликлар каби замонавий криптотаҳлил усуллари ва ушбу усуллар бўйича алгоритм бардошлилигини баҳолашга намуна мисоллари, янги таклиф этилган блокли симметрик шифрлаш алгоритмларини замонавий криптотаҳлил усулларига бардошлилигини баҳолаш қадамлари кетма-кетлигида ечилиши лозим бўлган масалалар ҳамда криптотаҳлил натижаларига асосланган ҳолда шифрлаш алгоритмини умумий баҳолаш бўйича тегишли тавсиялар келтирилган.

Мазкур қўлланма “Ахборот хавфсизлиги”, “Криптография ва криптотаҳлил” йўналишларида таълим олаётган бакалавр ва магистрантлар учун мўлжалланган бўлиб, ундан криптотаҳлил йўналишида илмий-тадқиқот олиб бораётган илмий-ходимлар ҳамда соҳа мутахассислари ҳам фойдаланишлари мумкин.

УЎК 004.056.550(075.8)
КБК 32.811.4я73
К 94

Тақризчилар:

Д.Я. Иргашева, т.ф.н., ТАТУ “Ахборот хавфсизлиги факультети” декани;

О.П. Аҳмедова, т.ф.н., ТАТУ “Криптология ва дискрет математика” кафедраси мудири;

Г.У. Жўраев, ф.-м.ф.н., ЎзМУ “Математик моделлаштириш ва криптотаҳлил” кафедраси доценти.

ISBN 978–9943–5034 – 8 – 9

МУНДАРИЖА

Кириш 4

I. Криптографик алгоритмлар бардошлилигига оид заифликлар ва криптографик ҳужумлар 8

1.1. Шифрлаш алгоритмлари криптобардошлилигига оид заифликлар 8

1.2. Блокли симметрик шифрлаш алгоритмларига нисбатан криптографик ҳужум турлари 12

II. Блокли симметрик шифрлаш алгоритмлари бардошлиликларини криптотаҳлил усуллари ёрдамида баҳолаш 19

2.1. Симметрик шифрлаш алгоритми алмаштиришларини умумий криптографик талаблар бўйича баҳолаш 20

2.2. Чизиқли криптотаҳлил усули 35

2.3. Дифференциал криптотаҳлил усули 67

2.4. Чизиқли-дифференциал криптотаҳлил усули 83

2.5. “Слайдли ҳужум” криптотаҳлил усули 94

2.6. Алгебраик криптотаҳлил усули 138

2.7. Интеграл криптотаҳлил усули 147

2.8. Аппарат хатоликларини генерациялашга асосланган криптотаҳлил усули 163

III. Криптотаҳлил натижалари бўйича блокли симметрик шифрлаш алгоритмлари бардошлилигини сонли баҳолаш 190

3.1. Шифрлаш алгоритмлари бардошлилигини сонли баҳолаш 190

3.2. DES ва ГОСТ 28147-89 блокли шифрлаш алгоритмлари бардошлилигини сонли баҳолаш 193

Хулоса 196

Фойдаланилган адабиётлар 197

1-илова 203

2-илова 210

3-илова 223

Кириш

Бугунги кунда криптография ва криптотаҳлил каби йўналишларга бўлинувчи криптология фани кўпчилик университетларда алоҳида фанлар сифатида ўтиб келинади.

Мазкур ҳолатдан келиб чиқиб, криптография йўналишида китоблар рус, инглиз ва бошқа тилларда кўплаб чоп этилган. Улар ичида криптограф олимлар Алферов А.П., Зубов А.Ю., Кузьмин А.С.[32], Баричев С.Г.[34], Иванов М.[40], Черемушкин А.В.[57], Ростовцев А.Г.[36-38], Маховенко Е.Б.[37,52], Василенко О.И.[35], Харин Ю.С.[54], Молдовян Н.А.[48-51], Шнайер Б.[62], Коблиц Н.[41], Menezes A.[53] ва бошқа муаллифлар томонидан ёзилган китобларни алоҳида қайд этиш лозим.

Ўзбек олимлари томонидан криптография соҳасида рус тилида Арипов М.М.[24], ўзбек тилида Ҳасанов П.Ф., Ҳасанов Х.П., Аҳмедова О.П.[29], Каримов М.М., Ғаниев С.К., Ташев К.А.[42], Ҳасанов Х.П.[29,56], Акбаров Д.Е.[26-29] каби муаллифлар томонидан ўқув қўлланма ва китоблар ёзилган.

Кейинги йигирма беш йиллик – криптологиянинг ҳамма масалалари бўйича илмий ишларнинг жуда жадал ўсиши билан тавсифланади. Криптологиянинг криптотаҳлил йўналиши эса фаол ривожланаётган тадқиқот соҳаси ҳисобланади.

Ахборот технологияларининг ривожланиши, ҳисоблаш қурилмаларининг такомиллашуви ҳамда криптотаҳлил усулларининг ютуқлари стандарт шифрлаш алгоритмлари асосида яратилган ва криптобардошли деб ҳисобланган айрим криптотизимлар бардошлилиги баҳосини катта савол остига қўйилишига сабаб бўлмокда.

Бироқ криптотаҳлил йўналишида илмий-техник ва ўқув адабиётлар ҳатто рус, инглиз ва бошқа тилларда жуда кам миқдорда ёзилганлигини кўриш мумкин. Масалан бу йўналишда рус тилида Бабенко Л.К., Ищукова Е.А.[33] томонидан ёзилган ўқув қўлланма ва Молдовян Н.А., Молдовян А.А.[50] томонидан ёзилган китобларни келтириш мумкин. Давлат тилида эса Ҳасанов П.Ф., Ҳасанов Х.П., Аҳмедова О.П., Давлетов А.Б.[55] томонидан ёзилган ўқув қўлланмаси.

Крипторафик алгоритмларни замонавий криптотаҳлил усулларига баҳолаш йўналишида ўзбек тилида китоб мавжуд эмас. Мазкур китоб шу йўлда қўйилган илк қадам бўлиб, унга

муаллифларнинг 2003 йилдан Тошкент ахборот технологиялари университети қошидаги Радиоэлектрон тизимлар ва ахборот технологиялари марказида “Ахборот хавфсизлиги” йўналиши бўйича магистрларга “Амалий криптотаҳлил” фанидан ўқиб келинаётган маърузалари асос қилиниб олинди.

Ўқув қўлланмадан олинган билим ва кўникмалар келажакда “Ахборот хавфсизлиги”, “Криптография ва криптотаҳлил” йўналишлари бўйича бакалавр ва магистрлар тайёрлашда Давлат таълим стандартлари асосида ўқитиладиган “Ахборотни криптографик муҳофаза қилиш усуллари”, “Криптография усуллари” ва “Криптотаҳлил усуллари” фанларида замонавий блокли симметрик шифрлаш алгоритмлари математик асослари, қўлланувчи криптотаҳлил усуллари ва улар бўйича баҳолаш натижалари каби бўлимлари мавзуларида бевосита қўлланилади.

Эътиборингизга ҳавола этилаётган “**Блокли симметрик шифрлаш алгоритмлари бардошлилигини замонавий криптотаҳлил усуллари билан баҳолаш**” деб номланувчи ўқув қўлланма мавжуд ёки янги таклиф этиладиган блокли симметрик шифрлаш алгоритмларини замонавий криптотаҳлил усулларига бардошлилигини баҳолаш ва уларнинг ҳар-бирлари натижаларига асосланиб шифрлаш алгоритмининг умумий бардошлилиги ёки аксинча хулосани чиқариш учун ечилиши лозим бўлган илмий масалаларга бағишланган 3 та бўлим ва иловалардан иборат.

Ўқув қўлланманинг I бўлимида шифрлаш алгоритмлари криптобардошлилигига оид заифликлар, блокли симметрик шифрлаш алгоритмлари учун қўлланувчи калит ва шифрлаш алгоритми ҳақидаги маълумотга эга бўлиш мақсадида таҳлил қилиш, калит ҳақида маълумотга эга бўлиш мақсадида шифрматн, очиқ матн, танлаб олинган очиқ матнлар, танлаб олинган шифрматнлар, танлаб олинган матнлар, танлаб олинган калитлар ёрдамида таҳлил қилиш каби криптографик ҳужум турлари ҳамда криптоалгоритмларнинг бардошлилик хусусиятлари бўйича таснифи ҳақидаги маълумотлар келтирилган.

Блокли симметрик шифрлаш алгоритмлари бардошлиликларини криптотаҳлил усулларига баҳолаш деб номланувчи II бўлимда симметрик шифрлаш алгоритми алмаштиришларини умумий криптографик талабларга, чизиқли, дифференциал, чизиқли-дифференциал, слайд, алгебраик, интеграл, аппарат хатолик-

ларини генерациялашга асосланган криптотаҳлил усулларига баҳолаш қадамлар кетма-кетлиги, улар бўйича олинган натижалар ҳамда таҳлил жараёнида ҳар бир криптотаҳлил усули бўйича ечилиши лозим бўлган масалалар хусусида сўз юритилган.

Ўқув қўлланманинг III бўлими блокли симметрик шифрлаш алгоритмларига қўлланилган криптотаҳлил натижалари бўйича бардошлилигини сонли баҳолашга бағишланган бўлиб, умумий криптобардошлик кўрсатгичи (УКК) деб номланувчи катталик, уни аниқлаш формуласи, мазкур катталик қиймати бўйича шифрлаш алгоритмининг ҳеч бўлмаганда битта криптотаҳлил усулига потенциал заифлиги ёки бардошлилиги ҳақида маълумотлар келтирилган. Шунингдек, Фейстель тармоғига асосланган DES, ГОСТ 28147-89 блокли симметрик шифрлаш алгоритмлари бардошликларини умумий криптобардошлик кўрсаткичи катталиги ёрдамида таҳлил қилишга намуна келтирилган.

Ўқув қўлланмада кўриб чиқилган замонавий криптотаҳлил усуллари стандарт блокли симметрик шифрлар туркимига мансуб DES, ГОСТ28147-89, AES алгоритмлари мисолларида баён қилинган. Мазкур ҳолатни эътиборга олиб, ўқувчига қўшимча маълумот сифатида мазкур шифрлаш алгоритмлари баёнлари 3 та иловада келтирилди.

Китобдаги симметрик шифрлаш алгоритми алмаштиришларини умумий криптографик талаблар бўйича баҳолаш, чизиқли криптотаҳлил, дифференциал криптотаҳлил усулларига оид материаллар ф.-м.ф.н. Курьязов Д.М., чизиқли-дифференциал криптотаҳлил, интеграл криптотаҳлил, алгебраик криптотаҳлил усулларига оид материаллар Саттаров А.Б. ва блокли симметрик шифрлаш алгоритмларига нисбатан криптографик ҳужум турлари, слайдли ҳужум криптотаҳлили, аппарат хатоликларини генерациялашга асосланган криптотаҳлил усулларига оид материаллар Аҳмедов Б.Б. томонларидан ёзилган.

Кириш, хулоса, иловалар, криптотаҳлил натижалари бўйича блокли симметрик шифрлаш алгоритмлари бардошлилигини сонли баҳолаш усули ва улар бўйича тавсияларга оид материаллар ф.-м.ф.н. Курьязов Д.М. ва Саттаров А.Б. томонларидан биргаликда тайёрланди.

Ўқув қўлланмани тайёрлашда яқиндан ёрдан берган тақризчилар т.ф.н. Иргашева Д.Я., т.ф.н. Аҳмедова О.П. ва ф.-м.ф.н. Жўраев Г.У. ларга муаллифлар ўз миннатдорчилигини изҳор этади.

Мазкур ўқув қўлланмада муайян камчиликлар бўлиши мумкин. Муаллифлар ҳурматли ўқувчиларнинг китоб ҳақидаги барча фикр ва мулоҳазаларини мамнуният билан қабул қилади.

I. КРИПТОГРАФИК АЛГОРИТМЛАР БАРДОШЛИЛИГИГА ОИД ЗАИФЛИКЛАР ВА КРИПТОГРАФИК ҲУЖУМЛАР

1.1. Шифрлаш алгоритмлари криптобардошлилигига оид заифликлар

Бугунги кунда криптографик алгоритмлар махсус ахборот-телекоммуникация тизимларининг ажралмас қисми бўлиб, улар заифликларини таҳлил этиш – ахборот хавфсизлигини таъминлашда муҳим ташкил этувчилардан бири ҳисобланади. Криптографик алгоритмларга боғлиқ бўлган ҳар қандай заифлик танишиш доираси (ошкоралик даражаси) чекланган ахборотларнинг чиқиб кетишига олиб келиши мумкин.

Криптографик алгоритмларга боғлиқ барча заифликлар қуйидаги синфларга ажратилади:

- фойдаланилган шифрлаш алгоритми криптобардошлилиги билан боғлиқ заифликлар;
- шифрлаш алгоритмидан нотўғри фойдаланиш билан боғлиқ заифликлар;
- криптографик тармоқ протоколлари заифликлари.

Дастлабки икки синфга тегишли заифликлар тизимда фойдаланилган шифрлаш алгоритмларини криптотаҳлил қилиш орқали аниқланса, учинчи синфга тегишли заифликларни аниқлаш криптотаҳлил билан биргаликда маълумотларни узатиш муҳитларини назорат қилиш ва ахборот тизимига фаол ҳужум ўтказиш орқали аниқланади.

Амалда кенг қўлланилувчи блокли шифрлаш алгоритмлари криптобардошлилиги билан боғлиқ заифликлар бевосита замонавий ахборотни ҳимоялаш криптотизимларининг муҳим заифликлари ҳам ҳисобланади.

Блокли шифрлаш алгоритмларини криптотаҳлил қилишдаги асосий ва дастлабки маълумотлар алгоритмнинг ўзига хос хусусиятларидир. Шифрлаш алгоритмини билган ҳолда, шифр модели ишончлилигини текшириш учун лозим бўладиган маълумотларни мустақил тарзда аниқлаш мумкин.

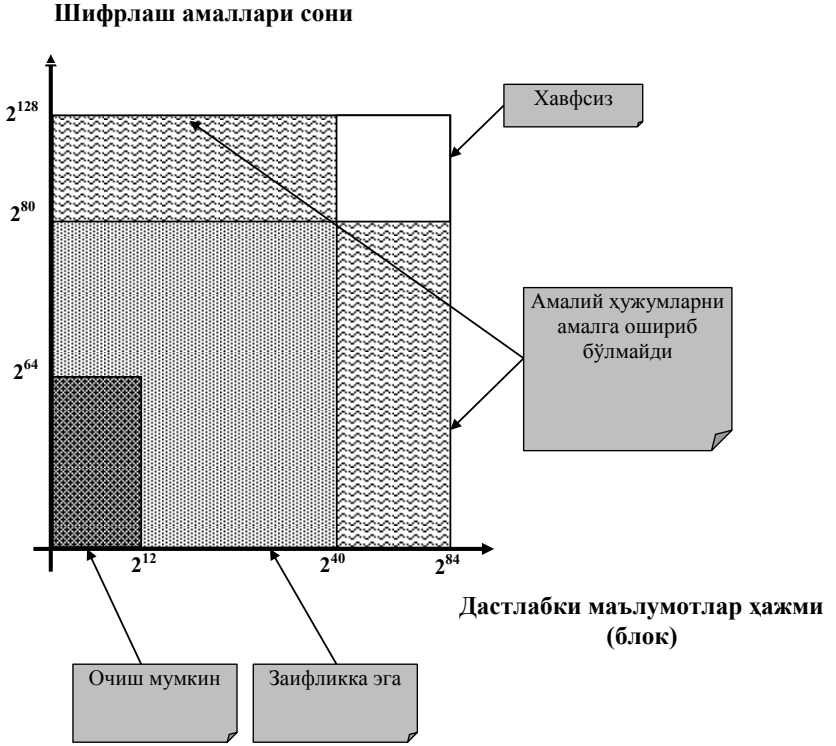
Аниқ бир усул ва уларнинг тегишли параметрларига асосланувчи **криптотаҳлил натижаси** шифрлаш алгоритмининг

хусусий модели (математик, эҳтимолий ва ҳ.к.) ҳисобланиб, ушбу криптотаҳлил усулини амалиётда қўллаш имкониятлари бўйича хулоса бериш учун асос бўлади. Криптотаҳлил ўтказишда лозим бўлган дастлабки маълумотлар (очиқ ёки шифр матн) ҳажми ва кўриниши, шунингдек ҳисоблаш ресурслари ҳажми моделнинг муҳим параметрлари ҳисобланади.

Бугунги кунда замонавий ЭҲМ имкониятлари, талаб этувчи дастлабки маълумотлар ва ҳисоблаш ресурсларига кўра ихтиёрий криптотаҳлил усулининг амалий аҳамиятини 1.1.1-расмда тасвирланган график асосида баҳолаш мумкин [59]. Шуни ҳам таъкидлаш лозимки, ЭҲМ имкониятларининг ошиши 1.1.1-расмда тасвирланган соҳалар кўламининг кенгайишига ҳам олиб келади.

Блокли шифрларга қўлланилувчи ихтиёрий криптотаҳлил усули натижасига таъсир этувчи асосий омиллардан бири, бу шифрда фойдаланилган махфий калит ўлчами (узунлиги) ҳисобланади. Шунга мувофиқ, шифрлаш алгоритмлари муаллифлари томонидан шифр махфий калит ўлчами айнан ЭҲМ (техник қурилмалар) ва замонавий криптотаҳлил имкониятларига боғлиқ тарзда ўрнатилади. Калит ўлчамининг етарлича катта бўлиши шифр бардошлилиги ошишига олиб келиши мумкин. Бироқ унинг дастурий ёки аппарат реализациясини қийинлаштиради ва аксинча калит ўлчамининг кичик бўлиши шифр дастурий ёки аппарат реализациясининг осон бўлишига хизмат қилган ҳолда бардошлиликни тушиб кетишига олиб келади.

Мазкур ҳолат шифрлаш алгоритмини билган ҳолда шифрматнни барча мумкин бўлган калитлар билан дешифрлаб чиқишга асосланган **«Калитларнинг барча мумкин бўлган вариантларини танлаш»** усулига бардошсиз бўлишига олиб келиши мумкин. Мисол учун, шифрлаш алгоритми калит узунлиги 100 бит бўлса, барча калит вариантлари сони 2^{100} га тенг, яъни калитлар тўплами қуввати $|K|=2^{100}$. DES шифрлаш алгоритми калити узунлиги 56 бит бўлиб, барча мумкин бўлган калитлар сони $|K|=2^{56}\approx 0.5*10^{17}$ га тенг. Бунда, агар ҳисоблаш қурилмаси шифрматнни битта калит билан дешифрлаш учун 10^{-6} секунд вақт сарфласа, 24 соатда барча калитлар билан шифрматнни дешифрлаб чиқиш учун $5.787*10^{5}$ дона ҳисоблаш қурилмаси керак бўлади [59].



1.1.1-расм. Турли криптотаҳлил усуллари амалий қўллаш имкониятларини баҳолаш.

Ушбу фикрларга асосланган ҳолда, криптография соҳасидаги муҳим масалалардан бири таклиф этилаётган шифрлаш алгоритми **калит ўлчамининг қандай узунликда бўлиши** ҳисобланади.

Бугунги кунда ахборот хавфсизлиги соҳасида етакчи институт ва ташкилотлар томонидан мазкур масала ечими бўйича турли тавсиялар (ҳисоблаш усуллари) ишлаб чиқилган. Қуйидаги 1.1.1-жадвалда, блокли шифрларнинг айрим (математик) криптотаҳлил усулларига криптобардошлилигини ишончли таъминловчи калит узунликлари келтирилган.

1.1.1-жадвал.

Шифр бардошлилигини таъминловчи калит ўлчамлари

Тавсия этувчининг шартли номи (эълон қилинган йил)	**Калит узунлиги** (бит)	**Фойдаланиш даври** (йил)	**Манба**
Lenstra / Verheul (2000)	81	2014	[22]
	82	2015	
	83	2016 – 2017	
	84	2018	
	85	2019	
Lenstra Updated (2004)	78	2014 – 2015	[14]
	79	2016	
	80	2017 – 2018	
	81	2019	
NIST (2012)	80	2010 гача	[20]
	112	2011 – 2030	
	128	2030 –?	
ANSSI (2014)	100	2014 – 2020	[17]
	128	2021 –?	
BSI (2015)	128	2015 – 2021	[38]
NSA (2015)	256	?	[10]
RFC3766 (2004)	102	2014	[8]
	103	2016	
	104	2017	
	105	2019	

Демак, жадвал қийматларидан келиб чиқиб, блокли симметрик шифрлаш алгоритмлари махфий сеанс калитлари 256 бит қийматдан кичик бўлиши тавсия қилинмайди. Бироқ блокли симметрик шифрлаш алгоритмлари сеанс калитининг юқорида келтирилган қийматда бўлиши унинг бардошли бўлиши учун зарурий шарт бўлиб, етарли ҳисобланмайди.

Амалиётда блокли симметрик шифрлаш алгоритми раундида фойдаланилган криптографик акслантиришлар умумий криптографик талабларга мос келмаса, мазкур алгоритм 2^{256} дан кичик мураккабликда тегишли криптотаҳлил усуллари билан заифликлари аниқланиши ёки муваффақиятли очилиши мумкин. Шунинг учун

ҳам замонавий криптотаҳлил фанида янги яратилган блокли симметрик шифрлаш алгоритми мавжуд (чизиқли, дифференциал, чизиқли-дифференциал, слайд, алгебраик, интеграл, аппарат хатоликлар ва бошқа) ва алгоритм хусусиятидан келиб чиқувчи криптотаҳлил усулларига текширилади. Текшириш натижалари бўйича шифрлаш алгоритмига тегишли ўзгартиришлар киритилади ёки бардошлилиги ҳақида хулосалар берилади.

Масалан, ахборотни ҳимоялаш қурилмасини яратиш "муҳандислик" иши деб қаралса, шифрлаш алгоритмининг криптотаҳлил масаласи эса мураккаб, махсус билимларга эга, юқори малакани талаб этувчи янги илмий масалани ечиш ҳисобланади.

Шунинг учун ҳам блокли симметрик шифрлаш алгоритмларини замонавий криптотаҳлил усулларига бардошлилигини баҳолашдаги текшириш қадамлари ва ҳар бир криптотаҳлил усули баҳоси бўйича алгоритмнинг умумий криптобардошлилиги, амалда қўлланиши мумкинлиги йўналишида ўқув қўлланма ва тавсиялар ишлаб чиқиш республикада криптотаҳлил фанидаги долзарб масалалардан бири ҳисобланади.

1.2. Блокли симметрик шифрлаш алгоритмларига нисбатан криптографик ҳужум турлари

Криптотаҳлил жараёни криптотаҳлилчи эга бўлган маълумотлар асосида олиб борилади. Криптотаҳлилчи эга бўлган маълумотларга кўра криптотаҳлил қуйидаги асосий турларга бўлинади [25, 62]:

1. Калит ва шифрлаш алгоритми ҳақида маълумотга эга бўлиш мақсадида шифрматнни таҳлил қилиш.

Криптотаҳлилчига фақат махфий калитда шифрланган шифрматн маълум бўлиб, шифрлаш алгоритми маълум эмас. Калит ва шифрлаш алгоритми ҳақида маълумотга эга бўлиш мақсадида криптотаҳлилчи шифрматн параметрларини, яъни шифрматн алфавити ёки шифрбелгиларини шифрматнда такрорланишининг сонли характеристикаларини (частоталарини) аниқлаб, очиқ матн қайси тилда ёзилгани, шифрлаш тури, алгоритмни ва калитни аниқлашга ҳаракат қилади.

2. Калит ҳақида маълумотга эга бўлиш мақсадида шифрматнларни таҳлил қилиш.

Криптотаҳлилчига битта k махфий калитда шифрланган $C_1, C_2, \ldots, C_i$ – шифрматнлар ва шифрлаш алгоритми маълум. Криптотаҳлилчининг вазифаси k калитни тиклаш, яъни битта k калит ва E акслантириш (шифрлаш алгоритми) билан $P_1, P_2, \ldots, P_i$ – очиқ матнларга мос шифрматнлар $C_1 = E_k(P_1)$, $C_2 = E_k(P_2), C_3 = E_k(P_3)$, …., $C_i = E_k(P_i)$ маълум бўлса, номаълум бўлган очиқ матнлар: P_1, P_2, ..., P_i ва k – калитни топиш ёки $C_{i+1} = E_k(P_{i+1})$ тенгликдан P_{i+1} очиқ матнни топиш.

3. Калит ҳақида маълумотга эга бўлиш мақсадида очиқ матн билан таҳлил қилиш.

Криптотаҳлилчига махфий калитда шифрланган бир нечта шифрматнлар ва уларга мос очиқ матнлар ҳамда шифрлаш алгоритми маълум.

Қуйидаги очиқ матн ва уларга мос келувчи шифрматн жуфтликлари: $(P_1, C_1 = E_k(P_1))$, $(P_2, C_2 = E_k(P_2))$, $(P_3, C_3 = E_k(P_3)), \ldots,$ $(P_i, C_i = E_k(P_i))$ ҳамда шифрлаш алгоритми маълум бўлганда, k – калитни ёки $C_{i+1} = E_k(P_{i+1})$ тенгликда номаълум бўлган P_{i+1} очиқ матнни топиш.

4. Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган очиқ матн билан таҳлил қилиш.

Криптотаҳлилчига махфий калитда шифрланган шифрматн, шифрлаш алгоритми ва криптотаҳлилчи ўзи танлаб олган очиқ матнлар, яъни ушбу жуфтликлар: $(P_1, C_1 = E_k(P_1)), (P_2, C_2 = E_k(P_2)),$ $(P_3, C_3 = E_k(P_3)), \ldots,$ $(P_i, C_i = E_k(P_i))$ маълум, криптотаҳлил натижаларига қулайлик туғдирувчи хусусиятларга эга бўлган: P_1, P_2, P_3, …, P_i – очиқ матнларни танлаш имконияти мавжуд. Криптотаҳлилчининг вазифаси: k – калитни ёки $C_{i+1} = E_k(P_{i+1})$ тенгликдан P_{i+1} очиқ матнни топиш.

5. Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган шифр матнлар билан таҳлил қилиш.

Криптотаҳлилчида махфий калитда шифрланган бир нечта: $C_1, C_2, \ldots, C_i$ – шифр матнларни танлаш ва уларга мос: $P_1 = D_k(C_1), \ldots, P_i = D_k(C_i)$ – очиқ матнларни ҳам олиш имконияти

мавжуд. Криптотаҳлилчининг вазифаси k – калитни топишдан иборат.

6. *Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган матнлар ёрдамида таҳлил қилиш.*

Криптотаҳлилчига махфий калитда шифрланган шифрматн, шифрлаш алгоритми ва криптотаҳлилчи ўзи танлаб олган бир ёки бир нечта очиқ ва алгоритм ёрдамида шифрланган шифрматн, бир ёки бир неча шифрматн ва алгоритм ёрдамида ҳосил қилинган очиқ матн маълум. Демак $(P_1, C_1 = E_k(P_1))$, $(P_2, C_2 = E_k(P_2))$, ..., $(P_i, C_{i1} = E_k(P_i))$ ва $(C_1, P_1 = D_k(C_1))$, $(C_2, P_2 = D_k(C_2))$,..., $(C_i, P_i = D_k(C_i))$ жуфтликлар маълум. Криптотаҳлилчининг вазифаси k – калитни топиш.

7. Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган калитлар ёрдамида таҳлил қилиш.

Криптотаҳлилчига махфий калитда шифрланган шифрматн ва шифрлаш алгоритми маълум. Криптотаҳлилчи бир нечта калитни танлаб олади ва алгоритм ёрдамида махфий калитга яқин бўлган калитни топади, яъни $(P_1, C_1 = E_{k1}(P))$, $(P_2, C_2 = E_{k2}(P))$, $(P_3, C_3 = E_{k3}(P))$, ..., $(P_n, C_n = E_{kn}(P))$ маълум. Криптотаҳлилчининг вазифаси k_1, k_2, k_3, …, k_n калитларнинг боғликликлари асосида шу шифрлаш алгоритми билан олинган ихтиёрий C – шифрматнни очадиган k – калитни топиш.

Юқорида келтирилган ва бошқа криптотаҳлил турларини криптотаҳлилчи эга бўлган маълумотлар билан боғлиқ ҳолда қуйидаги 1.2.1-жадвал кўринишда бериш мумкин.

1.2.1-жадвал.

Криптотаҳлил турлари

№	Криптотаҳлилчига маълум бўлган маълумотлар	Криптотаҳлил тури
1	1.1) шифрматн.	Калит ва шифрлаш алгоритми ҳақида маълумотга эга бўлиш мақсадида шифрматнни таҳлил қилиш.
2	2.1) шифрматн. 2.2) шифрлаш алгоритми.	Калит ҳақида маълумотга эга бўлиш мақсадида шифрматнни таҳлил қилиш.
3	3.1) шифрматн.	Калит ҳақида маълумотга

1.2.1-жадвалнинг давоми

	3.2) шифрлаш алгоритми. 3.3) очиқ матннинг бир қисми.	эга бўлиш мақсадида очиқ матн билан таҳлил қилиш.
4	4.1) шифрматн. 4.2) шифрлаш алгоритми. 4.3) эга бўлинган бир неча очиқ матнлар ичидан криптотаҳлилчи томонидан танлаб олинган очиқ матн ва алгоритм ёрдамида шифрланган шифрматн.	Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган очиқ матн билан таҳлил қилиш.
5	5.1) шифрматн. 5.2) шифрлаш алгоритми. 5.3) криптотаҳлилчи томонидан танлаб олинган шифрматн ва алгоритм ёрдамида дешифрланган очиқ матн.	Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган шифрматн ёрдамида таҳлил қилиш.
6	6.1) шифрматн. 6.2) шифрлаш алгоритми. 6.3)криптотаҳлилчи томонидан танлаб олинган очиқ матн ва алгоритм ёрдамида шифрланган шифрматн. 6.4) криптотаҳлилчи томонидан танлаб олинган шифрматн ва унга мос келган алгоритм ёрдамида дешифрланган очиқ матн.	Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган матнлар билан таҳлил қилиш.
7	7.1) шифрматн. 7.2) шифрлаш алгоритми. 7.3) ҳар хил калитлар орасидаги боғланишлар мавжуд.	Ҳақиқий калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган калитлар билан таҳлил қилиш.

Демак, криптотаҳлил турларига мувофиқ криптотаҳлилчи томонидан бирор шифрлаш алгоритмини баҳолаш натижасида ушбу шифрлаш алгоритмининг бардошлилиги юзасидан тегишли хулосалар келиб чиқади. Табиийки, алгоритмни бирор ҳужум орқали очиш (дешифрлаш) мумкин бўлса, у ҳолда, алгоритм бардошсиз ҳисобланади. Шу боис, **криптоалгоритмнинг**

криптотаҳлилчи ҳужумларига қарши тура олиш қобилятига "бардошлилик" дейилади.

Криптоалгоритмлар бардошлилик мураккабликларига боғлиқ равишда турли даражадаги муҳофазани таъминлайди. Мазкур ҳолатда очиқ матн ёки калит ҳақидаги маълумотга эга бўлиш имконияти асосий масала ҳисобланади.

Бугунги кунда криптоалгоритмлар бардошлилик хусусиятлари бўйича учта турда таснифланади [25]:

- назарий бардошли криптоалгоритмлар;
- бардошлилиги исботланувчи криптоалгоритмлар;
- бардошлилиги фараз қилинадиган (таъкидланадиган)

криптоалгоритмлар.

Қуйида криптоалгоритмларнинг бардошлилик турлари билан батафсил танишиб чиқамиз.

Назарий бардошли криптоалгоритмлар шундай шифрматнлар ҳосил қиладики, унга мувофиқ очиқ матнларни (ёки калитларни) бир қийматли аниқлаш учун криптотаҳлилчида етарли маълумот мавжуд бўлмайди ёки шифрматн бўйича очиқ матнга эга бўлиш назарий масала ҳисобланади. Ҳеч қандай криптотаҳлил, ҳатто "Калитларни тўлиқ танлаш" усули билан ҳам очиқ матн, калит ёки улар ҳақида керакли маълумотларга эга бўлиш мумкин эмас.

Демак, криптоалгоритмни таҳлил қилиш жараёнида криптотаҳлилчи керакли ҳажмдаги шифрматнларга эга бўлганда ҳам уларга мос очиқ матнларни тиклаш ёки уларга эга бўлиш имконияти мумкин бўлмаса, таҳлил қилинаётган криптоалгоритм назарий бардошли бўлади. Ушбу тоифа криптоалгоритмлар хавфсизлиги унда фойдаланилган сеанс калитни топиш мумкин эмаслигини тасдиқловчи теоремаларга асосланади. Масалан, криптографияда принципиал очилмайдиган шифрлар ҳақида биринчи марта К.Шеннон томонидан фикрлар юритилган бўлиб, "Бир марталик блокнотлар" ушбу тоифа шифрларга мисол бўлади.

Бироқ бу тоифа махфий тизимларни (шифрларни) амалиётда қўллашда ўзига хос муаммоларга дуч келинади. Масалан, фақат бир марталик ва очиқ матн узунлигига тенг бўлган калитларни сақлаш учун катта хажмдаги хотира талаб этилиши ва шу каби бошқа

жиҳатлари мавжуд. Шунинг учун ҳам бундай махфий тизимлар кўпроқ ўта муҳим давлат сирларига эга ахборотларни ҳимоялашда фойдаланилади.

Бардошлилиги исботланувчи криптоалгоритмлар математикада яхши ўрганилган ва унинг ечилиши бир қанча мутахассислар томонидан мураккаб деб топилган масалаларга асосланади.

Ушбу тоифадаги математик мураккаб масалалар қаторига “факторизация”, “дискрет логарифмлаш” кабиларни киритиш мумкин. Бугунги кунда бардошлилиги исботланувчи криптоалгоритмларга эса RSA, Диффи-Хеллман ва улар асосида қурилган бошқа асимметрик алгоритмлар мисол бўла олади.

Мазкур криптоалгоритмлар устунликлари улар асосидаги яхши ўрганилган математик мураккаб масалалар бўлса, камчилиги криптоалгоритмларга тегишли ўзгаритишларни киритиш (масалан қаралаётган мураккаб масаланинг математикада эффектив алгоритми топилса) имкониятларининг чекланганлиги ҳисобланади.

Криптоалгоритмлар асосидаги математик масалалар бардошлиликларини ошириш бевосита қаралаётган масала параметрлари узунликларини ошириш ёки уни тубдан бошқа математик масала мураккаблиги билан ўзгартириш орқали амалга оширилади.

Бардошлилиги фараз қилинадиган (таъкидланадиган) криптоалгоритмлар хусусий математик масалалар мураккабликларига асосланиб, уларни ечиш математикада яхши ўрганилган масалаларга олиб келинмайди.

Ушбу тоифадаги бардошли криптоалгоритмларга мисол сифатида O’zDSt 1105:2009, ГОСТ 28147-89, AES, FEAL ва бошқа симметрик блокли шифрлаш алгоритмларини келтириш мумкин. Демак, бардошлилиги фараз қилинадиган криптоалгоритмлар математикада кам ўрганилган масалалар билан характерланиб, шу каби масалалар бардошликларига асосланар экан.

Мазкур тоифадаги бардошли криптоалгоритмларда бирор заифликлар аниқланса, уларда тегишли ўзгартиришларни умумийликка зарар етказмаган ҳолда ошириш имконияти мавжуд.

Умумий ҳолда криптоалгоритмлар бардошлилиги бўйича аниқланган баҳо (хулоса) ва уларни олиш мураккаб масала бўлиб,

мазкур жараён криптоалгоритм муаллифлари ёки криптотаҳлилчи томонидан амалга оширилиши мумкин.

Демак, криптотаҳлилчи томонидан шундай криптотаҳлил усули таклиф этилсаки, унинг натижасида текширилаётган криптоалгоритм бардошлилик қиймати аввал эълон қилинган мураккаблик қийматидан кичик бўлса, у ҳолда, муаллиф томонидан эълон қилинган криптоалгоритм бардошлилиги рад этилади. Шунинг учун, янги яратилган криптоалгоритмлар амалда очиқ бўлиши ва уни кенг омма мутахассислар томонидан доимий таҳлил қилиниб, таҳлил натижалари бўйича криптоалгоритмлар такомиллаштирилиб борилиши зарур.

Назорат саволлари

1. Криптотаҳлил тушунчаси таърифини келтиринг.

2. Криптографик алгоритмлар заифликлари ва улар синфлари ҳақида маълумот беринг.

3. Замонавий ЭҲМ имкониятлари, дастлабки маълумотлар ва ҳисоблаш ресурслари бўйича криптотаҳлил усуллари амалий аҳамиятини изоҳланг

4. Шифрларнинг айрим криптотаҳлил усулларига бардошлилигини таъминловчи калит узунликлари ҳақида маълумот келтиринг.

5. Криптотаҳлилчи эга бўлган маълумотлар бўйича криптотаҳлил турлари ва уларнинг фарқли жиҳатлари ҳамда хоссалари баён қилинсин.

6. Бадошлилик тушунчасига таъриф беринг.

7. Криптоалгоритмларнинг бардошлилик хусусияти бўйича таснифи келтирилсин.

8. Назарий бардошли криптоалгоритмлар тушунчаси ва уларга мисоллар келтиринг.

9. Бардошлилиги исботланувчи криптоалгоритмлар тушунчаси ва уларга мисоллар келтиринг.

10. Бардошлилиги фараз қилинадиган криптоалгоритмлар тушунчаси ва уларга мисоллар келтиринг.

11. Криптоалгоритм бардошлилиги баҳоси қиймати тушунчаси ва унинг амалий аҳамияти ҳақида маълумот беринг.

12. Замонавий криптотаҳлил усуллари қайси мақсадда қўлланилади?

II. Блокли симметрик шифрлаш алгоритмлари бардошлиликларини криптотаҳлил усуллари ёрдамида баҳолаш

Маълумки, фойдаланувчининг у ёки бу шифрлаш алгоритмидан кутиши мумкин бўлган ҳимояланганликнинг энг максимум самарадорлиги қуйидаги иккита аломатдан ҳеч бўлмаса бирини бажарилиши билан тавсифланади:

1)шифрланган матнни очиш қиймати очилган маълумот қийматидан ошиб кетса;

2)шифрланган матнни очишга кетадиган вақт маълумотнинг ишга яроқлилик муддатидан ошиб кетса.

Шифрлаш алгоритмлари ҳимояланган дейилади, агар у юқорида кўрсатилган иккита талабга мос келса. Бироқ криптотаҳлил жараёнидаги асосий муаммо шундаки, берилган шифрлаш алгоритми ёрдамида ҳосил қилинган шифрматн криптотаҳлили учун керак бўлган ҳаракатларни сонли баҳолаш амалиётда жуда қийин.

Блокли симметрик шифрлаш алгоритмларига нисбатан аввалги бўлимда келтирилган криптотаҳлил турларига асосланиб амалга оширилувчи криптотаҳлилнинг бир нечта усуллари мавжуд бўлиб, улар таркибига қуйидагиларни киритиш мумкин:

– Тўлиқ танлаш усули.

– Акслантиришларни умумий криптографик талабларга текшириш усули.

– Чизиқли криптотаҳлил усули.

– Дифференциал криптотаҳлил усули.

– Чизиқли-дифференциал криптотаҳлил усули.

– Слайдли ҳужум криптотаҳлил усули.

– Интеграл криптотаҳлил усули.

– Алгебраик криптотаҳлил усули.

– Аппарат хатоликларини генерациялашга асосланган криптотаҳлил усули ва ҳоказо.

Қуйида ушбу криптотаҳлил усуллари, уларнинг блокли симметрик шифрлаш алгоритмларига қўлланишлари, шунингдек, улар билан боғлиқ ечилиши лозим бўлган масалалар ҳақида батафсил тўхталамиз.

2.1. Симметрик шифрлаш алгоритми алмаштиришларини умумий криптографик талаблар бўйича баҳолаш

Симметрик шифрлаш алгоритмлари ҳар қандай криптографик алмаштиришларини $GF(2^n)$ фазони $(X=(x_1,x_2,...,x_n))$ бошқа $GF(2^m)$ фазога $(Y=(y_1,y_2,...,y_m))$ акслантириш сифатида қараб, ушбу акслантиришни буль функциялар орқали қуйидагича ифодалаш мумкин [48, 49]:

$$Y=\varphi(X):\ GF(2^n)\to GF(2^m),\ X=(x_1,x_2,...,x_n),\ Y=(y_1,y_2,...,y_m).$$

Акслантириш эса $\varphi(x)=\{f_1(X),f_2(X),...,f_m(X)\}$ – вектор буль функциялар (компоненталар) кўринишида тасвирланади. Бу ерда $f_i,x_i,y_i\in GF(2)$ ($f_i,x_i,y_i=\{0,1\}$).

Демак, блокли симметрик шифрлаш алгоритмидаги бирор криптографик алмаштиришни баҳолаш жараёнида унга математик модел бўлган, берилган буль функция хоссаларини ўрганиш етарли ҳисобланади. Қуйида буль функция ва акслантиришларни баҳолаш учун зарур бўлган айрим математик тушунчалар келтириб ўтилади.

Баланслашганлик ва регулярлик хоссалари

Шифрлаш алгоритмида фойдаланилган криптографик алмаштиришнинг муҳим факторларидан бири бу алмаштиришга мос буль компоненталарнинг “баланслашганлик”, алмаштиришнинг эса “регулярлик” хоссаларини бажариши ҳисобланади. Ушбу шартлар бажарилиши қаралаётган блокли шифрлаш алгоритмига нисбатан статистик криптоҳужум турларини олдини олишга хизмат қилади. Шунинг учун, алгоритмнинг бирор криптографик алмаштиришини таҳлил қилишда ушбу алмаштиришга нисбатан баланслашганлик ва регулярлик хоссаларига текшириш зарурий шартлар сифатида қаралади [32, 48, 49].

2.1.1-таъриф. $f(x),\ x\in GF(2^n)$ – буль функция баланслашган дейилади, агар унинг чинлик жадвалида “0” ва “1” лар сони тенг бўлса, яъни:

$$\#\{x\mid f(x)=0\}=\#\{x\mid f(x)=1\}=2^{n-1}$$

$Y=\varphi(X):\ GF(2^n)\to GF(2^m)$ – акслантириш регуляр дейилади, агар Y – функция чиқишида унинг барча (2^m та) чиқувчи қийматлари 2^{n-m} тадан такрорланса.

Айрим ҳолларда $f(x)$ – буль функцияси ўрнига унга қўшма функция бўлган $f^{\wedge}(x)=1-2\cdot f(x)=(-1)^{f(x)}$ – функцияни кўриш мақсадга мувофиқ бўлади.

Уолш-Адамар алмаштириши

Уолш-Адамар алмаштириши берилган буль функциянинг *баланслашганлик*, *чизиқсизлик* ва *корреляцион иммунитетлик* каби хоссаларини аниқлаш учун хизмат қилиб, бирор блокли симметрик шифрлаш алгоритмининг чизиқли, дифференциал, корреляцион ва бошқа криптотаҳлил усулларига бардошлилигини баҳолашда муҳим бўлган воситалардан бири ҳисобланади [32, 62].

2.1.2-таъриф. $f(x),\ x\in GF(2^n)$ – функциянинг $f^{\wedge}(x)$ – қўшма буль функцияси ва $\alpha\in GF(2^n)$ учун Уолш-Адамар алмаштириши деб: $GF(2^n)\rightarrow Z$, бутун қиймат қабул қилувчи қуйидаги:

$$U^{\wedge}{}_{\alpha}(f)=\sum_{x\in GF(2^n)}(-1)^{f(x)}\cdot(-1)^{<\alpha,x>}=\sum_{x\in GF(2^n)}(-1)^{f(x)\oplus<\alpha,x>} \qquad (2.1.1)$$

чизиқли алмаштиришга айтилади [47]. Бу ерда, $<\alpha,x>=\alpha_1\cdot x_1+\alpha_2\cdot x_2+...+\alpha_n\cdot x_n$ (скаляр кўпайтма), $\alpha=(\alpha_1,\alpha_2,...,\alpha_n)$ – вектор.

Уолш-Адамар алмаштиришига нисбатан $f^{\wedge}(x)$ – қўшма буль функция баланслашган дейилади, агар $\alpha=0=(0,0,...,0)$ бўлганда $U_0^{\wedge}(f)=0$ тенглик ўринли бўлса.

Буль функцияларнинг чизиқсизлик характеристикалари

Қаралаётган шифрлаш алгоритмини чизиқли криптотаҳлил усулига бардошлилигини баҳолашдаги муҳим параметрлардан бири, бу алгоритм акслантиришларининг “чизиқсизлиги” ҳисобланади. Бирор $\varphi(x)=\{f_1(x),f_2(x),...,f_m(x)\}$ акслантиришга нисбатан чизиқсизлик тушунчасини киритишдан аввал буль функция учун чизиқсизлик тушунчаларини бериш зарур.

2.1.3-таъриф. $f(x),\ x\in GF(2^n)$ – буль функциянинг чизиқсизлиги деб, қуйидаги тенглик билан аниқланувчи қийматга айтилади [48, 49]:

$$N(f)=2^{n-1}-\frac{1}{2}\cdot\max_{\forall\alpha\in GF(2^n)}\left|U_{\alpha}^{\wedge}(f)\right| \qquad (2.1.2)$$

2.1.1-тасдиқ. Агар $f(x),\ x \in GF(2^n)$ – буль функция баланслашмаган бўлса, у ҳолда қуйидаги тенгсизлик ўринли [37]:

$$N(f) \le \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1}, & агар\ n - жуфт\ бўлса. \\ \left\lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \right\rfloor, & агар\ n - ток\ бўлса. \end{cases} \quad (2.1.3)$$

Бу ерда $\lfloor \bullet \rfloor$ – белги $(\bullet)$ аргументдан кичик ёки унга тенг бўлган максимал жуфт сонни англатади.

Агар $f(x),\ x \in GF(2^n)$ – буль функция баланслашган бўлса, у ҳолда қуйидаги тенгсизлик ўринли:

$$N(f) \le \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1} - 2, & агар\ n - жуфт\ бўлса. \\ \left\lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \right\rfloor, & агар\ n - ток\ бўлса. \end{cases} \quad (2.1.4)$$

Берилган $f(x),\ x \in GF(2^n)$ – буль функция чизиқсизлик даражасига тескари бўлган тушунча, бу “чизиқлилик” тушунчаси бўлиб, у қуйидагича ифодаланади:

$$L(f) = 1 - \frac{1}{2^{n-1}} N(f), \quad N(f) = 2^{n-1}(1 - L(f)) \quad (2.1.5)$$

бу ерда, $L(f)$ – берилган $f(x)$ буль функциянинг чизиқлилик даражаси.

2.1.4-таъриф. $Y = \varphi(x)$: $GF(2^n) \to GF(2^m)$ – буль (вектор) акслантиришнинг чизиқсизлиги ва чизиқлилиги деб, мос равишда қуйидаги тенгликлар билан аниқланувчи қийматларга айтилади [48, 49]:

$$N(\varphi(x)) = \min_{\substack{c \in GF(2^m) \\ c \ne 0}} N < c, \varphi >,\ L(\varphi(x)) = \max_{\substack{c \in GF(2^m) \\ c \ne 0}} L < c, \varphi > \quad (2.1.6)$$

бу ерда, $\varphi = \{f_1, f_2, ..., f_m\}$, $c = (c_1, c_2, ..., c_m)$, $< c, \varphi >= c_1 f_1(x) + c_2 f_2(x) + ... + c_m f_m(x)$ (яъни, $< c, \varphi >$ – скаляр кўпайтма натижасидаги буль функция).

Буль функцияларнинг корреляцион иммунитетлик даражаси

Корреляцион иммунитетлик даражаси тушунчаси қаралаётган симметрик шифрлаш алгоритмининг статистик ҳужум турларига, яъни кириш блокларининг қайд қилинган (фиксирланган) битлар

учун алмаштиришнинг криптографик баҳосини аниқлашда муҳим элементлардан бири ҳисобланади [49].

2.1.5-таъриф. $f(x),\ x \in GF(2^n)$ – буль функция "k" – даражали корреляцион иммунитетга эга (CI(k) – каби белгиланади, $1 \le k < n$) дейилади, агар $1 \le Wt(\alpha) \le k$ – шартни қаноатлантирувчи барча $\alpha \in GF(2^n)$ векторлар учун $U_{\alpha}^{\wedge}(f) = 0$ ўринли бўлса.

Бу ерда $Wt(\alpha)$ – "α" вектор учун "**Хемминг оғирлиги**" бўлиб, $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ – вектордаги бирлар сонини англатади.

Демак, берилган $f(x)$ – буль функциянинг корреляцион иммунитетлик даражаси "k" га тенг бўлса, у ҳолда $Y = f(x)$ функция қиймати ихтиёрий $x \in GF(2^n)$ – аргумент "k" та компонентида статистик боғлиқсиз ҳисобланади.

Буль функцияларнинг қатъий лавин самарадорлик ва тарқалиш тамойили даражалари

Берилган $f(x),\ x \in GF(2^n)$ – буль функциянинг бир қисм аргументлари ўзгариши (яъни $1 \le k < n$, $x_1, x_2, ..., x_k$ – аргументлар назарда тутилмоқда) натижасида $f(x)$ – буль функция қийматининг ўзгариш эҳтимоллигини баҳолашда тарқалиш тамойили ва қатъий лавин самарадорлик тушунчалари муҳим ўрин тутади. Ушбу тушунчалар ҳам криптографик алмаштиришларни баҳолаш масалалари билан бевосита боғлиқ.

Айтайлик, $\Delta f(x, \beta) = f(x) \oplus f(x \oplus \beta)$, $x, \beta \in GF(2^n)$, $f(x) \in GF(2)$ ўринли бўлсин.

2.1.6-таъриф. $f(x),\ x \in GF(2^n)$ – буль функция қатъий лавин самарадорлик даражасига эга дейилади, агар $Wt(\beta)$=1 бўлган барча β – векторлар учун $\Delta f(x, \beta)$ баланслашган буль функция бўлса.

2.1.7-таъриф. $f(x),\ x \in GF(2^n)$ – буль функция "k" – тартибли қатъий лавин самарадорликка эга (SAC(k) – каби белгиланади) дейилади, агар $f(x)$ – буль функциянинг ихтиёрий "k" та $x_1, x_2, ..., x_k$ – аргументларини фиксирлашдан (0 ёки 1 қиймат билан алмаштиришдан) ҳосил бўлган $f(x)$ – функция қатъий лавин самарадорлик даражасига эга бўлса.

2.1.8-таъриф. $f(x),\ x \in GF(2^n)$ – буль функция “e” – даражали тарқалиш тамойилига эга дейилади, агар Хеминг оғирлиги $1 \le Wt(\beta) \le e$ ораликда бўлган барча $\beta \in GF(2^n)$ - векторлар учун $\Delta f(x,\beta)$ – функция баланслашган буль функция бўлса.

Буль акслантиришларининг алгебраик иммунитети

Блокли симметрик шифрлаш алгоритмларининг бугунги кунда замонавий ва ривожланаётган криптотаҳлил усулларидан бири бўлган алгебраик криптотаҳлил усулига бардошлилигини текширишда муҳим бўлган параметр, бу алгоритм акслантиришларининг “алгебраик иммунитети” ҳисобланади. Мазкур параметр қийматининг юқори бўлиши шифрлаш алгоритмининг алгебраик криптотаҳлил усулига нисбатан бардошли бўлиши учун асос бўлиб хизмат қилади. Ушбу тушунча *f(x)* – буль функциянинг алгебраик чизиқсизлик даражаси билан узвий боғлиқдир.

2.1.9-таъриф. $f(x),\ x \in GF(2^n)$ – буль функция алгебраик чизиқсизлик даражаси (*deg(f)*) деб, унинг АНФ таркибидаги энг юқори даражали бирҳад даражасига айтилади.

2.1.10-таъриф. Айтайлик, бирор $Y = \varphi(x):\ GF(2^n) \to GF(2^m)$ – акслантиришни қаноатлантирувчи буль тенгламалар системаси қуйидагича бўлсин:

$$G = \begin{cases} g_1(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ g_2(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ g_3(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ \ldots \\ g_r(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0. \end{cases} \qquad (2.1.7)$$

$Y = \varphi(x)$ – функциянинг *Алгебраик иммунитети (AI(Y))* деб, (2.1.7) системадаги тенгламаларнинг минимал алгебраик чизиқсизлик даражасига айтилади [43].

Чиқувчи битлар боғлиқсизлиги тамойили

Шифрлаш алгоритми акслантиришларидан чиқувчи қийматларнинг кирувчи қийматлар билан боғлиқлиги ва чиқувчи қийматларнинг ўзаро боғлиқсизлигини кўрсатувчи тамойил “Битлар боғлиқсизлиги тамойили” (Bit Independence Criterion, (BIC)) ҳисобланади [23].

2.1.11-таъриф. $Y=\varphi(x):\ GF(2^n)\to GF(2^n)$ – акслантириш *битлар боғлиқсизлиги тамойилини* қаноатлантиради дейилади, агар ихтиёрий $i,j,k\in\{1,2,3,...,n\},\ j\neq k$ – қийматлар учун, акслантиришга кирувчи *i*-битни инверциялаш (тескарилаш) акслантиришдан чиқувчи *j*- ва *k*-битларнинг ўзаро боғлиқсиз тарзда ўзгаришини тақазо этса.

Акслантиришдан чиқувчи иккита бит боғлиқсизлигини аниқлаш (ўлчаш) учун чиқувчи векторнинг *j*- ва *k*-компоненталари ўртасидаги корреляция коэффициенти $BIC(a_j,a_k)$ дан фойдаланилади:

$$BIC\left(a_j,a_k\right)=\max_{1\le i\le n}\left|corr\left(a_j^{ei},a_k^{ei}\right)\right| \tag{2.1.8}$$

бу ерда, $A^{ei}=\varphi(x)\oplus\varphi(x\oplus ei)=\left[a_1^{ei},a_2^{ei},a_3^{ei},...,a_n^{ei}\right]$, $corr(x,y)=\frac{1}{2^n}\sum_{i=1}^{2^n}(2x_i-1)(2y_i-1)$, $x,y,ei\in GF(2^n)$, ei – *i*-бити 1 га қолган барча битлари 0 га тенг бўлган вектор.

Умумий ҳолда, $Y=\varphi(x)$ – функция учун *BIC* параметр қиймати қуйидагича аниқланади:

$$BIC=\max_{1\le j,k\le n,\ j\neq k}BIC\left(a_j,a_k\right) \tag{2.1.9}$$

Ушбу параметр учун $0\le BIC\le 1$ – ўринли бўлиб, айнан ушбу қиймат $Y=\varphi(x)$ функцияни битлар боғлиқсизлиги тамойилини қанчалик қаноатлантиришини кўрсатади. Яъни агар $BIC=0$ бўлса, чиқувчи битлар максимал боғлиқсизликка эга ва аксинча агар $BIC=1$ бўлса, боғлиқликка эга дейиш мумкин.

Мазкур келтирилган тушунчалардан маълумки, блокли симметрик шифрлаш алгоритми алмаштиришларининг юқорида келтирилган барча хоссалари ва сонли характеристикалари ушбу шифрлаш алгоритмининг криптобардошлилигига ўз таъсирини кўрсатади. Шунга кўра, бирор блокли симметрик шифрлаш алгоритми (ўрнига қўйиш) алмаштиришига нисбатан юқоридаги фикрларни умумлаштирган ҳолда ишлаб чиқилган *умумий криптографик талаблар* қуйида келтирилган [48, 49]:

1. $Y=\varphi(x)=\{f_1(x),f_2(x),...,f_m(x)\}:GF(2^n)\to GF(2^m)$ – акслантиришни ташкил этувчи $f_i(x)$ – буль функцияларининг баланслашган бўлишлиги.

2. $f_i(x)$ – буль функцияларнинг алгебраик чизиқсизлик даражасини ($\deg(f_i)$) – юқори бўлишлиги.

3. $f_i(x)$ – буль функцияларнинг юқори корреляцион иммунитетлик даражаларига эга бўлишлиги;

4. $f_i(x)$ – буль функцияларнинг юқори тартибли қатъий лавин самарадорлик (SAC) ва тарқалиш тамойиллари (PC) кўрсаткичларига эга бўлишлиги.

5. $f_i(x)$ – буль функцияларнинг юқори чизиқсизлик қийматларига $(N(f_i))$ эга бўлишлиги.

6. $\varphi(x)$ – акслантириш учун $N(\varphi(x))$ – қийматнинг катта ва $L(\varphi(x))$ – қийматнинг кичик бўлишлиги.

7. $\varphi(x)$ – акслантириш учун $AI(\varphi(x))$ – қийматнинг катта бўлишлиги.

8. $\varphi(x)$ – акслантириш учун BIC – қийматнинг нолга яқин бўлишлиги.

Криптография амалиёти шуни кўрсатадики, мазкур келтирилган барча талабларни қаноатлантирувчи ягона буль функция ёки акслантиришлар мавжуд эмас. Бунинг сабаби, айрим талабларнинг ўзаро зидлиги (масалан: чизиқсизлик ва корреляцион иммунитетлик тушунчалари ўзаро зид) ҳисобланади. Шу боис, шифрлаш алгоритмлари таркибида у ёки бу талабни қаноатлантирувчи функцияларнинг комбинациясидан фойдаланиш мақсадга мувофиқ.

Таъкидлаш лозимки, блокли симметрик шифрлаш алгоритмлари криптобардошлилигини таъминлашда мазкур келтирилган талаблар зарурий, бироқ етарли ҳисобланмайди. Шунингдек, турли ёндашувдаги криптотаҳлил усулларининг вужудга келиши ушбу криптографик талаблар сонини ошишига ҳам олиб келади.

Қуйида буль функция ва акслантиришларнинг юқорида келтирилган айрим параметрларини ҳисоблаш юзасидан намуналар келтирилган [39]**.**

Айтайлик, $f: GF(2^4) \to GF(2^2)$ – тўрт аргументли акслантириш бўлиб, унинг чинлик жадвали қуйидагича бўлсин.

$$f(x)=\{0,0,0,0,0,0,1,1,0,1,1,1,1,1,0,0,1\}$$

Демак, ушбу функциянинг АНФ кўринишидаги буль функцияси қуйидагича ифодаланади:

$$f(x) = x_1x_3 \oplus x_2x_3 \oplus x_4.$$

Функция чинлик жадвалидаги ноллар сони бирлар сонига тенг бўлганлиги сабабли ушбу буль функция баланслашган ҳисобланади. Алгебраик чизиқсизлик даражаси эса $\deg(f) = 2$ га тенг.

Мазкур буль функциянинг қўшма функциясига нисбатан барча $\alpha \in 2^4$ – векторлар учун Уолш-Адамар алмаштириши қуйидагича ҳисобланади:

$$U^{\wedge}_{\alpha_1}(f) = \sum_{x \in GF(2^4)} (-1)^{f(x) \oplus <\alpha_1, x_1>} = 0,$$

$$U^{\wedge}_{\alpha_2}(f) = 0,\ U^{\wedge}_{\alpha_3}(f) = 0,\ U^{\wedge}_{\alpha_4}(f) = 0,\ U^{\wedge}_{\alpha_5}(f) = 0,\ U^{\wedge}_{\alpha_6}(f) = 0,$$

$$U^{\wedge}_{\alpha_7}(f) = 0,\ U^{\wedge}_{\alpha_8}(f) = 0,\ U^{\wedge}_{\alpha_9}(f) = 8,\ U^{\wedge}_{\alpha_{10}}(f) = 0,\ U^{\wedge}_{\alpha_{11}}(f) = 0,$$

$$U^{\wedge}_{\alpha_{12}}(f) = 8,\ U^{\wedge}_{\alpha_{13}}(f) = 8,\ U^{\wedge}_{\alpha_{14}}(f) = 0,\ U^{\wedge}_{\alpha_{15}}(f) = 0,\ U^{\wedge}_{\alpha_{16}}(f) = -8.$$

бу ерда, $\alpha_1 = (0, 0, 0, 0)$, $\alpha_2 = (0, 0, 0, 1)$, $\alpha_3 = (0, 0, 1, 0)$, $\alpha_4 = (0, 0, 1, 1)$, $\alpha_5 = (0, 1, 0, 0)$, $\alpha_6 = (0, 1, 0, 1)$, $\alpha_7 = (0, 1, 1, 0)$, $\alpha_8 = (0, 1, 1, 1)$, $\alpha_9 = (1, 0, 0, 0)$, $\alpha_{10} = (1, 0, 0, 1)$, $\alpha_{11} = (1, 0, 1, 0)$, $\alpha_{12} = (1, 0, 1, 1)$, $\alpha_{13} = (1, 1, 0, 0)$, $\alpha_{14} = (1, 1, 0, 1)$, $\alpha_{15} = (1, 1, 1, 0)$, $\alpha_{16} = (1, 1, 1, 1)$.

Демак, f – функция учун қуйидаги тенглик ўринли бўлиб, у максимал чизиқсизлик даражасига эга бўлди:

$$N(f) = 2^{4-1} - \frac{1}{2} \cdot \max_{\alpha_i \in GF(2^4)} \left| U^{\wedge}_{\alpha_i}(f) \right| = 2^3 - \frac{1}{2} \cdot 8 = 4.$$

Буль функция учун ҳисобланган корреляцион иммунитетлик даражалари эса қуйидаги жадвалда келтирилган.

2.1.1-жадвал.

f – функциянинг корреляцион иммунитетлик даражалари.

	$1 \le Wt(\alpha) \le k$	$U^{\wedge}_{\alpha}(f)$		$1 \le Wt(\alpha) \le k$	$U^{\wedge}_{\alpha}(f)$		$1 \le Wt(\alpha) \le k$	$U^{\wedge}_{\alpha}(f)$
k=0	0000	0	k=2	1100	8		0000	0
	0000	0		0000	0		0001	0
	0001	0		0001	0		0010	0
k=1	0010	0		0010	0		0011	0
	0100	0		0011	0	k=4	0100	0
	1000	8	k=3	0100	0		0101	0
	0000	0		0101	0		0110	0
k=2	0001	0		0110	0		0111	0
	0010	0		0111	0		1000	8
	0011	0		1000	8		1001	0

2.1.1-жадвалнинг давоми.

	0100	0		1001	0		1010	0
	0101	0		1010	0		1011	8
	0110	0		1011	8		1100	8
	1000	8		1100	8		1101	0
	1001	0		1101	0		1110	0
	1010	0		1110	0		1111	-8

Жадвалда келтирилган қийматлардан маълумки, берилган f – буль функциянинг корреляцион иммунитетлик даражаси нолга тенг.

Қуйида, **ГОСТ 28147-89 шифрлаш алгоритми S_1 – блоки** (ГОСТ Р 34.11-94 стандартида тестлаш учун берилган S_1-блок) буль функция компонентaларининг АНФ кўринишлари ва уларга нисбатан Уолш-Адамар алмаштириши асосида ҳисобланган чизиқсизлик қийматлари келтирилган:

$f_1(x) = x_2 \oplus x_4 \oplus x_3 \oplus x_2x_4 \oplus x_2x_3x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_1x_2x_4$

$U^{\wedge}{}_{\alpha}(f) = \{0, 8, -4, 4, 0, 0, 4, 4, -4, -4, 0, 0, 4, -4, 0, 8\}$

$N(f_1) = 4;$

$f_2(x) = x_4 \oplus x_3 \oplus x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus 1$

$U^{\wedge}{}_{\alpha}(f) = \{0, -4, -4, -8, 4, 0, 0, -4, 4, 0, 0, -4, 0, -4, -4, 8\}$

$N(f_2) = 4;$

$f_3(x) = x_4 \oplus x_2x_4 \oplus x_2x_3x_4 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2x_4$

$U^{\wedge}{}_{\alpha}(f) = \{0, 8, -4, -4, 0, 0, -4, 4, 4, 4, 8, 0, -4, 4, 0, 0\}$

$N(f_3) = 4;$

$f_4(x) = x_3 \oplus x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_3$

$U^{\wedge}{}_{\alpha}(f) = \{0, -4, 0, 4, 4, 0, 4, 8, 8, -4, 0, -4, -4, 0, 4, 0\}$

$N(f_4) = 4.$

Мазкур S_1 – блокнинг $AI(S_1)$ – параметр қийматини аниқлаш учун хизмат қилувчи (2.1.7) ифода кўринишида ҳосил қилинган энг кичик даражали тенгламалар қуйида келтирилган:

1. $y_3 \oplus y_1 \oplus x_4x_3 \oplus x_4x_1 \oplus x_4 \oplus x_3 \oplus x_2 = 0.$
2. $y_4 \oplus y_2 \oplus y_1 \oplus x_4x_3 \oplus x_4x_2 \oplus x_4x_1 \oplus x_2 \oplus 1 = 0.$
3. $x_1y_3 \oplus x_1y_1 \oplus x_4x_2 \oplus x_4x_1 \oplus x_4 = 0.$
4. $x_1y_4 \oplus x_1y_2 \oplus x_1y_1 \oplus x_4x_3 \oplus x_4x_1 \oplus x_4 = 0.$
5. $x_2y_2 \oplus x_1y_2 \oplus x_4x_2 \oplus x_4x_1 \oplus x_4 \oplus x_3x_2 \oplus x_3x_1 \oplus x_3 = 0.$

6. $x_2y_3 \oplus x_1y_2 \oplus x_1y_1 \oplus y_1 \oplus x_4 \oplus x_3x_1 \oplus x_3 \oplus x_2 \oplus x_1 = 0$.

7. $x_2y_4 \oplus x_2y_1 \oplus x_1y_1 \oplus x_4x_3 \oplus x_4x_1 \oplus x_3x_1 = 0$.

8. $x_3y_1 \oplus x_2y_1 \oplus x_1y_1 \oplus y_1 \oplus x_4x_1 \oplus x_3x_1 \oplus x_2x_1 \oplus x_1 = 0$.

9. $x_3y_2 \oplus x_2y_1 \oplus x_1y_2 \oplus y_2 \oplus y_1 \oplus x_4x_1 \oplus x_4 \oplus x_3x_2 \oplus x_3x_1 \oplus x_2x_1 \oplus 1 = 0$.

10. $x_3y_3 \oplus x_2y_1 \oplus x_1y_1 \oplus y_2 \oplus x_4x_3 \oplus x_4x_1 \oplus x_3x_2 \oplus x_3 \oplus x_2 \oplus x_1 \oplus 1 = 0$.

11. $x_3y_4 \oplus x_1y_2 \oplus x_1y_1 \oplus y_1 \oplus x_4x_3 \oplus x_4 \oplus x_3x_2 \oplus x_3x_1 \oplus x_3 \oplus x_2x_1 \oplus x_1 = 0$.

12. $x_4y_1 \oplus x_1y_2 \oplus x_1y_1 \oplus y_2 \oplus x_4x_2 \oplus x_4 \oplus x_2 \oplus 1 = 0$.

13. $x_4y_2 \oplus x_2y_1 \oplus x_1y_1 \oplus y_2 \oplus y_1 \oplus x_4x_2 \oplus x_4x_1 \oplus x_3x_2 \oplus x_3x_1 \oplus x_2x_1 \oplus 1 = 0$.

14. $x_4y_3 \oplus x_2y_1 \oplus y_2 \oplus y_1 \oplus x_4x_2 \oplus x_3x_2 \oplus x_2x_1 \oplus x_1 \oplus 1 = 0$.

15. $x_4y_4 \oplus x_2y_1 \oplus x_1y_1 \oplus y_2 \oplus x_4x_3 \oplus x_3x_2 \oplus x_3 \oplus x_2x_1 \oplus x_2 \oplus x_1 \oplus 1 = 0$.

16. $y_1y_2 \oplus y_2 \oplus y_1 \oplus x_4x_2 \oplus x_3x_2 \oplus x_2x_1 \oplus 1 = 0$.

17. $y_1y_3 \oplus x_2y_1 \oplus x_1y_2 \oplus x_1y_1 \oplus y_1 \oplus x_4 \oplus x_3x_2 \oplus x_2x_1 \oplus x_2 = 0$.

18. $y_1y_4 \oplus x_2y_1 \oplus x_1y_2 \oplus x_1y_1 \oplus y_1 \oplus x_4x_3 \oplus x_4x_2 \oplus x_4x_1 \oplus x_4 \oplus x_3x_2 \oplus x_3 \oplus x_2x_1 \oplus x_1 = 0$.

19. $y_2y_3 \oplus x_2y_1 \oplus y_2 \oplus y_1 \oplus x_4x_1 \oplus x_4 \oplus x_3x_2 \oplus x_3x_1 \oplus x_2x_1 \oplus 1 = 0$.

20. $y_2y_4 \oplus x_2y_1 \oplus x_4x_3 \oplus x_3x_1 = 0$.

21. $y_3y_4 \oplus x_2y_1 \oplus x_1y_2 \oplus x_1y_1 \oplus y_2 \oplus x_4x_2 \oplus x_4x_1 \oplus x_4 \oplus x_3x_2 \oplus x_3 \oplus x_2x_1 \oplus x_2 \oplus x_1 \oplus 1 = 0$.

Ушбу аниқланган барча тенгламалар учун $deg=2$ тенглик ўринли бўлганлигидан $AI(S_1)=2$ тенглик келиб чиқади.

Қуйидаги 2.1.2 ва 2.1.3 - жадвалларда эса, **ГОСТ 28147-89 алгоритмининг барча S-блокларини** умумий криптографик талаблар бўйича баҳолаш натижалари келтирилган.

2.1.2-жадвал.

S_1 - S_4 – блокларнинг талаблар бўйича баҳолаш натижалари

Баҳолаш параметрлари	**S_1-блок**				**S_2-блок**				**S_3-блок**				**S_4-блок**			
	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4
баланслanганлик	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
регулярлик	+				+				+				+			
deg(f)	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
N(f)	4	4	4	4	4	4	4	4	4	4	4	4	2	4	2	4
N(S)	4				2				2				2			
CI(f)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SAC(f)	2	2	2	0	2	0	2	2	2	2	0	2	4	2	2	2
AI(S)	2				2				2				2			

2.1.3-жадвал.

S_5 – S_8 - блокларнинг талаблар бўйича баҳолаш натижалари

Баҳолаш параметрлари	**S_5-блок**				**S_6-блок**				**S_7-блок**				**S_8-блок**			
	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4
баланслanганлик	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
регулярлик	+				+				+				+			
deg(f)	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
N(f)	4	4	4	4	4	4	2	4	4	4	4	2	4	4	4	4
N(S)	2				2				2				2			
CI(f)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SAC(f)	0	2	2	2	2	2	4	2	2	2	0	2	2	2	2	2
AI(S)	2				2				2				2			

Келтирилган натижалар шуни кўрсатадики, *N(S)* – параметр қийматига кўра ГОСТ 28147-89 алгоритми фақат S_1-блок жадвали максимал, *AI(S)* – параметр қийматига кўра эса барча S-блок жадваллари максимал кўрсаткичга эга бўлди.

AES шифрлаш алгоритми SubBytes – акслантиришини (S-блок) умумий талаблар бўйича баҳолаш натижалари қуйидаги 2.1.4-жадвалда келтирилган.

2.1.4-жадвал.

SubBytes – акслантиришини талаблар бўйича баҳолаш натижалари

Баҳолаш параметрлари	**Sub Bytes**							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
баланслашганлик	+	+	+	+	+	+	+	+
регулярлик	+							
deg(*f*)	7	7	7	7	7	7	7	7
N(*f*)	112	112	112	112	112	112	112	112
N(*S*)	112							
CI(f)	0	0	0	0	0	0	0	0
SAC(f)	6	8	8	8	8	6	6	6
AI(S)	2							

Маълумки, 8 аргументли баланслашган буль функция учун *deg*(*f*)=7, S-блок учун эса *N*(*S*)=112 ва *AI(S)*=3 қийматлар бўлиши мумкин бўлган максимал кўрсаткичлар ҳисобланади. AES алгоритмига нисбатан келтирилган натижалар шуни кўрсатадики, *SubBytes* акслантириши *deg*(*f*) ва *N(S)* параметрлар қийматига кўра максимал бўлиб, *AI(S)* – параметр қийматига кўра максимал эмас.

LOKI шифрлаш алгоритми S – блок жадвалини умумий талаблар бўйича таҳлил натижалари эса қуйидаги 2.1.5-жадвалда келтирилган.

2.1.5-жадвал.

S – блок жадвалининг талаблар бўйича баҳолаш натижалари

Баҳолаш параметрлари	**S – блок (LOKI)**							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
баланслашганлик	+	+	+	+	+	+	+	+
регулярлик	+							
deg (*f*)	11	11	11	10	10	10	11	11
N (*f*)	1770	1838	1856	1812	1872	1888	1902	1850
N (*S*)	1728							
CI(f)	0	0	0	0	0	0	0	0
SAC(f)	334	446	458	496	448	316	506	698

DES алгоритми S – блокларини умумий криптографик талаблар бўйича баҳолаш натижалари қуйидаги 2.1.6-жадвалда келтирилган.

2.1.6-жадвал.

S_1-S_8 – блок жадвалларининг талаблар бўйича баҳолаш натижалари

Баҳолаш параметрлари	**S_1**	**S_2**	**S_3**	**S_4**	**S_5**	**S_6**	**S_7**	**S_8**
deg (f_i)	5	5	5	4	5	4	5	5
N(*S*)	14	16	16	16	12	18	14	16
SAC(f)	8	14	12	6	10	10	12	10

Келтирилган натижалар шуни кўрсатадики, LOKI алгоритми S-блокини ифодаловчи буль функциялар ҳамда DES алгоритми S-блоклари *deg*(*f*) ва *N*(*S*) – параметрлар қийматларига кўра турли кўрсаткичларга эга.

Умумий ҳолда, бирор симметрик шифрлаш алгоритми алмаштиришларини текширишдан олинган натижаларни *deg*(*f*), *N*(*S*), *CI*(*S*) ва *AI(S)* параметрлари бўйича максимал кўрсаткичга қанчалик мос ёки унга яқин эканлигини баҳолашда қуйидаги 2.1.7-жадвалда келтирилган қийматлардан фойдаланиш мумкин (тавсия этилади) [39, 43].

2.1.7-жадвал.

Криптографик параметрларнинг максимал қийматлари

Параметрлар	**Алмаштириш аргументлари сони**					
	4	**5**	**6**	**8**	**12**	**16**
deg(*f*)	3	4	5	7	11	15
N(*S*) (*S-регуляр*)	4	12	24	112	1984	32512
N(*S*) (*S-регуляр эмас*)	6	12	28	120	2016	32640
CI(*f*)	3	4	5	7	11	15
AI(S)	2	2	2	3	4	5

Умумий ҳолда, янги таклиф этилган ёки мавжуд стандарт блокли симметрик шифрлаш алгоритми акслантиришларини криптографик талаблар бўйича баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида алгоритм **бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.1.8-жадвал.

Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Иш хулосаси
I.	Акслантиришларнинг кириш ва чиқиш битларига мос чинлик жадвалларини тузиш	Чинлик жадвалини амалий қуриш мумкин	Кейинги босқичга ўтиш мумкин
		Чинлик жадвалини амалий қуриб бўлмайди	Текширилаётган акслантиришни чинлик жадвали асосида баҳолаб бўлмайди
II.	Акслантиришларнинг мос буль функция компоненталари учун АНФлар қуриш ва уларнинг $deg(f_i)$ – параметр қийматларини аниқлаш	$deg(f_i)$ – қиймати максимал (ёки унга яқин)	Кейинги босқичга ўтиш мумкин
		$deg(f_i)=1$	Текширилаётган акслантиришдан шифрлаш алгоритми таркибида чизиқсиз акслантириш сифатида фойдаланиб бўлмайди
III.	Акслантиришлар (буль компоненталари) учун *регулярлик* (*балансланганлик*) хоссасини текшириш	Регуляр (балансланган)	Кейинги босқичга ўтиш мумкин
		Регуляр (балансланган) эмас	Текширилаётган акслантириш заифликка эга бўлиб, ундан шифрлаш алгоритми таркибида фойдаланиш мақсадга мувофиқ эмас
IV.	Акслантиришлар мос буль функция компоненталари учун $CI(f_i)$ – параметр қийматини аниқлаш	$CI(f_i)$ – қиймати максимал (ёки унга яқин)	Текширилаётган акслантиришдан шифрлаш алгоритми таркибида чизиқсиз акслантириш сифатида фойдаланиб бўлмайди
		$CI(f_i)=0$	Кейинги босқичга ўтиш мумкин
V.	Акслантиришлар (буль компоненталари) учун $N(\varphi(x))(N(f_i))$ – параметр қийматини аниқлаш	$N(\varphi(x))(N(f_i))$ – қиймати максимал (ёки унга яқин)	Кейинги босқичга ўтиш мумкин
		$N(\varphi(x))=0$ $(N(f_i)=0)$	Текширилаётган акслантиришдан шифрлаш алгоритми таркибида чизиқсиз акслантириш сифатида фойдаланиб бўлмайди

2.1.8-жадванинг давоми.

VI.	Акслантиришлар мос буль функция компоненталари учун $SAC(f_i)$ – параметр қийматини аниқлаш	$SAC(f_i)$	Кейинги босқичга ўтиш мумкин
VII.	Акслантиришлар учун $AI(\varphi(x))$ – параметр қийматини аниқлаш	$AI(\varphi(x))$ – қиймати максимал (ёки унга яқин)	Кейинги босқичга ўтиш мумкин
		$AI(\varphi(x))=1$	Текширилаётган акслантиришдан шифрлаш алгоритмини алгебраик криптотаҳлил усулига бардошлиликни таъминловчи акслантириш сифатида фойдаланиб бўлмайди
VIII.	**Якуний хулоса**	Юқорида олинган криптографик талаблар натижалари асосида алгоритм криптобардошлиги юзасидан хулоса чиқариш – барча кўрсаткичларни умумлаштирган ҳолда амалга оширилади. Агар барча криптографик талаблар алгоритмнинг мос равишда бирор акслантириши орқали максимал (ёки унга яқин) бажарилса, у ҳолда, "*алгоритм криптобардошли бўлиши мумкин"* деб, аксинча, айрим талабларни қаноатлантирувчи бирорта ҳам акслантириш мавжуд бўлмаса "*алгоритм заифликка эга (криптобардошсиз) бўлиши мумкин*" деб хулоса чиқариш мақсадга мувофиқ.	

Таъкидлаш лозимки, криптографик талабларга мос параметр қийматларини амалий ҳисоблаш имконияти блокли симметрик шифрлаш алгоритмлари учун муҳим аҳамият касб этади. Агарда, акслантиришларни умумий криптографик талабларга текширишнинг амалий имконияти мавжуд бўлмаса, у ҳолда, шифрлаш алгоритми акслантиришининг бардошлилиги ёки бардошсизлиги юзасидан хулоса чиқариш нотўғри ҳисобланади.

Назорат саволлари

1. Умумий криптографик талабларни сананг ва уларнинг ҳар бирини шифр бардошлилигига таъсирини тушунтиринг.

2. Ўзаро зид бўлган талабларни сананг ва ушбу зиддиятни изоҳланг.

3. Умумий криптографик талабларни қаноатлантирувчи акслантиришлар шифрлаш алгоритми криптобардошлилигини тўлиқ таъминлаш учун етарлими?

4. Текширилаётган акслантириш ўлчами умумий криптографик талабларга текшириш мураккаблигига қандай таъсир кўрсатади?

5. Тасодифий ишлаб чиқилган акслантиришларни умумий криптографик талабларни қаноатлантиришдаги ўрнини изоҳланг.

6. Тасодифий ишлаб чиқилган акслантиришлар ўлчамининг умумий криптографик талабларни қаноатлантиришдаги ўрни қандай?

7. ГОСТ 28147-89 шифрлаш алгоритми S-блокларини умумий криптографик талабларга текшириш натижалари баён қилинсин.

8. DES шифрлаш алгоритми S-блокларининг умумий криптографик талабларга текшириш натижаларини баён қилинг.

9. AES шифрлаш алгоритми S-блокининг умумий криптографик талабларга текшириш натижаларини баён қилинг.

10.DES, ГОСТ 28147-89 ва AES алгоритмлари S-блокларини умумий криптографик талабларга текшириш натижалари бўйича ўзаро фарқларини баён қилинг.

2.2. Чизиқли криптотаҳлил усули

Чизиқли криптотаҳлил усули Япониялик криптограф M.Matsui томонидан 1993 йилда DES шифрлаш алгоритмига қарши ҳужум тури сифатида ишлаб чиқилган [28]. Мазкур усул кейинчалик, FEAL, SAFER, RC2 алгоритмларга ҳам қўлланилиб, тегишли натижалар олинган.

M.Matsui томонидан DES алгоритми турли раундларига мазкур криптотаҳлил усулини қўллаш орқали аниқланган натижалари қуйидаги 2.2.1-жадвалда келтирилган [33].

2.2.1-жадвал.

DES алгоритмининг чизиқли криптотаҳлил натижалари

Раундлар сони	Раунд калитини топиш учун керак бўладиган очиқ матнлар сони
8	2^{21}
12	2^{33}
16	2^{47}

Чизиқли криптотаҳлил усулида шифрлаш алгоритми ва унга

мос танлаб олинган очиқ матн ва шифр матн жуфтликлари маълум деб олинади. Криптотаҳлилчининг вазифаси қуйидаги:

$$X[i_1,i_2,...,i_n]\oplus Y[j_1,j_2,...,j_m]=K[k_1,k_2,...,k_p],\ \text{бу ерда,}$$
$$X[i_1,i_2,...,i_n]=X[i_1]\oplus X[i_2]\oplus....\oplus X[i_n]$$
$$Y[j_1,j_2,...,j_m]=Y[j_1]\oplus Y[j_2]\oplus....\oplus Y[j_m] \qquad (2.2.1)$$
$$K[k_1,k_2,...,k_p]=K[k_1]\oplus K[k_2]\oplus....\oplus K[k_p]$$

тенгликдан энг яқин (тўғри) чизиқли аппроксимацияни аниқлаш, яъни таҳлил қилинаётган алгоритм акслантиришлари хоссаларидан келиб чиқиб, энг самарали натижа берувчи чизиқли боғланишни танлашдан иборат. Танланган аппроксимация тенгламаларида тенгликнинг чап томони, яъни $X[i_1,i_2,...,i_n]\oplus Y[j_1,j_2,...,j_m]$ нинг қиймати 0 ёки 1 эканлигини аниқлаш учун етарлича кўп миқдордаги очиқ матн ва шифр матн жуфтликлари устида статистик таҳлил олиб бориш керак. Натижада, фақат калит битлари иштирок этган тенгламалар системаси ҳосил бўлади.

Амалиётда фойдаланилган калит битларини тўлиқ ёки кўпроқ қисмини аниқлаш учун мазкур тенгламадан бир нечтасини қуриш ҳамда улар ёрдамида ҳосил қилинган тенгламалар системасини ечиш талаб этилади. Шунга мувофиқ, чизиқли криптотаҳлил усулини ўтказишда криптотаҳлилчи асосий вазифаси сифатида қуйидагиларни келтириш мумкин:

1. Эффектив чизиқли боғланишни аниқлаш.
2. Статистик таҳлил олиб бориш асосида фақатгина калит битлари орқали ифодаланувчи тенгламалар системасини қуриш.
3. Тенгламалар системасини ечиш орқали калит битларини аниқлаш.

Эффектив чизиқли боғланишни аниқлашда шифрлаш алгоритми таркибида фойдаланилган чизиқсиз акслантиришлар хусусиятлари муҳим ўрин тутади. Бугунги кунда мавжуд аксарият блокли симметрик шифрлаш алгоритмлари таркибида чизиқсиз акслантириш сифатида S – блок жадвалидан фойдаланилган. S – блок жадвалига нисбатан чизиқли аппроксимация тенгламаларини тузишда “корреляцион матрица” жадвалидан фойдаланиш самарали ҳисобланиб, айнан ушбу жадвал чизиқли криптотаҳлилнинг асосий характеристикаси ҳисобланади [33].

Корреляцион матрица. S – блок учун эффектив аппроксимация тенгламасини тузиш

Айтайлик, $Y=\varphi(X):\ GF(2^n)\to GF(2^m)$ – шифрлаш алогоритмида фойдаланилган бирор чизиқсиз акслантириш бўлсин. Яъни $X=(x_1,x_2,...x_n)$ – акслантиришга кирувчи битларни, $Y=(y_1,y_2,...y_m)$ – акслантиришдан чиқувчи битларни ифодалайди.

2.2.1-таъриф. $Y=\varphi(X)$ – акслантиришга нисбатан корреляцион матрица деб, ҳар бир (i,j) - элементи қуйидаги тенглик билан аниқланувчи C – жадвалга айтилади:

$$C(i,j)=\#\{X\,|\langle X,i\rangle=\langle Y,j\rangle\} \qquad (2.2.2)$$

Бу ерда, $i\in 2^n$, $j\in 2^m$ $\langle X,i\rangle=x_1i_1\oplus x_2i_2\oplus\ldots\oplus x_ni_n$, $\langle Y,j\rangle=y_1j_1\oplus y_2j_2\oplus\ldots\oplus y_mj_m$.

Таърифдан корреляцион матрица акслантиришга кирувчи ва чиқувчи битлар ҳар хил позициялари (ўринларининг) ўзаро боғланишларини, яъни кирувчи i – битларни XOR амали ёрдамида йиғиндисининг чиқувчи j – битларни XOR амали ёрдамида йиғиндисига неча марта тенг бўлишини ифодалайди.

Қуйида DES шифрлаш алгоритми S_6 – блоки учун корреляцион матрица ва у асосида эффектив аппроксимация тенгламаларини тузишга намуна келтирилган.

Маълумки, DES шифрлаш алгоритми таркибида 8 та $Y=S(X)$: $GF(2^6)\to GF(2^4)$, S-блок жадвалидан фойдаланилган. 2.2.2-жадвалда қаралаётган S_6-блок берилган.

2.2.2 – жадвал.

DES алгоритмнинг S_6 – блоки

S_6	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***	***16***
1	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
2	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
3	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Ушбу S_6 – блокка нисбатан (2.2.2) ифода орқали ҳосил қилинган корреляцион матрица жадвали қуйидагича шаклланади (2.2.3-жадвал).

2.2.3-жадвал.

DES алгоритми S_6 – блоки учун корреляцион матрица

C(i,j)		j														
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
i	**1**	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
	2	32	32	32	34	26	34	26	34	38	30	34	28	32	32	36
	3	32	32	32	30	30	30	30	30	26	34	30	36	40	32	36
	4	32	34	30	34	30	40	32	34	34	32	36	36	40	38	30
	5	32	38	26	34	38	36	28	30	30	24	36	40	36	30	22
	6	36	30	30	32	32	34	30	32	32	30	34	24	36	34	34
	7	28	34	34	36	28	34	30	32	32	34	30	36	32	26	34
	8	34	30	32	28	30	30	24	34	32	40	38	38	28	32	30
	9	30	38	36	32	38	34	32	30	32	36	38	30	32	32	42
	10	34	34	36	34	36	24	34	32	34	30	32	26	28	36	30
	11	30	26	40	34	32	40	30	32	30	22	36	34	32	28	34
	12	30	32	34	34	28	34	40	28	30	32	30	30	28	34	36
	13	34	36	34	30	28	34	36	36	34	28	30	34	44	42	32
	14	34	32	38	28	34	28	30	30	32	30	28	26	40	34	36
	15	30	36	30	28	38	32	30	34	32	30	32	30	32	34	32
	16	34	32	30	32	34	28	**18**	28	30	28	26	32	34	20	42
	17	34	32	30	36	30	40	38	28	30	28	26	36	30	32	30
	18	34	32	30	30	32	34	24	26	40	30	40	28	34	36	30
	19	34	32	30	30	32	26	32	30	36	26	28	32	30	40	42
	20	30	34	32	34	28	28	30	30	28	28	34	28	30	26	28
	21	38	30	28	38	24	28	30	34	40	36	26	28	38	30	32
	22	26	38	32	36	34	26	32	32	30	30	36	32	34	30	32
	23	26	34	36	28	34	30	36	32	38	26	32	32	34	26	36
	24	32	30	34	32	32	30	34	30	34	36	28	34	30	32	32
	25	20	30	22	24	28	38	30	26	26	40	28	30	38	36	32
	26	40	34	30	34	34	28	32	32	24	38	34	30	30	28	32
	27	28	34	34	38	34	32	32	24	36	30	30	34	30	32	32
	28	32	32	32	30	26	34	30	32	28	36	40	34	26	34	34
	29	36	36	32	30	22	30	30	32	24	24	32	34	30	30	26
	30	36	40	28	28	28	32	32	30	34	30	26	38	30	34	34
	31	32	28	36	32	28	32	36	34	34	30	30	30	34	30	34
	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32

2.2.3-жадванинг давоми.

	33	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
	34	36	32	28	30	34	30	42	34	26	30	**46**	32	32	34	44
	35	36	32	28	34	30	34	38	30	30	34	26	32	32	28	36
	36	32	30	34	30	34	32	24	30	30	32	28	36	32	42	34
	37	32	34	30	30	26	28	36	34	34	32	36	32	36	26	34
	38	40	34	38	32	36	38	38	28	32	38	30	36	36	26	30
	39	32	38	42	28	24	30	30	20	40	34	34	32	32	34	30
	40	34	34	28	32	34	30	32	30	36	32	30	38	20	36	34
	41	30	34	40	36	26	26	32	34	28	28	30	38	32	36	30
	42	38	30	36	34	32	28	34	28	26	30	28	30	36	36	34
	43	34	30	32	42	36	28	30	36	30	38	32	38	40	36	30
	44	30	40	26	34	36	34	32	36	30	32	22	30	28	34	24
	45	34	36	34	30	36	26	36	28	34	36	30	34	28	34	24
	46	38	24	26	32	26	32	30	38	36	30	32	38	32	30	36
	47	34	36	42	24	38	36	30	42	36	38	28	34	32	30	32
	48	34	32	30	32	34	36	26	32	34	32	30	28	30	40	30
	49	34	32	30	36	30	32	30	32	34	32	30	32	26	36	34
	50	30	32	34	34	24	30	32	30	24	34	32	20	30	36	26
	51	30	32	34	26	32	30	32	34	36	30	36	32	34	32	30
	52	30	30	36	30	32	28	30	30	28	32	30	40	34	34	36
	53	22	42	32	34	28	28	30	42	32	32	30	32	34	30	32
	54	22	26	32	28	38	30	32	32	26	26	28	32	30	34	32
	55	38	38	36	28	30	42	28	24	26	30	32	32	30	30	36
	56	32	26	38	36	36	30	26	30	26	40	32	30	34	32	32
	57	36	34	34	28	32	30	30	34	26	28	32	34	34	36	32
	58	36	38	30	26	30	24	32	32	28	34	34	38	34	32	32
	59	40	30	26	22	38	28	32	32	32	26	30	26	34	28	24
	60	32	32	32	30	34	34	38	28	32	32	28	30	38	30	30
	61	36	28	40	30	30	38	30	44	28	28	28	30	26	34	30
	62	32	24	32	40	36	28	32	26	34	26	34	38	34	34	30
	63	28	20	32	20	28	28	36	30	34	34	30	38	30	30	30

Мазкур жадвал қийматларидан i=6 (000110_2) ва j=1 (0001_2) бўлганда $C(6,1)$=36 тенглик ўринли. Бу эса, (2.2.2) тенгликка мувофиқ, S – блокка кирувчи барча қийматларнинг қайсидир 36 тасида $\langle (x_1, x_2, x_3, x_4, x_5, x_6), (000110) \rangle = x_4 \oplus x_5$ – тенглик қийматини $\langle (y_1, y_2, y_3, y_4), (0001) \rangle = y_4$ – тенглик қиймати билан бир хил бўлишини

англатади. Демак, $x_4 \oplus x_5 = y_4$ – аппроксимация тенгламаси бажарилиш эҳтимоллиги $p = \frac{36}{64} = 0.5625$, унинг четланиши эса $\Delta = |1 - 2 * p| = 0.125$. Корреляцион матрица барча қийматларини таҳлил қилиш орқали аниқлаш мумкинки, DES шифрлаш алгоритми S_6 – блокига нисбатан қуйидаги аппроксимация тенгламалари энг эффектив тенгламалар ҳисобланади (2.2.4-жадвал).

2.2.4-жадвал.

S_6 – блок учун эффектив аппроксимация тенгламалари

№	*(i, j)*	*C(i,j)*	Тенгламалар	Эҳтимоллик қиймати (*p*)	Четланиш қиймати (Δ)
1	(16,7)	18	$x_2 = y_2 \oplus y_3 \oplus y_4$	0,2813	0,4375
2	(34,11)	46	$x_1 \oplus x_5 = y_1 \oplus y_3 \oplus y_4$	0,7188	0,4375

Кўриш мумкинки, ҳосил бўлган биринчи тенглама бажарилиш эҳтимоллиги нолга яқин, бироқ ушбу тенглик ихтиёрий қисмига “1” – қийматни XOR амали ёрдамида қўшиш орқали *p*=0,7188 эҳтимоллиги билан бажарилувчи тенгликка эга бўлинади (масалан,: $x_2 = y_2 \oplus y_3 \oplus y_4 \oplus 1$).

DES алгоритми қолган S – блоклари ва ихтиёрий шифрлаш алгоритми S – блокларига нисбатан корреляцион матрицалар ва улар асосида эффектив аппроксимация тенгламаларини қуриш ҳам юқорида баён қилинган кетма-кетликда амалга оширилади. Тенглама учун четланиш қиймати қанчалик юқори бўлса, криптотаҳлил усули эффективлиги ҳам шу қадар юқори бўлади.

Демак, шифрлаш алгоритмларида фойдаланилган S-блок акслантиришларига нисбатан қурилган корреляцион матрица қийматига қараб, ушбу алгоритм чизиқли криптотаҳлил усулига бардошли ёки бардошсиз эканлиги ҳақида дастлабки хулосаларни айтиш мумкин.

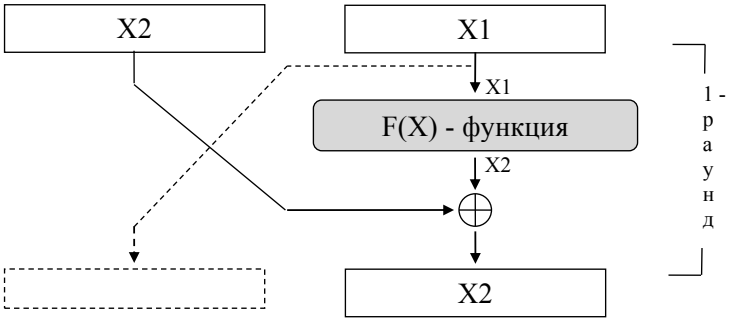
Фейстель тармоғига асосланган шифрлаш алгоритми учун аппроксимация тенгламасини тузиш

Юқорида таъкидландики, чизиқли криптотаҳлил усулининг асосий моҳияти мос очиқ ва шифр матн битлари ҳамда фойдаланилган калит битлари ўртасидаги ўзаро юқори эҳтимолликда бажарилувчи боғланишларни аниқлашдан иборат. Шунга кўра, эффектив боғланишларни (аппроксимация тенглама-

ларини) қуришга таъсир этувчи омиллардан бири, бу шифрлаш алгоритмининг қандай тармоққа асосланганидир.

Қуйида Фейстель тармоғига асосланган шифрлаш алгоритмлари ҳар хил раундлари учун очиқ матн, шифр матн ва калит битларини боғловчи чизиқли боғланишларни аниқлаш усуллари келтирилади.

Дастлаб битта раунд учун чизиқли боғланишларни аниқлаш жараёнини кўриб ўтамиз. Маълумки, Фейстель тармоғи моҳиятига асосан шифрлаш алгоритмига кирувчи блок иккита L_0 ва R_0 қисмларга ажралади. Кузатишларни раунд функциясига кирувчи қисм ҳисобланган, R_0 – ўнг қисмдан бошлаймиз. 2.2.1-расмда ифодаланганидек, R_0 – ўнг қисмнинг чизиқли боғланишда иштирок этувчи битлар позициясини шартли равишда X1 - деб белгилаймиз.



2.2.1-расм. 1 та раунд учун чизиқли боғланишларни аниқлаш схемаси.

Умумий ҳолда, боғланишда иштирок этувчи битлар позициясининг мумкин бўлган вариантлари қуйидагича:

$$X \in \{\{0,0,0,\ldots,0\}, \{0,0,0,\ldots,0,1\},..., \underbrace{\{1,1,1,\ldots,1\}}_{N/2}\} \qquad (2.2.3)$$

Бу ерда, “1” - қиймат ўзининг жойлашган тартиб рақамига мос келувчи битнинг чизиқли боғланишда иштирок этишини, “0” эса, аксинча, иштирок этмаслигини билдиради. *N* – алгоритмга кирувчи битлар сони (масалан 64,128 ва ҳ.к.).

X1 битлар позицияси раунд функциясига кириб, чиқишда маълум бир X2 битлар позициясига аксланади. Шу билан бирга, раунд функциясига асосан фойдаланилган раунд калитининг чизиқли боғланишда иштирок этадиган битлари ҳам аниқланади.

Фейстель тармоғига асосан 1-раунд функциясидан чиқувчи битларга L_0 – чап қисмнинг мос битлари XOR амали ёрдамида қўшилиб, натижада, R_1 – ўнг қисм ҳосил қилинади. Шунга асосан ҳамда 1-рауннддан чиқувчи X2-битлар позициясини билган ҳолда, L_0 ва R_1 ларнинг X2-битлар позицияларини чизиқли боғланишда иштирок этиши маълум бўлади. 2.2.1-расмда тасвирланганидек, 1-рауннддан чиқувчи L_1 – чап қисмнинг ҳеч қайси бити ҳосил қилинган чизиқли боғланишда иштирок этмайди.

Кейинги схемаларни изоҳлашда осонлик бўлиши учун қуйидаги белгилашларни киритамиз:

$L_{i-1,}\ R_{i-1}$ – i-раундга кирувчи чап ва ўнг қисмлар;

$L_{i,}\ R_i$ – i-рауннддан чиқувчи чап ва ўнг қисмлар;

F(X) – раунд функциясига мос равишда битлар позициясини акслантирувчи функция;

L_i [X] – L_i – қисмнинг X – позициясида жойлашган битларини XOR амали бўйича йиғиндиси. X - битлар позицияси (2.2.3) да ифодаланган. Масалан, L [001010]= $L_3 \oplus L_5$.

K_i [$X^{(K)}$] – i-раунд калитининг $X^{(K)}$ – позициясида жойлашган битларини XOR амали бўйича йиғиндиси. Бу ерда $X^{(K)}$ – раунд функциясига кирувчи X-битлар позициясининг раунд функцияси ичидаги, яъни раунд калитини қўллаш босқичидаги ҳолати. Демак, $X^{(K)}$ – раунд калитининг битлар позициясини ифодаловчи массив бўлиб, унинг элементлари сони раунд калити битлари сонига тенг.

<$X_i \oplus X_j$> ифода X_i ва X_j - ларнинг мос битларини XOR амали бўйича қўшишдан ҳосил бўлган битлар позицияси.

Юқорида киритилган белгилашлар асосида 1 та раунд учун қурилган чизиқли боғланиш умумий кўринишини қуйидагича ифодалаш мумкин:

$$R_0 [X1] \oplus L_0 [X2] \oplus R_1 [X2] = K_1 [X1^{(K)}] \qquad (2.2.4)$$

Кейинги раундлар учун қуриладиган чизиқли боғланишлар ҳам (2.2.4) каби ифодаланади.

Қуйидаги 2.2.2-2.2.3-расмларда иккита раунд учун чизиқли боғланишларни аниқлаш схемалари келтирилган.

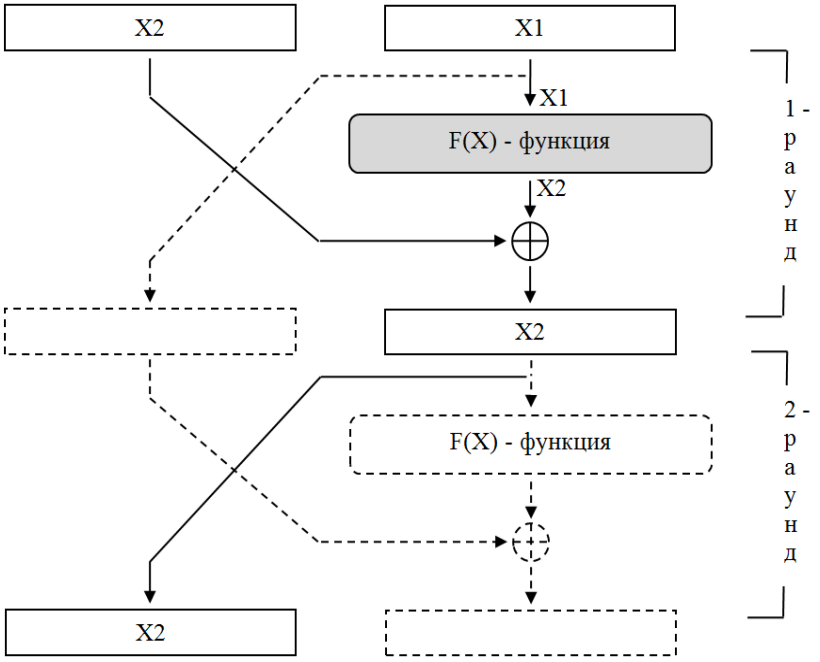
2.2.2-схемага асосан қурилган чизиқли боғланишнинг умумий кўриниши қуйидагича ифодаланади:

$$R_0\,[X1] \oplus L_0\,[X2] \oplus L_2\,[X2] = K_1\,[X1^{(K)}] \qquad (2.2.5)$$

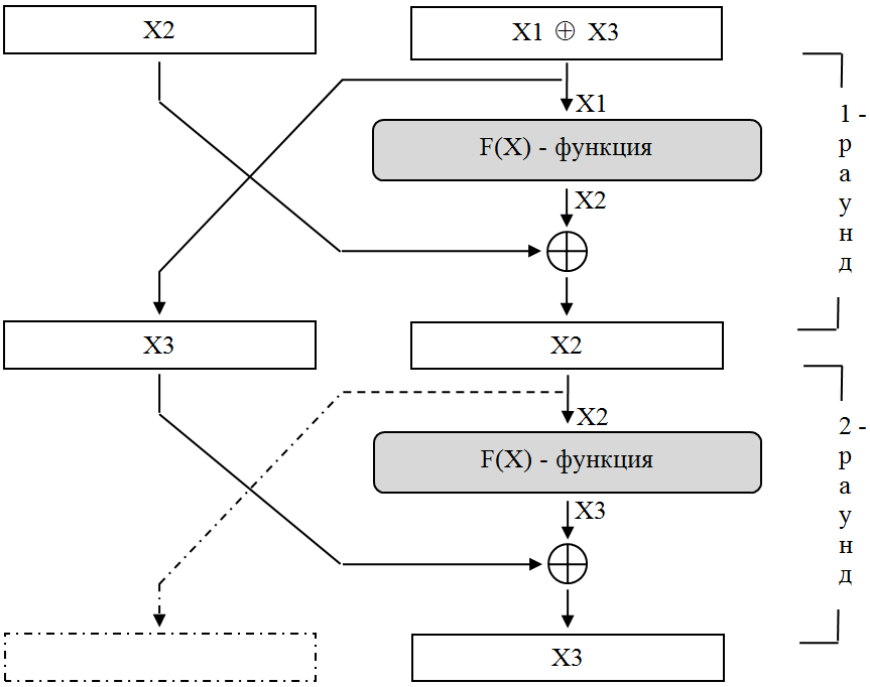
2.2.3-схемага асосан қурилган чизиқли боғланиш умумий кўриниши эса қуйидача ифодаланади:

$$R_0[<X1 \oplus X3>] \oplus L_0[X2] \oplus R_2[X3] = K_1[X1^{(K)}] \oplus K_2[X2^{(K)}] \qquad (2.2.6)$$

Иккита раунд учун келтирилган чизиқли боғланишларни аниқлашнинг 1 ва 2-схемалари фарқи шундаки, 1-схема орқали топилган чизиқли боғланишларда фақатгина 1-раунд калитигина иштирок этиб, 2-раунд калити иштирок этмайди. 2-схемада эса ҳар икки раунд калитлари иштирок этади.

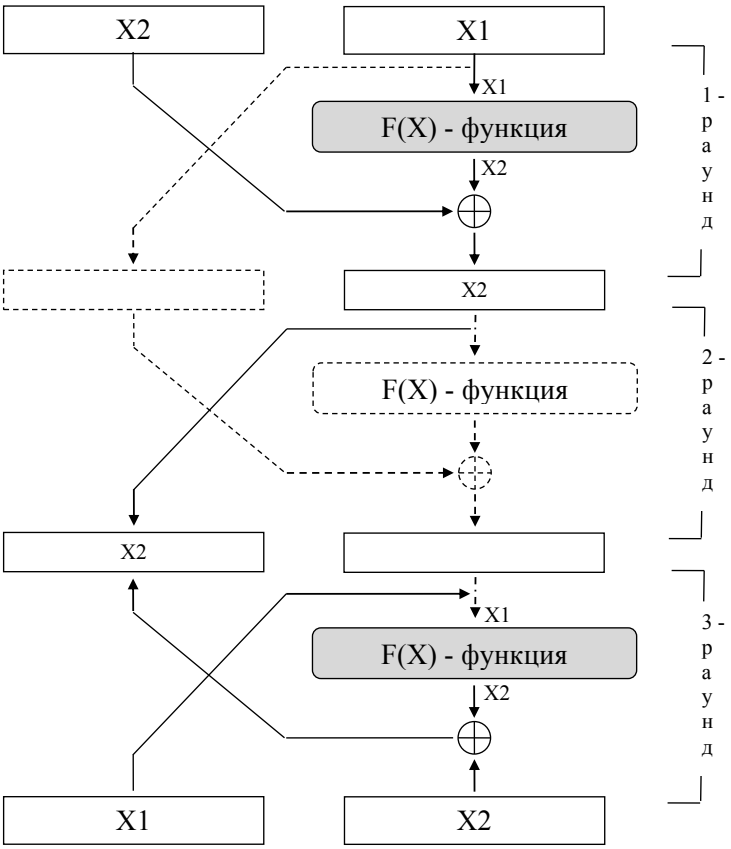


2.2.2-расм. 2 та раунд учун чизиқли боғланишларни аниқлаш 1-схемаси.



2.2.3-расм. 2 та раунд учун чизиқли боғланишларни аниқлаш 2-схемаси.

Қуйида бошқа раундлар учун чизиқли боғланишларни аниқлаш схемаларига нисбатан ҳам бир нечта ўхшаш схемалар келтирилган. Амалиётда қайси бир схемадан фойдаланиш, айни вақтда қайси раунд калити битлари маълум ёки қайси раунд калити битларини аниқлаш масаласига боғлиқ. 2.2.4-расмда 3 та раунд учун чизиқли боғланишларни аниқлаш схемаси келтирилган.

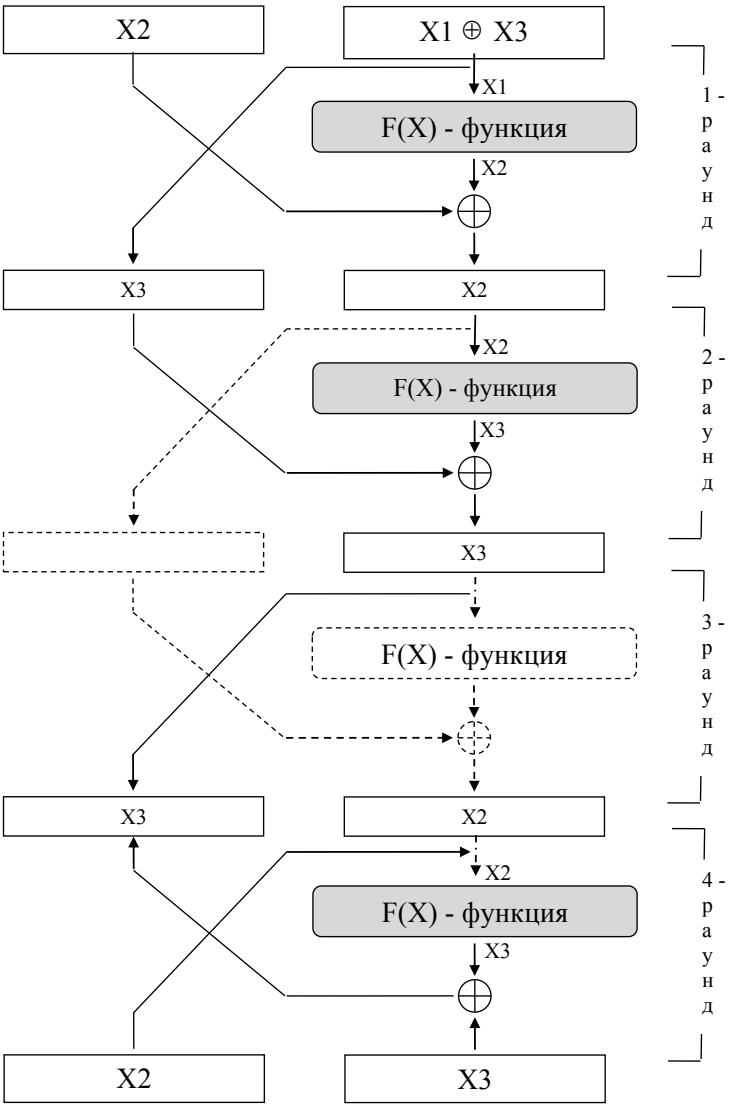


2.2.4-расм. 3 та раунд учун чизиқли боғланишларни аниқлаш схемаси.

Мазкур схемага асосан қурилган чизиқли боғланиш умумий кўриниши қуйидагича ифодаланади:

$$R_0[X1] \oplus L_0[X2] \oplus L_3[X1] \oplus R_3[X2] = K_1[X1^{(K)}] \oplus K_3[X1^{(K)}] \qquad (2.2.7)$$

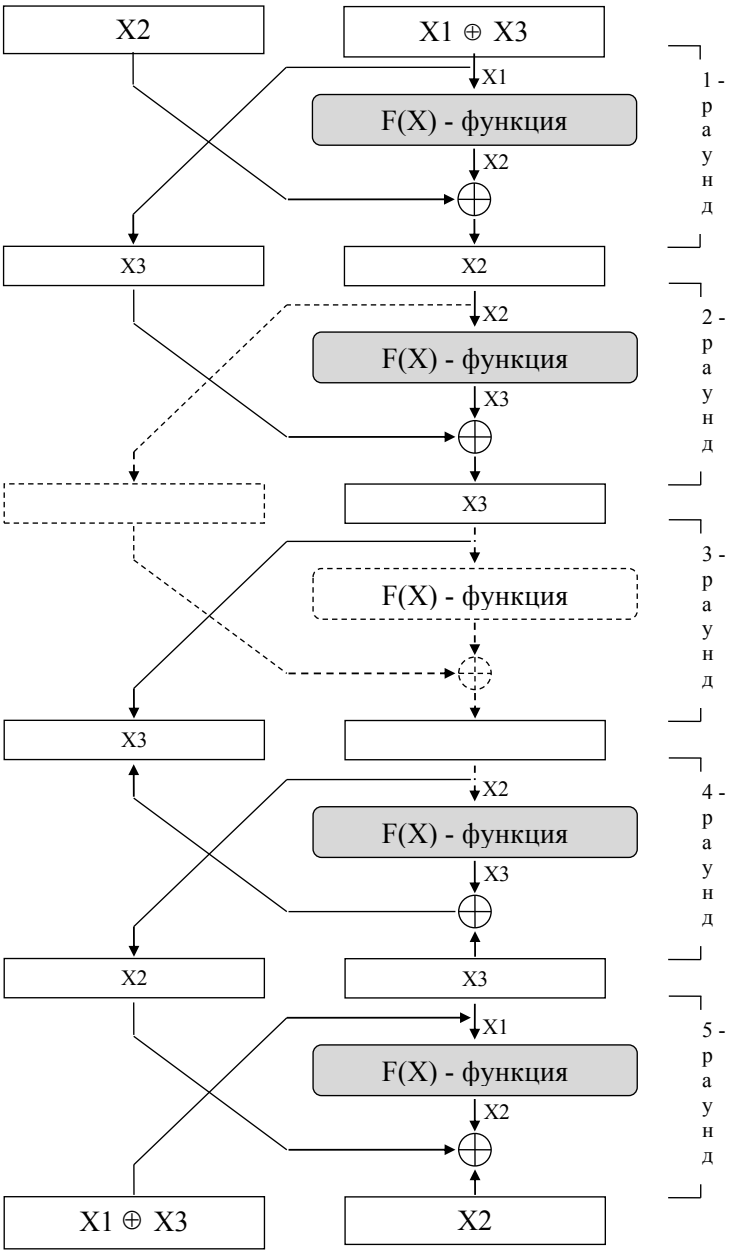
Қуйидаги 2.2.5-расмда 4 та раунд учун чизиқли боғланишларни аниқлаш схемаси келтирилган.



2.2.5-расм. 4 та раунд учун чизиқли боғланишларни аниқлаш схемаси.

Мазкур схемага асосан қурилган чизиқли боғланишнинг умумий кўриниши қуйидагича ифодаланади:

$$R_0[<X1 \oplus X3>] \oplus L_0[X2] \oplus L_4[X2] \oplus R_4[X3] = K_1[X1^{(K)}] \oplus K_2[X2^{(K)}] \oplus \oplus K_4[X2^{(K)}] \quad (2.2.8)$$



2.2.6-расм. 5 та раунд учун чизиқли боғланишларни аниқлаш схемаси.

2.2.6-расмда келтирилган 5 та раунд учун чизиқли боғланишларни аниқлаш схемасига кўра қурилган чизиқли боғланиш умумий кўриниши қуйидагича ифодаланади:

$$R_0[<X1 \oplus X3>] \oplus L_0[X2] \oplus L_5[<X1 \oplus X3>] \oplus R_5[X2] = K_1[X1^{(K)}] \oplus K_2[X2^{(K)}] \oplus K_4[X2^{(K)}] \oplus K_5[X1^{(K)}] \qquad (2.2.9)$$

5 та раундгача бўлган ҳолатда *i*-раунд функциясидан чиқувчи битлар позициясига мос келувчи L_{i-1} – чап қисм битлар позициясини мослаш масаласи муаммо туғдирмайди. Чунки мазкур ҳолатда L_{i-1} - чап қисм битлар позициясини тўғридан-тўғри кириш битлари позициясига боғлаш имконияти мавжуд.

6 ва ундан ортиқ раундларда юқорида таъкидланган муаммо яққол намоён бўлади. Буни қуйидаги 2.2.7-расмда келтирилган 6 та раунд учун чизиқли боғланишларни аниқлаш схемасидан ҳам кўриш мумкин. Схемада ифодаланганидек, 3-раунддан чиқувчи битлар позициясига мос равишда, L_2 – қисмнинг X4-битлар позициясини аниқлаш керак бўлади. Кузатилаётган дастлабки кириш битлари позициялари L_2 – қисмнинг X2-битлар позициясига мос келади. Аксарият ҳолларда X2=X4 шарт бажарилмайди. Ушбу шартнинг бажарилиши айрим хусусий ҳолларда кузатилиши мумкин. Масалан, раунд функцияси кучсиз бўлган криптоалгоритмларда, яъни раунд функциясида “аралаштириш” ва “тарқатиш” хусусиятларига эга бўлган акслантиришлар қатнашмаган криптоалгоритмлар назарда тутилмоқда. Амалиётда бундай алгоритмлардан фойдаланилмайди.

Айтайлик, ихтиёрий L_i – қисмнинг X-битлар позициясини дастлабки кириш битлари позициялари орқали ифодалаш талаб этилсин. Мазкур масалани ҳал этиш учун L_i – битлар позициясини дастлабки раундга кирувчи ҳолатгача Фейстель тармоғига траекторияси бўйича тескари тарзда кузатиш лозим. Ушбу тескари тарзда кузатиш натижасида дастлабки кирувчи блокнинг қайси битлар позицияси ушбу L_i – битлар позициясини ҳосил қилганлиги аниқланади.

Битлар позицияларини тескари тарзда кузатиш жараёнида F(X)-функциясидан чиқувчи битлар позицияларини билган ҳолда, ушбу функцияга кирувчи битлар позицияни аниқлаш масаласи келиб чиқади. Масала ечими сифатида, қуйида келтирилган икки хил усулдан (2.2.7 ва 2.2.8-расмлар) фойдаланиш мумкин.

1-усул. Маълумки, L_i – қисмнинг аниқланиши талаб этилган X-битлар позицияси (i+1)-раунд функциясидан чиқувчи битлар позициясига мос келади. Ўз навбатида L_i – қисмнинг ушбу битлар позициясига (i-1)-раунд функциядан чиқувчи битлар позицияси мос келиши зарур. Демак, (i-1)-раунд функциясига кирувчи битлар позицияси сифатида, (i+1)-раунд функциясига кирувчи битлар позициясини танлаш мумкин. Масалан, 2.2.7-расмда ифодаланган схемада 1-раундга кирувчи битлар позицияси сифатида, 3-раундга кирувчи, яъни X3-битлар позициясини танлаш мумкин. Ушбу ҳолат учун қуйидаги тенглик ўринли:

$$F(X3) = X4 \Rightarrow F^{-1}(X4) = X3 \qquad (2.2.10)$$

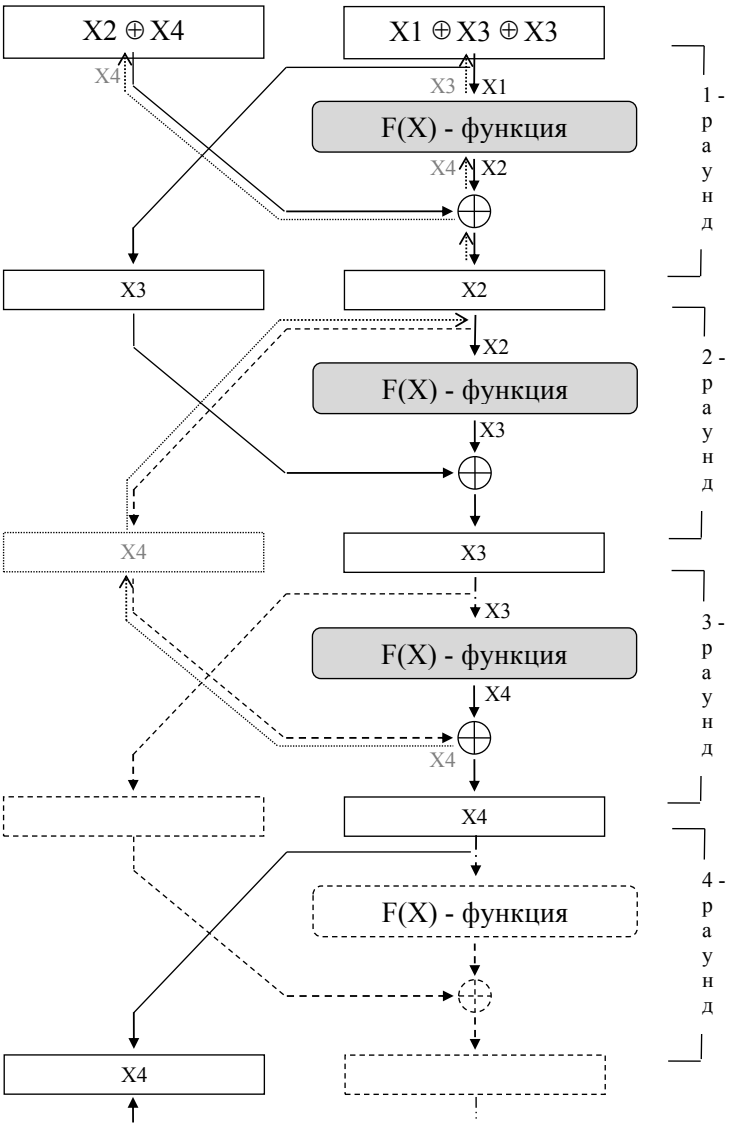
Мазкур схемага асосан қурилган чизиқли боғланиш умумий кўриниши қуйидагича ифодаланади:

$$R_0[X1] \oplus L_0[X2 \oplus X4] \oplus L_6[X2 \oplus X4] \oplus R_6[X3] = K_1[<X1^{(K)} \oplus X3^{(K)}>] \oplus K_2[X2^{(K)}] \oplus K_3[X3^{(K)}] \oplus K_5[X3^{(K)}] \oplus K_6[X2^{(K)}] \qquad (2.2.11)$$

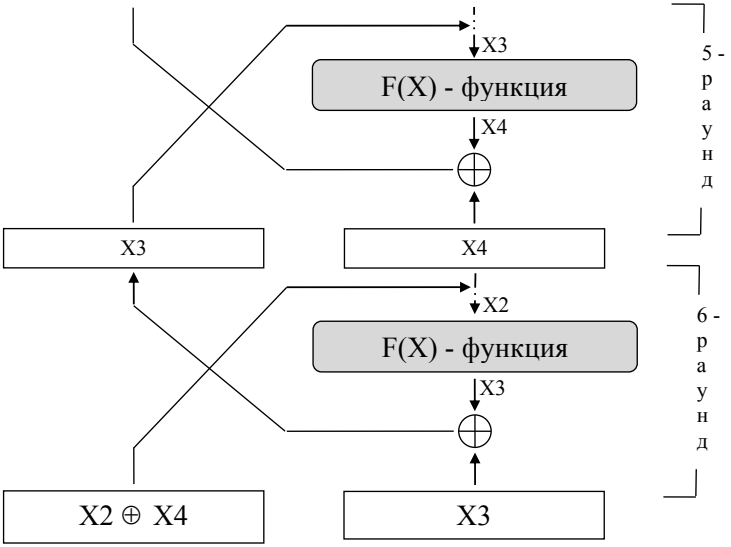
Келтирилган 1-усулга асосан, ихтиёрий L_i – қисмнинг X-битлар позициясини ҳосил қилиш учун, дастлабки раунд функциясига кирувчи битлар позицияси сифатида 3-раундга кирувчи битлар позициясини танлаш етарли ҳисобланади.

2-усул. Юқорида келтирилган 1-усулда $F(X3)=X4 \Rightarrow F^{-1}(X4)= X3$ тенглик ўринли деб олинди. Бундан келиб чиқадики, $F(X3)=X4$ тенгликнинг бажарилиш эҳтимоллиги қанча бўлса, $F^{-1}(X4)=X3$ тенгликнинг ҳам бажарилиш эҳтимоллиги шунга тенг бўлади. Шуни таъкидлаш жоизки, раунд функциясидан чиқувчи X4-битлар позицияга мос келувчи, X3 дан фарқли бўлган, юқори эҳтимолликка эга бир неча кирувчи битлар позициялари мавжуд. $F^{-1}(X4)=X3$ тенгликни ундан юқори эҳтимолликка эга бўлган, $F^{-1}(X4)=X4^{-1}$ тенглик билан алмаштирилса, якунда ҳосил бўладиган чизиқли боғланиш бажарилиш эҳтимоллиги ҳам мос равишда юқори бўлади.

Демак, раунд функциясидан чиқувчи битлар позициясига мос келувчи, энг юқори эҳтимолликка эга бўлган кирувчи битлар позициясини танлаш керак бўлади. Бунинг учун F(X)-функциясига мос равишда, $F^{-1}(X)$-тескари функциясини қуриш талаб этилади. Ушбу тескари функция рауддан чиқувчи битлар позициясини билган ҳолда, раундга кирувчи битлар позициясини аниқлашга хизмат қилади.



Давоми 51-бетда.



2.2.7-расм. 6 та раунд учун чизиқли боғланишларни аниқлаш схемаси (1-усул).

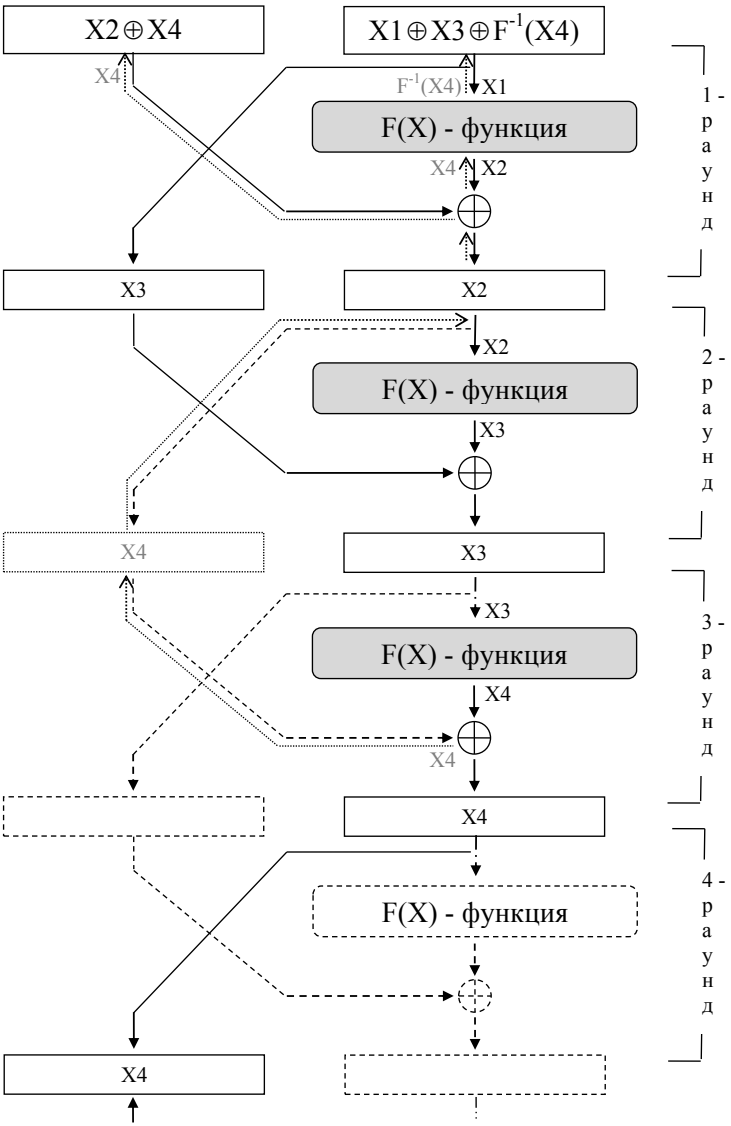
2.2.8-расмда келтирилган схемага асосан қурилган чизиқли боғланишнинг умумий кўриниши қуйидагича ифодаланади:

$$R_0[<X1 \oplus X3 \oplus F^{-1}(X4)>] \oplus L_0[X2 \oplus X4] \oplus L_6[X2 \oplus X4] \oplus R_6[X3] =$$
$$K_1[<X1^{(K)} \oplus X4^{-1(K)}>] \oplus K_2[X2^{(K)}] \oplus K_3[X3^{(K)}] \oplus K_5[X3^{(K)}] \oplus$$
$$K_6[X2^{(K)}] \qquad (2.2.12)$$

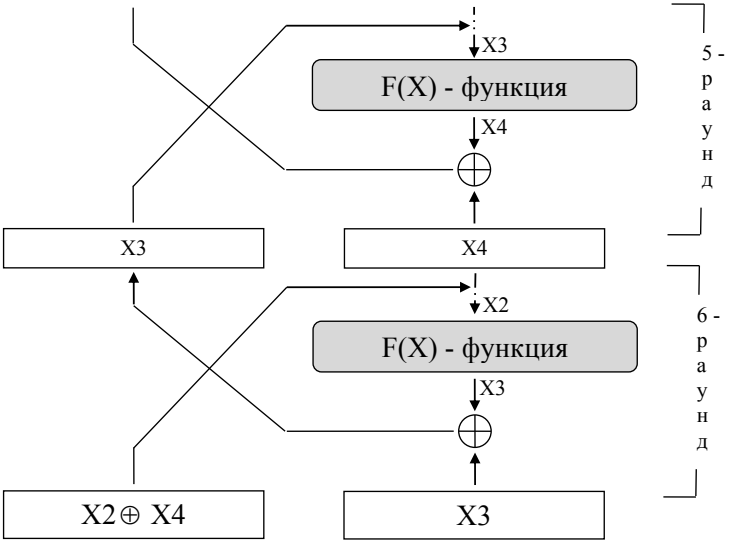
Бу ерда, $X^{-1(K)}$ – тескари раунд функциясига кирувчи X - битлар позициясининг раунд функцияси ичидаги, яъни раунд калитини қўллаш босқичидаги ҳолати.

Шуни таъкидлаш лозимки, амалиётда ҳамма криптоалгоритмларга нисбатан ҳам $F^{-1}(X)$-тескари функция қуришнинг имконияти бўлавермайди. Бу алгоритм раунд функциясида фойдаланилган криптографик акслантиришларнинг хусусиятларига боғлиқ.

6 рауддан юқори бўлган раундларга нисбатан ҳам чизиқли боғланишлар қуриш юқорида келтирилган метод асосида амалга оширилади.



Давоми 53-бетда.



2.2.8-расм. 6 та раунд учун чизиқли боғланишларни аниқлаш схемаси (2-усул).

Жумладан, 8 та раунд учун қурилган чизиқли боғланишлар умумий ифодаси қуйидагича кўринишда бўлади:

$$R_0[<X1 \oplus X3 \oplus F^{-1}(X4) \oplus X5 \oplus F^{-1}(F^{-1}(X5))>] \oplus L_0[X2 \oplus X4 \oplus F^{-1}(X5)] \oplus L_8[F^{-1}(X5) \oplus X4 \oplus F^{-1}(X3)] \oplus R_8[X5 \oplus X3] = K_1[<X1^{(K)} \oplus X4^{-1(K)} \oplus (X5^{-1})^{-1(K)}>] \oplus K_2[X2^{(K)} \oplus X5^{-1(K)}] \oplus K_3[X3^{(K)}] \oplus K_4[X4^{(K)}] \oplus K_6[X4^{(K)}] \oplus K_7[X3^{(K)}] \oplus K_8[X5^{-1(K)} \oplus X3^{-1(K)}] \quad (2.2.13)$$

Юқорида келтирилган, Фейстель тармоғига асосланган шифрлаш алгоритмлари учун чизиқли криптотаҳлил усулини ўтказиш методини аниқ бир шифрлаш алгоритмига нисбатан қўллаш, алгоритм учун битлар позициясини раунд функциясига мос ва тескари тарзда акслантирувчи F(X) ва $F^{-1}(X)$ – функцияларини қуриш масалаларини ҳал қилишни талаб этади.

S – блок учун тузилган боғлиқлик тенгламасининг бажарилиш эҳтимоллигини ҳисоблаш юқорида келтирилган эди. Алгоритмнинг турли раундига нисбатан ҳосил қилинган умумий боғлиқлик тенгламасини бажарилиш эҳтимоллигини ҳисоблашда эса қуйида келтирилган леммадан фойдаланилади.

2.2.1-лемма. Агар $S_{(1)}, \ldots, S_{(n)}$ – боғлиқсиз тасодифий иккилик катталиклар бўлса, у ҳолда, қуйидаги тенглик ўринли:

$$\Delta_{um}(S_{(1)} \oplus S_{(2)} \oplus \ldots \oplus S_{(n)}) = \prod_{i=1}^{n} \Delta(S_{(i)}) \quad (2.2.14)$$

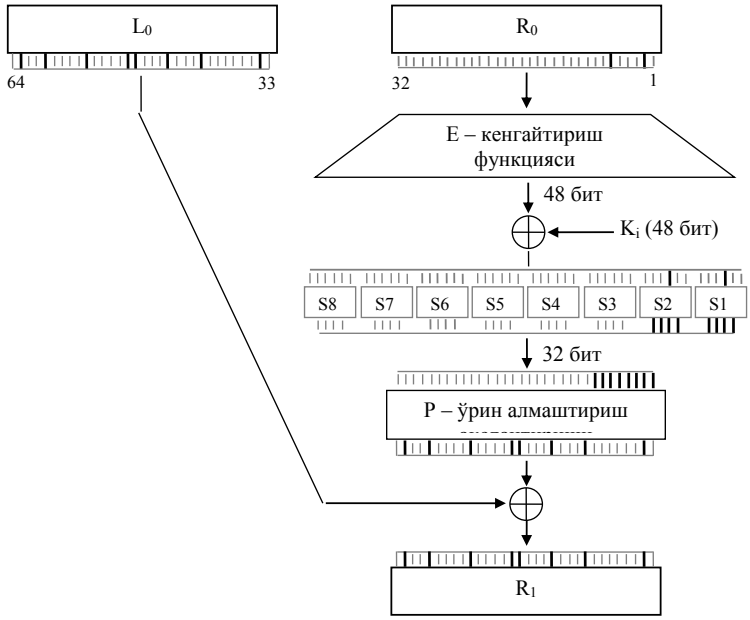
Демак, ушбу леммага мувофиқ, n та боғлиқсиз аппроксимация тенгламасини ўзаро XOR амали орқали қўшиш натижаси ҳосил бўлган якуний тенгламанинг четланиш қиймати барча четланишлар кўпайтмасига тенг бўлади. Мазкур четланиш қиймати орқали якуний ($p_{ит}$) эҳтимоллик қиймати эса қуйидагича аниқланади:

$$p_{ит} = \frac{|\Delta_{ит} - 1|}{2} \qquad (2.2.15)$$

Қуйида DES шифрлаш алгоритми учун аппроксимация тенгламаларини қуришга намуналар келтирилган.

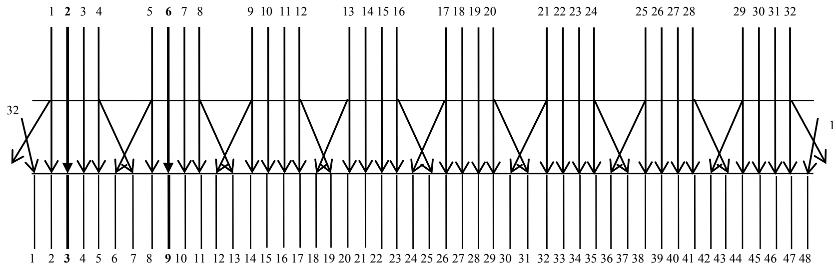
Дастлаб **бир раундли DES алгоритмига** нисбатан аппроксимация тенгламаларини тузишни келтириб ўтамиз.

Айтайлик, 1-раунд функциясига кирувчи битлар позицияси X={0,0,0,0,…0,1,0,0,0,1,0} – бўлсин. Ушбу ҳолда 2.2.1-расм ва DES алгоритми раунд функцияси акслантиришларига мувофиқ, унинг бир раундлик боғлиқлик (позицияларни кузатиш) схемаси қуйидагича тасвирланади (2.2.9-расм):



2.2.9-расм. DES алгоритми битта раунди мисолида битлар позициясини кузатиш.

Раунд функциясига кўра, X={0,0,0,0,…0,1,0,0,0,1,0} – кирувчи битлар позицияси E – кенгайтириш функцияси орқали бошқа битлар позициясига аксланади.



2.2.10-расм. E-кенгайтириш жадвалининг схематик кўриниши.

2.2.10-расмда ифодаланганидек, кирувчи 2- ва 6-битлар позицияси мос равишда 3- ва 9-битлар позициясига аксланади. Демак, кирувчи битлар позициялари E – кенгайтириш функция-сидан сўнг, U= {0,0,0,0,…0,1,0,0,0,0,0,1,0,0} – битлар позициясига аксланади.

Маълумки, E – кенгайтириш жадвалига асосан киришдаги айрим битлар позицияси чиқишда такрорий равишда иштирок этади. Масалан, 4-бит позицияси ўз навбатида 5- ва 7-битлар позициясига аксланади.

Ушбу ҳолатда, иккита бир хил чиқиш битлари позициясидан бирини танлаш лозим. Акс ҳолда, чизиқли боғланишда ушбу бир хил битлар позицияси қисқариб (ейишиб) кетиб, натижада нотўғри аппроксимация тенгламаси ҳосил бўлади.

Раунд функциясининг кейинги босқичида U= {0,0,0,0,… ....0,1,0,0,0,1,0,0} – битлар позицияси S-блок акслантиришларига нисбатан қурилган корреляцион матрицаларга мос равишда аксланади.

$$0\,0\,0\,0\,0\,0\;\;0\,0\,0\,0\,0\,0\;\;0\,0\,0\,0\,0\,0\;\;0\,0\,0\,0\,0\,0\;\;0\,0\,0\,0\,0\,0\;\;0\,0\,0\,0\,0\,0\;\;\underbrace{0\,0\,0\,0\,1\,0}_{S2}\;\;\underbrace{0\,0\,0\,0\,1\,0}_{S1}$$

S_1-блокка мос келувчи (0,0,0,0,1,0) – битлар позицияси, ўзининг қийматига мос келувчи 4-сатрдаги энг катта четланишга эга бўлган, 44 қиймат жойлашган устун тартиб рақамига мос ҳолда, (1,1,1,1) га p_1=0,6875 эҳтимоллик билан аксланади.

2.2.5-жадвал.

S_1-блок учун корреляцион матрица жадвали

i \ j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
…															
4	34	30	28	30	32	28	26	30	36	40	34	32	30	26	44
…															

S_2-блокка мос келувчи (0,0,0,0,1,0) – битлар позицияси, ўзининг қийматига мос келувчи 4-сатрдаги энг катта четланишга эга бўлган, 42 қиймат жойлашган устун тартиб рақамига мос ҳолда, (1,1,1,1) га p_1=0,6563 эҳтимоллик билан аксланади.

2.2.6-жадвал.

S_2-блок учун корреляцион матрица жадвали.

i \ j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
…															
4	30	34	36	34	32	36	38	32	38	30	32	34	32	32	42
…															

Қолган S-блок акслантиришлари учун кирувчи битлар позицияси (0,0,0,0,0,0) бўлгани учун, мос равишда чиқувчи битлар позицияси ҳам (0,0,0,0) бўлади. Натижада, S-блокларга кирувчи $U=\{0,0,0,0,\ldots 0,1,0,0,0,1,0,0\}$ – битлар позицияси S-блоклардан чиқувчи $V=\{0,0,\ldots,0,1,1,1,1,1,1,1,1\}$ – битлар позициясига аксланади.

Раунд функцияси охирги босқичида қўлланилган P-ўрин алмаштириш акслантиришидан сўнг раунд функциясидан чиқувчи битлар позицияси қуйидагича кўриниш олади:

$$Y=\{0,1,0,0,1,0,0,0,0,0,1,0,0,0,0,0,1,1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,0,0,0,1,0\}.$$

Ихтиёрий кирувчи битлар позицияси ва ихтиёрий раунд учун акслантириш (позицияларни кузатиш) жараёни ҳам худди шу тарзда амалга оширилади.

Демак, намунага мос ҳолда аниқланган мазкур битлар позицияси ва (2.2.4) ифодага кўра, 1-раунд учун чизиқли боғланиш қуйидагича кўринишда бўлади:

$$R_0[X]\oplus L_0[Y]\oplus R_1[Y]=K_1[U] \qquad (2.2.16)$$

Яъни 1-раунд учун $p_{um} = \frac{|\Delta_{um} - 1|}{2} = \frac{\left|3/8 \cdot 15/128 - 1\right|}{2} = 113/256$ – эҳтимоллик билан қуйидаги аппросимация тенгламаси ўринли:

$$\begin{gathered} R(0)_2 \oplus R(0)_6 \oplus L(0)_{34} \oplus L(0)_{41} \oplus L(0)_{45} \oplus L(0)_{49} \oplus L(0)_{50} \oplus L(0)_{55} \\ \oplus L(0)_{60} \oplus L(0)_{63} \oplus R(1)_2 \oplus R(1)_9 \oplus R(1)_{13} \oplus R(1)_{17} \oplus R(1)_{18} \oplus \\ R(1)_{23} \oplus R(1)_{28} \oplus R(1)_{31} = \\ = K(1)_2 \oplus K(1)_6 \end{gathered} \quad (2.2.17)$$

Кўриш мумкинки, қурилган тенгламада фақатгина очиқ матн, шифр матн ва калит битлари иштирок этди.

Қуйида **уч раундли DES алгоритмига** нисбатан аппрокси-мация тенгламаларини тузиш масаласига наъмуна келтирилади.

Юқорида келтирилган 2.2.4-расм ва (2.2.7) ифодаларга мувофиқ, ушбу ҳолда 1- ва 3-раундлар учун мос равишда кирувчи ва чиқувчи битлар позициялари бир хил бўлган тенгламалардан фойдаланиш талаб этилади. Шунга кўра, айтайлик 1- ва 3-раундга кирувчи битлар позицияси X={0,0,0,0,0,0,0,0,1,0,0,…0,} – бўлсин. Ушбу позицияни 1- ва 3-раунд функцияларидан ўтказиш жараёни бир хил бўлади. Демак, кирувчи битлар позициялари E – кенгайтириш функциясидан сўнг, қуйидаги битлар позициясига акcланади: U={0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,…0}. Раунд функциясининг кейинги босқичида U= {0,0,0,0,0,0,0,0,0,0, 0,0,0,0,1,0,0,…0} – битлар позицияси S-блок акслантиришларига нисбатан қурилган корреляцион матрицаларга мос равишда акcланади.

$$\underbrace{}_{}\text{000000 00000}\underbrace{\text{0 01000}}_{S6}\text{0 000000 000000 000000 000000 000000}$$

S_6-блокка мос келувчи (0,1,0,0,0,0) – битлар позицияси, ўзининг қийматига мос келувчи 16-сатрдаги энг катта четланишга эга бўлган, 18 қиймат жойлашган устун тартиб рақамига мос ҳолда, (0,1,1,1) га p_1=0,2813 эҳтимоллик билан акcланади. Қолган S-блок акслантиришлари учун кирувчи битлар позицияси (0,0,0,0,0,0) бўлгани учун, мос равишда чиқувчи битлар позицияси ҳам (0,0,0,0) бўлади. Натижада, S-блокларга кирувчи U – битлар позицияси S-блоклардан чиқувчи $V = \{0,0,0,0,0,0,0,0,0,1,1,1,0,0,\ldots,0\}$ – битлар позициясига акcланади.

Р-ўрин алмаштириш акслантиришидан сўнг эса раунд функциясидан чиқувчи битлар позицияси қуйидагича кўриниш олади:

$$Y = \{0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0\}$$

Демак, намунага мос ҳолда аниқланган мазкур битлар позицияси ва (2.2.7) ифодага кўра, 3 та раунд учун чизиқли боғланиш қуйидагича кўринишда бўлади:

$$R_0[X] \oplus L_0[Y] \oplus L_3[X] \oplus R_3[Y] = K_1[U] \oplus K_3[U] \qquad (2.2.18)$$

Яъни, $p_{ит} = \frac{\left|7/16 \cdot 7/16 - 1\right|}{2} = 207/512$ – эҳтимоллик билан қуйидаги аппросимация тенгламаси ўринли:

$$R(0)_9 \oplus L(0)_6 \oplus L(0)_{16} \oplus L(0)_{30} \oplus L(3)_9 \oplus R(3)_6 \oplus R(3)_{16} \oplus L(3)_{30} = \\ = K(1)_{14} \oplus K(3) \qquad (2.2.19)$$

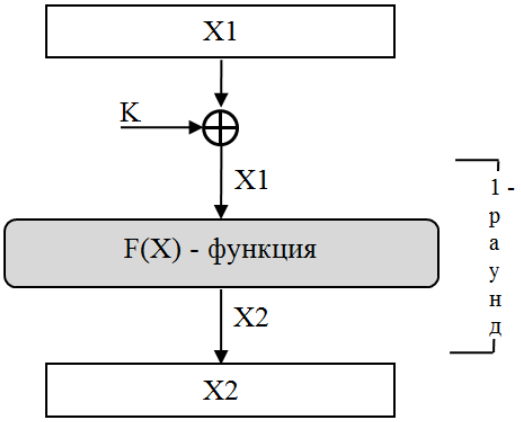
Кўриш мумкинки, қурилган ушбу тенгламада ҳам фақатгина очиқ матн, шифр матн ва калит битлари иштирок этди.

SP тармоғига асосланган шифрлаш алгоритми учун аппроксимация тенгламасини тузиш

Бугунги кунда O‘zDSt 1105:2009, AES, SERPENT ва бошқа кўплаб замонавий блокли симметрик шифрлаш алгоритмлари SP тармоғига асосланган. Қуйида мазкур тармоққа асосланган шифрлаш алгоритмлари учун очиқ матн, шифр матн ва калит битларини боғловчи чизиқли боғланишларни аниқлаш усули келтирилади.

Маълумки, SP тармоғи моҳиятига асосан шифрлаш алгоритмига кирувчи блок бир неча бор раунд функциясидан ўтказилади ва шу тарзда шифр матн ҳосил қилинади. Шунингдек, аксарият алгоритмларда очиқ матн блокига 1-раундга киришдан аввал ҳам махфий калит қўшилади.

Дастлаб битта раундли алгоритмга нисбатан боғлиқлик тузишни кўриб ўтамиз.



2.2.11-расм. 1 та раунд учун чизиқли боғланишларни аниқлаш схемаси.

Алгоритм схемалари ва унга мос боғлиқлик тенгламаларини ифодалашда Фейстель тармоғига нисбатан юқорида киритилган белгилашлардан ҳамда уларга қўшимча тарзда қуйидаги белгилашлардан фойдаланамиз:

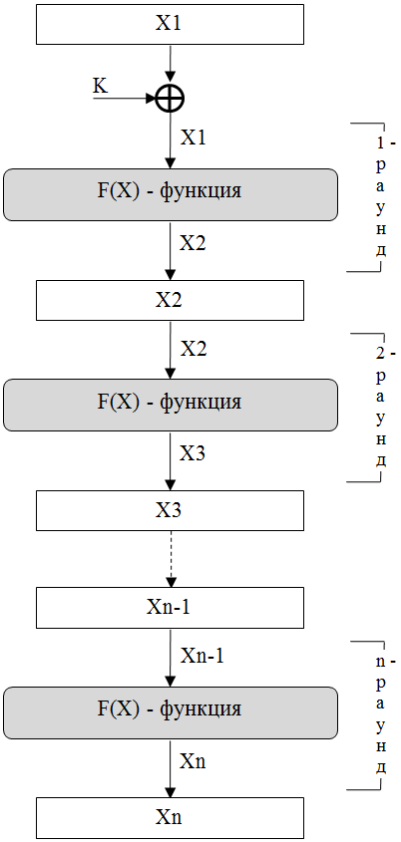
P_{i-1} – i-раундга кирувчи блок;

P_i – i-раунддан чиқувчи блок.

Киритилган белгилашлар ва 2.2.11-расмда келтирилган схема асосида 1 та раунд учун қурилган чизиқли боғланишнинг умумий кўринишини қуйидагича ифодалаш мумкин:

$$P_0 [X1] \oplus P_1 [X2] = K_0 [X1^{(K)}] \oplus K_1 [X1^{(K)}] \qquad (2.2.20)$$

SP тармоғига асосланган бир неча раундли шифрлаш алгоритми учун Фейстель тармоғидан фарқли ўлароқ, очиқ матн, шифр матн ва калит битлари орқали ифодаланган чизиқли боғлиқликни тузиш мураккаблик туғдирмайди. Айтайлик *n* та раунддан иборат алгоритм қаралаётган бўлсин (2.2.12-расм).



2.2.12-расм. n та раунд учун чизиқли боғланишларни аниқлаш схемаси.

2.2.12-расмда келтирилган схемага кўра, *n* та раунд учун қурилган чизиқли боғланишнинг умумий кўриниши қуйидагича ифодаланади:

$$P_0[X1] \oplus P_n[Xn] = K_0[X1^{(K)}] \oplus K_1[X1^{(K)}] \oplus K_2[X2^{(K)}] \oplus \ldots \oplus K_n[Xn^{(K)}] \quad (2.2.21)$$

Мазкур турдаги алгоритмнинг турли раундига нисбатан ҳосил қилинган умумий боғлиқлик тенгламасини бажарилиш эҳтимоллигини ҳисоблашда қуйида келтирилган леммадан фойдаланилади.

2.2.2-лемма [33]**.** (Йиғувчанлик леммаси) *n* та чизиқли эркли тасодифий $X_1, X_2, ..., X_n$ иккилик қийматлар учун қуйидаги:

$$P_{ит}(X_1 \oplus ... \oplus X_n = 0) = 1/2 + 2^{n-1}\ ((p_1 - 1/2)\cdot(p_2 - 1/2)\cdot_{....}\cdot(p_n - 1/2)) \quad (2.2.22)$$

тенглик ўринли бўлади. Шунингдек, агар барча *i* лар учун p_i=0 ёки p_i=1 бўлса, у ҳолда, $P(X_1 \oplus_{...} \oplus X_n = 0) = 0$ ёки $P(X_1 \oplus_{...} \oplus X_n = 0) = 1$ бўлади. Агар барча *i* лар учун p_i=1/2 бўлса, у ҳолда, $P(X_1 \oplus_{...} \oplus X_n = 0) = 1/2$ ўринли.

Қуйида SP тармоғига асосланган ўқув шифрлаш алгоритмига (2.2.13-расмга мувофиқ) чизиқли криптотаҳлил усулининг қўлланиши бўйича намуна келтирилади. Қаралаётган 3 раундли ўқув шифрлаш алгоритми (2.2.13-расм) раунд функциясида 3 та бир хил S – блок жадвалидан фойдаланилган бўлиб, у қуйидагича:

2.2.6-жадвал.
S-блок жадвали

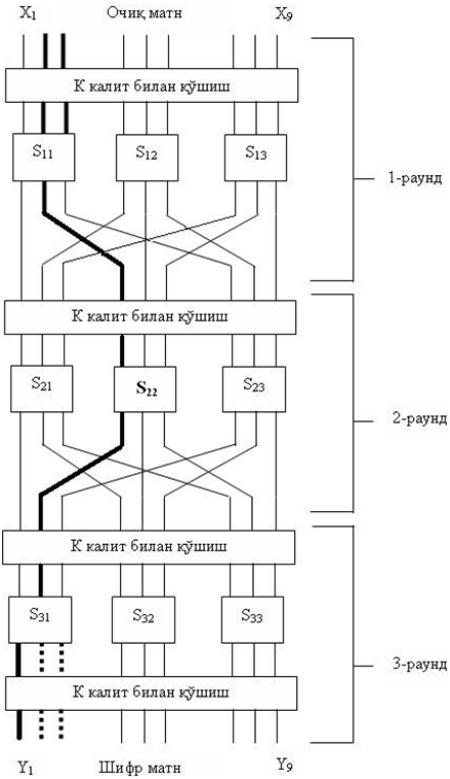
Кириш	0	1	2	3	4	5	6	7
Чиқиш	3	1	4	2	6	0	5	7

Ушбу S – блок жадвалига мувофиқ корреляцион матрица жадвали эса қуйидагича кўринишга эга:

2.2.7-жадвал.
S-блок учун корреляцион матрица жадвали

i \ j	1	2	3	4	5	6	7
1	4	4	4	2	2	2	6
2	4	4	4	6	2	6	6
3	4	**0**	4	4	4	4	4
4	4	4	4	6	2	2	2
5	4	4	**8**	4	4	4	4
6	**0**	4	4	4	4	4	4
7	4	4	4	6	6	2	6

Айтайлик, алгоритмга кирувчи битлар позицияси X={0,1,1,0,0, 0,0,0,0} – бўлсин. Ушбу ҳолда, 2.2.12-расм ва ушбу алгоритм раунд функцияси акслантиришларига мувофиқ, уч раундлик боғлиқлик (позицияларни кузатиш) схемаси қуйидагича бўлади:



2.2.13-расм. SP тармоғига асосланган 3 раундли шифрлаш алгоритми схемаси.

Алгоритм схемасига кўра, 1-раундга ҳам X – битлар позицияси кириб, S – жадвали орқали бошқа битлар позициясига аксланади. Ушбу акслантириш S – блокка нисбатан тузилган корреляцион матрицага мос равишда аксланади.

$$\underbrace{011}_{\mathbf{S_{11}}}\ 000\ \ 000$$

S_{11}-блокка мос келувчи (0,1,1) – битлар позицияси, ўзининг қийматига мос келувчи 3-сатрдаги энг катта четланишга эга бўлган, 0 қиймат жойлашган устун тартиб рақамига мос ҳолда, (0,1,0) га p_1=0 эҳтимоллик билан аксланади.

Қолган S-блок акслантиришлари учун кирувчи битлар позицияси (0,0,0) бўлгани учун, мос равишда чиқувчи битлар

позицияси ҳам (0,0,0) бўлади. Натижада, 1-раунд S-блокларига кирувчи битлар позицияси S-блоклардан ва схемага мувофиқ ўрин алмаштириш акслантиришидан сўнг $U_1 = \{0,0,0,1,0,0,0,0,0,0\}$ – битлар позициясига аксланади. Худди шу каби кузатиш давом эттирилса 2-раунднинг ўрин алмаштириш акслантиришидан сўнг $U_2 = \{0,1,0,0,0,0,0,0,0,0\}$ – битлар позициясига аксланади.

Сўнгги раундда ўрин алмаштириш акслантиришидан фойдаланилмаганлиги учун, кузатилаётган битлар позицияси 3-раунд S – блок жадвалидан ва калит қўшиш акслантиришидан сўнг $U_3 = \{1,0,0,0,0,0,0,0,0,0\}$ – битлар позициясига аксланади.

Ихтиёрий кирувчи битлар позицияси ва ихтиёрий раунд учун акслантириш (позицияларни кузатиш) жараёни ҳам худди шу тарзда амалга оширилади.

Демак, намунага мос ҳолда аниқланган мазкур битлар позициясига ва (2.2.21) ифодага кўра, ушбу алгоритм учун чизиқли боғланиш қуйидагича кўринишда бўлади:

$$P_0[X] \oplus P_3[U_3] = K_0[X^{(K)}] \oplus K_1[U_1^{(K)}] \oplus K_2[U_2^{(K)}] \oplus K_3[U_3^{(K)}] \qquad (2.2.23)$$

Яъни $P_{um} = 1/2 + 2^{3-1}((0/8 - 1/2) \cdot (3/4 - 1/2) \cdot (3/4 - 1/2)) = 3/8$ – эҳтимоллик билан қуйидаги аппроксимация тенгламаси ўринли:

$$P(0)_2 \oplus P(0)_3 \oplus P(3)_1 = K(0)_2 \oplus K(0)_3 \oplus K(1)_4 \oplus K(2)_2 \oplus K(3)_1 \qquad (2.2.24)$$

Кўриш мумкинки, тузилган тенгламада фақатгина очиқ матн, шифр матн ва барча раунд калит битлари иштирок этди.

Демак, Фейстель ёки SP тармоғига асосланган шифрлаш алгоритмлари учун **умумий боғлиқликни (аппроксимация тенгламасини) қуриш**да юқорида келтирилган усулларга таяниш кифоя. Бироқ, (2.2.1) тенгликдаги 2^n та кирувчи битларни, 2^m та чиқувчи битлар билан мумкин бўлган барча боғланишлари ичидан энг эффективларини танлаш амалий мураккаб масала бўлади (ГОСТ 28147-89 ва DES алгоритмларида *n* ва *m* ларнинг максимал қиймати 64 га тенг).

Чизиқли криптотаҳлил усулининг кейинги асосий босқичларидан бири, **статистик таҳлил олиб бориш асосида фақатгина калит битлари орқали ифодаланувчи тенгламалар системасини қуриш**дир.

Айтайлик тузилган аппроксимация тенгламалари “чап қисми” фақат очиқ ва шифр матн битларига боғлиқ, “ўнг қисми” эса фақат калит битларига боғлиқ бўлсин. Ушбу ҳолда тенгламалар маълум эҳтимоллик билан бажарилгани боис, бирор очиқ ва шифр матн қийматларини мазкур тенглама чап қисмига қўйиш орқали ҳосил бўлган тенглама ҳар доим ҳам тўғри ечим бермайди. Шунинг учун, тенгламалар чап қисмига бир нечта очиқ ва шифр матн қийматларини мос равишда қўйиш асосида ушбу қисмнинг натижавий қиймати “0” ёки “1” эканлиги аниқланади. Ушбу статистикадан сўнг эса, фақатгина калит битларига боғлиқ тенглама ҳосил бўлади. Статистиканинг қийинчилик даражаси тузилган тенгламалар бажарилиш эҳтимоллигига узвий боғлиқ бўлиб, эҳтимоллик қиймати қанчалик 0,5 га яқинлашса (мазкур ҳолат раундлар сони ошган сари кузатилади) чап қисм қийматини аниқлаш учун ҳам шу қадар кўп очиқ ва шифр матн талаб этилади.

Криптотаҳлил сўнгги жараёни, яъни **калит битларига боғлиқ бўлган тенгламалар системасини ечиш** ҳам амалиётда турли қийинчилик туғдиради. Булардан энг асосийси, тенгламалар системасини бир қийматли ечиш масаласидир. Аслида r раундли шифрлаш алгоритмини тўлиқ калит битларини аниқлаш учун ўзаро чизиқли боғлиқсиз $r \cdot Kn$ та тенглама етарли. Бу ерда Kn–раунд калитининг битлар сони (ГОСТ 28147-89 алгоритмида $Kn = 32$, DES шифрлаш алгоритмида эса $Kn = 48$). Лекин топилган ҳар бир тенглама ҳам бошқалари билан ўзаро чизиқли боғлиқсиз ва энг асосийси юқори четланишда бўлавермайди.

Ушбу санаб ўтилган барча математик, вақт ва хотира билан боғлиқ муаммолар шифрлаш алгоритми раунд акслантиришларига бевосита боғлиқ ҳолда ҳал этилади.

Умумий ҳолда, блок узунлиги n – бит бўлган мавжуд ёки янги таклиф этилган блокли симметрик шифрлаш алгоритмини чизиқли криптотаҳлил (ЧК) усулига бардошлилигини баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.2.8-жадвал.
Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Изланаётган калит битларини очиқ ва шифр матн битларига боғловчи эффектив аппроксимация тенгламаларини қуриш ва улар четланиши қиймати Δ ни аниқлаш	Қуриш мумкин ва $\Delta>0$	Кейинги босқичга ўтиш мумкин
		Назарий қуриб бўлмайди ёки $\Delta=0$	Алгоритм ЧК усулига назарий бардошли[1]
II.	Статистика ўтказиш учун лозим бўлган матнлар сони – W ни аниқлаш ($W \approx \frac{1}{\Delta^2}$)	$W \leq 2^n$ ва реал вақт мобайнида W та матн устида статистика ўтказиш амалий мумкин	Кейинги босқичга ўтиш мумкин
		$W>2^n$ (ёки реал вақт мобайнида W та матн устида статистика ўтказишнинг амалий имкони йўқ)	Алгоритм ЧК усулига назарий (ёки амалий) бардошли
III.	Статистика ўтказиш орқали калит битларига боғлиқ бўлган тўғри аппроксимация тенгламаларини қуриш	Статистика натижа берди ва тўғри тенгламалар қурилди	Кейинги босқичга ўтиш мумкин
		Статистика натижа бермади ва тўғри тенгламалар қурилмади	Алгоритм ЧК усулига амалий бардошли

[1] Мазкур жадвал ва бундан кейинги барча жадвалларда келувчи **“Алгоритм ЧК (ёки бошқа) усулига назарий ёки амалий бардошли (бардошсиз)”** – жумласи ушбу алгоритмнинг криптотаҳлил натижасида аниқланган калитга нисбатан бардошли (бардошсиз) эканлигини англатади. Яъни агар калитнинг барча битлари аниқланса, алгоритм бардошсиз, агар калитнинг айрим битлари аниқланса, алгоритм айнан ушбу битларни аниқлашга нисбатан бардошсиз бўлади.

2.2.8-жадвалнинг давоми.

IV.	Якуний тенгламалар системасини ечишнинг самарали усулини ва унга мувофиқ ечиш учун талаб этилувчи амаллар сони – N ни аниқлаш	Реал вақт мобайнида N та амални бажариш амалий мумкин ва системани ечиш учун лозим бўлган ҳотира ҳажми амалий мавжуд	Кейинги босқичга ўтиш мумкин
		Реал вақт мобайнида N та амални бажаришнинг амалий имкони йўқ ёки системани ечиш учун лозим бўлган ҳотира ҳажми амалий мавжуд эмас	Алгоритм ЧК усулига амалий бардошли
V.	Тенгламалар системасини ечиш орқали изланаётган калит битларини аниқлаш	Калит битлари аниқланди	Алгоритм ЧК усулига бардошсиз
		Калит битлари аниқланмади	Алгоритм ЧК усулига амалий бардошли

Назорат саволлари

1. Чизиқли криптотаҳлил усули асосий қадамлар кетма-кетлиги нималардан иборат?

2. Фейстель тармоғига асосланган шифрлаш алгоритми учун чизиқли криптотаҳлил усули асосий моҳиятини тушунтиринг.

3. SP тармоғига асосланган шифрлаш алгоритми учун чизиқли криптотаҳлил усули асосий моҳиятини тушунтиринг.

4. Корреляцион матрица тушунчасига таъриф беринг ва криптотаҳлил жараёнида қандай мақсадда фойдаланишини изоҳланг.

5. Эффектив аппроксимация тенгламасига изоҳ беринг ва унинг таҳлил самарадорлигига таъсирини тушунтиринг.

6. Фейстель тармоғига асосланган шифрлар икки ва ундан ортиқ раундлари учун эффектив аппроксимация тенгламаларини қуришнинг қандай усуллари мавжуд?

7. Аппроксимация тенгламасидаги номаълумлар сони криптотаҳлил самарадорлигига қандай таъсир кўрсатади?

8. Аппроксимация тенгламаси четланиш қиймати криптотаҳлил самарадорлигига қандай таъсир кўрсатади?

9. Шифрлаш алгоритми раундлар сони криптотаҳлил самарадорлигига қандай таъсир кўрсатади?

10. Шифрлаш алгоритми таркибидаги ўрин алмаштириш акслантиришининг таҳлил самарадорлигига таъсири қандай?

11. Мазкур криптотаҳлил жараёнида бир нечта очиқ матн ва уларга мос шифр матн қийматлари нима учун талаб этилади?

12. Чизиқли криптотаҳлил усули статистик ҳужум турига тегишли эканлигини изоҳланг.

2.3. Дифференциал криптотаҳлил усули

Дифференциал криптотаҳлил (ДК) усули Исроил криптографлари E.Biham ва A.Shamir томонидан 1990 йилда DES алгоритмига қарши ҳужум тури сифатида ишлаб чиқилган [33]. ДК усулида шифрлаш алгоритми ва унга мос танлаб олинган очиқ матн ва шифр матн маълум деб олинади. Мазкур криптотаҳлил усули стандарт 16-раундли DES алгоритмини амалий жиҳатдан тўлиқ очиш имкониятини бермаса ҳам (2^{47}та матн керак бўлади), қисқартирилган раундли масалан, 8-раундли, 6-раундли DES алгоритмини муваффақиятли очиш имконини беради.

Кейинчалик дифференциал криптотаҳлил Shefri, Khafre, REDOC-II, LOCI, LOCI91, Lucifer, Skipjack, ORYX, SPEED, SAFER, IDEA, Feal, RC2, RC5, MacGuffin, ICE, SEED, MISTY1, Nimbus, Rijndael, SPECTR-H64, SPECTR-128, DDP-S64, DDP-S128 каби алгоритмларга қўлланилиб, тегишли натижалар олинган.

ДК усулининг моҳияти бирор алгоритмга кирувчи X, X' ва унинг айирмаси ΔX, чиқувчи Y, Y' ҳамда унинг айирмаси ΔY қийматлардан фойдаланиб калитни топишдан иборатдир. Мазкур усулни амалиётда қўллаш мураккаблиги шундан иборатки, етарлича кўп миқдордаги очиқ матн ва шифр матн жуфтликлари устида таҳлил олиб бориш керак бўлади. Қуйидаги жадвалда r раундли DES алгоритми калитини топиш учун керак бўладиган очиқ матнлар сони келтирилган [33].

2.3.1-жадвал.

DES алгоритмини дифференциал криптотаҳлил натижалари

Раундлар сони	Калитни топиш учун керак бўладиган очиқ матнлар сони
8	2^{14}
10	2^{24}
12	2^{31}
14	2^{39}
16	2^{47}

Умумий ҳолда Фейстель тармоғига асосланган блокли шифрлаш алгоритмларига ДК усули қуйидаги қадамлар кетма-кетлиги асосида амалга оширилади:

1. Эҳтимоллиги катта бўлган ($P>1/2^n$) ((ΔX, (ΔY) жуфтлик, яъни дифференциал танланади.
2. Танланган айирмаси (XOR) ΔX га тенг очиқ матнлар ва уларга мос айирмаси ΔY га тенг шифр матнлар учун акслантиришга кириши мумкин бўлган қийматлар тўплами $IN_j(B'_j, C'_j)$ аниқланади.
3. Ҳосил бўлган тўплам ҳар бир элементига танланган очиқ матнни қўшиш (XOR) натижасида мумкин бўлган қисм калитлар тўплами $Test_j\ (E, E^*, C'_j)$ тузилади.
4. Юқоридаги қадамлар калитлар тўплами кесишмаси ягона қийматни қабул қилмагунча такрорланади. Бу қиймат эса ҳақиқий қисм калитни ифодалайди.

Қуйида дифференциал криптотаҳлил асосида ётувчи базавий тушунчаларни келтирамиз.

Узунлиги n битга тенг B'_j ва узунлиги m га тенг C'_j сатрлар учун $IN_j(B'_j, C'_j)$ тўплам қуйидагича аниқланади [33]:

$$IN_j(B'_j, C'_j) = \{B_j \in (Z_2)^n : S_j(B_j) \oplus S_j(B_j \oplus B'_j) = C'_j\}, \qquad (2.3.1)$$

бу ерда, $IN_j(B'_j, C'_j) - S_j$ блок учун кирувчи XOR B'_j га ва чиқувчи XOR C'_j га тенг бўлган жуфтликлар тўплами, (') – белгилаш икки матн XOR йиғиндисини билдиради.

Ҳосил бўлган тўплам ҳар бир элементига танланган очиқ матнни қўшиш (XOR) натижасида мумкин бўлган қисм калитлар тўплами $Test_j\ (E, E^*, C'_j)$ қуйидагича аниқланади:

$$Test_j\ (E, E^*, C'_j) = \{B_j \oplus E_j : B_j \in IN_j(E'_j, C'_j)\}, \qquad (2.3.2)$$

бу ерда, E_j ва E_j^* – узунлиги n битга ва C'_j узунлиги m битга тенг бўлган сатрлар.

Келтирилган тушунчалардан маълумки, симметрик шифрлаш алгоритми криптографик алмаштиришларини ДК усулига бардошлилигини баҳолашда асосий характеристикаларидан бири алгоритмда фойдаланилган чизиқсиз акслантиришларнинг айирмалар матрицаси ҳисобланади.

2.3.1-таъриф. Элементлари қуйидаги:

$$\delta = \Delta_{a\to b}^{(F)} \left| F(x) \oplus F(x \oplus a) = b \right| \quad x, a \in Z_2^n, b \in Z_2^m \qquad (2.3.3)$$

ифода билан аниқланадиган матрицага айирмалар матрицаси дейилади. Бу ерда, F – симметрик шифрлаш алгоритмидаги чизиқсиз акслантириш.

(2.3.3) формула билан аниқланувчи энг катта элемент акслантиришга нисбатан айирмалар матрицасининг максимуми дейилади ва δ_F каби белгиланади.

Қуйида 4-бит кириш ва 4-бит чиқишни ифодаловчи S-блок (2.3.2-жадвал) жадвалига нисбатан айирма матрица тузишга намуна келтирилган.

2.3.2-жадвал.

S-блок жадвали

Кириш	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Чиқиш	**9**	**4**	**10**	**13**	**8**	**0**	**1**	**6**	**14**	**11**	**12**	**5**	**3**	**2**	**15**	**7**

Мазкур берилган S-блок жадвалига мувофиқ (2.3.1) ифода асосида ишлаб чиқилган айирмалар матрицаси қуйидаги 2.3.3-жадвалда келтирилган.

2.3.3-жадвал.

S-блок жадвалининг айирмалар матрицаси

$\Delta^{(F)}_{a\to b}$		***b***															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
a	**0**	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	2	0	0	0	2	0	4	4	2	0	0	0	2	0	0
	2	0	0	2	2	0	2	2	0	0	4	0	0	2	0	2	0
	3	0	2	0	0	4	0	0	2	0	0	0	2	0	2	4	0
	4	0	2	2	2	2	0	0	0	0	2	0	4	0	2	0	0
	5	0	0	0	0	0	0	0	0	2	2	2	2	**8**	0	0	0
	6	0	2	4	0	0	0	0	2	2	0	0	0	2	2	0	2
	7	0	0	0	0	2	4	2	0	0	2	2	0	0	0	2	2
	8	0	2	2	0	0	0	2	2	2	0	0	2	0	0	2	2
	9	0	2	2	2	0	0	2	0	0	2	4	0	0	0	0	2
	10	0	2	2	0	4	2	2	4	0	0	0	0	0	0	0	0
	11	0	2	0	4	0	2	0	0	2	0	0	0	2	0	0	4
	12	0	0	0	2	0	2	4	0	0	0	4	2	0	2	0	0
	13	0	0	2	2	2	0	0	2	0	0	2	2	0	2	2	0
	14	0	0	0	2	2	2	2	0	0	2	0	0	0	2	0	4
	15	0	0	0	0	0	0	0	0	4	0	2	2	2	2	4	0

Айирма матрица жадвалига кўра, мазкур S-блок учун δ_F=8 ўринли бўлиб, a=5 – кирувчи айирма $P = {8}/{2^4} = 0.5$ – эҳтимоллик билан b=12 – чиқувчи айирмага аксланади.

2.3.1-тасдиқ. Айирмалар матрицасининг эҳтимоллиги $P_{ij} \geq {2}/{2^n}$ бўлган элементлар учун ДК усулидан фойдаланиб, қаралаётган шифрлаш алгоритми маълум раунд калитларини топиш мумкин.

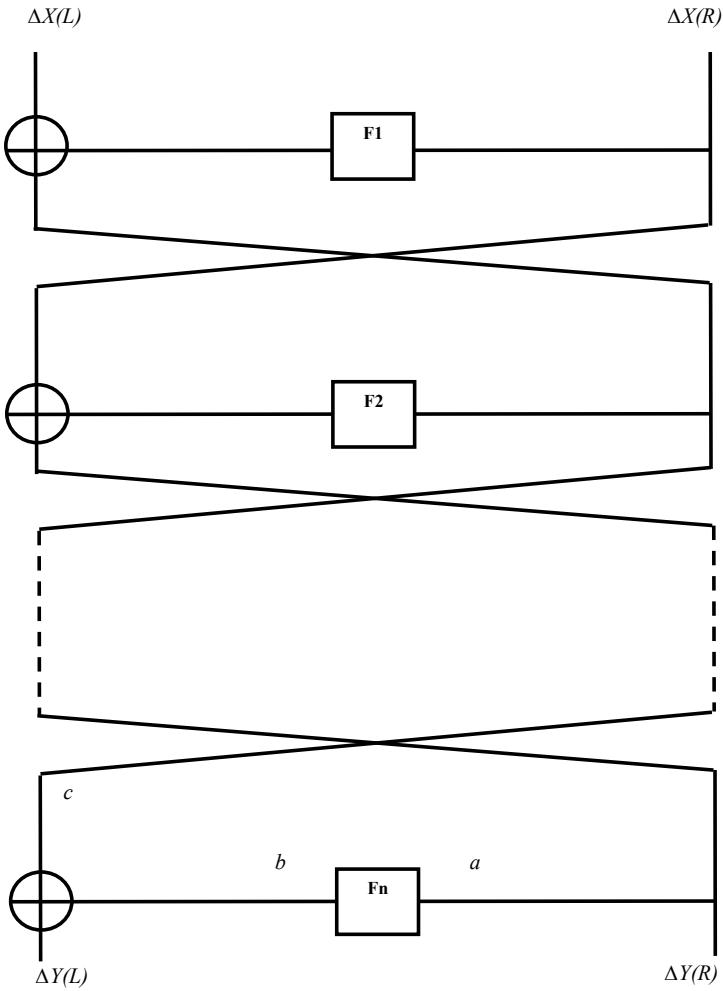
Демак, криптоалгоритмда фойдаланилган S-блок акслантиришларига нисбатан қурилган айирмалар матрицасига қараб, ушбу алгоритмнинг ДК усулига бардошли ёки бардошсиз эканлиги ҳақида дастлабки хулосаларни айтиш мумкин.

Қуйида Фейстель ва SP тармоғига асосланган шифрлаш алгоритмларига ДК усулини қўллашнинг умумий моҳиятлари келтирилган.

Фейстель тармоғига асосланган шифрлаш алгоритмлари учун дифференциал криптотаҳлил усули

Фейстель тармоғига асосланган шифрлаш алгоритмларига ДК усулини қўллашда дастлаб сўнгги раундда фойдаланилган махфий

калит қиймати аниқланади. Айтайлик, *n* та рауңддан иборат бирор шифрлаш алгоритми қаралаётган бўлсин (2.3.1-расм).



2.3.1-расм. Фейстель тармоғига асосланган шифрлаш алгоритми схемаси.

Мазкур ҳолда, 2.3.1-расмда ифодаланган белгилашлар ва қисм калитни аниқлашнинг юқорида келтирилган усулига (*test* – тўплам асосида) асосан, сўнгги раунд қисм калитларини аниқлашда криптотаҳлилчининг дастлабки асосий вазифаси юқори эҳтимоллик билан бажарилувчи *(a,b)* – жуфтликларни аниқлашдир. Мазкур жараён қаралаётган алгоритми акслантиришлари хусусияти боғлиқ ҳолда амалга оширилади.

Ушбу жуфтликлар топилгандан сўнг, калитни аниқлашдаги статистика жараёнида фойдаланилувчи, XOR йиғиндиси ΔX га тенг бўлган бир нечта очиқ матнлар жуфтлиги ва уларга мос равишда ўнг ярим қисмининг XOR йиғиндиси $\Delta Y(R)$ га тенг бўлган шифр матнлар жуфтлигини танлаш лозим.

Схема хусусиятига кўра, *Fn* – функцияга кирувчи *a* – айирма қиймати учун $a=\Delta Y(R)$ тенглик ўринли ва ушбу айирмани берувчи матн жуфтликлари (яъни, шифр матнларнинг ўнг ярим қисми) ҳам маълум.

Fn – функциядан чиқувчи *b* – айирма қиймати учун $b=\Delta Y(L)\oplus c$ тенглик ўринли бўлиб, $\Delta Y(L)$ – нинг қиймати маълум. Шунга кўра, тенгликдаги *c* – қийматни аниқлаш эса, 1-раундга кирувчи айирмаларни маълум эҳтимоллик билан раунд акслантиришидан ўзгаришини кузатиш орқали амалга оширилади.

Кузатилаётган айирма иккита матн йиғиндисидан иборат бўлганлиги сабабли, айирма қийматини раунд акслантиришларидан ўтказишда, ушбу акслантиришларни қуйидаги тенгликни бажариш ёки бажармаслик хоссаси муҳим аҳамият касб этади:

$$F(x1)\oplus F(x2)=F(x1\oplus x2) \qquad (2.3.4)$$

Агарда бирор акслантириш учун унга кириши мумкин бўлган барча қийматларда (2.3.4) тенглик бажарилса, у ҳолда ушбу акслантиришга кирувчи айирма акслантириш амалига мос тарзда чиқувчи айирма аксланади. Аксинча, тенглик бажарилмаса, кирувчи айирма қиймати ушбу акслантиришга нисбатан тузилган айирмалар матрицаси жадвалига мувофиқ чиқувчи айирмага ўзгаради. Ихтиёрий функция учун айирмалар матрицасини тузиш юқоридаги каби амалга оширилади.

Демак, раунд финкциясига кирувчи ва чиқувчи айирма қийматларини билган ҳолда, *test* – тўплам тузиш орқали қисм калит қийматлари аниқланади. Маълумки, ушбу тўплам чизиқсиз (S-блок)

акслантиришга кирувчи ва чиқувчи айирмаларга нисбатан амалга оширилади. *(a,b)* – жуфтликлар аниқланганидан сўнг, ушбу функция таркибидаги чизиқсиз акслантиришларга нисбатан кирувчи ва чиқувчи қийматларни ҳам қийинчиликсиз аниқлаш мумкин.

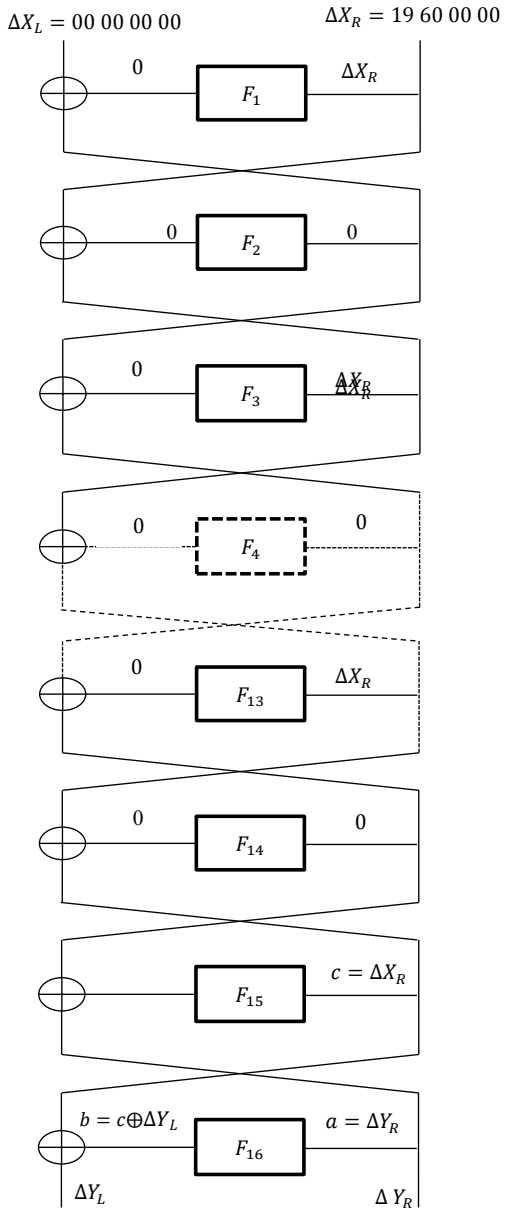
Келтирилган фикрларга асосланган ҳолда Фейстель тармоғига асосланган шифрлаш алгоритми учун ДК усулини қўллашнинг умумий алгоритми қуйидагича (схемадаги белгилашлардан фойдаланилади):

1. Сўнгги раунд k_i – қисм калитини аниқлашда фойдаланиладиган c – айирма қийматининг бажарилиш эҳтимоллиги максимал ($P>2/2^n$) бўлишини таъминловчи $(\Delta X, \Delta Y)$ – жуфтлик аниқлансин.
2. *(a,b)* – жуфтлик қийматлари орқали сўнгги раунд чизиқсиз функциясига кирувчи ва чиқувчи *(a1,b1)* – жуфтлик қийматлари аниқлансин.
3. Очиқ матн учун $\Delta X=x_i \oplus x_j$ ва шифр матн учун $\Delta Y(R)=y(r)_i \oplus y(r)_j$ – шартлар ўринли бўлувчи (X_i, X_j, Y_i, Y_j) – жуфтликлар аниқлансин.
4. 2- ва 3- қадамда аниқланган жуфтликлар асосида навбатдаги *Test* – тўплам тузилсин.
5. Агар барча *Test* – тўплам элементларини кесиштириш натижасида ягона қиймат ҳосил бўлса ёки қайсидир қиймат қолган қийматларга нисбатан сезиларли даражада кўплаб *Test* – тўпламлар таркибида ҳосил бўлса, ушбу қийматни k_i – қисм калит варианти сифатида эълон қилинсин, акс ҳолда 3-қадамга қайтилсин.
6. Тамомлансин.

Шифрлаш алгоритмининг ихтиёрий раунд калитларини аниқлаш ҳам шу алгоритм асосида амалга оширилади (яъни дастлаб n – раунд, кейин n-1 – раунд, ..., 1-раунд калити аниқланади).

Қуйида, 16 раундли DES шифрлаш алгоритми учун ДК усулини қўллашга намуна келтирилган.

Мазкур намуна сўнгги раундга кирувчи ва чиқувчи бўлган эффектив айирмаларни аниқлашга қаратилган (2.3.2-расм).



2.3.2-расм. DES шифрлаш алгоритми учун оптимал айирмани кузатиш схемаси.

Бу ерда, c – айирма эҳтимоллигини юқори бўлишини таъминловчи кирувчи айирмалар сифатида S-блокнинг айирма матрицасига нолдан фарқли айирма кирганда нол айирма чиқишини таъминловчи қийматларни олиш мумкин. Мазкур айирмалардан бири сифатида “19 60 00 00 00_{16}” – айирма қийматини олиш мумкин. Чунки, ушбу 32 битлик айирма қиймати раунд функциясидан ўтказилганда раунд чиқишида “00 00 00 00 00_{16}” – айирма қийматни ҳосил бўлиши кузатилади. Буни қуйидагича кузатиш мумкин.

Таъкидлаш керакки, DES алгоритмининг Фейстель функцияси таркибидаги *кенгайтириш* ва *ўрин алмаштириш* акслантиришлари учун (2.3.4) тенглик бажарилади, S-блок жадвали учун эса бажарилмайди.

DES шифрлаш алгоритми раунд функцияси акслантиришларига мувофиқ, раундга кирувчи “19 60 00 00 00” – қиймат кенгайтириш акслантиришидан ўтгандан сўнг, S_1-блокка “000011_2”, S_2-блокка “110010_2”, S_3-блокка “101100_2”, қолган барча S-блокларга эса “000000_2” айирма кириши кузатилади.

S-блок жадвалларининг айирмалар матрицасига мувофиқ, ушбу нолдан фарқли айирмалар мос равишда p_1=14/64, p_2=8/64 ва p_3=10/64 эҳтимоллик билан “0000_2” айирмаларга аксланади. Кирувчи нол айирмалар эса, p=1 эҳтимоллик билан “0000_2” айирмаларга аксланади. S-блокдан чиқувчи нол айирмаларни DES алгоритми Фейстель функциясининг сўнгги ўрин алмаштириш акслантиришидан ўтказиш натижасида ҳам нол айирмалар ҳосил бўлади.

Демак, схемада тасвирлангани каби, ушбу намуна учун $a=\Delta Y_L$ ва $b=c\oplus\Delta Y$ – тенгликлар ўринли бўлиб, c – айирманинг бажарилиш эҳтимоллиги қуйидагича:

$$p_{um} = \left(\frac{14}{64} * \frac{8}{64} * \frac{10}{64}\right)^6 = \left(\frac{35}{8192}\right)^6 \approx \left(\frac{1}{2^{7.87}}\right)^6 = 2^{-47.22}$$

Мазкур қийматлар, сўнгги раунднинг S_1, S_2, S_3 – блоклар киришида фойдаланилган мос равиш $k_1 \in 2^6$, $k_2 \in 2^6$ ва $k_3 \in 2^6$ – қисм калит қийматларини топишга хизмат қилади.

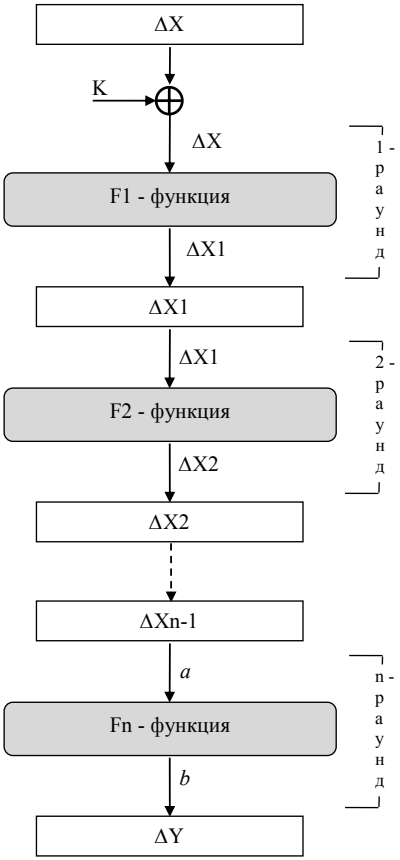
SP тармоғига асосланган шифрлаш алгоритмлари учун ДК усули

SP тармоғига асосланган шифрлаш алгоритмларига ДК усулини қўллашда ҳам Фейстель тармоғига нисбатан юқорида келтирилган фикрлар ўринли. Бироқ мазкур ҳолда сўнгги раунд калитларини аниқлаш жараёни тубдан фарқ қилиб, ушбу жараён қуйидагича амалга оширилади.

Айтайлик n та раунддан иборат бирор шифрлаш алгоритми қаралаётган бўлсин (2.3.3-расм). Алгоритм хусусиятига кўра, мазкур ҳолда b=ΔY тенглик ўринли бўлиб, ушбу айирмани берувчи шифр матн жуфтликлари ҳам маълум. Fn – функцияга кирувчи a – айирма қиймати эса, 1-раундга кирувчи айирмани маълум эҳтимоллик билан раунд акслантиришидан ўзгаришини кузатиш орқали аниқланади. Шунингдек, SP тармоғига асосланган аксарият шифрлаш алгоритмларининг раунд функцияси таркибидаги сўнгги акслантириш раунд калитларини қўшиш ҳисобланади.

Шунга кўра, юқори эҳтимоллик билан топилган (a,b) – жуфтликлар асосида **сўнгги раунднинг k_i калитини аниқлаш**да қуйидаги кетма-кетликдан фойдаланиш мумкин:

1. $a_i=x_1 \oplus x_2$ – шартни қаноатлантирувчи x_1 ва x_2 – матнларнинг бўлиши мумкин бўлган қийматлар тўплами ҳосил қилинади (k_i, a_i, x_1, x_2 – ларнинг ўлчами алгоритмдаги S-блок ўлчамига тенг).
2. Ҳосил қилинган x_1 ва x_2 – матнларнинг барча элементлари учун $d_i=F(x_1) \oplus F(x_2)$ – қийматлар ҳисобланади.
3. $d_i=b_i$ – шартни қаноатлантирувчи x_1 ва x_2 – матн қийматлари ажратиб олиб, уларни z_1 ва z_2 – тўпламлар орқали белгилаймиз.
4. b_i – айирмага мос бўлган y_1 ва y_2 – шифр матнларнинг изланаётган k_i қисмни қўшишдан ҳосил бўлган қийматлари учун $K_1=F(z_1) \oplus y_1$ ва $K_2=F(z_1) \oplus y_2$ – тўплам қийматлари ҳосил қилинади.
5. K_1 ва K_2 – тўплам қийматлари изланаётган k_i калитнинг мумкин бўлган вариантлари бўлади.



2.3.3-расм. SP тармоғига асосланган шифрлаш алгоритми схемаси.

Қуйида SP тармоғига асосланган ўқув шифрлаш алгоритмига чизиқли криптотаҳлил усулининг қўлланиши бўйича намуна келтирилади.

Мазкур намуна берилган айирма ҳамда унга мос очиқ ва шифр матн асосида сўнгги раундда фойдаланилган қисм калитни топишга қаратилган.

Қаралаётган 3 раундли ўқув шифрлаш алгоритми (2.3.4-расм) раунд функциясида 3 та бир хил S – блок жадвалидан фойдаланилган бўлиб, у қуйидагича:

2.3.4-жадвал.

S-блок жадвали

Кириш	0	1	2	3	4	5	6	7
Чиқиш	7	0	6	5	2	1	3	4

2.3.5-жадвал.

S-блок жадвалининг айирмалар матрицаси

b / *a*	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	8	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4
2	0	4	0	0	0	4	0	0
3	0	0	4	0	0	0	4	0
4	0	4	0	0	0	4	0	0
5	0	0	4	0	0	0	4	0
6	0	0	0	0	8	0	0	0
7	0	0	0	4	0	0	0	4

Айтайлик, $\Delta X=001001000_2$ – кирувчи айирма берилган бўлсин.

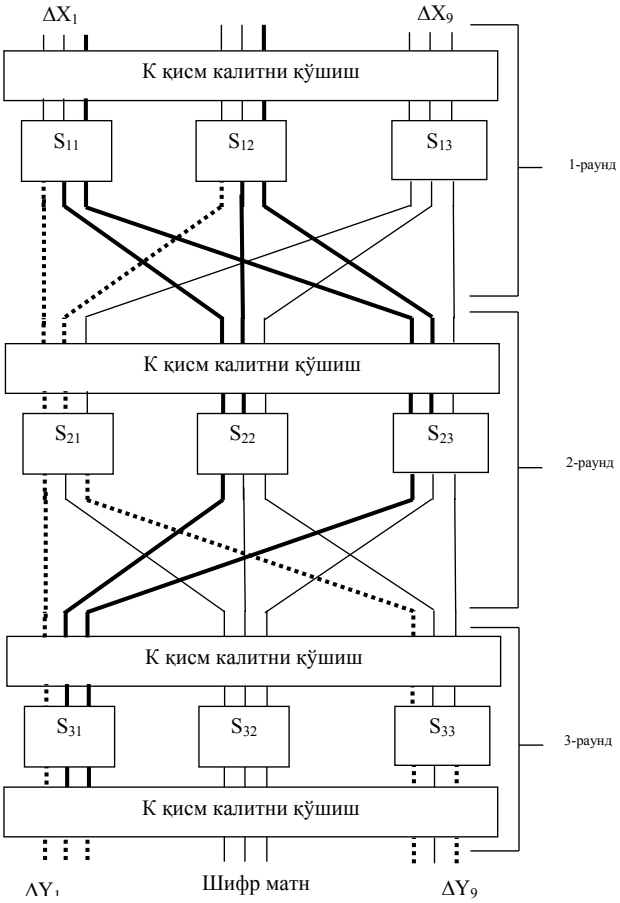
Демак, 1-раунд киришида 001_2 қиймат S_{11} ва S_{12} блокларга, 000_2 қиймат S_{13} блокка киради. Айирма матрицадан маълумки, 000_2 айирма кирганда ҳар доим 000_2 айирма чиқади. Шунинг учун S_{13} блокдан чиқувчи айирма 000_2 га тенг. 2.3.5-жадвалга кўра 001_2 айирма кирганда, чиқувчи айирма 011_2 ёки 111_2 га тенг бўлади. Натижада, биринчи раунд ўрин алмаштиришларидан кейин иккинчи раундга {*xx*0 110 110} айирма киради. Бу ерда *x* номаълум бит ҳисобланади. Шунингдек, 2.3.5-жадвалга кўра, кирувчи айирма 110_2 га тенг бўлса, чиқувчи айирма 100_2 га тенг бўлади. Агар кирувчи айирма 010_2 ёки 100_2 бўлса, чиқишдаги айирма 001_2 ёки 101_2 га тенг бўлади. Шундай қилиб, ўрин алмаштиришлардан кейин, учинчи раундга {*x*11 000 *x*0*x*} айирма кириб келади. Бундай ҳолда S_{31} блокка кирувчи айирма 011_2 ёки 111_2 га тенг бўлиши мумкин. 011_2 орттирма кирганда чиқувчи айирма 010_2 ёки 110_2 га тенг, 111_2 кирганда эса чиқувчи айирма 011_2 ёки 111_2 бўлиши мумкин.

Берилган айирмага мос очиқ ва шифр матнлар жуфтлиги қуйидагича бўлсин:

2.3.6-жадвал.

Очиқ ва шифр матн жуфтликлари

№	X	Y	X'	Y'
1	111010111	011111111	110011111	000111111
2	011001001	101110001	010000001	011110001
3	011101110	011000100	010100110	101000101
4	110101000	110101000	111100000	001101000
5	110100111	001111001	111101111	110111001



2.3.4-расм. SP тармоғига асосланган шифрлаш алгоритми схемаси.

2.3.6-жадвалда биринчи жуфтлик матнни таҳлил жараёнини кўриб чиқамиз. Бу кирувчи очиқ матнга мос келувчи, чиқувчи шифр матннинг айирмаси $\Delta Y=011111111_2 \oplus 000111111_2= 011000000_2$ га тенг.

Демак, 000_2 га тенг бўлмаган айирма S_{31} блокларда мавжуд. S_{31} блокдан чиқувчи айирма эса 011_2 га тенг. Олдин аниқланганидек, S_{31} блокка 011_2 ёки 111_2 айирма кириши мумкин.

2.3.5-жадвалга кўра S_{31} блокдан $\Delta Y_1=011_2$ айирма чиқиши учун кирувчи айирма 111_2 га тенг бўлиши лозим. 111_2 кирувчи айирма берувчи ифодалар эса қуйидагилар:

1. $000 \oplus 111$	5. $100 \oplus 011$
2. $001 \oplus 110$	6. $101 \oplus 010$
3. $010 \oplus 101$	7. $110 \oplus 001$
4. $011 \oplus 100$	8. $111 \oplus 000$

Ушбу кирувчи ҳар бир жуфтлик битларга мос келувчи чиқувчи ҳар бир жуфтликлар мавжуд бўлиб, фиксирланган S-блокларга асосан, бу жуфтликларнинг кўриниши қуйидагича:

1. $111 \oplus 100=011$	5. $010 \oplus 101=111$
2. $000 \oplus 011=011$	6. $001 \oplus 110=111$
3. $110 \oplus 001=111$	7. $011 \oplus 000=011$
4. $101 \oplus 010=111$	8. $100 \oplus 111=011$

S_{31} блокдан чиқувчи айирма қиймат 011_2 га тенг. У қабул қилиши мумкин бўлган қийматлар 1,2,7,8 ифодаларда ҳосил бўлади. S_{31} дан чиқган қийматга қисм калит ҳисобланган K_1 ни қўшганимизда бизга маълум бўлган шифр матн ҳосил бўлиш керак. Натижада, қуйидаги тенгламаларга келамиз:

$111 \oplus K_1=011$	$011 \oplus K_1=011$
$100 \oplus K_1=000$	$000 \oplus K_1=000$
$100 \oplus K_1=011$	$000 \oplus K_1=011$
$111 \oplus K_1=000$	$110 \oplus K_1=000$

Ушбу тенгламалардан қисм калит ҳисобланган K_1 ни топадиган бўлсак, қуйидаги 100_2 ёки 111_2 ёки 000_2 ёки 011_2 қийматларни қабул қилиши мумкин.

Шу тартибда юқорида келтирилган бошқа очиқ ва шифр матнлар учун ҳам калит вариантларини тузиш мумкин бўлиб, уларни кесиштириш орқали калитнинг ягона қийматини аниқлаш мумкин.

Умумий ҳолда блок узунлиги n – бит бўлган мавжуд ёки янги таклиф этилган блокли симметрик шифрлаш алгоритмини ДК усулига бардошлилигини баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.3.7-жадвал.

Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Алгоритм тегишли акслантиришларига нисбатан айирмалар матрицасини тузиш	Матрицани амалий қуриш мумкин	Кейинги босқичга ўтиш мумкин
		Матрицани амалий қуриб бўлмайди	Алгоритмни ДК усулига баҳолаб бўлмайди
II.	Сўнгги раунднинг изланаётган k_i – қисм калитини аниқлашда фойдаланиладиган *(a,b)* –қийматнинг бажарилиш эҳтимоллиги максимал ($p>1/2^n$) бўлишини таъминловчи *(ΔX, ΔY)* – оптимал айирмани аниқлаш	Айирма мавжуд ($p>1/2^n$)	Кейинги босқичга ўтиш мумкин
		Айирма мавжуд эмас ($p\leq 1/2^n$)	Алгоритм ДК усулига назарий бардошли
III.	Оптимал айирмага мувофиқ статистика учун лозим бўлган матнлар сони – W ни аниқлаш ($W \geq \frac{1}{p}$)	$W\leq 2^n$	Кейинги босқичга ўтиш мумкин
		$W>2^n$	Алгоритм ДК усулига назарий бардошли
IV.	W та матн устида статистика ўтказиш орқали калит қийматини аниқлаш учун талаб этилувчи умумий	Реал вақт мобайнида N та амални бажариш амалий мумкин	Кейинги босқичга ўтиш мумкин

2.3.7-жадвалнинг давоми.

	амаллар сони – *N* ни аниқлаш	Реал вақт мобайнида *N* та амални бажаришнинг амалий имкони йўқ	Алгоритм ДК усулига амалий бардошли
V.	Айирма ва матн жуфтликлари асосида статистика ўтказиб, изланаётган калит қийматини аниқлаш	Статистика натижа берди ва калит аниқланди	Алгоритм ДК усулига бардошсиз
		Статистика натижа бермади ва калит топилмади	Алгоритм ДК усулига амалий бардошли

Назорат саволлари

1. Дифференциал криптотаҳлил усулининг асосий қадамлар кетма-кетлиги нимадан иборат?

2. Фейстель тармоғига асосланган шифрлаш алгоритми учун дифференциал криптотаҳлил усулининг асосий моҳияти нимадан иборат?

3. SP тармоғига асосланган шифрлаш алгоритми учун дифференциал криптотаҳлил усулининг асосий моҳияти нимадан иборат?

4. Айирма матрица тушунчасига таъриф беринг ва ундан криптотаҳлил жараёнида қандай мақсадда фойдаланишини изоҳланг.

5. IN ва Test тўплам тушунчаларига таъриф беринг ва улардан криптотаҳлил жараёнида фойдаланишини изоҳланг.

6. Тузилган Test тўпламлар кесишмаси бўш тўпламни ташкил этиши мумкинми, агар мумкин бўлса, у қандай ҳолларда юз беради?

7. Оптимал дифференциал тушунчасига изоҳ беринг ва унинг таҳлил самарадорлигига таъсирини тушунтиринг.

8. Фейстель тармоғига асосланган шифрларга нисбатан икки ва ундан ортиқ раунд учун оптимал айирмани аниқлашнинг қандай усуллари мавжуд?

9. Айирма қийматидаги бирлар сони криптотаҳлил самарадорлигига қандай таъсир кўрсатади?

10. Шифрлаш алгоритми таркибидаги ўрин алмаштириш акслантиришининг таҳлил самарадорлигига таъсири қандай?

11. Шифрлаш алгоритми раундлар сони криптотаҳлил самарадорлигига қандай таъсир кўрсатади?

12. Криптотаҳлил жараёни учун бир нечта очиқ матн ва уларга мос шифр матн қийматлари нима учун талаб этилади?

13. Дифференциал криптотаҳлил асосида шифрлаш алгоритми барча раунд калитларини топиш босқичларини тушунтиринг.

14. Дифференциал криптотаҳлил усулини статистик ҳужум турига тегишли эканлигини изоҳланг.

15. Дифференциал криптотаҳлил усули самарадорлиги нималарга боғлиқ?

16. Дифференциал криптотаҳлил усулининг чизиқли ва бошқа криптотаҳлил усулларидан афзал ва камчилик жиҳатлари нимада?

2.4. Чизиқли-дифференциал криптотаҳлил усули

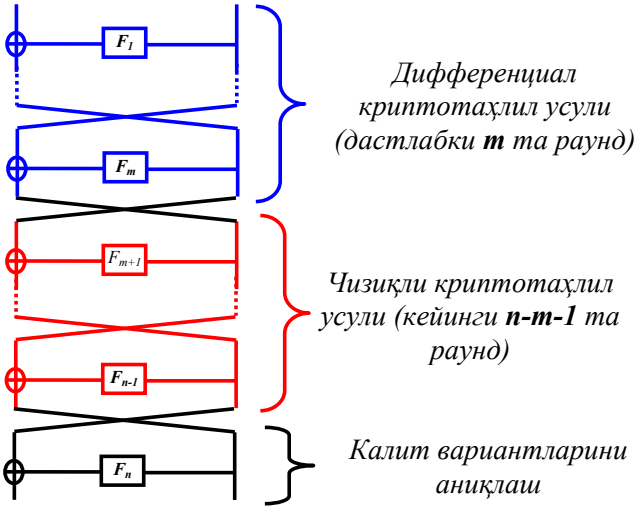
Чизиқли – дифференциал криптотаҳлил (ЧДК) усули [33] – Мартин Хеллман ва Сьюзен Лангфорд томонидан 1994 йилда DES шифрлаш алгоритмига қарши ҳужум тури сифатида таклиф этилган. Ушбу криптотаҳлил усули асосан Фейстель тармоғига асосланган шифрларга қўлланилиб, **танланган очиқ матн асосидаги ҳужум тури** синфи таркибига киради.

Ғоя муаллифлари томонидан ЧДК усулини қўллаб, 512 та очиқ матн ёрдамида DES шифрлаш алгоритмида фойдаланилган махфий калит 10 битини 80% эҳтимоллик билан аниқлашга эришилган. Очиқ матн сонини 768 тага ошириш орқали бу эҳтимоллик қийматини 95% гача етказиш мумкин.

Шунингдек, ушбу криптотаҳлил усули бугунги кунга қадар турли мутахассислар томонидан DES, Serpent, ГОСТ 28147-89 ва бошқа айрим шифрлаш алгоритмларига қўлланилган ва тегишли натижалар олинган.

ЧДК усули қурилиш тамойили чизиқли криптотаҳлил (ЧК) ҳамда дифференциал криптотаҳлил (ДК) усулларини умумлаш-

тиришга асосланган бўлиб, Фейстель тармоғига асосланган *n* раундли шифрлаш алгоритми учун унинг умумий қўлланилиш схемаси 2.4.1-расмда келтирилган.



2.4.1-расм. ЧДК усулининг умумий қўлланиш схемаси.

Яъни криптотаҳлилнинг дастлабки қадамида кирувчи (1-раундга кирувчи) айирмани билган ҳолда *m* – рауңдан чиқувчи айирма қиймати ДК усули орқали аниқланади, кейинги қадамда *n-1* - рауңдан чиқувчи айирма қиймати ЧК усули орқали аниқланади. Сўнгги қадамда эса охирги раунд функциясига кирувчи ва функциядан чиқувчи айирма ва шифр матн қийматларини билган ҳолда сўнгги раунд функциясида фойдаланилган калит вариантлари статистика ўтказиш (текшириб кўриш) орқали аниқланади.

Криптотаҳлил самарадорлиги ҳам айнан ДК ва ЧК усуллари самарадорлигига, яъни улар орқали аниқланган сўнгги раунд функциясидан чиқувчи айирма қийматининг тўғри аниқланганлигига боғлиқдир.

Қуйида, 7 раундан иборат бўлган DES шифрлаш алгоритмига ЧДК усули қўлланилишига намуна келтирилган [1, 44, 60].

Мазкур намунада, ЧДК усулини қўллаш учун қуйидаги таҳлил параметрлари танланган:

Кирувчи айирма: $\Delta X=(\Delta X_L, \Delta X_R)=(60000000_{16}, 00000000_{16})$;

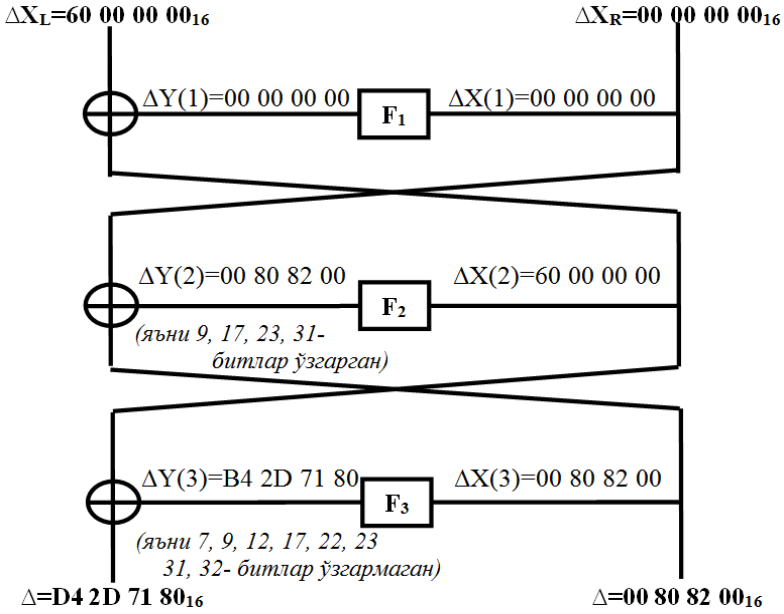
ДК усули қўлланилувчи раундлар: *даслабки 3 та (1 дан 3 гача) раунд;*

ЧК усули қўлланилувчи раундлар: *кейинги 3 та (4 дан 6 гача) раунд;*

Криптотаҳлил ўтказишдан мақсад: *сўнгги раундда фойдаланилган* $K(7) \in 2^{48}$ *раунд калитининг дастлабки* $K(7)_1 \in 2^6$ *қисм калит қийматини аниқлаш.*

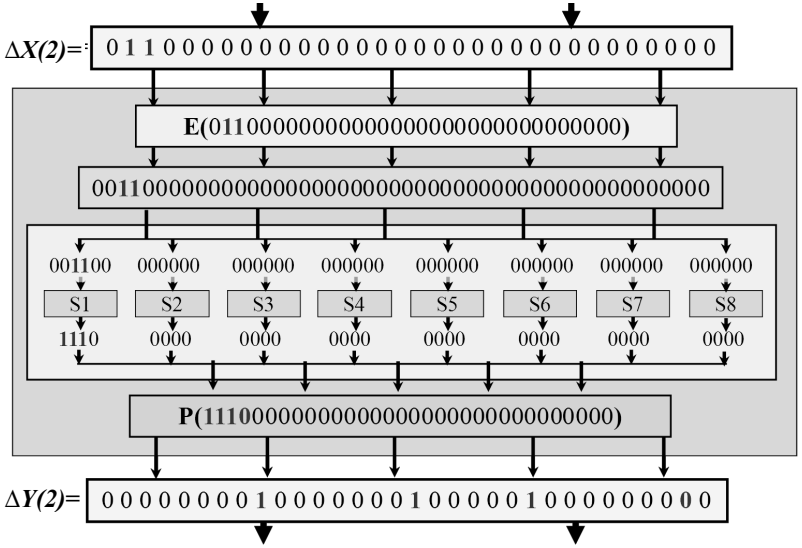
DES шифрлаш алгоритми бошланғич *IP* ва охирги IP^{-1} ўрин алмаштириш акслантиришлари криптотаҳлил қийинчилигига ва унинг самарадорлигига таъсири йўқлиги учун, уларни ташлаб ўтиш (криптотаҳлил кетма-кетлигини осон тушунтириш мақсадида) мумкин.

Криптотаҳлилнинг дастлабки қадамида ДК усули орқали алгоритмнинг 3-раундидан чиқувчи айирма қиймати аниқланади (2.4.2-расм).



2.4.2-расм. ДК усулини қўллаш натижаси.

Кирувчи ΔX айирма қийматига кўра, дастлабки раунд функциясига (F_1) нол айирма киради. Ушбу ҳолда, ДК усулига мувофиқ F_1 – функция чиқишида ҳам нол айирма ҳосил бўлади. $\Delta X(2)$ айирма қийматига кўра, F_2 – функция таркибидаги S_1 – блокнинг киришига нолдан фарқли айирма (яъни, 001100_2 қиймат), қолган барча блоклар киришига эса нолга тенг бўлган айирма киради. Шунга мувофиқ, F_2 – функциядан юқори эҳтимоллик билан 00808200_{16} айирма (айирмани раунд S блокларидан ўтказишда тегишли айирма матрицаси жадвалидан фойдаланилади ва юқори эҳтимолликда чиқувчи айирма танланади) чиқади (2.4.3-расм).



2.4.3-расм. F_2 – функцияга кирувчи айирманинг ўзгариш жараёни.

Демак, F_2 функция акслантиришларидан ўтувчи айирма қиймати ўзгаришига кўра, ушбу функциядан чиқувчи айирманинг 9, 17, 23 ва 31-ўринларидаги битлар қиймати маълум эҳтимоллик билан ҳосил бўлган, яъни кирувчи айирмага нисбатан ўзгарганлиги, қолган ўриндаги битлар қиймати эса p=1 эҳтимоллик билан ўзгармаганлиги (яъни нолга тенг) кузатилади.

Кейинги 3-раунд учун эса $\Delta X(3)$ айирма қиймати ўзгаришини кузатиш орқали F_3–функциядан юқори эҳтимоллик билан $B42D7180_{16}$ айирма чиқиши маълум бўлади (2.4.4-расм). Мазкур ҳол учун кўриш мумкинки, F_3 функциядан чиқувчи айирманинг 7,

9, 12, 17, 22, 23, 31 ва 32-ўринларидаги битлар қиймати p=1 эҳтимоллик билан ўзгармаганлиги (яъни, нолга тенг), қолган ўриндаги барча битлар қиймати эса маълум эҳтимоллик билан ўзгарганлиги кузатилади.

Демак, ДК усули орқали алгоритмнинг 3-раундидан чиқувчи айирма қиймати Δ=D42D718000808200$_{16}$ – эканлиги аниқланди.

Криптотаҳлилнинг кейинги қадамида ЧК усулини навбатдаги 3 та раундга қўллаш орқали алгоритмнинг 6-раундидан чиқувчи тегишли ($K(7)_1$ – қисм калитни аниқлаш имконини берувчи) айирма қиймати аниқланади (2.4.5-расм).

ЧК усулининг S – блок жадваллари учун аппроксимация тенгламаларини тузиш қоидасига асосан, DES алгоритми S_5 – блокига нисбатан p=3/16 эҳтимоллик билан бажарилувчи қуйидаги (1) аппроксимация тенгламасини қуриш мумкин:

$$X_2 \oplus Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4 = K_2 \qquad (2.4.1)$$

Ҳосил қилинган аппроксимация тенгламасини DES алгоритми кенгайтириш ҳамда ўрин алмаштириш акслантиришларини ҳисобга олган ҳолда 4-раунд функцияси кириши ва чиқишига кўра ифодаланса, қуйидаги (2.4.2) аппроксимация тенгламасига эга бўлинади:

$$X(4)_{17} \oplus Y(4)_3 \oplus Y(4)_8 \oplus Y(4)_{14} \oplus Y(4)_{25} = K(4)_{26} \qquad (2.4.2)$$

бу ерда, $(N)_m$ ифода учун N – раунд қийматини, m – бит ўрнини англатади.

4-раунд учун ҳосил қилинган аппроксимация тенгламаси каби 6-раунд учун ҳам айнан S_5 – блокка нисбатан аппроксимация тенгламасини тузиб ҳамда 3 та раунд учун статистик аналог тенгламасини қуриш усулига кўра 3-6-раунд учун умумий аппроксимация тенгламаси тузилса, қуйидаги (2.4.3) аппроксимация тенгламаси ҳосил бўлади:

$$X(4)_{17} \oplus Y(4)_3 \oplus Y(4)_8 \oplus Y(4)_{14} \oplus Y(4)_{25} \oplus X(6)_{17} \oplus Y(6)_3 \oplus Y(6)_8 \oplus Y(6)_{14} \oplus Y(6)_{25} = K(4)_{26} \oplus K(6)_{26} \qquad (2.4.3)$$

(2.4.3) аппроксимация тенгламаси четланиш қиймати $\Delta=\Delta_1*\Delta_2$=25/64 га, бажарилиш эҳтимоллиги эса p=(1–Δ)/2=39/128 .

Таҳлил жараёнида айирма (яъни 2 та кирувчи X_1 ва X_2 маълумотларнинг XOR йиғиндиси) кўриб чиқилаётганлиги сабаб,

ҳар бир кирувчи маълумот учун аппроксимация тенгламаси тузилиб, ҳосил бўлган иккита тенглама модул 2 бўйича ўзаро қўшилса, қуйидаги ўнг қисми нолга ва чап қисми модул 2 бўйича мос битларни йиғиндисига тенг бўлган (2.4.4) тенгликка эга бўлинади:

$$\Delta X(4)_{17} \oplus \Delta Y(4)_3 \oplus \Delta Y(4)_8 \oplus \Delta Y(4)_{14} \oplus \Delta Y(4)_{25} \oplus \Delta X(6)_{17} \oplus \Delta Y(6)_3 \oplus \Delta Y(6)_8 \oplus \Delta Y(6)_{14} \oplus \Delta Y(6)_{25} = 0 \quad (2.4.4)$$

X_1 ва X_2 маълумотлар бир хил қийматли калит ёрдамида шифрланганлиги сабабли, тенглама ўнг қисми нолга тенг бўлади. Унинг бажарилиш эҳтимоллиги эса X_1 ва X_2 маълумотлар учун тузилган аппроксимация тенгламалари эҳтимоллиги кўпайтмасига тенг, яъни: p=(39/128)*(39/128)≈0,0928. Бироқ ушбу тенглик чап тарафига “1” қийматни модул 2 бўйича қўшиш натижасида тенглама эҳтимоллиги p≈0,9072 га ўзгаради.

Фейстель тармоғи хусусиятига кўра, $\Delta Y(4)=\Delta X(3)\oplus\Delta X(5)$, $\Delta Y(6)=\Delta X(5)\oplus\Delta X(7)$ ва $\Delta X(6)=\Delta Y(7)\oplus\Delta Y(L)$ ифодалар ўринли. Ушбу ифодалардан фойдаланиш асосида тегишли алмаштиришлар бажариб, (2.4.4) тенгламани қуйидагича ифодалаш мумкин:

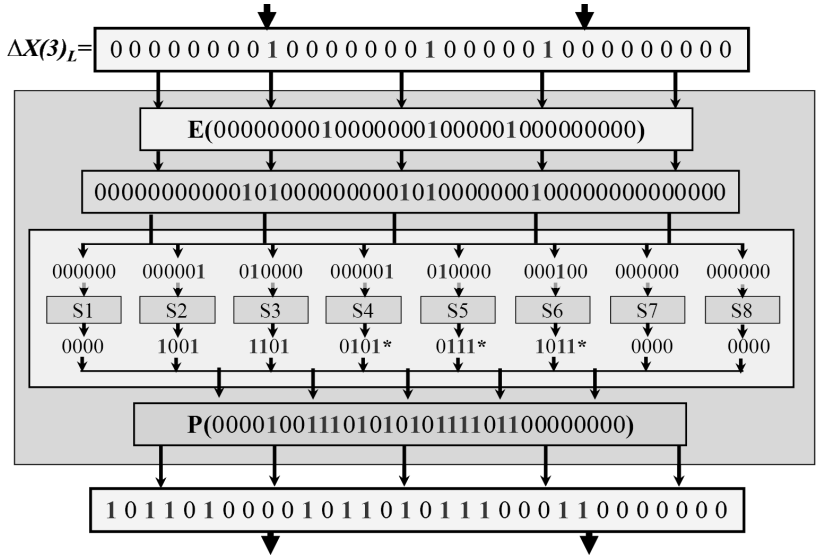
$$\Delta X(4)_{17} \oplus \Delta X(3)_3 \oplus \Delta X(3)_8 \oplus \Delta X(3)_{14} \oplus \Delta X(3)_{25} \oplus \Delta \boldsymbol{Y(7)_{17}} \oplus \Delta Y(L)_{17} \oplus \Delta X(7)_3 \oplus \Delta X(7)_8 \oplus \Delta X(7)_{14} \oplus \Delta X(7)_{25} = 0 \quad (2.4.5)$$

Дифференциал криптотаҳлил натижаси ва 7-раунддан чиқувчи айирма қийматлар маълумлигига кўра, (2.4.5) тенгламадаги $\Delta X(3)$, $\Delta X(4)$, $\Delta X(7)$ ва $\Delta Y(L)$ айирма қийматлари ҳам маълум. Демак, мазкур тенгламада фақатгина $\Delta \boldsymbol{Y(7)_{17}}$ – айирма қиймати номаълум бўлиб, уни ушбу тенгламани ечиш орқали аниқлаш мумкин. Айнан ушбу айирма қиймати $K(7)_1$ – қисм калитни аниқлаш учун хизмат қилади.

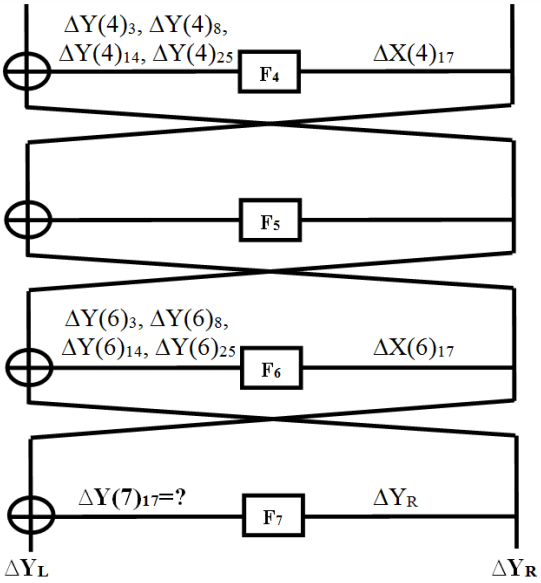
Криптотаҳлилнинг сўнгги қадами $K(7)_1$ – қисм калит қийматини аниқлашга қаратилади. Қуйида ушбу жараён умумий моҳияти келтирилган.

ЧК натижасига кўра, $\Delta Y(7)_{17}$ – айирма қиймати маълум. DES шифрлаш алгоритми раунд функцияси ўрин алмаштириш жадвалига мувофиқ эса, F_7 – функциянинг 17-чиқувчи бити S_1 – блокнинг 2-чиқувчи бити эканлиги келиб чиқади.

Танланган кирувчи айирмани қаноатлантирувчи бир нечта очиқ матн ва унга мос шифр матн қийматлари криптотаҳлилчига маълум. Сўнгги раунд функциясига кирувчи қиймат шифр матн ярим блокини ташкил этганлиги учун, F_7 – функцияга кирувчи матнлар ҳам криптотаҳлилчига маълум бўлади.

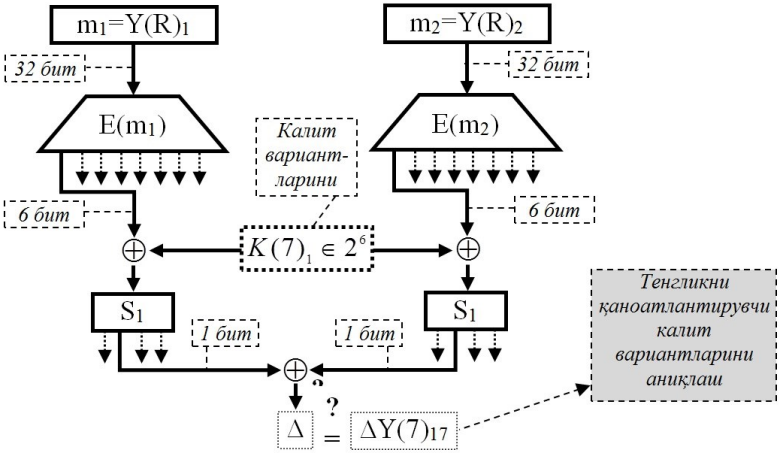


2.4.4-расм. F_3 – функцияга кирувчи айирманинг ўзгариш жараёни.



2.4.5-расм. ЧК усулини қўлланиш схемаси.

Демак, F_7 – функцияга кирувчи матн ҳамда S_1 – блокдан чиқувчи айирма 2-битини билган ҳолда, S_1 – блокка кирувчи 6 бит маълумот билан қўшилувчи калит битларини аниқлаш мумкин. Ушбу жараённи схематик модели қуйидагича (2.4.6-расм):



2.4.6-расм. Статистика орқали $K(7)_1$ – калит қийматини аниқлаш схемаси.

Яъни S_1 – блоки киришидаги 6 бит айирмани берувчи матн жуфтликларига қўшилиши мумкин бўлган $K_1(7) \in 2^6$ калитларни мос равишда қўшиш ва уларни S_1 – блокдан ўтказиш орқали ҳосил бўлган чиқувчи матнлар 2-битларининг йиғиндиси билан аввал аниқланган $\Delta Y(7)_{17}$ айирмани солиштириш орқали амалга оширилади. Натижада ЧДК усулини қўллаб калит битларини тўлалигича ва аниқ қийматини аниқлаш бир нечта очиқ ва унга мос бир хил калит билан шифрланган шифр матн жуфтликларини талаб этади.

Демак, тақдим этилган юқоридаги намуна таҳлилига кўра, **ЧДК усулининг Фейстель тармоғига асосланган блокли симметрик шифрлаш алгоритмига қўллаш учун қуйидаги масалалар ҳал қилиниши лозим**:

1). *Раундлар сонининг ДК ва ЧК усулларига тақсимланиши.*

2). *Керакли аппроксимация тенгламаларини тузиш.*

3). *Самарадорлиги юқори бўлган айирма кўринишини аниқлаш.*

4). *Сўнгги раунд калит қиймати вариантларини аниқлаш.*

Мазкур масалалар ечими таҳлил қилинаётган алгоритм тузилишига узвий боғлиқ бўлиб, уларни ечишда қуйидаги тавсияларга асосланиш мумкин:

– таҳлил қилинаётган шифрлаш алгоритмининг ДК ва ЧК усулларига тақсимланиши шифрлаш *алгоритми раундлар сонига* ҳамда *ДК ва ЧК усуллари самарадорлигига* (қўллаш мумкинлигига) боғлиқ тарзда аниқланади;

– ЧК усулини қўллаш орқали ҳосил қилинадиган аппроксимация тенгламалари *шифрлаш алгоритми раундлар сонига* ҳамда изланаётган *сўнгги раунд қисм калитига* боғлиқ тарзда тузиб олинади;

– таҳлил учун лозим бўлган айирма кўринишини *ДК самарадорлигига* ва тузилган *аппроксимация тенгламасига* боғлиқ тарзда аниқланади;

– сўнгги раунд калит қиймати вариантларини аниқлаш эса, юқорида келтирилган намуна каби статистика ўтказиш орқали аниқланади.

Умумий ҳолда, Фейстель тармоғига асосланган *n (n>4)* та раундли ва блок узунлиги *m* бит бўлган мавжуд ёки янги таклиф этилган симметрик шифрлаш алгоритмини ЧДК усулига бардошлилигини баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.4.1-жадвал.

Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Алгоритм тегишли акслантиришлари учун айирмалар матрицасини тузиш	Матрицани амалий қуриш мумкин	Кейинги босқичга ўтиш мумкин
		Матрицани амалий қуриб бўлмайди	ДК усулидан фойдаланиб бўлмайди
II.	ДК ва ЧК усулларининг тақсимланишини аниқлаш	ДК ва ЧК қўлланилувчи раундлар	Кейинги босқичга ўтиш мумкин

2.4.1-жадвалнинг давоми.

III.	Аниқланувчи сўнгги раунд қисм калитига ($K(n)_i$) боғлиқ ҳолда керакли (самарали) аппроксимация тенгламасини қуриш (ушбу тенглама орқали статистика учун керак бўлган $\Delta Y(n)_i$ – айирма қиймати аниқланади)	Самарали тенглама мавжуд	Кейинги босқичга ўтиш мумкин
		Самарали тенглама мавжуд эмас (тенглама қуриб бўлмайди *ёки* унинг бажарилиш эҳтимоллиги 0,5 га тенг)	ЧК усулидан фойдаланиб бўлмайди (ЧК қўлланилувчи раундни ўзгартириш лозим)
IV.	Аниқланган аппроксимация тенгламасига боғлиқ ҳолда, ДК қўлланилувчи раундлардан чиқувчи айирманинг бажаралиш эҳтимоллиги (p) максимал бўлишини таъминловчи кирувчи айирма қийматини аниқлаш	Айирма мавжуд ($p>1/2^n$)	Кейинги босқичга ўтиш мумкин
		Айирма мавжуд эмас ($p\leq 1/2^n$)	ДК усулидан фойдаланиб бўлмайди (ДК қўлланилувчи раундни ўзгартириш лозим)
V.	$\Delta Y(n)_i$ – айирма қийматининг ҳосил бўлиш эҳтимоллигига (p) боғлиқ тарзда статистика учун лозим бўлган матнлар сони – W ни аниқлаш ($W \geq \frac{1}{p}$)	$W\leq 2^m$	Кейинги босқичга ўтиш мумкин
		$W>2^m$	Алгоритм ЧДК усулига назарий бардошли
VI.	W та матн устида статистика ўтказиш орқали калит қийматини аниқлаш учун талаб этилувчи умумий амаллар сони – N ни аниқлаш	Реал вақт ичида N та амални бажариш амалий мумкин	Кейинги босқичга ўтиш мумкин
		Реал вақт ичида N та амални бажаришнинг амалий имкони йўқ	Алгоритм ЧДК усулига амалий бардошли

2.4.1-жадвалнинг давоми.

VII.	Айирма ва матн жуфтликлари асосида статистика ўтказиш орқали изланаётган $K(n)_i$ қисм калит қийматини аниқлаш	Статистика натижа берди ва $K(n)_i$ аниқланди	Алгоритм ЧДК усулига бардошсиз
		Статистика натижа бермади ва $K(n)_i$ аниқланмади	Алгоритм ЧДК усулига амалий бардошли

Назорат саволлари

1. Чизиқли-дифференциал криптотаҳлил усулининг асосий қадамлар кетма-кетлиги нималардан иборат?

2. Беш раундли S_DES алгоритмига чизиқли-дифференциал криптотаҳлил усулини қўллашда чизиқли криптотаҳлил усулидан кандай мақсадда фойдаланилади?

3. S_DES алгоритмига чизиқли-дифференциал криптотаҳлил усулини қўллаб, сўнгги раунд калит қийматини аниқлаш қадамлар кетма-кетлигини изоҳланг.

4. Раундлар сони турлича (5, 6, 7, ...) бўлган S_DES алгоритмига чизиқли-дифференциал криптотаҳлил усулини қўллашда қандай ўзгаришлар кузатилади?

5. Чизиқли-дифференциал криптотаҳлил усулида, чизиқли ҳамда дифференциал криптотаҳлил усуллари нималарга боғлиқ тарзда ўзаро раундларга тақсимланади?

6. Крипотаҳлил усули самарадорлиги қайси параметрларга боғлиқ?

7. Мазкур таҳлил усулида кирувчи айирма қийматини ихтиёрий танлаш мумкинми?

8. DES алгоритмига чизиқли-дифференциал криптотаҳлил усулини қўллашда чизиқли криптотаҳлил усулидан қандай мақсадда фойдаланилади?

9. Чизиқли-дифференциал криптотаҳлил усулида фойдаланиладиган аппроксимация тенгламаларининг сўнгги раунд қисм калити билан қандай боғлиқлиги бор?

10. Чизиқли ҳамда дифференциал криптотаҳлил усуллари тақсимланишида дастлаб чизиқли сўнгра дифференциал криптотаҳлил усулидан фойдаланиш мумкинми?

11. Таҳлил учун лозим бўлган кирувчи айирмани танлашда нималарга эътибор берилади?

12. Раундлар сони 10 бўлган DES алгоритмига чизиқли-дифференциал криптотаҳлил усулини қўллашда, чизиқли криптотаҳлил усулидан қайси раундларда фойдаланиш мумкин?

13. DES алгоритмига чизиқли-дифференциал криптотаҳлил усулини қўллаб, барча раундлар калит қийматларини аниқлаш кетма-кетлигини қандай амалга оширилади?

14. Чизиқли ва дифференциал криптотаҳлил усулига бардошли бўлган бирор шифрлаш алгоритми чизиқли-дифференциал криптотаҳлил усулига бардошсиз бўлиши мумкинми?

2.5. “Слайдли ҳужум” криптотаҳлил усули

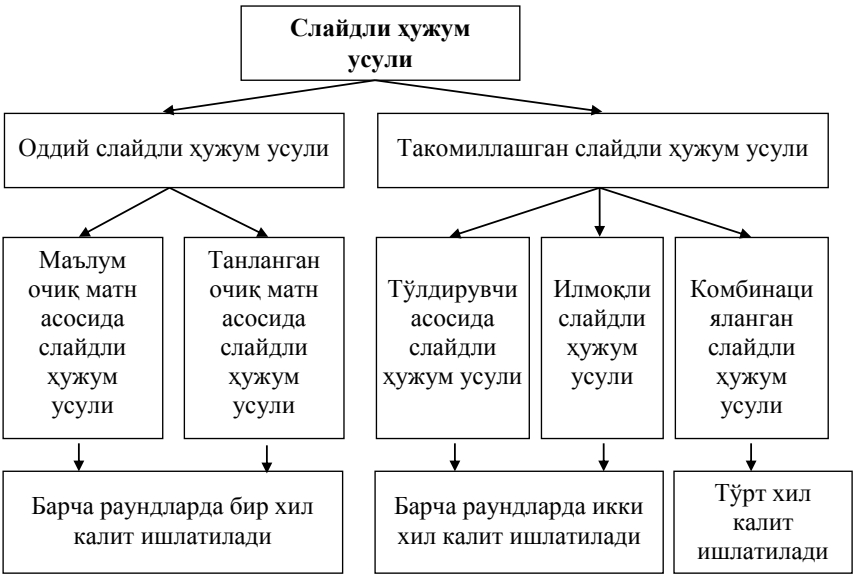
Фейстель тармоғига асосланган шифрлаш алгоритмларига нисбатан қўлланилувчи юқорида кўриб чиқилган замонавий криптотаҳлил усулларини ўтказишда, алгоритмда фойдаланилган раундлар сони катта аҳамиятга эга.

Шифрлаш алгоритмларида ҳар бир қўшилган раунд унда фойдаланилган чизиқсиз акслантиришларга қўйилган умумий криптографик талабларни қаноатлантирмаганда ҳам криптотаҳлилчи имкониятларининг кескин камайишига олиб келади.

Мазкур ҳолат шифрлаш алгоритми раундлари сонига боғлиқ бўлмаган “Слайдли ҳужум” ёки “Сирпанувчи ҳужум” (Slide attack) деб номланувчи янги криптотаҳлил усулини қўллаш заруриятини келтириб чиқарди. Ушбу криптотаҳлил усули 1999 йилда Алекс Брюков ва Дэвид Вагнерлар томонидан таклиф қилинган [33].

Бугунги кунга келиб мазкур криптотаҳлил усулининг қуйидаги икки тури кенг оммалашган (2.5.1-расм):

1. Оддий слайдли ҳужум.
2. Такомиллашган слайдли ҳужум.

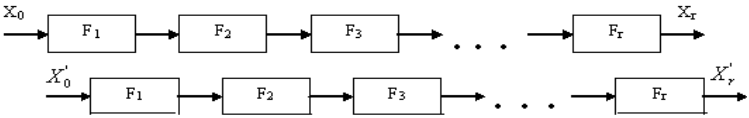


2.5.1-расм. Слайдли ҳужум криптотаҳлили усули классификацияси.

Статистик криптотаҳлил усуллари қаторига кирувчи мазкур ҳужум усулини қўллашда дастлаб бир нечта слайдли жуфтликларни аниқлаш талаб этилади. Криптотаҳлил асосий вазифаси, алгоритмнинг раунд калитларини топиш ва функциялари бардошлилигини баҳолашдан иборат.

2.5.1-таъриф. F – функция "*бардошсиз*" деб аталади, агар маълум $F(x_1,k)=y_1$ ва $F(x_2,k)=y_2$ икки тенгликдан k калитни аниқлаш осон бўлса [2, 3].

Мазкур усулнинг ғояси шундаки, жараёнлардан бири иккинчисидан бир раундга кечиктирилиб, иккита шифрлаш жараёнини ўзаро мос қўйиш асос қилиб олинади (2.5.2-расм).



2.5.2-расм. Оддий слайдли ҳужум схемаси.

Айтайлик, x_0 ва $x_0^{'}$ бошланғич очиқ матнлар ва улар мос кетма-кетликлари $x_j=F_j(x_{j-1})$ ва $x_j^{'}=F_j(x_{j-1}^{'}),\ j=\overline{1,...,r}$ берилган бўлсин.

2.5.1-тасдиқ. Агар $x_1 = x_0^{'}$ шарт бажарилса, у ҳолда уларга мос қийматлар жуфтлиги учун $x_r = x_{r-1}^{'}$ тенглик ўринли бўлади, яъни $x_{j+1} = F(x_j) = F(x_{j-1}^{'}) = x_j^{'}, \quad j = 1,...,r$ [2, 3].

2.5.2-таъриф. (P,C) ва (P',C') жуфтлик слайд жуфтлик дейилади, агар $F(P) = C$, $F(P^{'}) = C^{'}$, $C = P^{'}$, $F(P) = P^{'}$ ва $F(C) = C^{'}$ шартлар бажарилса [2, 3]. Бу ерда $(P,P^{'})$ – очиқ матнлар, $(C,C^{'})$ – эса уларга мос шифрматнлар.

Демак, агар $(P_i,C_i), (P^{'}_i,C^{'}_i)$ жуфтликлар слайд жуфтлик ҳосил қилса, у ҳолда $F(P_i) = P^{'}_i$ ва $F(C_i) = C^{'}_i$ тенгликлар ўринли бўлади. Фейстель тармоғига асосланган алгоритмларда $F((l,r),k) = ((l \oplus f(r),r),k)$ – функция раунд функциясига кирувчи маълумотнинг фақат ярмини модификациялайди. Шунинг учун $F(x) = x^{'}$ – шартни x маълумотнинг чап қисми ва $x^{'}$ маълумотнинг ўнг қисми билан таққослаш ёрдамида текшириш мумкин. Бу шарт маълум очиқ матн асосидаги ҳужумнинг мураккаблигини $2^{n/2}$ та маълум матнгача камайтиришга ёрдам беради [3].

Тўлдирувчи асосидаги слайдли ҳужум оддий слайдли ҳужумдан фарқли уларок икки раундли ўзига хос шифрлаш жараёни модели кўринишида ўтказилиб, иккита раундда фойдаланилган ҳар хил калитни топишга қаратилади. Икки раундли ўзига хос шифрлаш жараёнига оддий слайдли ҳужумни қўллаганда иккинчи жараённи икки раундга кечиктириб шифрлаш жараёнларини таққослаш мантиқан тўғри келади.

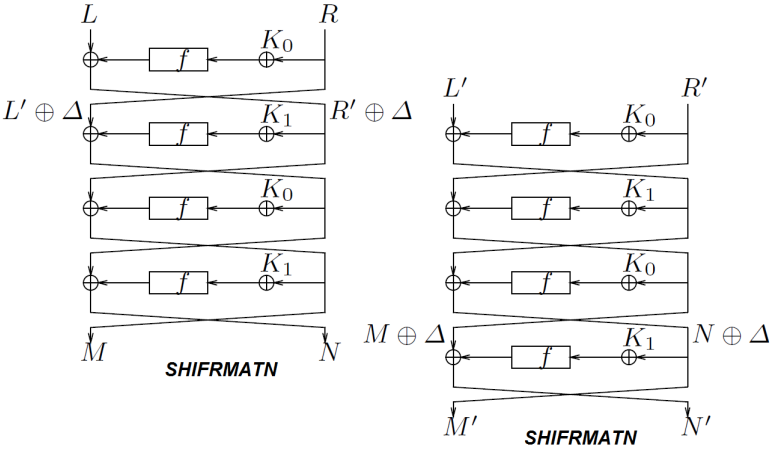
Агар ҳар бир раундда иккита шифрлаш жараёнлари ўртасида $\Delta = K_0 \oplus K_1$ калитлар фарқи киритилса, у ҳолда, бир раундга кечиктирилган шифрлаш жараёнларини таққослаш имконияти ҳосил бўлади. Бу ҳолатда икки раундли шифрлаш жараёнидан бир раундли ўзига хос шифрлаш жараёнига, ҳамда слайдли жуфтликлар ўртасида қандайдир Δ фарқга эга бўлинади. Бундай ҳужумни ўтказиш учун шундай очиқ ва шифр матнлар жуфтлигини танлаш керакки, улар фарқи калитлар фарқига тенг бўлиши лозим.

Агар $F(P) \oplus P' = \Delta$ тенглик ўринли бўлса, P ва P' очиқ матнлар жуфтлиги Δ слайдли фарқга эга бўлади. Ушбу фарқ p=1 эҳтимоллик билан раунддан-раундга ўтади ва шу йўл билан шифр матнлар фарқига олиб келади. Ушбу ҳолда очиқ матнни $P=(L,R)$ ва шифр матнни $C=(N,M)$ каби белгиланса қуйидаги:

$$(L', R') = (R, L \oplus f(K_0 \oplus R)) \oplus (\Delta, \Delta);$$
$$(N', M',) = (M \oplus f(K_1 \oplus N \oplus \Delta), N) \oplus (\Delta, \Delta);$$
$$L' = R \oplus \Delta \quad \textit{ва} \quad M' = N \oplus \Delta$$

тенгликка эга бўлинади (2.5.3-расм).

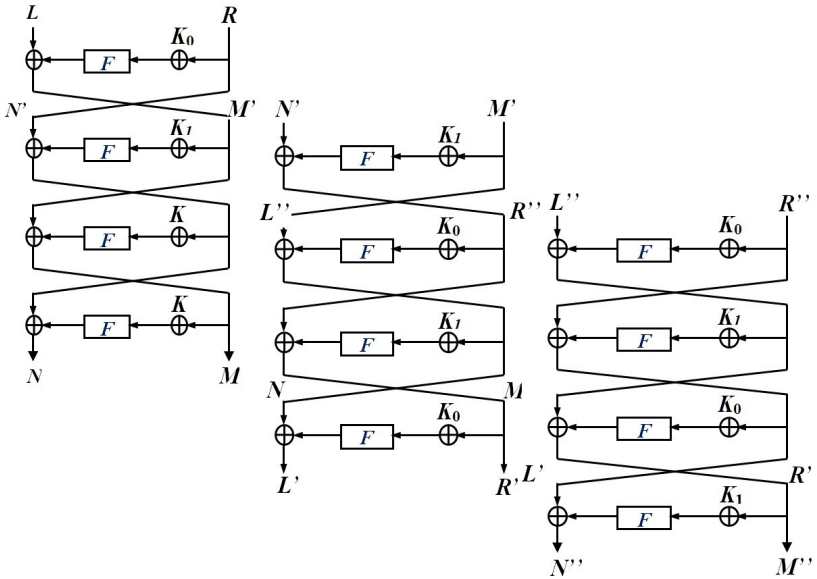
Шундай қилиб, $L' \oplus M' = R \oplus \Delta \oplus N \oplus \Delta = R \oplus N$ ва $R = L' \oplus \Delta$ дан $\Delta = R \oplus L'$ қийматни топиш мумкин. Ушбу усулда Δ фарқни топиш мураккаб бўлсада, мумкин бўлган калитлар сонини камайтириб, ҳақиқийсини аниқлаш имконияти мавжуд.



2.5.3-расм. Тўлдирувчи асосида слайдли ҳужум схемаси.

Фейстель тармоғига асосланган шифрлаш алгоритмларида (DES, S-DES каби) бошланғич ва охирги ўрин алмаштиришлар ҳисобга олинмаса, шифрлаш ва дешифрлаш жараёнлари калитларни тескари тартибда фойдаланиши билан фарқ қилади. Яъни, агар шифрлашда K_0 ва K_1 калитлар ишлатилган бўлса, дешифрлашда эса тескари тартибда K_1 ва K_0 кўринишида ишлатилади. Бундай ўхшашлик дешифрлаш жараёнини бир раундга кечиктириб, шифрлаш жараёнига мос қўйган ҳолда, "**Илмоқли слайдли ҳужум**" усулини ўтказиш имкониятини келтириб чиқаради (2.5.4-расм). Бунда шифрлашнинг биринчи раунди ва дешифрлашнинг охирги раундидан ташқари барча раундларда слайд жуфтликлар мос келади. Слайд жуфтликлар учун қуйидаги шартлар бажарилиши лозим [3]:

$$(N', M') = (R, L \oplus f(K_0 \oplus R)),$$
$$(L', R') = (M \oplus f(K_0 \oplus N), N).$$



2.5.4-расм. Илмоқли слайдли ҳужум схемаси.

$N'=R$ ва $R'=N$ тенгликлардан фойдаланиб, слайд жуфтликлар ёрдамида K_0 калитнинг битларини оддий слайдли ҳужум каби аниқлаш мумкин. Аниқланган K_0 калит ёрдамида бир раундга кечикган дешифрлаш жараёнига шифрлаш жараёнини бир (бошланғич ҳолатда икки) раундга кечиктириб K_1 калитни топиш мумкин.

“**Комбинацияланган слайдли ҳужум**” илмоқли ва тўлдирувчи асосидаги слайдли ҳужум усулларини биргаликда қўлланишидан иборат бўлиб, шифрлаш ва дешифрлаш жараёнларини икки раундга кечиктириб, қуйидагича таққослаш мумкин:

$$k_0, k_1, k_2, k_3, k_0, k_1, \ldots$$

$$k_0, k_1, k_2, k_3, k_0, k_1, \ldots$$

Ушбу ҳолда $(k_1 \oplus k_3, k_0 \oplus k_2)$ фарқлар ҳосил бўлади. Мазкур таҳлилни ўтказиш учун $2^{n/2}$ тадан кам бўлмаган матнларни таҳлил қилиш талаб этилади ҳамда жараённинг ўзи ҳам мураккабдир [2]. Комбинацияланган слайдли ҳужумни қўллашда илмоқли слайдли ҳужум хусусиятига кўра, шифрлаш жараёнига дешифрлаш жараёнини бир раундга кечиктирган ҳолда калитлар ўртасидаги фарқни қуйидаги кўринишда тасвирлаш мумкин:

$$k_0, k_1, k_2, k_3, k_0, k_1, \ldots$$
$$k_3, k_2, k_1, k_0, k_3, k_2, \ldots$$

Бу ерда юқори қатор шифрлаш жараёнига, қуйи қатор эса дешифрлашга (ёки k_3, k_2, k_1 ва k_0 қисм калитлар кетма-кет қўлланилган шифрлаш жараёнига) мос келади, ҳамда $(0, k_1 \oplus k_3)$ слайдли $(k_1 \oplus k_3 = \Delta)$ айирмага эга матнлар билан тўлдирувчи асосида слайдли ҳужумни қўллаб, k_0 қийматини топиш мумкин. Кейинги босқичда дешифрлаш жараёнига шифрлаш жараёнини бир раундга кечиктириб калитлар ўртасидаги фарқни қуйидагича келтириш мумкин:

$$k_3, k_2, k_1, k_0, k_3, k_2, \ldots$$
$$k_0, k_1, k_2, k_3, k_0, k_1, \ldots$$

Бу ерда юқори қатор дешифрлаш (ёки k_3, k_2, k_1 ва k_0 қисм калитлар кетма-кет қўлланилган шифрлаш) жараёнига, қуйи қатор эса шифрлашга мос келади, ҳамда $(0, k_2 \oplus k_0)$ слайдли айирмага $(k_2 \oplus k_0 = \Delta')$ эга матнлар билан тўлдирувчи асосида слайдли ҳужумни қўллаб, k_3 қийматини топиш мумкин. k_1 ва k_3 калитларни эса, танланган Δ ва Δ' лар орқали $(k_1 \oplus k_3 = \Delta)$ ва $(k_2 \oplus k_0 = \Delta')$ тенгликлардан аниқлаш мумкин. 2.5.5-расмда юқорида келтирилган икки босқич бирлаштириб тасвирланган.

Қуйида, “Слайдли ҳужум” криптотаҳлил усулининг қўлланилишига намуна келтирилган.

Оддийлик учун танланган очиқ матн асосида слайдли ҳужум усулини DES шифрлаш алгоритми асосида қурилган S-DES ўқув алгоритмига қўлланилиши кўриб чиқилади. Ушбу алгоритмнинг блок ва махфий калит узунлиги 8 бит бўлиб, икки раунд ҳамда бошланғич IP ва якуний IP^{-1} ўрин алмаштиришларга эга [3]. Ҳар бир раунднинг F_k функцияси таркибида кенгайтириш (E/P), ўрнига қўйиш (S-блок), 8 битли қисм (раунд) калит билан қўшиш, ўрин алмаштириш (P) амалга оширилади (2.5.6-расм).

2.5.1-жадвал.

IP бошланғич ўрин алмаштириш

IP							
2	6	3	1	4	8	5	7

2.5.2-жадвал.

IP^{-1} якуний ўрин алмаштириш.

IP^{-1}							
4	1	3	5	7	2	8	6

2.5.3-жадвал.

Кенгайтириш ўрин алмаштириш жадвали

E/P							
3	1	4	3	2	1	4	2

2.5.4-жадвал.

S–блоклар

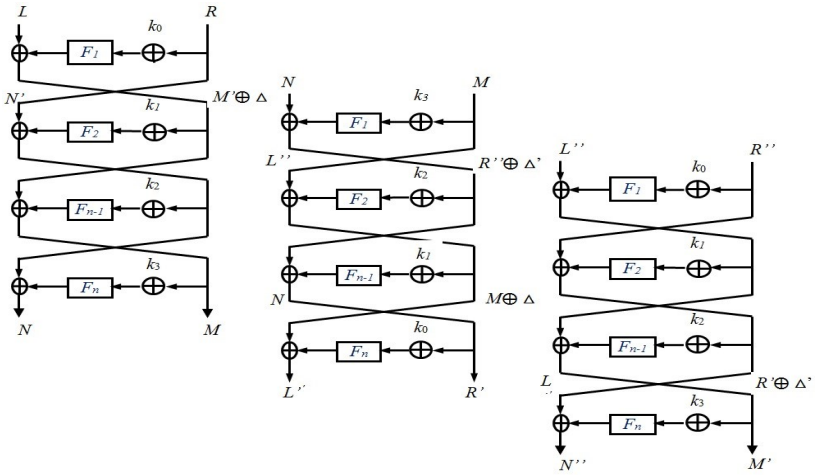
S_0	**00**	**01**	**10**	**11**
00	0	2	1	1
01	1	3	0	2
10	0	3	2	3
11	2	1	3	0

S_1	**00**	**01**	**10**	**11**
00	0	1	3	2
01	3	2	0	1
10	1	0	1	3
11	3	2	0	2

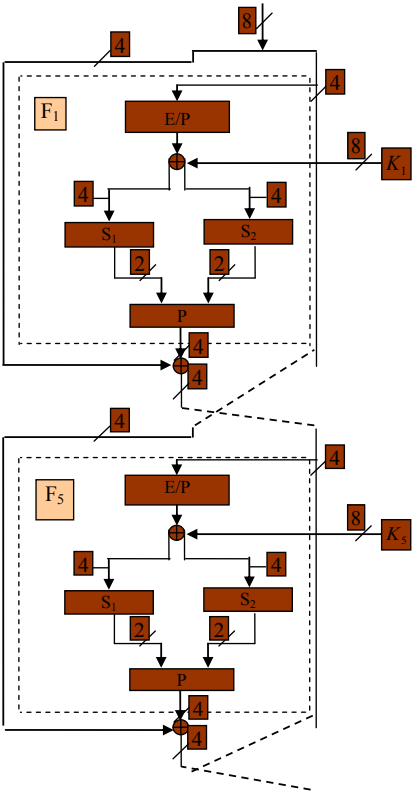
2.5.5-жадвал.

Ўрин алмаштириш жадвали

P			
4	2	3	1



2.5.5-расм. Комбинацияланган слайдли ҳужум схемаси.



2.5.6-расм. S-DES алгоритми блок схемаси.

S-DES ўқув алгоритмига оддий слайдли ҳужум усулини қўллашда барча раундлар учун бир хил 8 битли k калит олинади. Бу ҳолда берилган маълумотни калит билан модул икки бўйича қўшиш F функция олдида эмас, унинг ўзида бажарилади. Шунингдек, бошланғич ва якуний алмаштиришлар криптотаҳлил натижаларига таъсир кўрсатмаганлиги учун уларни ташлаб ўтиш мумкин.

Умумий ҳолда, криптотаҳлил жараёни қуйидаги алгоритм асосида олиб борилади:

1. Киритилсин: X, X', Y, Y', K, S, P, E, массивлар;

X=[8 bit], X'=[8 bit], K=[8 bit], Y=[8 bit], Y'=[8 bit], S=[2,15], P=[4 bit], E=[8 bit].

2. $X^{'}=X\_L^{'}||X\_R^{'}$, $X=X\_L||X\_R$, $K=K_1||K_2$, $Y^{'}=Y\_L^{'}||Y\_R^{'}$, $Y=Y\_L||Y\_R$, $U_1=X\_L$, $U_2=X\_R$, $U_3=X\_L^{'}$, $U_4=X\_R^{'}$, $G_1=Y\_L$, $G_2=Y\_R$, $G_3=Y\_L^{'}$, $G_4=Y\_R^{'}$.

3. Агар $U_1=U_4$ бўлса, у ҳолда Buffer1=X ва Buffer2=$X^{'}$ ўзлаштирилсин, акс ҳолда 2-қадамга қайтилсин.

4. Агар $G_2=G_3$ бўлса, у ҳолда Buffer3=Y ва Buffer3=$Y^{'}$ ўзлаштирилсин, акс ҳолда 2-қадамга қайтилсин.

5. 2 ва 3 шартларни қаноатлантирувчи жуфтликлар слайд жуфтликлар деб олинади.

6. F функция чиқиш қиймати аниқланади, яъни 4 бит: $F = X^{'}\_L \oplus X\_R$.

7. F функция чиқиши ўрин алмаштиришдан ўтказилади: $Urin\_almashtirish = F$.

8. $Urin\_almashtirish$ нинг 2 тадан битлари S_0 ва S_1 блок чиқиши сифатида олинади.

9. $X\_R^{'}$ қийматни кенгайтириш жадвалига киритилади ва 4 бит 8 битга кенгайтирилади: $T[i] = X[E[i]]$.

10. T[i] массив иккита қисмга ажратилади: $T[i] = T_1[i]||T_2[i]$.

11. Агар $S[i]=S_0$ бўлса, у ҳолда, Kirish1[i] массивга ўзлаштирилсин;

Агар $S[i]=S_1$ бўлса, у ҳолда Kirish2[i] массивга ўзлаштирилсин.

12. Қийматлар қўшилади: T_1 [i]$\oplus$$Kirish_1$ [i] ва K1 [i] тўпламга ўзлаштирилсин;

T_2 [i]$\oplus$$Kirish_2$ [i] ва K2 [i] тўпламга ўзлаштирилсин.

13. F функция чиқиш қиймати аниқланади: $F = Y\_L \oplus Y^{'}\_R$.

14. F функция чиқиши ўрин алмаштиришдан ўтказилади: $Urin\_almashtirish = F$.

15. $Urin\_almashtirish$ нинг 2 та бити S_0 блок, 2 та бити S_1 чиқиши сифатида олинади.

16. $Y\_L^{'}$ қийматни кенгайтириш жадвалига киритилади ва 4 бит 8 битга кенгайтирилади: $T[i] = Y[E[i]]$.

17. T [i] массив иккита қисмга ажратилади: $T[i] = T_1[i]||T_2[i]$.

18. Агар S[i]=S_0 бўлса, у ҳолда, Kirish1[i] массивга ўзлаштирилсин;

Агар S[i]=S_1 бўлса, у ҳолда, Kirish2[i] массивга ўзлаштирилсин.

19. Қийматлар қўшилади: T_1[i]$\oplus$Kirish$_1$[i] ва K1[i] тўпламга ўзлаштирилсин;

T_2 [i]$\oplus$Kirish$_2$[i] ва K2[i] тўпламга ўзлаштирилсин.

20. Агар K1[i]=K1[i] у ҳолда K_1[i] га ўзлаштирилсин;

Агар K2[i]=K2[i] у ҳолда K_2[i] га ўзлаштирилсин;

K[i]=K_1[i]||K_2 [i] махфий калит вариантлари сифатида олинади.

Слайдли ҳужум криптотаҳлил усули учун $2^{n/2}$ та жуфт (P_i, C_i) очиқ-ёпиқ матнлар жуфтлиги олиниб, уларнинг орасидан слайд жуфтликлар топилади. Топилган очиқ-ёпиқ матнлар орасидан "Туғилган кун" парадоксига кўра ҳеч бўлмаганда бир жуфт шундай (i, i') индекслар топиладики, қандайдир қисм калит учун $F(P_i) = P'_i$ ва $F(C_i) = C'_i$ тенгликлар бир вақтда бажарилади [3, 33]. Махфий калит битларини тўла аниқлаш учун бир нечта слайдли жуфтликлар керак бўлади, бу эса криптотаҳлил учун мураккаб масала ҳисобланади. Мумкин бўлган слайд жуфтликлар оралиғини қисқартириб ишни енгиллаштириш учун ихтиёрий тўрт битли маска (ниқоб) киритилади. Ушбу маска орқали слайдли жуфтлик таърифига мос келувчи матнлар жуфтлиги танлаб олинади. Слайдли жуфтлик шартига кўра 1-очиқ матннинг ўнгдаги 4 бити билан 2-очиқ матнинг чапдаги 4 бити маскага тенг. Мазкур матнларга мос 1-шифрматннинг чапдаги 4 бити 2-шифрматнинг ўнгдаги 4 битига тенг бўлади.

Слайдли ҳужум ўтказиш учун $P_i = (x = X\_L, y_i = X\_R)$ очиқ матнли тасодифий танланган ўнг қисмлари билан фарқланадиган массив ва тасодифий танланган чап қисмлари билан фарқланадиган $P'_j = (y'_j, x)$ массив танланади. Кейин танланган матнлар тасодифий танланган 8 битли $k = (k_1, k_2)$ калит билан шифрланади, у иккита 4 битли калитдан ташкил топган (уларнинг ҳар бири S-блок киришига таъсир этади). Таҳлил учун танланган $P_i = (x, y_i)$ ва $P'_j = (y'_j, x)$ массивларни шифрлаш натижалари 2.5.6 – 2.5.7 жадвалларда келтирилган.

2.5.6-жадвал.

K калит билан $P_i = (x, y_i)$ *массивни шифрлаш натижалари*

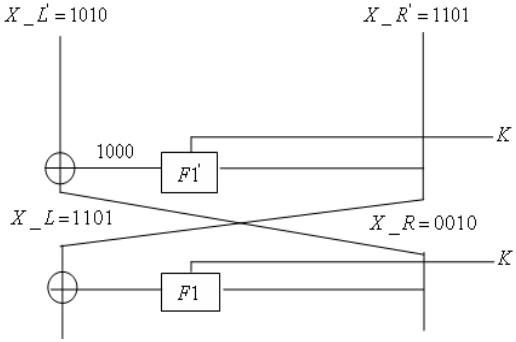
№	X_L	X_R	Y_L	Y_R
1	1101	0110	0101	1100
2	1101	0001	1101	1110
3	1101	0010	1001	1010
4	1101	1000	0000	0111

2.5.7-жадвал.

K калит билан $P_j^{'} = (y_j^{'}, x)$ *массивни шифрлаш натижалари*

№	X_L'	X_R'	Y_L'	Y_R'
1	1010	1101	1010	1101
2	0010	1101	0101	1111
3	1110	1101	1100	1000
4	1100	1101	0000	0011

Шундай қилиб, 16 та жуфт очиқ матнга эга бўлинди. Ушбу жадвалларда келтирилган шифрлаш натижаларини таҳлил қилиб аниқлаш мумкинки, слайдли жуфтликни аниқлаш шартини иккита матнлар жуфтлиги қаноатлантиради. Матнларнинг биринчи жуфтлигини 2.5.6-жадвалнинг N_3 матни ва 2.5.7-жадвалнинг N_1 матнини ташкил этади. Топилган слайд жуфтлик таҳлил қилинади. Бунинг учун 2.5.7-расмда кўрсатилган шифрлашнинг биринчи икки раунди кўриб чиқилади.



2.5.7-расм. Биринчи раунд биринчи слайд жуфтлик таҳлили.

$X\_R^{'}$ ва X_L қийматларининг маълумлиги $F_1^{'}$ функция кириши ҳақидаги маълумотни беради. X_R ва $X\_L^{'}$ қийматлар маълум бўлганлиги учун F функция чиқиш қиймати $X\_R \oplus X\_L^{'} = 1000_2$ га тенг. Чиқишдан олдин F функция берилганлари ўрин алмаштириш

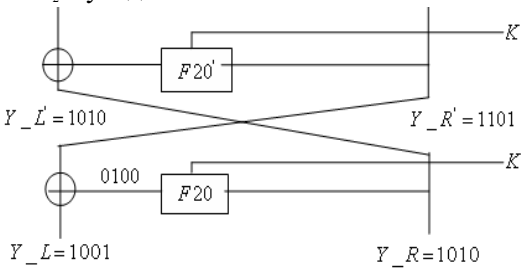
жадвалга мувофиқ алмаштириш бажарилса, унда бир қадам ортга қайтиб S блок чиқишида 0100_2 қиймат ҳосил бўлади, яъни 01_2 S_0 блокнинг чиқиши, 00_2 эса S_1 блок чиқишини беради. F функциянинг кириш маълумоти кенгайтириш ўрин алмаштиришига учрайди. Демак, F функциянинг 1101_2 кириши 11101011_2 қийматга ўзгаради, у $k=(k_1,k_2)$ калит билан қўшилади, яъни S_0 блок кириши $1110_2 \oplus k_1$ чиқишда 01_2 қийматни беради, S_1 блок кириши $1011_2 \oplus k_2$ чиқишда 00_2 қийматни беради.

Келтирилган 2.5.8-жадвалдан фойдаланиб аниқлаш мумкинки, агар S_0 блок киришига $0000_2, 0101_2, 1011_2, 1100_2$ ёки 1111_2 қийматлардан бири кирса, у ҳолда, чиқишида 01_2 қиймат ҳосил бўлади. Шундай қилиб, киришнинг ҳар бир мумкин бўлган қийматларига 1110_2 қийматни қўшиб, k_1 нинг мумкин бўлган қийматлари топилади. Булар $1110_2, 1011_2, 0101_2, 0010_2$ ёки 0001_2 бўлади. Шу тарзда S_1 блок киришига $0011_2, 1010_2$, 1101_2 ёки 1110_2 қийматлардан бири кирса, унинг чиқишида 00_2 қиймат ҳосил бўлишини кўрсатиш мумкин. Демак, мумкин бўлган қийматларга 1011_2 қийматни қўшиб, k_2 нинг мумкин бўлган қийматини олиш мумкин. Булар $1000_2, 0001_2, 0110_2$ ёки 0101_2 бўлади.

Энди шу слайд жуфтлик учун шифрлашнинг сўнгги икки раунди кўриб чиқилади (2.5.8-расм). Y_L' ва Y_R маълумлиги F_{20}' функция кириш қиймати ҳақида маълумот беради. Y_R' ва Y_L қийматларни маълумлиги ҳудди шу F_{20} функциянинг чиқиш қийматини аниқлашга имкон беради, у 0100_2га тенг. F_{20} функцияга кирувчи маълумот кенгайтириш ўрин алмаштиришидан ўтади. Демак, 1010_2 кириш 01010101_2 қийматга ўзгаради ва $K=(k_1,k_2)$ калитга қўшилади. Шифрлаш жараёнида матн иккита бўлакка ажратилади ва ҳар бир бўлаги калит қисми билан қўшилиб, кейин эса мос S блок киришига келиб тушади. Энди 8 битли махфий калитни иккита $K=k_1 \| k_2$ 4 битли қисм калитлар йиғиндиси сифатида келтирилади, яъни S_0 блокнинг $0101 \oplus k_1$ кириши чиқишда 00_2 қиймат беради, S_1 блокнинг $0101 \oplus k_2$ кириши эса чиқишда 01_2 беради.

Агар S_0 блокка $0010_2, 0111_2$ ёки 1000_2 қийматлардан бири кирган бўлса, у ҳолда, унинг чиқишида 00_2 қиймат ҳосил бўлади. Шундай

қилиб, ҳар бир мумкин бўлган кириш қийматга 0101_2 қийматни қўшиб k_1 калитнинг мумкин бўлган қийматлари топилади. Булар $0111_2, 0010_2$ ёки 1101_2 бўлади.



2.5.8-расм. Охирги раунд биринчи слайдли жуфтлик таҳлили.

Агар S_1 блокка $0000_2, 0010_2, 0101_2, 1011_2$ ёки 1100_2 қийматлардан бири кирган бўлса, у ҳолда унинг чиқишида 01_2 аниқланади. Демак, ҳар бир мумкин бўлган кириш қийматига 0101_2 қийматни қўшиб k_2 нинг мумкин бўлган қийматлари олинади. Булар $0101_2, 0111_2, 0000_2, 1110_2$ ёки 1001_2 бўлади.

Шифрлаш ҳар бир раундида бир хил калитдан фойдаланилганлиги учун биринчи ва сўнгги раундлар учун k_1 ва k_2 қийматлар мос келиши керак. Шунинг учун k_1 ва k_2нинг барча мумкин бўлган қийматларини таққослаб шуни кўриш мумкинки, биринчи ва сўнгги раундларда қўлланилиши мумкин бўлган $k_1 = 0010_2$ва $k_2 = 0101_2$ калитларнинг ягона қийматига эга бўламиз. Натижада, қидирилаётган калит $k = 00100101_2$ га тенг бўлади.

Слайдли ҳужум криптотаҳлил усулини Фейстель тармоғига асосланган ҳақиқий алгоритмларга (DES ва ГОСТ 28147-89 мисолида) қўлланиши бўйича қуйидагича тавсияларни келтириш мумкин.

Ушбу алгоритмларда шифрланадиган маълумотлар узунлиги, слайд жуфтликларни топишда вақт бўйича қийинчиликка олиб келади, шу мақсадда биринчи навбатда слайд жуфтликларни топишда қуйидаги усуллардан фойдаланиш мумкин.

1-усул

1. Бошланғич маълумотлар сифатида иккита файл танланади, узунликлари ихтиёрий бўлиши мумкин.

2. Бирор *K* калит билан биринчи ва иккинчи файллар шифрланади ва янги файлларга ёзиб қўйилади.

3. Қуйидагича иккита шарт текширилади:

1-шарт: *биринчи файл биринчи байтининг ўнгдаги 4 битини иккинчи файл биринчи байтининг чапдаги 4 битига тенг бўлса;*

2-шарт: *биринчи файл биринчи байт шифрматнининг чапдаги 4 битини иккинчи файл биринчи байт шифрматнининг ўнгдаги 4 битига тенг бўлса.*

4. Юқоридаги икки шартни қаноатлантирувчи очиқ ва мос шифрматнлар жуфтлиги “Слайд жуфтлик” деб эълон қилинади ва натижада (X,X') *ва* (Y,Y') жуфтлик ҳосил бўлади.

2-усул

1. Бошланғич маълумотлар сифатида битта файл танланади, ихтиёрий узунликда бўлиши мумкин.

2. Бирор *K* калит билан файл шифрланади ва янги файлга ёзиб қўйилади.

3. Қуйидагича иккита шарт текширилади:

1-шарт: *файл биринчи байтининг ўнгдаги 4 битини иккинчи байтининг чапдаги 4 битига тенг бўлса;*

2-шарт: *файл биринчи байт шифрматнининг чапдаги 4 битини иккинчи байт шифрматнининг ўнгдаги 4 битига тенг бўлса*.

4. Юқоридаги икки шартни қаноатлантирувчи очиқ ва мос шифрматнлар жуфтлиги “Слайд жуфтлик” деб эълон қилинади ва натижада (X,X') *ва* (Y,Y') жуфтлик ҳосил бўлади.

DES алгоритмига нисбатан ГОСТ 28147-89 алгоритмида акслантириш функциялари фарқ қилганлиги учун, слайдли ҳужум криптотаҳлил усулини ўтказишда алоҳида ёндашиш керак. Жумладан, бунда 32 битли кирувчи матннинг ўнг томонига 32 битли калит 2^{32} модул бўйича қўшилади. Яъни $(R_i+K_i)mod2^{32}=T_i$ кўринишида бўлади, бундан эса $K_i=(T_i-R_i)mod2^{32}$ ифода орқали калитнинг қийматини бир қийматли топиш мумкин.

Иккала алгоритмда ҳам S-блок акслантиришлари мавжуд бўлиб, ГОСТ 28147-89 алгоритмда S-блоклар махфий ҳисобланади. Бу эса ўз навбатида ҳар бир S-блоклар алоҳида криптотаҳлил ўтказишни талаб қилади. S-блок акслантиришларида тўрт бит кириб тўрт бит

чиқади, бу эса бир қийматли акслантиришни ифодалайди, яъни кирувчи ягона маълумотга чиқувчи битта маълумот мос келади. DES алгоритмида эса кирувчи тўртта маълумотга чиқишда битта маълумот мос келади, бу слайдли ҳужум ўтказишда S-блокдан орқага қайтиш жараёнида калитнинг тўртта варианти ҳосил бўлади. Саккизта S-блокдан орқага қайтишда 2^{16} мумкин бўлган вариантлар ҳосил бўлиб, слайдли ҳужумда ўзига яраша танлаш билан боғлиқ бўлган масалани ечишга олиб келади.

ГОСТ 28147-89 алгоритмининг S-блокларида эса бир қийматли мослик бўлгани учун бундай муаммо кузатилмайди. 11 разрядли чапга циклик суриш ва чап кирувчи томон билан XOR амаллари бир қийматли орқага қайтишини ҳисобига слайдли ҳужум усулини қўллаш мураккаб масалага олиб келмайди.

Алгоритм учун слайдли жуфтлик топилгандан сўнг, қисм калитнинг битларини топиш мумкин бўлади. Слайдли жуфтликларга нисбатан ҳисоблаш жараёнлари кўп вақтни талаб қилганлиги сабабли маска (ниқоб) деб аталувчи қўшимча восита киритилади. Махфий калитнинг битларини тўла аниқлаш учун, алгоритм, очиқ ва уларга мос шифрматнлар ҳамда берилган маска бўйича бир нечта слайдли жуфтликлар керак бўлади.

Умумий ҳолда, мавжуд ёки янги таклиф этилган Фейстельь тармоғи асосидаги блокли симметрик шифрлаш алгоритмини оддий слайдли ҳужум усули ёрдамида баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.5.8-жадвал.

Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Алгоритмнинг тегишли акслантиришлари ва ўрнатилган калит асосида оддий слайдли ҳужум шартларини қаноатлантирувчи барча слайд жуфтликларни аниқлаш. Яъни, танланган очиқ матнлар	Слайд жуфтликлар мавжуд	Мазкур слайд жуфтликлар билан калит битларини аниқлаш мумкинлигини текшириб кўриш натижасида хулоса берилади

2.5.8-жадвалнинг давоми

	ва уларга мос шифрматнларни аниқлаш	Слайд жуфтликлар мавжуд эмас (реал вақт давомида топилмади)	Алгоритмни оддий слайдли ҳужум усулига баҳолаб бўлмайди
II.	Аниқланган барча слайд жуфтликлар асосида иккита шифрлаш жараёнини бир-биридан бир раундга кечиктириб, биринчи ва охирги раунд мосликлари учун, раунд акслантиришларидан тескари тартибда ўтказиб, мумкин бўлган калит вариантларини аниқлаш	Биринчи ва охирги раундда аниқланган калитлар ўзаро тенг, ушбу калитлардан мумкин бўлган калитлар тўплами ҳосил бўлади	Мазкур аниқланган мумкин бўлган калитларни ҳақиқийлигига текшириш натижасида хулоса берилади
		Биринчи ва охирги раундда аниқланган калитлар ўзаро тенг эмас, яъни барча жараёнларда ҳар хил калитлар аниқланиши	Мавжуд калитга нисбатан алгоритм оддий слайдли ҳужум усулига баҳолаб бўлмайди
III.	Аниқланган мумкин бўлган калитларни ҳақиқийликка текшириш. Мумкин бўлган калитлар ёрдамида аниқланган слайдли жуфтлик матнларни шифрлаш жараёнидан ўтказиб, мавжуд шифрматнлар билан солиштириш	Аниқланган калитлар оддий слайдли ҳужум усулининг барча шартларини қаноатлантирди	Алгоритм барча раундларда бир хил калит ишлатилганда оддий слайдли ҳужум усулига бардошли эмас
		Аниқланган калитлар ёрдамида очиқ матнларни шифрлашда ҳосил бўлган шифрматнлар мавжуд шифр-матнларга тенг эмас	Алгоритм барча раундларда бир хил калит ишлатилганда оддий слайдли ҳужум усулига амалий бардошли

Қуйида тўлдирувчи асосида слайдли ҳужум криптотаҳлил усулининг қўлланилишига намуна келтирилган.

Тўлдирувчи асосида слайдли хужум усулини қўллаш учун S-DES ўқув алгоритми модификацияланган варианти танланди. Мазкур криптотаҳлил усулида калитлар ўртасидаги фарқ кирувчи маълумотлар фарқини ҳам таъминлаши керак. S-DES ўқув алгоритмида саккиз битли кирувчи маълумот иккига бўлиниб, тўрт бити *E* кенгайтириш жадвалидан ўтади ва саккиз битли калит қўшилади. Мазкур ҳолда кирувчи маълумотнинг тўрт битли фарқи калитларнинг саккиз битли фарқига тенг бўлиши талаб қилинади. Бу ўз навбатида ўзаро фарқлар ҳар хил ўлчамини вужудга келтиради.

Кенгайтириш жадвалига кўра тўрт битли маълумот битларининг такрорланиши ҳисобига саккиз битга айланади. Яъни 4 битли (m'_1, m'_2, m'_3, m'_4) маълумот кенгайтириш ўрин алмаштиришдан кейин $(m'_4, m'_1, m'_2, m'_3, m'_2, m'_3, m'_4, m'_1)$ га тенг бўлади. Битлар такрорланиши саккиз битли қийматнинг мумкин бўлган 256 та вариантини 16 тага тушишига олиб келади. Демак, маълумотлар ўртасидаги фарқ ҳам кенгайтириш жадвалидан ўтиб саккиз битли кўринишга битлар такрорланиши ҳисобига эга бўлади. Калитларнинг саккиз битли фарқида ҳам битлар такрорланиши кўзатилади. Ушбу ҳолат тўрт битли кирувчи маълумотга тўрт битли калит кенгайтириш жадвалидан олдин қўшилиши билан бир хил бўлади, яъни $E(M \oplus K)=E(M) \oplus K$.

Олинган маълумот биринчи 4 бити S_0 блокка кириб, чиқишда 2 битли кетма-кетлик ҳосил бўлади, қолган 4 бити эса иккинчи S_1 блокка кириб чиқишда 2 битли кетма-кетлик ҳосил бўлади. S_0 ва S_1 блокларнинг чиқишидаги 4 битли маълумот P ўрин алмаштириши амалга оширилади.

S-DES симметрик шифрлаш алгоритмига тўлдирувчи асосида слайдли ҳужумда $\Delta = 0100_2$ деб белгилаб, 2.5.9 – 2.5.10-жадвалларда келтирилган слайд жуфтликлар орқали ўтказилади.

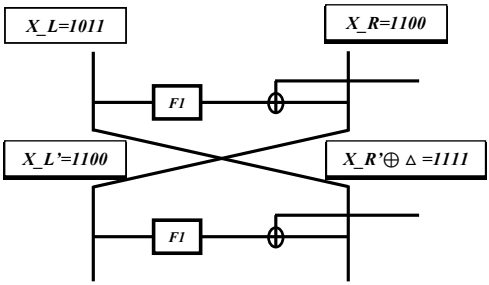
2.5.9-жадвал

№	L	R	N	M
1	1110	0010	1100	1100
2	1011	1100	1101	1101

2.5.10-жадвал

№	L’	R’	N’	M’
1	0110	0110	1100	1000
2	1000	1011	0111	1001

Шундай қилиб, икки жуфт очиқ ва унга мос шифр матнга эга бўлинди. 2.5.9 – 2.5.10-жадвалларда келтирилган слайдли жуфтликлардан 2 қаторда турган слайдли жуфтликни танлаб, тўлдирувчили слайдли ҳужум усули кетма кетлигини кўриб чиқиш мумкин. Ушбу слайдли жуфтликлар Фейстел тармоғига қуйидагича жойлашади:



2.5.9-расм. Биринчи раунд биринчи слайдли жуфтлик таҳлили.

Биринчи R очиқ матннинг ўнг қисми қийматлари ва иккинчи очиқ матннинг чап $L'\oplus\Delta$ қисм қийматлари маълум бўлгани $F_1^{'}$ функция кириши ҳақида маълумот беради. L ва $R^{'}\oplus\Delta$ қийматлар ҳам маълум бўлгани учун F_1 функция чиқиш қийматини аниқлаш мумкин ва у 0000_2 тенг бўлади .

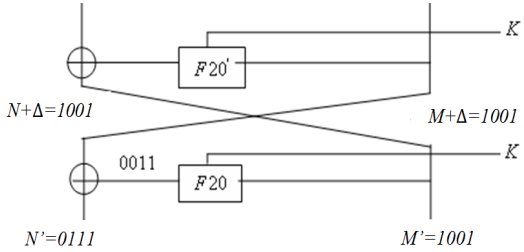
Берилганлар $F_1^{'}$ функциядан чиқишдан олдин 2.5.5-жадвалга мувофиқ ўрин алмашса, бир қадам ортга қайтиб, S блок чиқишида 0100_2 қиймат пайдо бўлишини топамиз, ушбу қийматни 2.5.5-жадвалига кўра ўрин алмаштирилса S_i блоклардан чиқган қийматларни аниқлаймиз, яъни 00_2 S_0-блок чиқиши, 01_2 эса S_1-блок чиқиши. Бу қийматлардан S_i блокга кириши мумкин бўлган қийматларни 2.5.8-жадвалдан аниқлаш мумкин бўлиб, улар қуйидагича:

S_0: 0001, 0111, 1100; S_1: 0000, 0001, 0110, 1010, 1101.

S блокга кириши мумкин бўлган қийматларни 2.5.3-жадвал бўйича кенгайтириш жадвалига кириш қиймати 01111101_2 бўлади. Қиймат кенгайтириш ўрин алмаштириш жадвалидан ортга қайта олади ва 1110_2 қиймат ҳосил бўлади. Бу қийматга биринчи очиқ матннинг ўнг тарафи қўшилиб k_0 қиймат ҳосил бўлади:

$$k_0 = 1110_2 \oplus R = 1110_2 \oplus 1100_2 = 0010_2.$$

k_1 калитни топиш учун охирги раундга кириш ва чиқиш қийматларидан фойдаланилади. 2.5.10-жадвалдаги слайд жуфтликлар Фейстель тармоғига қуйидагича жойлашади (2.5.10-расм):



2.5.10-расм. Охирги раундда слайдли жуфтликлар жойлашуви.

F функциядан чиқувчи қиймат қуйидагича аниқланади $(N \oplus \Delta) \oplus N' = 1001_2 \oplus 0111_2 = 1110_2$. Бу олинган натижани аралаштириш жадвалидан ортга қайтарилиб 0111_2 қийматга эга бўлинади, натижада $S_0=01_2$, $S_1=11_2$ қийматлар ҳосил бўлади. Шунга кўра, S блокка кириши мумкин бўлган қийматлар қуйидагича:

S_0: 0000, 0110, 1010, 1101, 1111; S_1: 0011, 0111, 1000, 1111.

Ушбу қийматларни *E* кенгайтириш жадвалидан тескари тартибда қайтарилади.

2.5.11-жадвал

№	4	1	2	3	2	3	4	1	E
14	1	1	0	1	0	1	1	1	+
20	1	1	1	1	1	1	1	1	+

Ушбу жадвалда кенгайтириш жадвалидан ортга қайтиши мумкин бўлган 20 та вариантдан 2 та 1011_2 ва 1111_2 тўғри келиши кўрсатилган. Олинган натижани охирги раунд ўнг кириши билан қўшиб k_1 ни мумкин бўлган қийматлари топилади:

$$k_1 = (M \oplus \Delta) \oplus 1011_2 = 1001_2 \oplus 1011_2 = 0010_2$$
$$k_1 = (M \oplus \Delta) \oplus 1111_2 = 1001_2 \oplus 1111_2 = 0110_2$$

Олинган натижаларга кўра $k_0=0010_2$, $k_1=0010_2$ ва $k_1=0110_2$. Умумий калитлар $k_0=00100010_2$ ва $k_0=00100110_2$ га тенг бўлди.

Умумий ҳолда **S-DES симметрик шифрлаш алгоритмига тўлдирувчили слайдли ҳужум криптотаҳлил усулини қўллаш алгоритм** қуйидагича**:**

1. Киритилсин X=[8 бит], X'=[8 бит], $К_0$=[4 бит], $К_1$=[4 бит], Y=[8 бит], Y'=[8 бит], E=[8 бит], Δ=[4 бит].

2. X=L||R, X'=M ||N, K=$К_0$ ||$К_1$, Y=L' ||R', Y'=M'||N'.

3. Охирги раунд кириши, яъни слайдли жуфтликнинг иккинчи қисми: $V_1 = M \oplus \Delta$, $V_2 = N \oplus \Delta$.

4. Агар $R' = L \oplus \Delta$ ва $L' = R \oplus \Delta$ бўлса, у ҳолда, *Буффер1*=X ва *Буффер2*=X' ўзлаштирилсин акс ҳолда 2-қадамга қайтилсин.

5. Агар $L' = R \oplus \Delta$ ва $R' = L \oplus \Delta$ бўлса, у ҳолда *Буффер1*=X ва *Буффер2*=Y ўзлаштирилсин акс ҳолда 2-қадамга қайтилсин.

6. *F* функция чиқиш қийматини аниқланади, яъни 4 бит: $F = X \oplus R' \oplus \Delta$.

7. *F* функция чиқиши ўрин алмаштириш жадвалида ўтказилади: *Urin_almashtirish=F*.

8. *Urin_almashtirish* нинг 2 та бити S_0 блокга, 2 та бити S_1 чиқиши сифатида олинади.

9. C [i] массив иккита қисмга ажратилади: $C[i] = C_1[i] || C_2[i]$.

10. Агар C[i]=C_0 бўлса, у ҳолда, *Кириш1*[i] массивга ўзлаштирилсин;

Агар C[i]=C_1 бўлса, у ҳолда, *Кириш2*[i] массивга ўзлаштирилсин.

11. *F* функциядан чиқиш қийматлар аниқланади:

a. Агар *Кириш1*[i] *Кириш2*[i]=*Urin_almashtirish* бўлса, *Чиқиш[i]* массивга ўзлаштирилсин;

b. акс ҳолда олинмасин.

12. Танлаб олинган *Чиқиш [i]* қийматлар *F* функция чиқиши ўрин алмаштиришдан ўтказилади $Urin\_almashtirish = Z$.

13. $К_1$ нинг мумкин бўлган варинтлари топилади: $k_1 = Z \oplus R$

Агар $V_2 = N \oplus \Delta$ ва $V_1 = M \oplus \Delta$ бўлса, *Буффер3*=X' ва *Буффер4*=Y' ўзлаштирилсин, акс ҳолда 2-қадамга қайтилсин.

14. *F* функция чиқиш қийматини аниқланади, яъни 4 бит: $F = M' \oplus M \oplus \Delta$.

15. *F* функция чиқиши ўрин алмаштириш жадвалида ўтказилади: *Urin_almashtirish=F*.

16. *Urin_almashtirish* нинг 2 та бити C_0 блокга, 2 та бити C_1 чиқиши сифатида олинади.

17. C1 [i] массив иккита қисимга ажратилади: $C1[i] = C_1[i] || C_2[i]$.

18. Агар C[i]=C_0 бўлса, у ҳолда, *Кириш1*[i] массивга ўзлаштирилсин;

Агар C[i]=C_1 бўлса, у ҳолда, *Кириш2*[i] массивга ўзлаштирилсин.

19. *F* функциядан чиқиш қийматлар аниқланади:

a. Агар *Кириш1*[i] *Кириш2*[i]=*Urin_almashtirish* бўлса, *Чиқиш [i]* масивга ўзлаштирилсин;

b. акс ҳолда олинмасин.

20. Танлаб олинган *Чиқиш [i]* қийматлар *F* функция чиқиши ўрин алмаштиришдан ўтказилади *Urin_almashtirish*=Z_2.

21. K_2 нинг мумкин бўлган варинтлари топилади: $k_2 = Z_2 \oplus N \oplus \Delta$.

22. Чиқарилсин K_1 ва K_2.

DES шифрлаш алгоритмида худди ўқув алгоритми сингари, 32 битли маълумот 16 та битининг такрорланиши ҳисобига *E* кенгайтириш жадвали орқали 48 битли маълумотга айланади ҳамда 48 битли калит қўшилади. Бу ерда ҳам слайд жуфтликларнинг 32 битли фарқи калитларнинг 48 битли фарқига тенг бўлишини таъминлаш керак бўлади. Ушбу масалани ечишда икки хил ёндашишни таклиф этиш мумкин:

1. Раунд функциясида маълумотга калитни қўшиш акслантиришини E кенгайтириш жадвалидан олдин амалга ошириш, бунда калитни маълумот узунлигига тенг қилиб олиш мумкин бўлади.

2. Раунд функциясини ўзгартирмасдан олиб, слайдли ҳужумни амалга ошириш учун мумкин бўлган барча калитлардан фойдаланилмайди. 32 битли маълумотлар фарқини 48 битли калитлар фарқи билан тенглигини таъминлаш мақсадида, калитларни фақатгина уларнинг фарқлари E кенгайтириш жадвалидан тескари тартибда қайтиши мумкин бўлган вариантларини олиш мумкин.

ГОСТ 28147-89 шифрлаш алгоритмида калит битларининг $mod 2^{32}$ бўйича кирувчи матн битларига қўшилиши, тўлдирувчи асосида слайдли ҳужум усулининг асосий шартларидан бири бўлган, ўзаро калитлар ва слайд жуфтликлар орасидаги Δ фарқнинг бир эҳтимоллик билан раундлар охиригача сақланмаслигига олиб келади. Бу эса ихтиёрий калитлар учун тўлдирувчи асосида слайдли ҳужум ўтказиш имкониятини йўққа чиқаради. Демак, ГОСТ 28147-89 шифрлаш алгоритми учун тўлдирувчи асосидаги слайдли ҳужум фақат $\Delta = 0$ ва $\Delta = 2^{31}$ бўлган ҳолларда ўтказиш мумкин. $\Delta = 0$ ҳол,

яъни калитлар ўзаро тенг бўлиши оддий слайдли ҳужумга олиб келади. Демак, фақат битта ҳолда, яъни $\Delta = 2^{31}$ га шартни бажарадиган калитлар учун бу усулни қўллаш мумкин.

Умуман олганда, шунга ўхшаш (*mod* 2^n) амали қўлланилган алгоритмларга слайдли ҳужум усули қўллашда, ГОСТ 28147-89 алгоритмидаги каби, калитлар ва слайд жуфтликлар ўртасидаги ўзаро фарқнинг сақланишини таъминлаш учун фарқни фақатгина 2^{n-1} га тенг қилиб олиш мумкиндир.

Умумий ҳолда мавжуд ёки янги таклиф этилган блокли симметрик шифрлаш алгоритмини Тўлдирувчи асосида слайдли ҳужум усули ёрдамида баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.5.12-жадвал.

Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Алгоритмнинг тегишли акслантиришлари ва ўрнатилган калитлар билан тўлдирувчи асосида слайдли ҳужум шартларини қаноатлантирувчи барча слайд жуфтликларни аниқлаш. Яъни, танланган очиқ матнлар ва уларга мос шифрматнлар, ҳамда калитлар ўртасидаги ўзаро фарқ биринчи ва охирги раундлардаги слайдли жуфтликлар ўртасидаги ўзаро фарққа тенг	Слайд жуфтликлар мавжуд, калитлар ўртасида фарқ очиқ ва шифрматнлар ўртасидаги ўзаро фарқга тенг	Мазкур слайдли жуфтликлар билан калит битларини аниқлаш мумкинлиги текшириб кўриш натижасида хулоса берилади
		Слайд жуфтликлар мавжуд эмас (реал вақт мобайнида топилмади)	Алгоритмни тўлдирувчи асосида слайдли ҳужум усулига баҳолаб бўлмайди
II.	Аниқланган барча слайдли жуфтликлар асосида иккита шифрлаш жараёнини	Биринчи ва охирги раундда аниқланган калитлар	Ҳосил бўлган биринчи раунд калитига слайдли жуфтликлар

2.5.12-жадвалнинг давоми

	бир-биридан бир раундга кечиктириб, биринчи ва охирги раунд мосликлари учун, раунд акслантиришларидан тескари тартибда ўтказиб, мумкин бўлган калит вариантларини аниқлаш	ўртаси-даги фарқ, слайд жуфтликлар ўртасидаги ўзаро фарқга тенг бўлса, биринчи раунд калити учун мумкин бўлган калитлар тўплами ҳосил бўлади	ўртасидаги фарқни қўшиш орқали иккинчи раунд калити аниқланади. Мазкур аниқланган мумкин бўлган калитларни ҳақиқийлигига текшириш натижасида хулоса берилади
		Биринчи ва охирги раундда аниқланган ҳар хил калитлар ўртасидаги фарқ, слайд жуфтликлар ўртасидаги ўзаро фарқга тенг бўлмаса	Изланаётган калитга нисбатан алгоритм тўлдирувчи асосида слайдли ҳужум усулига баҳолаб бўлмайди
III.	Аниқланган мумкин бўлган калитларни ҳақиқийликка текшириш. Мумкин бўлган калитлар ёрдамида аниқланган слайдли жуфтлик матнларни шифрлаш жараёнидан ўтказиб, мавжуд шифрматнлар билан солиштириш	Аниқланган калитлар тўлдирувчи асосида слайдли ҳужум усулининг барча шартларини қаноатлантирди	Алгоритм барча раундларда икки хил калит ишлатилганда тўлдирувчи асосида слайдли ҳужум усулига бардошли эмас
		Аниқланган калитлар ёрдамида очиқ матнларни шифрлашда ҳосил бўлган шифрматн-лар мавжуд шифр-матнларга тенг эмас	Алгоритм барча раундларда икки хил калит ишлатилганда тўлдирувчи асосида слайдли ҳужум усулига амалий бардошли

Қуйида илмоқли слайдли ҳужум криптотаҳлил усулининг S-DES алгоритмига қўлланилишига намуна келтирилган.

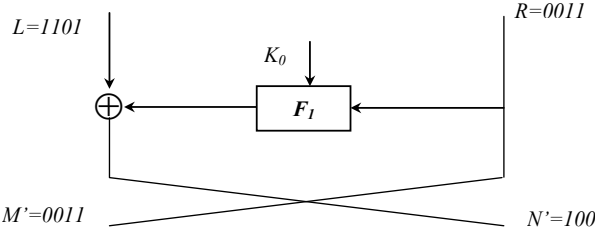
Мазкур ҳолда, кирувчи очик матн узунлиги 8 бит ҳамда калитлар узунлиги 8 битдан бўлган икки хил k_0 ва k_1 калитлар ишлатилади. Криптотаҳлил жараёни қуйидаги жадвалда келтирилган слайд жуфтликларидан фойдаланган ҳолда амалга оширилади (2.5.11-расм).

2.5.13-жадвал.

Слайд жуфтликлари

№	L	R	M	N	M'	N'	L'	R'
1	1101	0011	**1001**	**0101**	**0011**	**1000**	**1101**	**1001**

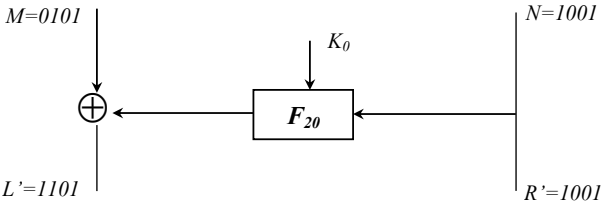
№	T	Б	T'	Б'
1	**1110**	**1000**	**0111**	**1101**



2.5.11-расм. Илмоқли слайдли ҳужум биринчи раунди.

F функцияга кирувчи R=0011_2 қиймат кенгайтириш жадвалидан сўнг $E(R)$=10010110_2 қийматга ўзгаради. *F* функциядан чиқувчи қиймат қуйидагича $N' \oplus L = 1000_{\,2} \oplus 1101_{\,2} = 0101_{\,2}$ аниқланади. Илмоқли слайдли ҳужум шартига кўра аралаштириш жадвали ҳисобга олинмайди ва S_0=01_2, S_1=01_2 қийматлар аниқланади. Ушбу қийматлардан S_0 блокка кириши мумкин бўлган қийматлар 0000, 0110, 1010, 1101 ва 1111_2 га тенг бўлади. S_1 га кириши мумкин бўлган қийматлар эса 0000, 0001, 0110, 1010 ва 1101_2 бўлади. Ушбу топилган қийматлар орқали k_{01} калитни мумкин бўлган қийматлари S-DES алгоритми акслантириш хусусиятига кўра қуйидаги кўринишда ҳисобланади:

$S = E(R) \oplus K \Rightarrow K = E(R) \oplus S$, булар 1001, 1111, 0011, 0100 ва 0110_2 га тенг бўлади. k_{02} калитни мумкин бўлган қийматлари ҳам худди шу тарзда топилади ва $k_{02} = 0110_{\,2} \oplus 0000_{\,2} = 0110_{\,2}$, 0111_2, 0000_2, 1100_2, 1011_2 га тенг бўлади. Қуйида, иккинчи слайд жуфтликларни S-DES алгоритмига жойлашиши келтирилган:



2.5.12-расм. Илмоқли слайдли ҳужум йигирманчи раунди.

F функцияга кирувчи қийматлар аниқланади. *N=1001* қиймат кенгайтириш жадвалидан қуйидагича кенгаяди *E(N)=11000011*. *F* функциядан чиқувчи қиймат қуйидагича аниқланади $M \oplus L' = 0101_2 \oplus 1101_2 = 1000_2$. Илмоқли слайдли ҳужум шартига кўра аралаштириш жадвали ҳисобга олинмайди ва бундан кўриниб турибдики $S_0=10_2$, $S_1=00_2$ қийматлар чиққанлиги маълум бўлади. Ушбу қийматлардан S_0 блокка кириши мумкин бўлган қийматлар 0011_2, 0101_2 ва 1001_2 га тенг бўлади. S_1 кириши мумкин бўлган қийматлар ҳам худди шу тарзда аниқланади. Ушбу топилган қийматлар орқали k_{01} калитни мумкин бўлган $k_{01} = 1100_2 \oplus 0011_2 = 1111_2$, 1001_2 ва 1101_2 қийматлари аниқланади. k_{02} калитни мумкин бўлган қийматлари $k_{02} = 0011_2 \oplus 0101_2 = 0110_2$, 1010_2, 1000_2 ва 1101_2 га тенг бўлади. Олинган натижалардан калитни мумкин бўлган қийматини аниқлаш керак (2.5.14-жадвал). Бунда икки усулда ҳам бир хил чиққан қийматлар калит битлари бўлиши мумкин.

2.5.14-жадвал

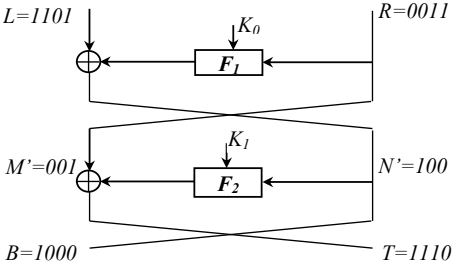
K_{01}-биринчи раунд	1001	1111	~~0011~~	~~0100~~	~~0110~~
K_{01}-охирги раунд	1111	1001	~~1101~~		
K_{02}-биринчи раунд	0110	~~0111~~	~~0000~~	~~1100~~	~~1011~~
K_{02}-охирги раунд	0110	~~1010~~	~~1000~~	~~1101~~	

2.5.14-жадвалдан k_{01}=1001, 1111 ва k_{02}=0110 калитни ҳақиқийсини топиш учун биринчи раундга кирувчи очиқ матнни шифрлаб шифр матн билан таққослаб кўрилади.

R=0011 қиймат кенгайтириш жадвалидан сўнг қуйидаги 10010110_2 қийматга ўзгаради ва $K_1=10010110_2$ билан қўшилиб $10010110_2 \oplus 10010110_2 = 00000000_2$ қиймат ҳосил бўлади. $S_1=01_2$, $S_2=01_2$ қийматлар бирлашган ҳолда *F* функциядан чиқувчи қиймат

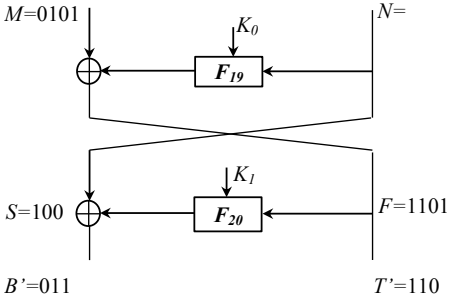
ҳисобланади, яъни 0101_2. $L \oplus F(R \oplus K_0) = 1101_2 \oplus 0101_2 = 1000_2$ тенгликдан K_0=10010110_2 келиб чиқади.

K_1 калит топиш учун илмоқли слайдли ҳужум қоидасига биноан икки раундга кечиктириб шифрлаш жараёнини мос қўйиш йўли орқали аниқланади. Бу вақтда олдинги таҳлил орқали топилган K_0 калит аниқ деб олинади.



2.5.13-расм. Илмоқли слайдли ҳужум иккинчи раунди.

F функцияга кирувчи N'=1000_2 қиймат E кенгайтириш жадвалидан қуйидагича кенгаяди: 01000001_2. F функциядан чиқувчи қиймат $M' \oplus B = 0011_2 \oplus 1110_2 = 1101_2$ топилади. Илмоқли слайдли ҳужум шартига кўра аралаштириш жадвали ҳисобга олинмайди ва S_0=11_2, S_1=01_2 бўлади. Ушбу қийматлардан S_0 блокга кириши мумкин бўлган қийматлар $0010_2, 0100_2, 1011_2, 1100_2$ ва 1110_2 га, S_1 блокка кириши мумкин бўлган қийматлар эса $0000_2, 0001_2, 0110_2 1010_2$ ва 1101_2 га тенг бўлади. Ушбу топилган қийматлар орқали k_{11} калитни мумкин бўлган қийматлари $k_{11} = 0100_2 \oplus 0010_2 = 0110_2$, 0000_2, 1111_2, 1000_2 ва 1010_2 га, k_{12} калитни мумкин бўлган қийматлари эса $k_{12} = 0001_2 \oplus 0000_2 = 0001_2$, 0000_2, 0111_2, 1011_2 ва 1100_2 га тенг бўлади.



2.5.14-расм. Иккинчи шифрлаш жараёни йигирманчи раунди.

K_0 калит аниқ бўлганлиги учун биринчи жараённинг шифр матнини иккинчи шифрлаш жараёнининг ўн тўққизинчи раундига кириш бўлиб ҳисобланади. K_0 калит билан шифрлаш жараёни: $(N \oplus K_0) = 11000011_2 \oplus 10010110_2 = 01010101_2$ ушбу қийматлар $S_0=0101_2=10_2$, $S_1=0101_2=00_2$ қийматлар чиқади. $F(E(N \oplus K_0)) \oplus M = 1000_2 \oplus 0101_2 = 1101_2$ қийматлар ҳосил бўлиб, бу иккинчи шифрлаш жараёнинг йигирманчи раундига кирувчи қийматларни беради.

K_1 калит битларини топиш учун S, F ва B', T' қийматлардан фойдаланган ҳолда йигирманчи раундга слайдли ҳужум ўтказилади. F функцияга кирувчи $F=1101_2$ қиймат кенгайтириш жадвалидан кенгайиб 11101011_2 ҳосил бўлади. F функциядан чиқувчи қиймат қуйидагича $B' \oplus S = 0111_2 \oplus 1001_2 = 1110_2$ топилади. Илмоқли слайдли ҳужум шартига кўра аралаштириш жадвали ҳисобга олинмайди, бундан кўриниб турибдики, $S_0=11_2$, $S_1=10_2$ га тенг бўлади. Булардан S_0 блокга кириши мумкин бўлган қийматлар 0010_2, 0100_2, 1011_2, 1100_2 ва 1110_2, S_1 блокка кириши мумкин бўлган қийматлар эса, 0010, 0100 ва 1100 га тенг бўлади. Ушбу топилган қийматлар орқали k_{11} калитнинг мумкин бўлган қийматлари $k_{11} = 1110_2 \oplus 0010_2 = 1100_2$, 1010_2, 0101_2, 0010_2 ва 0000_2 га тенг чиқади. Худди шу тарзда k_{12} калитни мумкин бўлган қийматлари $k_{12} = 1011_2 \oplus 0010_2 = 1001_2$, 1111_2 ва 0111_2 га тенг бўлади.

2.5.15-жадвал.

K_{11}-биринчи раунд	~~0110~~	0000	~~1111~~	~~1000~~	1010
K_{11}-охирги раунд	~~1100~~	1010	~~0101~~	~~0010~~	0000
K_{12}-биринчи раунд	~~0001~~	~~0000~~	0111	~~1011~~	~~1100~~
K_{12}-охирги раунд	~~1001~~	~~1111~~	0111		

Мазкур жадвалдан $\boldsymbol{K_1}$ калитнинг мумкин бўлган қийматлари 00000111_2, 10100111_2 га тенг эканлиги келиб чиқади.

Умумий ҳолда **S-DES симметрик шифрлаш алгоритмига илмоқли слайдли ҳужум криптотаҳлил усулини қўллаш алгоритм** қуйидагича**:**

1. Киритилсин *X=[8 бит], X'=[8 бит], K_0=[8 бит], K_1=[8 бит]; Y=[8 бит], Y'=[8 бит], E=[8 бит], D=[8 бит], D'=[8 бит].*
2. *X=L||R, X'=M||N, Y=L'||R', Y'=M'||N', D=T||B, D'=T'||B';*
   $K_0=K_{01}$ || K_{02}, $K_1=K_{11}$ || K_{12}.

3. F функция чиқиш қийматини аниқланади, яъни 4 бит: $F1 = L \oplus N'$.

4. 3-қадамдан чиқган натижа 2 бити S_0 блокга, 2 бити S_1 чиқиши сифатида олинади.

5. C[i] массив иккита қисимга ажратилади: $C[i] = C_1[i] || C_2[i]$;

6. Агар $C[i]=C_0$ бўлса, у ҳолда, *Кириш1[i]* массивга ўзлаштирилсин.

а. Агар $C[i]=C_1$ бўлса, у ҳолда, *Кириш2[i]* массивга ўзлаштирилсин.

7. P қийматни кенгайтириш жадвалига киритилади ва 4 бит 8 битга кенгайтирилади: $U[i] = R[E[i]]$.

8. $U[i]$ массив икки қисимга ажратилади: $U[i] = U_1[i] || U_2[i]$.

9. Қийматлар қўшилади: $U_1[u] \oplus$ *Кириш11[u]* ва *K12[u]* тўпламга ўзлаштирилсин;

$U_2[u] \oplus$ *Кириш21 [u]* ва *K22 [u]* тўпламга ўзлаштирилсин.

10. Агар *K11 [u]=K21 [u]* у ҳолда $K_1[u]$ га ўзлаштирилсин;

Агар *K21 [u]=K22 [u]* у ҳолда $K_2[u]$ га ўзлаштирилсин.

11. $K_j[u]=K_{1u}[u] || K_{2u}[u]$ махфий калит варианти сифатида олинади.

12. $K_j[u]=K_{кj}[u]$ юклатилсин.

20-раунд

13. F функция чиқиш қийматини аниқланади, яъни 4 бит: $F2 = L' \oplus M$.

14. $K_0=K_1$[i].

15. 4-қадамга қайтилсин.

2-раунд

16. F функция чиқиш қийматини аниқланади, яъни 4 бит: $F3 = M' \oplus T$.

17. 4-қадамга қайтилсин.

19-раунд

18. F функция чиқиш қийматини аниқланади, яъни 4 бит: $F4 = F(E(N \oplus K_0) \oplus M)$.

19. F 4=F; N=C;

20. 4-қадамга қайтилсин.

20-раунд

21. F функция чиқиш қийматини аниқланади, яъни 4 бит: $F3 = B' \oplus S$.

22. 4-қадамга қайтилсин.

23. K_{jk} лар чоп етилсин.

Умумий ҳолда мавжуд ёки янги таклиф этилган блокли симметрик шифрлаш алгоритмини Илмоқли слайдли ҳужум усули ёрдамида баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.5.16-жадвал.

Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Алгоритмнинг икки раундли ўзига хослиги икки хил раунд калитлари ва тегишли акслантиришлари асосида илмоқли слайдли ҳужум шартларини қаноатлантирувчи барча слайд жуфтликларни аниқлаш. Яъни, танланган очиқ матнлар ва уларга мос шифрматнлар, ҳамда калитлар ўртасидаги ўзаро фарқ слайдли жуфтликлар ўртасидаги ўзаро фарқга ва раунд охирида шифрматнлар ўртасидаги ўзаро фарқга тенг	Слайд жуфтликлар мавжуд	Мазкур слайдли жуфтликлар билан калит битларини аниқлаш мумкинлиги текширилиб кўриш натижасида хулоса берилади
		Слайд жуфтликлар мавжуд эмас (реал вақт мобайнида топилмади)	Алгоритмни илмоқли слайдли ҳужум усулига баҳолаб бўлмайди
II.	Аниқланган барча слайд жуфтликлар асосида биринчи шифрлаш жараёнига иккинчи дешифрлаш жараёнини бир раундга кечиктириб, биринчи ва охирги раунд мосликлари учун, раунд акслантиришларидан	Биринчи ва охирги раундда аниқланган калитлар ўзаро тенг, ушбу калитлардан биринчи раунд калити учун мумкин бўлган	Иккинчи раунд калитини аниқлаш натижасида тегишли хулоса берилади

2.5.16-жадвалнинг давоми

	тескари тартибда ўтказиб, мумкин бўлган калит вариантларини аниқлаш	калитлар тўплами ҳосил бўлади	
		Биринчи ва охирги раундда аниқланган калитлар ўзаро тенг эмас, яъни барча жараёнларда ҳар хил калитлар аниқланиши	Аниқланган слайд жуфтликлар асосида ўрнатилган калитларга нисбатан алгоритм илмоқли слайдли ҳужум усулига баҳолаб бўлмайди
III.	Аниқланган барча слайдли жуфтликлар асосида биринчи дешифрлаш жараёнига иккинчи шифрлаш жараёнини бир раундга кечиктириб, биринчи ва охирги раунд мосликлари учун, раунд акслантиришларидан тескари тартибда ўтказиб, мумкин бўлган калит вариантларини аниқлаш	Биринчи ва охирги раундда аниқланган калитлар ўзаро тенг, ушбу калитлардан иккинчи раунд калити учун мумкин бўлган калитлар тўплами ҳосил бўлади	Мазкур аниқланган мумкин бўлган калитларни ҳақиқийлигига текшириш натижасида хулоса берилади
		Биринчи ва охирги раундда аниқланган калитлар ўзаро тенг эмас, яъни барча жараёнларда ҳар хил калитлар аниқланиши	Аниқланган слайдли жуфтликлар асосида ўрнатилган калитларга нисбатан алгоритм илмоқли слайдли ҳужум усулига баҳолаб бўлмайди

2.5.16-жадвалнинг давоми

IV.	Аниқланган мумкин бўлган калитларни ҳақиқийликка текшириш. Мумкин бўлган калитлар ёрдамида аниқланган слайдли жуфтлик матнларни биринчи шифрлаш жараёнида ҳосил бўлган шифрматнларни, ҳамда иккинчи дешифрлаш жараёнларида ҳосил бўлган очиқ матнларни, мавжуд шифрматнлар ва очиқ матнлар билан солиштириш	Аниқланган калитлар илмоқли слайдли ҳужум усулининг барча шартларини қаноатлантирди	Алгоритм барча раундларда икки хил калит ишлатилганда илмоқли слайдли ҳужум усулига бардошли эмас
		Аниқланган калитлар ёрдамида очиқ матнларни шифрлашда ҳосил бўлган шифрматнлар мавжуд шифр-матнларга тенг эмас	Алгоритм барча раундларда икки хил калит ишлатилганда илмоқли слайдли ҳужум усулига амалий бардошли

Қуйида комбинацияланган слайдли ҳужум криптотаҳлил усулининг S-DES алгоритмига қўлланилишига намуна келтирилган.

S-DES алгоритми Фейстель тармоғи бўйича қурилган блокли шифрлаш алгоритми бўлганлиги учун унга танланган очиқ матн асосидаги комбинацияланган слайдли ҳужум криптотаҳлил усулини қўллаш мумкин.

Комбинацияланган слайдли ҳужум тўлдирувчи асосидаги слайдли ҳужум ва илмоқли слайдли ҳужум усуллари биргаликда ишлатилади. Шунга кўра, калит функцияга киришдан олдин шифрланувчи (дешифрланувчи) маълумотнинг ўнг қисмига қўшилиб кейин кириши лозим. Тўлдирувчи асосидаги слайдли ҳужум усули қўлланилишида олинган S-DES алгоритмининг модификацияланган схемасидан фойдаланилади.

Оддийлик учун ҳар хил 4 битли 4 та $k_0k_1k_2k_3$ калит олинади. Бу ҳолда берилган маълумотни калит билан қўшиш (XOR) F функция олдида бажарилади. Шунингдек, ишни соддалаштириш мақсадида бошланғич ва якуний алмаштиришлар ташлаб кетилади.

Комбинацияланган слайдли ҳужум криптотаҳлил усулини S-DES ўқув алгоритмига қўллаш икки босқичга бўлинади, чунки битта криптотаҳлил ўтказиш билан алгоритмда фойдаланилган барча калитларнинг битларини топиш имконияти мавжуд эмас. Дастлабки босқичда фақат алгоритмда фойдаланилган k_0 калитни топиш мумкин. Қолган калит битларини топиш иккинчи босқичда амалга оширилади.

Дастлабки босқични амалга оширишда ихтиёрий тарзда 4 битли x қиймат танланади. Айтайлик, $x=1000$ бўлсин, бундан кейин $2^{\%4}=2^{8\%4}=2^2=4$ та $P_i=(x=X\_L, y_i=X\_R)$ очиқ матнли тасодифий танланган ўнг қисмлари билан фарқланадиган массив ва $2^{\%4}=2^{8\%4}=2^2=4$ та тасодифий танланган чап қисмлари билан фарқланадиган $P_j^{'}=(y_j^{'},x)$ массив олинади. Кейин танланган матнларни тасодифий 4 битли 4 та $k_0k_1k_2k_3$ калит билан шифрланади. $P_i=(x,y_i)$ ва $P_j^{'}=(y_j^{'},x)$ массивларни шифрлашнинг натижалари 2.5.17 – 2.5.18 жадвалларда келтирилган.

2.5.17-жадвал .

К махфий калит ёрдамида $P_i=(x,y_i)$ массивни шифрлаш натижалари

№	X_L	X_R	Y_L	Y_R
1	0101	1000	0101	1101
2	0101	1000	1101	1110
3	1001	1000	1111	0011
4	1101	1000	0000	0111

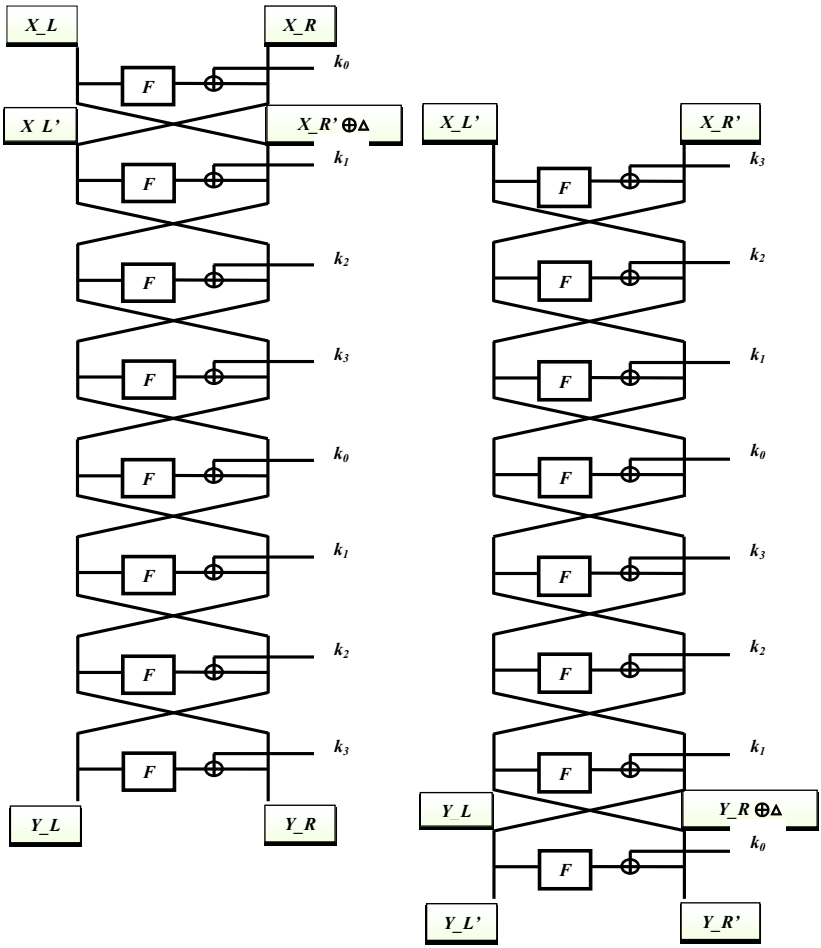
2.5.18-жадвал.

К махфий калит ёрдамида $P_j^{'}=(y_j^{'},x)$ массивни шифрлаш натижалари

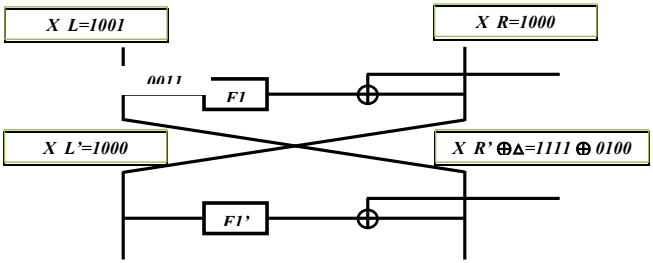
№	X_L'	X_R'	Y_L'	Y_R'
1	1000	1110	0100	1111
2	1000	1101	0101	1111
3	1000	0010	1100	0101
4	1000	1101	0000	0011

Шундай қилиб, 16 жуфт очиқ матнга эга бўлинди. 2.5.17-2.5.18-жадвалларда келтирилган шифрлаш натижалари таҳлил қилинса, слайдли жуфтлик шартини иккита матнлар жуфтлиги қаноатлантиради. Топилган жуфтликлар таҳлилида S-DES алгоритмида қўлланувчи алмаштириш жадвали билан ишлашга тўғри келганлиги

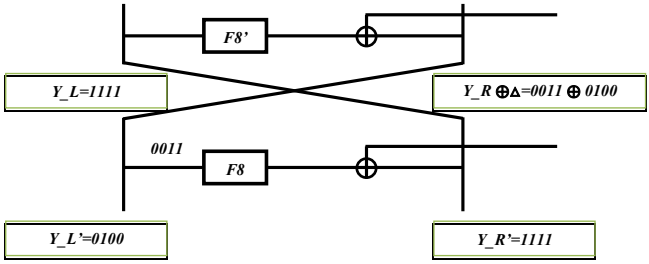
ва ишни осон қилиш учун 2.5.4-жадвалда кўрсатилгани каби S-блокларнинг кириши ва чиқиши таққосланади. Матнларнинг биринчи жуфтлигини 2.5.17-жадвалнинг N_3 матни ва 2.5.18-жадвалнинг N_1 матни ташкил этади. Топилган слайд жуфтлик таҳлил қилинади. Бунинг учун 2.5.15-расмда кўрсатилган шифрлашнинг биринчи икки раунди кўриб чиқилади. X_R ва X_L' қийматларининг маълумлиги F_1' функция кириши ҳақидаги маълумотни беради. X_L ва X_R' қийматлар маълум бўлганлигидан F функция чиқиш қийматини аниқлаш мумкин. Шунингдек, жараёнлардан бири бир раундга кечиктириб қўшилганда k_1 ва k_3 калитлар устма-уст тушиб қолади. Шу сабабли уларнинг фарқини йўқотиш учун биринчи жараённинг X_L кирувчи қийматига Δ қўшилиб келган деб олинади. Бундан F функция чиқиш қиймати 0011_2 га тенглиги аниқланади. Чиқишдан олдин F функция берилганлари S блокка мувофиқ алмаштиришга учраса, унда бир қадам ортга қайтиб S блок чиқишида 1010_2 қиймат пайдо бўлиши топилади, яъни 10_2 S_0 блокнинг чиқиши, 10_2 эса S_1 блокнинг чиқишини беради. Демак, S_0 блок киришига 0001_2, 0111_2, 1010_2 ёки 1100_2 қийматлардан бири кирса, чиқишида 10_2 қиймат, S_1 блок киришига 0011_2, 0101_2, 1101_2 ёки 1111_2 қийматлардан бири кирса, унинг чиқишида 10_2 қиймат ҳосил бўлишини кузатиш мумкин. Ҳосил бўлган натижалардан, E кенгайтириш жадвалидан орқага қайтариш мумкин бўлган S блокларга кирувчи (S_0 блокка кирувчи қайсидир қийматига S_1 блокка кирувчи қайсидир) қийматлар жуфтлиги танлаб олинади. Натижада E кенгайтириш шартларини (яъни мос битларнинг тенг бўлишини) бажарувчи S_0 ва S_1 блоклар жуфтликларини танлаб олинади. Қаралаётган матнлар учун (S_0,S_1) жуфтлик (0111_2,1101_2) ва (1100_2,0011_2) бўлганда E кенгайтириш жадвалидан ортга қайтариб мос равишда 1110_2 ва 1001_2 эканлиги аниқланади. Аниқланган қийматлардан калитни топиш учун бу қийматларни биринчи жараёнга кирувчи X_R га XOR амали бўйича қўшиб калит вариантлари топилади. Бунга кўра дастлабки икки раунд бўйича калит вариантлари 0110_2, 0001_2 га тенглиги аниқланади.



2.5.15-расм. Биринчи босқич слайдли ҳужум ўтказиш схемаси.



2.5.16-расм. Биринчи раунд биринчи слайдли жуфтлик таҳлили.



2.5.17-расм. Охирги раунд биринчи слайд жуфтлик таҳлили.

$Y\_R^{'}$ ва Y_L маълумлиги $F_8^{'}$ функция кириш қиймати ҳақида маълумот беради. $Y\_L^{'}$ ва Y_R қийматларни маълумлиги эса F_8 функциянинг чиқиш қийматини аниқлашга имкон беради ва у 0011_2 га тенг. Бу қийматни чиқишдан олдин S блокка мувофиқ алмаштирилганлиги сабабли ундан бир қадам ортга қайтиб, S блок чиқишида 1001_2 қиймат пайдо бўлиши топилади, яъни 10_2 S_0 блокнинг чиқиши, 01_2 эса S_1 блокнинг чиқишини беради. S_0 блок киришига 0001_2, 0111_2, 1010_2 ёки 1100_2 қийматлардан бири кирса, чиқишида 10_2 қиймат ҳосил бўлиши ва S_1 блок киришига 0001_2, 0111_2, 1000_2 ёки 1010_2 қийматлардан бири кирса, унинг чиқишида 01_2 қиймат ҳосил бўлиши кузатилади. Мумкин бўлган S_0 ва S_1 блокларга кирувчи қийматларнинг E кенгайтиришдан ортга қайта оладиганлари (0111_2, 1101_2) ва (1100_2, 0011_2) танланади. Улардан E кенгайтиришга кирувчи қийматлари 1110_2 ва 1001_2 экан. Олинган натижаларни Y_R XOR бўйича қўшиб калитнинг мумкин бўлган қийматлари 0110_2 ва 0001_2 келиб чиқади. Ушбу топилган слайд жуфтлик учун ўтказилган таҳлил натижасида биринчи иккита раунддан аниқланган калитнинг иккита вариантлари охирги икки раундга ўтказилган таҳлилда мумкин бўлган калит 0110_2 ва 0001_2 лар такрорланди. Шу сабабли 2.5.19-жадвалда келтирилган иккинчи слайд жуфтликдан фойдаланиб таҳлил ўтказилади.

Матнлар иккинчи жуфтлигини 2.5.18-жадвалнинг N_1 матни ва 2.5.19-жадвал N_3 матни ташкил этади. Бунда ҳам X_R ва $X\_L^{'}$ қийматларининг маълумлиги $F_1^{'}$ функция кириши ҳақидаги маълумотни беради. X_L ва $X\_R^{'}$ қийматлар маълум бўлганлиги учун F функция чиқиш қийматини аниқлаш мумкин. Берилган қийматлардан фойдаланиб юқоридаги каби дастлабки ва охирги икки раундга нисбатан ўтказилган таҳлилда калитнинг мумкин

бўлган варианти 0110_2 га тенг эканлиги маълум бўлади. Иккита слайд жуфтлиги бўйича ўтказилган таҳлилда калитнинг 0110_2 қиймати такрорланганлиги сабабли унинг ўзи калит деб элон қилиниши мумкин ва биринчи босқич бўйича таҳлил иши тўхтатилади.

Худди шундай иккинчи босқич учун ҳам таҳлил олиб борилади. Бунда биринчи босқичдан фарқли равишда иккинчи дешифрлаш жараёнига нисбатан биринчи шифрлаш жараёни бир раундга кечиктириб мос равишда қўшилади. Натижада калитлар қуйидаги тартибда устма-уст тушади:

$$k_3\ k_2\ k_1\ k_0\ k_3\ k_2\ k_1\ k_0 \ldots$$

$$k_0\ k_1\ k_2\ k_3\ k_0\ k_1\ k_2\ k_3 \ldots$$

Бу ерда k_1 ва k_3 калитлар мос равишда устма-уст тушса, у ҳолда k_0 ва k_2 калитлар кесишади. Бу фарқларни йўқ қилиш учун тўлдирувчили слайдли ҳужум хусусиятларидан келиб чиқган ҳолда k_0 ва k_2 калитларнинг $\Delta'\ (k0 \oplus k2 = \Delta')$ фарқидан фойдаланилади. Натижада калитлар юқоридаги каби устма-уст тушганлиги сабабли алгоритмда фойдаланилган k_3 калитнинг қийматини аниқлаш мумкин бўлади.

Иккинчи босқични амалга оширишда соддалик учун x қиймати дастлабки босқичдаги каби $x = 1000$ бўлсин, бундан кейин $2^{n/4} = 2^{8/4} = 2^2 = 4$ та $P_i = (x = X\_L, y_i = X\_R)$ очиқ матнли тасодифий танланган ўнг қисмлари билан фарқланадиган массив ва $2^{n/4} = 2^{8/4} = 2^2 = 4$ тасодифий танланган чап қисмлари билан фарқланадиган $P_j^{'} = (y_j^{'}, x)$ массив олинади.

Танланган матнларни дастлабки босқичда тасодифий танланган 4 битли 4 та $k_0 k_1 k_2 k_3$ калит билан шифрланади. $P_i = (x, y_i)$ ва $P_j^{'} = (y_j^{'}, x)$ массивларни шифрлашнинг натижалари 2.5.19 – 2.5.20 - жадвалларда келтирилган.

2.5.19-жадвал.

K калит ёрдамида $P_i = (x, y_i)$ массивни дешифрлаш натижалари

№	X_L'	X_R'	Y_L'	Y_R'
1	0111	1000	1101	1110
2	0110	1000	0100	0101
3	1101	1000	0000	0111
4	0011	1000	1011	0110

2.5.20-жадвал.

K калит ёрдамида $P_j' = (y_j', x)$ массивни шифрлаш натижалари

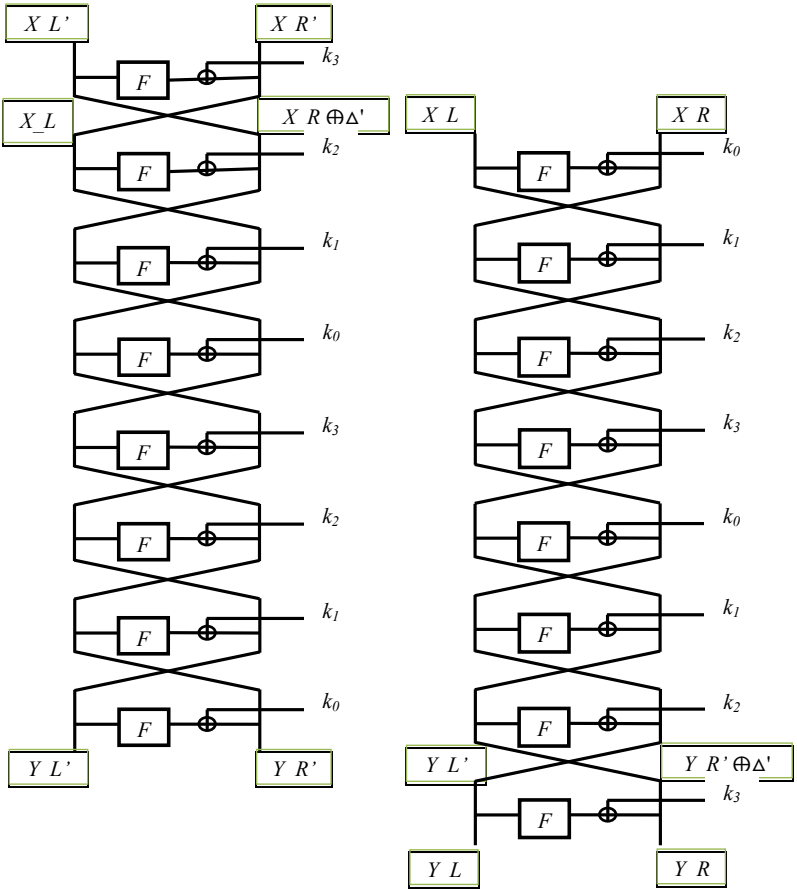
№	X_L	X_R	Y_L	Y_R
1	1000	0111	0100	0100
2	1000	1101	0101	1111
3	1000	0010	1110	1011
4	1000	1101	0000	0011

Матнларнинг биринчи жуфтлигини 2.5.19-жадвалнинг N_2 матни ва 2.5.20-жадвалнинг N_1 матни ташкил этади. Топилган слайдли жуфтлик таҳлил қилинади. Бунинг учун 2.5.18-расмда кўрсатилган шифрлашнинг биринчи икки раунди кўриб чиқилади. Криптотаҳлилни амалга ошириш 2.5.19-расмда келтирилган схемага асосан олиб борилади.

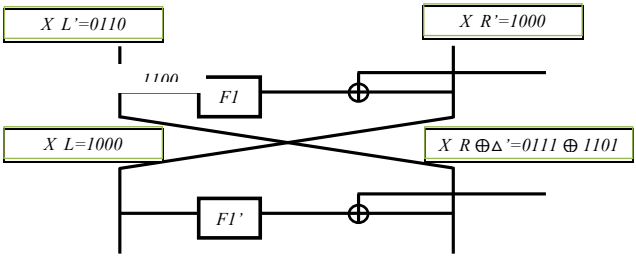
X_L ва X_R' қийматларининг маълумлиги F функция кириши ҳақидаги маълумотни беради. X_R ва X_L' қийматлар маълум бўлганлиги учун F функция чиқиш қийматини аниқлаш мумкин. Шунингдек, жараёнлардан бири бир раундга кечиктириб қўшганимизда k_0 ва k_2 калитлар устма-уст тушади. Шу сабабли уларнинг фарқини йўқотиш учун биринчи жараённинг X_L' кирувчи қийматига Δ' қўшилиб келган деб олинади. Бундан F функция чиқиш қиймати 1100_2 га тенглиги аниқланади.

Чиқишдан олдин F функция берилганлари S-блок жадвалига мувофиқ алмаштиришга учраса, унда бир қадам ортга қайтиб S блок чиқишида 0101_2 қиймат пайдо бўлиши топилади, яъни 01_2 S_0 блокнинг чиқиши, 01_2 эса S_1 блокнинг чиқишини беради.

Қуйида S-блок жадвалидан фойдаланиб S_0 блок киришига 0010_2, 0011_2, 0100_2 ёки 1101_2 қийматлардан бири кирса чиқишида 01_2 қиймат, S_1 блок киришига 0001_2, 0111_2, 1000_2 ёки 1010_2 қийматлардан бири кирса, унинг чиқишида 01_2 қиймат ҳосил бўлиши кузатилади. Ҳосил бўлган натижаларни E кенгайтириш жадвалидан орқага қайтариш мумкин бўлган S блокларга кирувчи (S_0 блокка кирувчи айрим қийматига S_1 блокка кирувчи қайсидир) қийматлар жуфтлиги танлаб олинади. Натижада, E кенгайтириш шартларини (яъни мос битларнинг тенг бўлишини) бажарувчи S_0 ва S_1 блоклар жуфтликларини танлаб олинади.

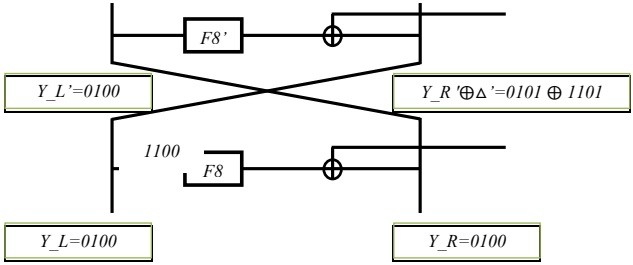


2.5.18-расм. Иккинчи босқич слайдли ҳужум ўтказиш схемаси.



2.5.19-расм. Биринчи раунд биринчи слайд жуфтлик таҳлили.

Қаралаётган матнлар учун (S_0, S_1) жуфтлик (0010_2, 1000_2), (0100_2, 0001) ва (1101_2, 0111_2) бўлганда E кенгайтириш жадвалидан ортга қайтариб мос равишда 0100_2 ва 1010_2 эканлиги аниқланади. Аниқланган қийматлардан калит топиш учун бу қийматларни биринчи жараёнга кирувчи X_R га XOR амали бўйича қўшилади. Бунга кўра дастлабки икки раунд бўйича калит вариантлари 1100_2, 0010_2 ва 0000_2 га тенг бўлади. Қуйида мазкур слайдли жуфтлик учун шифрлашнинг сўнгги икки раунди кўриб чиқилади.



2.5.20-расм. Охирги раунд биринчи слайдли жуфтлик таҳлили.

Y_L' ва Y_R маълумлиги F_8' функция кириш қиймати ҳақида маълумот беради. Y_R' ва Y_L қийматлар маълумлиги худди шу F_8 функциянинг чиқиш қийматини аниқлашга имкон беради ва у 1100_2 га тенг. Бу қийматни чиқишдан олдин S-блок жадвалига мувофиқ алмаштирилганлиги сабабли ундан бир қадам ортга қайтиб S блок чиқишида 0101_2 қиймат пайдо бўлиши топилади, яъни 01_2 S_0 блокнинг чиқиши, 01_2 эса S_1 блокнинг чиқишини беради. S-блок жадвалдан фойдаланиб S_0 блок киришига 0010_2, 0011_2, 0100_2 ёки 1101_2 қийматлардан бири кирса чиқишида 01_2 қиймат ҳосил бўлиши ва S_1 блок киришига 0001_2, 0111_2, 1000_2 ёки 1010_2 қийматлардан бири кирса, унинг чиқишида 01_2 қиймат ҳосил бўлиши кузатилади. Мумкин бўлган S_0 ва S_1 блокларга кирувчи қийматларнинг E кенгайтиришдан ортга қайта оладиганлари (0010_2, 1000_2), (0100_2, 0001_2) ва (1101_2, 0111_2) танлаб олинади. Уларнинг E кенгайтириш акслантришига кирувчи қийматлари 0001_2, 1000_2 ва 1110_2 бўлади. Олинган натижаларни Y_R XOR бўйича қўшиш орқали калитнинг мумкин бўлган қийматлари: 0101_2, 1100_2 ва 1010_2 га тенг эканлиги келиб чиқади. Топилган слайд жуфтлик учун ўтказилган таҳлилда биринчи иккита раунддан аниқланган калит вариантларидан охирги икки раундга ўтказилган таҳлилда мумкин бўлган калитнинг 1100_2 қиймати такрорланди.

Олинган натижаларни тасдиқлаш учун топилган иккинчи слайд жуфтлик бўйича таҳлил ўтказилади. Матнларнинг иккинчи жуфтлигини 2.5.19-жадвалнинг N_4 матни ва 2.5.20-жадвалнинг N_3 матни ташкил этади. Бунда ҳам X_L ва $X\_R^{'}$ қийматларининг маълумлиги $F_1^{'}$ функция кириши ҳақидаги маълумотни беради. X_R ва $X\_L^{'}$ қийматлар маълум бўлганлиги учун F функция чиқиш қийматини аниқлаш мумкин. Берилган қийматлардан фойдаланиб юқоридаги каби дастлабки ва охирги икки раундга нисбатан ўтказилган таҳлил натижасида калитнинг мумкин бўлган варианти 1100_2 га тенглиги аниқланди. Иккита слайд жуфтлиги бўйича ўтказилган таҳлилда калитнинг 1100_2 қиймати такрорланганлиги сабабли уни калит деб эълон қилиш мумкин ва иккинчи босқич бўйича таҳлил қилиш тўхтатилади.

Бизга $k1 \oplus k3 = \Delta$ ва $k0 \oplus k2 = \Delta'$ қийматлар маълум бўлганлиги сабабли биринчи ва иккинчи босқичларда аниқланган k_0 ва k_3 ларнинг қийматларидан k_1 ва k_2 калитларнинг қиймати қуйидагича аниқланади:

$$k0 \oplus k2 = \Delta' \rightarrow k2 = k0 \oplus \Delta' \rightarrow k2 = 0110 \oplus 1101,$$

$$k1 \oplus k3 = \Delta \rightarrow k1 = k3 \oplus \Delta \rightarrow k1 = 1100 \oplus 0100.$$

Тенгликлардан барча калитларни аниқлаш мумкин. Демак, фойдаланилган ҳақиқий калит қуйидагича:

$$k0 = 0110, k1 = 1000, k2 = 1011, k3 = 1100\ .$$

Умумий ҳолда мавжуд ёки янги таклиф этилган блокли симметрик шифрлаш алгоритмини Комбинацияланган слайдли ҳужум усули ёрдамида баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.5.21-жадвал.

Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Алгоритмнинг тўрт раундли ўзига хослиги тўрт хил раунд калитлари ва тегишли аксланти-ришлари асосида икки босқичли	Слайд жуфтликлар мавжуд	Мазкур слайд жуфтликлар билан калит битларини аниқлаш мумкинлиги текширилиб

2.5.21-жадвалнинг давоми

	комбинацияланган слайдли ҳужум шартларини қаноатлантирувчи биринчи босқич барча слайд жуфтликларни аниқлаш. Яъни, биринчи босқичда 2- ва 4-раунд калитлари ўртасидаги ўзаро биринчи фарқ биринчи ва охирги раундлардаги слайдли жуфтликлар ўртасидаги ўзаро фарққа тенг		кўриш натижасида хулоса берилади
		Слайд жуфтликлар мавжуд эмас (реал вақт мобайнида топилмади)	Алгоритмни комбинацияланган слайдли ҳужум усулига баҳолаб бўлмайди
II.	Аниқланган барча слайдли жуфтликлар асосида биринчи шифрлаш жараёнига иккинчи дешифрлаш жараёнини бир раундга кечиктириб, биринчи ва охирги раунд мосликлари учун, раунд акслантиришларидан тескари тартибда ўтказиб, мумкин бўлган калит вариантларини аниқлаш	Биринчи ва охирги раундда аниқланган калитлар ўзаро тенг ва ўртасидаги фарқ слайдли жуфтликлар фарқига тенг, ушбу калитлардан биринчи раунд калити учун мумкин бўлган калитлар тўплами ҳосил бўлади	Аниқланган биринчи раунд калитига слайдли жуфтликлар ўртасидаги фарқни қўшиш орқали тўртинчи раунд калити ҳосил қилинади. Иккинчи раунд калитини аниқлаш натижасида якуний хулоса берилади
		Биринчи ва охирги раундда аниқланган калитлар ўзаро тенг эмас ёки улар ўртасидаги фарқ слайдли жуфтликлар фарқига тенг эмас	Аниқланган слайдли жуфтликлар асосида ўрнатилган калитларга нисбатан алгоритмни комбинацияланган слайдли ҳужум усулига баҳолаб бўлмайди

2.5.21-жадвалнинг давоми

III.	Алгоритмнинг тўрт раундли ўзига хослиги тўрт хил раунд калитлари ва тегишли акслантиришлари асосида иккинчи босқич учун комбинацияланган слайдли ҳужум шартларини қаноатлантирувчи барча слайд жуфтликларни аниқлаш. Яъни, иккинчи босқичда 1- ва 3-раунд калитлари ўртасидаги ўзаро ик-кинчи фарқ 1- ва охирги раундлардаги слайдли жуфтликлар ўртасидаги ўзаро фарққа тенг	Слайд жуфтликлар мавжуд	Мазкур слайдли жуфтликлар билан калит битларини аниқлаш мумкинлиги текширилиб кўриш натижасида хулоса берилади
		Слайд жуфтликлар мавжуд эмас (реал вақт мобайнида топилмади)	Алгоритмни комбинацияланган слайдли ҳужум усулига баҳолаб бўлмайди
IV.	Аниқланган барча слайдли жуфтликлар асосида биринчи дешифрлаш жараёнига иккинчи шифрлаш жараёнини бир раундга кечиктириб, биринчи ва охирги раунд мосликлари учун, раунд акслантиришларидан тескари тартибда ўтказиб, мумкин бўлган калит вариантларини аниқлаш	Биринчи ва охирги раундда аниқланган калитлар ўзаро тенг ва уларнинг фарқи слайд жуфтликлар фарқига тенг, ушбу калитлардан иккинчи раунд калити учун мумкин бўлган калитлар тўплами ҳосил бўлади	Аниқланган 1-раунд калитига слайдли жуфтликлар ўртасидаги фарқни қўшиш орқали 3-раунд калити ҳосил қилинади. Мазкур аниқланган мумкин бўлган калитларни ҳақиқийлигига текшириш натижасида хулоса берилади
		Биринчи ва охирги раундда	Аниқланган слайд жуфтликлар

2.5.21-жадвалнинг давоми

		аниқланган калитлар ўзаро тенг эмас ёки улар ўртасидаги фарқ слайд жуфтликлар фарқига тенг эмас	асосида ўрнатилган калитларга нисбатан алгоритмни комбинацияланган слайдли ҳужум усулига баҳолаб бўлмайди
V.	Аниқланган мумкин бўлган калитларни ҳақиқийликка текшириш. Мумкин бўлган калитлар ёрдамида аниқланган слайдли жуфтлик матнларни биринчи шифрлаш жараёнида ҳосил бўлган шифрматнларни, ҳамда иккинчи дешифрлаш жараёнларида ҳосил бўлган очиқ матнларни, мавжуд шифрматнлар ва очиқ матнлар билан солиштириш	Аниқланган калитлар комбинацияланган слайдли ҳужум усулининг барча шартларини қаноатлантирди	Алгоритм барча раундларда тўрт хил калит ишлатилганда комбинацияланган слайдли ҳужум усулига бардошли эмас
		Аниқланган калитлар ёрдамида очиқ матнларни шифрлашда ҳосил бўлган шифрматнлар мавжуд шифр-матнларга тенг эмас	Алгоритм барча раундларда тўрт хил калит ишлатилганда комбинацияланган слайдли ҳужум усулига амалий бардошли

Умумий ҳолда юқорида келтирилган маълумотларга таяниб, хулоса ўрнида айтиш мумкинки, слайдли ҳужум усулларини ўтказиш учун зарур бўлган слайд жуфтликларини генерация қилиш етарлича кўп вақтни талаб этади. Айнан мазкур масаланинг самарали ечилиши ушбу ҳужум турлари самарадорлигига ҳам ўз таъсирини кўрсатади.

Слайдли ҳужум криптотаҳлил усулининг ГОСТ 28147-89 ва DES шифрлаш алгоритмларининг бир, икки ва тўрт раундли ўзига хос кўринишларига қўлланилишидан, мазкур ҳужум шартларини қаноатлантирувчи слайдли жуфтликларни аниқлаш бўйича умумий хулоса бериб бўлмаслиги маълум бўлди. Шунингдек, алгоритм раундлар сони, калитлар ва раунд акслантиришларининг ўзгариши

слайдли жуфтликларни аниқлашга бир текис таъсир кўрсатмади. Ҳар хил калитлар асосида ГОСТ 28147-89 алгоритми учун танланган очиқ матн асосида мумкин бўлган 2^{32} та матндан 32 разрядли Галуа генератори ёрдамида 2^{18} та матн таҳлил қилинди (частотаси 2,8 ГГц, оператив хотираси 3,5 Гб ЭҲМда 250 соатда). Натижада, киритилган икки хил калитлар учун 2^6 ва 2^5га яқин слайдли жуфтликлар топилиб, уларнинг фақат ярмида ҳақиқий калит ҳосил қилинди. Таъкидлаш жоизки, фақат бир ёки иккита слайдли жуфтликлардан ҳам калитни тўлиқ аниқлаш мумкин, ва аксинча, аниқланган слайдли жуфтликлардан бирортаси ҳам ҳақиқий калитни аниқлаш имконини бермаслиги мумкин. Шу сабабдан, амалда слайдли ҳужумни самарали ўтказиш учун зарур слайдли жуфтликлар сонини аниқловчи катталикни олдиндан аниқлаб бўлмайди.

Назорат саволлари

1. Слайдли ҳужум криптотаҳлил усулининг қўлланилиши нимага асосланган?

2. Слайдли жуфтлик тушунчаси ва унга мисоллар келтиринг.

3. Қандай ҳолларда акслантириш функцияси кучсиз дейилади ва унга мисоллар келтиринг.

4. Фейстель тармоғига асосланган симметрик шифрлаш алгоритмларига слайдли ҳужум усули қўлланилишининг ўзига хос хусусиятлари нимада?

5. Тўлдирувчи слайдли ҳужум усули қўлланилишини изоҳлаб беринг.

6. Илмоқли слайдли ҳужум усули қўлланилишини изоҳлаб беринг.

7. Комбинацияланган слайдли ҳужум усули қўлланилишини изоҳлаб беринг.

8. Мазкур слайдли ҳужум усуллари қўлланилишидан олинадиган натижаларнинг назарий ва амалий аҳамиятлари нимада?

9. Слайдли ҳужум усулларининг самарадорлиги нималарга боғлиқ?

10. Слайдли ҳужум криптотаҳлил усулининг статистик ҳужум турига тегишли эканлигини изоҳланг.

2.6. Алгебраик криптотаҳлил усули

Маълумки, ҳар қандай блокли симметрик шифрлаш алгоритмлари чекли $\mathbb{M}_2^n$ тўплам (очиқ матнлар тўплами) элементларини бирор қоида ва махфий параметр (калит) асосида $\mathbb{C}_2^n$ тўплам (шифр матнлар тўплами) элементларига акслантирувчи функция ҳисобланади. Натижада мазкур функцияни бирор алгебраик тенгламалар системаси (ТС) кўринишида ифодалаш мумкин. Блокли симметрик шифрлаш алгоритмларига нисбатан алгебраик криптотаҳлил (АК) усули ҳам айнан ушбу ғояга асосланган бўлиб, унинг туб моҳияти шифрлаш алгоритмини ифодаловчи чекли майдонда аниқланган *алгебраик тенгламалар системасини тузиш* (1-босқич) ва ушбу *тенгламалар системасини ечиш* (2-босқич) орқали шифрлаш калитини аниқлашдан иборатдир [45].

Ахборот назарияси асосчиси бўлган Клод Элвуд Шенноннинг «Бардошли шифрлаш алгоритмини очиш учун, кўп ўзгарувчили тенгламалар системасини ечиш талаб этилади» – маъносидаги ғояни таклиф этиши АК усулини шифрлаш алгоритмларига нисбатан ҳужум (криптотаҳлил) усули сифатида пайдо бўлишига туртки бўлди [61]. Айнан ушбу ғояга асосланган алгебраик криптотаҳлил усулининг бугунги кундаги ривожланиши (асосан 2000 йиллардан сўнг) унинг таклифини тасдиқламоқда.

АК усули очиқ ва шифр матн асосидаги ҳужум турига мансуб бўлиб, унинг асосий қийинчилиги, мумкин бўлган барча ТСни қуриш ва уни ечиш билан баҳоланади. Шу боис, АК жараёнида алгебраик чизиқсизлик даражалари паст бўлган тенгамалар системасини қуриш ва уни ечишнинг оптимал йўллари қидирилади.

Криптотаҳлилнинг **тенгламалар системасини ечиш** босқичи шифрлаш алгоритмида фойдаланилган махфий калит (ёки айрим битларини) қийматини аниқлашга олиб келади. Бугунги кунда чекли майдонда аниқланган чизиқсиз тенгламалар системасини ечишга қаратилган кўплаб усуллар (масалан: Бухбергер, F4, F5, F5C, G2V, GVW, SAT-solvers, XL, XL2, XLF, XSL, FXL, XFL, WXL, HXL, MutantXL ва MXL2) таклиф этилган ва улардан АК ўтказишда бевосита фойдаланиб келинмоқда [46]. Жумладан, криптотаҳлил жараёнида кенг қўлланилувчи усуллардан бири бўлган MutantXL усулининг қадамлар кетма-кетлиги қуйидагича [46]:

1. Инициализация. *P(x)=0–тенгламалар системасининг алгебраик чизиқсизлик даражаси D (D=max{deg(p)}) аниқлансин.*

2. Бартараф этиш. *P(x) – тенгламалар системаси чизиқлилаштирилсин (бунда ҳар бир чизиқсиз ўзгарувчи янги чизиқли ўзгарувчи билан алмаштирилади ёки чизиқли ўзгарувчи сифатида тушинилади).*

3. Ечиш*. Тенгламалар системаси таркибидан ягона ўзгарувчига (x_i) боғлиқ бўлган тенглама топилса x_i ўзгарувчи ва у орқали қолган номаълумлар қиймати аниқлансин. Агар барча номаьлумлар қиймати топилса MutantXL алгоритми якунлансин, акс ҳолда давом эттирилсин.*

4. Ажратиб олиш. *Система таркибидан даражаси D дан кичик бўлган тенгламалар M (яъни мутант тенгламалар тўплами) тўпламга ажратиб олинсин. Ушбу M тўпламдаги тенгламаларга даражаси D-d (d – мутант тенгламанинг даражаси) га тенг бўлган барча бирхадлар кўпайтирилиб янги тенгламалар ҳосил қилинсин. Ҳосил бўлган янги тенгламалар бошланғич тенгламалар системасига бирлаштирилсин.*

5. Кенгайтириш. *Мутант тенгламалар топилмаган ҳолда D нинг қиймати D+1 га ўзгартирилсин ва системанинг барча тенгламаларига даражаси D-deg(p) (deg(p) – система таркибидаги тенгламанинг даражаси) га тенг бўлган барча бирхадлар кўпайтирилсин. Кўпайтириш натижасида ҳосил бўлган янги тенгламалар бошланғич тенгламалар системасига бирлаштирилсин. 1-қадамга қайтилсин.*

Криптотаҳлилнинг шифрлаш алгоритмини **тенгламалар системаси орқали ифодалаш** босқичи эса, умумий ҳолда қуйидаги қисм қадамлар асосида амалга оширилади [45, 46]:

a) *шифрлаш алгоритмини декомпозициялаш;* яъни, очиқ матн битларини шифр матн битлари билан боғловчи энг қисқа йўл ҳамда ушбу йўлда жойлашган ва ўзаро мустақил ишлайдиган ҳар бир акслантириш алоҳида элементларга ажратилади;

b) *ҳар бир элементни алгебраик ифодалаш;* яъни, ҳар бир акслантириш учун, уларни кириши ва чиқишини боғловчи имконият даражасида минимал алгебраик чизиқсизлик даражасига эга бўлган ТС ҳосил қилинади. Бир турга мансуб бўлган акслантиришлар учун ТС ҳосил қилиш бир хил тарзда амалга оширилади. Мазкур ТС фақат номаълумлари билан фарқланади;

c) *ҳар бир элементнинг кириши ва чиқишини бошқа элементлар ҳамда калит, очиқ матн ва шифр матн битлари билан ўзаро боғлаш.* Яъни ҳар бир элементга мос тенгламалар асосида тўлиқ шифрлаш алгоритмини ифодаловчи умумий ТС шакллантирилади. Умумий ТС шакллантирилганидан сўнг, қиймати маълум бўлган номаълумлар (очиқ ва шифр матн битларини ифодаловчи номаълумлар) қийматлари билан алмаштирилади. Қолган номаълумларни эса, тенгламалар системасини ечиш орқали аниқлаш мумкин. Айнан ушбу номаълумлар кейинчалик калит қийматини аниқлаш имконини беради.

Таъкидлаш лозимки, ТС қуриш жараёни таҳлил қилинаётган шифрлаш алгоритми тузилиши ва унинг ташкил этувчи элементлари хусусиятларига боғлиқ ҳолда амалга оширилиб, ихтиёрий шифр учун ТС қуришнинг универсал ва оптимал ечими мавжуд эмас.

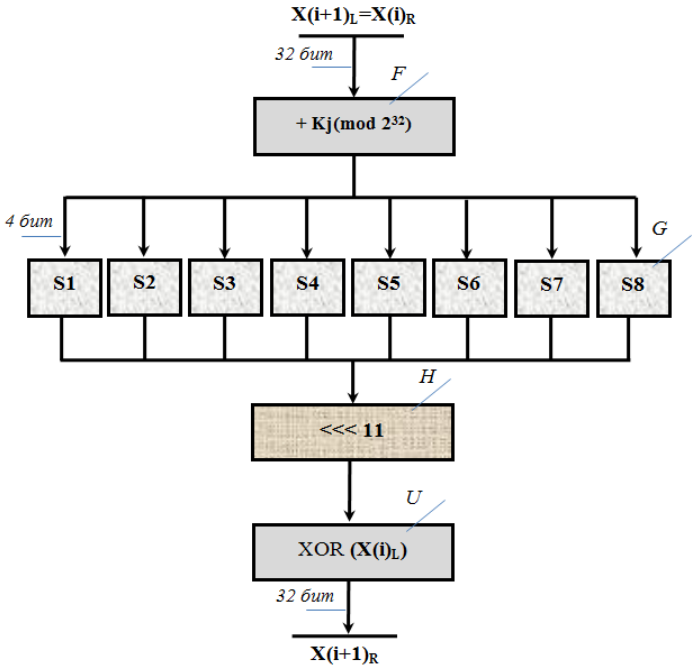
Қуйида ГОСТ 28147-89 шифрлаш алгоритмини тенгламалар системаси орқали ифодалаш жараёнига намуна келтирилган.

Мазкур намуна, АК усулини қўллаш орқали шифрлаш алгоритмини *deg*=2 (алгебраик чизиқсизлик даражаси) ўринли бўлган ТС орқали ифодалашга қаратилган.

ГОСТ 28147-89 [31] шифрлаш алгоритмини декомпозициялашда унинг 2.6.1-расмда келтирилган бир раундлик структурасига таяниш мумкин (бу ерда: $X(i)_R$ ($X(i)_L$) – *i*-раунд функциясига кирувчи маълумотнинг ўнг (чап) 32 бит қисми).

Мазкур схемага кўра, ГОСТ 28147-89 алгоритмининг ҳар бир раундида фойдаланилган акслантиришларни 4 турга (*F, H, G, U* – функциялар) ва 11 та қисм элементларга ажратиш мумкин. Шунингдек, раундлар сони ошиши билан очиқ ва шифр матн орасидаги элементлар сони ҳам ошади.

Қисм элементларга ажратишда шифрлаш алгоритмида фойдаланилган чизиқсиз акслантиришлар муҳим ахамият касб этади. Чунки айнан ушбу турдаги акслантириш ўлчами катта бўлса, уларни ифодаловчи ТС қуриш кўплаб ҳисоблашларни талаб этади. Шунинг учун, ажратилган ҳар бир элементнинг кириш ва чиқиш ўлчами имкон қадар кичик бўлиши лозим.



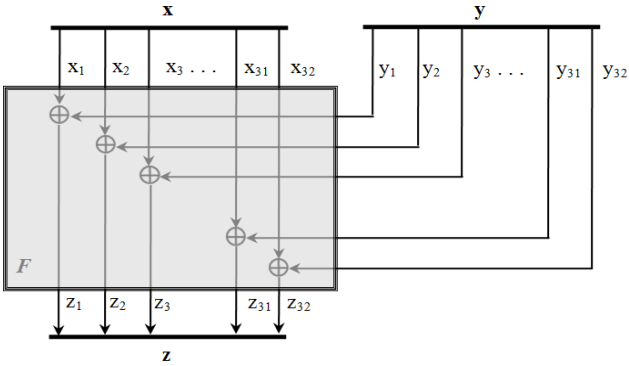
2.6.1-расм. ГОСТ 28147-89 алгоритмининг i-раунд декомпазицион схемаси.

Мазкур схемага кўра, ГОСТ 28147-89 алгоритмининг ҳар бир раундида фойдаланилган акслантиришларни 4 турга (*F, H, G, U* – функциялар) ва 11 та қисм элементларга ажратиш мумкин. Шунингдек, раундлар сони ошиши билан очиқ ва шифр матн орасидаги элементлар сони ҳам ошади.

Қисм элементларга ажратишда шифрлаш алгоритмида фойдаланилган чизиқсиз акслантиришлар муҳим ахамият касб этади. Чунки айнан ушбу турдаги акслантириш ўлчами катта бўлса, уларни ифодаловчи ТС куриш кўплаб ҳисоблашларни талаб этади. Шунинг учун, ажратилган ҳар бир элементнинг кириш ва чиқиш ўлчами имкон қадар кичик бўлиши лозим.

ГОСТ 28147-89 алгоритми учун ҳосил қилинган қисм элементларни алгебраик ифодалашда *U, H, G, F* – функцияларни кўриб ўтиш етарли.

***z=U(x,y)* функция** – узунлиги 32 бит бўлган кирувчи *x* ва *y* қийматларни 2 модул бўйича қўшиш (⊕) жараёнини амалга оширади (2.6.2-расм).

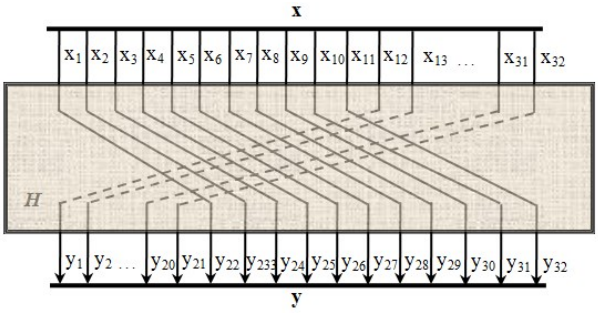


2.6.2-расм. U(x,y) – функция схемаси.

Демак, ушбу акслантириш учун *deg*=1 ўринли бўлган қуйидаги тенгламалар системасини қуриш мумкин:

$$\begin{cases} z_1 = x_1 \oplus y_1 \\ z_2 = x_2 \oplus y_2 \\ z_3 = x_3 \oplus y_3 \\ \dots\dots\dots \\ z_{31} = x_{31} \oplus y_{31} \\ z_{32} = x_{32} \oplus y_{32} \end{cases} \qquad (2.6.1)$$

***y=H(x)* функция** – узунлиги 32 бит бўлган кирувчи *x* маълумотни 11 бит чапга циклик суриш жараёнини амалга оширади (2.6.3-расм).



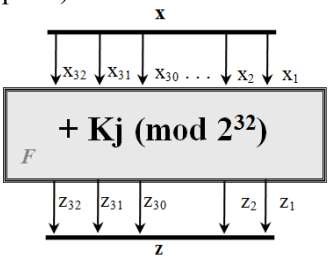
2.6.3-расм. H(x) – функция схемаси.

Мазкур акслантириш учун эса қуйидаги тенгламалар системаси ўринли:

$$\begin{cases} y_1 = x_{12} \\ y_2 = x_{13} \\ \dots\ \dots\ \dots \\ y_{21} = x_{32} \\ y_{22} = x_1 \\ y_{23} = x_2 \\ \dots\ \dots\ \dots \\ y_{32} = x_{11} \end{cases} \qquad (2.6.2)$$

***y=G(x)* функция** – 4 бит кирувчи маълумотни 4 бит чиқувчи маълумотга акслантирувчи ($\mathbb{F}_2^2 \rightarrow \mathbb{F}_2^2$) S – блок жадвал акслантиришини амалга оширади (S – блок жадвали ўзгарувчан бўлиб, махфий параметр ҳисобланади). Ушбу акслантиришни алгебраик ифодалашда [35] ишда таклиф этилган алгоритмдан фойдаланиш мумкин. Мазкур алгоритмга мувофиқ ушбу акслантириш *deg*=2 бўлган ТС орқали бир қийматли ифодаланади.

***z=F(x,k)* функция** – узунлиги 32 бит бўлган кирувчи *x* ва *k* (раунд калити) қийматларни 2^{32} модул бўйича қўшиш жараёнини амалга оширади (2.6.4-расм).



2.6.4-расм. F(x) – функция схемаси.

F(x) – функция ҳам криптотаҳлил жараёнида муҳим аҳамият касб этади ва ГОСТ 28147-89 шифрлаш алгоритмининг алгебраик криптотаҳлил усулига бардошлилигини таъминловчи асосий воситалардан бири ҳисобланади. Мазкур функциянинг алгебраик хусусиятига кўра, уни *deg*=1 ёки *deg*=2 ўринли бўлган ТС орқали бир қийматли ифодалаб бўлмайди. Шу боис, ушбу функцияни алгебраик ифодалаш мақсадида олиб борилган изланишлар ва экспериментлар натижасида, *z=F(x,k)* – функцияга нисбатан *p*=0,75

эҳтимоллик билан бажарилувчи криптотаҳлил учун энг самарали бўлган қуйидаги тенгламалар мавжудлиги аниқланди [46]:

$$\begin{gathered} z_1=x_1\oplus k_1, \\ z_i=x_i\oplus k_i\oplus k_{i-1}, \\ z_i=x_i\oplus x_{i-1}\oplus k_i. \\ 2\le i\le 32 \end{gathered} \qquad (2.6.3)$$

ТС тузиш жараёни кетма-кетлигига мувофиқ, барча элементлар учун алгебраик ифодалаш масаласи ҳал этилганидан сўнг, уларни ўзаро боғлаш, яъни улар асосида тўлиқ шифрлаш алгоритмини ифодаловчи умумий тенгламалар системасини шакллантириш лозим.

ГОСТ 28147-89 алгоритми Фейстель функцияси элементларини боғлаш (яъни Фейстель функциясига кириш ва чиқиш орқали ифодаланувчи тенгламаларни шакллантириш) *U, H, G, F* – функциялар учун тузилган тенгламалардан фойдаланиб амалга оширилади. Бунинг учун, ҳар бир элементнинг чиқишини ифодаловчи номаълумлар кейинги элементнинг мос киришини ифодаловчи тенгламалар билан алмаштирилади. Ушбу алмаштириш натижасида ҳам $deg\le 2$ ўринли бўлган тенгламалар ҳосил бўлади.

ГОСТ 28147-89 алгоритми барча раундларини боғлаш (яъни, раунд тенгламаларини очиқ ёки шифр матн элементлари билан боғлаш) Фейстель схемаси хусусиятларидан фойдаланиб амалга оширилади. Демак, ушбу жараёнда қуйидаги тенгликлардан фойдаланиш мумкин:

$$X(1)_i=P(R)_i \qquad (2.6.4)$$

$$X(2)_i=P(L)_i\oplus Y(1)_i \qquad (2.6.5)$$

$$X(t)_i=P(R)_i\oplus \sum_{\substack{j=2,\\ j\bmod 2=0}}^{t-1} Y(j)_i\text{, агар } t \text{ – тоқ бўлса,} \qquad (2.6.6)$$

$$X(t)_i=P(L)_i\oplus \sum_{\substack{j=1,\\ j\bmod 2\neq 0}}^{t-1} Y(j)_i\text{, агар } t \text{ – жуфт бўлса,} \qquad (2.6.7)$$

$$Y(31)_i=C(L)_i\oplus P(L)_i\oplus \sum_{\substack{j=1,\\ j\bmod 2\neq 0}}^{29} Y(j)_i \qquad (2.6.8)$$

$$Y(32)_i=C(R)_i\oplus P(R)_i\oplus \sum_{\substack{j=1,\\ j\bmod 2\neq 0}}^{30} Y(j)_i \qquad (2.6.9)$$

$$X(32)_i=C(R)_i \qquad (2.6.10)$$

бу ерда: P_i (C_i) – очиқ (шифр) матн блокининг i-бити.

Мазкур алмаштириш натижасида ҳам deg≤2 ўринли бўлган якуний тенгламалар системаси ҳосил бўлади. Ушбу системанинг самарали ечилиши раунд калит битларининг аниқланишига олиб келиши мумкин. Шунингдек, эҳтимоллик билан бажарилувчи тенгламалардан тўғри ечим олиш учун кўплаб матнларга нисбатан шакллантирилган системани ечиш талаб этилади.

Умумий ҳолда, мавжуд ёки янги таклиф этилган блокли симметрик шифрлаш алгоритмини АК усулига бардошлилигини баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади. Бу ерда *C=E(M,K)* (*M – очиқ матн, C – шифр матн, K – махфий калит*).

2.6.1-жадвал.
Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Шифрлаш алгоритмини *M, C* ва оралиқ махфий параметрлар (раунд калитлари ва раундга кирувчи ёки чиқувчи ўзгрувчилар) орқали *deg=min* (*min* – кичик натурал сон) ўринли бўлган ТС кўринишида ифодалаш	ТСни қуришнинг назарий ечими (ёки амалий имкони) мавжуд эмас	Алгоритм АК усулига назарий (ёки амалий) бардошли
		ТСни амалий қуриш мумкин	Кейинги босқичга ўтиш мумкин
II.	ТСни ечишнинг самарали усулини ва унга мувофиқ ТСни ечиш учун лозим бўлган ҳотира ҳажми – *H* ни ҳамда амаллар сони – *N* ни аниқлаш	*H* ўлчамдаги ҳотира ҳажми амалий мавжуд эмас ёки реал вақт мобайнида *N* та амални бажариш-нинг амалий имкони йўқ	Алгоритм АК усулига амалий амалий бардошли
		H ўлчамдаги ҳотира ҳажми амалий мавжуд ва	Кейинги босқичга ўтиш мумкин

2.6.1-жадвалнинг давоми

		реал вақт мобайнида N та амални бажариш амалий мумкин	
III.	ТСни ечиш орқали махфий калит (ёки унинг айрим қисмлари) қийматини аниқлаш	Калит (ёки унинг қисмлари) аниқланмади	Алгоритм АК усулига амалий бардошли
		Калит (ёки унинг қисмлари) аниқланди	Алгоритм АК усулига бардошсиз

Назорат саволлари

1. Алгебраик криптотаҳлил усулининг асосий қадамлар кетма-кетлиги нимадан иборат?

2. Чекли майдонда аниқланган алгебраик тенглама тушунчасига таъриф беринг ва унга мисоллар келтиринг.

3. Тенгламалар системасини ечишнинг MutantXL усули асосий қадамлар кетма-кетлигини тушунтиринг.

4. Шифрлаш алгоритмини декомпозициялаш деганда нимани тушунасиз ва унинг муҳим жиҳатлари нималардан иборат?

5. Шифрлаш алгоритми акслантиришларини алгебраик ифодалаш тушунчаси ва унинг муҳим жиҳатлари нималардан иборат?

6. Шифрни ифодаловчи алгебраик тенгламалар сони ва улар алгебраик чизиқсизлик даражалари мазкур криптотаҳлил самарадорлигига қандай таъсир этади?

7. Алгебраик криптотаҳлил усулининг мураккаблик даражаси асосан нималарга боғлиқ?

8. ГОСТ 28147-89 шифрлаш алгоритми акслантиришларини алгебраик ифодалаш жараёнларини тушунтиринг.

9. Шифрлаш алгоритми таркибидаги ўрин алмаштириш акслантиришининг таҳлил самарадорлигига таъсири қандай?

10. Шифрлаш алгоритми раундлар сони криптотаҳлил самарадорлигига қандай таъсир кўрсатади?

11. Алгебраик ва чизиқли криптотаҳлил усулларини ўзаро таққосланг.

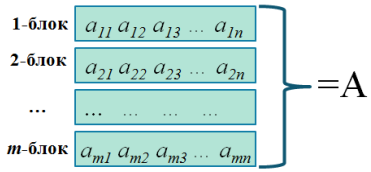
12. Мазкур криптотаҳлил усулини бошқа криптотаҳлил усуллари билан биргаликда қўллаш мумкинки, агар мумкин бўлса, ушбу жараённи тушунтиринг.

2.7. Интеграл криптотаҳлил усули

Интеграл криптотаҳлил (ИК) усули – Даниялик криптограф Ласр Кнудсен томонидан 1997 йилда «Квадрат» (Square) шифрлаш алгоритмига ҳужум тури сифатида таклиф этилди [7, 15, 63]. Шунинг учун, айрим манбаларда бу хужум турини «Square-ҳужум» деб номланади. Кейинчалик, ушбу ҳужум турининг аналоглари турли хил номлар остида бир нечта илмий мақолаларда пайдо бўлди ва умумий холда *интеграл криптотаҳлил* номи остида қабул қилинди. «*Интеграл криптотаҳлил*» термини биринчи бор 1999 йилда «Integral cryptanalysis of SAFER» нашрида келтирилган (таклиф этилган) [13].

ИК усули *адаптив танланган очиқ матнлар асосидаги ҳужум* тури ҳисобланади ва асосан SP тармоғига асосланган шифрлаш алгоритмлари учун қўлланилади. Ушбу усулнинг асосий ғояси пайдо бўлгандан сўнг, турли мутахассислар томонидан ушбу криптотаҳлил усули янада мукаммаллаштирилди ва Square шифрига ўхшаш бўлган CRYPTON, Rijndael ва SHARK каби алгоритмларга қўлланилди. ИК усулининг турли модификациялари Hierocrypt, IDEA, Camellia, Skipjack, MISTY1, MISTY2, SAFER++, KHAZAD ва FOX шифрлаш алгоритмларига ҳам қўлланилиб, тегишли натижалар олинган [64].

ИК усулини SP тармоғига асосланган бирор блокли симметрик шифрлаш алгоритмига қўллаш учун, танлаб олинган очиқ матнлар ва уларга мос шифрматнларнинг махсус тўплами ҳамда шифрлаш алгоритми маълум бўлиши лозим. Криптотаҳлил учун очиқ матнлар тўпламини (A) танлаш қуйидаги тартибда амалга оширилади (2.7.1-расм).



2.7.1-расм. Очиқ матнлар тўплами.

Ушбу расмда, m – танлаб олинувчи блоклар сони ва $m=2^{N*V}$, N – a_{ij} элементни битлар сонига тенг (a_{ij} элемент узунлиги алгоритмнинг чизиқсиз акслантириши кириш ўлчамига тенг, масалан: AES алгоритми учун N=8), V ($1<V<n$) – шифрлаш алгоритми раундлар сонига, n – қаралаётган алгоритм блок узунлигига боғлиқ (масалан, 128 битли AES алгоритми учун n=128/8=16) ҳолда аниқланувчи сонлар (m – сонини аниқлаш бўйича кейинчалик маълумот берилади).

Мазкур A – очиқ матнлар тўплами қуйидагича аниқланувчи **актив** ва **пассив** элементлардан ташкил топиши керак, яъни:

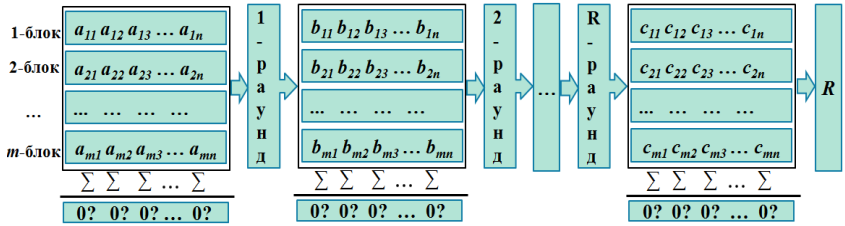
- агар $j=1..n$ учун $a_{1,j}\neq a_{2,j}\neq a_{3,j}...\neq a_{m,j}$ бажарилса, очиқ матнлардаги $a_{i,j}$ $(i=1…m,\ j=const)$ элементлар **актив элементлар** ҳисобланади;
- агар $j=1..n$ учун $a_{1,j}=a_{2,j}=a_{3,j}...=a_{m,j}$ бажарилса, очиқ матнлардаги $a_{i,j}$ $(i=1…m,\ j=const)$ элементлар **пассив элементлар** ҳисобланади.

Юқоридаги шартлар асосида танлаб олинган A – очиқ матнлар тўплами элементлари учун [1, n] – ораликдан олинган барча j га нисбатан қуйидаги тенглик ўринли (яъни баланслашган) [13]:

$$\sum_{i=1}^{m} a_{i,j} = 0 \qquad (2.7.1)$$

бу ерда, йиғинди – XOR (2 модул бўйича қўшиш) амали асосида бажарилади.

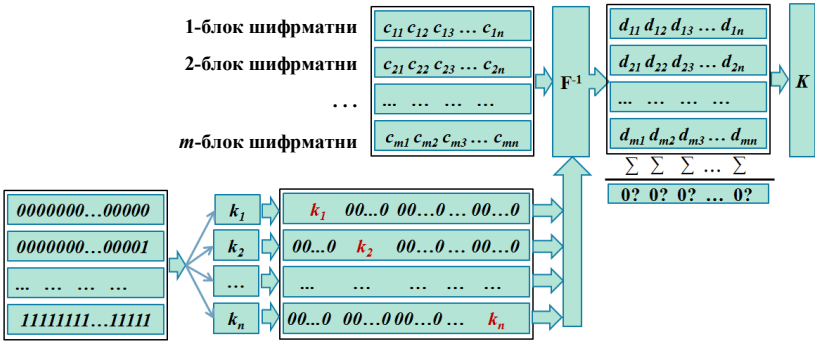
Криптотаҳлил асосида, танлаб олинган А тўплам хусусиятининг шифрлаш алгоритми раундларидан ўтганда қандай ўзгаришини (**актив**, **пассив**, **аралаш** (актив ҳам эмас пассив ҳам эмас)) аниқлаш ётади (2.7.2-расм).



2.7.2-расм. Очиқ матнлар тўпламини кузатиш схемаси.

SP тармоғига асосланган аксарият шифрлаш алгоритмларида раунд калитлари mod2 амал бўйича қўшилади. Шунга кўра, калит қўшиш жараёни кузатилаётган тўплам элементлари қийматларининг ўзгаришига олиб келади, бироқ тўплам хусусиятини ўзгартирмайди (яъни, элементларнинг актив ёки пассивлик хусусиятини ўзгартирмайди). Шунинг учун, тўпламни кузатишда калит қўшиш жараёни инобатга олинмайди, шунингдек, калит қиймати криптотаҳлилчи учун махфий бўлади. Шифрлаш алгоритмларида ИК усулига бўлган асосий камчилиги ҳам айнан калит қўшиш акслантиришларининг ушбу хусусияти ҳисобланади. Юқоридаги фикрлар нафақат калит қўшиш акслантириши, балки тўплам хусусиятини ўзгартирмайдиган ихтиёрий акслантириш учун ҳам ўринли. Масалан, S-блок акслантириши актив элементни актив, пассив элементни пассив элементга ўзгартиради. Шу боис, S-блок жадвали махфий бўлган шифрлаш алгоритмларига ҳам ИК усулини қўллаш мумкин.

Агар кузатилаётган очиқ матнлар тўплами бирор R-раунддан чиқиш ҳолатида баланслашганлик хусусияти бузилиб ҳамда актив ва пассив байтлар мавжуд бўлмаса, у ҳолда, R раундли шифрлаш алгоритми сўнгги раундида фойдаланилган махфий калитни топиш мумкин. Яъни шифрлаш алгоритми сўнгги раундида фойдаланилган калит қийматини аниқлаш сўнгги раундга кирувчи тўплам элементлари учун (2.7.1) тенглик бажарилишини ҳамда сўнгги раунддан чиқувчи маълумотни (шифрматнни) билган ҳолда статистика ўтказиш йўли орқали амалга оширилади. Ушбу жараённи амалга ошириш функционал схемаси 2.7.3-расмда келтирилган.



2.7.3-расм. Сўнгги раунд калит қийматини аниқлашнинг функционал схемаси.

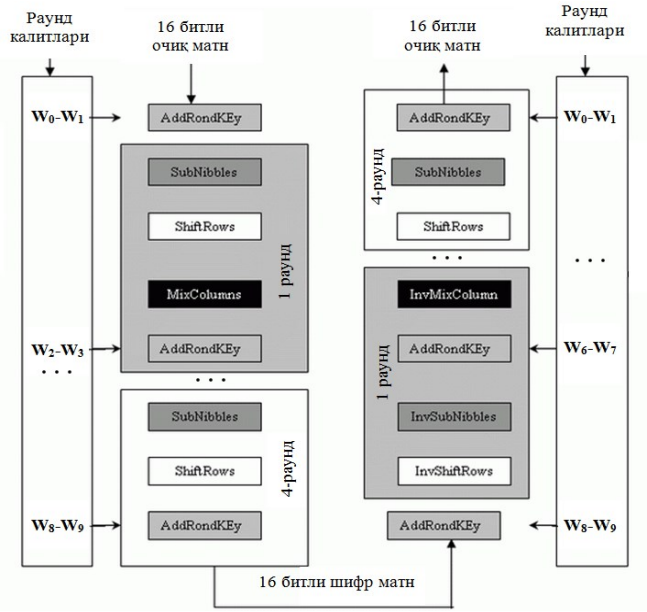
Яъни очиқ матнларга мос шифр матнлар тўпламини бирор танлаб олинган калит асосида бир раунд дешифрланади. Агар дешифрлашдан ҳосил бўлган матнлар тўплами учун (2.7.1) тенглик бажарилса, ушбу калит номзод калитлар рўйхатига қўшилади. Ушбу жараён барча танлаб олинган калитлар устида амалга оширилади.

Демак, бирор n раундли шифрлаш алгоритмига интеграл криптотаҳлил усулини қўллаб m-раунд калитини аниқлашда, *m-раундга киришда баланслашган* ва *m-раунддан чиқишда баланслашмаган* тўплам ҳосил бўлишини таъминлаб берувчи очиқ матнлар тўпламини танлаш масаласи ҳал этилиши лозим.

Қуйида, 4 раундли S_AES шифрлаш алгоритмига ИК усули қўлланилишига намуна келтирилган.

Мазкур намуна ИК усулини қўллаш орқали *сўнгги раундда фойдаланилган* $K(4) \in 2^{16}$ *раунд калитининг дастлабки* $K(4)_1 \in 2^4$ *қисм калит қийматини аниқлашга* қаратилган.

S_AES симметрик шифрлаш алгоритми SP тармоғига асосланган бўлиб, маълумотларни қайта ишлаш блок узунлиги 16 битга тенг. Алгоритм 2x2 ўлчамли ҳолат жадвали устида акслантиришни амалга ошириб, SubNibbles, ShiftRows, MixColumns ва AddRoundKey акслантиришларини [19] ўз ичига олади (2.7.4-расм). S_AES алгоритмининг асосий чизиқсиз акслантириши SubNibbles блоки бўлиб, 4 бит кириш маълумотни 4 бит чиқиш маълумотга акслантиради.



2.7.4-расм. 4 раундли S_AES алгоритми схемаси.

Очиқ матнлар тўпламини танлаш шартига мувофиқ, ушбу ҳолда шифрлаш алгоритмининг 4-раундига киришда баланслашган ва 4-рауддан чиқишда баланслашмаган тўплам ҳосил бўлишини таъминлаб берувчи очиқ матнлар тўпламини танлаш лозим. Шунга мувофиқ, 4 раундли S_AES алгоритмига ИК усулини қўллаш учун қуйидагича $P_i=p_{i1}p_{i2}p_{i3}p_{i4}$ (i=0,1,2,...,15) очиқ матнлар тўплами танланди:

P_0=0000 0101 1110 1111
P_1=0001 0101 1110 1111
P_2=0010 0101 1110 1111
P_3=0011 0101 1110 1111
P_4=0100 0101 1110 1111
P_5=0101 0101 1110 1111
P_6=0110 0101 1110 1111
P_7=0111 0101 1110 1111

P_8=1000 0101 1110 1111
P_9=1001 0101 1110 1111
P_{10}=1010 0101 1110 1111
P_{11}=1011 0101 1110 1111
P_{12}=1100 0101 1110 1111
P_{13}=1101 0101 1110 1111
P_{14}=1110 0101 1110 1111
P_{15}=1111 0101 1110 1111

Ушбу очиқ матнларнинг дастлабки ярим байт (p_{i1}) лари ўзаро фарқли бўлиб, улар актив элементлар бўлади. Қолган элементлари ўзаро бир хил (яъни, p_{i2}=0101, p_{i3}=1110, p_{i4}=1111) бўлиб, улар пассив элементлар бўлади.

Юқоридаги (2.7.1) тенгликка кўра, мазкур 16 та матн мос элементларининг модул 2 бўйича йиғиндиси нолга (ушбу ҳолда 0000 га) тенг бўлади. Масалан, актив элементлар йиғиндиси қуйидагича ҳосил қилинади:

$$\sum_{i=0}^{15} p_{i,1} = 0000 \oplus 0001 \oplus 0010 \oplus 0011 \oplus 0100 \oplus 0101 \oplus 0110 \oplus 0111 \oplus$$
$$\oplus 1000 \oplus 1001 \oplus 1010 \oplus 1011 \oplus 1100 \oplus 1101 \oplus 1110 \oplus 1111 = 0000$$

Криптотаҳлил жараёнини шартли икки босқичга, яъни **очиқ матнлар тўпламини кузатиш** ва **сўнгги раунд калитини аниқлаш** босқичларига ажратган ҳолда, мазкур босқичларни қуйидагича амалга оширамиз.

S_AES шифрлаш алгоритми биринчи раундидаги дастлабки акслантириш SubNibbles акслантириши бўлиб, ҳар бир ҳолат ярим байтларини жадвал асосида алмаштириш жараёнини амалга оширади. SubNibbles акслантиришига тескари акслантириш InvSubNibbles бўлиб, ушбу акслантиришлар қуйидаги 2.7.1 ва 2.7.2-жадвалларда келтирилган.

2.7.1-жадвал.

SubNibbles жадвали

Кириш	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Чиқиш	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7

2.7.2-жадвал.

InvSubNibbles жадвали

Кириш	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Чиқиш	14	3	4	8	1	12	10	15	7	13	9	6	11	2	0	5

Демак, кузатилаётган тўпламнинг **SubNibbles** акслантиришидан кейинги ўзгариши қуйидагича бўлади:

B_0=SubNibbles(0000,0101,1110,1111)=1110 1111 0000 0111
B_1=SubNibbles(0001,0101,1110,1111)=0100 1111 0000 0111
B_2=SubNibbles(0010,0101,1110,1111)=1101 1111 0000 0111
B_3=SubNibbles(0011,0101,1110,1111)=0001 1111 0000 0111
B_4=SubNibbles(0100,1111,0000,0111)=0010 1111 0000 0111
B_5=SubNibbles(0101,1111,0000,0111)=1111 1111 0000 0111
B_6=SubNibbles(0110,1111,0000,0111)=1011 1111 0000 0111
B_7=SubNibbles(0111,1111,0000,0111)=1000 1111 0000 0111
B_8=SubNibbles(1000,1111,0000,0111)=0011 1111 0000 0111
B_9=SubNibbles(1001,1111,0000,0111)=1010 1111 0000 0111
B_{10}=SubNibbles(1010,1111,0000,0111)=0110 1111 0000 0111
B_{11}=SubNibbles(1011,1111,0000,0111)=1100 1111 0000 0111
B_{12}=SubNibbles(1100,1111,0000,0111)=0101 1111 0000 0111

B_{13}=SubNibbles(1101,1111,0000,0111)=1001 1111 0000 0111
B_{14}=SubNibbles(1110,1111,0110,0111)=0000 1111 0000 0111
B_{15}=SubNibbles(1111,1111,0110,0111)=0111 1111 0000 0111

Кўриш мумкинки, ушбу акслантиришдан кейин ҳам фақат b_{i1} – қисмлар актив элемент, қолган қисмлар пассив элемент шартини бажаради. Алгоритмнинг кейинги акслантириши ShiftRow акслантириши бўлиб, ҳолат жадвалининг 2-сатр элементлари ўрнини ўзаро алмаштириш амалини бажаради. Шунга кўра, кузатилаётган тўпламнинг **ShiftRows** акслантиришидан кейинги ҳолати қуйидагича бўлади:

C_0= 1110 0111 0000 1111
C_1= 0100 0111 0000 1111
C_2= 1101 0111 0000 1111
C_3= 0001 0111 0000 1111
C_4= 0010 0111 0000 1111
C_5= 1111 0111 0000 1111
C_6= 1011 0111 0000 1111
C_7= 1000 0111 0000 1111
C_8= 0011 0111 0000 1111
C_9= 1010 0111 0000 1111
C_{10}= 0110 0111 0000 1111
C_{11}= 1100 0111 0000 1111
C_{12}= 0101 0111 0000 1111
C_{13}= 1001 0111 0000 1111
C_{14}= 0000 0111 0000 1111
C_{15}= 0111 0111 0000 1111

Ушбу акслантиришдан кейин ҳам фақат c_{i1} – қисмлар актив элемент, қолган қисмлар пассив элемент шартини бажаради. Кейинги акслантириш MixColumn акслантириши бўлиб, фиксирланган $\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$ матрицага ҳолат жадвалини чекли майдонда кўпайтириш амалини бажаради. Кузатилаётган тўпламнинг MixColumn акслантиришдан кейинги ҳолати қуйидагича бўлади:

D_0=1111 0110 1101 0010
D_1=0010 0001 1101 0010
D_2=1010 0000 1101 0010
D_3=1101 1011 1101 0010
D_4=1100 0100 1101 0010
D_5=1000 1101 1101 0010
D_6=0000 1100 1101 0010
D_7=0101 1010 1101 0010
D_8=1011 1111 1101 0010
D_9=0011 1110 1101 0010
D_{10}=0100 0101 1101 0010
D_{11}=1001 0010 1101 0010
D_{12}=0001 0011 1101 0010
D_{13}=0110 1000 1101 0010
D_{14}=1110 1001 1101 0010
D_{15}=0111 0111 0000 1111

Ҳосил бўлган қийматлардан маълумки, MixColumn акслантиришидан сўнг тўпламда битта эмас, иккита актив бўлаклар ҳосил бўлди, яъни d_{i1}, d_{i2} – қисмлар актив элемент, қолган қисмлар пассив элемент шартини бажаради.

Кейинги акслантириш AddRoundKey акслантириши бўлиб, блок узунлигига тенг бўлган раунд калитлари жадвалини модул 2 амали

бўйича ҳолат жадвалига қўшишни амалга оширади. Юқорида таъкидланганидек, раунд калитларини қўшиш блоки кузатилаётган тўплам элементлари қийматининг ўзгаришига олиб келади, лекин тўпламнинг хусусиятига (баланслашганлигига) таъсир қилмайди. Шунинг учун ҳам криптотаҳлил жараёнида ушбу блок эътиборга олинмайди. Аммо қаралаётган мазкур мисолда, криптотаҳлил сўнггида аниқланувчи калит билан солиштириш мақсадида, калит қўшиш блоки ҳам киритилди. Шунга кўра айтайлик, қаралаётган шифрлаш алгоритмида ҳар бир раунд калити бир хил бўлиб, унинг қиймати қуйидагича бўлсин: K=1010 0011 1111 0100. Кузатилаётган тўпламнинг AddRoundKey акслантиришидан кейинги ўзгариши эса, қуйидагича бўлади:

E_0=0101 0101 0010 0110
E_1=1000 0010 0010 0110
E_2=0000 0011 0010 0110
E_3=0111 1000 0010 0110
E_4=0010 1110 0010 0110
E_5=0110 0111 0010 0110
E_6=1010 1111 0010 0110
E_7=1111 1001 0010 0110
E_8=0001 1100 0010 0110
E_9=1001 1101 0010 0110
E_{10}=1110 0110 0010 0110
E_{11}=0011 0001 0010 0110
E_{12}=1011 0000 0010 0110
E_{13}=1100 1011 0010 0110
E_{14}=0100 1010 0010 0110
E_{15}=1101 0100 0010 0110

Кўриш мумкинки, калит қўшилганидан кейин ҳам элементларнинг актив ва пассивлик хусусиятлари ўзгармади. Умумий ҳолда, ушбу кузатилаётган тўпламнинг 1-раунд акслантиришларидан кейинги ўзгаришлари 2.7.3-жадвалда келтирилган.

2.7.3-жадвал.

Кузатилаётган тўпламнинг 1-рауддан кейинги ўзгариши

Акс-ш	**SubNibbles**	**ShiftRow**	**MixColumn**	**AddRoundKey**
1-блок	1110|1111|0000|0111	1110|0111|0000|1111	1111|0110|1101|0010	0101|0101|0010|0110
2-блок	0100|1111|0000|0111	0100|0111|0000|1111	0010|0001|1101|0010	1000|0010|0010|0110
3-блок	1101|1111|0000|0111	1101|0111|0000|1111	1010|0000|1101|0010	0000|0011|0010|0110
4-блок	0001|1111|0000|0111	0001|0111|0000|1111	1101|1011|1101|0010	0111|1000|0010|0110
5-блок	0010|1111|0000|0111	0010|0111|0000|1111	1000|1101|1101|0010	0010|1110|0010|0110
6-блок	1111|1111|0000|0111	1111|0111|0000|1111	1100|0100|1101|0010	0110|0111|0010|0110
7-блок	1011|1111|0000|0111	1011|0111|0000|1111	0000|1100|1101|0010	1010|1111|0010|0110
8-блок	1000|1111|0000|0111	1000|0111|0000|1111	0101|1010|1101|0010	1111|1001|0010|0110
9-блок	0011|1111|0000|0111	0011|0111|0000|1111	1011|1111|1101|0010	0001|1100|0010|0110
10-блок	1010|1111|0000|0111	1010|0111|0000|1111	0011|1110|1101|0010	1001|1101|0010|0110
11-блок	0110|1111|0000|0111	0110|0111|0000|1111	0100|0101|1101|0010	1110|0110|0010|0110
12-блок	1100|1111|0000|0111	1100|0111|0000|1111	1001|0010|1101|0010	0011|0001|0010|0110
13-блок	0101|1111|0000|0111	0101|0111|0000|1111	0001|0011|1101|0010	1011|0000|0010|0110
14-блок	1001|1111|0000|0111	1001|0111|0000|1111	0110|1000|1101|0010	1100|1011|0010|0110
15-блок	0000|1111|0000|0111	0000|0111|0000|1111	1110|1001|1101|0010	0100|1010|0010|0110
16-блок	0111|1111|0000|0111	0111|0111|0000|1111	0111|0111|1101|0010	1101|0100|0010|0110
(XOR)∑=	**0000|0000|0000|0000**	**0000|0000|0000|0000**	**0000|0000|0000|0000**	**0000|0000|0000|0000**

Ушбу кўриб ўтилган кузатиш жараёни каби S_AES шифрлаш алгоритмининг кейинги раундлари учун ҳам тўплам ўзгаришини кузатиб борамиз. Шунга кўра кузатилаётган тўпламнинг шифрлаш алгоритми 2-раундидан кейинги ўзгариши қуйидаги 2.7.4-жадвалда келтирилган.

2.7.4-жадвал.

Кузатилаётган тўпламнинг 2-раундан кейинги ўзгариши

Акс-ш	SubNibbles	ShiftRow	MixColumn	AddRoundKey
1-блок	1111|1111|1101|1011	1111|1011|1101|1111	0111|0011|1001|1011	1101|0000|0110|1111
2-блок	0011|1101|1101|1011	0011|1011|1101|1101	0000|1000|1101|1101	1010|1011|0010|1001
3-блок	1110|0001|1101|1011	1110|1011|1101|0001	0100|0001|0110|1010	1110|0010|1001|1110
4-блок	1000|0011|1101|1011	1000|1011|1101|0011	1110|1101|0010|1100	0100|1110|1101|1000
5-блок	1101|0000|1101|1011	1101|1011|1101|0000	0001|0111|0100|1001	1011|0100|1011|1101
6-блок	1011|1000|1101|1011	1011|1011|1101|1000	1011|1011|0111|0010	0001|1000|1000|0110
7-блок	0110|0111|1101|1011	0110|1011|1101|0111	1111|0010|1010|0000	0101|0001|0101|0100
8-блок	0111|1010|1101|1011	0111|1011|1101|1010	1100|0000|0011|0100	0110|0011|1100|0000
9-блок	0100|0101|1101|1011	0100|1011|1101|0101	1001|0110|1110|0110	0011|0101|0001|0010
10-блок	1010|1001|1101|1011	1010|1011|1101|1001	1000|1001|0101|0001	0010|1010|1010|0101
11-блок	0000|1011|1101|1011	0000|1011|1101|1011	0101|1110|0001|0111	1111|1101|1110|0011
12-блок	0001|0100|1101|1011	0001|1011|1101|0100	0110|1100|1100|0101	1100|1111|0011|0001
13-блок	1100|1110|1101|1011	1100|1011|1101|1110	0010|0101|1011|1000	1000|0110|0100|1100
14-блок	0101|1100|1101|1011	0101|1011|1101|1100	1010|0100|1111|1110	0000|0111|0000|1010
15-блок	0010|0110|1101|1011	0010|1011|1101|0110	0011|1010|1000|0011	1001|1001|0111|0111
16-блок	1001|0010|1101|1011	1001|1011|1101|0010	1101|1111|0000|1111	0111|1100|1111|1011
(XOR)∑=	**0000|0000|0000|0000**	**0000|0000|0000|0000**	**0000|0000|0000|0000**	**0000|0000|0000|0000**

Жадвал қийматларидан маълумки, 2-раундан сўнг тўпламнинг барча элементлари актив элементга ўзгарди. Кузатилаётган тўпламнинг шифрлаш алгоритми 3-раундидан кейинги ўзгариши қуйидаги 2.7.5-жадвалда келтирилган.

2.7.5-жадвал.

Кузатилаётган тўпламнинг 3-раундан кейинги ўзгариши

Акс-ш	SubNibbles	ShiftRow	MixColumn	AddRoundKey
1-блок	1001|1110|1011|0111	1001|0111|1011|1110	0110|1000|0001|0100	1100|1011|1110|0000
2-блок	0110|1100|1101|1010	0110|1010|1101|1100	1101|0001|1111|1110	0111|0010|0000|1010
3-блок	0000|1101|1010|0000	0000|0000|1010|1101	0000|0000|0100|0011	1010|0011|1011|0111
4-блок	0010|0000|1001|0011	0010|0011|1001|0000	0000|0001|1000|0001	1010|0010|0111|0101
5-блок	1100|0010|1100|1001	1100|1001|1100|0010	0110|0011|0011|1101	1100|0000|1100|1001
6-блок	0100|0011|0011|1011	0100|1011|0011|0011	1001|0110|0011|0011	0011|0101|1100|0111
7-блок	1111|0100|1111|0010	1111|0010|1111|0100	0110|1011|1010|0001	1100|1000|0101|0101
8-блок	1011|0001|0101|1110	1011|1110|0101|0001	0001|0100|1101|1001	1011|0111|0010|1101
9-блок	0001|1111|0100|1101	0001|1101|0100|1111	1010|0110|0001|1010	0000|0101|1110|1110
10-блок	1101|0110|0110|1111	1101|1111|0110|0110	1001|1011|0110|0110	0011|1000|1001|0010
11-блок	0111|1001|0000|0001	0111|0001|0000|1001	1011|1101|0001|1000	0001|1110|1110|1100
12-блок	0101|0111|0001|0100	0101|0100|0001|0111	0111|0110|1101|1011	1101|0101|0010|1111
13-блок	0011|1011|0010|0101	0011|0101|0010|1011	1111|1001|0011|1010	0101|1010|1100|1110
14-блок	1110|1000|1110|0110	1110|0110|1110|1000	1101|0101|0010|0100	0111|0110|1101|0000
15-блок	1010|1010|1000|1000	1010|1000|1000|1010	1110|1100|1100|1110	0100|1111|0011|1010
16-блок	1000|0101|0111|1100	1000|1100|0111|0101	0000|0100|0011|0001	1010|0111|1100|0101
(XOR)∑=	**0000|0000|0000|0000**	**0000|0000|0000|0000**	**0000|0000|0000|0000**	**0000|0000|0000|0000**

Кузатилаётган тўпламнинг 3-раунддан кейинги ўзгаришига кўра, барча элементлар аралаш (яъни, актив ҳам эмас, пассив ҳам эмас) элементга ўзгарди. Лекин кўриш мумкинки, барча элементлар учун (2.7.1) тенглик ўринли, яъни тўплам элементлари балансланган. Ушбу тўпламнинг шифрлаш алгоритми 4-раундидан кейинги ўзгариши 2.7.6-жадвалда келтирилган (маълумки, сўнгги раундда MixColumn акслантиришидан фойдаланилмайди).

2.7.6-жадвал.

Кузатилаётган тўпламнинг 4-раунддан кейинги ўзгариши

Акс-ш	SubNibbles	ShiftRow	MixColumn	AddRoundKey
1-блок	0101|1100|0000|1110	0101|1110|0000|1100		1111|1101|1111|1000
2-блок	1000|1101|1110|0110	1000|0110|1110|1101		0010|0101|0001|1001
3-блок	0110|0001|1100|1000	0110|1000|1100|0001		1100|1011|0011|0101
4-блок	0110|1101|1000|1111	0110|1111|1000|1101		1100|1100|0111|1001
5-блок	0101|1110|0101|1010	0101|1010|0101|1110		1111|1001|1010|1010
6-блок	0001|1111|0101|1000	0001|1000|0101|1111		1011|1011|1010|1011
7-блок	0101|0011|1111|1111	0101|1111|1111|0011		1111|1100|0000|0111
8-блок	1100|1000|1101|1001	1100|1001|1101|1000		0110|1010|0010|1100
9-блок	1110|1111|0000|0000	1110|0000|0000|1111		0100|0011|1111|1011
10-блок	0001|0011|1010|1101	0001|1101|1010|0011		1011|1110|0101|0111
11-блок	0100|0000|0000|0101	0100|0101|0000|0000		1110|0110|1111|0100
12-блок	1001|1111|1101|0111	1001|0111|1101|1111		0011|0100|0010|1011
13-блок	1111|0110|0101|0000	1111|0000|0101|0110		0101|0011|1010|0010
14-блок	1000|1011|1001|1110	1000|1110|1001|1011		0010|1101|0110|1111
15-блок	0010|0111|0001|0110	0010|0110|0001|0111		1000|0101|1110|0011
16-блок	0110|1000|0101|1111	0110|1111|0101|1000		1100|1100|1010|1100
(XOR)∑=	**0001|0110|0111|0011**	**0001|0011|0111|0110**		**0001|0011|0111|0110**

Алгоритм 4-раундидан сўнг ҳосил бўлган тўплам элементлари учун (2.7.1) тенглик бажарилмайди, яъни тўплам элементлари балансланмаган. **Демак**, танланган очиқ матнлар тўплами учун 4-раундга киришда балансланган ва 4-раунддан чиқишда балансланмаган тўплам ҳосил бўлиши кузатилди. Айтиш лозимки, раунд калитларини қўшиш блоки бажарилмаганда ҳам ушбу хусусият сақланади. Айнан мазкур хусусият сўнгги раундда фойдаланилган раунд калитини аниқлаш имконини беради.

Сўнгги раунд калит қийматини аниқлаш мазкур раундга кирувчи тўплам элементлари учун (2.7.1) тенглик бажарилиши ҳамда сўнгги раунддан чиқувчи маълумотни (шифр матн) билган ҳолда, юқорида келтирилган қоида асосида статистика ўтказиш орқали амалга оширилади. Қуйида сўнгги раундда фойдаланилган $K(4) \in 2^{16}$ раунд калитининг дастлабки $K(4)_1 \in 2^4$ қисм калитини топиш жараёнини кўриб ўтамиз.

Бизга (криптотаҳлилчига) маълум бўлган шифр матнлар тўплами қуйидагича (2.7.6-жадвалга кўра):

T_0=1111 1101 1111 1000
T_1=0010 0101 0001 1001
T_2=1100 1011 0011 0101
T_3=1100 1100 0111 1001
T_4=1111 1001 1010 1010
T_5=1011 1011 1010 1011
T_6=1111 1100 0000 0111
T_7=0110 1010 0010 1100
T_8=0100 0011 1111 1011
T_9=1011 1110 0101 0111
T_{10}=1110 0110 1111 0100
T_{11}=0011 0100 0010 1011
T_{12}=0101 0011 1010 0010
T_{13}=0010 1101 0110 1111
T_{14}=1000 0101 1110 0011
T_{15}=1100 1100 1010 1100

$K(4)_1$ – қисм калитнинг мумкин бўлган қийматлари тўплами эса қуйидагича:

$$K(4)_1=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$$

Ушбу қисм калитнинг ҳақиқий қийматини аниқлаш учун, T_i шифрматнларнинг дастлабки барча $t_{i,1}$ – элементларини (4 бит) $K(4)_1$ калитнинг бирор тахминий "k" қиймати асосида қуйидаги формула ёрдамида бир раундга дешифрлаймиз:

$$R_i=InvSubNibbles(InvShiftRow(AddRoundKey(t_{i,1},k))),\ i=[0,15] \quad (2.7.2)$$

Алгоритм схемасига кўра, ушбу дешифрлаш натижаси 3-раунд чиқиши ва 4-раунд киришига тўғри келади. Юқорида аниқландики, 4-раунд киришида тўплам элементлари учун (2.7.1) тенглик бажарилади. Демак, ҳосил қилинган 16 та R_i қийматлар учун $\sum_{i=0}^{15} R_i = 0$ тенглик бажарилса, $K(4)_1$ калитнинг қиймати "k" га тенг бўлиши мумкин деб хулоса қиламиз, акс ҳолда "k" нотўғри қиймат бўлади.

Шунга кўра, қисм калитлар тўпламининг иккинчи қиймати, яъни $K(4)_1$=0001 учун ушбу бир раундга дешифрлаш жараёни қуйидаги 2.7.7-жадвалда келтирилган.

2.7.7-жадвал.

Шифрматнни 1 раундга дешифрлаш жараёни

$t_{i,1}$ – элементлар	4-раунд акслантиришлари			R_i
	AddRoundKey	**InvShiftRow**	**InvSubNibbles**	
1111	1110	1110	0000	R_0
0010	0011	0011	1000	R_1
1100	1101	1101	0010	R_2
1100	1101	1101	0010	R_3
1111	1110	1110	0000	R_4
1011	1010	1010	1001	R_5
1111	1110	1110	0000	R_6
0110	0111	0111	1111	R_7

2.7.7-жадвалнинг давоми

0100	0101	0101	1100	R_8
1011	1010	1010	1001	R_9
1110	1111	1111	0101	R_{10}
0011	0010	0010	0100	R_{11}
0101	0100	0100	0001	R_{12}
0010	0011	0011	1000	R_{13}
1000	1001	1001	1101	R_{14}
1100	1101	1101	0010	R_{15}
$\sum R_i$			**1100**	

Дешифрлаш натижасидан маълумки, ҳосил бўлган элементлар учун $\sum_{i=0}^{15} R_i = 1100 \neq 0000$ тенглик ўринли. Демак, $K(4)_1$ нинг қиймати “0001” эмаслиги аниқланди. Калит қийматларининг қолган вариантлари учун ҳам солиштирув жараёни шу тарзда давом этади. Шунга кўра, мумкин бўлган қисм калитлар тўпламидаги қолган барча қийматлар учун бажарилган дешифрлаш натижалари ва ҳосил бўлган элементлар йиғиндиси 2.7.8-жадвалда келтирилган.

2.7.8-жадвал.

$K(4)_1$ – қисм калитни аниқлаш жараёни

$t_{i,1}$	**Мумкин бўлган қисм калитлар тўплами**															
	0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
	InvSubNibbles(InvShiftRow(KeyAddition($t_{i,1}$,k_j)))															
1111	0101	0000	0010	1011	0110	1001	1101	0111	1111	1010	1100	0001	1000	0100	0011	1110
0010	0100	1000	1110	0011	1010	1111	0001	1100	1001	0110	0111	1101	0000	0101	1011	0010
1100	1011	0010	0000	0101	0111	1101	1001	0110	0001	1100	1010	1111	1110	0011	0100	1000
1100	1011	0010	0000	0101	0111	1101	1001	0110	0001	1100	1010	1111	1110	0011	0100	1000
1111	0101	0000	0010	1011	0110	1001	1101	0111	1111	1010	1100	0001	1000	0100	0011	1110
1011	0110	1001	1101	0111	0101	0000	0010	1011	1000	0100	0011	1110	1111	1010	1100	0001
1111	0101	0000	0010	1011	0110	1001	1101	0111	1111	1010	1100	0001	1000	0100	0011	1110
0110	1010	1111	0001	1100	0100	1000	1110	0011	0000	0101	1011	0010	1001	0110	0111	1101
0100	0001	1100	1010	1111	1110	0011	0100	1000	1011	0010	0000	0101	0111	1101	1001	0110
1011	0110	1001	1101	0111	0101	0000	0010	1011	1000	0100	0011	1110	1111	1010	1100	0001
1110	0000	0101	1011	0010	1001	0110	0111	1101	1010	1111	0001	1100	0100	1000	1110	0011
0011	1000	0100	0011	1110	1111	1010	1100	0001	0110	1001	1101	0111	0101	0000	0010	1011
0101	1100	0001	1111	1010	0011	1110	1000	0100	0010	1011	0101	0000	1101	0111	0110	1001
0010	0100	1000	1110	0011	1010	1111	0001	1100	1001	0110	0111	1101	0000	0101	1011	0010
1000	0111	1101	1001	0110	1011	0010	0000	0101	1110	0011	0100	1000	0001	1100	1010	1111
1100	1011	0010	0000	0101	0111	1101	1001	0110	0001	1100	1010	1111	1110	0011	0100	1000
$\sum R_i$	**0110**	**1100**	**0111**	**1101**	**0101**	**1111**	**1101**	**0111**	**0101**	**1111**	**0000**	**1010**	**0101**	**1111**	**1001**	**0011**

Мазкур статистика жадвалига кўра, қисм калитнинг “1010” қийматида ҳосил бўлган элементлар учун $\sum_{i=0}^{15} R_i = 0000$ тенглик бажарилганлиги боис, изланаётган калит қиймати $K(4)_1$=1010 эканлиги аниқланди. Қолган қисм калитларни ҳам айнан ушбу статистика жадвалини тузиш орқали аниқлаш мумкин. **Демак**, ИК усули орқали S_AES шифрлаш алгоритми сўнгги раундида

фойдаланилган 16 битли калит қийматини аниқлаш $2^4{*}4=2^6$ та перебор амалини (дешифрлаш амалини) талаб этади.

Келтирилган намунадан маълумки, умумий ҳолда, бирор алгоритмнинг сўнгги раундида фойдаланилган n – битли калит қийматини бир раундга дешифрлаш орқали аниқлаш $2^E \cdot \frac{n}{E}$ (E – S-блок ўлчами) та перебор амалини талаб этиб, тўлиқ перебор (2^n та) сонидан етарлича кичик бўлади. Статистиканинг умумий дешифрлашлар сони эса $2^E \cdot \frac{n}{E} \cdot |C|$ ($|C|$ – шифр матн блоклари сони) тани ташкил этади.

Бир раундга дешифрлаш орқали калитни аниқлаш, қачонки сўнгги раунд киришида баланслашган тўплам ҳосил бўлгандагина мумкин. Агар мазкур ҳолат кузатилмаса, дешифрлаш раундлар сонини ошириш орқали ҳам калит қийматини аниқлаш мумкин. Масалан, 6 раундли бирор шифрлаш алгоритм учун 6-раунд киришида баланслашган тўплам ҳосил бўлишини таъминловчи кирувчи A – тўплам мавжуд эмас. Бироқ 5-раунд киришида баланслашган тўплам ҳосил бўлишини таъминловчи кирувчи тўплам мавжуд. Шунга кўра, 5-раунд кириши учун (2.7.1) тенгликни бажарилишини билган ҳолда, шифр матн тўпламини 2 раундга дешифрлаш орқали 5 ва 6-раунд калитларини аниқлаш мумкин. Ушбу ҳолда 2 раундга дешифрлаш учун талаб этилувчи вариантлар сони тўлиқ вариантлар сонидан кам бўлиши талаб этилади, акс ҳолда криптотаҳлил самарадорликка эга бўлмайди.

ИК жараёнида калитни аниқлашга қаратилган статистика натижасида ҳақиқий калит сифатида бир нечта қийматлар ҳосил бўлиши ҳам мумкин. Ушбу ҳолда танланган тўплам шартини қаноатлантирувчи бошқа матнлар тўплами устида ҳам статистика ўтказилади ва барча статистика натижаларини умумлаштирган ҳолда калитнинг ягона қиймати аниқланади.

Таъкидлаш лозимки, криптотаҳлил учун керак бўлган тўплам тузилиши (яъни нечта актив ёки пассив элементлардан ташкил топиши ва уларнинг жойлашиш ўрни) ҳамда уни ташкил этувчи матн блоклари сони таҳлил қилинаётган шифрлаш алгоритми тузилишига (акслантиришларига) ва раундлар сонига боғлиқ бўлади.

Криптотаҳлил жараёнида дастлабки масала, керакли раунд киришида баланслашганликни таъминловчи тўплам тузилишини аниқлашдир. Агар бирор шифрлаш алгоритми учун бўлиши мумкин бўлган оптимал тўпламнинг баланслашганлик хусусияти сақланувчи энг юқори раунд қиймати r_1 га тенг бўлса, ҳамда тўлиқ вариантдан кам амал талаб этувчи энг кўп дешифрлаш раундлари сони r_2 та бўлса, у ҳолда, r_1+r_2 та раунд учун ИК усулини қўллаш мумкин бўлади. Масалан, блок узунлиги 128 битга тенг бўлган AES шифрлаш алгоритми учун баланслашганлик сақланувчи энг юқори раунд 5-раунд чиқишида кузатилиб, уни таъминловчи оптимал тўплам тузилиши қуйидагича [63]:

$$P = p_1p_2p_3,..., p_{16} = A_1ППA_2A_3A_4ПППA_5A_6ПППA_7A_8.$$

Бу ерда, $П$ ($\Pi \in 2^8$) – пассив элементлар, ҳамда A_i ($A_i \in 2^8$) – актив элементнинг ташкил этувчилари бўлиб, $A=A_1||A_2||A_3||A_4||A_5||A_6||A_7||A_8$ ($A \in 2^{64}$) – актив элемент ҳисобланади. Тўлиқ перебордан кам амал талаб этувчи энг кўп дешифрлаш раундлари сони эса 2 та бўлиб, умумий ҳолда 7 раундли AES шифрлаш алгоритмига ИК усулини қўллаб 6 ва 7-раунд калитларини аниқлаш учун 2^{64} та адаптив танланган очиқ матн ва унга мос шифр матн ҳамда 2^{44} та танлов талаб этилади.

Умумий ҳолда ИК усулини қўллаш учун қуйидаги икки масала ҳал қилиниши талаб этилади:

1. **Оптимал очиқ матнлар тўплами тузилишини аниқлаш** (тўпламнинг шифрлаш алгоритми раундларидан ўтиш хусусиятига боғлиқ ҳолда).
2. **Сўнгги раундда фойдаланилган калит қийматини аниқлаш** (статистика ўтказиш орқали).

Шунга кўра, раундлар сони – n (n>1) та ва блок узунлиги m – бит бўлган мавжуд ёки янги таклиф этилган блокли симметрик шифрлаш алгоритмини интеграл криптотаҳлил усулига бардошлилигини баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.7.9-жадвал.
Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Бўлиши мумкин бўлган энг юқори (катта) r_1-раунд киришида балансланшганлик хусусияти сақланувчи оптимал тўплам – A нинг тузилишини аниқлаш	$r_1=1$ ёки $r_1=\varnothing$	Алгоритм ИК усулига назарий бардошли
		$r_1>1$	Кейинги босқичга ўтиш мумкин
II.	A – оптимал тўплам тузилишига боғлиқ ҳолда статистика учун лозим бўлган энг кам матнлар сони – W ни аниқлаш	$W>2^m$ (ёки W та матнни сақлаш учун ҳотира ҳажми амалий мавжуд эмас)	Алгоритм ИК усулига назарий (ёки амалий) бардошли
		$W\leq 2^m$ ва W та матнни сақлаш учун ҳотира ҳажми амалий мавжуд	Кейинги босқичга ўтиш мумкин
III.	Дешифрлаш орқали сўнгги r_2 та раунднинг бирор қисм калитини аниқлаш учун талаб этилувчи энг кам амаллар сони – N ни аниқлаш ($r_2=n-r_1+1$)	Реал вақт мобайнида N та амални бажаришнинг амалий имкони йўқ	Алгоритм ИК усулига амалий бардошли
		Реал вақт мобайнида N та амални бажариш амалий мумкин	Кейинги босқичга ўтиш мумкин
IV.	Статистика ўтказиш орқали бирор $K(n)$, $K(n-1)$, $K(n-2)$,..., $K(n-r_2-1)$ – қисм калитлар қийматини аниқлаш	Қисм калитлар аниқланмади	Алгоритм ИК усулига амалий бардошли
		Қисм калитлар аниқланди	Алгоритм ИК усулига бардошсиз

Назорат саволлари

1. Интеграл криптотаҳлил усули асосий моҳияти нимадан иборат?

2. Интеграл криптотаҳлил усулини қўллашда очиқ матнларни танлаш қандай мезон асосида амалга оширилади?

3. Ихтиёрий танланган очиқ матн ва унга мос шифр матн асосида интеграл криптотаҳлил усулини қўллаш мумкинми?

4. Интеграл криптотаҳлил усулининг самарадорлик даражаси нималарга боғлиқ?

5. AES шифрлаш алгоритмини интеграл криптотаҳлил усулига бардошлигини таминлашда шифрлаш алгоритмида фойдаланилган акслантиришлар ўрнини изоҳланг.

6. AES шифрлаш алгоритмини интеграл криптотаҳлил усулига бардошлигини таминлашда шифрлаш алгоритмида фойдаланилган раунд калитини қўшиш амалининг қандай ўрни бор?

7. Интеграл криптотаҳлил усули орқали AES алгоритми сўнгги раундида фойдаланилган калитни аниқлашдаги танлашлар сони нималарга боғлиқ?

8. Блок узунлиги турлича (128, 196, 256 бит) бўлган AES алгоритмига интеграл криптотаҳлил усулини қўллашнинг қандай ўхшаш ва фарқли жиҳатлари мавжуд?

9. Интеграл криптотаҳлил усулини қўллашда параллел ҳисоблаш жараёнининг қандай таъсири мавжуд?

10. Интеграл криптотаҳлил усулини мавжуд статистик криптотаҳлил усулларидан (Дифференциал, Чизиқли ва бошқа) афзал ва камчилик жиҳатлари нималардан иборат?

11. Интеграл криптотаҳлил усули орқали калитни аниқлашдаги танлашлар сонини кескин ошириш учун шифрлаш алгоритмида қандай турдаги акслантиришлардан фойдаланиш мақсадга мувофиқ?

12. SP тармоғига асосланган блокли симметрик шифрлаш алгоритмининг интеграл криптотаҳлил усулига бардошлилигини таъминловчи умумий криптографик талаблар нималардан иборат?

13. Фейстельь тармоғига асосланган блокли симметрик шифрлаш алгоритмларига интеграл криптотаҳлил усулини қўллаш мумкинми?

14. Интеграл криптотаҳлил усулини янада такомиллаштириш мумкинми?

2.8. Аппарат хатоликларини генерациялашга асосланган криптотаҳлил усули

Айни вақтда стандарт шифрлаш алгоритмлари муҳим камчиликларидан бири уларнинг реал техник криптотаҳлил усулларига нисбатан бардошсиз эканлигини кўрсатмоқда, хусусан, “аппарат хатоликларини генерациялашга асосланган криптотаҳлил” усулларига. Бу усулнинг моҳияти, алгоритм акслантиришларининг маълум жойларидаги айрим битларини ўзгартиришга эришиш мақсадида, ҳимоя аппаратига иссиқлик, юқори частотали, ионизациялаш ва бошқа ташқи таъсир усулларидан фойдаланган ҳолда таъсир этишдир. Бундай ўзгартириш киритишга асосланган таҳлил усули маълумотни ўзгартириш киритилгунга қадар ва ўзгартирилганидан сўнг эга бўлган маълумотларини солиштириш орқали охирги раунд калити ва кейинчалик барча раунд калитлари тўғрисида қийматлар топишга қаратилган.

Аппарат хатоликларини генерациялаш таҳлил усулининг базавий элементларига мувофиқ, шифрларнинг бу турдаги ҳужумга нисбатан бардошлилиги, уларнинг охирги раунд калитлари K_R ни тўлиқ кўриб чиқиш (тотал перебор) мураккаблигига тенг кучли эканлигини кўриш мумкин.

Ҳақиқатан ҳам, Фейстель тармоғига асосланган блокли шифрлаш алгоритмлари охирги раунд калитлари қуйидагича аниқланади:

1. $X_R=X_R\oplus F(X_L,K_R)$ – хатосиз кўриниши.
2. $X'_R=X_R\oplus F(X'_L,K_R)$ – генерация қилинган хатолик билан кўриниши.

Бу ерда,

X_R – маълумотнинг хатосиз ўнг блоки;
X_L – маълумотнинг хатосиз чап блоки;
X'_R – маълумотнинг хатоли ўнг блоки;
X'_L – маълумотнинг хатоли чап блоки;
K_R – раунд калити;
$\oplus$ - XOR (модуль 2 бўйича қўшиши амали).

Икки тенгламани қўшиб қуйидаги тенгламага эга бўламиз:

$$X_R\oplus X'_R = F(X_L,K_R) \oplus F(X'_L,K_R).$$

Таъкидлаш жоизки, бу каби тенгламалар системасини бир нечта турли хил очиқ ва ёпиқ матнларга нисбатан қуриш мумкин. *F* функциянинг кўринишига боғлиқ бўлмаган ҳолда тенгламалар системаси ягона ечимини топиш раунд калитлари K_R ни топишни тўлиқ кўриб чиқиш усулига тенг кучли. Раунд калитлари K_R ни тўлиқ кўриб чиқиш усули билан топишнинг энг юқори қиймати қуйидаги кўринишга эга:

$M_{K(r)} = 2^m h M_F$, бу ерда h – системадаги тенгламалар сони, M_F – раунд алмаштиришларининг ҳисоблаш мураккаблигининг қиймати, m – калит узунлиги.

Худди шу тартибда кейинги раунд калитларини топиш қийматининг катталигини ҳам ҳисоблаш мумкин. Барча r раундли калитлар жадвалини топишнинг энг юқори қиймати қуйидагига тенг: $M=2^m h M_F r$. Шундай қилиб, Фейстель схемасига асосланган ихтиёрий блокли шифрни очиш қийинчилиги, битта раунд калитини топиш қийинчилигига (2^m) пропорционалдир.

ГОСТ 28147-89 алгоритмида 2^{32} модул бўйича қўшиш амалининг ишлатилганлиги, S-блок ўлчами кичиклиги ва орқага бир қийматли қайтиши, S-блок акслантиришлари маълум ва аппарат хатоликларини генерациялаш имконияти мавжуд бўлганда, мазкур ҳужумга нисбатан бардошсиз эканлигини кўрсатмоқда.

Мазкур аппарат хатоликларини генерациялашга асосланган криптотаҳлил ўтказиш қадамлар кетма-кетлигини тушунтириш соддароқ бўлиши учун, **ГОСТ 28147-89 шифрлаш алгоритми ўқув варианти мисолида кўриб ўтилади.**

ГОСТ 28147-89 ўқув шифрлаш алгоритми блоки узунлиги 16 бит. Махфий калит ($K=K_0, K_1, K_2, K_3$) узунлиги 32 бит бўлиб, шифрлаш раундлари сони 16 га, раунд калити узунлиги 8 бит ва S-блоклар сони 2 та.

Шифрлаш жараёнида кириш блоки чап қисми (R_0)га дастлаб (K_0) калит 2^8 модул бўйича қўшилиб, йиғинди кичик тўрт битликларга ажратилган ҳолда S_1 ва S_2 алмаштиришлардан ўтганидан сўнг катта разрядлар томонга 3 бит циклик равишда сурилади ва натижага L_0 блок 2 модул бўйича қўшилади (2.8.1-расм).

2.8.1-жадвал.

Раундлар қисм калитларининг ишлатилиш тартиби

Раундлар	**Ишлатилиш тартиби**
1-4 раунд	K_0, K_1, K_2, K_3
4-8 раунд	K_0, K_1, K_2, K_3
8-12 раунд	K_0, K_1, K_2, K_3
12-16 раунд	K_3, K_2, K_1, K_0

2.8.2-жадвал.

S_1 – блок

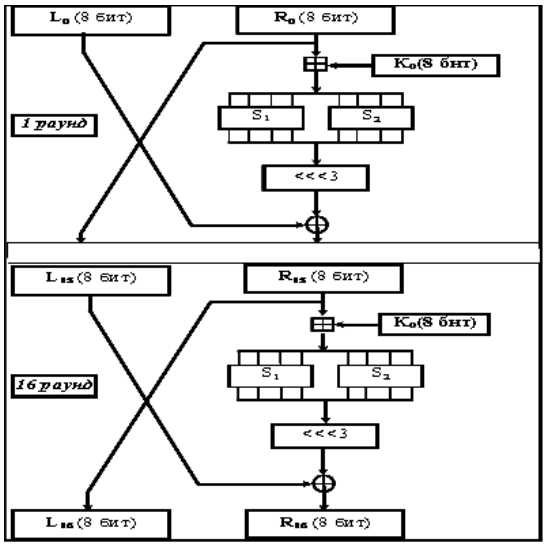
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9

2.8.3-жадвал.

S_2 – блок

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11

ГОСТ 28147-89 ўқув шифрлаш алгоритми учун аппарат хатоликларини генерациялашга асосланган таҳлил, алмаштириш охирги раундида фойдаланилган қисм калит *(K_0)*ни топиш, кейин эса босқичма-босқич равишда аввалги раундларга қайтиб калитнинг қолган *(K_1, K_2, K_3)* элементларини ҳам топишга қаратилган.



2.8.1-расм. ГОСТ 28147-89 – ўқув алгоритми схемаси

Кириш блоки *i*-қадамида бажарилган алмаштиришдан сўнг чиққан қийматларини чап (катта) ва ўнг (кичик) разрядларини мос равишда L_i ва R_i деб белгилаб оламиз. У ҳолда, алгоритмга асосан қуйидагиларга эга бўлинади:

$$R_{16} = R_{15}; \qquad (2.8.1)$$

$$L_{16} = f(R_{15} \boxplus K_0) \oplus L_{15}, \qquad (2.8.2)$$

бу ерда $\boxplus$ – 2^8 модул бўйича қўшиш амали, $\oplus$ – XOR (2 модул бўйича қўшиш амали);

$f()$ – $R_{16} \boxplus K_0$ йиғиндини 4 битли блокларга ажратиб уларни S-блок жадвалидан ўтказиб, натижани циклик равишда 3 бит чапга (катта разрядлар томонга) сурувчи функция.

Шифрлаш қурилмаси киришига ихтиёрий 16 битли блок берилиб, чиқишида эса иккита 8 битли (L_{16}, R_{16}) қийматларга эга бўлинади. Шифрлаш жараёнида R_{15} блокнинг кичик 4 битларида хатоликларни генерациялаш мақсадида техник қурилмага ташқи таъсир кўрсатилади. Бу ҳолда юқоридаги тенглама чап қисми кўриниши қуйидагича бўлади:

$$L`_{16} = f(R`_{15} \boxplus K_0) \oplus L_{15} \qquad (2.8.3)$$

бу ерда, $R`_{15}$, R_{15} блокдан кичик разрядларидан бирига фарқ қилади.

(2.8.2 ва 2.8.3) тенгламаларни модул 2 бўйича қўшиб қуйидагига ҳосил қилинади.

$$L_{16} \oplus L`_{16} = f(R_{15} \boxplus K_0) \oplus f(R`_{15} \boxplus K_0) \qquad (2.8.4)$$

ёки (2.8.1) тенгликни эътиборга олиб,

$$L_{16} \oplus L`_{16} = f(R_{16} \boxplus K_0) \oplus f(R`_{16} \boxplus K_0). \qquad (2.8.5)$$

Хатоликни R_{15} блокнинг қолган учта разрядларида ҳам амалга ошириб, яна учта тенгламага эга бўлиш мумкин. Дастлабки кириш R_{15} блокига бошқа қийматлар бериб яна ҳудди шундай тўртта тенгламалар системасига ҳам эга бўлинади.

Шундай қилиб, кириш блокига турлича қийматлар бериб, R_{15} нинг барча мумкин бўлган 16 та қийматига эришиш мумкин. Ҳар бир кириш блокига нисбатан тўртта ҳатоликни амалга ошириш орқали жами 4*16=64 та тенгламага эга бўлинади [11].

Аммо осонгина аниқлаш мумкинки барча тенгламалар боғлиқли бўлиб, тенгламалар системасини қуйидагича кўринишга келтириш мумкин бўлади [21].

$$\begin{cases} f(K_0) \oplus f(K_0 \boxplus 1) = A_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f(K_0) \oplus f(K_0 \boxplus 16) = A_{16} \end{cases} \qquad (2.8.6)$$

бу ерда, A_i коэффициентлар (2.8.5) кўринишидаги тенгламаларнинг чап томонларининг модул 2 бўйича йиғиндиси [11, 21].

(2.8.5) тенглама кўринишини қуйидагича алмаштириш мумкин:

$$g2(L_{16} \oplus L`_{16}) = h2(R_{16} \boxplus K_0) \oplus h2(R`_{16} \boxplus K_0) \qquad (2.8.7)$$

бу ерда, $g2$ – функция, $L_{16} \oplus L`_{16}$ йиғиндининг кичик тўрт битларини 3 бит циклик равишда ўнг (кичик разрядлар) томонга сурувчи функция.

$h2$ – функция эса, кичик тўрт биларни $S(2)$ блок бўйича алмаштирувчи функция.

K_0 калит кичик тўрт битлари қабул қилиши мумкин бўлган барча 16 та вариантини (2.8.7) тенгламага қўйиб чиқиш орқали, улар ичидан тенгламани қаноатлантирмаганларини ташлаб юбориб, тенгламани қаноатлантирганлари мумкин бўлган калит сифатида олиб қолинади [4, 11, 21].

Агар (2.8.7) тенгламадан K_0 калит кичик тўрт битларини топиш имкони бўлмаса, яъни тенгламани қаноатлантирадиган қисм калитлар топилмаса, у ҳолда, бошқа кириш блокини бериб мазкур амални давом эттириш ёки R_{15} нинг қолган учта кичик битлардан бирида хатоликни амалга ошириш мумкин.

Тажрибада кўриш мумкинки калит кичик тўрт битларини бир қийматли аниқлаш учун битта тенгламага эга бўлиш етарли ҳисобланади.

Қуйида мазкур криптотаҳлил усулининг ГОСТ 28147-89 ўқув алгоритмига қўлланиши бўйича намуна келтирилган.

Кирувчи қиймат: kl=6B 6C = 01101011 01101100

Калит: kkkk=6B 6B 6B 6B=01101011 01101011 01101011 01101101

L_0 =0110 1101, R_0=0110 1100

2.8.4-жадвал.

16 раундли ГОСТ 28147-89 ўқув алгоритмининг кириш қийматлари

Раундлар	Раундлардан чиқиш қийматлари	Чиқиш блокининг чап қисми (L_i)	Чиқиш блокининг ўнг қисми (R_i)
0	*6B6C=0110 1011 0110 1100*	L_0 *=0110 1101*	R_0*=0110 1100*
1	*6CBC=0110 1100 1011 1100*	L_1 *=0110 1100*	R_1*=1011 1100*
....	.....	.....	.....
15	*29DF=0010 1001 1101 1111*	L_{15}*=0010 1001*	R_{15}*=1101 1111*
16	*DFEF=1101 1111 1110 1111*	$L_{16}=R_{16}$*=1101 1111*	$R_{16}=L_{16}$*=1110 1111*

Такидлаш лозимки, 16 - раунд чиқишидаги қийматлар (2.8.1) ва (2.8.2) тенгламаларга асосан қуйидагича бўлади.

$$L_{16} = f(R_{15} \boxplus K_0) \oplus L_{15} = f(R_{16} \boxplus K_0) \oplus L_{15} \qquad (2.8.8)$$

$R_{16} = R_{15}$ *=DF=1101 1111;* L_{15}*=0010 1001;* k_0*=0110 1101*

$$L_{16} = f(R_{15} \boxplus K_0) \oplus L_{15} = f(R_{16} \boxplus K_0) \oplus L_{15}$$
$$= f(1101\ 1111 \boxplus 0110\ 1011) \oplus 0010\ 1001$$
$$= 1110\ 1111$$

Охирги раундда ишлатилган K_0 калитнинг кичик тўрт битларини топиш учун охирги раундга кирувчи $R_{16} = R_{15}$ *=DF=1101 1111* блокнинг охирги кичик тўрт битларида хатоликни генерациялашга эришилади. Мазкур мисол орқали хатоликни кичик тўрт битларида навбати билан амалга оширилган ҳолат учун кўриб чиқилади. Амалий жиҳатдан эса охирги раундда ишлатилган калит кичик тўрт битларини топиш учун $R_{16} = R_{15}$ *=DF=1101 1111* блок бирор битида хатоликни генерациялаш кифоя. Сўнгра ҳар хил кириш блокларини бериш орқали жами 16 та тенгламадан калит кичик тўрт битларини топиш мумкин [9, 11].

1. Хатоликка $R_{16} = R_{15}$ *=DF=1101 1111* кириш блоки энг кичик разрядида эришилди.

У ҳолда, $R`_{16} = R`_{15}$ *=DF=1101 1110* га тенг бўлади.

$$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} =$$
$$= f(1101\ 1110 \boxplus 0110\ 1011) \oplus 0010\ 1001 = 1011\ 0111$$

$R`_{16} \boxplus K_0$ =1101 1110$\boxplus$ 0110 1011=0100 1001

$S_1(0100)=1101$, $S_2(1001)=0011$ $S_1||S_2(1101\ 0011)$ |1001 1110 <<3

1001 1110 ⊕ 0010 1001=1011 0111

$A_1 = L_{16} \oplus L`_{16}$= 11101111 ⊕ 1011 0111 = 0101 1000 | 3 >> 0000 1011

$$f(R_{16} \boxplus K_0) \oplus f(R`_{16} \boxplus K_0) = L_{16} \oplus L`_{16} = A_1 \quad (2.8.9)$$

$$f(1101\ 1111 \boxplus k_4k_5k_6k_7) \oplus f(1101\ 1110 \boxplus k_4k_5k_6k_7) = 0000\ 1011 \quad (2.8.10)$$

Хатолик айнан кириш блоки энг кичик разрядида кузатилганлиги учун S_2 блокдан чиқишларни кузатиш кифоя. У ҳолда, юқоридаги тенгламани қуйидаги кўринишда ёзиш мумкин:

$$S_2(1111 \boxplus k_4k_5k_6k_7) \oplus S_2(1110 \boxplus k_4k_5k_6k_7) = 1011 \quad (2.8.11)$$

Бу ердан K_0 калит кичик битлари ($k_4k_5k_6k_7$) қабул қилиши мумкин бўлган барча 16 та қийматини (2.8.11) тенгламага олиб бориб қўйиб, тенгламани қаноатлантирганларини мумкин бўлган калит сифатида олинади.

2.8.5-жадвал.

2.8.11 тенгламанинг ечимлари жадвали

$k_4k_5k_6k_7$	$S_2(1111 \boxplus k_4k_5k_6k_7)$	$S_2(1110 \boxplus k_4k_5k_6k_7)$	$S_2(i) \oplus S_2(i+1)$	A_{11}=1011
0000	$S_2(15) = 1001$	$S_2(14) = 0101$	1001⊕0101 = 1100	1011
0001	$S_2(0) = 1110$	$S_2(15) = 1001$	1110⊕1001 = 0111	1011
0010	$S_2(1) = 1011$	$S_2(0) = 1110$	1011⊕1110 = 0101	1011
0011	$S_2(2) = 0100$	$S_2(1) = 1011$	0100⊕1011 = 1111	1011
0100	$S_2(3) = 1100$	$S_2(2) = 0100$	1100⊕0100 = 1000	1011
0101	$S_2(4) = 0110$	$S_2(3) = 1100$	0110⊕1100 = 1010	1011
0110	$S_2(5) = 1101$	$S_2(4) = 0110$	1101⊕0110 = 1011	1011
0111	$S_2(6) = 1111$	$S_2(5) = 1101$	1111⊕1101 = 0010	1011
1000	$S_2(7) = 1010$	$S_2(6) = 1111$	1010⊕1111 = 0101	1011
1001	$S_2(8) = 0010$	$S_2(7) = 1010$	0010⊕1010 = 1000	1011
1010	$S_2(9) = 0011$	$S_2(8) = 0010$	0011⊕0010 = 0001	1011
1011	$S_2(10) = 1000$	$S_2(9) = 0011$	1000⊕0011 = 1011	1011
1100	$S_2(11) = 0001$	$S_2(10) = 1000$	0001⊕1000 = 1001	1011
1101	$S_2(12) = 0000$	$S_2(11) = 0001$	0000⊕0001 = 0001	1011
1110	$S_2(13) = 0111$	$S_2(12) = 0000$	0111⊕0000 = 0111	1011
1111	$S_2(14) = 0101$	$S_2(13) = 0111$	0101⊕0111 = 0011	1011

(2.8.11) тенгламани қаноатлантирувчи мумкин бўлган калитлар, $k_4k_5k_6k_7$={0110,1011}

2. Хатоликка $R_{16} = R_{15}$ =*DF=11011111* кириш блокининг энг кичик разрядидан битта олдинги қийматида эришилган ҳолат учун.

У ҳолда, $R`_{16} = R`_{15}$ =*DF=1101 1101* га тенг бўлади.

$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} =$
$f(1101\ 1101 \boxplus 0110\ 1011) \oplus 0010\ 1001 = 1011\ 1111$

$R`_{16} \boxplus K_0$ =1101 1101⊞ 0110 1011=0100 1000

S_1 (0100)=1101, S_2 (1000)=0010, $S_1||S_2$(1101 0010), 1001 0110<<3

1001 0110 ⊕ 0010 1001=1011 1111

$A_2 = L_{16} \oplus L`_{16}$= 1110 1111 ⊕ 1011 1111 = 0101 0000 | 3 >>
0000 1010

$$f(R_{16} \boxplus K_0) \oplus f(R`_{16} \boxplus K_0) = L_{16} \oplus L`_{16} = A_2 \quad (2.8.12)$$

$$f(1101\ 1111 \boxplus k_4k_5k_6k_7) \oplus f(1101\ 1101 \boxplus k_4k_5k_6k_7) = 0000\ 1010 \quad (2.8.13)$$

Бу ерда ҳам, хатолик айнан кириш блоки кичик разрядида кузатилганлиги учун S_2 блокдан чиқишларни кузатиш кифоя. У ҳолда, юқоридаги тенгламани қуйидаги кўринишда ёзиш мумкин:

$$S_2(1111 \boxplus k_4k_5k_6k_7) \oplus S_2(1101 \boxplus k_4k_5k_6k_7) = 1010 \quad (2.8.14)$$

(2.8.14) тенгламага кўра K_0 калитнинг кичик битлари $k_4k_5k_6k_7$={0011, 1011} га тенг.

3. Хатоликка $R_{16} = R_{15}$ =*DF=1101 1111* кириш блокининг энг кичик разрядидан иккита олдинги қийматида эришилган ҳолат учун.

У ҳолда, $R`_{16} = R`_{15}$ =*DF=1101 1011* га тенг бўлади.

$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} =$
$f(1101\ 1011 \boxplus 0110\ 1011) \oplus 0010\ 1001 = 1101\ 0111$

$R`_{16} \boxplus K_0$ =1101 1011⊞ 0110 1011=0100 0110

S_1 (0100)=1101,S_2 (0110)=1111, $S_1||\ S_2$ (1101 1111),<<3 1111 1110

1111 1110 ⊕ 0010 1001=1101 0111

$A_3 = L_{16} \oplus L`_{16}$= 1110 1111 ⊕ 1101 0111 = 0011 1000 | 3>>
0000 0111

$$f(R_{16} \boxplus K_0) \oplus f(R`_{16} \boxplus K_0) = L_{16} \oplus L`_{16} = A_3 \quad (2.8.15)$$

$$f(1101\ 1111 \boxplus k_4k_5k_6k_7) \oplus f(1101\ 1011 \boxplus k_4k_5k_6k_7) = = 0000\ 0111$$

Олдинги қийматлар каби, бу ерда ҳам юқоридаги тенгламани кўринишини қуйидагича келтириш мумкин:

$$S_2(1111 \boxplus k_4k_5k_6k_7) \oplus S_2(1011 \boxplus k_4k_5k_6k_7) = 0111 \qquad (2.8.16)$$

(2.8.16) тенгламага кўра K_0 калитнинг кичик битлари $k_4k_5k_6k_7$={1011} га тенг бўлади.

4. Хатоликка $R_{16} = R_{15}$ =*DF=1101 1111* кириш блокининг энг кичик разрядидан учта олдинги қийматида эришилган ҳолат учун.

У ҳолда, $R`_{16} = R`_{15}$ =*DF=1101 0111* га тенг бўлади.

$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} =$
$f(1101\ 0111 \boxplus 0110\ 1011) \oplus 0010\ 1001 = 1000\ 1111$

$R`_{16} \boxplus K_0$ =1101 0111⊞ 0110 1011=0100 0010

$S_1(0100)=1101, S_2(0010)=0100, S_1||S_2(1101\ 0100)$ | <<3 1010 0110

1010 0110 ⊕ 0010 1001=1000 1111

$A_3 = L_{16} \oplus L`_{16}$= 1110 1111 ⊕ 1000 1111 = 0110 0000 | 3 >> 0000 1100

$$f(R_{16} \boxplus K_0) \oplus f(R`_{16} \boxplus K_0) = L_{16} \oplus L`_{16} = A_4 \qquad (2.8.17)$$

$$f(1101\ 1111 \boxplus k_4k_5k_6k_7) \oplus f(1101\ 0111 \boxplus k_4k_5k_6k_7) = 0000\ 1100 \qquad (2.8.18)$$

Хатолик айнан кириш блокининг кичик разрядида кузатилганлиги учун S_2 блокдан чиқишларни кузатиш кифоя. У ҳолда, (2.8.18) тенглама қуйидаги ифодага ўзгаради:

$$S_2(1111 \boxplus k_4k_5k_6k_7) \oplus S_2(0111 \boxplus k_4k_5k_6k_7) = 1100 \qquad (2.8.19)$$

Бу тенгламадан K_0 калитнинг кичик битлари $k_4k_5k_6k_7$={0001,0011, 1001, 1011} га тенг бўлади.

Умумий ҳолда мумкин бўлган калитлар тўплами қуйидагича бўлди:

1. $k_4k_5k_6k_7$={0110, 1011}
2. $k_4k_5k_6k_7$={0011, 1011}
3. $k_4k_5k_6k_7$={1011}
4. $k_4k_5k_6k_7$={0001,0011, 1001, 1011}

Мумкин бўлган калитларнинг қийматлар тўпламидан кесишмада турган $k_4k_5k_6k_7$=1011 қиймат K_0 калитнинг кичик битлари

эканлигини топиш мумкин. Ҳақиқатдан ҳам очиқ матнни шифрлашни амалга оширишда калитнинг қийматини K_0=*6B*= $k_0k_1k_2k_3\ k_4k_5k_6k_7$=*0110 1011* деб белгилаб олинган эди.

Демак, K_0 калитнинг кичик битлари тўғри топилган.

Раундларда ишлатилган қисм калитлар кейинги битларини топиш.

Энди, охирги раундда ишлатилган K_0 калит дастлабки битлари ($k_0k_1k_2k_3$) ни топишда ҳам, юқорида таклиф этилган усулдан фойдаланиш мумкин.

Фақат калит қолган $k_0k_1k_2k_3$ битларини топишда 16-раундга кирувчи $R_{15,4}$ блок кичик тўрт битларига $K_{0,4}$ калитнинг кичик тўрт битлари қўшилганда, битларнинг ўзидан олдинги битларга таъсир этиши ҳолати кузатилиши мумкин [6, 11, 21].

Шунинг учун K_0 калитнинг дастлабки битлари ($k_0k_1k_2k_3$) ни топишда айнан битларнинг кўчиш ҳолатини эътиборга олиш керак бўлади.

16-раундга кирувчи $R_{15,4}$ блок кичик тўрт битларига $K_{0,4}$ калитнинг кичик тўрт битлари қўшилганда, битларнинг ўзидан олдинги битларга таъсир этиши ҳолати охирги икки кичик битларнинг йиғиндиси 16 дан катта ёки тенг бўлгандагина кузатилади, яъни $R_{15,4} \boxplus K_{0,4} \geq 16$ [11, 21].

Бунинг учун тенгламалар системасини тузишда махсус кириш блокларидан фойдаланиш шарт эмас. Таъкидлаш лозимки, битларнинг кўчиш ҳолати ўзидан олдинги кичик тўрт битларга фақатгина 1 бит йиғиндиси кўринишида таъсир этади [21].

Бу фактни тенгламалар системасини тузишда эътиборга олиб қуйидагича:

$$\begin{cases} f\left(R_{16}^{(13)} \boxplus K_0 \boxplus r\right) \oplus f(R_{16} \boxplus K_0 \boxplus r) = L_{16}^{(13)} \oplus L_{16} \\ f\left(R_{16}^{(14)} \boxplus K_0 \boxplus r\right) \oplus f(R_{16} \boxplus K_0 \boxplus r) = L_{16}^{(14)} \oplus L_{16} \\ f\left(R_{16}^{(15)} \boxplus K_0 \boxplus r\right) \oplus f(R_{16} \boxplus K_0 \boxplus r) = L_{16}^{(15)} \oplus L_{16} \\ f\left(R_{16}^{(16)} \boxplus K_0 \boxplus r\right) \oplus f(R_{16} \boxplus K_0 \boxplus r) = L_{16}^{(16)} \oplus L_{16} \end{cases} \quad (2.8.20)$$

бу ерда,

$$r = \begin{cases} 1, & R_{15,4} \boxplus K_{0,4} \geq 16 \\ 0, & R_{15,4} \boxplus K_{0,4} < 16 \end{cases} \quad (2.8.21)$$

тенгламалар системасидан фойдаланиб K_0 калитнинг дастлабки битлари ($k_0k_1k_2k_3$) ни топиш мумкин.

Шифрлаш қурилмаси киришига ихтиёрий 16 битли блок бериб, чиқишда эса иккита 8 битли (L_{16}, R_{16}) қийматларга эга бўлинади. Шифрлаш жараёнида хатоликларни генерациялаш мақсадида қурилмага ташқи таъсир кўрсатилиб, хатолик R_{15} блокнинг дастлабки битларида амалга ошишига эришилади [9, 11].

У ҳолда, (2.8.1) ва (2.8.2) тенглама чап қисми кўриниши қуйидагича бўлади:

$$L`_{16} = f(R`_{15} \boxplus K_0) \oplus L_{15}, \qquad (2.8.22)$$

бу ерда, $R`_{15}$ блок R_{15} блокдан фақатгина ката разрядларидан бирига фарқ қилади. (2.8.2) ва (2.8.3) тенгламаларни бирлаштириб модул 2 бўйича қўшилади. Тенгламалар системасини тузишда битларнинг кўчиш ҳолати кузатилиши мумкинлигини ҳисобга олиб ($R_{15,4} \boxplus K_{0,4} \geq 16$) уни қуйидагича кўринишда тасвирлаш мумкин:

$$L_{16} \oplus L`_{16} = f(R_{15} \boxplus K_0 \boxplus r) \oplus f(R`_{15} \boxplus K_0 \boxplus r) \qquad (2.8.23)$$

ёки (2.8.1) тенгликни этиборга олиб,

$$L_{16} \oplus L`_{16} = f(R_{16} \boxplus K_0 \boxplus r) \oplus f(R`_{16} \boxplus K_0 \boxplus r). \qquad (2.8.24)$$

Юқорида таъкидлаганидек, бу ерда ҳам жами 64 та тенгламага эга бўлиш мумкин. (2.8.24) тенгламанинг кўринишини қуйидагича алмаштирилади.

$$g1(L_{16} \oplus L`_{16}) = h1(R_{16} \boxplus K_0 \boxplus r) \oplus h1(R`_{16} \boxplus K_0 \boxplus r) \qquad (2.8.25)$$

бу ерда, $g1$ – функция, $L_{16} \oplus L`_{16}$ йиғинди битларини 3 бит циклик равишда ўнг (кичик разрядлар) томонга сурувчи функция;

$h1$ – функция эса, дастлабки битларни $S(1)$ блок бўйича алмаштирувчи функция.

K_0 калитнинг дастлабки битлари қабул қилиши мумкин бўлган барча 16 та вариантини (2.8.25) тенгламага қўйиб чиқиш орқали, улар ичидан тенгламани қаноатлантирмаганларини ташлаб юборилиб, тенгламани қаноатлантирганлари мумкин бўлган калит сифатида олиб қолинади [4, 11, 21].

Агар (2.8.25) тенгламадан K_0 калитнинг тўрт битларининг топишнинг имкони бўлмаса, яъни тенгламани қаноатлантирадиган

қисм калитлар топилмаса, у ҳолда, бошқа кириш блокини бериб, мазкур амални давом эттириб ёки R_{15} нинг қолган учта битларида бирида хатоликни амалга оширишга уриниб кўрилади [5].

I. K_0 калит дастлабки битлари ($k_0k_1k_2k_3$)ни топишда, дастлаб 16-раундга кирувчи $R_{15,4}$ блок кичик тўрт битларига $K_{0,4}$ калит кичик тўрт битлари қўшилганда, битларнинг кўчиш бўлмаган ($R_{15,4} \boxplus K_{0,4} < 16$) ҳолати кўриб чиқилади. Бунда ($k_0k_1k_2k_3$) ни топишни юқорида айтилганидек ($k_4k_5k_6k_7$)ни топиш каби амалга оширилади.

Фикр тўғрилигини қуйидаги мисол ёрдамида текшириб кўрамиз:

Кирувчи қиймат: 11=31 31 = 00110001 00110001

Калит: kkkk=6B 6B 6B 6B=01101011 01101011 01101011 01101101

L_0 *=0011 0001* R_0*=0011 0001*

2.8.9-жадвал.

16 раундли ўқув алгоритмида битларни кўчишини кузатиш

Раундлар	Раундлардан чиқиш қийматлари *(L_i, R_i)*	*($R_i \boxplus K_0$)*	*Кўчиш*
0	*31 31=00110001 00110001*	*31⊞ 6B*	-
1	*31 B4=00110001 10110100*	*B4⊞ 6B*	+
2	*B4 7C=10110100 01111100*	*7C⊞ 6B*	+
3	*7C 66=01111100 01100110*	*66⊞ 6B*	+
4	*66 A3=01100110 10100011*	*A3⊞ 6B*	-
5	*A3 4C=10100011 01001100*	*4C⊞ 6B*	+
6	*4C F5=01001100 11110101*	*F5⊞ 6B*	+
7	*F5 3C=11110101 00111100*	*3C⊞ 6B*	+
8	*3C 25=00111100 00100101*	*25⊞ 6B*	+
9	*25 C9=00100101 11001001*	*C9⊞ 6B*	+
10	*C9 14=11001001 00010100*	*14⊞ 6B*	-
11	*14 86=00010100 10000110*	*86⊞ 6B*	+
12	*86 CD=10000110 11001101*	*CD⊞6B*	+
13	*CD 97=11001101 10010111*	*97⊞ 6B*	+
14	*97 EF=10010111 11111110*	*EF⊞6B*	+
15	*EF D3=11111110 11010011*	*D3⊞6B*	-
16	*D3 C6=11010011 11000110*		-

Охирги раундда ишлатилган K_0 калитнинг дастлабки битлари ($k_0k_1k_2k_3$) ни топиш учун охирги раундга кирувчи $R_{16} = R_{15}$ *=D3=1101 0011* блокнинг дастлабки битларида

хатоликни генерациялашга эришилади. Биз бу мисол орқали хатоликни дастлабки битларда навбати билан амалга оширилган ҳолат учун кўриб чиқилади [4].

1. Хатоликка $R_{16} = R_{15}$ =*D3=1101 0011* кириш блокининг катта разрядининг охирги битида эришилди.

У ҳолда, $R`_{16} = R`_{15}$ =*C3=1100 0011* га тенг. $L_{16} = C6$; $L_{15} = EF$;

$$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} = f(C3 \boxplus 6B) \oplus EF = 43$$

$$A_1 = L_{16} \oplus L`_{16} = \text{C6} \oplus 43 = 85 = 10000101 \mid 3 >> \underline{1011\ 0000}$$

$$L_{16} \oplus L`_{16} =$$

$f(R_{16} \boxplus K_0 \boxplus r) \oplus f(R`_{16} \boxplus K_0 \boxplus r)$ (2.8.20) тенгламадан *(r=0)*

$$f(1101\ 0011 \boxplus k_0k_1k_2k_3) \oplus f(1100\ 0011 \boxplus k_0k_1k_2k_3) = 1011\ 0000$$

Хатолик айнан кириш блокининг катта разрядининг охирги разрядларида кузатилганлиги учун S_1 блокдан чиқишларни кузатиш кифоя. У ҳолда, юқоридаги тенгламани қуйидаги кўринишда ёзиш мумкин:

$$S_1(1101 \boxplus k_0k_1k_2k_3) \oplus S_1(1100 \boxplus k_0k_1k_2k_3) = 1011$$

Бу тенгламадан K_0 калитнинг дастлабки битлари $k_0k_1k_2k_3$={0110,1111} га тенг бўлади.

2. Хатоликка $R_{16} = R_{15}$ =*D3=1101 0011* кириш блоки катта разрядининг охиридан битта олдинги битида эришилди.

У ҳолда, $R`_{16} = R`_{15} = F3$=*1111 0011* га тенг. $L_{16} = C6$; $L_{15} = EF$

$$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} = f(F3 \boxplus 6B) \oplus EF = C3$$

$$A_2 = L_{16} \oplus L`_{16} = \text{C6} \oplus C3 = 05 = 00000101 \mid 3 >> \underline{1010\ 0000}$$

тенгламага эга бўламиз.

$$S_1(1101 \boxplus k_0k_1k_2k_3) \oplus S_1(1111 \boxplus k_0k_1k_2k_3) = 1010.$$

Тенгламани қаноатлантирувчи мумкин бўлган калит $k_0k_1k_2k_3$={0110}.

3. Хатоликка $R_{16} = R_{15}$ =*D3=1101 0011* кириш блоки катта разрядининг охирги битидан иккита олдинги битида эришилди.

У ҳолда, $R`_{16} = R`_{15}$ =*93=1001 0011* га тенг бўлади.

$$L_{16} = C6;\ L_{15} = EF$$

$$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} = f(93 \boxplus 6B) \oplus EF = 46$$

$$A_3 = L_{16} \oplus L`_{16} = C6 \oplus 46 = 80 = 1000000 \mid 3 >> \underline{0001\ 0000}$$

тенгламага эга бўламиз.

$$S_1(1101 \boxplus k_0k_1k_2k_3) \oplus S_1(1001 \boxplus k_0k_1k_2k_3) = 0001$$

Бу тенгламадан K_0 калитнинг дастлабки битлари $k_0k_1k_2k_3$={0110,1101, 1111}.

4. Хатоликка $R_{16} = R_{15}$ =*D3=1101 0011* кириш блокининг энг катта разрядидаги битда эришилди.

У ҳолда, $R`_{16} = R`_{15} = 53$=*0101 0011* га тенг бўлади.

$$L_{16} = C6;\ L_{15} = EF$$

$$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} = f(53 \boxplus 6B) \oplus EF = C1$$

$$A_4 = L_{16} \oplus L`_{16} = C6 \oplus C1 = 07 = 00000111 \mid 3 >> \underline{1110\ 0000}$$

$$S_1(1101 \boxplus k_0k_1k_2k_3) \oplus S_1(0101 \boxplus k_0k_1k_2k_3) = 1110.$$

Бу тенгламадан *($k_0k_1k_2k_3$)*ларнинг қабул қилиши мумкин бўлган қийматлари $k_0k_1k_2k_3$={0110,1110} га тенг бўлади.

Умумий ҳолда мумкин бўлган калитлар тўплами қуйидагича бўлди:

1. $k_0k_1k_2k_3$={0110,1111}
2. $k_0k_1k_2k_3$={0110}
3. $k_0k_1k_2k_3$={0110,1101,1111}
4. $k_0k_1k_2k_3$={0110,1110}

Мумкин бўлган калитларнинг қийматлар тўпламидан кесишмада турган $k_0k_1k_2k_3$=0110 қиймат K_0 калитнинг дастлабки битлари эканлигини топиш мумкин.

Ҳақиқатан ҳам очиқ матнни шифрлашни амалга оширишда калитнинг қийматини K_0=*6B*= $k_0k_1k_2k_3\ k_4k_5k_6k_7$=*0110 1011* деб белгиланган эди.

Демак, K_0 калитнинг дастлабки битлари тўғри топилди.

II. Энди эса, 16-раундга кирувчи $R_{15,4}$ блокнинг кичик тўрт битларига $K_{0,4}$ калитнинг кичик тўрт битлари қўшилганда, битларнинг кўчиб ўтган, яъни $R_{15,4} \boxplus K_{0,4} \geq 16$ ҳолатида

K_0 калитнинг дастлабки битлари ($k_0k_1k_2k_3$) ни топишда (2.8.20) ва (2.8.21) тенгламалар системасидан фойдаланиш мумкин.

Айтилган фикрлар тўғрилигини қуйидаги мисол ёрдамида текшириб кўрамиз:

Киручи қиймат: xl=78 6C = 0111 1000 0110 1100

Калит: kkkk=6B 6B 6B 6B=01101011 01101011 01101011 01101101

L_0 =0111 1000 R_0=0110 1100

2.8.10-жадвал.

16 раундли ГОСТ 28147-89 ўқув алгоритмида битларни кўчишини кузатиш

Раундлар	Раундлардан чиқиш қийматлари *(L_i, R_i)*	*(R_i ⊞ K_0)*	*Кўчиш*
0	*78 6C=01111000 01101100*	*6C⊞ 6B*	+
1	*6C AF*=01101100 *10101111*	*AF⊞ 6B*	+
2	*AF 29=10101111 00101001*	*29⊞ 6B*	+
3	*29 1A=00101001 00011010*	*1A⊞ 6B*	+
4	*1A 42=00011010 01000010*	*42⊞ 6B*	-
5	*42 A2=01000010 10100010*	*A2⊞ 6B*	-
6	*A2 78=10100010 01111000*	*78⊞ 6B*	+
7	*78 40=01111000 01000000*	*40⊞ 6B*	-
8	*40 F0=01000000 11110000*	*F0⊞ 6B*	-
9	*F0 4C=11110000 01001100*	*4C⊞ 6B*	+
10	*4C A6=01001100 10100110*	*A6⊞ 6B*	+
11	*A6 11=10100110 00010001*	*11⊞ 6B*	-
12	*11 A1=00010001 10100001*	*A1⊞6B*	-
13	*A1 13=10100001 00010011*	*13⊞ 6B*	-
14	*13 8E=00010011 10001110*	*8E⊞6B*	+
15	*8E 8A=10001110 10001010*	*8A⊞6B*	+
16	*8A 67=10001010 01100111*		

K_0калитнинг дастлабки битлари ($k_0k_1k_2k_3$) ни топишни бошлаймиз. Яъни юқорида таъкидланганидек охирги раундга кирувчи $R_{16} = R_{15} = 8A$*=1000 1010* блокнинг дастлабки битларида хатоликни генерациялашга эришамиз. Биз хатоликни дастлабки битларда навбати билан амалга оширилган ҳолат учун кўриб чиқамиз [5, 9].

1. Хатоликка $R_{16} = R_{15} =$*8A=1000 1010* кириш блокининг катта разрядининг охирги битида эришилди.

У ҳолда, $R`_{16} = R`_{15}$ =9A=*1001 1010* га тенг бўлади. $L_{16} = 67$*;* $L_{15} = 8E$;

$$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} = f(8A \boxplus 6B) \oplus 8E = E4,$$

$$A_1 = L_{16} \oplus L`_{16} = 67 \oplus E4 = 83 = 10000011 \mid 3 >> \underline{0111\ 0000},$$

$$L_{16} \oplus L`_{16} = f(R_{16} \boxplus K_0 \boxplus r) \oplus f(R`_{16} \boxplus K_0 \boxplus r),$$

тенгламадан *(r=1)*

$$f(1000\ 1010 \boxplus k_0k_1k_2k_3 \boxplus 1) \oplus f(1000\ 1010 \boxplus k_0k_1k_2k_3 \boxplus 1) = 0111\ 0000.$$

Хатолик айнан кириш блоки катта разряди охирги битида кузатилганлиги учун S_1 блокдан чиқишларни кузатиш кифоя. У ҳолда, юқоридаги тенгламани қуйидаги кўринишда ёзиш мумкин.

$$S_1(1000 \boxplus k_0k_1k_2k_3 \boxplus 1) \oplus S_1(1001 \boxplus k_0k_1k_2k_3 \boxplus 1) = 0111.$$

Бу тенгламадан $(k_0k_1k_2k_3)$ларнинг қабул қилиши мумкин бўлган қийматлари $k_0k_1k_2k_3$={0110} га тенг бўлади.

2. Хатоликка $R_{16} = R_{15}$ =*8A=1000 1010* кириш блоки катта разрядининг охирги битидан битта олдинги битида эришилди.

У ҳолда, $R`_{16} = R`_{15} = AA$=*1010 1010* га тенг бўлади. $L_{16} = 67$; $L_{15} = 8E$;

$$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} = f(AA \boxplus 6B) \oplus 8E = E3,$$

$$A_1 = L_{16} \oplus L`_{16} = 67 \oplus E3 = 84 = 10000100 \mid 3 >> \underline{1001\ 0000},$$

$$L_{16} \oplus L`_{16} = f(R_{16} \boxplus K_0 \boxplus r) \oplus f(R`_{16} \boxplus K_0 \boxplus r),$$

тенгламадан *(r=1)*

$$f(1000\ 1010 \boxplus k_0k_1k_2k_3 \boxplus 1) \oplus f(1010\ 1010 \boxplus k_0k_1k_2k_3 \boxplus 1) = 1001\ 0000$$

Яъни $S_1(1000 \boxplus k_0k_1k_2k_3 \boxplus 1) \oplus S_1(1010 \boxplus k_0k_1k_2k_3 \boxplus 1) = 1001.$

Бу тенгламадан $(k_0k_1k_2k_3)$ларнинг қабул қилиши мумкин бўлган қийматлари $k_0k_1k_2k_3$={0110}.

3. Хатоликка $R_{16} = R_{15}$ =*8A=1000 1010* кириш блоки катта разрядининг охирги битидан иккита олдинги битида эришилди.

У ҳолда, $R`_{16} = R`_{15} = CA$=*1100 1010* га тенг бўлади. $L_{16} = 67$; $L_{15} = 8E$;

$$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} = f(CA \boxplus 6B) \oplus 8E = E7,$$

$$A_1 = L_{16} \oplus L`_{16} = 67 \oplus E7 = 80 = 10000000 \mid 3 >> \underline{0001\ 0000},$$

$$L_{16} \oplus L`_{16} =$$

$f(R_{16} \boxplus K_0 \boxplus r) \oplus f(R`_{16} \boxplus K_0 \boxplus r)$ (2.20) тенгламадан *(r=1)*

$$f(1000\ 1010 \boxplus k_0k_1k_2k_3 \boxplus 1) \oplus f(1100\ 1010 \boxplus k_0k_1k_2k_3 \boxplus 1) = 0001\ 0000$$

Яъни $S_1(1000 \boxplus k_0k_1k_2k_3 \boxplus 1) \oplus S_1(1100 \boxplus k_0k_1k_2k_3 \boxplus 1) = 0001$.

Бу тенгламадан $(k_0k_1k_2k_3)$ларнинг қабул қилиши мумкин бўлган қийматлари $k_0k_1k_2k_3$={0110, 1101, 1111}.

4. Хатоликка $R_{16} = R_{15}$ =*8A=1000 1010* кириш блоки катта разрядининг охирги битида эришилди.

У ҳолда, $R`_{16} = R`_{15} = 0A$*=0000 1010* га тенг. $L_{16} = 67$; $L_{15} = 8E$;

$$L`_{16} = f(R`_{16} \boxplus K_0) \oplus L_{15} = f(0A \boxplus 6B) \oplus 8F = E1,$$

$$A_4 = L_{16} \oplus L`_{16} = 67 \oplus E1 = 86 = 10000110 \mid 3 >> \underline{1101\ 0000},$$

$L_{16} \oplus L`_{16} = f(R_{16} \boxplus K_0 \boxplus r) \oplus f(R`_{16} \boxplus K_0 \boxplus r)$ тенгламадан *(r=1)*

$$f(1000\ 1010 \boxplus k_0k_1k_2k_3 \boxplus 1) \oplus f(0000\ 1010 \boxplus k_0k_1k_2k_3 \boxplus 1) = 1101\ 0000$$

Яъни $S_1(1000 \boxplus k_0k_1k_2k_3 \boxplus 1) \oplus S_1(0000 \boxplus k_0k_1k_2k_3 \boxplus 1) = 1101$.

$(k_0k_1k_2k_3)$ ларнинг қабул қилиши мумкин бўлган барча 16 та қийматини сўнгги тенгламага олиб бориб қўйилади ва тенгламани қаноатлантирган қийматларни мумкин бўлган калит сифатида олинади.

Мумкин бўлган калитлар $k_0k_1k_2k_3$={0110,1110}.

Умумий ҳолда мумкин бўлган калитлар тўплами қуйидагича бўлди:

1. $k_0k_1k_2k_3$={0110}
2. $k_0k_1k_2k_3$={0110}
3. $k_0k_1k_2k_3$={0110, 1101, 1111}
4. $k_0k_1k_2k_3$={0110, 1110}

Мумкин бўлган калитлар қийматлар тўпламидан кесишмада турган $k_0k_1k_2k_3$=0110 қиймат K_0 калитнинг дастлабки битлари

эканлигини топиш мумкин. Ҳақиқатан ҳам очиқ матнни шифрлашни амалга оширишда калитнинг қийматини K_0=*6B*= $k_0k_1k_2k_3\ k_4k_5k_6k_7$=*0110 1011* деб белгилаб олинган эди [6, 18, 21].

Демак, K_0 калитнинг дастлабки битлари тўғри топилган.

Юқорида ўқув алгоритмига аппарат хатоликларини генерация-лашга асосланган криптотаҳлил усулининг қўлланилиш модели асосида стандарт ГОСТ 28147-89 шифрлаш алгоритмига мазкур усулнинг қадамлар кетма-кетлиги қуйидаги кўринишда бўлади.

Алгоритмнинг қадамлар кетма-кетлиги:

1. L_0 ва R_0 кирувчи қийматлар ўрнатилади.

2. $i=\overline{32\ 1}$, $j=\overline{1\ 8}$ ва $r=\overline{8\ 1}$ санагичлар ўрнатилади.

3. $L_i=f(R_{i-1} \boxplus K_j) \oplus L_{i-1}$ (*i-1* раундда) хатоликни генерациялашни *i*-раундга кирувчи R_{i-1} блокнинг охирги тўрт битларидан бошлаб амалга оширилади $L`_i=f(R`_{i-1} \boxplus K_j) \oplus L_{i-1}$.

4. Тенгламаларни (2 mod) қўшиб қуйидаги тенгламага эга бўлинади:

$$g^{\gg 11}(L_i \oplus L`_i) = h_s(R_{i.4} \boxplus K_{j.4}) \oplus h_s(R`_{i.4} \boxplus K_{j.4}).$$

5. i – раундда ишлатилган $K_{j.4}$ қисм калитнинг битларини топиш бошланади.

6. Хатолик охирги тўрт битларда амалга оширилганлигини билган ҳолда тенгламани $S_r(R_{i.4} \boxplus K_{j.4}) \oplus S_r(R`_{i.4} \boxplus K_{j.4}) = (L_i \oplus L`_i)^{\gg 11}$ кўринишга келтирилади ва бу ердан $K_{j.4}$ нинг қабул қилиши мумкин бўлган барча 16 та қийматини тенгламага олиб бориб қўйилади ва тенгламани қаноатлантирганлари номзод калит сифатида олиб қўйилади. Агар тенгламани қаноатлантирадиган $K_{j.4}$ қийматлари бўлмаса, у ҳолда, 1 қадамга қайтиб бошқа кирувчи блоклар берилади ёки хатоликни R_{i-1} блокнинг охирги тўрт битларининг бошқа битларида амалга оширилади.

7. $K_{j.4}$ калит дастлабки битларини топиш учун хатоликни R_{i-1} блокнинг дастлабки битларида амалга оширилади. Фақатгина бунда битларни перенос ҳолатини этиборга олинади ва тенглама кўриниши қуйидагича ўзгартирилади;

$$S_{r-1}\left(R_{i.4} \boxplus K_{j.4} \boxplus k\right) \oplus S_{r-1}\left(R`_{i.4} \boxplus K_{j.4} \boxplus k\right) = (L_i \oplus L`_i)^{\gg 11}$$

$$k = \begin{cases} 1, & R_{i,4} \boxplus K_{j,4} \geq 16 \\ 0, & R_{i,4} \boxplus K_{j,4} < 16 \end{cases}.$$

8. Охирги тенгламадан ҳудди 6-қадамдаги каби ҳисоблашларни амалга оширилади ва $K_{j.4}$ калитнинг охирги тўрт битларидан олдинги битлари топилади.

9. i - раундда ишлатилган $K_{j.4}$ қисм калитнинг қолган битларини топиш учун хатоликни R_{i-1} блокнинг дастлабки битларида навбати билан амалга оширилади ва 7 – қадамдаги формуладан фойдаланиб топилади.

10. i - раундда ишлатилган $K_{j.4}$ қисм калитнинг барча битлари топилганидан сўнг алгоритмнинг қадамлар кетма-кетлиги тўхтатилади.

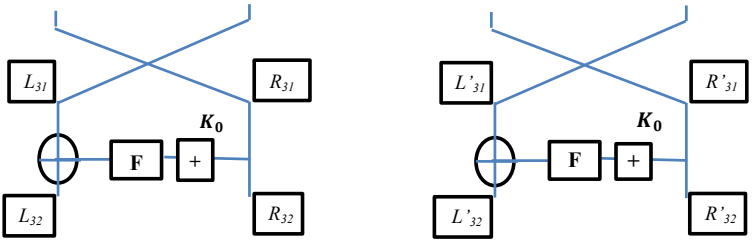
ГОСТ 28147-89 стандарт шифрлаш алгоритми учун аппарат хатоликларини генерациялашга асосланган таҳлил, алмаштиришнинг охирги раундида фойдаланилган қисм калит (K_0) ни топиш, кейин эса босқичма-босқич равишда аввалги раундларга қайтиб калитнинг қолган $(K_1, K_2, K_3, K_4, K_5, K_6, K_7)$ элементларини топишга қаратилган.

Кириш блокининг i- қадамида бажарилган алмаштиришдан сўнг чиққан қийматларини чап (катта) ва ўнг (кичик) разрядларини мос равишда L_i ва R_i деб белгилаб оламиз. У ҳолда, алгоритмга асосан қуйидагиларга эга бўлинади:

$$R_{32} = R_{31}; \qquad (2.8.26)$$

$$L_{32} = f(R_{31} \boxplus K_0) \oplus L_{31}. \qquad (2.8.27)$$

бу ерда, $\boxplus$ – 2^{32} модул бўйича; $\oplus$ – XOR (2 модул бўйича қўшиш амали)



2.8.2-расм. ГОСТ 28147-89 алгоритмининг сўнгги раунди схемаси.

$f()\ -R_{31} \boxplus K_0$ йиғиндини 4-битли блокларга ажратиб уларни алмаштириш жадвали ($S-$блок)дан блокдан ўтказиб, натижани циклик равишда 11-бит чапга (катта разрядлар томонга) сурувчи функция. Шифрлаш қурилмасининг киришига ихтиёрий 64-битли блок берилиб, чиқишида эса иккита 32-битли (L_{32}, R_{32}) қийматларга эга бўлинади. Шифрлаш жараёнида R_{31} блокнинг кичик 4-битларида хатоликларни генерациялаш мақсадида техник қурилмага ташқи таъсир кўрсатилади.

У ҳолда, юқоридаги тенглама чап қисми кўриниши қуйидагича бўлади:

$$L`_{32} = f(R`_{31} \boxplus K_0) \oplus L_{31} \qquad (2.8.28)$$

бу ерда, $R`_{31}$ блок R_{31} блокдан фақатгина кичик разрядларидан бирига фарқ қилади.

(2.8.27) ва (2.8.28) тенгламаларни XOR амали бўйича қўшиб қуйидаги тенгликлар ҳосил қилинади:

$$L_{32} \oplus L`_{32} = f(R_{31} \boxplus K_0) \oplus f(R`_{31} \boxplus K_0) \qquad (2.8.29)$$

ёки (2.8.26) тенгликни этиборга олиб,

$$L_{32} \oplus L`_{32} = f(R_{32} \boxplus K_0) \oplus f(R`_{32} \boxplus K_0). \qquad (2.8.30)$$

Хатоликни R_{31} блокнинг қолган учта разрядларида ҳам амалга ошириб яна учта тенгламага эга бўлиш мумкин. Дастлабки кириш R_{31} блокига бошқа қийматлар бериб яна ҳудди шундай тўртта тенгламалар системасига ҳам эга бўлинади.

Шундай қилиб, кириш блокига турлича қийматлар бериб, R_{31}нинг барча мумкин бўлган 16 та қийматига эришиш мумкин. Ҳар бир кириш блокига нисбатан тўртта ҳатоликни амалга ошириш орқали жами 4*16=64 та тенгламага эга бўлинади.

Ҳосил бўлган тенгламалар бир-бирига боғлиқ бўлиб, улардан қуйидаги 16 та тенгламадан иборат тенгламалар системасини ҳосил қилиш мумкин:

$$\begin{cases} f(K_0) \oplus f(K_0 \boxplus 1) = A_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f(K_0) \oplus f(K_0 \boxplus 16) = A_{16} \end{cases} \qquad (2.8.31)$$

бу ерда, A_i коэффицентлар (2.8.30) кўринишидаги тенгламаларнинг чап томонларининг XOR бўйича йиғинди натижасини ифодалайди.

(2.8.30) тенгламанинг кўринишини қуйидагича алмаштириш мумкин:

$$g2(L_{16} \oplus L`_{16}) = h2(R_{16} \boxplus K_0) \oplus h2(R`_{16} \boxplus K_0) \qquad (2.8.32)$$

бу ерда, $g2 - L_{16} \oplus L`_{16}$ йиғиндининг кичик тўрт битларини 3-бит циклик равишда ўнг (кичик разрядлар) томонга сурувчи функция;

$h2$– кичик тўрт битларни $S(2)$ блок бўйича алмаштирувчи функция;

K_0 калит кичик тўрт битлари қабул қилиши мумкин бўлган барча 16 та вариантини (2.8.32) тенгламага қўйиб, улар ичидан тенгламани қаноатлантирганларини мумкин бўлган калит сифатида олинади.

Тажрибада кўриш мумкинки калитнинг кичик тўрт битларини бир қийматли аниқлаш учун битта тенгламага эга бўлиш етарли ҳисобланади.

Охирги раундда ишлатилган K_0 калитнинг охирги кичик битларидан олдинги битлари ($k_{32.0}k_{32.1}$ ... $k_{32.27}k_{32.28}$) ни топиш учун 32-раундга кирувчи $R_{31,4}$ блокнинг кичик тўрт битларига $K_{32,4}$ калитнинг охирги кичик тўрт битлари қўшилганда, битларнинг ўзидан олдинги битларга таъсир этиши ҳолати кузатилиши мумкин. Мазкур ҳолат охирги кичик тўрт битларнинг йиғиндиси 16 дан катта ёки тенг бўлганда кузатилади, яъни $R_{15,4} \boxplus K_{0,4} \geq 16$. Буни тенгламалар системасини тузишда эътиборга олиб қуйидагича ёзиш мумкин:

$$\begin{cases} f\left(R_{32}^{(29)} \boxplus K_0 \boxplus r\right) \oplus f(R_{32} \boxplus K_0 \boxplus r) = L_{32}^{(29)} \oplus L_{32} \\ f\left(R_{32}^{(30)} \boxplus K_0 \boxplus r\right) \oplus f(R_{32} \boxplus K_0 \boxplus r) = L_{32}^{(30)} \oplus L_{32} \\ f\left(R_{32}^{(31)} \boxplus K_0 \boxplus r\right) \oplus f(R_{32} \boxplus K_0 \boxplus r) = L_{32}^{(31)} \oplus L_{32} \\ f\left(R_{32}^{(32)} \boxplus K_0 \boxplus r\right) \oplus f(R_{32} \boxplus K_0 \boxplus r) = L_{32}^{(32)} \oplus L_{32} \end{cases} \qquad (2.8.33)$$

бу ерда,

$$r = \begin{cases} 1, & R_{31,4} \boxplus K_{0,4} \geq 16 \\ 0, & R_{31,4} \boxplus K_{0,4} < 16 \end{cases} \qquad (2.8.34)$$

Қуйида, ГОСТ 28147-89 алгоритмига аппарат хатоликларини генерациялашга асосланган криптотаҳлил усулини қўллаш натижасида калитни тиклашга доир намуна келтирилган.

Кирувчи қиймат:
salomjon=73616C6F6D6A6F6E$_{16}$=01110011011000010110110001
10111101101101011010100110111101101110$_2$

Калит:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa=61616161616161616161616161
61616161616161616161616161616161616161616161$_{16}$=0110000101
10000101100001011000010110000101100001011000010110000101100
00010110000101100001011000010110000101100001011000010110000
01011000010110000101100001011000010110000101100001011000010
11000010110000101100001011000010110000101100001011000010110
00010110000101100001011000010110000101100001011000010110000101
10000101100001$_2$

Шифр матн:
p`ЄЬgŕ]=*F060AADC67830F5D$_{16}$=11110000011000001010101011011*
10001100111100000110000111101011101$_2$

2.8.11-жадвал.

ГОСТ 28147-89 алгоритми криптотаҳлили натижаси

Хатолик ўрни	**Тенгламалар**	**Номзод калитлар**	**Ҳақиқий калит(4-бит)**
0	S7(0111+K28K29K30K31) ⊕ S7(0110 + K28K29K30K31)= 1101	{**0001**} {0100} {0110} {1001} {1100} {1111}	$K_{28}K_{29}K_{30}K_{31}$ ={0001}
1	S7(0111+K28K29K30K31) ⊕ S7(0101 + K28K29K30K31) = 0011	{0000} {**0001**} {1010}	
2	S7(0111+K28K29K30K31) ⊕ S7(0011+ K28K29K30K31) = 1100	{**0001**} {1100}	
3	S7(0111+ K28K29K30K31) ⊕ S7(1111+K28K29K30K31) = 1000	{0000} {**0001**} {1000} {1001}	
4	S6(0110+K24K25K26K27) ⊕ S6(0111 + K24K25K26K27) = 1110	{**0110**} {1000}	$K_{24}K_{25}K_{26}K_{27}$ ={0110}
5	S6(0110+K24K25K26K27) ⊕ S6(0100+ K24K25K26K27) = 1000	{**0110**}	
6	S6(0110+K24K25K26K27) ⊕ S6(0010+ K24K25K26K27) = 0110	{**0110**} {1100}	
7	S6(0110+K24K25K26K27) ⊕ S6(1110+ K24K25K26K27) = 0101	{0001} {**0110**} {1001} {1110}	
8	S5(0011+K20K21K22K23) ⊕ S5(0010+ K20K21K22K23) = 0111	{**0001**}	$K_{20}K_{21}K_{22}K_{23}$ ={0001}
9	S5(0011+K20K21K22K23) ⊕ S5(0001+ K20K21K22K23) = 1101	{**0001**}	
10	S5(0011+K20K21K22K23) ⊕ S5(0111+ K20K21K22K23) = 0100	{**0001**} {0010}	
11	S5(0011+K20K21K22K23) ⊕ S5(1011+ K20K21K22K23) = 1110	{**0001**} {0010} {0011} {1001} {1010} {1011}	
12	S4(1000+K16K17K18K19) ⊕ S4(1001+ K16K17K18K19) = 1001	{**0110**}	$K_{16}K_{17}K_{18}K_{19}$ ={0110}

2.8.11-жадвалнинг давоми

13	S4(1000+K16K17K18K19) ⊕ S4(1010+ K16K17K18K19) = 1101	{0000} {0011} {**0110**} {1001}	
14	S4(1000+K16K17K18K19) ⊕ S4(1100+ K16K17K18K19) = 1100	{0011} {**0110**}	
15	S4(1000+K16K17K18K19) ⊕ S4(0000+ K16K17K18K19) = 0110	{0001} {**0110**} {1001} {1110}	
16	S3(1111+K12K13K14K15) ⊕ S3(1110 + K12K13K14K15) = 0100	{**0001**}	$K_{12}K_{13}K_{14}K_{15}$ ={0001}
17	S3(1111+K12K13K14K15) ⊕ S3(1101 + K12K13K14K15) = 0010	{ **0001** }	
18	S3(1111+K12K13K14K15) ⊕ S3(1011 + K12K13K14K15) = 1100	{**0001**} {1010}	
19	S3(1111+K12K13K14K15) ⊕ S3(0111 + K12K13K14K15) = 1001	{**0001**} {0010} {1001} {1010}	
20	S2(0000+K8K9K10K11+1) ⊕ S2(0001+K8K9K10K11+1) = 1100	{0010} {**0110**}	$K_8K_9K_{10}K_{11}$ ={0110}
21	S2(0000+K8K9K10K11+1) ⊕ S2(0010+K8K9K10K11+1) = 1101	{**0110**}	
22	S2(0000+K8K9K10K11+1) ⊕ S2(0100+K8K9K10K11+1) = 0101	{0010} {**0110**} {1010}	
23	S2(0000+K8K9K10K11+1) ⊕ S2(1000+K8K9K10K11+1) = 1001	{**0110**} {1111}	
24	S1(1101 + K4K5K6K7) ⊕ S1(1100 + K4K5K6K7) = 0010	{**0001**} {1001}	$K_4K_5K_6K_7$ ={0001}
25	S1(1101 + K4K5K6K7) ⊕ S1(1111 + K4K5K6K7) = 1011	{**0001**}	
26	S1(1101 + K4K5K6K7) ⊕ S1(1001 + K4K5K6K7) = 1101	{**0001**}	
27	S1(1101 + K4K5K6K7) ⊕ S1(0101 + K4K5K6K7) = 1010	{0000} {**0001**} {1000} {1001}	
28	S0(0101 + K0K1K2K3) ⊕ S0(0100 + K0K1K2K3) = 1101	{0100} {**0110**}	$K_0K_1K_2K_3$ ={0110}
29	S0(0101+K0K1K2K3)⊕ S0(0111+K0K1K2K3) = 0011	{**0110**}	
30	S0(0101 + K0K1K2K3) ⊕ S0(0001 + K0K1K2K3) = 0010	{0000} {**0110**}	
31	S0(0101 + K0K1K2K3) ⊕ S0(1101 + K0K1K2K3) = 1110	{**0110**} {1110}	

Айрим шифрлаш алгоритмлари учун аппарат хатоликларини генерациялашга асосланган криптотаҳлил усули, фақат математик таҳлилга асосланган ананавий криптотаҳлилларга нисбатан самаралироқ эканлигини кўрсатмоқда.

Жумладан, ГОСТ 28147-89 стандарт шифрлаш алгоритми бўйича олиб борилган тадқиқотлар, мазкур алгоритмнинг тегишли аппарат хатоликларини генерация қилишни бошқариш имконияти

мавжуд бўлганда, ушбу ҳужумга нисбатан бардошсиз эканлигини кўрсатмоқда.

Таъкидлаш лозимки, ГОСТ 28147-89 алгоритмда 2^{32} модул бўйича қўшиш амалининг ишлатилиши, S–блоклар ўлчамининг кичиклиги ва орқага бир қийматли қайтиши, аппарат хатоликларини генерациялашга асосланган криптотаҳлил хужумини қўллашга имконият келтириб чиқаради. Шундан келиб чиққан ҳолда, шифрлаш алгоритмлари учун тегишли қурилмаларни яратишда ташқи физик таъсирлардан ҳимоялаш чора тадбирларини амалга ошириш мақсадга мувофиқдир.

ГОСТ 28147-89 алгоритми бўйича олиб борилган изланишлар, бу алгоритм S – блок акслантиришлари маълум ва аппарат хатоликларини генерациялаш имконияти мавжуд бўлганда, алгоритмда 2^{32} модул бўйича қўшиш амалининг ишлатилиши, S – блоклар ўлчамининг кичиклиги ва орқага бир қийматли қайтиши, раунд калитларини генерация қилиш жараёнида мураккаб математик ва мантиқий функцияларнинг қўлланилмаслиги, кичик узунликдаги раунд калитларидан такроран фойдаланилганлиги аппарат хатоликларини генерациялашга асосланган криптотаҳлил ҳужумини қўллашга имконият келтириб чиқаради.

Умумий ҳолда, мавжуд ёки янги яратилган блокли шифрлаш алгоритмини Аппарат хатоликларини генерациялашга асосланган криптотаҳлил усули ёрдамида баҳолаш жараёни қуйидаги **“Баҳолаш натижалари” жадвалини тўлдириш** ва у асосида **алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш** босқичларини ўз ичига олади.

2.8.12-жадвал.

Криптотаҳлил натижаси

№	Бажарилувчи иш	Иш натижаси	Якуний хулосаси
I.	Шифрлаш алгоритми маълум блокларидаги айрим битларни ўзгартиришга эришиш мақсадида, ҳимоя аппаратига иссиқлик, юқори частотали, иони-	Ташқи таъсир ўтказиш имконияти мавжуд	Ихтиёрий битларга таъсир ўтказишни бошқариш мумкин бўлганда, калит битларини аниқлаш мумкинлиги текширилиб хулоса берилади

2.8.12-жадвалнинг давоми

	зациялаш ва бошқа ташқи физик таъсир ўтказиш	Ташқи таъсир ўтказиш имконияти мавжуд эмас	Алгоритмни аппарат хатоликларини генерациялашга асосланган криптотаҳлил усулига баҳолаб бўлмайди
II.	Танланган очиқ матн ва мос шифрматнлар ҳамда алгоритмнинг охирги раундида фиксирланган битларни ўзгартирилиши асосида раунд функциясига кирувчи ва чиқувчи ҳақиқий матнлар билан уларнинг модификацияланган кўринишлари ўртасидаги боғланишни ҳосил қилиш	Боғлиқлик натижасида бир қийматли тенглик ҳосил қилинади	Мазкур тенглик натижасида калит битларини аниқлаш мумкинлигини текшириш натижасида хулоса берилади
		Боғлиқлик натижасида бир қийматли тенглик мавжуд эмас	Танланган ташқи таъсир асосида аппарат хатоликларини генерациялаш криптотаҳлил усулига баҳолаб бўлмайди. Бошқа ташқи физик таъсир ўтказиш йўли билан баҳолаш
III.	Алгоритмда фойдаланилган асосий раунд акслантириши, яъни ҳар бир S блоклар учун кирувчи ва чиқувчи битлар ўртасидаги боғлиқликни ифодаловчи тенгликларни ажратиб олиш	Раунд акслантириши-шига кирувчи $n = p * q$ ўлчамли битлар, q битли кириш ва чиқишга эга p та S блоклар учун боғлиқлик тенгликлари мавжуд	Ҳосил бўлган тенгликлардан иборат тенгламалар системасини ечиш мумкинлиги текширилиб хулоса берилади
		Ҳар бир S блоклар учун боғлиқлик	Танланган ташқи таъсир асосида аппарат хатоликларини

2.8.12-жадвалнинг давоми

		тенгликлари мавжуд эмас	генерациялаш криптотаҳлил усулига бардошли. Бошқа ташқи физик таъсир ўтказиш йўли билан баҳолаш.
IV.	Охирги раундда ҳосил бўлган тенгликлардан иборат тенгламалар системасини ечиш орқали мумкин бўлган калитлар тўпламини ҳосил қилиш	Тенгламалар системаси бир қийматли ечимга эга ва мумкин бўлган калитлар тўплами ҳосил қилинади	$n = p * q$ бит узунликдаги калит битлари мураккаблиги $2^n = 2^{p*q}$ тўлиқ танлаш усулидан фарқли уларок $q * 2^q$ мураккаблик билан аниқланади ҳамда бошқа раунд калит битларини аниқлаш мумкинлиги билан баҳоланади
		Тенгламалар системаси бир қийматли ечимга эга эмас	Калит битларини аниқлаш мураккаблиги тўлиқ танлаш мураккаблигига яқин ва ҳисоблаш техникаси имкониятидан юқори.
V.	Охирги раундга қўлланилган ташқи физик таъсир каби бошқа раунд калитларини аниқлаш	Барча раунд мумкин бўлган калит битлари тўпламини танланган очиқ матн ва мос шифрматнлар ёрдамида ҳақиқийликка текшириш	Текшириш натижаси ижобий бўлганда аппарат хатоликларини генерациялашга асосланган криптотаҳлил усулига бардошли эмас

Назорат саволлари

1. Шифрлаш жараёнида аппарат хатоликлар қандай вужудга келишини мисолларда тушунтиринг.

2. Аппарат хатоликларини генерациялашга асосланган криптотаҳлил усулининг асосий моҳияти нимадан иборат?

3. Криптотаҳлил жараёнида аппарат хатоликларини ҳосил қилишнинг қандай ёндашувлари мавжуд?

4. Аппарат хатолиги содир бўлган раунд ёки бит ўрнининг криптотаҳлил жараёнига таъсири қандай?

5. Аппарат хатолиги содир этилганидан сўнг, махфий калит қийматини аниқлаш қандай қадамлар кетма-кетлигида амалга оширилади?

6. ГОСТ 28147-89 шифрлаш алгоритмига аппарат хатоликларини генерациялашга асосланган криптотаҳлил усулини қўллаш моҳиятини тушунтиринг.

7. Шифрлаш алгоритми таркибидаги чизиқли ва чизиқсиз акслантиришларнинг мазкур таҳлил самарадорлигига таъсири қандай?

8. Шифрлаш алгоритми раундлар сони криптотаҳлил самарадорлигига қандай таъсир кўрсатади?

9. Аппарат хатоликларини генерациялашга асосланган криптотаҳлил усулини бошқа мавжуд криптотаҳлил усуллари билан ўзаро таққосланг.

10. Аппарат хатоликларини генерациялашга асосланган криптотаҳлил усули самарадорлиги нималарга боғлиқ?

III. КРИПТОТАҲЛИЛ НАТИЖАЛАРИ БЎЙИЧА БЛОКЛИ СИММЕТРИК ШИФРЛАШ АЛГОРИТМЛАРИ БАРДОШЛИЛИГИНИ СОНЛИ БАҲОЛАШ

3.1. Шифрлаш алгоритмлари бардошлилигини сонли баҳолаш

Блокли симметрик шифрлаш алгоритмларини юқорида келтирилган криптотаҳлил усулларига бардошлилигини баҳолаш қадамлари натижаларига кўра алгоритм криптобардошлилигини сонли баҳолаш муҳим ва қийин илмий масала ҳисобланади. Криптотаҳлил натижасида аниқланган турли бардошлилик кўрсаткичлари амалиётда ҳар доим ҳам ўз исботини топмаслиги мумкин. Шунинг учун криптология соҳасидаги кўплаб фикрлар назарий исботи билан бир қаторда эксперимental исботни ҳам талаб этади ва ихтиёрий шифрлаш алгоритми криптобардошлилиги унинг барча замонавий крипто-таҳлил усулларига нисбатан қарши тура олиш қобилияти билан баҳоланади.

Агар криптотаҳлил жараёнида шифрни очиш имкониятини берувчи камида битта криптотаҳлил усули мавжуд бўлса, у ҳолда, мазкур шифр криптобардошсиз ҳисобланади. Шунга кўра, шифрлаш алгоритмлари криптобардошлилигини сонли баҳолашда, унга нисбатан қўлланилган барча криптотаҳлил усуллари натижалари асосида **умумий криптобардошлилик кўрсаткичи (УКК) деб номланувчи катталикни** шакллантириш мақсадга мувофиқ ҳисобланади.

Очиқ адабиётлар таҳлилига мувофиқ, замонавий блокли шифрлаш алгоритми криптобардошлилигини баҳолашда қуйидаги криптотаҳлил усулларидан фойдаланиш тавсия этилади:

- дифференциал криптотаҳлил;
- чизиқли криптотаҳлил;
- чизиқли-дифференциал криптотаҳлил;
- интеграл криптотаҳлил;
- алгебраик криптотаҳлил;
- слайд криптотаҳлил;
- тўлиқ танлов усули.

Техник криптоҳужум (қўшимча каналлардан ҳосил бўлувчи маълумотлар асосидаги ҳужум) турларини замонавий шароитларда амалиётга татбиқ қилиш имкониятлари деярли мавжуд бўлмаган-

лиги учун (одатда шифрлаш қурилмалари криптотаҳлилчидан маълум узоқликда жойлашиб, қурилмага нисбатан бирор таъсир ўтказиш имконияти мавжуд бўлмайди), мазкур криптотаҳлил усуллари натижаларини **УКК** катталик таркибига киритиш тафсия этилмайди.

Умумий криптобардошлилик кўрсаткичи қиймати қуйидаги формула билан аниқланади [59]:

$$F_{\Sigma} = \sum_{i=1}^{S} f_i(W, N, P_d); \;\; F_{\Sigma} < F_d \tag{3.1.1}$$

Бу ерда, s – криптотаҳлил усуллари сони; f_i – шифрлаш алгоритмининг бирор криптотаҳлил турига бардошлилигини дастлабки маълумотлар (очиқ ёки шифр матн) сонига ўрнатилган чеклов (W), ҳисоблаш ресурслари (шифрлаш/очиқ матнга ўгириш амаллари) сонига ўрнатилган чеклов (N) ва ушбу чекловлар асосида шифрлаш алгоритмини очишга ўрнатилган (белгиланган) эҳтимоллик (P_d) билан характерланувчи функция ҳисобланади. Амалиётда ушбу W ва N параметрларнинг қийматлари мавжуд замонавий ҳисоблаш техникаларининг имкониятлари асосида белгиланади.

Мазкур f_i – функция қиймати қуйидагича аниқланади:

$$f_i(W, N, P_d) = \begin{cases} 0, \;\; \forall W, N \;\; P_{W,N} < P_d \\ 1, \;\; P_{W,N} \geq P_d \\ \dfrac{P_d}{\left(1 + \dfrac{W'}{W}\right)\left(1 + \dfrac{N'}{N}\right)}, \;\; P_{W,N} < P_d, \;\; \exists\, W', N' : P_{W',N'} \geq P_d \end{cases} \tag{3.1.2}$$

Яъни, ушбу функция 0 қиймат олади, агар ўрнатилган ҳар қандай чекловларда ҳужумни муваффақиятли ўтказиш эҳтимоллиги берилган P_d эҳтимолликдан кичик бўлса, агар ўрнатилган чекловларда ҳужумни муваффақиятли ўтказиш эҳтимоллиги берилган P_d эҳтимолликка тенг ёки ундан катта бўлса, у ҳолда, функция 1 қиймат қабул қилади. Агар ҳужумни муваффақиятли ўтказиш эҳтимоллиги берилган эҳтимолликка тенг ёки ундан катта бўлишини таъминловчи ҳолат (чеклов) мавжуд бўлса, у ҳолда, функция қиймати ўрнатилган эҳтимоллик қийматини талаб этилувчи маълумотлар (W') ва мавжуд маълумотлар нисбатига ҳамда талаб этилувчи (N') ва мавжуд ҳисоблаш ресурслари нисбатига бўлиш орқали ҳисобланади.

(3.1.2) ифодадаги *W'* ва *N'* параметр қийматлари айнан криптотаҳлил натижасига боғлиқ тарзда аниқланади. Мазкур қийматлар ушбу ўқув қўлланманинг аввалги қисмида келтирилган баҳолаш жадвалларидаги *W* ва *N* параметр қийматлари билан устма-уст тушади. Таъкидлаш лозимки, шифрлаш алгоритмларини айрим криптотаҳлил усулларига бардошлилигини баҳолашда аввалдан *W* ва *N* параметр қийматларини аниқлаб бўлмайди (масалан Слайдли ҳужум криптотаҳлил усулида слайд жуфтликларини топиш учун талаб этилувчи ҳисоблашлар ва таҳлил қилинувчи матнлар сонини аввалдан аниқлаш мураккаб). Ушбу ҳолатларда эса, шифрлаш алгоритми криптобардошлилиги юзасидан фақатгина ўтказилган статистикалар натижасидагина хулоса бериш мумкин бўлади.

Бугунги кунда замонавий ЭҲМлар имкониятларидан келиб чиқиб, **УКК** қийматнинг $F_d=s*10^{-6}$ дан ошиши, тадқиқ қилинаётган блокли шифрлаш алгоритми ҳеч бўлмаганда битта криптотаҳлил ҳужумига потенциал заиф эканлигини англатади.

УКК физик маъносига кўра:

- қиймат 1 га яқинлашганда шифрлаш алгоритмига ҳеч бўлмаганда битта амалий қўллаш мумкин бўлган криптотаҳлил усули мавжудлигини;
- қиймат 1 дан *N* гача бўлганда шифрлаш алгоритмига бир нечта амалий қўллаш мумкин бўлган криптотаҳлил усули мавжудлигини;
- қиймат 1 дан етарлича кичик бўлганда шифрлаш алгоритмига ҳеч бўлмаганда битта криптотаҳлил усулини амалий қўллаш учун олдин мавжуд бўлган ресурсларга (дастлабки маълумотлар ёки ҳисоблаш қуввати) қандай минимал сондаги ресурсларни қўшиш лозимлигини англатади.

Блокли шифрлаш алгоритми критобардошлилигини ҳисоблашнинг **УКК** қиймати бўйича мазкур ёндашуви алгоритмнинг барча криптотаҳлил ҳужумларига қарши бардошли ёки бардошсиз эканлигини аниқлаш имконини беради. Агар **УКК** қиймати 1 га яқин бўлса, у ҳолда, криптотаҳлил ҳужумларидан бирини ўтказиш мақсадга мувофиқ, агар кўрсаткич қиймати 0 га тенг бўлса, у ҳолда, алгоритм ишончлилиги унинг ҳатто назарий очиш (криптотаҳлил назариясида жиддий тарзда ўзгаришларсиз) имкониятини ҳам бермайди, агар **УКК** қиймати 1 дан етарлича кичик бўлса, у ҳолда

кейинчалик ҳужумларни такомиллаштириш ёки ҳужумни қўллашдаги чекловларни қисқартириш йўналишидаги тадқиқотларни ўтказиш мақсадга мувофиқ бўлади.

Таъкидлаш лозимки, сўнгги вақтларда илмий ҳамжамиятда шифрлаш алгоритмларини лойиҳалаш ва таҳлил қилишга бўлган эътиборнинг янада ўсиши кузатилмоқда. Ушбу ҳолатни халқаро миқёсдаги конференцияларга тақдим этилувчи шифрлаш алгоритмларига бағишланган мақолалар сони ва олиб борилаётган очиқ танловлар илмий-даражасини ортишида ҳам кўриш мумкин. Таҳлил объекти бирор "шифр" бўлган ва турли мақсадларга қаратилган илмий-тадқиқотлар доирасида мавжуд шифрлаш алгоритмларини таҳлил қилиш билан бирга янги шифрлаш алгоритмлари, шунингдек самарали бўлган криптотаҳлил усуллари ҳам таклиф этилмоқда. Бу эса, **амалда фойдаланиб келинаётган шифрлаш алгоритмларини маълум вақт оралиқларида (узлуксиз) янги турдаги ҳужум усулларига баҳолаб бориш муҳим вазифа** эканлигини яна бир бор кўрсатади.

3.2. DES ва ГОСТ 28147-89 блокли шифрлаш алгоритмлари бардошлилигини сонли баҳолаш

Юқорида таклиф этилган баҳолаш усулига мувофиқ, қуйида DES ва ГОСТ 28147-89 блокли шифрлаш алгоритмлари криптобардошлилигини **УКК** асосида таҳлил қилишга намуна келтирилган.

DES шифрлаш алгоритми калит узунлигини тўлиқ танлов усули асосида очиш мумкин бўлгани учун мазкур шифр бугунги кунда стандарт алгоритм сифатида фойдаланилмайди. Ҳисоблаш ресурслари кўп маблағ талаб этганлиги сабабли, алоҳида фойдаланувчилар ва катта бўлмаган компания ёки ташкилотлар учун тўлиқ танлов усули орқали криптотаҳлилни амалга ошириш имконияти мавжуд эмас. Бироқ йирик компания ва ташкилотлар учун мазкур ҳужумни амалга ошириш имкони мавжуд.

ГОСТ 28147-89 блокли шифрлаш алгоритми ҳозирги кунда кўплаб давлатларнинг стандарти ҳисобланиб, ундан амалда катта ҳажмдаги маълумотларни шифрлаш учун фойдаланилмоқда.

Айтайлик, криптотаҳлил учун ўртанилган чекловлар, яъни дастлабки маълумотлар сифатида $W=2^{30}$ та очиқ матн ва битта калит

билан шифрланган унга мос шифр матнлар, ҳисоблаш ресурслари ҳажми эса 3 ГГц частотали Pentium 4 синфига тегишли 1024 та стандарт ЭҲМ воситаси бўлсин. Тўрт ядроли ЭҲМ ва оптимал реализация бўлганда назарий тезликка яқин ҳисобланган, яъни секундига 150 Мбайт тезликда шифрлашга эришилганда битта ЭҲМ секундига 2^{24} атрофида ва 1024 та ЭҲМ секундига 2^{34} шифрлаш амалини бажариши мумкин.

Дешифрлаш учун ажратилган вақт эса, 8 кун бўлсин, демак, $60*60*24*8=2^{20}$ секунда 2^{54} та шифрлаш амалини бажариш мумкин. Очиқ манбаларда келтирилган маълумотларга кўра, танланган шифрлаш алгоритмларининг тўлиқ раундига нисбатан қўлланилган айрим криптотаҳлил усуллари натижалари қуйидаги жадвалда келтирилган [58, 59]:

3.1.1-жадвал.

Криптотаҳлил усуллари натижалари

Криптотаҳлил усули	**Калитни аниқлаш учун талаб этилувчи матнлар ва амаллар сони**	
	DES	**ГОСТ 28147-89**
Чизиқли криптотаҳлил	$W=2^{43}$, $N=2^{43}$	–
Дифференциал криптотаҳлил	$W=2^{55}$, $N=2^{55}$	–
Алгебраик криптотаҳлил	–	$W=2^{64}$, $N=2^{248}$
Тўлиқ танлов	$W=2^{1}$, $N=2^{56}$	$W=2^{1}$, $N=2^{256}$

Шифрлаш алгоритмларига қўллашдан олинган мазкур натижалар асосида DES алгоритми учун **УКК** қиймати қуйидагига тенг бўлади:

$$F_{\Sigma}(DES)=\frac{1}{\left(1+\frac{2^{43}}{2^{30}}\right)*1}+\frac{1}{\left(1+\frac{2^{55}}{2^{30}}\right)*\left(1+\frac{2^{55}}{2^{54}}\right)}+\frac{1}{1*\left(1+\frac{2^{56}}{2^{54}}\right)},$$

$$F_{\Sigma}(DES)\approx 1.2e-4+9.9e-9+0.2\approx 0.200122$$

Ушбу қийматдан берилган шартлар асосида DES алгоритмини очиш имкони мавжуд эмас, бироқ чекловларнинг бироз ўзгариши шифрни амалий очиш мумкинлигини кўрсатади. Яъни, шифрнинг потенциал заифлигини кўрсатувчи омил **УКК** қийматнинг 1 га яқинлиги ҳисобланади ва у шифрлаш алгоритмини тўлиқ танлов усули ёрдамида биз танлаган шартлар (чекловлар) дан бироз кўпроқ ҳисоблаш қийинчилиги билан амалий очиш мумкинлигини билдиради.

ГОСТ 28147-89 алгоритми учун эса, **УКК** қиймати қуйидагига тенг бўлади:

$$F_{\Sigma}\left(GOST\right)=\frac{1}{\left(1+\frac{2^{64}}{2^{30}}\right)*\left(1+\frac{2^{248}}{2^{54}}\right)}+\frac{1}{1*\left(1+\frac{2^{256}}{2^{54}}\right)},$$

$$F_{\Sigma}\left(GOST\right)\approx 2.31e-69+1.5e-61\approx 1.555e-61$$

Мазкур алгоритм учун ҳисобланган **УКК** қиймати 1 дан жуда узоқда бўлиб, хатто ўрнатилган чекловларни ўзгартириш натижасида ҳам шифрни очиш имконияти мавжуд эмас, яъни ГОСТ 28147-89 шифрлаш алгоритми бугунги кунда етарлича криптобардошли ҳисобланар экан.

Назорат саволлари

1. Қандай шарт бажарилганда**,** шифр криптобардошсиз ҳисобаланади?

2. Умумий криптобардошлилик кўрсатгичи тушунчасининг асосий моҳияти нимадан иборат?

3. Умумий криптобардошлилик кўрсатгичи деб номланувчи катталик қайси турдаги криптотаҳлил усуллари учун аниқланади?

4. Умумий криптобардошлилик кўрсатгичи формуласи ҳақида маълумот беринг.

5. Умумий криптобардошлилик кўрсатгичи қабул қилиши мумкин бўлган қийматларнинг шифрлаш алгоритми бардошлилиги билан боғлиқ жиҳатларини тушунтиринг.

6. Умумий криптобардошлилик кўрсатгичи қандай қиймат қабул қилса, блокли шифрлаш алгоритми ҳеч бўлмаганда битта криптотаҳли усулига заиф ҳисобаланади?

7. Умумий криптобардошлилик кўрсатгичи тушунчаси физик маъноси нимадан иборат?

8. DES алгоритми криптобардошлилигини умумий криптобардошлилик кўрсатгичи асосида таҳлил қилиш қадамларини тушунтиринг ва улар бўйича олинган хулосаларни изоҳланг.

9. ГОСТ28147-89 алгоритми криптобардошлилигини умумий криптобардошлилик кўрсатгичи асосида таҳлил қилиш қадамларини тушунтиринг ва улар бўйича олинган хулосаларни изоҳланг.

10. Бирор шифрлаш алгоритми учун ҳисобланган умумий криптобардошлилик кўрсатгичи 0 ёки 1 (ёки 1 дан кичик) қийматларга тенг бўлса, улар қандай маъноларни англатади?

ХУЛОСА

Бугунги кунда мавжуд криптоҳужум усуллари таҳлилига кўра ҳар бир криптотаҳлил усули бирор шифрлаш алгоритмига нисбатан, яъни алгоритмнинг ўзига хос хусусиятлари ва мавжуд заифликларига таянган ҳолда ишлаб чиқилган.

Мавжуд усулларни янги яратилган ёки бошқа хусусиятларга эга бўлган шифрлаш алгоритмларига қўллаш ўз навбатида криптотаҳлилчидан уларни такомиллаштиришга қаратилган қўшимча билимларни талаб этади.

Амалиётда янги тузилиш схемаси ва акслантиришларга асосланган шундай блокли шифрлаш алгоритми яратиладики, унга нисбатан аввал мавжуд бўлган криптотаҳлил усулларини қўллаш имконияти мутлақо мавжуд бўлмайди. Мазкур ҳолат ушбу алгоритмнинг мавжуд криптотаҳлил усулларига бардошли бўлишини таъминласада, “алгоритм бардошли” деган хулосани олишга етарли эмас.

Янги ёндашув асосида яратилган алгоритмларнинг ўзига хос бўлган ва муаллиф томонидан аниқланмаган айрим заифликлари мавжуд бўлиши мумкин. Кейинчалик мазкур заифликларнинг криптотаҳлилчи томонидан аниқланиши эса, янги яратилган алгоритмни криптобардошсиз бўлишига олиб келади. Шу боис ҳам, криптография соҳасидаги мутахассислар томонидан асосан аввал ўрганилган ва яхши хусусиятларга (криптобардошли, осон ва арзон аппарат реализация қилинувчи, тезкор ишлай олувчи, мослашувчан) эга акслантириш ва схемалар асосидаги блокли симметрик шифрлаш алгоритмлари таклиф этилмоқда.

Ўқув қўлланмада келтирилган криптотаҳлил усуллари қўлланиши турли ёндашувларга асосланган шифрлаш алгоритмлари мисолида намуналар келтирилмаган бўлсада, улар туб моҳияти, баҳолаш босқичлари, натижаларига кўра алгоритм бардошлилиги якуний хулосаларини бериш имкон қадар умумийлик асосида баён этилди.

Тақдим этилган ўқув қўлланмадан ахборот хавфсизлиги ва криптология йўналишларида таълим олаётган талабалар, шунингдек Республикада блокли симметрик шифрлаш алгоритмларини криптотаҳлил усулларига бардошлилигини баҳолаш ва шифрлаш алгоритми амалий бардошлилиги йўналишида илмий-тадқиқот ишларини олиб борувчи илмий ходимлар фойдаланишлари мумкин.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Biham E., Dunkelman O., Keller N. Enhancing differential-linear cryptanalysis. In Y. Zheng, editor, Advances in Cryptology - Asiacrypt 2002, volume 2501 of Lecture Notes in Computer Science, pages 587–592. IACR, Springer, 2002.

2. Biryukov A., Wagner D. "Advanced Slide Attacks" in Advanced Cryptology EUROCRYPT 2000.

3. Biryukov A., Wagner D. "Slide Attacks" in Proceeding of Fast Software Encryption. Springer-Verlag 1999.

4. Biryukov A., Wagner D. Advanced Slide Attacks//Advances in Cryptology–Eurocrypt'2000//Lecture Notes in Computer Science. Springer-Verlag.–2000.-V.1807.- P.589.

5. Charnes C., O'Connor L., Pieprzyk J., Safavi-Naini R., Zeng Y. Comments on Soviet Encryption Algorithm // Advances in Cryptology – EUROCRYPT'94 // Lecture Notes in Computer Science. Springer-Verlag. – 1995. – V.950. – P. 433-438.

6. Cristoffersson P. Message authentication and encryption combined. Computers & Sucurity, 7(1), 1988.

7. Daemen J., Knudsen L., and Rijmen V., The block cipher square. In E. Biham, edi-tor, Fast Software Encryption 1997, pages 149–165. Springer-Verlag, 1997. Lecture Notes in Computer Science Volume 1267.

8. Determining Strengths for Public Keys Used for Exchanging Symmetric Keys, RFC 3766, H.Orman and P.Hoffman, 04/2004.

9. Diffie W., Hellman M. New directions in cryptography // IEEE Trans. Inform. Theory, Vol 22, 6 (1976). P. 644–654.

10. Fact Sheet Suite B Cryptography, NSA, 08/2015.

11. Federal Information Processing Standards Publication 46-2. Data encryption standard (DES). National Bureau of Standards, 1993 December 30.

12. Hellman M. and Langford S.K. Differential-linear cryptanalysis. In Y. Desmedt, editor, Advances in Cryptology - Crypto '94, volume 839 of Lecture Notes in Computer Science, pages 17–25. IACR, Springer, 1994.

13. Hu Y., Zhang Y., and Xiao G., "Integral cryptanalysis of SAFER+", Electronics Letters, vol.35, (no.17), IEE, 19 Aug. 1999, p.1458-1459.

14. Key Lengths, Arjen K. Lenstra, The Handbook of Information Security, 06/2004.

15. Knudsen L. and Wagner D., “Integral Cryptanalysis”, *Proceedings of FSE 2002*, Lecture Notes In Computer Science Vol.2365, pp.112-127, Springer-Verlag, Berlin, 2002.

16. Kryptographische Verfahren: Empfehlungen und Schlüssellängen, TR-02102-1 v2015-1, BSI, 02/2015.

17. Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI, 02/2014.

18. Muftic S., Kantardzic M. Some Problems of Information Generation during Data Retrieval from Files. Proc. ETAN Conf., Banja Luka, Yugoslavia, 1977.

19. Raphael Chung-Wei Phan, Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students. Published in Cryptologia, XXVI (4), 2002.

20. Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 3, NIST, 07/2012.

21. Rivest R.L. The RC5 Encryption Algorithm // "Fast Software Encryption", Second International Workshop Proc., LNCS vol. 1008, Springer-Verlag, 1995, pp. 86-96.

22. Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal Of Cryptology, vol. 14, p. 255-293, 2001.

23. Vergili I., Yücel M. Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen n×n S-Boxes, Turk J Elec Engin, Vol.9, No 2, pp. 137-145, 2001.

24. Арипов М.М., Пудовченко Ю. Основы криптологии.- Тошкент, 2004 г.

25. Авдошин С.М., Савельева А.А. Проблемы оценки криптозащищённости информационных систем.–Программная инженерия. Бизнес-информатика №2(04) –2008 г.

26. Акбаров Д.Е., Ясинский В.В. Математика в становлении науки криптологии. –Киев.: Политехника, 2001.-42 с.

27. Акбаров Д.Е., Нуриев Ш.З., Ахмадалиев Ш.Ш. Криптография асосларида математика. Фарғона, 2003. -48 б.

28. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланиши - Тошкент, “Ўзбекистон маркаси” нашриёти, 2009, 432 бет.

29. Акбаров Д.Е., Ҳасанов П.Ф., Ҳасанов Х.П., Аҳмедова О.П. Криптографиянинг математик асослари. Ўқув қўлланма - Тошкент, 2010, 210 бет.

30. Аҳмедова О.П. Параметрлар алгебраси асосида носимметрик криптотизимлар яратиш усули ва алгоритмлари // Номзодлик диссертация иши, Тошкент, 2007.

31. Алгоритм криптографического преобразования ГОСТ 28147-89, ИПК Издательство Стандартов, Москва, 1996 г.

32. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. – М., Гелиос АРВ, 2002. – 480 с.

33. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. - М., «Гелиос АРВ», 2006. – 376с.

34. Баричев С.Г., **Серов Р.Е.** Основы современной криптографии.Учебное пособие.-Москва: Лори Горячая Линия,-Телеком, 2002.-152 с.

35. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. МЦНМО, 2003.-328 с.

36. Ростовцев А.Г. Алгебраические основы криптографии.-СПБ.: Мир и Семья, Интерлайн, 200.

37. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. НПО «Профессионал», Санкт-Петербург. 2004г. - 478 с.

38. Ростовцев А.Г., Маховенко Е.Б. Введение в криптографию с открытым ключом.-СПб.: «Мир и Семья», 2001.-336 с.

39. Жуков А.Е. Нелинейность булевых функций: Курс лекций. – М., МГТУ, 2006 г.

40. Иванов М. Криптографические методы защиты информации в компьютерных системах и сетях. – М., «Кудиц-Образ», 2001, 368 стр.

41. Коблиц Н. Курс теории чисел и криптографии. – М. Научное изд-во ТВП, 2001г. – 261 с.

42. Каримов М.М., Ғаниев С.К., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. Т., Алоқачи, 2008, 282 бет.

43. Курьязов Д. М., Саттаров А.Б. Буль функцияларнинг алгебраик бордошлилик даражалари ва уларни узлуксиз ва блокли шифрларни криптотаҳлил қилиш масалаларида қўлланиш. Илмий-тадқиқот ҳисобот иши. Тошкент, 2015 й.- 120 бет.

44. Курьязов Д.М., Саттаров А.Б. ГОСТ 28147-89 шифрлаш алгоритми учун чизиқли-дифференциал криптотаҳлил усулини қўллаш ва унинг дастурий таъминотини яратиш. Илмий-тадқиқот ҳисобот иши, Тошкент, 2012 й. –82 бет.

45. Курьязов Д.М., Саттаров А.Б. Алгебраик криптотаҳлил усули ва унинг блокли симметрик шифрлаш алгоритмлари криптотаҳлил масалаларида қўлланишини тадқиқ қилиш. Илмий-тадқиқот ҳисобот иши, Тошкент, 2014 й. – 60 бет.

46. Қиличев Ж.Р. Алгебраик криптотаҳлил усули ва унинг ГОСТ 28147-89 шифрлаш алгоритмига қўлланишини тадқиқ этиш. Ахборот хавфсизлиги йўналиши бўйича магистр даражасидаги диссертация иши. Тошкент, 2015 й. – 113 бет.

47. Логачёв О.А., **Сальников А.А.**, **Ященко В.В.** Булевы функции в теории кодирования и криптологии. – М. Изд. МЦНМО, 2004. – 470 с.

48. Молдовян А.А., Молдавян Н.А., Гуц Н.Д., Изотов Б.В. Криптография Скоростные шифры . – Санк-Петербург, “БХВ-Петербург”, 2002. – 494 с.

49. Молдовян А.А., **Молдовян Н.А.**, **Советов Б.Я.** Криптография. – Санкт-Петербург, Изд. «Лань», 2001. – 224 с.

50. Молдавян А.А., Молдавян Н.А. Криптография от примитивов к синтезу алгоритмов. Санкт –Петербург «БХВ-Петербург» 2004 г. 448 с.

51. Молдавян А.А., Молдавян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005 г. 288 с.

52. Маховенко Е.Б. Теоретико-числовые методы в криптографии. Учебное пособие.- М.:Гелиос АРВ, 2006.-320 с.

53. Menezes A.,van Oorschot P, Vanstone S. Handbook of applied cryptography.CRC Press, 1997.Доступно с http://www.cacr.math.uwaterioo.ca/hac/.

54. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии: Учебное пособие. – Минск, ООО «Новое знание», 2003. – 382 с.

55. Ҳасанов П.Ф., Ҳасанов Х.П., Аҳмедова О.П., Давлетов А.Б. Криптотаҳлил ва унинг махсус усуллари. Ўқув қўлланма - Тошкент, 2010, 175 бет.

56. Ҳасанов Х.П. Токомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари.Тошкент, 2008 й., 208 бет.

57. Черемушкин А.В. Лекции по арифметическом алгоритмам в криптографии.-М.: МЦНО, 2002.

58. Панасенко С.П. Стандарт шифрования ГОСТ 28147-89. Обзор криптоаналитических исследований. URL: http://www.inssl. com/standart-ofcipher.

59. Романченко А.М. Метод оценивания результатов криптоанализа блочного шифра. Труды СПИИРАН. 2015. Вып. 2(39). ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн) // www.proceedings.spiiras.nw.ru.

60. Саттаров А.Б. Блокли симметрик шифрлаш алгоритмлари учун чизиқли-дифференциал криптотаҳлил усулини қўллаш ва унинг дастурий таъминотини яратиш. Ахборот хавфсизлиги йўналиши бўйича магистр даражасидаги диссертация иши. Тошкент, 2011 й., 100 бет.

61. Шеннон К. Теория связи в секретных системах // http://www.enlight.ru/ crypto/articles/shannon/shann__i.htm.

62. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М., Изд. ТРИУМФ, 2003. – 816 с.

63. Яхшибоев А.М. AES симметрик шифрлаш алгоритми учун интеграл криптотаҳлил усули. Ахборот хавфсизлиги йўналиши бўйича магистр даражасидаги диссертация иши. Тошкент, 2014 й., – 83 б.

64. http://ru.wikipedia.org/wiki/Кнудсен,_Ларс.

1-илова

DES блокли симметрик шифрлаш алгоритми

DES[2] (Data Encryption Standard) симметрик шифрлаш алгоритми 1974-76 йилларда яратилган бўлиб, 1980 йилда АҚШ Стандартлар ва технологиялар миллий институти NIST томонидан FIPS PUB 46 номи остида давлат стандарти сифатида қабул қилинган. DES алгоритми Фейстельь тармоғига асосланган ва 64-битли маълумотлар блокини турли ўрин алмаштиришлар ва акслантиришлар комбинациясига асосланиб 56 битли k калит билан шифрлашни амалга оширади.

Шифрлаш жараёни кирувчи блокни бошланғич ўрин алмаштириши, 16 марта шифрлаш циклни такрорланиши ҳамда охирги битларни ўрин алмаштиришидан иборат (1.1-расм). Алгоритмда келтирилган ўрин алмаштириш, кенгайтириш ва S-блок жадваллари фиксирланган бўлиб, улар алгоритм бажарилиши жараёнида ўзгартиришларсиз фойдаланилади.

Мазкур схемада фойдаланилган белгилашлар:

L_i ва R_i – 64 битли блокнинг чап ва ўнг қисмлари;

$\oplus$ – 2 модул бўйича қўшиш амали;

k_i – 48 битли i-цикл калитлари;

f – шифрлаш функцияси;

IP – бошланғич ўрин алмаштириш.

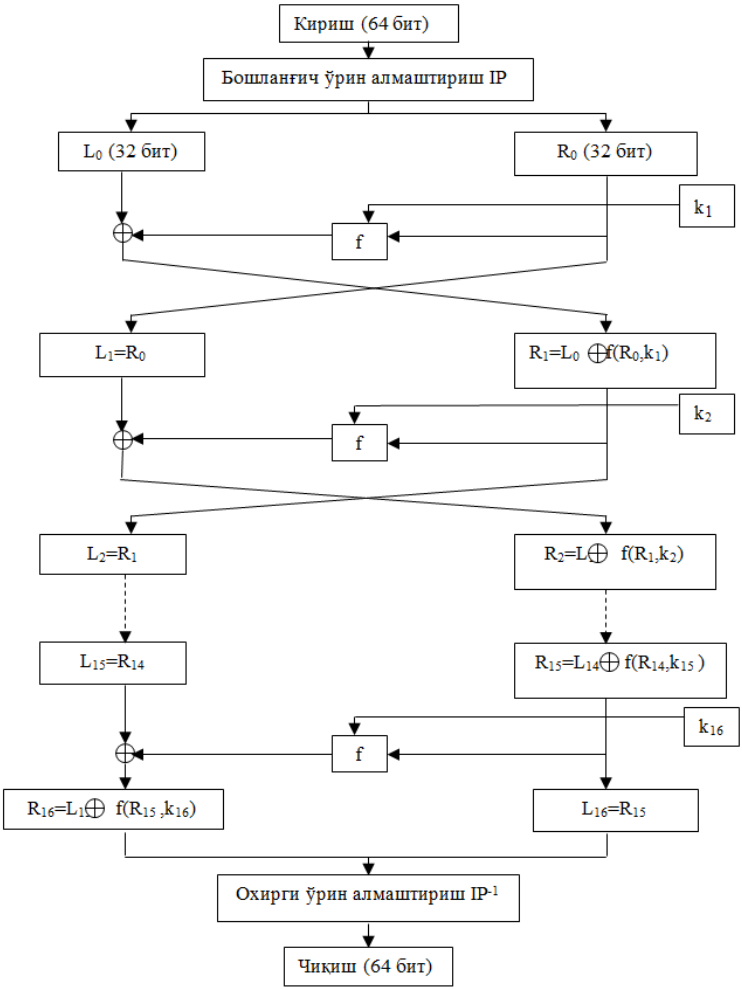
Маълумотнинг T блокини шифрлашда унинг барча битлари 1.1-жадвалга кўра IP бошланғич ўрин алмаштирилади.

1.1-жадвал.

IP алмаштириши

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

[2] FIPS 46-3/ Data Encryption Standard (DES) // http://www.csrc.nist.gov – Reaffirmed October 25, 1999.



1.1-расм. DES шифрлаш алгоритмининг блок-схемаси.

Бунда 58-бит *T* блокнинг 1-бити, 50-бит 2-бити ва ҳ.к, кўринишда ўрин алмаштириш бажарилади. Ўрин алмаштиришдан кейин ҳосил бўлган *IP(T)* блок мос равишда икки: L_0, 1-битдан 32-битгача ва R_0, 33-битдан 64-битгача бўлган блокларга ажралади. Кейин Фейстель акслантиришларига асосланган 16 марта такрорланувчи итератив шифрлаш жараёни бажарилади.

Айтайлик, $T_{i-1}=L_{i-1}R_{i-1}$ – (i-1) итерация натижаси бўлсин. У ҳолда, i-итерация натижаси $T_i = L_iR_i$ қуйидаги формуладан аниқланади:

$$L_i = R_{i-1};$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i), \quad i=1,\ldots,16.$$

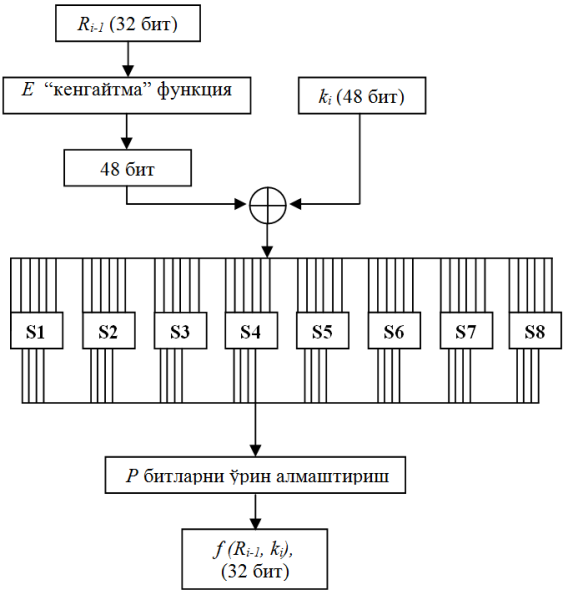
Бу ерда, f – шифрлаш функция аргументи 32 битли R_{i-1} вектор ва 56 битли шифрлаш k калитидан тегишли акслантиришлар асосида олинган 48 битли k_i калитдан иборат. $T_{16} = R_{16}L_{16}$ охирги итерация натижаси. Шифрлаш тугаши билан T_{16} қиймат устида IP^{-1} қайта ўрин алмаштириш бажарилади.

Шифрланган маълумотни очиқ матнга ўгириш (дешифрлаш) учун юқоридаги бажарилган ишлар тескари тартибда бажарилади, унинг математик модели қуйидаги формула билан аниқланади:

$$R_{i-1} = L_i;$$

$$L_{i-1} = R_i \oplus f(L_i, k_i), \quad i=16,\ldots,1.$$

$f(R_{i-1}, k_i)$ – шифрлаш функцияси қийматини ҳисоблаш схемаси 1.2-расмда тасвирланган.



1.2-расм. Алгоритм Фейстель функцияси схемаси.

f – шифрлаш функцияси қийматини ҳисоблашда E “кенгайтма” функцияси, S_1, S_2,....S_8 блоклар, P ўрин алмаштиришлардан фойдаланилади. R_{i-1}(32 бит) вектор ва k_i (48 бит) калитлар f - функция аргументи ҳисобланади.

E “кенгайтма” функция 32 битли R_{i-1} векторни 1.2-жадвал ёрдамида бир хил битларни такрорлаш орқали $E(R_{i-1})$ 48 битли вектор ҳосил қилади.

1.2-жадвал.

E - кенгайтма жадвали

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Масалан, 1.2-жадвалга мувофиқ $E(R_{i-1})$ векторнинг биринчи учта бити мос равшида R_{i-1} векторни 32, 1 ва 2-битлари, охирги учта бити эса R_{i-1} векторни 31, 32, 1-битлари ҳисобланади.

Ҳосил бўлган натижа мос раунд k_i калитга 2 модул бўйича қўшилади ва 6 битлик 8 та $B_1,B_2,...B_8$ блоклар кетма-кетлиги ҳосил қилинади.

$$E(R_{i-1}) \oplus k_i = B_1,B_2,...B_8 .$$

Сўнгра ҳар бир B_j блок 4-битли B'_j блокка мос S_j - жадвал ёрдамида алмаштирилади. S_j -блоклар рўйхати 1.3-жадвалда келтирилган.

1.3-жадвал.

S-блок жадваллари

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

1.3-жадвалнинг давоми

							S_3								
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
							S_4								
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
							S_5								
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
							S_6								
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
							S_7								
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
							S_8								
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Қуйида B_j блокнинг B'_j блокга ўзгартирилишини битта мисол орқали келтирамиз. Масалан, B_2 блок $\{111010_2\}$ тенг бўлсин. B_2 блок биринчи разряди a_1=1 ва охирги разряди a_6=0 дан ташкил топган $a=a_1a_6$ сонининг иккилик саноқ системасидаги ёзуви бўлса, бу соннинг ўнлик саноқ системасидаги қиймати 4 дан катта бўлмайди, яъни $0 \le a < 4$. Орадаги 4 та $b=a_2a_3a_4a_5=1101_2$ дан ташкил топган b сони эса $0 \le b < 16$ муносабатни қаноатлантиради. Натижада қаралаётган мисол учун a=2, b=13.

S_2 жадвал сатрлари 0 дан a гача бўлган сонлар билан устунлари эса 0 дан b гача бўлган сонларда рақамлаб чиқилган. Шундай қилиб, (a, b) сонлар жуфтлиги жадвалдаги a-сатр ва b-устун кесишмасида

турган бирор сонни аниқлайди. Мисолда (2, 13) сонлар жуфтлиги кесишмасида турган сон S_2 – жадвалга мувофиқ 3 га тенг. Ушбу сонни иккилик саноқ системасига ўтказиб, $B'_2 = \{0011_2\}$ ни ҳосил қиламиз.

$f(R_{i-1}, k_i)$ нинг қиймати, P битли ўрин алмаштиришларни 1.4-жадвалдан фойдаланиб ҳосил қилинади.

1.4-жадвал.

P – ўрин алмаштириш жадвали

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Ҳар бир итерацияда k_i (48 бит) калитнинг айни пайтдаги қиймати фойдаланилади. Ушбу қийматлар дастлабки k калитдан қуйидагича шакллантирилади.

Дастлаб фойдаланувчи ихтиёрий 56 бит узунликдаги калитни танлайди. 8,16,....64 - ўринларда турган 8 та бит калитга шундай қўшиладики ундаги ҳар бир байт тоқ сондаги бирлик рақамларини ўз ичига олсин. Бироқ ушбу битлар шифрлаш жараёнларида қатнашмайди. Бундай қоида бўйича калитларни генерация қилиш, уларни узатиш ва сақлаш жараёнида учрайдиган айрим хатоликларни аниқлаш имкониятларини тақдим этади. 56 бит калитда тегишли ўрин алмаштиришлар 1.5-жадвалга мувофиқ амалга оширилади.

1.5-жадвал.

Ўрин алмаштириш жадвали

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Ушбу ўрин алмаштириш ҳар бири 28 битдан иборат бўлган иккита C_0 ва D_0 блоклар билан аниқланади (улар мос равишда

жадвалнинг юқори ва пастки қисмларини эгаллаган). C_0 нинг учта олдинги битлари калитнинг 57, 49, 41 учта битларига мос келади ва жадвал асосида давом эттирилади. Кейин, индуктив йўл билан C_i ва D_i (i=1,…16) блоклар аниқланади. Агар C_{i-1} ва D_{i-1} блоклар аниқланган бўлса, у ҳолда C_i ва D_i блоклар уларни 1.6-жадвалга асосан бир ёки иккита чапга циклик суриш билан ҳосил қилинади.

1.6-жадвал.

Раунд калитлари учун суриш қийматлари

i-раунларсони	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Суришлар сони	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Энди, k_i ($1 \le i \le 16$) калитни аниқлаймиз. k_i калит 48 битдан ташкил топган бўлиб, улар 1.7-жадвалга асосан C_iD_i блок битларидан танлаб олинган. Таъкидлаш жойизки, C_iD_i блокдаги 56 битдан 8 таси (9,18,22,25,35,38,43,54 рақамли) k_i да йўқ.

1.7-жадвал.

Битларни танлаш жадвали

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

DES шифрлаш алгоритми 1997 йилда “Калитнинг барча мумкин бўлган вариантлари” бўйича амалга оширилувчи криптохужум усулига бардошсиз бўлганлиги сабаб, 2002 йил 26 майда RIJNDAEL шифри асосида AES FIPS-197 номи билан АҚШ янги стандарт шифрлаш алгоритми қабул қилинган.

2-илова

AES блокли симметрик шифрлаш алгоритми

AES FIPS-197[3] стандарт шифрлаш алгоритми SP-тармоқ асосида яратилган. Мазкур алгоритм ва байтлар устида амаллар бажаради. Шифрланиши лозим бўлган очиқ матн 128 бит бўлган блокларга ажратилиб, ҳар-бир блок мос равишда 16 байт сифатида қаралади. Ҳар бир байт эса $GF(2^8)$ чекли майдон элементларини ифодалайди. $GF(2^8)$ майдон элементларини даражаси 7 дан катта бўлмаган кўпҳад сифатида тасвирлаш мумкин. Агарда байтлар қуйидаги:

$$\{a_7a_6a_5a_4a_3a_2a_1a_0\},\ a_i \in \{0,1\},\ i = \overline{0...7}$$

кўринишда тасвирланган бўлса, у ҳолда, майдон элементлари қуйидагича кўпҳад кўринишида ифодаланади:

$$a_7 \cdot x^7 + a_6 \cdot x^6 + a_5 \cdot x^5 + a_4 \cdot x^4 + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0 .$$

Мисол учун, {11010101} байтга $x^7 + x^6 + x^4 + x^2 + a_0$ кўринишдаги кўпҳад мос келади.

Шунингдек, алгоритмда $GF(2^8)$ майдон элементлари учун аддитивлик ва мультипликативлик хоссаларига эга бўлган қўшиш ва кўпайтириш амаллари аниқланган.

Кўпҳадларни қўшиш. AES алгоритмида кўпҳадларни қўшиш $\oplus$ **(XOR)** (берилган кўпҳадларга мос келувчи иккилик саноқ системасидаги сонлар мос битларини mod 2 бўйича қўшиш) амали орқали бажарилади. Масалан $x^7 + x^6 + x^4 + x^2 + x$ ва $x^7 + x^5 + x^3 + x + 1$ кўпҳадлар натижаси қуйидагича ҳисобланади:

$$(x^7 + x^6 + x^4 + x^2 + x) \oplus (x^7 + x^5 + x^3 + x + 1) = (x^6 + x^5 + x^4 + x^3 + x^2 + 1)$$

Ушбу амал иккилик ва ўн олтилик саноқ системаларида қуйидагича ифодаланади:

$$\{11010110\}_2 \oplus \{10101011\}_2 = \{01111101\}_2 \text{ ва } D6_{16} \oplus AB_{16} = 7D_{16}.$$

Чекли майдонда исталган нолга тенг бўлмаган a элемент учун унга тескари бўлган $-a$ элемент мавжуд ва $a + (-a) = 0$ тенглик

[3] FIPS Publication 197. Specification for the Advanced Encryption Standard // http://www.csrc.nist.gov – November 26, 2001.

ўринли. Бу ерда нол элементи сифатида $\{00\}_{16}$ қаралади. $GF(2^8)$ майдонда $a \oplus a = 0$ тенглик ўринли.

Кўпҳадларни кўпайтириш. AES алгоритмида кўпҳадларни кўпайтириш қуйидагича амалга оширилади:

- иккита кўпҳад ўнлик саноқ системасида кўпайтирилади;
- еттинчи даражадан катта бўлган ҳар қандай кўпҳадни саккизинчи даражали $\varphi(x) = x^8 + x^4 + x^3 + x + 1$ келтирилмайдиган кўпҳадга бўлганда қолдиқда етти ва ундан кичик бўлган даражадаги кўпҳадлар ҳосил бўлиб, улар натижа сифатида олинади, бунда бўлиш жараёнида бажариладиган айириш амали иккилик саноқ системасида, юқорида келтирилгани каби $\oplus$ амали асосида бажарилади.

Ушбу киритилган кўпайтириш амалини $\bullet$ билан белгилаймиз.

Масалан, $(x^6 + x^4 + x^2 + x + 1)$ ва $(x^7 + x + 1)$ кўпҳадлар қуйидагича кўпайтирилади:

- бу кўпҳадлар ўнлик саноқ системасида кўпайтирилади:
$(x^6 + x^4 + x^2 + x + 1) \bullet (x^7 + x + 1) = (x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1)$;

- натижа қаралаётган майдонда аниқланган қуйидаги $\varphi(x) = x^8 + x^4 + x^3 + x + 1$ келтирилмайдиган кўпҳадга бўлинади ва қолдиқ олинади

$$(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^7 + x^6 + 1)$$

Ҳақиқатан ҳам $(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) = (x^5 + x^3) \bullet$

$\bullet (x^8 + x^4 + x^3 + x + 1) \oplus (x^7 + x^6 + 1)$.

Ҳар қандай нолга тенг бўлмаган элемент учун $a \bullet 1 = a$, тенглик ўринли. $GF(2^8)$ майдонда бир элемент сифатида $\{01\}_{16}$ тушунилади.

Киритилган кўпайтириш амали умумий ҳолда қуйидагича бажарилади. Ихтиёрий еттинчи даражали:

$$a_7 x^7 + a_6 x^6 + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

кўпҳадни x га кўпайтириб, қуйидагига эга бўламиз:

$$a_7 x^8 + a_6 x^7 + a_5 x^6 + a_4 x^5 + a_3 x^4 + a_2 x^3 + a_1 x^2 + a_0 x.$$

Бу кўпҳадни $\varphi(x) = x^8 + x^4 + x^3 + x + 1 = 1\{1b\}$ модул бўйича ҳисоблаб, чекли $GF(2^8)$ майдонга тегишли элементни ҳосил

қиламиз. Бунинг учун a_7=1 бўлганда $\varphi(x)=x^8+x^4+x^3+x+1$ кўпҳадни юқорида олинган 8 даражали кўпҳаддан *XOR* амали билан айириш кифоя, яъни :

$(a_7\oplus 1)x^8+(a_6\oplus 0)x^7+(a_5\oplus 0)x^6+(a_4\oplus 0)x^5+(a_3\oplus 1)x^4+(a_2\oplus 1)x+$
$+(a_1\oplus 0)x^2+(a_0\oplus 1)x+1=(a_6\oplus 0)x^7+(a_5\oplus 0)x^6+(a_4\oplus 0)x^5+(a_3\oplus 1)x^4+ +(a_2$
$\oplus 1)x^3+(a_1\oplus 0)x^2+(a_0\oplus 1)x+1,$ бу ерда, a_7=1 бўлгани учун

$(a_7\oplus 1)x^8=(1\oplus 1)x^8=0.$

Агарда a_7=0 бўлса, у ҳолда, натижа $a_6 x^7+...+a_1x^2+ a_0 x$ кўпҳаднинг ўзи бўлади.

Айтайлик, *x time*( ) функция юқорида киритилган кўпайтириш амалига нисбатан берилган кўпҳадни *x* га кўпайтиришни ифодаласин. Ушбу функцияни *n* марта қўллаб x^n га кўпайтириш амали аниқланади. Бевосита ҳисоблаш билан қуйидагилар ўринли эканлигига ишонч ҳосил қилиш мумкин:

$\{57\}\bullet\{13\}=\{fe\},$

чунки

$\{57\}\bullet\{02\}=x\ time\ (\{57\})=\{ae\}$

$\{57\}\bullet\{04\}=x\ time\ (\{ae\})=\{47\}$

$\{57\}\bullet\{08\}=x\ time\ (\{47\})=\{8e\}$

$\{57\}\bullet\{10\}=x\ time\ (\{8e\})=\{07\},$

бундан,

$\{57\}\bullet\{13\}=\{57\}\bullet(\{01\}\oplus\{02\}\oplus\{10\})=\{57\}\oplus\{ae\}\oplus\{07\}=\{fe\}.$

Юқорида таъкидланганидек алгоритм акслантиришлари байтлар ва тўрт байтли сўзлар устида амал бажаради. Тўрт байтли сўзларни коэфицентлари $GF(2^8)$ чекли майдондан олинган даражаси учдан катта бўлмаган кўпҳадлар кўринишида ифодалаш мумкин:

$a(x)=a_3x^3+a_2x^2+a_1x+a_0,$

бу ерда, $a_i=(a_7^i a_6^i a_5^i a_4^i a_3^i a_2^i a_1^i a_0^i)$, $a_j^i\in\{0;1\}$, *i=0,1,2,3; j=0, 1, ...,7.*

Бу каби иккита кўпҳадларни қўшиш ўхшаш ҳадлари олдидаги коэффициентларни $\oplus$ амали билан қўшиш орқали амалга оширилади, яъни:

$a(x)+b(x)=(a_3\oplus b_3)x^3+(a_2\oplus b_2)x^2+(a_1\oplus b_1)x+(a_0\oplus b_0).$

Кўпайтириш амали қуйидагича амалга оширилади. Иккита тўрт байтли сўзлар мос кўпҳадлар билан ифодаланган бўлсин:

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \text{ ва } b(x) = b_3x^3 + b_2x^2 + b_1x + b_0.$$

Кўпайтириш натижаси олтинчи даражадан катта бўлмаган кўпҳад

$$a(x)\,b(x) = c(x) = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0,$$

бўлиб, бу ерда, $c_0 = a_0 \bullet b_0$, $c_1 = a_1 \bullet b_0 \oplus a_0 \bullet b_1$, $c_2 = a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2$, $c_3 = a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3$, $c_4 = a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3$, $c_5 = a_3 \bullet b_2 \oplus a_2 \bullet b_3$, $c_6 = a_3 \bullet b_3$.

Кўпайтириш натижаси тўрт байтли сўздан иборат бўлиши учун, учинчи даражадан катта бўлган ҳар қандай кўпҳадни тўртинчи даражали $\varphi(x) = x^4 + 1$ келтирилмайдиган кўпҳадга бўлганда қолдиқда учинчи ва ундан кичик бўлган даражадаги кўпҳадлар ҳосил бўлишини ҳисобга олган ҳолда, улар натижа сифатида олинади. Бунда бўлиш жараёнида бажариладиган айириш амали иккилик саноқ системасида, юқорида келтирилгани каби, $\oplus$ амали асосида бажарилади.

Қуйидаги ифода ўринли: $x^i \bmod (x^4 + 1) = x^{i \bmod 4}$.

Шундай қилиб, $a(x)$ ва $b(x)$ кўпҳадлар $\otimes$-кўпайтмасини ифодаловчи

$$a(x) \otimes b(x) = d(x) = d_3x^3 + d_2x^2 + d_1x + d_0,$$

натижавий $d(x)$ –кўпҳад коэфициентлари қуйидагича аниқланади:

$$d_0 = a_0 \bullet b_0 \oplus a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3,\ d_1 = a_1 \bullet b_0 \oplus a_0 \bullet b_1 \oplus a_3 \bullet b_2 \oplus a_2 \bullet b_3,$$

$$d_2 = a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2 \oplus a_3 \bullet b_3,\ d_3 = a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3.$$

Юқорида келтирилган амалларни матрица кўринишида қуйидагича ифодалаш мумкин:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \bullet \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Квадрат архитектурага эга AES блокли шифрлаш алгоритми ўзгарувчан узунликдаги калитлар орқали шифрланади. Калит узунлиги 128, 192 ёки 256 битга тенг бўлади. Ўқув қўлланмада AES

шифрлаш алгоритми блоклар узунлиги 128 бит бўлган ҳол кўриб чиқилган.

Блок ўлчами 128 битга тенг кириш, бу 16 байтли массив 4 та қатор ва 4 та устундан иборатдир (ҳар бир сатр ва ҳар бир устун бу ҳолда 32 разрядли (битли) сўз деб қаралади).

Шифрлаш учун кираётган маълумот байтлари:

$$s_{00}, s_{10}, s_{20}, s_{30}, s_{01}, s_{11}, s_{21}, s_{31}, s_{02}, s_{12}, s_{22}, s_{32}, s_{03}, s_{13}, s_{23}, s_{33},$$

кўринишида белгиланади.

Кириш маълумотлари қуйидаги 2.1-жадвалдаги квадрат массив кўринишида ифодаланади. Яъни байтларни тартиб билан устун бўйича тўлдириб борилади. Биринчи тўртта байт ($s_{00}, s_{10}, s_{20}, s_{30}$) биринчи устунга мос тушади, иккинчи тўртта байт ($s_{01}, s_{11}, s_{21}, s_{31}$) иккинчи устунга мос тушади, учинчи тўртта байт ($s_{02}, s_{12}, s_{22}, s_{32}$) учинчи устунга мос тушади, тўртинчи тўртта байт ($s_{03}, s_{13}, s_{23}, s_{33}$) тўртинчи устунга мос тушади.

2.1-жадвал.

Кириш маълумотлари ҳолат жадвали

s_{00}	s_{01}	s_{02}	s_{03}
s_{10}	s_{11}	s_{12}	s_{13}
s_{20}	s_{21}	s_{22}	s_{23}
s_{30}	s_{31}	s_{32}	s_{33}

Худди шундай тартибда шифрлаш калити ҳам квадрат жадвал шаклида киритилади. Улар 128 бит = 16 байт = 4 сўз (тўртта 32 битлик блок) дан иборат:

$$k_{00}, k_{10}, k_{20}, k_{30}, k_{01}, k_{11}, k_{21}, k_{31}, k_{02}, k_{12}, k_{22}, k_{32}, k_{03}, k_{13}, k_{23}, k_{33}\ .$$

2.2-жадвал.

Шифрлаш калити ҳолат жадвали

k_{00}	k_{01}	k_{02}	k_{03}
k_{10}	k_{11}	k_{12}	k_{13}
k_{20}	k_{21}	k_{22}	k_{23}
k_{30}	k_{31}	k_{32}	k_{33}

Шунингдек, AES шифрлаш алгоритми раундлар сони N_r ва калит узунлик N_k ларига боғлиқ ҳолда қўлланилади. Мазкур боғлиқлик қуйидаги 2.3-жадвалда келтирилган.

2.3-жадвал.

AES алгоритми калит узунлиги ва раундлар сонининг боғлиқлиги

Калит узунлиги (N_k)	*Раудлар сони (N_r)*
$N_k=4$ *128 бит*	*10*
$N_k=6$ *192 бит*	*12*
$N_k=8$ *256 бит*	*14*

AES шифрлаш алгоритми раунд акслантиришлари. Ҳар бир раунд шифрлаш жараёнлари қуйида келтирилган тўртта акслантиришлардан фойдаланилган ҳолда амалга оширилади:

1)***SubBytes*** – алгоритмда қайд этилган 16x16 ўлчамли жадвал асосида байтларни алмаштириш, яъни S -блок акслантиришларини амалга ошириш;

2) ***ShiftRows*** – алгоритмда берилган жадвалга кўра ҳолат байтларини циклик суриш;

3) ***MixColumns*** – устун элементларини аралаштириш, яъни алгоритмда берилган матрица бўйича кўпайтиришни амалга ошириш;

4) ***AddRoundKey*** **–** раунд калитларини қўшиш, яъни блоклар мос битларни ***XOR*** амали билан қўшиш.

Қуйида ушбу келтирилган акслантиришлар математик моделлари ва улар умумий қўлланиш схемалари келтирилади.

SubBytes **(S-блок акслантириш жадвали) –** акслантириши ҳар бир ҳолат байтларига боғлиқсиз ҳолда байтларни чизиқли бўлмаган амаллар асосида ўрин алмаштиради. Ушбу жараён иккита босқичдан иборат бўлиб:

а) ҳар бир s_{ij} ҳолат байт учун mod $(x^8+x^4+x^3+x+1)$ бўйича s_{ij}^{-1} тескариси қуйидаги формула орқали топилади:

$$s_{ij}s_{ij}^{-1} \equiv 1 \bmod (x^8+x^4+x^3+x+1);$$

б) ҳар бир s_{ij} элемент тескариси бўлган s_{ij}^{-1} ни $b = s_{ij}^{-1}$ деб, бир байтдан иборат b сонини унинг битлари орқали $b=(b_0,b_1,\ldots,b_7)$ тасвирлаб, унинг устида қуйидаги афин акслатириши бажарилади:

$$Cb + c \,(\bmod x^8 + 1) = b'.$$

Бу ерда, $C = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ матрица ва $c = (c_0, c_1, \ldots, c_7) =$ $(1,1,0,0,0,1,1,0)$ – вектор алгоритмда берилган ўзгармас ифодага эга бўлиб, кетирилган афин акслантириши

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} (\text{mod } 257) = \begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix}$$

кўринишда амалга оширилади.

Натижавий $b' = (b_0', b_1', \ldots, b_7')$ векторнинг координаталари

$$b_i' = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i, \quad i=0,1,2,\ldots,7;$$

ифода билан ҳисобланади.

Алгоритм дастурий таъминоти ва аппарат қурилмасини яратишда қулайлик туғдириш мақсадида а) ва б) қисмларда берилган барча мантиқий ва арифметик амалларни бажариш натижалари 2.4-жадвалда келтирилган *S*-блок шаклда тасвирланган.

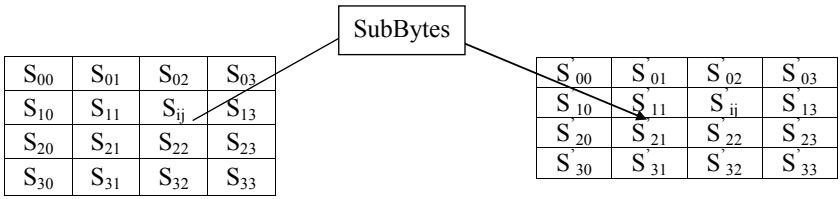
S-блок жадвалидан фойдаланиш қоидаси қуйидагича. Аввало, берилган s байт 16-лик саноқ системасида $s=(s_0 s_1 s_2 s_3 s_4 s_5 s_6 s_7) = \{s_0 s_1 s_2 s_3, s_4 s_5 s_6 s_7\} = \{xy\}$ каби ифодаланади, мазкур байтнинг SubBytes акслантириши бўйича натижаси сифатида *x*-сатр ва *y*-устунлар кесишмасидаги байт олинади. Мисол учун, SubBytes {62} = {*aa*} тенг.

2.4-жадвал.

S блок алмаштириш жадвали

x	*y*															
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
0	63	7c	77	7b	12	6b	6f	c5	30	01	67	2b	fe	d7	*a*b	76
1	c*a*	82	c9	7d	f*a*	59	47	f0	*a*d	d4	*a*2	*a*f	9c	*a*4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	*a*5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9*a*	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	62	5*a*	*a*0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6*a*	cb	be	39	4*a*	4c	58	cf
6	d0	ef	*aa*	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	*a*8
7	51	*a*3	40	8f	92	9d	38	f5	bc	b6	d*a*	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	*a*7	7e	3d	64	5d	18	73
9	60	81	4f	dc	22	2*a*	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	*ac*	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	*a*9	6c	56	f4	e*a*	65	7*a*	*ae*	08
c	b*a*	78	25	2e	1c	*a*6	b4	c6	e8	dd	74	1f	4d	bd	8b	8*a*
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

SubBytes (S -блок акслантиришлари жадвали) байтларни алмаштириш жараёни умумий схемасини қуйидагича тасвирлаш мумкин



ShiftRows **(Ҳолат байтларини циклик суриш)** акслантириши қўлланиши қуйидагича амалга оширилади. Ҳолат байтларини циклик суришда ҳолат жадвали сатрлари қуйидагича белгилаб олинади.

2.5-жадвал.

Ҳолат жадвали

0-сатр	S'_{00}	S'_{01}	S'_{02}	S'_{03}
1-сатр	S'_{10}	S'_{11}	S'_{12}	S'_{13}
2–сатр	S'_{20}	S'_{21}	S'_{22}	S'_{23}
3-сатр	S'_{30}	S'_{31}	S'_{32}	S'_{33}

ShiftRows акслантиришида жадвалдаги охирги учта сатр ҳар бир байтлари чапга циклик, яъни 1-сатр 1 байтга, 2-сатр 2 байтга, 3-сатр 3 байтга сурилади.

2.6-жадвалда сатрларни циклик суриш бажарилгандан кейинги байтлар ўрни қай тарзда ўзгариши кўрсатилган.

2.7-жадвал.

Ҳолат байтларини циклик суриш жадвали

S'_{00}	S'_{01}	S'_{02}	S'_{03}	*ShiftRows* →	S'_{00}	S'_{01}	S'_{02}	S'_{03}
S'_{10}	S'_{11}	S'_{12}	S'_{13}		S'_{11}	S'_{12}	S'_{13}	S'_{10}
S'_{20}	S'_{21}	S'_{22}	S'_{23}		S'_{22}	S'_{23}	S'_{20}	S'_{21}
S'_{30}	S'_{31}	S'_{32}	S'_{33}		S'_{33}	S'_{30}	S'_{31}	S'_{32}

***MixColumns* (Устун элементларини аралаштириш) акслантиришида** ҳар-бир ҳолат устун элементлари учинчи даражадан катта бўлмаган кўпҳаднинг коэффицентлари сифатида ифодаланиб, ушбу

$$g(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

кўпҳадга x^4+1 модуль бўйича кўпайтирилади.

Қуйидагича белгилаш киритамиз:

$$s_{00} = s'_{00}, s_{10} = s'_{11}, s_{20} = s'_{22}, s_{30} = s'_{33},$$
$$s_{01} = s'_{01}, s_{11} = s'_{12}, s_{21} = s'_{23}, s_{31} = s'_{30},$$
$$s_{02} = s'_{02}, s_{12} = s'_{13}, s_{22} = s'_{20}, s_{32} = s'_{31},$$
$$s_{03} = s'_{03}, s_{13} = s'_{10}, s_{23} = s'_{21}, s_{33} = s'_{32}$$

Натижада кўпҳадлар кўпайтмасининг матрицалар кўринишидаги ифодаси қуйидагича:

$$\begin{bmatrix} s'_{0j} \\ s'_{1j} \\ s'_{2j} \\ s'_{3j} \end{bmatrix} = \begin{bmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{bmatrix} \bullet \begin{bmatrix} s_{0j} \\ s_{1j} \\ s_{2j} \\ s_{3j} \end{bmatrix}, 0 \le c \le 3,$$

бўлади, бу ерда, c – устун номери.

Охирги тенглик:

$$s'_{0c} = (\{02\} \bullet s_{0c}) \oplus (\{03\} \bullet s_{1c}) \oplus s_{2c} \oplus s_{3c},$$
$$s'_{1c} = s_{0c} \oplus (\{02\} \bullet s_{1c}) \oplus (\{03\} \bullet s_{2c}) \oplus s_{3c},$$
$$s'_{2c} = s_{0c} \oplus s_{1c} \oplus (\{02\} \bullet s_{2c}) \oplus (\{03\} \bullet s_{3c}),$$
$$s'_{3c} = (\{03\} \bullet s_{0c}) \oplus s_{1c} \oplus s_{2c} \oplus (\{02\} \bullet s_{3c},$$

тенгликларга эквивалент.

AddRoundKey **(Раунд калитларини қўшиш) акслантириш**да ҳолат блокининг битлари калит блоки мос битлари билан характеристикаси икки бўлган чекли майдонда қўшилади, яъни, массив ҳар бир устуни ва шу устун элементлари калит массиви мос устун ва элементларига XOR амали билан қўшилади.

Раунд калитларини ишлаб чиқиш алгоритми (*Key Schedule*)

Раунд калитлари дастлабки калитдан, алгоритмда кўзда тутилган барча раундлар учун яратиб олинади. Ушбу жараён:

- калитни кенгайтириш (**Key Expansion**)
- раунд калитларини танлаш (**Round Key Selection**);

босқичларидан иборат.

Раунд калитлари умумий битлари сони кириш маълумоти битлари сонини (l) раунд сонига кўпайтмасига ва яна битта кириш маълумотининг битлари сонини йиғиндисига тенг. 10 раундли шифрлаш алгоритми учун 128*10+128=1408 бит раунд калити керак бўлади, яъни $l(N_r+1)=128 \cdot 11=1408$ бит.

Демак, 128 бит узунликдаги блок ва 10 раунд учун 1408 бит раунд калитлари талаб қилинади.

Дастлаб калитни кенгайтиришда, 128 битли (16 байт, символ) бошланғич кирувчи калитни тўртта (w_1, w_2, w_3, w_4) 32 битдан бўлган бўлакка бўлинади. Қолган кенгайтирилган калитлар мана шу тўртта (w_1, w_2, w_3, w_4) кенгайтирилган калитлар ёрдамида топилади. Яъни кенгайтирилган калитлар (2.1) ва (2.2) формулалар асосида ҳисоблаб топилади. Кенгайтирилган калитлар сони эса қуйидагича аниқланади:

$$N[w(i)] = 4(N_r + 1).$$

Биз кўраётган ҳолатда N_r=10 га тенг. Буни билган ҳолда $N[w(i)]$ топилади:

$$N[w(i)] = 4*(10+1) = 44$$

Демак, 10 та раундга эга бўлган шифрлаш учун 44 та кенгайтирилган калитлар керак бўлар экан.

Раунд калитлари кенгайтирилган калитлардан қуйида баён қилинган қоида асосида яратилади. Калитлар генерациясининг формулалари қуйидаги кўринишларга эга:

$$w[i] = w[i-1] \oplus w[i-N_k], \qquad (2.1)$$

ва

$$w[i] = SubWord\,(RotWord\,(w[i-1]))\oplus Rcon[\,i/N_k]\oplus w[i-N_k]. \qquad (2.2)$$

Демак, i=4,8,12,16,20,… қийматлар учун (2.2) формуладан фойдаланиб, кенгайтирилган калитлар топилади. Яъни i нинг 4 га каррали, 4 га қолдиқсиз бўлинадиган қийматларида (2.2) формуладан фойдаланилади. Қолган барча i=5,6,7,9,10,11,13,... қийматларида (2.1) формуладан фойдаланилади. Бу ерда $w(i)$ – 32 бит сўзлардан иборат.

Масалан, раунд калитининг узунлиги 128 бит бўлганда, у тўртта кенгайтирилган калитга тенг бўлади, яъни:

$$128 : 32 = 4 \text{ демак, } \quad w(i) = 1,2,3,4$$

$w_1 = W_1, W_2, W_3, W_4, W_5, W_6, W_7, W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{15}, W_{16}, W_{17}, W_{18}, W_{19}, W_{20}, W_{21}, W_{22}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}, W_{29}, W_{30}, W_{31}, W_{32};$

$w_2 = W_{33}, W_{34}, W_{35}, W_{36}, W_{37}, W_{38}, W_{39}, W_{40}, W_{41}, W_{42}, W_{43}, W_{44}, W_{45}, W_{46}, W_{47}, W_{48}, W_{49}, W_{50}, W_{51}, W_{52}, W_{53}, W_{54}, W_{55}, W_{56}, W_{57}, W_{58}, W_{59}, W_{60}, W_{61}, W_{62}, W_{63}, W_{64};$

$w_3 = W_{65}, W_{66}, W_{67}, W_{68}, W_{69}, W_7, W_{71}, W_{72}, W_{73}, W_{74}, W_{75}, W_{76}, W_{77}, W_{78}, W_{79}, W_8, W_{81}, W_{82}, W_{83}, W_{84}, W_{85}, W_{86}, W_{87}, W_{88}, W_{89}, W_9, W_{91}, W_{92}, W_{93}, W_{94}, W_{95}, W_{96};$

$w_4 = W_{97}, W_{98}, W_{99}, W_{100}, W_{101}, W_{102}, W_{103}, W_{104}, W_{105}, W_{106}, W_{107}, W_{108}, W_{109}, W_{110}, W_{111}, W_{112}, W_{113}, W_{114}, W_{115}, W_{116}, W_{117}, W_{118}, W_{119}, W_{120}, W_{121}, W_{122}, W_{123}, W_{124}, W_{125}, W_{126}, W_{127}, W_{128};$

2.8-жадвал.

Алгоритм барча раунд калитлари

0 – раунд калити, кириш калити	$w_0, w_1, w_2, w_3.$

2.8-жадвалнинг давоми

1 – раунд калити	$\boldsymbol{w_4}$, w_5, w_6, w_7.
2 – раунд калити	$\boldsymbol{w_8}$, w_9, w_{10}, w_{11}.
3 – раунд калити	$\boldsymbol{w_{12}}$, w_{13}, w_{14}, w_{15}.
4 – раунд калити	$\boldsymbol{w_{16}}$, w_{17}, w_{18}, w_{19}.
5 – раунд калити	$\boldsymbol{w_{20}}$, w_{21}, w_{22}, w_{23}.
6 – раунд калити	$\boldsymbol{w_{24}}$, w_{25}, w_{26}, w_{27}.
7 – раунд калити	$\boldsymbol{w_{28}}$, w_{29}, w_{30}, w_{31}.
8 – раунд калити	$\boldsymbol{w_{32}}$, w_{33}, w_{34}, w_{35}.
9 – раунд калити	$\boldsymbol{w_{36}}$, w_{37}, w_{38}, w_{39}.
10 – раунд калити	$\boldsymbol{w_{40}}$, w_{41}, w_{42}, w_{43}.

2.8-жадвалда раунд калитлари келтирилган бўлиб, 0 – раунд калити бошланғич кириш калити ҳисобланади, тўқ қора ранг билан берилган кенгайтирилган калитлар (2.2) формуладан ҳисоблаб олинади, қолган калитлар эса (2.1) формуладан ҳисоблаб топилади.

(2.2) формуладаги акслантиришлар қуйидаги функциялар асосида амалга оширилади:

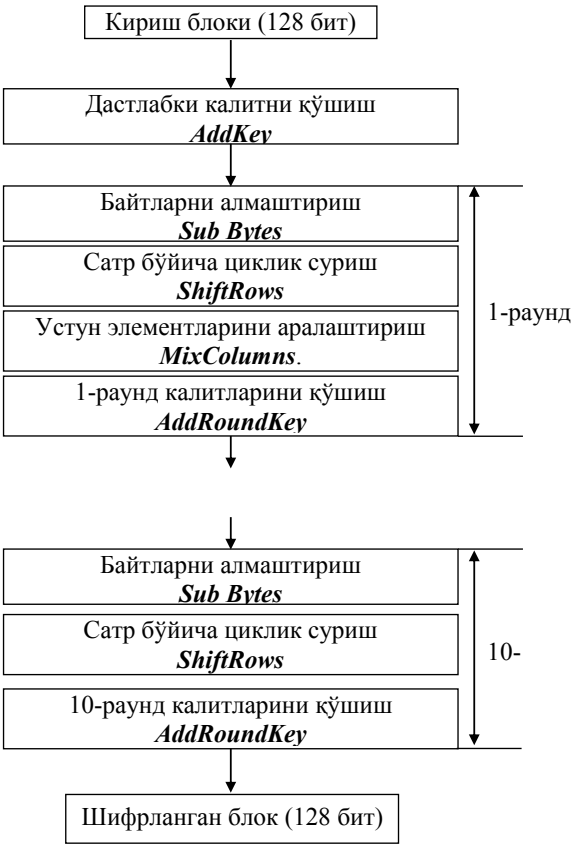
• ***RotWord*** — 32 битли сўзни байт бўйича қуйидаги кўринишда суриш бажарилади.

$$\{a_0\, a_1\, a_2\, a_3\} \rightarrow \{a_1\, a_2\, a_3\, a_0\};$$

• ***SubWord*** — S блокдан ва ***SubBytes*** функциясидан фойдаланган ҳолда байт бўйича акслантириш бажарилади.

• ***Rcon*** *[j]* = 2^{j-1}, бу ерда $j=(i/N_k)$, i/N_k – бўлиш натижаси бутун сон чиқади, чунки N_k =const бўлиб, i нинг N_k га каррали қийматлари учун бўлиш амали бажарилади.

Қуйида AES алгоритми шифрлаш жараёни блок схемаси келтирилган**:**


Кириш блоки (128 бит)
Дастлабки калитни қўшиш
AddKey
Байтларни алмаштириш
Sub Bytes
Сатр бўйича циклик суриш
ShiftRows
Устун элементларини аралаштириш
MixColumns.
1-раунд калитларини қўшиш
AddRoundKey
1-раунд
Байтларни алмаштириш
Sub Bytes
Сатр бўйича циклик суриш
ShiftRows
10-раунд калитларини қўшиш
AddRoundKey
10-
Шифрланган блок (128 бит)

3-илова

ГОСТ 28147-89 блокли симметрик шифрлаш алгоритми

1978 йили Собиқ иттифоқда стандарт криптоалгоритм яратиш бўйича гуруҳ ташкил этилиб, гуруҳ аъзоларига қуйидаги талабларни қаноатлантирувчи алгоритм яратиш юклатилган:

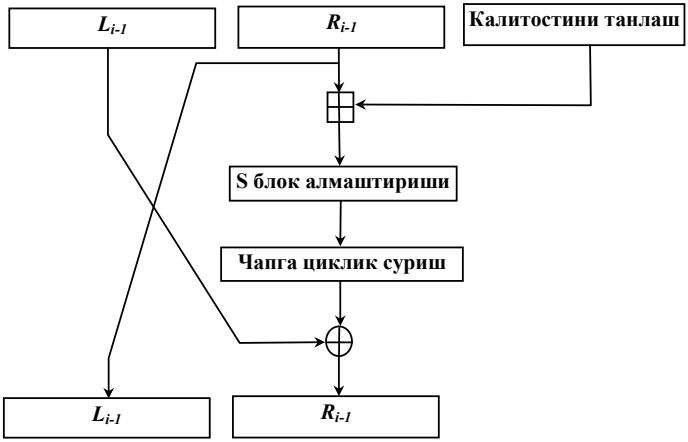
- алгоритмда бажариладиган амаллар компьютер ҳисоблаш имкониятлари билан уйғунлаша олиши (масалан, берилганлар қийматлари ва улар бўйича алгоритм ҳисоблаш натижалари иккилик кўринишда 32 разрядлидан катта бўлмаслиги);
- алгоритм очиқ бўлиши, бардошлилиги алгоритм сир тутилишига эмас, балки сеанс калитига боғлиқ бўлиши.

Гуруҳ аъзолари изланишлари натижасида 1980-1983 йилларда Фейстель тармоғи асосидаги ГОСТ 28147-89[4] стандарт блокли симметрик шифрлаш алгоритми ишлаб чиқилган ва маълум давргача кенг оммадан сир тутилган. Мазкур алгоритм собиқ иттифоқ стандартлаштириш давлат қўмитасининг 1989 йилдаги тегишли қарори билан тасдиқланган. Ушбу алгоритм махфийлик даражаси ихтиёрий бўлган ахборотни ҳеч қандай чекловсиз шифрлаш имконини беради.

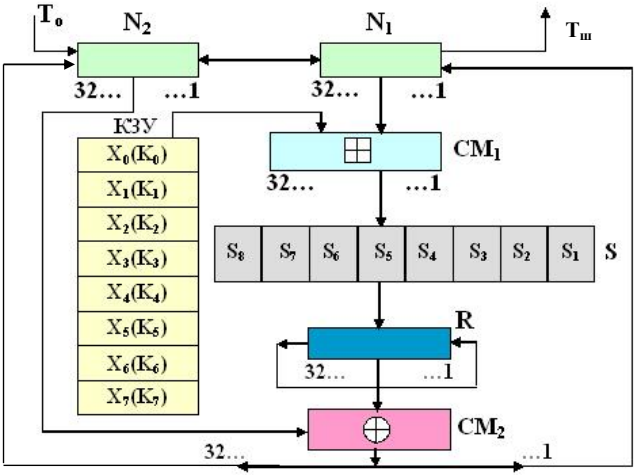
Стандарт бир-биридан айрим фарқларга эга бўлган 4 та ишлаш режимига эга. Булар: оддий алмаштириш, гаммалаш, тескари боғланишли гаммалаш ва имитовставкадан иборат. ГОСТ28147-89 шифрлаш алгоритмида *i*-раунд бажарилиш блок-схемаси 3.1-расмда келтирилган.

Оддий алмаштириш режими. ГОСТ 28147-89 шифрлаш алгоритми 64 битли маълумотлар блокини 256 бит узунликдаги калит билан шифрлайди. Бундан ташқари, алгоритмда қўшимча калитлардан фойдаланиш ҳам кўзда тутилган. Алгоритм 32 раундлик шифрлашни амалга оширади. Дастлаб, шифрланувчи 64 битлик маълумот, ҳар бири 32 битдан иборат бўлган N_1 ва N_2 блокларга ажратилади (Фейстель тармоғи хусусиятига кўра). ГОСТ 28147-89 шифрлаш алгоритмининг оддий ўрин алмаштириш усулидаги схемаси 3.2-расмда келтирилган.

[4] ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989.



3.1-расм. і-раунд бажарилиш блок-схемаси.



3.2-расм. ГОСТ 28147-89 шифрлаш алгоритми схемаси.

Мазкур схемада фойдаланилган белгилашлар:

T_o, $T_ш$ – мос равишда очиқ ва шифр маълумот;

N_1, N_2 – 32 разрядли регистрлар;

$СМ_1$ – сумматор 2^{32} модул бўйича қўшиш;

$СМ_2$ – сумматор 2 модул бўйича қўшиш;

R – 32 разрядли регисторда 11 бит циклик суриш;

КЗУ – 256 бит хажмдаги калитларни сақлашга қаратилган хотира воситаси;

S – ўрин алмаштириш блоклари.

Ушбу алгоритм Фейстель тармоғига асосланганлиги сабаб, унинг шифрлаш жараёнида, ҳар бир *i*-раундда k_i раунд калитдан фойдаланиб, қуйидаги амаллар бажарилади:

$L_i=R_{i-1}$;

$R_i=L_{i-1}\oplus f(R_{i-1}, k_i)$,

бу ерда, *f* – функция R_{i-1} ўнг 32 битлик блокни mod 2^{32} бўйича, 32 битли k_i раунд калитга қўшади. Бу натижа 8 та 4 битлик маълумотларга ажратилади, олинган ҳар бир 4 битлик маълумотлар 0 дан 15 гача бўлган сонларни ифодалаб, мос равишда алгоритмда кўрсатилган 8 та *S* блокларга берилади. Биринчи 4 битлик маълумот S_1 блокга, иккинчи 4 битлик маълумот S_2 блокга ва кейингилари шу тартибда давом этади.

Ҳар бир *S* блок 0 дан 15 гача бўлган сонларнинг такрорланмайдиган жойлашувидан иборат. Алгоритмда *S* блоклар махфий сақланиши таъкидлаб ўтилган. Қуйида Россия марказий банки томонидан фойдаланиб келинган *S* блоклар келтирилган:

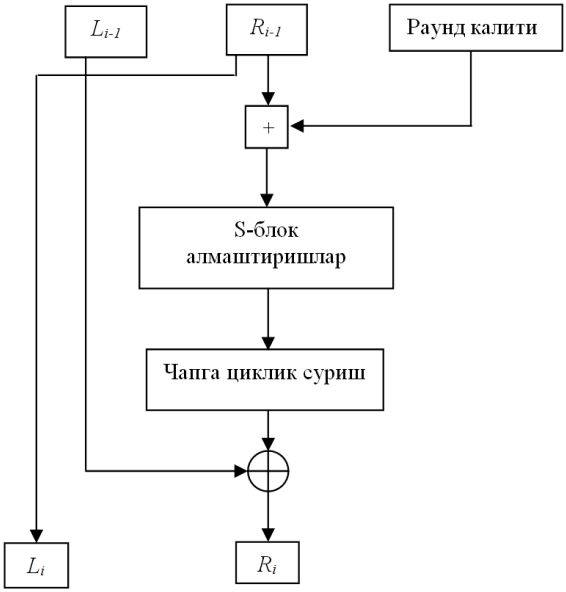
S_1:	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
S_2:	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
S_3:	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
S_4:	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
S_5:	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
S_6:	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S_7:	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S_8:	1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

Алгоритмнинг *i*-раунд схемаси 3.3-расмда келтирилган.

S-блок алммаштириши қуйидагича бажарилади. Масалан, бирор S_4 блокка 4 битдан иборат бўлган 0111_2 маълумот берилган бўлса, унинг ўнлик саноқ системасидаги ифодаси 7 бўлгани учун *S* блокдан чиқувчи ифодаси 1111_2 бўлади. Сабаби, S_4 блокнинг 7 - устинида 15 сони турибди.

Мисолда кўрсатилганидек, 8 та *S* блокларга 4 битдан берилган 32 битли маълумот, мос равишда акслантирилиб, 8 та *S* блоклардан ҳар бири 4 битдан иборат бўлган 32 битлик маълумот чиқади. Бу

чиққан маълумот чапга 11 бит циклик сурилади, сўнгра 32 битлик L_{i-1} чап блок билан mod 2 бўйича қўшилиб, натижа R_i ўнг блокга ёзилади, ўнг R_{i-1} блок эса, L_i чап блокга ўтади.



3.3-расм. і - раунд блок-схемаси.

32 битлик ҳар бир раунд калитлари дастлабки берилган 256 битлик калитга кўра қуйидаги тартибда раундларда фойдаланилади:

Раундлар	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Калитлар	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8
Раундлар	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Калитлар	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_8	k_7	k_6	k_5	k_4	k_3	k_2	k_1

Раундларда калитлардан фойдаланиш тартибига кўра, 1 – 24 раундлар оралиғида калитлардан фойдаланиш тартиби бир хилда такрорланади, 25 – 32 раундлар оралиғида калитлар тескари тартибда фойдаланилади.

Гаммалаш режимида – дастлабки битлар кетма-кетлиги гамма битлар кетма-кетлиги билан mod 2 амали бўйича қўшилади. Гамма эса оддий алмаштириш тартибига кўра ҳосил қилинади. Гаммани шакллантиришда иккита махсус доимий сон ҳамда 64 хонали

иккилик кетма-кетлик синхрописилкадан фойдаланилади. Ахборотни фақат синхропосилка борлигида дешифрлаш мумкин. Синхропосилка махфий бўлмаган ва очиқ ҳолда компьютер хотирасида сақланиши ёки алоқа канали орқали узатилиши мумкин бўлган параметр ҳисобланади.

Тескари боғланишли гаммалаш режимида – жараён гаммалаш ҳолатидан фақат шифрлашни биринчи қадамидаги ҳаракатлар билан фарқланади.

Имитовставка режими – дастлабки ахборотни ва махфий калитни ўзгартириш функцияси ҳисобланади. У *k* бит узунликдаги иккилик кетма-кетликдан иборат бўлиб, *k* нинг қиймати нотўғри ахборотнинг зўрлаб киритилиш эҳтимоллиги $P_{зк}$ билан $P_{зк}=1/2^k$ муносабат орқали боғланган. Имитовставкани шакллантириш методи қуйидаги босқичлар кетма-кетлигидан иборат:

Очиқ маълумот 64 битли T(i) (i=1,2,3,….m) блокларга ажратилади, бу ерда, m – шифрланувчи маълумот ҳажми орқали аниқланади. Биринчи блок T(1) оддий алмаштириш методи биринчи 16 итерацияларига биноан ўзгартирилади. Калит сифатида дастлабки маълумот шифрланишида ишлатиладиган калит олинади. Олинган 64 битли иккилик сўз иккинчи блок T(2) билан mod 2 бўйича қўшилади. T(1) блок устида қандай итерацион ўзгартиришлар бажарилган бўлса, жамлаш натижаси устида ҳам худди шундай ўзгартиришлар амалга оширилади ва охирида T(3) блок билан mod 2 бўйича қўшилади. Бундай ҳаракатлар дастлабки маълумотнинг (m-1) блоки бўйича такрорланади. Агар охирги T(m) блок тўлиқ бўлмаса, у 64 хонагача ноллар билан тўлдирилади. Бу блок T(m-1) блок ишланиш натижаси билан mod 2 бўйича қўшилади ва оддий алмаштириш методининг биринчи 16 итерациялари бўйича ўзгартирилади. Ҳосил бўлган 64 хонали блокдан k бит узунликдаги сўз ажратиб олинади ва бу сўз имитовставка деб эълон қилинади. Имитовставка шифрланган маълумотнинг охирига жойлаштирилади. Бу маълумот олингандан сўнг, у дешифрланади. Дешифрланган маълумот бўйича имитовставка аниқланади ва келган имитовставка қиймат билан таққосланади. Агар имитовставкалар мос келмаса, дешифрланган маълумот нотўғри деб ҳисобланади.

КУРЬЯЗОВ ДАВЛАТЁР МАТЯКУБОВИЧ,
САТТАРОВ АЛИЖОН БОЗОРБОЕВИЧ,
АХМЕДОВ БАРДОШ БОБОНАЗАРОВИЧ.

БЛОКЛИ СИММЕТРИК ШИФРЛАШ АЛГОРИТМЛАРИ БАРДОШЛИЛИГИНИ ЗАМОНАВИЙ КРИПТОТАҲЛИЛ УСУЛЛАРИ БИЛАН БАҲОЛАШ

(ЎҚУВ ҚЎЛЛАНМА)

Тошкент – «Aloqachi» – 2017

Муҳаррир: М. Миркомилов
Тех. муҳаррир: А. Тоғаев
Мусаввир: Б. Эсанов
Мусаҳҳиҳа: Ф. Тагаева
Компьютерда саҳифаловчи: Н. Ҳасанова

Нашр.лиц.іі № 176, 11.06. 2010. Босишга рухсат этилди 30.11.2017 йил.
Бичими 60x84 $^{1}/_{16}$. «Times Uz» гарнитураси. Офсет усулида босилди.
Шартли босма табоғи 14,0. Нашр босма табоғи 14.25.
Тиражи 60. Буюртма № 63.

«Nihol print» ОК да чоп этилди.
Тошкент шаҳри, Мухтор Ашрафий кўчаси 99./101.