SIMMETRIK SHIFRLASH ALGORITMINI TAKOMILLASHTIRISH VA KRIPTOTAHLIL USULLARI YORDAMIDA BAHOLASH

O. Allanov, I. Boyquziyev, N. Safoyev

O'ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI
VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

O. Allanov, I. Boyquziyev, N. Safoyev

SIMMETRIK SHIFRLASH ALGORITMINI TAKOMILLASHTIRISH VA KRIPTOTAHLIL USULLARI YORDAMIDA BAHOLASH

MONOGRAFIYA

Toshkent
"IQTISOD-MOLIYA"
2022

UDK: 003.26

KBK: 32.811.4

Taqrizchilar:

Z.T. Xudoyqulov – Muhammad al-Xorazmiy nomidagi TATU “Kriptologiya ” kafedrasi mudiri, PhD, dotsent.;

O.P.Axmedova – UNICON.UZ” DUK – Fan-texnika va marketing tadqiqotlari markazi Axborot xavfsizligi va kriptologiya ilmiy tadqiqot bo‘limi boshlig‘i, t.f.n.

Simmetrik shifrlash algoritmini takomillashtirish va kriptotahlil usullari yordamida baholash: *Monografiya* / O. Allanov, I. Boyquziyev, N. Safoyev. –T.: “Iqtisod-Moliya”, 2022 yil, – 132 b.

Monografiyada simmetrik blokli shifrlash algoritmlarining kriptografiyadagi o‘rni, ularning kriptobardoshliligini aniqlashga qaratilgan kriptotahlillash usullari, zamonaviy simmetrik blokli shifrlash algoritmlarining kriptotahlil natijalari keltirilgan. Shuningdek, O‘zbekiston Respublikasi ma’lumotlarni shifrlash standarti hisoblangan O‘Z DSt 1105:2009 algoritmini algebraik va integral kriptotahlil usullari bo‘yicha baholash, uning tarkibidagi o‘rin almashtirish va aralashtirish akslantirish usullari uchun parametrlarni statik tanlash orqali ushbu algoritmni takomillashtirish masalasi ko‘rib chiqilgan. Bundan tashqari, takomillashtirilgan O‘Z DSt 1105:2009 algoritmi ham algebraik va integral kriptotahlil usullari yordamida baholangan va uning shifrlash tezligini boshqa zamonaviy simmetrik blokli shifrlash algoritmlari shifrlash tezliklari bilan solishtirish natijalari keltirilgan.

Ushbu monografiya kriptografiya va kriptoanaliz, xususan, simmetrik blokli shifrlash algoritmlarini yaratish va ularning bardoshliligini baholash sohasida ilmiy izlanish olib borayotgan mutaxassislar uchun tavsiya etiladi hamda mazkur sohada oliy ta’lim muassasalari talabalari va magistrlari foydalanishi uchun tavsiya etiladi.

UDK: 004.056.55
KBK:

ISBN978-9943-7982-9-8

QISQARTMA SO‘ZLAR RO‘YXATI

MSHA – Ma’lumotlarni shifrlash algoritmi;

Rasshifrovkalash – kalitga ega bo‘lgan qonuniy foydalanuvchining shifrmatnni dastlabki matnga o‘girish jarayoni;

O‘z DSt 1105:2009 – Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi;

ShaklSeansKalitBayt() – O‘z DSt 1105:2009 algoritmida seans kalitidan *S* jadvallarni generatsiyalash funksiyasi;

ShaklSeansKalit() – seans kalitidan maxsus diamatritsalarni generatsiyalash funksiyasi;

ShaklBosqichKalit() – O‘z DSt 1105:2009 algoritmida raund kalitlarini generatsiyalash funksiyasi;

Qo‘shBosqichKalit() – O‘z DSt 1105:2009 algoritmida shifrlanayotgan ochiq matn bloki bilan raund kalitini qo‘shish funksiyasi;

BaytAlmash() – O‘z DSt 1105:2009 algoritmida shifrlanayotgan ochiq matn blogi elementlarini *S* jadvalning mos elementlari bilan bayt sathida almashtirishning akslantirishi;

Aralash() – O‘z DSt 1105:2009 algoritmida shifrlanayotgan ochiq matn blogini maxsus tuzilmali diamatritsaga ko‘paytirish funksiyasi;

Sur() – O‘z DSt 1105:2009 algoritmida shifrlanayotgan ochiq matn blogini belgilangan satr va ustun bo‘yicha surish funksiyasi.

KIRISH

Hozirgi kunda axborotni himoyalash masalalarini yechishda kriptografik himoya o‘zining yuqori ishonchliligi va kafolatliligi bilan yetakchi o‘rinni egallamoqda. Xususan, Accenture kompaniyasi taqdim etgan ma’lumotga ko‘ra “2019-yilda tashkilotlar tomonidan kriptografik himoya mexanizmlaridan foydalanish natijasida 0,85 million AQSh dollari tejalgan”[1]. Axborotning konfidensiallik, yaxlitlik xususiyatlarini ta’minlashda va rad etishdan himoyalashda kriptografik himoya muhim ahamiyat kasb etgani bois, kriptografik algoritmlarning bardoshligini baholash hozirgi kundagi dolzarb masalalardan biri hisoblanadi. Hozirda bardoshli kriptografik algoritmlarni yaratish, ularni xavfsizlik nuqtayi nazaridan baholash masalalariga AQSh, Rossiya Federatsiyasi, Isroil, Belgiya, Janubiy Koreya, Kanada va boshqa rivojlangan davlatlarda katta e’tibor qaratilmoqda.

Shu sababli, axborotning konfidensialligini ta’minlashda kriptografik shifrlash algoritmlaridan foydalanishga qaratilgan usul va algoritmlarni yaratish, bardoshlik va samaradorlik nuqtayi nazaridan takomillashtirish hamda ularning xavfsizligini kriptotahlil usullari yordamida baholashga oid ko‘plab ilmiy tadqiqotlar olib borilmoqda. Shu o‘rinda, axborotni shifrlashda tezkor simmetrik blokli algoritmlardan foydalanish va ularning kriptobardoshligini tahlillashning yangi yondashuvlariga bag‘ishlangan ilmiy-amaliy tadqiqotlarga alohida e’tibor qaratish zarur hisoblanadi.

Respublikamizda davlat va xo‘jalik boshqaruv organlarida axborotni himoyalashning kriptografik mexanizmlarini tatbiq etish, xususan, davlat xizmatlaridan masofadan foydalanishda foydalanuvchilarning haqiqiyligini tekshirish va ma’lumotlar konfidensialligini ta’minlashga qaratilgan keng qamrovli chora-tadbirlar amalga oshirilmoqda. 2022-2026-yillarga mo‘ljallangan yangi o‘zbekistonning taraqqiyot strategiyasida, jumladan «kiberjinoyatchilikning oldini olish tizimini yaratish»[2] bo‘yicha vazifalari belgilangan. Ushbu vazifalarni amalga oshirishda mavjud milliy kriptografik algoritmlarni xavfsizlik nuqtayi nazaridan baholash va ularni takomillashtirish muhim vazifalardan biri hisoblanadi.

Monografiyaning birinchi bobida simmetrik blokli shifrlash algoritmlarining kriptografiyadagi o‘rni, qo‘llanilish sohalari va ularni

[1]https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
[2]O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son Farmoni

yaratish usullari keltirilgan. Shuningdek, simmetrik blokli shifrlash algoritmlarini kriptotahlillash usullari va zamonaviy simmetrik blokli shifrlash algoritmlarining kriptotahlil natijalari bayon qilingan.

Ikkinchi bobda O‘z DSt 1105:2009 shifrlash algoritmining tavsifi, algebraik va integral kriptotahlilga oid ma’lumotlar keltirilgan.

Uchunchi bobda o‘rin almashtirish va aralashtirish akslantirishlari uchun parametrlarni statik tanlash, O‘z DSt 1105:2009 shifrlash algoritmi asosida takomillashtirilgan shifrlash algoritmini ishlab chiqish masalalari o‘rin olgan.

Monografiyaning to‘rtinchi bobi O‘z DSt 1105:2009 shifrlash algoritmi asosida takomillashtirilgan shifrlash algoritmining integral va algebraik kriptotahliliga oid ma’lumotlar, takomillashtirilgan shifrlash algoritmini amaliyotda qo‘llash natijalariga bag‘ishlangan.

I BOB. SIMMETRIK BLOKLI SHIFRLASH ALGORITMLARINING TAHLILI

1.1-§. Simmetrik blokli shifrlash algoritmlarining kriptografiyadagi o‘rni

Bugungi kunda raqamli aloqa va elektron ma’lumotlar almashinuvi jadal o‘sib borayotgan bir vaqtda, kiber fazoda xavfsizlik to‘g‘risida to‘liq o‘ylanmasdan aloqalar o‘rnatilmoqda. Hozirda barcha o‘z shaxsiy ma’lumotlari va axborotini aynan kiber fazoda almashmoqda. Aksariyat hollarda esa, kiber fazoda xavfsizlik ta’minlanmagan yoki kiberjinoyatchilar tomonidan xavf mavjud bo‘ladi. Bu esa zamonaviy kriptografik himoya usullaridan foydalanishni taqozo etadi.

Kriptografiya – axborotni kiberjinoyatchilar yoki qonuniy qabul qiluvchidan boshqa foydalanuvchilar foydalanishidan himoyalash bilan shug‘ullanib, Internet orqali kriptografik algoritmlar yordamida maxfiy axborotni almashinish imkoniyatini beradi. Umumiy holda kriptografik algoritmlar uchta guruhga bo‘linadi (1.1-rasm) [1]:

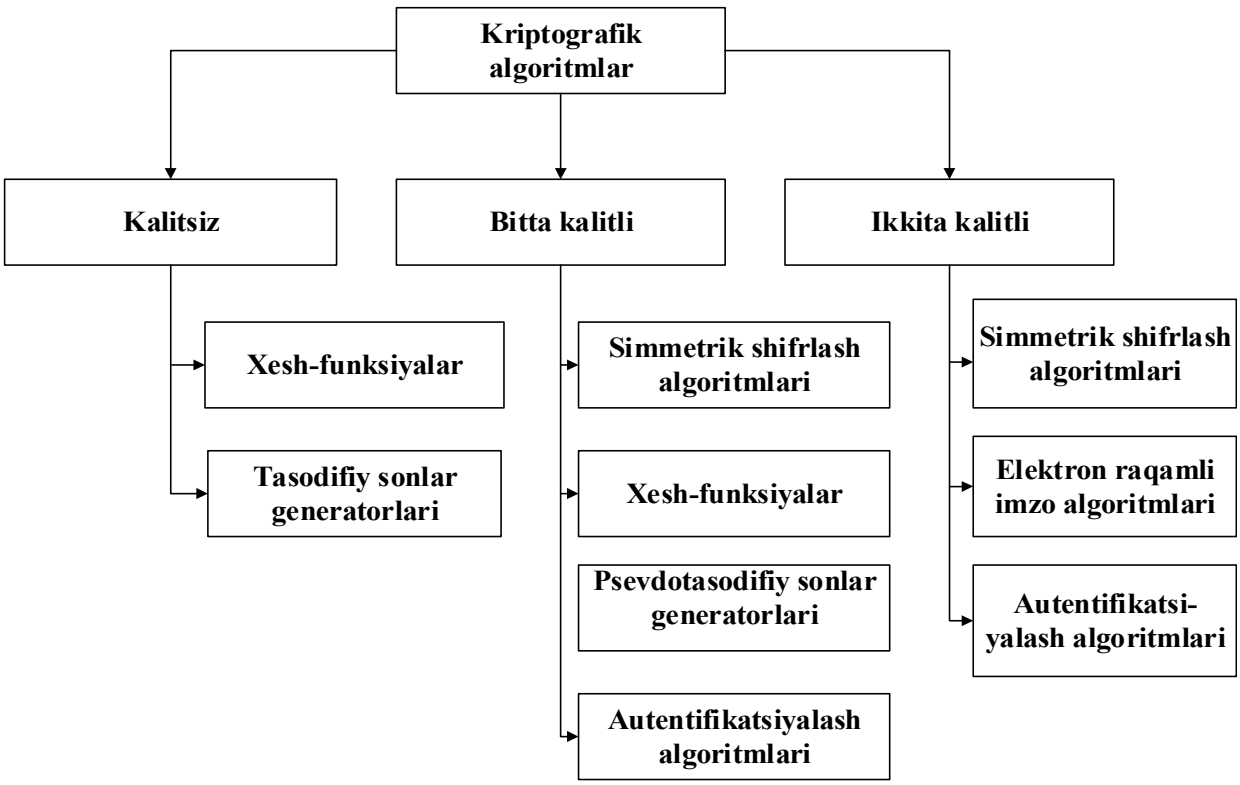
– *kalitsiz algoritmlar,* kriptografik akslantirish jarayonida hech qanday kalitdan foydalanilmaydi;

– *yagona kalitli algoritmlar,* hisoblash jarayonida yagona maxfiy kalitdan foydalaniladi;

– *ikki kalitli algoritmlar,* hisoblash jarayonida ikki ko‘rinishdagi: shaxsiy va ochiq kalitlardan foydalaniladi [115].

Simmetrik shifrlash algoritmlari yagona kalitli algoritm hisoblanib, ochiq ma’lumotlar bloklarini shifrlashda va “rasshifrovkalash”da yagona kalitdan foydalaniladi. Simmetrik shifrlash algoritmlari ma’lumotni akslantirish tartibiga ko‘ra ikki turga: *blokli* va *oqimli* shifrlarga bo‘linadi [2]. Blokli shifrlashda axborot o‘zgarmas uzunlikdagi bloklarga (masalan, 64 yoki 128 bit) bo‘linadi va ular navbati bilan shifrlanadi. Ma’lumotni bloklarga ajratish imkoni mavjud bo‘lmaganda esa, oqimli shifrlardan foydalaniladi [3].

Blokli simmetrik shifrlar *psevdotasodifiy almashtirishlar (Pseudo Random Permutations, PRP)* deb ataluvchi matematik obyektlarga asoslangan bo‘lib, bunda teskarisi mavjud funksiya n bitli ochiq matn m va maxfiy kalit k ni qabul qilib, chiqishda n bitli shifrmatn c ni hosil qiladi. O‘zgarmas uzunlikdagi kalit k uchun foydalanilgan PRP funksiyaning natijasi tasodifiy n bitli biyektiv funksiyadan ajratib bo‘lmasa, PRP funksiya *xavfsiz,* deb ataladi [37].



1.1-rasm. **Kriptografik algoritmlarning tasnifi**

Blokli simmetrik shifrlarni yaratishdan asosiy maqsad xavfsizlik va samaradorlikni ta'minlash yoki xavfsizlik yoki samaradorlikni ta'minlash oson vazifa hisoblansada, har ikkalasini birga amalga oshirish "san'atdir" [4].

Blokli shifrlarni ichki tuzilishiga ko‘ra 5 ta: *o‘rniga qo‘yish – almashtirish tarmoqlari (Substitution Permutation Networks, SPN), Feystel tarmog‘i (Feistel networks), qo‘shish-aylantirish-XOR (Add-Rotate-XOR, ARX), chiziqsiz aloqali siljitish registorlariga (non-linear feedback shift register, NLFSR) asoslangan va gibrid* turlarga ajratiladi [38]. SP tarmoqlariga asoslangan shifrlash algoritmlariga AES (Advanced Encryption Standard) standartini [39], NOEKEON [40], ICEBERG [41], mCrypton [42] va PRESENT [43]larni, Feystel tarmog‘iga DES (Data Encryption Standard) [6], GOST R 28147-89 [7] standartini, Camellia [44], SEA [45] va CLEFIA [46] algoritmlarini, ARX tarmog‘iga IDEA (International Data Encryption Algorithm) [47],HIGHT [48], SPECK [8] va LEA [49] algoritmlarini, NLFSRga asoslangan algoritmlarga KeeLoq [9], KATAN va KTANTAN oilasini [50] hamda gibrid turiga Hummingbird [51] va PRESENT-GRP [52] algoritmlarini misol keltirish mumkin.

Simmetrik blokli shifrlash algoritmlari bir nechta bosqichlardan (*raund*lardan) iborat bo‘lib, har bir raund aralashtiruvchi va tarqatuvchi

akslantirishlardan tuzilgan. Mazkur tuzilish tamoyili, har bir raund shifrlash jarayonini har xil kalitlar bilan bir xil turdagi akslantirishlarni amalga oshirishga, hamda rasshifrovkalash jarayonini raund akslantirishlari va kalitlarini teskari tartibda qo‘llash orqali amalga oshirish imkonini beradi. Algoritm asosini tashkil etuvchi, raund shifrlash jarayonini amalga oshiruvchi, aralashtirish va tarqatish xususiyatlariga ega bo‘lgan funksiyalar *asosiy akslantirishlar* deyiladi [2].

Blokli shifrlar ikkita: E shifrlash va D rasshifrovkalash algoritmidan iborat. Har ikki algoritm ham ikki kirish: n bitli kirish bloki va k bitli kalitni qabul qiladi va n bitli chiqish blokni hosil qiladi. Rasshifrovkalash algoritmi D shifrlash algoritmining inversi hisoblanadi, $D = E^{-1}$. Formal holda shifrlash funksiyasini quyidagicha yozish mumkin [5]:

$$E_K(P) \coloneqq E(P, K): \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$

Bu yerda, k – kalit K ning bitdagi uzunligi, P – ochiq matn bo‘lib, blok uzunligini n bitga teng va C – shifrmatn deb atalib, n bit blok uzunligiga ega. Har bir kalit K uchun, $\{0,1\}^n$ ni hosil qilishda $E_K(P)$ funksiyasini invertlash talab qilinadi. E funksiyaning inverti quyidagicha ifodalanib, kirishda kalit K va shifrmatn C qabul qilib, chiqishda ochiq matn P ni hosil qiladi:

$$E_K^{-1}(C) = D_K(C) \coloneqq D(K, C): \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$

Kriptografiyada *blokli shifrlarning amallar rejimi (block cipher mode of operation)* tushunchasi mavjud bo‘lib, axborotni himoyalash (masalan, konfidensiallik va autentifikatsiya) uchun blokli shifrlardan foydalanish algoritmi hisoblanadi. Blokli shifrlarning o‘zi faqat bloklar deb ataluvchi o‘zgarmas uzunlikdagi bitlar guruhini kriptografik almashtirish (shifrlash va rasshifrovkalash) uchun mo‘ljallangan. Blokli shifrlar rejimi esa birdan ortiq ma‘lumotlar blokini xavfsiz kriptografik almashtirish uchun shifrni yagona blok akslantirishini qanday amalga oshirish tartibini ifodalaydi.

Aksariyat blokli shifrlar rejimi shifrlash/ rasshifrovkalash amali uchun *boshlang‘ich vektor (initialization vector, IV)* deb ataluvchi unikal binar ketma-ketlikni talab qiladi. Boshlang‘ich vektorni takrorlanmas va tasodifiy bo‘lishi talab qilinadi. Turli boshlang‘ich vektorlardan foydalanish yagona ochiq matn va shifrlash kalitidan bir necha marta foydalangan taqdirda ham turli shifrmatnni hosil qilish imkoniyatini beradi. Blokli shifrlar rejimidan ma’lumot bloklari soni birdan ortiq bo‘lgan taqdirda foydalanish mumkin bo‘ladi va bunda blok uzunligi har

doim o‘zgarmas bo‘ladi.

Blokli shifrlar rejimi odatda axborot konfidensialligini yoki yaxlitligini, ba’zida esa ularning har ikkalasini ham ta’minlashda ishlatiladi [117].

Dastlabki blokli shifrlar rejimlari (Electronic codebook (ECB), Cipher block chaining (CBC), Output feedback (OFB) va Cipher feedback (CFB)) 1981-yilda DES standartining rejimlari sifatida FIPS PUB 81 nashrida keltirilgan [10]. 2001-yilda esa AES standartini qo‘shish orqali National Institute of Standards and Technology (NIST) tomonidan CTR (Counter) rejimini o‘z ichiga olgan SP800-38A nashrini chop etdi [11]. 2010-yilda esa SP800-38E nashrida NIST tomonidan XTS-AES (XEX Tweakable Block Cipher with Ciphertext Stealing) qo‘shildi [12]. Bundan tashqari, NIST tomonidan nashrlarga kiritilmagan, biroq, kriptografik kutubxonalarda keng qo‘llaniluvchi qator rejimlar mavjud (masalan, Ciphertext stealing (CTS)).

Yuqorida keltirilgan blokli shifrlar rejimlari axborotning konfidensialligini ta’minlashga qaratilgan bo‘lib, axborot modikatsiyalanganligini aniqlash imkonini bermaydi. Buni amalga oshirishning qator usullari (Cipher block chaining message authentication code (CBC-MAC) [53], elektron raqamli imzo, The Keyed-Hash Message Authentication Code (HMAC) [13], Cipher-based Message Authentication Code (CMAC) [14] va Galois Message Authentication Code (GMAC) [15]) mavjud bo‘lsada, ular faqat yaxlitlikni ta’minlaydi.

Alohida-alohida konfidensiallik va yaxlitlikni ta’minlash usullarini birlashtirish murakkab bo‘lib, xatolarga bardoshsiz hisoblanadi [16]. Shuning uchun, konfidensiallik va yaxlitlikni yagona kriptografik amalda (shifrlash algoritmi) birlashtiruvchi rejimni yaratish zaruriyati paydo bo‘ldi. Mazkur vazifani bajaruvchi rejimlar umumiy holda *autentifikatsiyalangan shifrlash* deb nomlanib, ularga CCM (Counter with CBC-MAC) [17], GCM (Galois/Counter Mode) [15], CWC (Carter–Wegman + CTR mode) [54], EAX (Encrypt-then-authenticate-then-translate) [18], IAPM (Integrity Aware Parallelizable Mode) [55] va OCB (Offset Codebook Mode) [19] rejimlari misol bo‘ladi.

Simmetrik blokli shifrlar axborotni himoyalashda keng qamrovda foydalaniladi. Barcha shifrlash algoritmlari kabi simmetrik shifrlash algoritmlari axborot konfidensialligini ta’minlashda foydalanilib, uzluksiz shifrlarga nisbatan yuqori xavfsizlikni va ochiq kalitli shifrlash algoritmlariga nisbatan tezkorlikni ta’minlaydi hamda qator dasturiy, apparat-dasturiy vositalar ko‘rinishida amalga oshiriladi [112]. Masalan,

SSH, IPSec, TLS&SSL, VPN kabi protokollar blokli simmetrik shifrlarni o‘z ichiga olgan kriptografik kutubxonalardan foydalangan holda xavfsiz aloqani ta’minlaydi [105].

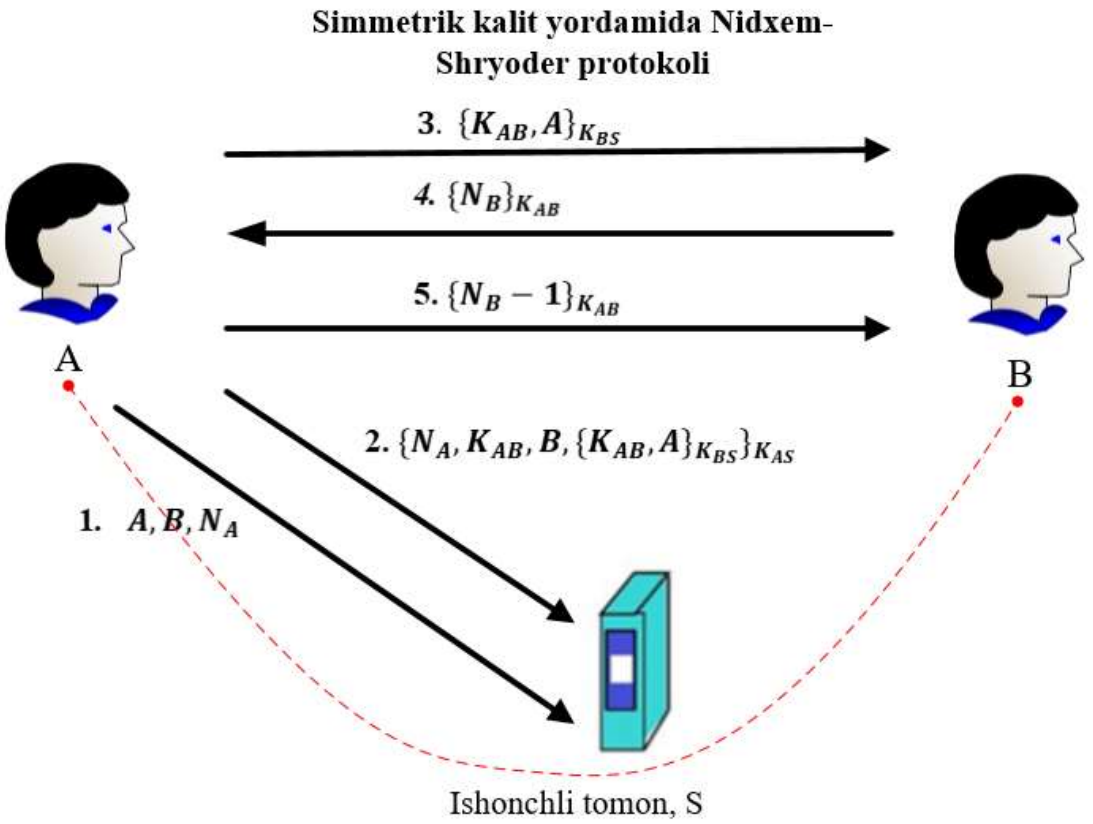
Blokli shifrlar axborot yaxlitligini ta’minlashda ham qo‘llanilib, ularga CBC-MAC, CMAC, GMAC kabilarni misol keltirish mumkin. Blokli shifrlar asosida axborot yaxlitligini ta’minlash oddiy xesh funksiyalardan farqi xesh qiymatni hosil qilishda kalitdan foydalanishi va foydalanilgan algoritmga ko‘ra tezligidir. Boshqacha aytganda, simmetrik blokli shifrlar kalitli xesh funksiyalarni qurish imkoniyatini beradi [106].

Blokli simmetrik shifrlar axborot konfidensialligi va yaxlitligini ta’minlashda nafaqat alohida-alohida tarzda, balki, yagona amalda ham bajarish imkoniyatiga ega. Bu esa foydalaniluvchi kalitlar sonini kamaytiradi va xatolikka bardoshli hisoblanadi. Bularga autentifikatsiyalangan shifrlash deb nomlanuvchi blokli shifrlar rejimlaridan foydalanilgan holatlarni keltirish mumkin. Blokli simmetrik shifrlardan autentifikatsiyalangan shifrlashda foydalanish alohida yaxlitlikni ta’minlashdagi rad etishdan himoyalash talab qilinmagan holatlar uchun o‘rinli bo‘lib, yuqori tezkorlikni taqdim etadi.

Blokli simmetrik shifrlar o‘zining tezkorligi va bitlarni yaxshi aralashtirish xususiyatiga ega bo‘lganligi ularni psevdotasodifiy sonlar generatorini qurishda ham foydalanish imkonini beradi. Amalda simmetrik blokli shifrlarning turli rejimlariga asoslangan qator psevdotasodifiy sonlar generatori mavjud bo‘lib, ularga Yarrow [56], Fortuna [57], ANSI X9.17 va ANSI X9.31 [20] algoritmlarini misol keltirish mumkin.

Bundan tashqari, simmetrik blokli shifrlar ko‘plab kriptografik protokollarda autentifikatsiya va seans kalitini uzatish maqsadida foydalanib kelinmoqda. Simmetrik blokli shifrlar ma‘lumotni shifrlash va rasshifrovkalashda yagona kalitdan foydalangani bois, ular asosan ishonchli uchinchi tomon ishtirok etgan protokollarni qurishda keng qo‘llaniladi (1.2-rasm). Ishonli uchinchi tomon xizmatiga asoslangan ko‘plab protokollar mavjud bo‘lib, unga Kerberos protokolini yaqqol misol keltirish mumkin [58].

Hozirda blokli simmetrik shifrlarni o‘z ichiga olgan ko‘plab ma‘lumotlarni shifrlash bo‘yicha davlat standartlari (O‘z DSt 1105:2009 [21], GOST R 28147-89 [7], AES [39]) va algoritmlar mavjud bo‘lib, ulardan yuqori maxfiy darajali ma’lumotlarni shifrlashdan oldin ularni kriptotahlilini amalga oshirish talab qilinadi.



1.2-rasm. **Blokli simmetrik shifrlardan foydalanilgan ishonchli uchinchi tomon xizmatiga asoslangan protokolning umumiy ko‘rinishi**

Keyingi bo‘limlarda simmetrik blokli shifrlarni kriptotahlillash usullari va zamonaviy blokli shifrlash algoritmlarining tahlil natijalari bilan tanishib chiqiladi.

1.2-§. Blokli shifrlash algoritmlarini kriptotahlillash usullari

Axborot tizimi xavfsizligi auditining asosiy jihatlaridan biri foydalanilgan kriptografik algoritmlarning ishonchligini baholash hisoblanadi. Kriptotahlil (grekcha *kryptós* – “maxfiy” va *analýein* – “zaiflashtirish” yoki “xalos qilish”) fan sohasi kalitsiz ochiq matnni tiklash (deshifrlash) bilan shug‘ullanib, fundamental asosi Kirxgof tomonidan yaratilgan [22] bo‘lib, unda xabarning maxfiyligi faqat kalitga bog‘liq bo‘lishi kerakligi aytilgan, ya’ni kalitdan boshqa barcha ma’lumotlar hujumchiga oshkor bo‘lishi kerak. Ushbu prinsipdan algoritmning maxfiyligi uning bardoshligini ta’minlashda muhim

emasligini ko‘rish mumkin.

Kriptotahlil kalitni bo‘lishi mumkin bo‘lgan sohasini kamaytirish uchun turli sharoitlarda shifrlash kaliti to‘g‘risida qo‘shimcha ma’lumot olishni maqsad qiladi. Kriptotahlil natijalari amalda qo‘llanilish darajalari bilan farqlanadi. L.Knudsen blokli shifrlarni kriptotahlil qilish usullarini olingan ma’lumot hajmi va sifati natijasiga qarab quyidagicha tasniflagan [23]:

– *to‘liq hujum* – kriptotahlilchi kalitni aniqlaydi;

– *global deduksiya* – kriptotahlilchi o‘rganilayotgan algoritmning funksional ekvivalentini ishlab chiqadi va kalitni bilmasdan shifrlash va deshifrlash imkoniga ega bo‘ladi;

– *xususiy deduksiya* – kriptotahlilchi ba’zi xabarlarni shifrlash yoki deshifrlash imkoniga ega bo‘ladi;

– *axborot deduksiyasi* – kriptotahlilchi ochiq matn yoki kalit bo‘yicha bir qancha ma’lumotni qo‘lga kiritadi.

Shifrlash algoritmini tahlil qilish deyilganda uni to‘liq amaliy tomondan “yo‘q qilish” – kalitni topish nazarda tutilmaydi. Kriptologiya fani doirasida agar shifrlash algoritmining kriptotahlil natijasi kalitning bo‘lishi mumkin bo‘lgan barcha variantlarini (Brute force attack) hisoblashga qaraganda samarali bo‘lsa, hujum amalga oshirilgan, deb hisoblanadi [118]. Masalan, faraz qilinsin biror shifrlash algoritmi uchun kalitning bo‘lishi mumkin bo‘lgan barcha variantlari 2^{128} ga teng bo‘lsin. Agar tanlangan kriptotahlil usulida ushbu shifrlash algoritmining kalitini aniqlashda 2^{110} ta amal talab qilinsa, hujum amalga oshirilgan, deb qaraladi. Ushbu usullar haqiqatda bo‘lishi qiyin bo‘lgan hajmdagi tanlangan ochiq matnlarni yoki hisoblash mashinasi xotirasini talab qilishi mumkin.

Kriptoalgoritmni tahlillashga qaratilgan harakatlar *hujum* sifatida qaraladi. Hujumlarni tasniflash va ularga to‘xtalib o‘tishdan oldin ba’zi belgilanishlarni keltirib o‘tish joiz. Ochiq matn x tartibida va shifrmatn y tartibida belgilanadi. Bu holda ochiq matndan shifrmatnni hosil qilishda foydalanilgan kalit k deb belgilanadi. Mazkur belgilanishlarga ko‘ra quyidagi tengliklarni yozish mumkin: $E_k(x) = y, D_k(y) = x$. Bu yerda, $E_k()$ va $D_k()$ ifodalar mos ravishda shifrlash va rasshifrovkalash funksiyalari.

Axborot xavfsizligining boshqa sohalarida bo‘lgani kabi, kriptotahlil sohasida ham *hujumchi modeli* tushunchasi mavjud bo‘lib, u kriptotahlilchiga berilgan ma’lumotlar va imkoniyatlarni xarakterlaydi.

Umumiy holda kriptotahlilda hujumchi modelini quyidagi 4 ta turga ajratish mumkin [59]:

– *Faqat shifrmatn asosida hujum.* Mazkur hujum modelida kriptotahlilchiga faqat turli $x_1, \dots, x_m$ ochiq matnlardan olingan $y_1, \dots, y_m$ shifrmatnlar beriladi va m yetarli sondagi ochiq matn $x_i, i = \overline{1,m}$ (yoki unga mos kalit k_i)lardan bittasini topish yoki buni amalga oshira olmasligiga ishonch hosil qilish talab qilinadi. Xususiy holatlarda, kalitlar uchun $k_1 = \dots = k_m$ shart yoki ochiq matnlar uchun $x_1 = \dots = x_m$ shart tanlanib olinishi mumkin.

– *Ochiq matn asosida hujum.* Mazkur hujum modelida kriptotahlilchiga ochiq matn va shifrmatn juftlari $(x_1, y_1), \dots, (x_m, y_m)$ beriladi va kamida bir juftlik uchun kalit k_i topish talab qilinadi. Xususiy holda, agar $k_1 = \dots = k_m = k$ shart o‘rinli bo‘lsa, k kalitni aniqlash yoki shifrmatn y_{m+1} dan ochiq matn x_{m+1} ni aniqlay olmasligiga ishonch hosil qilishi talab qilinadi.

– *Tanlangan ochiq matn asosida hujum.* Mazkur hujum modeli oldingisidan kriptotahlilchiga $x_1, \dots, x_m$ ochiq matnlarni tanlash imkoniyati berilishi bilan farqlanib, hujum maqsadi o‘zgarmaydi. Mazkur hujum modeli kriptohujumchi shifrlash vositasidan foydalanish imkoniyati mavjud bo‘lgan holati uchun joiz hisoblanadi.

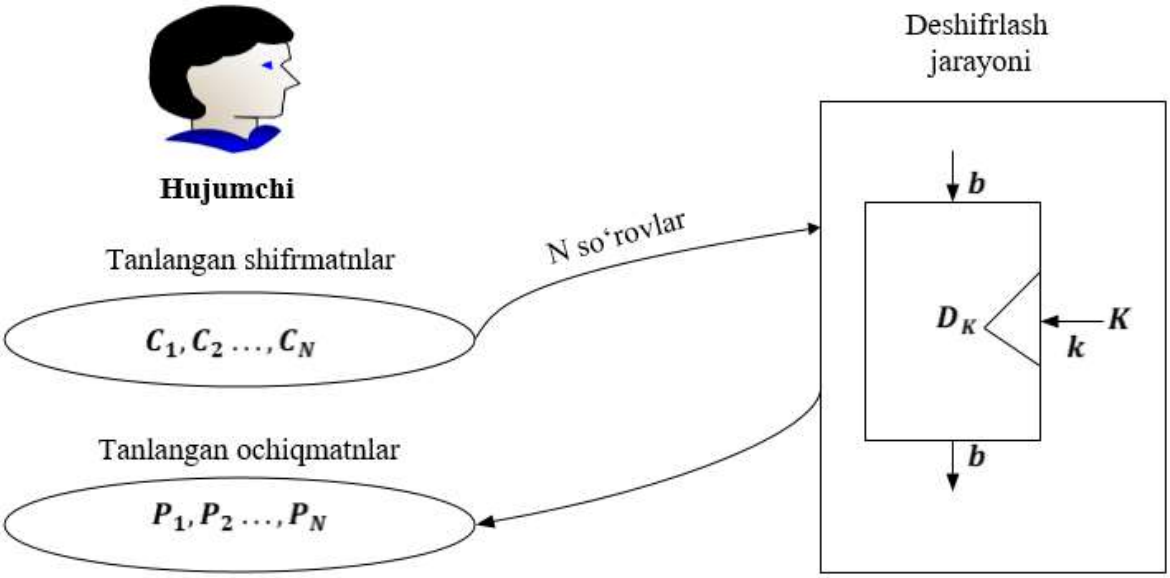
– *Adaptiv tanlangan ochiq matn asosida hujum.* Ushbu hujum modeli oldingi modelning xususiy ko‘rinishi bo‘lib, kriptotahlilchi nafaqat qaysi shifrmatndan foydalanishini tanlashi, balki oldingi shifrlash natijalaridan o‘rganilgan axborot asosida ochiq matnlar ketma-ketligini tanlashi mumkin bo‘ladi.

Bundan tashqari, *kalitga aloqador hujum* modeli mavjud bo‘lib, unda tanlangan ochiq matn asosida hujum kabi kriptotahlilchi ikkita turli kalit asosida bir ochiq matn uchun shifrmatnlarni hosil qilishi mumkin bo‘ladi. Bu yerda, kalitlar ma’lum bo‘lmasada, ular orasidagi farq ma’lum bo‘ladi. Masalan, ikkita kalit faqat bir bitida farq qiladi.

Yuqorida keltirilgan ixtiyoriy hujum modelida, ma’lum yoki tanlangan ochiq matnga (yoki shifrmatnga) mos bo‘lgan shifrmatnni (yoki ochiq matnni) faqat tizimni natija chiqarishiga undash orqali olish mumkin. Tizimga bo‘lgan bu undashlar *so‘rovlar,* deb atalib, tanlangan shifrmatnlarga asoslangan hujum modelining ko‘rinishi 1.3-rasmda keltirilgan.

Shuningdek, hujumlarni ularni amalga oshirish uchun zarur bo‘lgan resurslar miqdori bo‘yicha ham tasniflash mumkin [24]:

– *Ma’lumot (Data, D).* Ma’lumot miqdori so‘rovlar soni bilan o‘lchanadi. Masalan, kalit uzunligi blok uzunligidan kichik bo‘lganda “qo‘pol kuch” hujumi orqali topishda bitta ochiq matn bloki talab qilinadi.



1.3-rasm. **Tanlangan shifrmatnga asoslangan hujum modeli**

– *Vaqt (Time, T).* Vaqt miqdori kriptotahlilchi tomonidan offlayn rejimda amalga oshirilgan hisoblash qiymati bilan o‘lchanib, bu qiymat birligi odatda shifrlash algoritmi yoki rasshifrovkalash algoritmining bajarilish vaqti bilan bir xil bo‘ladi. Masalan, blok uzunligidan kichik bo‘lgan k bitli kalitni “qo‘pol kuch” hujumida topishga sarflangan vaqt sarfi 2^k shifrlash amaliga teng bo‘ladi.

– *Xotira (Memory, M).* Hujumchidan odatda so‘ralgan ochiq matnlar (mos holda shifrmatnlar) va tizimdan qaytarilgan unga mos shifrmatnlarni (mos holda ochiq matnlar) saqlash talab qilinadi. Hujumni amalga oshirish vaqtida hujumchi oraliq qiymatlarni saqlab borishi talab qilinadi. Buning uchun esa ma’lum xotira hajmi talab qilinadi. Ko‘p hollarda xotira hajmi blok o‘lchamida (b bit yoki unga mos bayt) keltiriladi. Masalan, blok uzunligidan kichik bo‘lgan k bitli kalitni “qo‘pol kuch” hujumida xotira ahamiyatsiz bo‘ladi.

Yuqorida keltirilgan uchlik (D, T, M) hujum murakkabligining o‘lchovi hisoblanib, simmetrik blokli shifrlarning kriptotahlillashning keng tarqalgan usullariga quyidagilarni keltirish mumkin [104]:

– chiziqli kriptotahlil usuli (linear cryptanalysis);

– differensial kriptotahlil usuli (differential cryptanalysis);

– chiziqli-differensial kriptotahlil usuli (linear-differential cryptanalysis);

– algebraik kriptotahlil usuli (algebraic crypanalysis);

– integral kriptotahlil usuli (integral cryptanalysis).

Chiziqli kriptotahlil usuli. Chiziqli kriptotahlil usuli Yaponiyalik kriptolog Misuru Masui tomonidan 1993-yilda DES va FEAL shifrlash algoritmidagi zaiflikni topish uchun ishlab chiqilgan [60].

Chiziqli kriptotahlil usulining mohiyati tanlab olingan ochiq matn Mva mavjud shifrmatn C bitlarini XOR amalidagi natijasi asosida kalit bitlarini aniqlashdan iborat:

$$M[i_1, i_2, \dots, i_n] \oplus C[j_1, j_2, \dots, j_n] = K[k_1, k_2, \dots, k_n]$$

Bu yerda:

$$M[i_1, i_2, \dots, i_n] = M[i_1] \oplus M[i_2] \dots \oplus \dots M[i_n],$$
$$C[j_1, j_2, \dots, j_n] = C[j_1] \oplus C[j_2] \dots \oplus \dots C[j_n],$$
$$K[k_1, k_2, \dots, k_n] = K[k_1] \oplus K[k_2] \dots \oplus \dots K[k_n].$$

Kriptotahlilchining vazifasi yuqorida keltirilgan tenglikdan eng yaqin (to‘g‘ri) chiziqli approksimatsiyani aniqlash, ya’ni tahlil qilinayotgan algoritm akslantirishlari xossalaridan kelib chiqib, eng samarali natija beruvchi chiziqli bog‘lanishni tanlashdan iborat. Tanlangan approksimatsiya tenglamalarida tenglikning chap tomonini qiymati 0 yoki 1 ekanligini aniqlashda yetarlicha ko‘p miqdordagi ochiq matn va shifr matn juftliklari ustida statistik tahlil olib borish kerak bo‘ladi. Natijada, faqat kalit bitlari ishtirok etgan tenglamalar sistemasiga ega bo‘linadi. Ushbu tenglamalar sistemasini yechish orqali kalit bitlarini aniqlash mumkin bo‘ladi.

Amaliyotda foydalanilgan kalit bitlarini to‘liq yoki ko‘proq qismini aniqlash uchun, mazkur tenglamadan bir nechtasini qurish hamda ular yordamida hosil qilingan tenglamalar sistemasini yechish talab etiladi.

Simmetrik blokli shifrlash algoritmlarida S-bloklar chiziqsiz akslantirishlarni ifodalaydi. Demak, S – bloklarni kriptotahlil qilish asosida algoritmning kriptobardoshligi xususida xulosa bildirish mumkin. S – bloklarni chiziqli kriptotahlil qilishda chiziqli approksimatsiya tenglamalarini tuzish talab qilinadi. Bunda, “korrelyatsion matritsa” jadvalidan foydalanish samarali usul hisoblanib, u chiziqli kriptotahlilning asosiy xarakteristikasini ifodalaydi [25].

DES shifrlash algoritmining 16 raundi uchun chiziqli kriptotahlil natijasi kalitni topishda 2^{47} ta tanlanadigan ochiq matnni va ular ustida 2^{43} ta shifrlash amalini bajarishni talab qilgan. FEAL shifrlash algoritmini chiziqli kriptotahlillash natijasi esa 16 raundi uchun kalitni topishda 2^{28} ta tanlangan va $2^{46,5}$ ma’lum ochiq matn talab qilgan [26].

Differensial kriptotahlil usuli. Mazkur kriptotahlil usuli Isroillik kriptogriflar E.Biham va A.Shamir tomonidan 1990-yilda DES algoritmini tahlillash uchun ishlab chiqilgan. Faraz qilinsin, x va x' ochiq matnlarning XOR amalidagi farqi $\Delta x \triangleq x \oplus x'$ teng bo‘lsa, ularning F funksiya natijasidagi farqi $\Delta y = F(x) \oplus F(x')$ ga teng bo‘ladi. Differensial kriptotahlilda asosiy e’tibor ushbu ikki hisoblashning *farqiga* qaratiladi.

Agar F tarkibida biror maxfiy parametr ishtirok etmasa, $F(x)$ va $F(x')$ qiymatlar farqini hisoblash muammosiz. Agar F funksiya simmetrik blokli shifrda shifrlash algoritmi E_K bo‘lsa, u holda funkiyaga kiruvchi va chiquvchi qiymatlar farqlari orasidagi bog‘lanish biror ehtimollikka ega bo‘ladi. Bu ehtimollik quyidagi tenglik bilan ifodalanadi:

$$\Pr[\Delta x \xrightarrow{E_K} \Delta y].$$

F funksiya chiziqli akslantirish bo‘lganida, kiruvchi va chiquvchi farqni hisoblashda ortiqcha muammo bo‘lmagani bois, differensial kriptotahlil usuli asosan simmetrik blokli shifrlash algoritmlaridagi chiziqsiz akslantirishlarga qaratiladi. Xususan, F chiziqli akslantirish bo‘lgan hol uchun quyidagi Lemma o‘rinli [25].

Lemma 1. *Ixtiyoriy kiruvchi farq* Δx *va* F *chiziqli funksiya uchun*

$$Pr\left[\Delta x \xrightarrow{F} F(\Delta x)\right] = 1$$

teng va $\Delta y \neq F(\Delta x)$*shartni qanoatlantiruvchi berilgan ixtiyoriy* Δy *uchun*

$$Pr\left[\Delta x \xrightarrow{F} \Delta y\right] = 0.$$

tenglik o‘rinli bo‘ladi.

F funksiya chiziqsiz bo‘lmagan holda chiquvchi farqni yuqori ehtimollik bilan topishning aniq usuli bo‘lmaydi. Boshqacha aytganda, simmetrik blokli shifrlardagi S jadvallar differensial kriptotahlilga bardoshlikni ta’minlaydi.

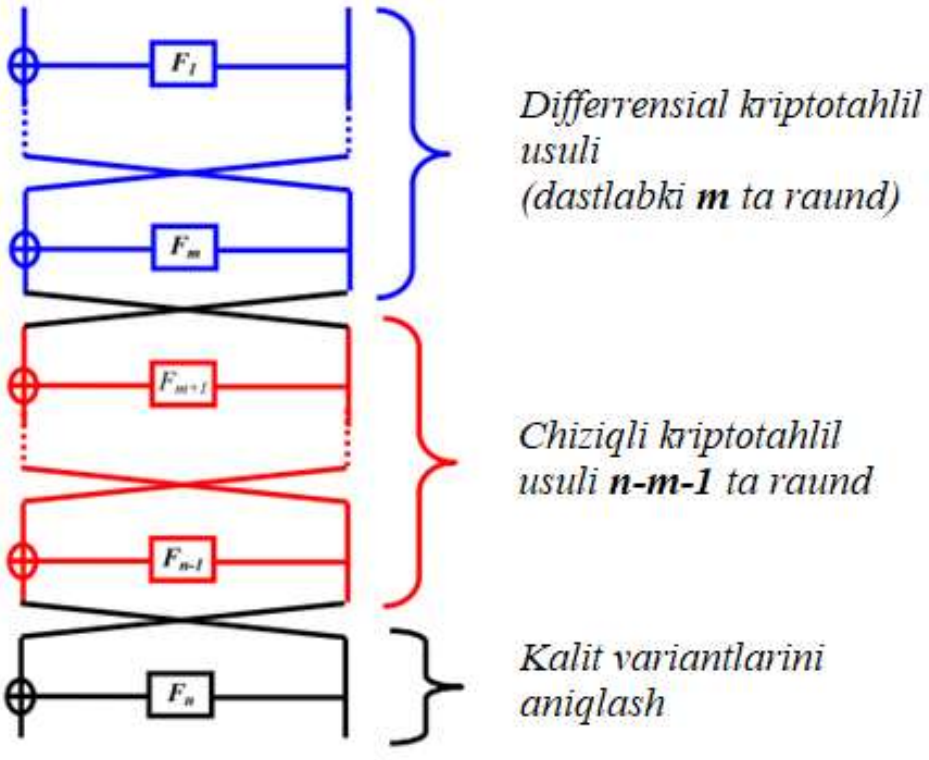
Differensial kriptotahlil usuli standart 16 raundli DES algoritmini amaliy jihatdan to‘liq ochish imkoniyatini bermasada (2^{47} ta ochiq matn kerak bo‘ladi), qisqartirilgan, 8 raundli yoki 6 raundli, DES algoritmi versiyalari uchun muvaffaqiyatli amalga oshirilgan.

Keyinchalik differensial kriptotahlil usuli yordamida 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 kabi algoritmlar baholangan [25].

Tahlillar natijasi ba’zi algoritmlarda ma’lum raunddan so‘ng chiziqsizlik darajasini ortishini, ba’zilarida esa differensial orttirmalarni aniqlash murakkablashini ko‘rsatdi. Bu esa, algoritmlarni tahlillashda dekompozitsiyalashni, ya’ni ma’lum raundda chiziqli kriptotahlil usulini, ma’lum raundda differensial kriptotahlilni qo‘llashni talab qiladi.

Chiziqli-differensial kriptotahlil usuli aynan dekompozitsiyalashga asoslangan bo‘lib, 1994-yilda M.Xellman va S.Langford tomonidan DES shifrlash algoritmiga qarshi hujum turi sifatida ishlab chiqilgan. Ushbu usul tanlangan ochiq matnga asoslangan bo‘lib, g‘oya mualliflari tomonidan 512 ta ochiq matn yordamida DES shifrlash algoritmida foydalanilgan maxfiy kalitning 10 bitini 80 % ehtimollik bilan aniqlashga erishilgan. Ochiq matn sonini 768 taga oshirish orqali bu ehtimollik qiymatini 95 %gacha yetkazish mumkin [25].

Chiziqli-differensial kriptotahlilini amalga oshirish chiziqli kriptotahlil hamda differensial kriptotahlil usullarini umumlashtirishga asoslangan bo‘lib, Feystel tarmog‘iga asoslangan n raundli shifrlash algoritmi uchun uning umumiy qo‘llanilish sxemasi 1.4-rasmda keltirilgan.



1.4-rasm. **Chiziqli-differensial kriptotahlilni amalga oshirish sxemasi**

Kriptotahlilning dastlabki qadamida (1-raundga) kiruvchi ayirmani bilgan holda m – raunddan chiquvchi ayirma qiymati differensial

kriptotahlil usuli orqali aniqlanib, keyingi qadamda $n-1$ - raunddan chiquvchi ayirma qiymati chiziqli kriptotahlil usuli orqali aniqlanadi. So‘nggi qadamda esa oxirgi raund funksiyasiga kiruvchi va funksiyadan chiquvchi ayirma hamda shifr matn qiymatlarini bilgan holda so‘nggi raund funksiyasida foydalanilgan kalitning barcha variantlari tekshirib ko‘rish orqali aniqlanadi.

Shu sababli, mazkur kriptotahlil usulining samaradorligi ham har ikkala kriptotahlil usullarining samaradorligiga, ya’ni ular orqali aniqlangan so‘nggi raund funksiyasidan chiquvchi ayirma qiymatining to‘g‘ri aniqlanganligiga bog‘liq bo‘ladi. Shuningdek, ushbu kriptotahlil usuli bugungi kunga qadar turli mutaxassislar tomonidan DES, Serpent, GOST 28147-89 va h. shifrlash algoritmlariga qo‘llanilgan va tegishli natijalar olingan [25].

Har qaday simmetrik blokli shifrlash algoritmlari ochiq matnni kalit asosida matematik funksiyalardan foydalanib shifrmatnga o‘tkazish vazifasini amalga oshiruvchi funksiya hisoblanadi. Bu esa mazkur funksiyani biror algebraik tenglamalar sistemasi orqali ifodalash imkoniyati mavjudligini ko‘rsatadi. Mazkur imkoniyatdan foydalanishga asoslangan simmetrik blokli shifrlarni tahlillash usuli bu – ***algebraik kriptotahlil (AK)***. Hosil qilingan tenglamalar sistemasini yechish va shifrlash kalitini topish *algebraik kriptotahlil usulining* vazifasi hisoblanadi.

Algebraik kriptotahlil usuli ochiq va shifr matn asosidagi hujum turiga tegishli bo‘lib, uning murakkabligi mumkin bo‘lgan barcha tenglamalar sistemasini qurish va yechish bilan baholanadi. Shu bois, mazkur kriptotahlil usulida algebraik chiziqsizlik darajalari past tenglamalar sistemasini ko‘rish va ularni yechishning samarali yo‘llarini topish muhim sanaladi [25].

Algebraik kriptotahlil usulida shifrlash algoritmi uchun tenglamalar sistemasi orqali ifodalash bosqichi quyidagi qadamlardan iborat:

a) *shifrlash algoritmini dekompozitsiyalash*: ya’ni, shifrlash algoritmining tashkil etuvchilarini imkon qadar kichik va alohida elementlar (chiziqli, chiziqsiz va boshqa akslantirishlar)ga ajratish.

b) *har bir elementni algebraik ifodalash*: ya’ni, har bir akslantirish uchun, ularni kirishi va chiqishini bog‘lovchi imkoniyat darajasida minimal algebraik chiziqsizlik darajasiga ega bo‘lgan tenglamalar sistemasi hosil qilinadi. Bir turga mansub bo‘lgan akslantirishlar uchun tenglamalar sistemasini hosil qilish bir xil tarzda

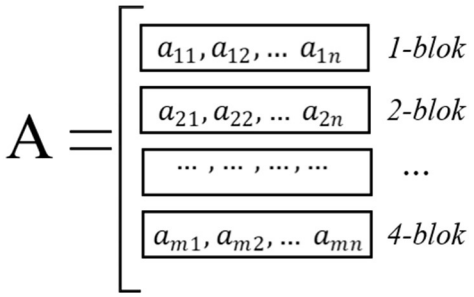
amalga oshiriladi. Mazkur tenglamalar sistemasi faqat noma’lumlari bilan farqlanadi.

c) *har bir elementning kirishi va chiqishini boshqa elementlar hamda kalit, ochiq matn va shifr matn bitlari bilan bog‘lash*. Ya’ni, har bir elementga mos tenglamalar asosida to‘liq shifrlash algoritmini ifodalovchi umumiy tenglamalar sistemasi shakllantiriladi.

Ta’kidlash lozimki, tenglamalar sistemasini qurish jarayoni tahlil qilinayotgan shifrlash algoritmi tuzilishi va uning tashkil etuvchi elementlari xususiyatlariga bog‘liq holda amalga oshirilib, ixtiyoriy shifr uchun tenglamalar sistemasini qurishning universal va optimal yechimi mavjud emas. Biroq, bugungi kunda chekli maydonda aniqlangan chiziqsiz tenglamalar sistemasini yechishga qaratilgan ko‘plab usullar (masalan: Buxberger, F4, F5, F5C, G2V, GVW, SAT-solvers, XL, XL2, XLF, XSL, FXL, XFL, WXL, HXL, MutantXL va MXL2) taklif etilgan va ulardan AK o‘tkazishda bevosita foydalanib kelinmoqda [25].

Bugungi kunda zamonaviy hisoblangan differensial va chiziqli kriptotahlil usullarining bir nechta shifrlash algoritmlariga samarali qo‘llanilishi, bu kriptotahlil usullariga bardoshli bo‘lgan yangi turdagi shifrlash algoritmlarini ishlab chiqilishiga turtki bo‘ldi. Ushbu shifrlash algoritmlariga misol qilib, Daniyalik kriptograf Lasr Knudsen tomonidan ishlab chiqilgan «Kvadrat» (Square) shifrlash algoritmini keltirish mumkin. Kvadrat shifrlash algoritmi chiziqli va differensial kriptotahlil usullariga yetarlicha bardoshli hisoblanadi. Biroq, mazkur shifrlash algoritmini ishlab chiqish jarayonida, algoritm kriptobardoshligini baholash maqsadida muallif tomonidan 1997-yili yangi hujum turi – ***integral kriptotahlil usuli*** o‘ylab topildi [25]. Ushbu kriptotahlil usuli *tanlab olingan ochiq matnlar asosidagi hujum* turiga tegishli bo‘lib, uni biror-bir blokli simmetrik shifrlash algoritmiga qo‘llashda, tanlab olingan ochiq matnlar va ularga mos shifrmatnlarning maxsus to‘plami hamda shifrlash algoritmi ma’lum bo‘lishi lozim.

Kriptotahlil uchun ochiq matnlar to‘plamini (A) tanlash quyidagi tartibda amalga oshiriladi (1.5-rasm).



1.5-rasm. **Ochiq matnlar to‘plami**

Ushbu rasmda, *m* – tanlab olinuvchi bloklar soni va $m=2^N$, *N* – a_{ij} elementni bitlar soni, *n* – qaralayotgan algoritm kiruvchi blok uzunligiga bog‘liq. Ushbu A – ochiq matnlar to‘plami quyidagicha aniqlanuvchi aktiv va passiv elementlardan tashkil topishi kerak, ya’ni:

– agar $j=1..n$ uchun $a_{1,j}\neq a_{2,j}\neq a_{3,j}...\neq a_{m,j}$ bajarilsa, ochiq matnlardagi $a_{i,j}$ $(i=1...m,\ j=const)$ elementlar aktiv elementlar hisoblanadi;

– agar $j=1..n$ uchun $a_{1,j}=a_{2,j}=a_{3,j}...=a_{m,j}$ bajarilsa, ochiq matnlardagi $a_{i,j}(i=1...m,\ j=const)$ elementlar passiv elementlar hisoblanadi.

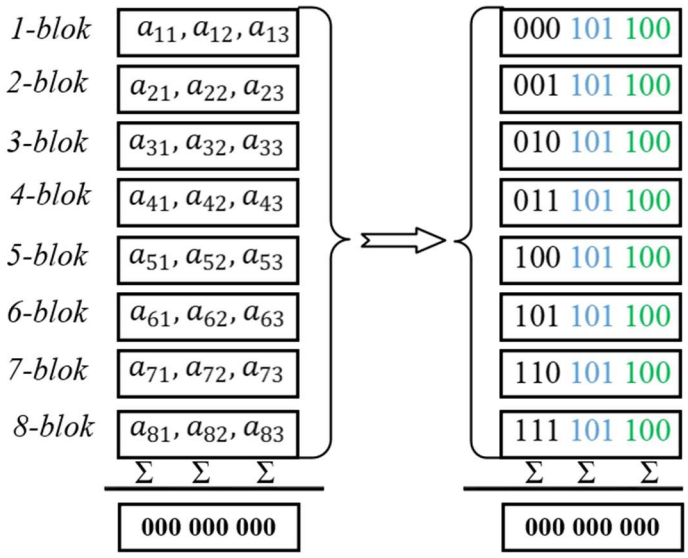
Teorema 1. Ushbu tanlab olingan A – ochiq matnlar to‘plami elementlari uchun quyidagi tenglik o‘rinli [50]:

$$\sum_{i=1}^{m} a_{ij} = 0$$

bu yerda, $j=1,2,3,\dots, n$.

Ochiq matnlar to‘plamini tanlab olishni quyidagi misolda qarab o‘tilada. Aytaylik a_1, a_2, a_3, – biror shifrlash algoritmi uchun kiruvchi blok hamda a_i – bir bayt (bitlar soni 3 ta) bo‘lsin, u holda tanlab olinuvchi bloklar soni 8 ta ($m=2^3=8$) bo‘ladi.

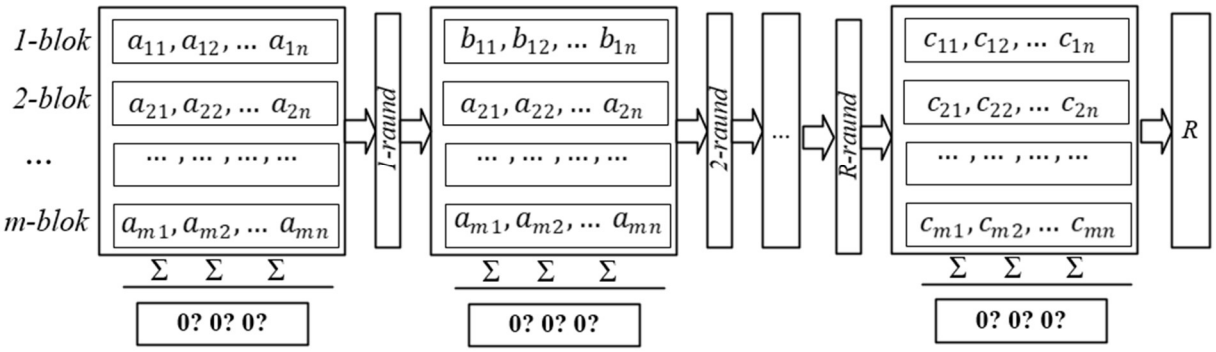
Ushbu bloklarni yuqoridagi talablar asosida quyidagicha shakllantirish mumkin (1.6-rasm):



1.6-rasm. **Ochiq matnlar to‘plami**

Ushbu tanlab olingan ochiq matnlar to‘plami uchun yuqoridagi teorema shartlari qanoatlanadi. Ya’ni, har bir ochiq matnlar blokining mos elementlari yig‘inidisi (*XOR*) nolga teng bo‘ladi. Shuningdek, ushbu ochiq matnlar to‘plamida mos ravishda birinchi elementlari aktiv, qolgan elementlari esa mos ravishda passiv elementlar hisoblanadi.

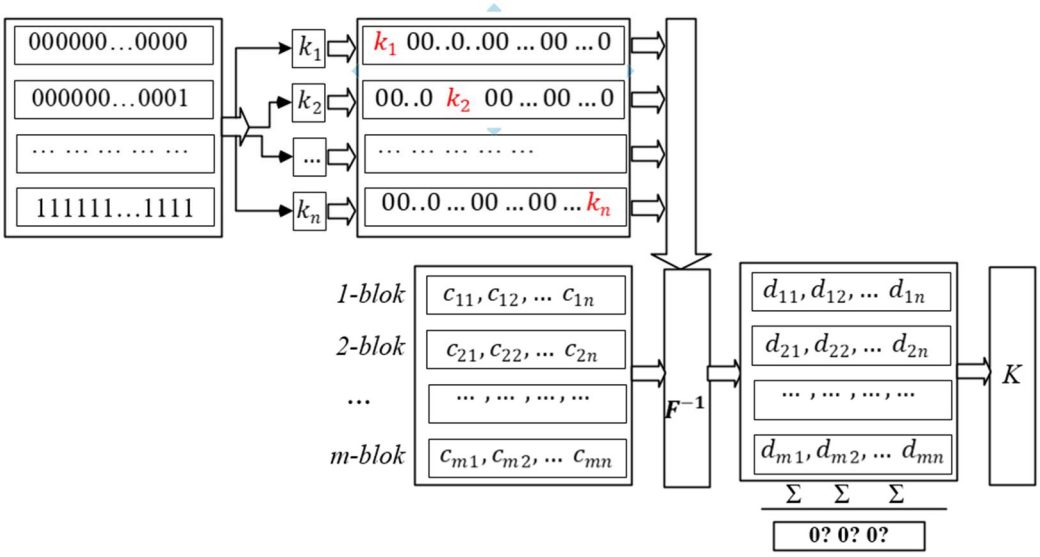
Kriptotahlil jarayonida, tanlab olingan A to‘plam xususiyatining shifrlash algoritmi raundlaridan o‘tganda qanday o‘zgarishi bo‘yicha tadqiqot olib boriladi (1.7-rasm). Agar kuzatilayotgan ochiq matnlar to‘plamining biror R-raunddan chiqish holatida balanslashganlik xususiyati buzulib, aktiv yoki passiv baytlar mavjud bo‘lmasa, u holda R raundli shifrlash algoritmining so‘nggi raundida foydalanilgan maxfiy kalitni topish imkoniyati tug‘iladi.



1.7-rasm. **Ochiq matnlar to‘plamini kuzatish sxemasi**

Demak, ochiq matnlar to‘plamini kuzatishda aktiv yoki passiv baytlarning mavjudligi qanchalik ko‘p raundda saqlanib, balanslashganlik

xususiyati bajarilsa, shifrlash algoritmining integral kriptotahlil usuliga kriptobardoshligi ham shu qadar past bo‘ladi.



1.8-rasm. **Kalit qiymatini aniqlashning funksional sxemasi**

Shifrlash algoritmining so‘nggi raundida foydalanilgan kalit qiymatini aniqlash esa, so‘nggi raundga kiruvchi to‘plamda aktiv (yoki passiv) bayt mavjudligini hamda so‘nggi raunddan chiquvchi ma’lumotni bilgan holda, statistika o‘tkazish yo‘li orqali amalga oshiriladi. 1.8-rasmda ushbu jarayonni amalga oshirishning funksional sxemasi keltirilgan.

Tanlab olingan ochiq matnlarga mos shifr matnlarni biror tanlab olingan kalit asosida bir raund deshifrlanadi. Agar deshifrlashdan hosil bo‘lgan matnlar uchun yuqoridagi teorema sharti bajarilsa, ushbu kalit nomzod kalitlar ro‘yxatiga qo‘shiladi. Ushbu jarayon, barcha tanlab olingan kalitlar uchun amalga oshiriladi.

Integral kriptotahlil usuli adaptiv tanlangan ochiq matnlar asosidagi hujum turi hisoblanib, asosan SP tarmog‘iga asoslangan shifrlash algoritmlari uchun qo‘llaniladi. Ushbu usulning asosiy g‘oyasi paydo bo‘lgandan so‘ng, turli mutaxassislar tomonidan ushbu kriptotahlil usuli yanada mukammallashtirildi va Square shifriga o‘xshash bo‘lgan CRYPTON, Rijndael va SHARK kabi algoritmlarga qo‘llanildi. IK usulining turli modifikatsiyalari Hierocrypt, IDEA, Camellia, Skipjack, MISTY1, MISTY2, SAFER++, KHAZAD va FOX shifrlash algoritmlariga ham qo‘llanilib, tegishli natijalar olingan [25].

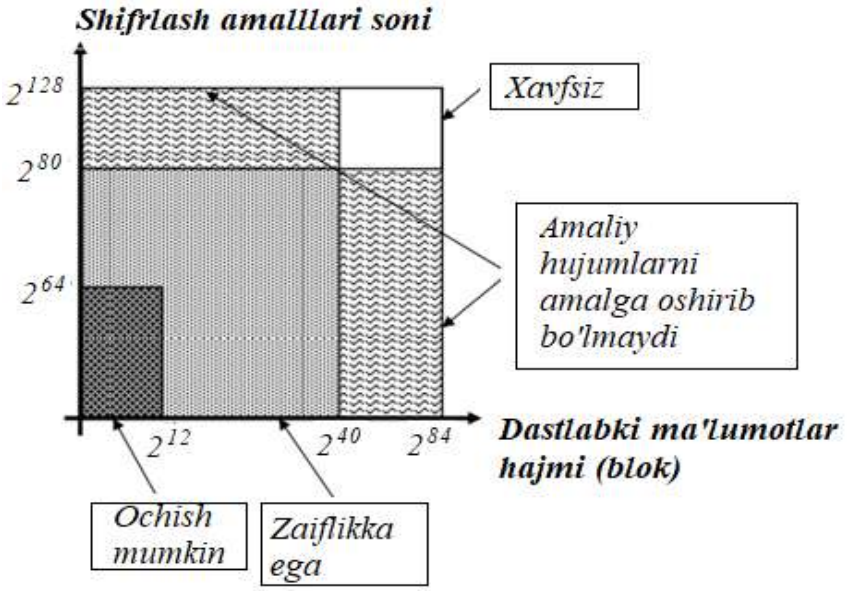
1.3-§. Zamonaviy simmetrik blokli shifrlash algoritmlarining kriptotahlili

Kompyuter texnologiyalarining rivojlanishi, yuqori qiyinchilikdagi masalalarni yechish imkoniyatlarini ortishi shifrlash algoritmlari va ular yordamida shifrlangan maxfiy xabarlarning oshkor bo‘lish xavfini orttirmoqda. Shu bois, kriptografik algoritmlarning bardoshligini tekshirish va uning natijasida algoritmlarni takomillashtirish yoki o‘zgartirish muhim masalalardan hisoblanadi. Kriptografik algoritm bilan bog‘liq bo‘lgan har qanday zaiflik tahdidchi uchun qo‘l kelishi va maxfiy ma’lumotning oshkor bo‘lishiga olib kelishi mumkin [103].

Bugungi kunda zamonaviy kompyuter imkoniyatlari talab etiluvchi dastlabki ma’lumotlar va hisoblash resurslariga ko‘ra ixtiyoriy kriptotahlil usulining amaliy ahamiyatini 1.9-rasmda tasvirlangan grafik asosida baholash mumkin. Shuni ta’kidlash lozimki, kompyuter imkoniyatlarining oshishi quyida tasvirlangan sohalar ko‘lamining kengayishiga ham sababchi bo‘ladi.

Ushbu fikrlarga asoslangan holda, kriptografiya sohasidagi muhim masalalardan biri taklif etilayotgan shifrlash algoritmi kalit o‘lchamining qanday uzunlikda bo‘lishi hisoblanadi.

Bugungi kunda axborot xavfsizligi sohasida yetakchi institut va tashkilotlar tomonidan mazkur masala yechimi bo‘yicha turli tavsiyalar ishlab chiqilgan. 1.1-jadvalda blokli shifrlarning ayrim kriptotahlil usullariga kriptobardoshligini ishonchli ta’minlovchi kalit uzunliklari keltirilgan [25].



1.9-rasm. **Turli kriptotahlil usullarini amaliy qo‘llash imkoniyatlarini baholash**

Demak, jadval qiymatlaridan kelib chiqib, blokli simmetrik shifrlash algoritmlari maxfiy seans kalitlari 128 bit qiymatdan kichik bo‘lishi tavsiya qilinmaydi.

Ma’lumki, qator davlatlarda axborotni kriptografik himoyalash usullari, xususan, simmetrik blokli shifrlash algoritmlari, bo‘yicha standartlar mavjud. Quyida ular orasidan keng tarqalgan simmetrik blokli shifrlash algoritmi va standartlari, ularning xususiyatlari, kriptotahlil natijalari haqida ma’lumotlar keltirilgan.

DES. Qabul qilingan standartlar orasida dastlabkilaridan biri – DES shifrlash algoritmi hisoblanadi. Ushbu algoritm 1977-yilda IBM (International Business Machines) kompaniyasi tomonidan yaratilgan va shu yilda Amerikaning standart shifrlash algoritmi sifatida qabul qilingan. DES shifrlash algoritmida 64 bitli blok uzunligi va 56 bitli kalit uzunligidan foydalaniladi. Algoritm Feystel tarmog‘iga asoslangan bo‘lib, 16 raund shifrlashni amalga oshiradi [107]. Biroq, algoritmda 56 bitli kalit qo‘llanilganligi uchun to‘liq kriptotahlilga uchragan va bugungi kunda bardoshli shifrlash algoritmi hisoblanmaydi. DES algoritmining shifrlash kalitini “to‘liq tanlash” kriptotahlil usuli yordamida 2^{55} ta qadamda topilgan [89]. Bundan tashqari, DES algoritmiga nisbatan chiziqli [58], differensial [59], chiziqli-differensial [84] va algebraik kriptotahlil [85] usullari qo‘llanilgan.

1.1-jadval

Shifr bardoshligini ta’minlovchi kalit o‘lchamlari [120]

Tavsiya etuvchining shartli nomi (e’lon qilingan yil)	**Kalit uzunligi (bit)**	**Foydalanish davri (yil)**
Lenstra / Verheul [27]	128	2076
	192	2159
	256	2243
Lenstra Updated [27]	128	2090
	192	2186
	256	2282
ECRYPT [28]	128	2018 - 2028
	192	2029 - 2068
	256	2029 - 2068
NIST [29]	128	2019 – 2030 & undan keyingi

	192	2019 – 2030 & undan keyingi
	256	2019 - 2030 & undan keyingi
ANSSI [30]	128	2021 - 2030
	192	> 2030
	256	> 2030
BSI [31]	128	2020 - 2022
	192	2023 - 2026
	256	2023 - 2026

Twofish. AES konkursi finalchilaridan biri bo‘lgan Twofish algoritmi 128 bit blok uzunligiga hamda kalit uzunligi 128, 192 va 256 bitga teng bo‘lgan simmetrik blokli shifrlash algoritm hisoblanadi. Bu shifrlash algoritmi Feystel tarmog‘iga asoslangan bo‘lib, 16 raundli F funksiya orqali kalitga bog‘liq holda hosil bo‘ladigan to‘rtta 8 bit kirish va 8 bit chiqishdan iborat S-jadvallar, GF(2^8) maydonda hisoblanadigan 4×4 o‘lchamdagi o‘zgarmas MDS matritsasi, PHT (pseuda-HAdamard transform) almashtirishlari, siklik surish va hosil qilinadigan kalit jadvallaridan iborat [93].

Shu vaqtgacha, Twofish algoritmiga qarshi bir qancha kriptotahlil usullari qo‘llanilgan. Xususan, S.Moriai va Y.L.Yin tomonidan taklif etilgan differensial kriptotahlil usulida 16-raund kalitini topish uchun 2^{51} ta tanlangan ochiq va 2^{77} ta differensial juftlik talab qilinishi aytilgan [66]. Biroq, bu hujum nazariy bo‘lib, algoritm muallifi B.Shnayer tomonidan amaliy jihatdan imkonsiz ekanligi aytilgan. Shuningdek, Twofish algoritmiga algebraik kriptotahlil usuli qo‘llanilib, 7200 sekundda 96 bit kalit topilgan [66].

Camellia. Camellia simmetrik blokli shifrlash algoritmida blok uzunligi 128 bit, kalit uzunliklari 128, 192 va 256 bitga teng. Algoritm Nippon Telegraph, Telephone Corporation va Mitsubishi Electric Corporation kompaniyalari tomonidan 2000-yilda ishlab chiqilgan. Yaponiyaning CRYPTREC tashkiloti tomonidan sanoat va davlat tomonidan foydalanish uchun tavsiya etilgan algoritm sifatida sertifikatlangan. Camellia algoritmi Feystel tarmog‘iga asoslangan bo‘lib, raund boshida va oxirida shakl almashtirish, chiziqli bo‘lmagan S-bokslar, har 16 sikldagi chiziqli tarqalish blokidan (bayt sathida XOR amali) va bayt almashtirishdan foydalanilgan. Kalit uzunligiga qarab, 18

raund (128-bitli kalitdan foydalanilganda) yoki 24 raundga (192 va 256-bitli kalitlardan foydalanilganda) teng bo‘lgan variantlari mavjud.

Camellia algoritmiga nisbatan bir qancha kriptotahlil usullari qo‘llanilgan. Xususan, differensial kriptotahlil usuli qo‘llanilganda algoritmning 192 bit kalitli variantining 4-raund kalitini topishda $2^{126.5}$ ta matn va $2^{189.32}$ bit xotira talab qilingan bo‘lsa [68], 256 bit kalitli varianti uchun 12-raund kalitini topish uchun $2^{119.8}$ matn va $2^{220.87}$ sekund vaqt talab qilingan [69]. Shuningdek, algoritmga nisbatan chiziqli-differensial tahlil usuli qo‘llanilgan va 9-raund kalitini topish uchun 2^{14} matn, $2^{185.5}$ bit xotira talab qilingan bo‘lsa, 10-raund kalitini topish uchun 2^{14} matn va $2^{245.6}$ bit xotira ta’lab qilingan [67]. Bundan tashqari, Camellia algoritmiga nisbatan integral kriptotahlil usuli qo‘llanilgan. Bunda algoritmning 128 bitli varianti uchun 9-raund kalitini topishda $2^{86.9}$ ta matn va 2^{66} bit xotira talab qilingan bo‘lsa, 256 bitli varianti uchun $2^{250.8}$ ta matn va $M=2^{66}$ bit xotira talab qilingan [70].

AES. AES standarti tarkibini 2000-yil 2-oktyabrda NIST tomonidan e’lon qilingan tanlov g‘olibiga aylangan Rijndeal algoritmi tashkil qiladi. Algoritm 2001-yil 28-fevralda nashr etilgan va 2001-yil 26-noyabrda AES FIPS 197 nomi bilan Amerika Qo‘shma shtatlar shifrlash standarti sifatida qabul qilingan [94]. AES algoritmida blok uzunligi 128 bit, kalit uzunliklari 128, 192 va 256 bitni tashkil qiladi. Shifrlash raundlari soni kalitlarga mos holda 10, 12 va 14 tani tashkil qiladi. AES shifrlash algoritmini yaratishda SPN tarmog‘idan foydalanilgan [95].

AES shifrlash algoritmiga nisbatan bir qancha kriptotahlil usullari qo‘llanilgan. Algoritmga 3-raundgacha amalga oshirilgan chiziqli kriptotahlil usuli 2^{32} ta matnni talab qilgan [71]. Differensial kriptotahlil usulida esa, AES-256 variantining 10-raund kalitini topishda $2^{244.4}$ matn, $2^{240.1}$ sekund vaqt va $2^{181.4}$ bit xotira talab qilingan [72]. AES standartiga nisbatan amalga oshirilgan integral kriptotahlil usulida AES-256 variantining 8-raundigacha bo‘lgan kalitlarini topishda 2^{128}-2^{119} ta tanlangan matn, 2^{104} bit xotira va 2^{204} sekund vaqt sarflangan [73]. Bundan tashqari, AES algoritmiga suriluvchi kriptotahlil usuli qo‘llanilgan va AES-256 varianti uchun 14-raund kalitini topishda 2^{131} sekund vaqt va 2^{65} bit xotira talab qilingan [74].

GOST R 34.12-2015. GOST R 34.12-2015 standarti Rossiya Federatsiyasining amaldagi ma’lumotlarni shifrlash algoritmi hisoblanadi. GOST R 34.12-2015 standarti Magma va Kuznechik algoritmlaridan iborat bo‘lib, standart 2015-yili 19-iyunda qabul qilingan va 2016-yil 1-yanvardan kuchga kirgan. Algoritm Rossiya

Federatsiyasining FSB (Federalnaya slujba bezopasnosti) va “Axborot texnologiyalari va aloqa tizimlari” OAJ (“InfoTeKS” OAJ) ishtirokida ishlab chiqilgan. GOST R 34.12-2015 tarkibidagi Kuznechik algoritmida 128 bit blok va 256 bit kalit uzunligidan foydalaniladi. Algoritm SPN (Substitution-permutation networks) tarmog‘i asosida qurilgan bo‘lib, 10 ta raundda shifrlash amallarini bajaradi.

Kuznechik algoritmiga nisbatan bir nechta kriptografik hujumlar amalga oshirilgan. Masalan, standart tarkibidagi Kuznechik algoritmga qaratilgan “O‘rtada uchrashish” hujumda 2^{113} ta matn, 2^{140} sekund vaqt va 2^{153} bit xotira talab qilgan [76]. Bundan tashqari, algoritmga nisbatan differensial kriptotahlil usuli qo‘llanilib, 3-raund kalitini topishda $2^{108} + 6 \cdot 2^{120}$ ta matn ustida statistik tahlil o‘tkazish kerak bo‘lgan [75].

SM4. SM4 algoritmi bu Xitoy Xalq Respublikasining amaldagi ma’lumotlarni shifrlash standarti hisoblanadi. SM4 standarti Xitoyda simsiz LAN va WAPI (WLAN Authentication and Privacy Infrastructure) muhiti uchun qo‘llanilib, dastlab SMS4 deb nomlangan bo‘lsa, 2012-yil 21-martdan SM4 nomiga o‘zgartirilgan [121]. SM4 algoritmi professor Lyu Shu-Vang tomonidan yaratilgan va 2006-yilda Xitoy milliy shifrlash standarti sifatida e’lon qilingan. Standart 128 bit blok va 128 bit kalit uzunligidan foydalaniladi. SM4 shifrlash algoritmi Feystel tarmog‘iga asoslangan bo‘lib, 32 raundli shifrlashni amalga oshiradi.

Hozirgi kunga qadar SM4 algoritmiga chiziqli va differensial kriptotahlil usullari qo‘llanilgan. Algoritmga qaratilgan chiziqli kriptotahlilda 24-raundgacha bo‘lgan shifrlash kalitlarini topishda $2^{122.6}$ sekund vaqt, $2^{126.6}$ ta matn va $2^{121.7}$ bit xotira talab qilishi aytilgan [77]. Differensial kriptotahlil usulida 23-raundgacha bo‘lgan kalitlarni topish uchun 2^{128} ta matn ustida tahlil o‘tkazish talab qilingan [78].

ARIA. Mazkur algoritm Janubiy Koreada 2004-yildan ma’lumotni shifrlash standarti sifatida tan olingan. ARIA algoritmi SPN tarmog‘ida yaratilgan bo‘lib, 128 bit blok uzunligiga hamda 128, 192 va 256 bit kalit uzunliklariga ega. Algoritm kalitlarga mos holda 12, 14 va 16 raundlarli shifrlashni amalga oshiradi. ARIA algoritmida ikkita 8×8 bit o‘lchamdagi S bloklar va ularning inversiyalaridan foydalanilgan. S bloklarning biri Rijndeal shifrlash algoritmidagi S blokka teng.

Ishlab chiquvchilar tomonidan algoritmni chiziqli, differensial kriptotahlil usullariga va rivojlanish davrida mavjud bo‘lgan barcha hujumlarga qarshi kafolatlangan bardoshlikka egaligi ta’kidlangan. Shunga qaramay, hozirgi kungacha ARIA shifrlash algoritmiga nisbatan bir qancha kriptotahlil hujumlari amalga oshirilgan. Algoritmning ARIA-

256 variantiga o‘tkazilgan chiziqli kriptotahlil usuli $2^{123.53}$ ta matn, $2^{238.13}$ sekund vaqt va $2^{239.95}$ bit bit xotirani talab qilgan [79]. Shuningdek, ARIA algoritmiga defferensial kriptotahlil usuli qo‘llanilib, 6-raund kalitini topish uchun 2^{121} ta matn va 2^{112} bit xotira zarurligi aniqlangan [80]. Bundan tashqari, chiziqli-differensial kriptotahlil usuli $2^{84.6}$ ta matn, $2^{215.3}$ sekund vaqt va 2^{224} bit xotira bilan 7-raund kalitini topish mumkinligi isbotlangan [81]. ARIA algoritmining 6-raundgacha bo‘lgan shifrlash kalitlari integral kriptotahlil usuli asosida $2^{124.4}$ ta matnni $2^{172.4}$ sekundda tahlil natijasida topilgan [82].

BelT. Mazkur shifrlash algoritmi Belorussiya Respublikasining simmetrik shifrlash va axborot yaxlitligini boshqarish bo‘yicha davlat standarti hisoblanadi. Standartning to‘liq nomi STB 34.101.31-2007 “Axborot texnologiyalari va xavfsizlik. Shifrlash va yaxlitlikni boshqarish uchun kriptografik algoritmlar”, deb nomlangan. Algoritm 2007-yilda dastlabki standart sifatida qabul qilingan va 2011-yilda yakuniy standart sifatida amalga oshirilgan. BelT algoritmida 256 bit kalit va 128 bit blok uzunligidan foydalaniladi. Shifrlash raundlari soni esa 8 taga teng. Algoritm Feystel va Lai-Messey tarmoqlari kombinatsiyasi asosida yaratilgan [96]. BelT algoritmiga ham bir qancha kriptotahlil usullari qo‘llanilgan. Xususan, differensial kriptotahlil usulida 4-raund kalitini topishda 2^{114} ta matn, $2^{237.14}$ sekund vaqt va 2^{224} bit xotira talab qilingan [83]. Algoritmga nisbatan qo‘llanilgan integral kriptotahlilni $T=2^{254.61}$ sekundda 2^{33} ta matn bilan $R=3\frac{6}{7}$ raundgacha davom ettirish mumkinligi ko‘rsatilgan [85].

DSTU 7624:2014. Mazkur standart Ukraina davlatining blokli simmetrik shifri “Axborot texnologiyalari. Axborotning kriptografik himoyasi. Simmetrik blokli shifrlash algoritmi”, deb nomlanib, 2015-yil 1-iyuldan kuchga kiritilgan. DSTU 7624:2014 standarti Davlat maxsus aloqa xizmati va yetakchi olimlar bilan hamkorlikda xalqaro ochiq kriptografik algoritmlarning milliy tanlovi tajribasi asosida ishlab chiqilgan [97]. Algoritm Kalina deb nomlanib, unda 128, 256, va 512 bitli bloklardan va xuddi shunday uzunlikdagi kalitlardan foydalanilgan. Kalitlarga mos holda 10, 14 va 18 raundlarda shifrlash amallari bajariladi. Kalina algoritmi SP tarmog‘i asosida ishlab chiqilgan. Algoritmga qo‘llanilgan differensial kriptotahlil usulida 4-raund kalitini topishda Kalina-128 varianti uchun $2^{14.6}$ sekund, Kalina-256 varianti uchun $2^{29.2}$ sekund hamda Kalina-512 varianti uchun $2^{58.4}$ sekund vaqt sarflangan [86]. Bundan tashqari, “O‘rtada uchrashish” hujum usulida Kalina-256

varianti uchun 7-raund kalitini topishda 2^{233} ta matn, $2^{502.2}$ sekund vaqt va 2^{170} bit xotira talab qilingan [87].

O‘z DSt 1105:2009. O‘zbekiston Respublikasida ham ma’lumotlarni shifrlash bo‘yicha milliy standart mavjud. O‘zbekiston Respublikasining Ma’lumotlarni shifrlash algoritmi (MShA) O‘z DSt 1105:2009 deb nomlanib, “UNICON.UZ” DUK tomonidan 2009-yil 15-oktyabrda yaratilgan va O‘zstandart agentligining №05-163-sonli qarori va O‘zbekiston aloqa va axborotlashtirish agentligining 19.10.2009 yildagi №328-sonli buyrug‘i bilan kuchga kiritilgan [122]. Ma’lumotlarni shifrlash algoritmi dasturiy, apparat yoki apparat-dasturiy kriptografik modullarda amalga oshirish uchun mo‘ljallangan [114]. Tashkilotlar, korxonalar va muassasalar EHM tarmoqlarida, alohida hisoblash komplekslarida yoki EHMda saqlanuvchi va uzatiluvchi ma’lumotlarning kriptografik muhofazasini amalga oshirishda mazkur standartdan foydalanishlari mumkin [21].

Bugungi kunga qadar O‘z DSt 1105:2009 algoritmining bardoshligi yetarli darajada kriptotahlil qilinmagan. Monografiyada algoritmga qaratilgan algebraik kriptotahlil natijasi 2-raund kalitini topishda 2^{73}sekund vaqt talab qilishini ko‘rsatgan [89]. O‘z DSt 1105:2009 algoritmining to‘liq tavsifi va tahlili keyingi boblarda batafsil keltiriladi. Yuqorida keltirilgan standart va algoritmlarning umumiy tahlil natijalari 1.2 va 1.3-jadvallarda o‘z aksini topgan.

1.2-jadval

Simmetrik blokli shifrlash standartlarining xususiyatlari [118]

Tegishlilik	Algoritm	Algoritm strukturasi	Blok uzunligi	Kalit uzunligi	Raundlar soni
IBM	DES	Feystel	64 bit	56 bit	16
Bryusom Shnayerom	Twofish	Feystel	128 bit	128, 192, 256 bit	16
CRYPTREC	Camellia	Feystel	128 bit	128, 192, 256 bit	18, 24
Amerika shifrlash standarti	Rijndael	SPN	128 bit	128, 192, 256 bit	10, 12, 14
Rossiya	GOST R 34.12-2015	SPN	128 bit	256 bit	10
Xitoy	SM4	Feystel	128 bit	128 bit	32

Janubiy koreya	ARIA	SPN	128 bit	128, 192, 256 bit	12, 14,16
Belorusiya	BelT	Feystel va Lai-Messey kombinasiyasi	128 bit	256 bit	8
Ukraina	DSTU 7624:2014	SPN	128, 256, 512 bit	128, 256, 512 bit	10, 14,18
O‘zbekistan	O‘z DSt 1105: 2009	SPN	128 bit	256, 512 bit	8

1.3-jadval

Zamonaviy simmetrik shifrlarning kriptotahlil natijalari (*D* – tanlangan ochiq matn yoki shifrmatnlar soni, *M* – xotira hajmi yoki operatsiyalar soni, T **– sarflangan vaqt, *R* – deshifrlangan raundlar soni)**

Shifrlash algoritmlari / Kriptotahlil usullari	**DES**	**Twofish**	**Camellia**	**Rijndael**	**GOST R 34.12-2015 (Kuznechik)**
Chiziqli kriptotahlil usuli	$D \in [2^{39}, 2^{41}]$, $M=2^{43}$ [63]	-	-	R=3, $D=2^{32}$ [71]	-
Differensial kriptotahlil usuli	$D=2^{47}$, $M=2^{47}$ [64]	R=16, $D=2^{51}$, $M=10^{15}$ bayt [65]	Camellia-192: R=14, $D=2^{126.5}$, $M=2^{189.32}$ [68]. Camellia-256: R=12, $D=2^{119.8}$, $T=2^{220.87}$ [69].	AES-256, R=8: -$D=2^{89.1}$, $M=2^{229.7}$. -$D=2^{111.1}$,$M=2^{224.3}$ [72].	R=3 , $D= 2^{108} + 6 * 2^{120}$ [75]
Chiziqli-differensial kriptotahlil usuli	R=8, M=512, 80% ehtimollik bilan 10 bit topilgan [89]	-	R=9, $D=2^{14}$, $M=2^{185.5}$. R=10, $D=2^{14}$, $M=2^{245.6}$ [67]	-	-
Algebraik kriptotahlil usuli	R=12, T=6 soat [90]	T=7200 sekundda 96 bit kalit topilgan [66]	-	-	-

Integral kriptotahlil usuli	-	-	Camellia-128: R=9, $D=2^{86.9}$, $M=2^{66}$. Camellia-256: $D=2^{250.8}$, $M=2^{66}$ [70].	AES-256, R=8, $D=2^{128}$-2^{119}, $M=2^{104}$, $T=2^{204}$ [73]	-
Boshqa hujum usullari	-	-	-	Suriluvchi kriptotahlil usuli: AES-256, R=14. $T=2^{131}$, 2^{65} [74].	“O‘rtada uchrashish” hujum usuli: $D=2^{113}$, $T=2^{140}$, $M=2^{153}$ [76].
Chiziqli kriptotahlil usuli	R=24, $T=2^{122.6}$, $D=2^{126.6}$, $M=2^{121.7}$ [77].	ARIA-256 $D=2^{123.53}$, $T=2^{238.13}$, $M=2^{239.95}$ [79]	-	-	-
Differensial kriptotahlil usuli	R=23, $D=2^{128}$ [78]	R=6, $D=2^{121}$, $M=2^{112}$ [80]	$R=4\frac{1}{7}$, $D=2^{114}$, $T=2^{237.14}$, $M=2^{224}$ [83].	**R=4:** Kalyna-128: $T=2^{14.6}$, Kalyna-256: $T=2^{29.2}$, Kalyna-512: $T=2^{58.4}$ [86].	-
Chiziqli-differensial kriptotahlil usuli	-	R=7, $D=2^{84.6}$, $T=2^{215.3}$, $M=2^{224}$ [81]	-	-	-
Algebraik kriptotahlil usuli	-	-	-	-	R=2, $T=2^{73}$ [88].
Integral kriptotahlil usuli	-	R=6, $D=2^{124.4}$, $T=2^{172.4}$[82]	$R=3\frac{6}{7}$, $D=2^{33}$, $T=2^{254.61}$ [84].	-	R=4, $D=2^{72}$ [2.3-bo‘lim].
Boshqa hujum usullari	-	-	Kalitga bog‘liq hujum R=5, $D=2^{123.28}$, $T=2^{228.4}$ [85].	“O‘rtada uchrashish” hujum usuli: R=7, DSTU Kalyna -256, $D=2^{233}$, $T=2^{502.2}$, $M=2^{170}$ [87].	-

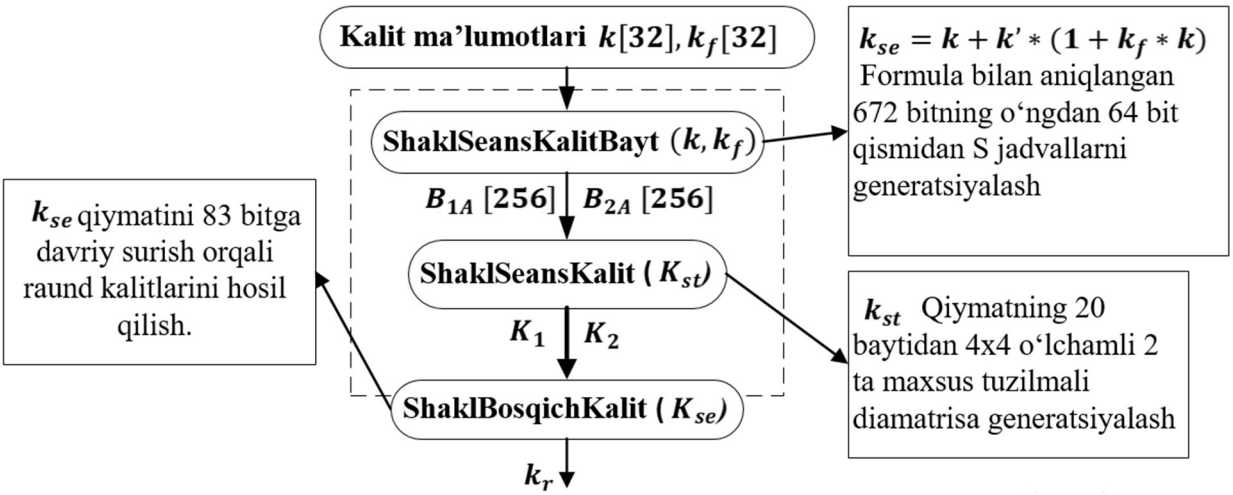
Shifrlash algoritmlarining kriptobardoshligi D – tanlangan ochiq matn yoki shifrmatnlar soni, M – xotira hajmi yoki operatsiyalar soni va T – sarflangan vaqt kabi resurslarning yuqori bo‘lishi bilan o‘lchanadi. Ya’ni ushbu resurslarni ta’minlash uchun hisoblash texnikasining imkoniyati yetmaganda ushbu algoritm kriptobardoshli hisoblanadi. 1.3-jadvalda simmetrik blokli shifrlash algoritmlariga qaratilgan eng yaxshi kriptotahlil natijalari keltirilgan. Simmetrik blokli shifrlash algoritmlarida R-raundda shifrlash amalga oshirilganligi sababli kriptotahlilni ham shuncha raund amalga oshirilganda algoritm to‘liq buzilgan hisoblanadi. Ushbu 1.3-jadvaldan ko‘rish mumkinki, DES shifrlash algoritmidan boshqa shifrlash algoritmlari to‘liq kriptotahlilga uchramagan.

II BOB. O‘Z DST 1105:2009 SHIFRLASH ALGORITMINING KRIPTOBARDOSHLIGINI ALGEBRAIK VA INTEGRAL KRIPTOTAHLIL USULLARI YORDAMIDA BAHOLASH

2.1-§. O‘z DSt 1105:2009 shifrlash algoritmining tavsifi

O‘z DSt 1105:2009 algoritmi O‘zbekiston Respublikasining amaldagi shifrlash standarti hisoblanadi. Ushbu “Ma’lumotlarni shifrlash algoritmi” (MSHA) standarti elektron ma’lumotlarni muhofaza qilish uchun mo‘ljallangan kriptografik algoritmni ifodalaydi [21]. MShA – simmetrik blokli shifr bo‘lib, 256 bit uzunlikdagi ma’lumotlar blokini shifrmatnga o‘girish va shifrmatnni dastlabki matnga o‘girish uchun 256 yoki 512 bit uzunlikdagi kriptografik kalitlardan foydalanadi.

Algoritm asosan ikki qismdan kalitlarni generatsiyalash va shifrlash/ rasshifrovkalash jarayonlaridan tashkil topgan. Kalitlarni generatsiyalash bosqichida shifrlash kaliti va funksional kalitdan foydalanib raund kalitlarini va S bloklarni hosil qilish bosqichlari bajariladi. Bu bosqichlar quyidagi 2.1-rasmda keltirilgan $ShaklSeansKalitBayt()$, $ShaklSeansKalit()$, $ShaklBosqichKalit()$ funksiyalarini ketma-ket bajarish orqali amalga oshiriladi [21].



2.1-rasm. **Raund kalitlari va S bloklarni generatsiyalash tartibi**

$ShaklSeansKalitBayt(k[32], k_f[32])$almashtirish funksiyasining vazifasi seans kalitini hosil qilish va uning yordamida S bloklarni generatsiyalashdan iborat.

Seans kaliti:

$$k_{se} = k + k' * (1 + k_f * k)$$

formula yordamida hosil qilingan qiymatning chapdan *672* bitini ajratib olish orqali hosil qilinadi.

Bu yerda, k va k_f – mos holda tanlangan shifrlash va funksional kalitlar, $k' - k_f$ning o‘ngdan *192* bitli qismi hisoblanadi.

Hosil qilingan seans kaliti yordamida $S-$ bloklarni generatsiyalash quyidagi tartibda amalga oshiriladi:

– k_{se}seans kalitining o‘ngdan *256+64* bitli qismi ajratib olinadi va uning chapdan *256* bitli qismidan baytli elementlardan tarkib topgan chiziqli massiv $k_{st} = [0,1,2,3, \dots 31]$, qolgan *64* bitli qismidan – bayt sathida elementlardan tarkib topgan chiziqli massiv $B = [0,1,2,3,4,5,6,7]$ shakllantiriladi;

– chiziqli massiv B elementlari $B_1 = [0,1,2,3]$ va $B_2 = [4,5,6,7]$ massivlarga ajratiladi va ulardan ma’lum qoidalar asosida (d_1, R_1, L_1) va (d_2, R_2, L_2) parametrlar uchliklari shakllantiriladi [21].

Yuqoridagi uchlik parametrlardan foydalanib bayt sathida shifrlash uchun, toq va juft raundlarda ishlatiladigan chiziqli massivlar juftligidan iborat $(B_{1A}[256], B_{2A}[256])$ S-bloklar quyidagicha formula yordamida hosil qilinadi:

$$i = 0 \div 255 \text{ uchun}$$

$$b_{sA}[i] \equiv \Big(\big((i + L) mod 256\big) + 1\Big) \mid^{ds} (mod\ 257)(mod\ 256) \quad (2.2)$$

Keyingi qadamda $ShaklSeansKalit\,(k_{st})$ funksiyasi yordamida shifrlash va rasshifrovkalashda ishlatiladigan diamatritsalar quyidagicha generatsiya qilinadi:

– baytli elementlardan tarkib topgan chiziqli massiv $k_{st} = [0,1,2,3, \dots 31]$ning chapdan *20* baytli elementlaridan tarkib topgan chiziqli massiv qismi $K_{ss} = [0,1,2,3, \dots 19]$ ajratib olinadi;

– $i = 0 - 19$ uchun, agar $K_{ss}[i] = 0$ bo‘lsa, u holda $K_{ss}[i]$ni $K_{ss}[i] - 1 (mod\ p)$ga almashtiriladi.

Chiziqli massiv K_{ss}ning elementlaridan ikki o‘lchamli $K_1[4,4]$ va $K_2[4,4]$ massivlari quyidagi tartibda shakllantiriladi:

chiziqli massiv $K_S = [0,1,2,3, \dots 19]$ ikkita chiziqli massivlar $k_{s1} = [0,1,2,3, \dots 9]$ va $k_{s2} = [10,11,12,13 \dots ,19]$ga ajratiladi va ularning har biri mos tarzda tartiblangan to‘plam $\{k_{s1}[0,1], k_{s1}[0,2], k_{s1}[0,3], k_{s1}[1,0], \{k_{s1}[2,0], k_{s1}[2,1], k_{s1}[2,2], k_{s1}[3,0], k_{s1}[3,1], k_{s1}[3,2]\}$ va $\{k_{s2}[0,1], k_{s2}[0,2], k_{s2}[0,3], k_{s2}[1,0], k_{s2}[2,0], k_{s2}[2,1], k_{s2}[2,2], k_{s2}[3,0], k_{s2}[3,1], k_{s2}[3,2]\}$ ga o‘zaro – bir qiymatli akslantiriladi va ularning har biridan mos tarzda ikkita $K_1[4,4]$ va $K_2[4,4]$ massivlarining $k_1[i,j], k_2[i,j]$ elementlari shakllantiriladi (bu yerda $i, j \in \{0,1,2,3\}$).

$K_S[4,4], s \in \{1,2\}$ massivlarining qolgan elementlari quyidagi qoida asosida shakllantiriladi:

– $j \in \{0,1,2,3\}$ uchun $i = j$ bo‘lganda, elementlar aynan va qiymati bo‘yicha $K_s[2,2]$ elementga teng;

– $i = 1, j = 0,2,3$ uchun elementlar aynan va qiymati bo‘yicha $K_s[1,0]$ elementga teng;

– $i = 2, j = 0,3$ uchun elementlar aynan va qiymati bo‘yicha $K_s[2,0]$ elementga teng.

Natijada, sh-shifrlash rejimida foydalanish uchun $K_s[8,4]$ sifatida quyidagi $K_1[4,4]$va $K_2[4,4]$ ikkita maxsus tuzilmali diamatritsa shakllanadi.

Massiv K_1

k_1 [0,0]	k_1[0,1]	k_1[0,2]	k_1 [0,3]
k_1 [1,0]	k_1[1,1]	k_1[1,2]	k_1[1,3]
k_1 [2,0]	k_1[2,1]	k_1[2,2]	k_1 [2,3]
k_1[3,0]	k_1[3,1]	k_1[3,2]	k_1 [3,3]

Massiv K_2

k_2[0,0]	k_2[0,1]	k_2[0,2]	k_2[0,3]
k_2[1,0]	k_2[1,1]	k_2[1,2]	k_2[1,3]
k_2[2,0]	k_2[2,1]	k_2[2,2]	k_2[2,3]
k_2[3,0]	k_2[3,1]	k_2[3,2]	k_2[3,3]

sh - shifrlash rejimidan foydalanishda maxsus tuzilmali diamatritsa $K_1[4,4]$uchun teskari maxsus tuzilmali diamatritsa $K_{1t}[4,4]$hisoblanadi. Shuningdek, dsh- rasshifrovkalash rejimidan foydalanishda ham maxsus tuzilmali diamatritsa $K_2[4,4]$ uchun teskari maxsus tuzilmali diamatritsa $K_{2t}[4,4]$ hisoblanadi.

Diaaniqlovchisi noldan farqli maxsus tuzilmali diamatritsa $K_{1i}[4,4]$ni (bu yerda,$i = \{1,2\}$) teskarilash uning ustida diaalmashtirish natijasida hosil bo‘lgan matritsaning teskari matritsasini hisoblash va hosil bo‘lgan teskari matritsa ustida diaalmashtirish amalini bajarish natijasini olishdan iborat.

Teskarilash natijasida ikkala $K_{1t}[4,4]$va $K_{2t}[4,4]$ ham maxsus tuzilmali diamatritsa ko‘rinishiga ega bo‘lgan quyidagi K_{1t} va K_{2t} massivlar hosil bo‘ladi:

Massiv K_{1t}

k_{1t} [0,0]	k_{1t}[0,1]	k_{1t}[0,2]	k_{1t}[0,3]
k_{1t} [1,0]	k_{1t}[1,1]	k_{1t}[1,2]	k_{1t}[1,3]
k_{1t} [2,0]	k_{1t}[2,1]	k_{1t}[2,2]	k_{1t}[2,3]
k_{1t}[3,0]	k_{1t}[3,1]	k_{1t}[3,2]	k_{1t}[3,3]

Massiv K_{2t}

k_{2t}[0,0]	k_{2t}[0,1]	k_{2t}[0,2]	k_{2t}[0,3]
k_{2t}[1,0]	k_{2t}[1,1]	k_{2t}[1,2]	k_{2t}[1,3]
k_{2t}[2,0]	k_{2t}[2,1]	k_{2t}[2,2]	k_{2t}[2,3]
k_{2t}[3,0]	k_{2t}[3,1]	k_{2t}[3,2]	k_{2t}[3,3]

sh – shifrlash rejimidan foydalanishda (K_{1t}, K_2) juftlik, dsh-rejimidan foydalanishda esa (K_1, K_{2t}) juftlik ishlatiladi.

Keyingi bosqichda $ShaklBosqichKalit(k_{se})$ almashtirish funksiyasi (chiziqli seans-bosqich kaliti massivini shakllantirish) yordamida raund kalitlari quyidagicha generatsiya qilinadi:

– *bosqich=1* va *m=sh* bo‘lsa, u holda chiziqli seans-bosqich kaliti massivi k_{se} o‘zgarishsiz qoldiriladi, agar *bosqich=0* va *m=dsh* bo‘lsa, u holda k_{se} massivi o‘ngga *672-(ye* x *83) mod 672* bitga suriladi;

– agar *bosqich>1* va *m=sh* bo‘lsa, unda davriy tarzda o‘ngga k_{se} massivi *83* bitga suriladi, agar *bosqich≥1* va *m=dsh* bo‘lsa, unda davriy tarzda chapga k_{se} massivi *83* bitga suriladi.

Chiziqli seans-bosqich kaliti massivining chap tomonidan *256* bitli qismini ajratib olib, undan elementlari bayt sathida berilgan $K_e[8,4]$ massivi shakllantiriladi. Bu almashtirish shifrlash jarayoni boshlangunga qadar hamma bosqichlar uchun amalga oshiriladi.

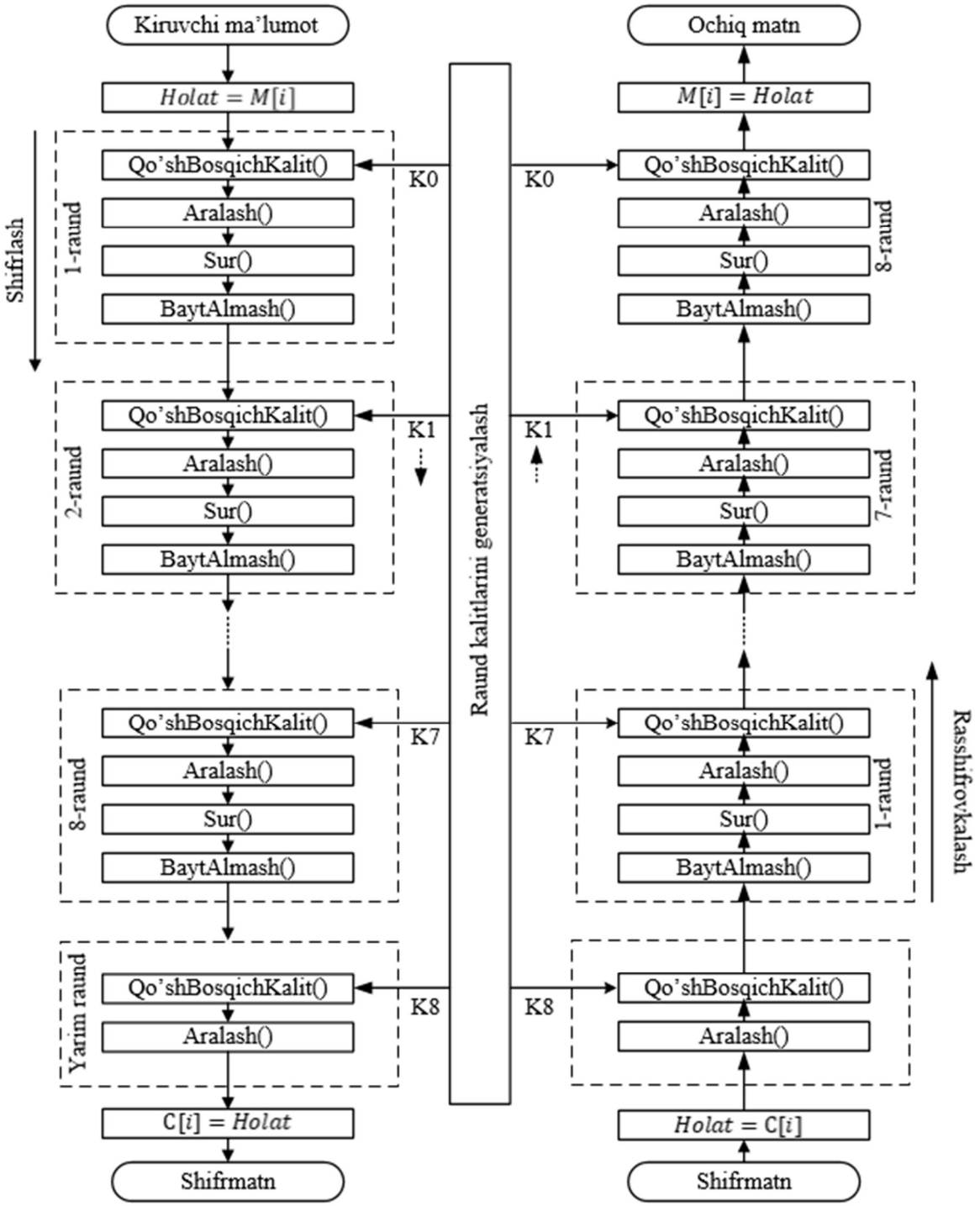
S bloklar generatsiya qilingandan so‘ng ECB rejimi uchun shifrlash/ rasshifrovkalash jarayoni quyidagi 2.2-rasmda ko‘rsatilgani kabi bajariladi.

Dastlab matnni shifrmatnga almashtirish rejimida ochiq matn, shifr matnni dastlabki matnga almashtirish rejimida esa shifrmatn kriptografik modulning *Holat[8,4]* massiviga yuklanadi. Keyin 8 ta raundning har birida *Qo‘shBosqishKalit (Holat,*K_e*), Aralash (Holat,*K_S*), Sur (Holat), BaytAlmash (Holat,*B_a*)* funksiyalari bajariladi. 8-raund tugagandan so‘ng esa faqat *Qo‘shBosqichKalit (Holat,* K_e*), Aralash (Holat,* K_S*)* funksiyalari bajariladi. Shifrlash jarayoni 2 xil rejimda amalga oshiriladi. Bular shifrmatn bloklarini ilaktirish (Cipher block chaining, CBC) va elektron kod kitobi (Electronic code book, ECB) rejimlaridir.

Ochiq matn *Holat [8,4]* massiviga yuklangandan so‘ng *Qo‘shBosqichKalit (Holat,*K_e*)* funksiyasi yordamida *Holat* massivi va $K_e[8,4]$ seans kaliti massivlarining har bir bayt sathdagi bir nomli elementlari ustida XOR amali quyidagi tartibda bajariladi:

0 $\leq c <$ *8* uchun

$$[h'[c,0], h'[c,1], h'[c,2], h'[c,3]] =$$
$$[h[c,0], h[c,1], h[c,2], h[c,3]] \oplus [ke[c,0], ke[c,1], ke[c,2], ke[c,3]].$$



2.2-rasm. **O‘z DSt 1105:2009 algoritmi shifrlash/ rasshifrovkalash jarayonininig tavsifi**

Natija *Holat* massiviga ko‘chiriladi. Keyin *Sur (Holat)* funksiyasi bajariladi. *Sur (Holat)* almashtirishi agar *m= sh* rejimida bo‘lsa, unda davriy tarzda *Holat* massivining $j-$ustuni avvalo, pastga $(j+1)\ (mod\ 8)$ baytga suriladi, keyin hosil bo‘lgan massivning $i-$satri o‘ngga $(i+1)\ (mod\ 4)$ baytga suriladi, aks holda *m=dsh* bo‘lsa, unda davriy tarzda *Holat* massivining $i-$satri avvalo, chapga $(i+1)\ (mod\ 4)$

baytga suriladi, so‘ngra hosil bo‘lgan massivning j – ustuni yuqoriga $(j + 1)\ (mod\ 8)$ baytga suriladi. Bu yerda, $0 \le i < 4, 0 \le j < 8$.

Keyingi amal *Aralash (Holat, K_s)* quyidagi amallarni bajarishdan iborat:

– agar *m=sh* bo‘lsa, unda $K_1 = K_{1t},\ K_2 = K_2$ qabul qilinadi, $H_1 ⊕_2 K_1 (mod\ p), H_2 ⊕_2 K_2\ (mod\ p)$ hisoblanadi, natija H_1, H_2 massivlariga yozilib, *Holat* massiviga ko‘chiriladi, aks holda, ya’ni *m=dsh* bo‘lsa, unda $K_1 = K_1,\ K_2 = K_{2t}$ qabul qilinadi, $H_1 ⊕_2 K_1 (mod\ p), H_2 ⊕_2 K_2\ (mod\ p)$ hisoblanadi, natija H_1, H_2massivlariga yozilib, *Holat* massiviga ko‘chiriladi.

So‘nggi funksiya *Bayt Almash (Holat,B_a)* almashtirishi quyidagi amallarni bajarishdan iborat:

– elementlari bayt sathida berilgan $Holat$ [8,4] massivi elementlari bayt sathida berilgan $Holat[8, 4]$ massivi ko‘rinishida nomlanadi;

– agar *m=sh* bo‘lsa, u holda $B_a[256] = B_{sA}[256]$ qabul qilinadi, $Holatb[8, 4]$ massivining har bir elementi B_a massivining adresi bo‘yicha unga mos elementi bilan almashtirilsin va natijaviy $Holatb$ $[8, 4]$ massivi bayt sathida berilgan $Holat[8, 4]$massiviga almashtiriladi, aks holda, ya’ni *m=dsh* bo‘lsa, u holda $B_a[256] = B_{sAD}[256]$ qabul qilinadi, $Holatb$ $[8, 4]$ massivining har bir elementi B_a massivining adresi bo‘yicha unga mos elementi bilan almashtiriladi va natijaviy $Holat$ $[8, 4]$ massivi bayt sathida berilgan $Holat$ $[8, 4]$massiviga almashtiriladi (bu yerda, $s \in \{1,2\}$). Almashtirish natijasining nusxasi *Holat* massiviga ko‘chiriladi va shifrmatn sifatida qabul qilinadi [110].

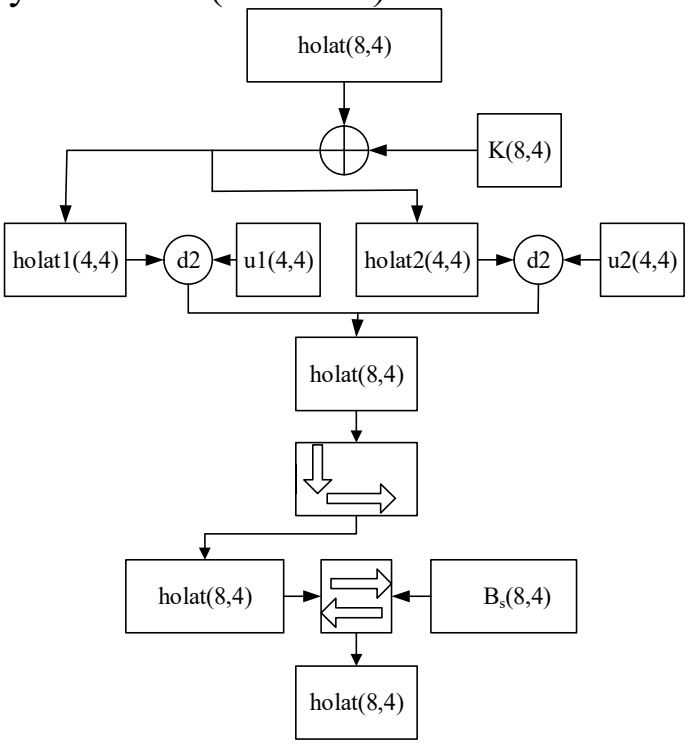
O‘z DSt 1105:2009 shifrlash algoritmidagi *BaytAlmash()* akslantirishidagi *B_1[256]* va *B_2[256]* jadvallar va *Aralash()* akslantirishida foydalanilgan maxsus tuzilmali *K_1[4, 4]* va *K_2[4, 4]* diamatritsalar dastlabki *k* – shifrlash kaliti hamda k_f – funksional kalit asosida dinamik tarzda hosil qilinadi. Mazkur holat shifrlash algoritmiga aniq baho berishga imkoniyat bermaydi. Bundan tashqari, kriptografik algoritmlarni yaratishga qo‘yilgan Kerkxoffs prinsipini qanoatlantirmaydi.

2.2-§. O‘z DSt 1105:2009 shifrlash algoritmining algebraik kriptotahlili

Mazkur bo‘limda O‘z DSt 1105:2009 simmetrik blokli shifrlash algoritmining algebraik kriptotahlil usuli bilan tanishib chiqiladi. O‘z DSt

1105:2009 shifrlash algoritmiga algebraik kriptotahlil usulini qo‘llashda quyidagi masalalarni alohida ko‘rib o‘tish lozim.

Dekompozisiyalash. Dekompozitsiyalash jarayonida shifrlash algoritmining ochiq matn bitlarini shifr matn bitlari bilan bog‘lovchi eng qisqa yo‘l hamda ushbu yo‘lda joylashgan va o‘zaro mustaqil ishlaydigan har bir akslantirish alohida elementlarga ajratiladi. O‘z DSt 1105:2009 algoritmini dekompozitsiyalashda uning quyida keltirilgan bir raundlik strukturasidan foydalaniladi (2.3-rasm).



2.3-rasm. **O‘z DSt 1105:2009 algoritmining bir raundlik dekompozitsion sxemasi**

Bu yerda,

$\oplus$ - akslantirish 2 modul bo‘yicha qo‘shish ($Qo'shBosqichKalit()$) amali, ushbu akslantirishni shartli ravishda X bilan belgilaymiz;

d_2 - akslantirish diamatritsaviy ko‘paytirish ($Aralash()$) amali, ushbu akslantirishni shartli ravishda A bilan belgilaymiz;

- akslantirish ustun va satr bo‘yicha surish ($Sur()$) amali, ushbu akslantirishni shartli ravishda S bilan belgilaymiz;

- akslantirish bayt bo‘yicha chiziqsiz almashtirish ($BaytAlmash()$) amali, ushbu akslantirishni shartli ravishda B bilan belgilaymiz.

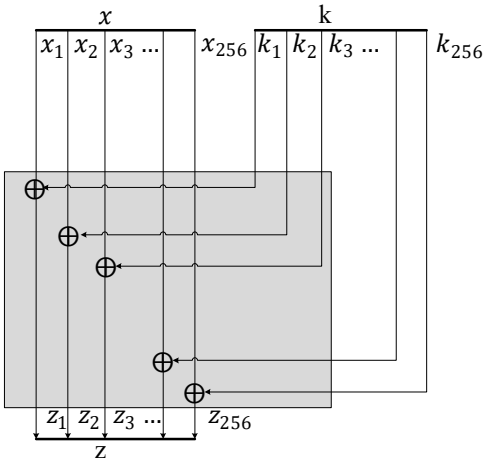
Keltirilgan sxemaga ko‘ra, O‘z DSt 1105:2009 algoritmining har bir raundida foydalanilgan akslantirishlarni 4 tur (*X, A, S, B* - funksiyalar)ga ajratish mumkin.

Qism elementlarga ajratishda shifrlash algoritmida foydalanilgan chiziqsiz akslantirishlar muhim ahamiyat kasb etadi. Chunki, aynan ushbu turdagi akslantirish o‘lchami katta bo‘lsa, ularni ifodalovchi tenglamalar sistemasini qurish ko‘plab hisoblashlarni talab etadi. Shuning uchun, ajratilgan har bir elementning kirish va chiqish o‘lchami imkon qadar kichik bo‘lishi lozim.

Ajratilgan elementlarni algebraik ko‘rinishda ifodalash jarayonida har bir element algebraik tenglamalar sistemasi ko‘rinishida shakllantiriladi. Ya’ni, har bir akslantirish uchun, ularni kirishi va chiqishini bog‘lovchi tenglamalar sistemasi hosil qilinadi. Bir turga mansub bo‘lgan akslantirishlar uchun tenglamalar sistemasini hosil qilish bir xil tarzda amalga oshiriladi. Tuzilgan tenglamalar sistemasi faqat noma’lumlari bilan farqlanadi.

O‘z DSt 1105:2009 algoritmi uchun hosil qilingan qism elementlarni algebraik ifodalashda X, A, S, B – funksiyalarni ko‘rib o‘tish yetarli.

$\boldsymbol{z = X(x, k)}$ – funksiya umumiy uzunligi 256 bit bo‘lgan, har bir elementi baytlardan tashkil topgan (8,4) o‘lchamli ikkita matritsa elementlarini mos ravishda 2 modul bo‘yicha qo‘shish ($\oplus$) jarayonini amalga oshiradi (2.4-rasm).

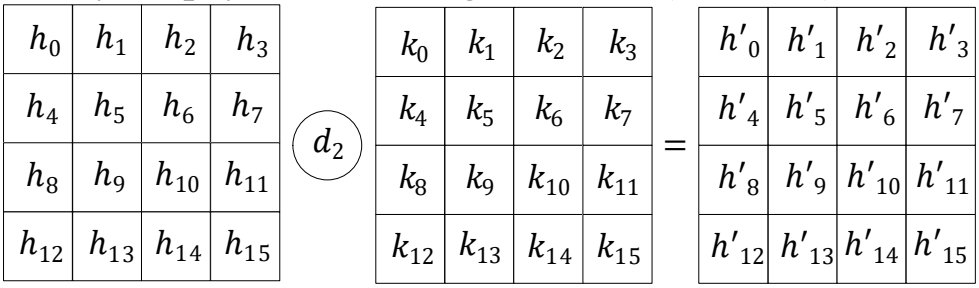


2.4-rasm. $X(x, k)$ **funksiya sxemasi**

Demak, ushbu akslantirish uchun quyidagicha tenglamalar sistemasini qurish mumkin:

$$\begin{cases} z_1 = x_1 \oplus k_1 \\ z_2 = x_2 \oplus k_2 \\ z_3 = x_3 \oplus k_3 \\ \dots\ \dots\ \dots \\ z_{255} = x_{255} \oplus k_{255} \\ z_{256} = x_{256} \oplus k_{256} \end{cases}$$

$\boldsymbol{y = A(x)}$ – funksiya umumiy uzunligi 128 bit bo‘lgan, har bir elementi baytlardan tashkil topgan (4,4) o‘lchamli ikkita matritsa ustida diamatritsaviy ko‘paytirishni amalga oshiradi (2.5-rasm).



2.5-rasm. Diamatritsaviy ko‘paytirish amali

Diamatritsaviy ko‘paytirishni amalga oshirish tartibi esa 2.1-jadvalda keltirilgan.

2.1-jadval

Aralash akslantirishida foydalanilgan diamatritsaviy ko‘paytirish formulasi

h’[0,0]	$h'_0=h_0(k_0+k_4+k_8+k_{12})-h_5k_4-h_{10}k_8-h_{15}k_{12}(modp)$
h’[1,1]	$h'_5=h_5(k_1+k_5+k_9+k_{13})-h_0k_1-h_{10}k_9-h_{15}k_{13}(modp)$
h’[2,2]	$h'_{10}=h_{10}(k_2+k_6+k_{10}+k_{14})-h_0k_2-h_5k_6-h_{15}k_{14}(modp)$
h’[3,3]	$h'_{15}=h_{15}(k_3+k_7+k_{11}+k_{15})-h_0k_3-h_5k_7-h_{10}k_{11}(modp)$
h’[0,1]	$h'_1=h_1(k_1+k_5+k_9+k_{13})+(h_0+h_4+h_8+h_{12})k_1-h_2k_9-$
h’[0,2]	$h'_2=h_2(k_2+k_6+k_{10}+k_{14})+(h_0+h_4+h_8+h_{12})k_2-h_1k_6-$
h’[0,3]	$h'_3=h_3(k_3+k_7+k_{11}+k_{15})+(h_0+h_4+h_8+h_{12})k_3-h_1k_7-$
h’[1,0]	$h'_4=h_4(k_0+k_4+k_8+k_{12})+(h_1+h_5+h_9+h_{13})k_4-h_6k_8-$
h’[1,2]	$h'_6=h_6(k_2+k_6+k_{10}+k_{14})+(h_1+h_5+h_9+h_{13})k_6-h_4k_2-$
h’[1,3]	$h'_7=h_7(k_3+k_7+k_{11}+k_{15})+(h_1+h_5+h_9+h_{13})k_7-h_4k_3-$
h’[2,0]	$h'_8=h_8(k_0+k_4+k_8+k_{12})+(h_2+h_6+h_{10}+h_{14})k_8-h_9k_4-$
h’[2,1]	$h'_9=h_9(k_1+k_5+k_9+k_{13})+(h_2+h_6+h_{10}+h_{14})k_9-h_8k_1-$
h’[2,3]	$h'_{11}=h_{11}(k_3+k_7+k_{11}+k_{15})+(h_2+h_6+h_{10}+h_{14})k_{11}-h_8k_3-$
h’[3,0]	$h'_{12}=h_{12}(k_0+k_4+k_8+k_{12})+(h_3+h_7+h_{11}+h_{15})k_{12}-h_{13}k_4-$
h’[3,1]	$h'_{13}=h_{13}(k_1+k_5+k_9+k_{13})+(h_3+h_7+h_{11}+h_{15})k_{13}-h_{12}k_1-$
h’[3,2]	$h'_{14}=h_{14}(k_2+k_6+k_{10}+k_{14})+(h_3+h_7+h_{11}+h_{15})k_{14}-h_{12}k_2-$

Jadvaldan ko‘rinadiki, $Aralash()$ akslantirishida chiqishdagi $h'[4,4]$ matritsaning diagonal elementlarini hosil qilishda kirishdagi $h[4,4]$ matritsaning 4 ta elementi, nodiagonal elementlarini hosil qilishda esa 7 ta elementi ishtirok etadi. Bu o‘lchamdagi akslantirish uchun

to‘g‘ridan to‘g‘ri tenglamalarni shakllantirish imkoniyati mavjud emasligi sababli akslantirishning kichraytirilgan (2, 3, 4 bitli) variantlari uchun tenglamalar shakllantirilib xususiyatlari o‘rganildi [108].

Ushbu akslantirishning kichraytirilgan variantlari uchun tuzilgan tenglamalarni tahlil qilish jarayonida, umumiy holda quyidagicha qonuniyat o‘rinli ekanligi ham aniqlandi:

Diamatritsa elementlari $k_0 = 01, k_4 = 01, k_8 = 01, k_{12} = 10$ bo‘lgan hol uchun h'_0 hosil qilish formulasi quyidagicha ko‘rinishga ega: $h'_0 = 1h_0 - 1h_5 - 1h_{10} - 2h_{15}(mod4)$.

Ushbu formulani quyidagi:

$$h'_0 = 1h_0 + 3h_5 + 3h_{10} + 2h_{15}(mod4) \qquad (2.4)$$

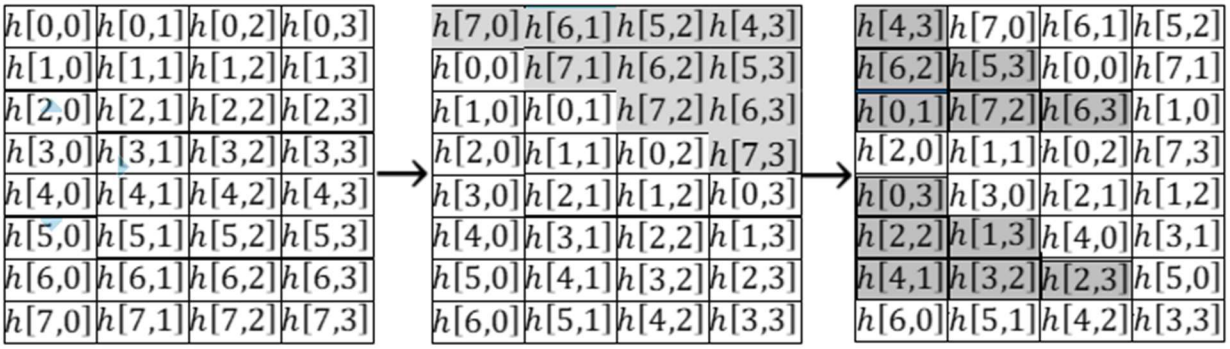
ko‘rinishda ifodalash mumkin. h'_0natijaviy qiymatning eng kichik bitini ifodalovchi tenglamada kirish bitlarining oxirgi bitlari qatnashishi ushbu kirish biti yuqoridagi yig‘indida toq yoki juft marta qatnashishiga bog‘liq. Ya’ni, chiqish bitini ifodalovchi tenglamada (2.4) yig‘indida toq marta qatnashgan kirish qiymatlarning oxirgi bitlari qatnashadi. Mazkur hol uchun $y_1 + x_2 + x_4 + x_6 = 0$ o‘rinli. Ushbu tenglamada x_8 – bit qatnashmaydi, chunki yuqoridagi (2.2) yig‘indida h_{15} qiymat 2 marta qatnashgan.

Katta razryad uchun tuzilgan tenglamalar uchun esa quyidagi qonuniyat o‘rinli: (2.4) yig‘indida toq marta qatnashgan qiymatlarning mos bitlari, (2.4) yig‘indida bir martadan ortiq qatnashgan qiymatlarning oxirgi bitlari va toq marta qatnashgan qiymatlarning oxirgi bitlari o‘zaro kombinatsiyalari (ko‘paytmalari) yig‘indisi natijaviy tenglamani hosil qiladi. Mazkur hol uchun: $y_1 + x_1 + x_2 * x_4 + x_2 * x_6 + x_3 + x_4 * x_6 + x_4 + x_5 + x_6 + x_8 = 0$ o‘rinli.

Ushbu qonuniyat har bir razryadni qo‘shish o‘zidan oldingi kichik razryadlarni qo‘shish natijasiga bog‘liq bo‘lgan sonlarni qo‘shish qoidasiga asoslangan.

Bu qonuniyat 12×3, 14×2, 16×4, 21×3 variantlar uchun ham o‘rinli ekanligi tajribalar yordamida aniqlandi. Shundan kelib chiqib, xulosa qilish mumkinki, ushbu qonuniyat 32×8 va 56×8 variantlar uchun ham o‘rinlidir.

$\boldsymbol{y = S(x)}$ funksiya umumiy uzunligi 256 bit bo‘lgan, har bir elementi baytlardan tashkil topgan (8,4) o‘lchamli matritsa elementlarini ustun bo‘yicha pastga va satr bo‘yicha o‘ngga surishni amalga oshiradi (2.6-rasm).

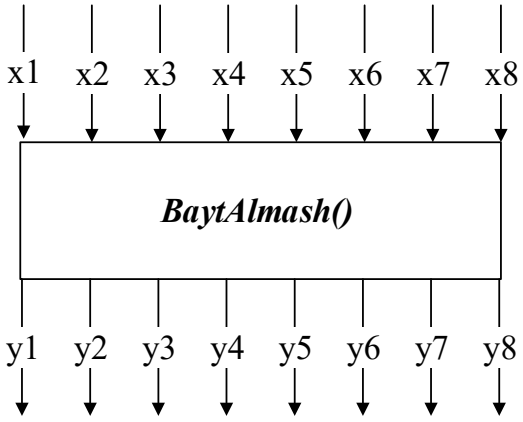


2.6-rasm. $S(x)$ **funksiya sxemasi**

Demak, ushbu akslantirish uchun quyidagi tenglamalar sistemasini qurish mumkin:

$$\begin{cases} y_1 = x_{153} \\ y_2 = x_{154} \\ y_3 = x_{155} \\ \dots\ \dots\ \dots \\ y_{129} = x_{25} \\ y_{130} = x_{26} \\ y_{131} = x_{27} \\ \dots\ \dots\ \dots \\ y_{256} = x_{128} \end{cases}$$

$\boldsymbol{y = B(x)}$ funksiya o‘lchami 8×8 bit bo‘lgan $BaytAlmash()$ akslantirishini amalga oshiradi ($BaytAlmash()$ jadvali o‘zgaruvchan bo‘lib, maxfiy kalit yordamida hisoblanadi) (2.7-rasm).



2.7-rasm.$BaytAlmash()$ **funksiya sxemasi**

Ushbu akslantirishga nisbatan to‘g‘ri (shifrlash) yo‘nalishda, teskari (rasshifrovkalash) yo‘nalishda va aralash (darajasi pasaytirilgan) algebraik tenglamalarni qurish mumkin, ya’ni:

1. $y_i = F(x_1, x_2, \dots, x_8)$, $i = 1,2, \dots,8$

2. $x_i = F(y_1, y_2, \dots, y_8)$, $i = 1,2, \dots ,8$

3. $F(x_1, x_2, \dots, x_8, y_1, y_2, \dots, y_8) = 0$

Birinchi ko‘rinishdagi to‘g‘ri (shifrlash) yo‘nalishda tuzilgan tenglamalar sistemasi akslantirishdan chiquvchi bitlarni akslantirishga kiruvchi bitlar orqali ifodalovchi tenglamalardan iborat bo‘ladi. Ikkinchi ko‘rinishdagi teskari (rasshifrovkalash) yo‘nalishda tuzilgan tenglamalar sistemasi akslantirishga kiruvchi bitlarni akslantirishdan chiquvchi bitlar orqali ifodalovchi tenglamalardan iborat bo‘ladi. Agar $BaytAlmash()$ jadvali regulyarlik shartini qanoatlantirsa birinchi va ikkinchi ko‘rinishdagi tenglamalar sistemasining maksimal darajasi $deg = 7$ ga teng bo‘ladi.

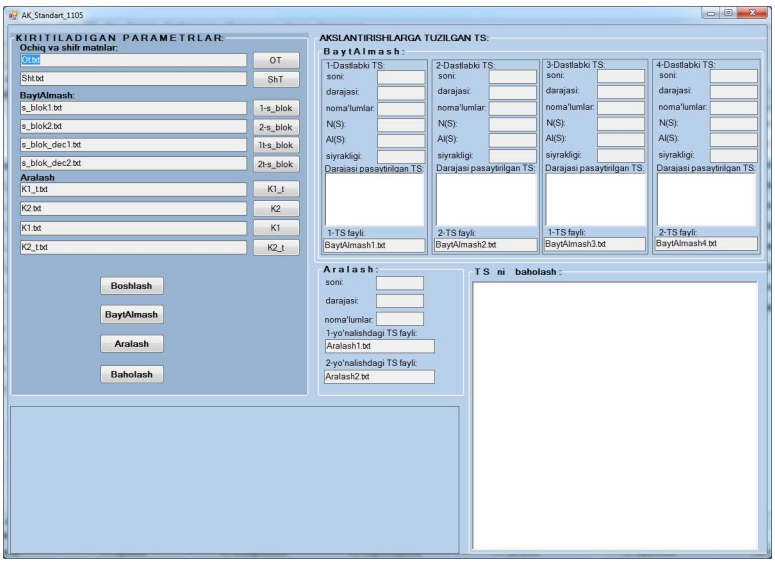
Mazkur akslantirishlardan $Aralash()$ va $BaytAlmash()$ akslantirishlari algoritmni ifodalovchi algebraik tenglamalar sistemasi parametrlariga ta’sir etadi. $Qo'shBosqichKalit()$ hamda $Sur()$ akslantirishlari esa chiziqli akslantirish bo‘lganligi sababli tenglamalar darajasi va noma’lumlar soniga ta’sir qilmaydi, lekin shifrlash jarayonida kalit bitlarini qo‘shish, bitlarni aralashtirish nuqtayi nazaridan ushbu akslantirishlar muhim hisoblanadi.

Shu bois, $Aralash()$ va $BaytAlmash()$ akslantirishlari uchun shakllantirilgan tenglamalar sistemasi algebraik xususiyatlari eksperimentlar o‘tkazish orqali tadqiq etildi. Eksperimentlar o‘tkazish uchun maxsus O‘z DSt 1105:2009 algoritmi akslantirishlarini algebraik tenglamalar sistemasi ko‘rinishida ifodalash dasturiy ta’minoti ishlab chiqildi. Dasturiy ta’minot oynasining umumiy ko‘rinishi 2.8-rasmda keltirilgan.

Ushbu dasturiy ta’minot quyidagi qismlardan iborat:

1. Kiritiladigan parametrlar.
2. Akslantirishlarga nisbatan tenglamalar sistemasi.
3. Tenglamalar sistemasini baholash (yechish qiyinchiligini baholash).

Dasturiy ta’minot, faylda ko‘rsatilgan almashtirish jadvallari va diamatritsalar qiymatlariga nisbatan $BaytAlmash()$ va $Aralash()$ akslantirishlari uchun tenglamalarni shakllantirish va faylga yozish funksional imkoniyatlariga ega.



2.8-rasm. **O‘z DSt 1105:2009 algoritmi akslantirishlarini algebraik tenglamalar sistemasi ko‘rinishida ifodalash dasturiy ta’minoti ishchi oynasi**

’minot quyidagi qismlardan iborat:

4. Kiritiladigan parametrlar.
5. Akslantirishlarga nisbatan tenglamalar sistemasi.
6. Tenglamalar sistemasini baholash (yechish qiyinchiligini baholash).

Dasturiy ta’minot, faylda ko‘rsatilgan almashtirish jadvallari va diamatritsalar qiymatlariga nisbatan $BaytAlmash()$ va $Aralash()$ akslantirishlari uchun tenglamalarni shakllantirish va faylga yozish funksional imkoniyatlariga ega.

M

’O‘z DSt 1105:2009 standart shifrlash algoritmida keltirilgan qoida

– shakllantirilgan almashtirish jadvallari uchun tuzilgan tenglamalar sistemasidagi 3 – darajali tenglamalar soni 441 tani tashkil qiladi. AES

uchun tuzilgan tenglamalar sistemasidagi 3 – darajali tenglamalar soni 471 tani, 2 – darajali tenglamalar soni esa 39 tani tashkil qiladi [91].

№			
			441
	94	3	441
	94	3	441
	70	3	441

v
o
‘O‘z DSt 1105:2009 standart shifrlash algoritmida keltirilgan qoida
)
o Diamatritsalar uchun shakllantirilgan tenglamalar sistemalari
parametrlaridan kelib chiqib, quyidagilarni xulosa qilish mumkin:
o – $Aralash()$ akslantirishi uchun shakllantirilgan tenglamalarning
darajalari hamda noma’lumlar soni akslantirishda foydalanilgan
diamatritsa elementlari qiymatiga bog‘liq ravishda o‘zgaradi;
o – standartda namuna sifatida keltirilgan kalitdan generatsiya
qilingan diamatritsadan foydalanilganda tenglamalarning darajalari tekis
taqsimlanadi.
‘ -
o
‘

№	Tenglamalar darajasi (ta)								Birhadlar soni
	Deg=	Deg=	Deg=	Deg=	Deg=	Deg=	Deg=	Deg=	
1.	4	4	4	4	4	4	4	4	14993
2.	4	6	2	6	2	4	4	4	13395
3.	4	4	4	4	4	4	4	4	14993
4.	4	6	2	5	3	4	4	4	17674
5.	4	4	4	4	4	4	4	4	4784
6.	4	8	0	7	1	7	1	4	7036
7.	4	4	4	4	4	4	4	4	14993
8.	4	7	1	7	2	6	1	4	17742
9.	4	4	9	3	3	3	3	3	3674
10.	4	5	3	4	4	4	4	4	15240

2
7
6
3
O
b
a
y

Mazkur jadvalda keltirilgan ma’lumotlar O‘z DSt 1105:2009 standart shifrlash algoritmi va uning akslantirishlarini algebraik kriptotahlil usuliga baholash uchun asos bo‘lib xizmat qiladi.

Olib borilgan tahlil natijalaridan quyidagi natija va xulosalar olindi:

1. O‘z DSt 1105:2009 standart shifrlash algoritmida foydalanilgan diamatritsaviy ko‘paytirish amali shakllantiriladigan tenglamalar sistemasining darajasi va undagi noma’lumlar sonining oshishini ta’minlaydi.

2.4-jadval

O‘z DSt 1105:2009 standart shifrlash algoritmi akslantirishlari

	Akslantirishlar tartibi	**1 raund**			**I**	**II**	**2 raund**			**I**	**II**
		TS	Deg	NS			TS	Deg	NS		
1.	XASB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
2.	XABS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
3.	XBSA	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
4.	XBAS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
5.	XSBA	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
6.	XSAB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
7.	AXSB	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
8.	AXBS	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
9.	ABSX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
10.	ABXS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
11.	ASBX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
12.	ASXB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
13.	SAXB	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
14.	SABX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
15.	SBXA	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
16.	SBAX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
17.	SXBA	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
18.	SXAB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
19.	BASX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
20.	BAXS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
21.	BXSA	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
22.	BXAS	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
23.	BSXA	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
24.	BSAX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}

– tenglamalar soni, Deg – darajasi, NS – noma’lumlar soni, I – TS ni ($\approx O(NS)^3$), II – TS ni saqlash uchun zarur xotira hajmi (bayt)

2. O‘z DSt 1105:2009 standart shifrlash algoritmida foydalanilgan $BaytAlmash()$ akslantirishi shakllantiriladigan tenglamalar sistemasining darajasi va undagi noma’lumlar sonining oshishini ta’minlaydi.

3. O‘z DSt 1105:2009 standart shifrlash algoritmida foydalanilgan $Aralash()$ hamda $BaytAlmash()$ akslantirishlaridan birgalikda

foydalanish algoritmning algebraik kriptotahlil usuliga bardoshligini oshiradi.

4. Raund kalitlaridan takroran foydalanish (masalan, O‘z DSt 1105:2009 standart shifrlash algoritmida ikkinchi raunddan boshlab har bir raund kaliti oldingi raund kalitidan 83 bitga farq qiladi) shifrlash algoritmining algebraik kriptotahlil usuliga bardoshligini kamaytiradi.

5. Raundlar sonining yuqori bo‘lishi O‘z DSt 1105:2009 standart shifrlash algoritmining algebraik kriptotahlil usuliga bardoshligini oshiradi.

6. SP tarmog‘iga asoslangan shifrlash algoritmlarida *S* jadval o‘lchamining yuqori bo‘lishi, agar *S* jadvali to‘g‘ri tanlansa, shifrlash algoritmining algebraik kriptotahlil usuliga bardoshligini oshiradi.

7. SP tarmog‘iga asoslangan shifrlash algoritmlarida raund kalitlari uzunligi o‘lchamining yuqori bo‘lishi, agar ular bir-biriga chiziqli bog‘liqsiz bo‘lsa, algoritmning algebraik kriptotahlilga bardoshligini oshiradi.

8. O‘z DSt 1105:2009 standart shifrlash algoritmida foydalanilgan *Aralash()* hamda *BaytAlmash()* akslantirishlaridan foydalaniladigan diamatritsa va almashtirish jadvallarining kalitga bog‘liq generatsiya qilinishi algoritmning algebraik kriptotahlil usuliga nisbatan turg‘un bardoshligini ta’minlamaydi.

9. Turli raundli O‘z DSt 1105:2009 standart shifrlash algoritmiga algebraik kriptotahlil usulini qo‘llashdan olingan tenglamalar sistemasini Mutant XL usuli orqali yechish imkoniyati nazariy mavjud [26].

10. O‘z DSt 1105:2009 standart shifrlash algoritmi ikkinchi raunddan boshlab shakllantiriladigan tenglamalar sistemasini saqlash uchun talab qilinadigan xotira hajmini ta’minlash imkoniyati mavjud emasligi sababli algebraik kriptotahlil usuliga bardoshli.

2.3-§. O‘z DSt 1105:2009 shifrlash algoritmining integral kriptotahlili

Tahlil natijalari shuni ko‘rsatadiki, integral kriptotahlil usulining samaradorligi shifrlash algoritmi strukturasi va unda foydalanilgan akslantirishlarning kriptografik xususiyatlariga uzviy bog‘liq sanaladi.

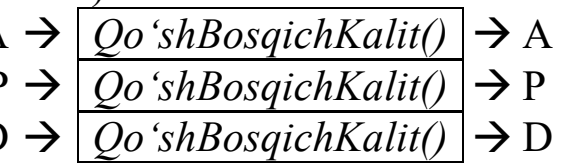
Ushbu xususiyatlar qatoriga akslantirishlarning *tarqatish* (sochish), *bir qiymatli akslantirish, aralashtirish* xususiyatlarini keltirish mumkin.

Ushbu bo‘limda, kiruvchi blok uzunligi 256 bit bo‘lgan O‘z DSt 1105:2009 shifrlash algoritmiga integral kriptotahlili bilan tanishib chiqiladi.

Demak, *n* raundli O‘z DSt 1105:2009 shifrlash algoritmiga integral kriptotahlil usulini qo‘llab m-raund kalitini aniqlashda, eng avvalo, tahlil qilinayotgan *m-raundga kirishda balanslashgan* va *m-raunddan chiqishda balanslashmagan* to‘plam hosil bo‘lishini ta’minlab beruvchi ochiq matnlar to‘plamini tanlash masalasi hal etilishi lozim [25].

O‘z DSt 1105:2009 shifrlash algoritmiga nisbatan ushbu masalani yechishda, dastlab algoritmning har bir akslantirishi xususiyatlarini ko‘rib chiqish maqsadga muvofiq. Shunga ko‘ra quyida, O‘z DSt 1105:2009 akslantirishlarining turli xil kiruvchi to‘plam elementlarini qanday o‘zgartirishi keltirib o‘tiladi.

O‘z DSt 1105:2009 algoritmining dastlabki akslantirishi $Qo'shBosqichKalit()$bo‘lib, raund kalitlari massivini holat massiviga modul 2 bo‘yicha qo‘shishni amalga oshiradi. Shunga ko‘ra, to‘plam elementining har bir holati uchun ushbu akslantirish ta’sirini quyidagicha ko‘rish mumkin (2.9-rasm).



2.9-rasm.$Qo'shBosqichKalit()$ **akslantirishining kiruvchi to‘plamlarga ta’siri**

Bu yerda: A – aktiv (A_i– agar tashkil etuvchilari turli tartibda joylashgan bo‘lsa) yoki P – passiv yoki D – aralash (D_0– balanslashgan bo‘lsa, D_1– balanslashmagan bo‘lsa).

O‘z DSt 1105:2009 algoritmining keyingi akslantirishi $Aralash()$ bo‘lib, holat massivining diamatritsaga diamatritsaviy ko‘paytirish asosidagi akslantirishni amalga oshiradi [21]. Ushbu akslantirishni ham, kriptotahlil jarayonida kuzatilayotgan turli xildagi to‘plamga nisbatan holat massiviga ta’sirini quyidagicha ko‘rish mumkin (2.10-rasm).

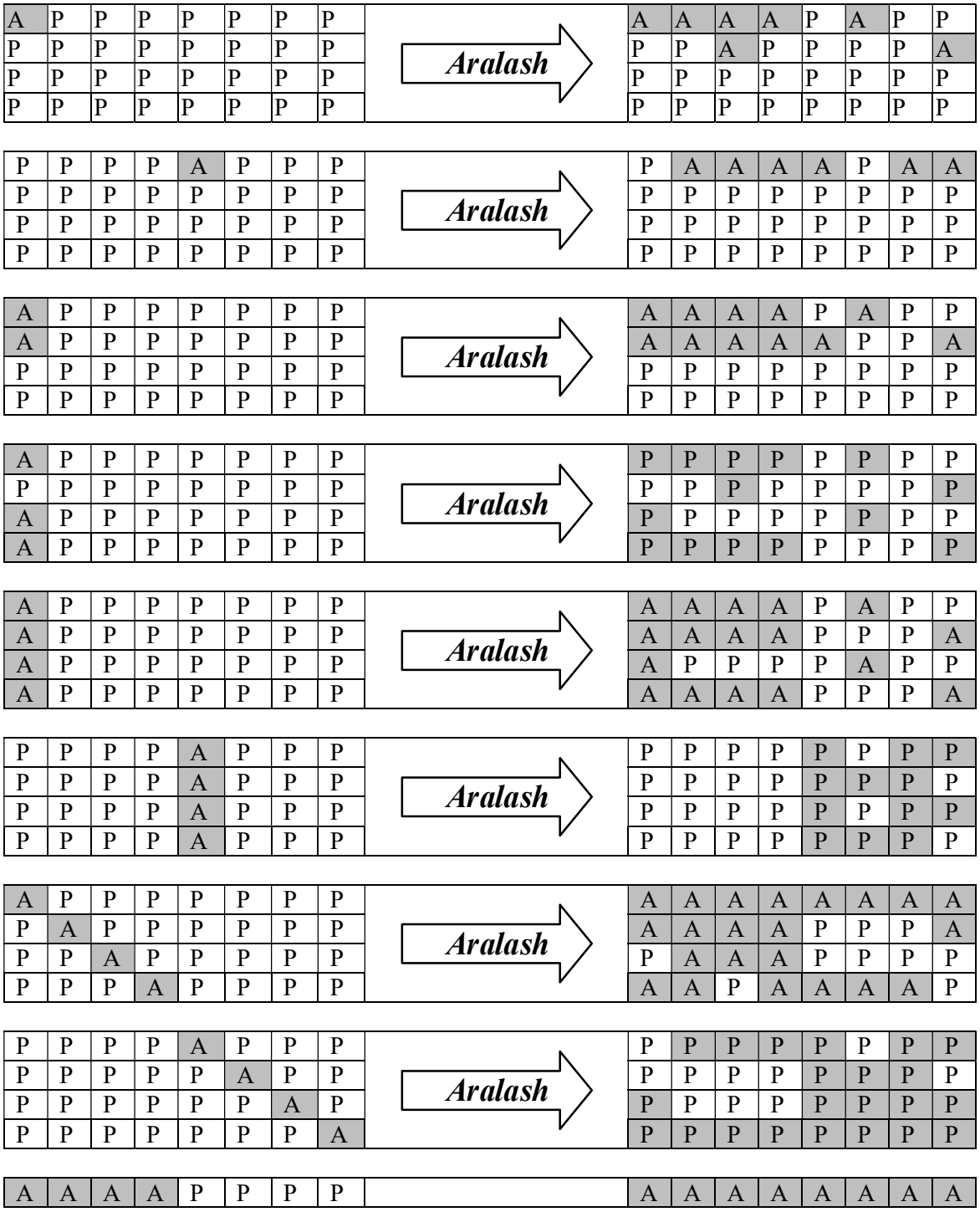
Demak, $Aralash()$ akslantirishining ushbu o‘zgartirishlariga ko‘ra quyidagi xulosalar o‘rinli:

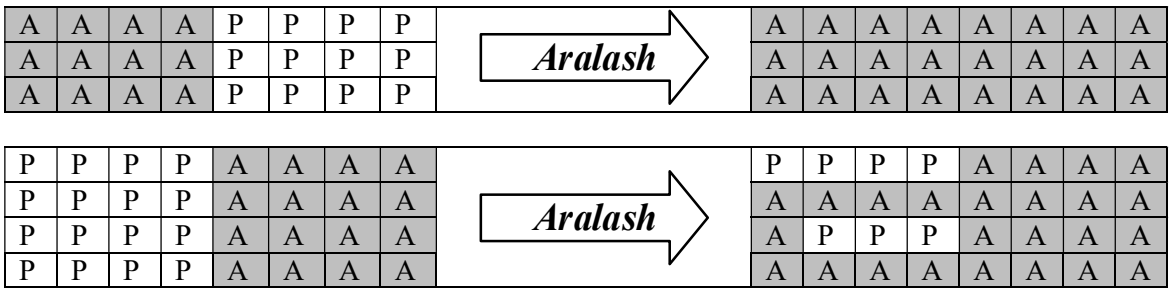
– agar kiruvchi holat massivining birinchi yoki o‘n yettinchi baytlari aktiv bo‘lib qolgan baytlari passiv bo‘lsa, ushbu akslantirish

chiqishida yettita bayti aktiv bo‘ladi, faqat bitta bayt bo‘lgan hollarning barchasida chiquvchi massivning oltita baytlari aktiv bo‘ladi;

– agar kiruvchi holat massivining alohida diamatritsalarga ko‘paytiriladigan 4×4 massivning 1,2,3,4,9,10,11,12 baytlari aktiv bo‘lsa, chiquvchi massivning barcha baytlari aktiv bo‘ladi;

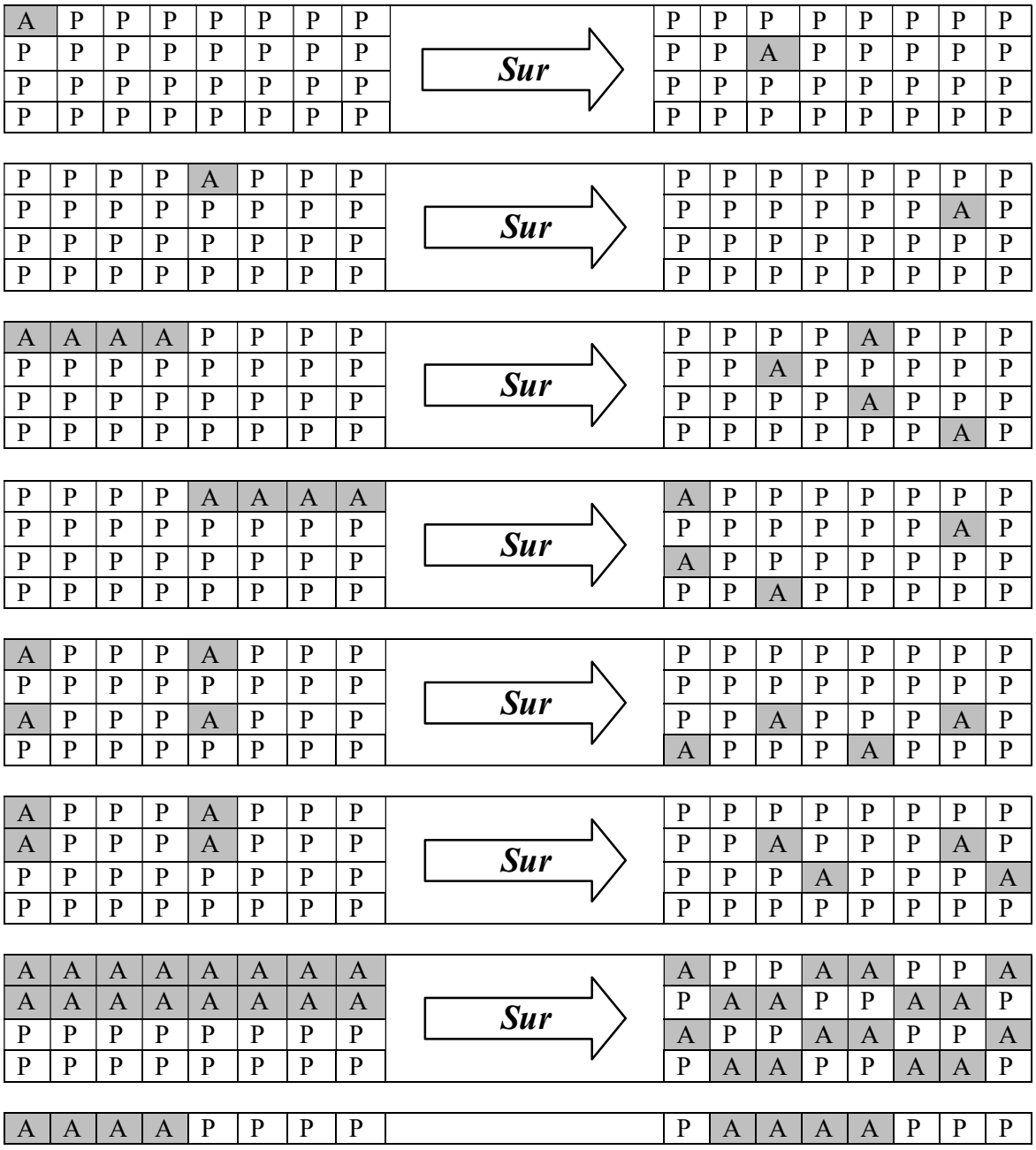
– agar kiruvchi holat massivining alohida diamatritsalarga ko‘paytiriladigan 4×4 massivning 5,6,7,8,13,14,15,16 baytlari aktiv bo‘lsa, chiquvchi massivning barcha baytlari aktiv bo‘lmaydi (1,2,3,4,18,19,20 baytlar passiv baytlar).

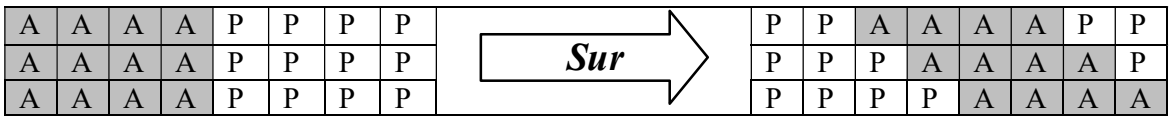




2.10-rasm. $Aralash()$ *akslantirishining kiruvchi to‘plamlarga ta’siri*

O‘z DSt 1105:2009 algoritmining keyingi raund akslantirishi $Sur()$ bo‘lib, holat massivi satrlarining turli siklik surilishini amalga oshiradi. Ushbu akslantirishni ham, kriptotahlil jarayonida kuzatilayotgan turli xildagi to‘plamga nisbatan holat massiviga ta’sirini quyidagicha ko‘rish mumkin (2.11-rasm).





2.11-rasm. $Sur()$ *akslantirishining kiruvchi to‘plamlarga ta’siri*

Demak, ushbu o‘zgarishlarga ko‘ra aytish mumkinki, $Sur()$ akslantirishiga kiruvchi to‘plamda ishtirok etishi mumkin bo‘lgan aktiv, passiv yoki aralash elementlar, akslantirish natijasida o‘z xususiyatini o‘zgartirmaydi, joylashgan o‘rni esa o‘zgaradi.

Demak, ushbu o‘zgarishlarga ko‘ra aytish mumkinki, agarda $BaytAlmash()$ akslantirishiga kiruvchi to‘plam aktiv va passiv yoki faqat aktiv yoki faqat passiv elementlardan tashkil topgan bo‘lsa, bu akslantirish aktiv va passiv elementlar soniga, joylashgan o‘rniga, balanslashganlik xususiyatiga ta’sir qilmaydi. Agarda $BaytAlmash()$ akslantirishiga kiruvchi to‘plam aralash elementlardan tashkil topgan bo‘lsa, akslantirish aralash elementlar soniga, joylashgan o‘rniga ta’sir qilmasdan, balanslashganlik xususiyatini o‘zgarishiga olib keladi.

O‘z DSt 1105:2009 algoritmining so‘nggi akslantirishi $BaytAlmash()$ bo‘lib, holat massivi elementlarini (bayt) bir-biriga bog‘liqsiz tarzda akslantirishni amalga oshiradi. Kriptotahlil jarayonida kuzatilayotgan to‘plamga nisbatan holat massivining har bir elementi yoki A – aktiv (A_i– agar tashkil etuvchilari turli tartibda joylashgan bo‘lsa) yoki ***P*** – passiv yoki ***D*** – aralash (D_0– balanslashgan bo‘lsa, D_1– – balanslashmagan bo‘lsa) element bo‘ladi. Shunga ko‘ra, to‘plam elementining har bir holati uchun $SubBytes()$ akslantirishi ta’sirini quyidagicha ko‘rish mumkin (2.12-rasm).

Agar aralash element balanslashgan bo‘lsa, u holda uning tarkibida har doim juft miqdorda toq va juft sonlar ishtirok etadi. Ushbu akslantirish natijasida balanslashgan aralash elementning balanslashmagan aralash elementga akslanishi sababi, juft sondagi juft va toq sonlarning toq sondagi juft va toq sonlarga akslanishidir.

A	→	***BaytAlmash***	→	A
P	→	***BaytAlmash***	→	P
D_0	→	***BaytAlmash***	→	D_0
D_1	→	***BaytAlmash***	→	D_1

2.12-rasm. $BaytAlmash()$ **akslantirishining kiruvchi to‘plamlarga ta’siri**

Demak, yuqoridagilarga ko‘ra aytish mumkinki, kriptotahlil jarayonida kuzatilayotgan to‘plam elementlari qanday xususiyatga ega bo‘lishidan qat’iy nazar, $Qo`shBosqichKalit()$ akslantirishi ularning xususiyatini o‘zgartirmaydi. Shifrlash algoritmlarining integral kriptotahlilga bo‘lgan asosiy kamchiligi ham aynan kalit qo‘shish akslantirishlarining ushbu xususiyati hisoblanadi.

O‘z DSt 1105:2009 algoritmi akslantirishlarining yuqorida ko‘rib o‘tilgan xususiyatlariga ko‘ra ma’lum bo‘ldiki, *m*-raundga kiruvchi to‘plamning balanslashgan va *m*-raunddan chiquvchi to‘plamning balanslashmagan bo‘lishi uchun, *m*-raundga kiruvchi to‘plam elementlari *aralash* (balanslashgan) element bo‘lishi talab etiladi. Algoritm akslantirishlarining mazkur xususiyatlari natijasiga ko‘ra, ushbu algoritmning ayrim raundlariga nisbatan quyidagi xulosalarni keltirish mumkin:

1. Bir-biridan kamida bitta bayti bilan farqlanuvchi ixtiyoriy ikkita ochiq matnlarni 2 raundli O‘z DSt 1105:2009 algoritmi orqali shifrlash natijasida, barcha baytlarga ta’sir qilishi kuzatiladi.
2. Barcha elementlari bir xil tartibga ega aktiv bayt bo‘lgan holat massivini 2 raundli O‘z DSt 1105:2009 algoritmi orqali shifrlash natijasida, barcha elementlari balanslashmagan aralash bayt bo‘lgan massiv hosil bo‘ladi (2.13-rasm).

A	A	A	A	A	A	A	A	2-raund	D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
A	A	A	A	A	A	A	A		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
A	A	A	A	A	A	A	A		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
A	A	A	A	A	A	A	A		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

2.13-rasm. **Kiruvchi to‘plamlarning 2-raunddan keyingi holati**

3. Dastlabki elementi aktiv, qolgan elementni passiv bayt bo‘lgan holat massivini 3 raundli O‘z DSt 1105:2009 algoritmi orqali shifrlash natijasida, barcha elementlari balanslashmagan aralash bayt bo‘lgan massiv hosil bo‘ladi (2.14-rasm).

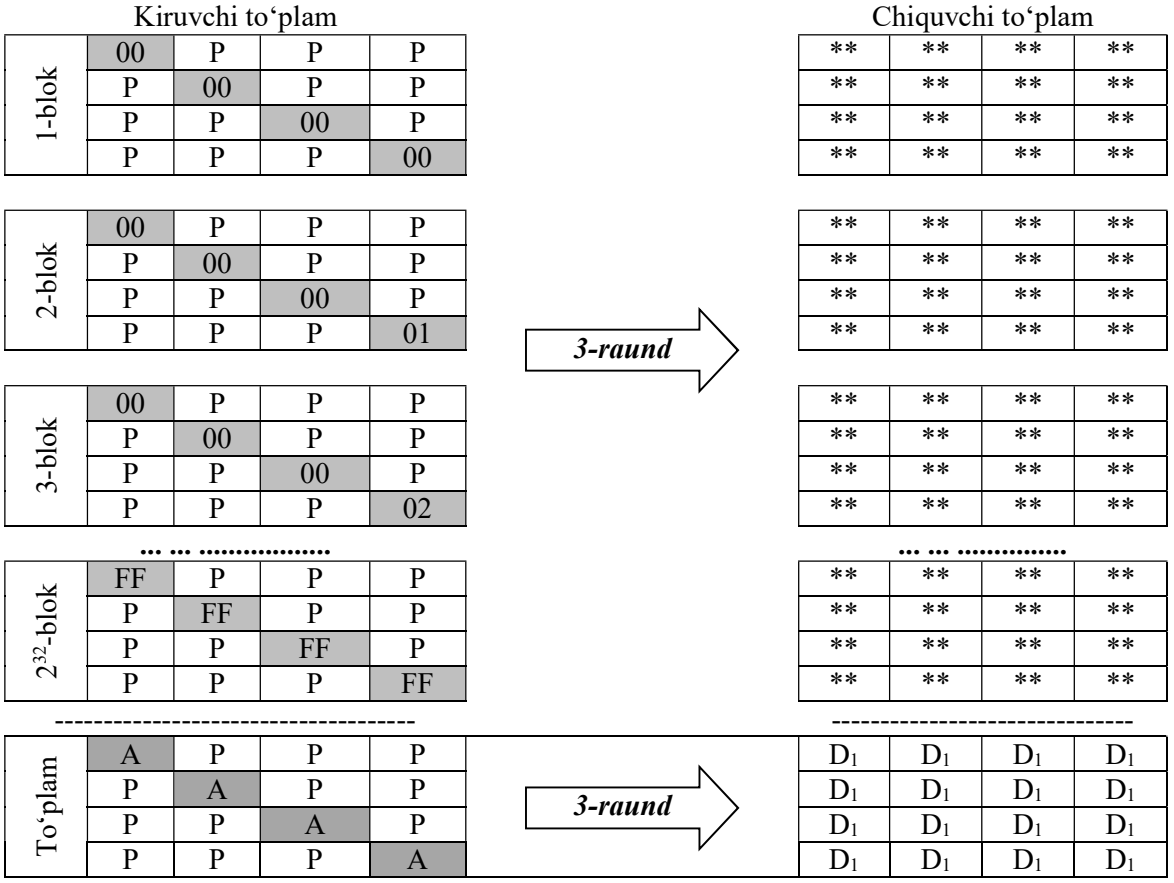
A	P	P	P	P	P	P	P	3-raund	D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
P	P	P	P	P	P	P	P		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
P	P	P	P	P	P	P	P		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
P	P	P	P	P	P	P	P		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

2.14-rasm. **Kiruvchi to‘plamlarning 3-raunddan keyingi holati**

4. Bir-biridan 4×4 holat massivlarining bosh diagonal baytlari bilan farq qiluvchi va ushbu baytlari turli xil aktiv bayt bo‘lgan 2^{32} ta

matnlar to‘plamini uch raundli O‘z DSt 1105:2009 algoritmi orqali shifrlash natijasida, barcha elementlari balanslashmagan massiv hosil bo‘ladi (2.15-rasm).

Ushbu keltirib o‘tilgan xulosalar O‘z DSt 1105:2009 algoritmiga integral kriptotahlil usuli qo‘llanishida ochiq matnlar to‘plamini tanlash masalasini yechish uchun xizmat qiladi.



2.15-rasm. **Kiruvchi to‘plamlarning 3-raunddan keyingi holati**

Olib borilgan tadqiqot natijasi shuni ko‘rsatadiki, integral kriptotahlil usuli bilan O‘z DSt 1105:2009 algoritmining so‘nggi raund kalitini topish quyidagi qadamlar asosida amalga oshiriladi:

I. Tegishli qoida asosida m ta $P_i(1 \le i \le m)$ matndan iborat bo‘lgan to‘plam tanlab olinsin (bu yerda, m – shifrlash algoritmi raundlar soniga bog‘liq holda aniqlanuvchi natural son).

II. Maxfiy kalit yordamida ushbu ochiq matnlarning T_i – shifr matnlari hosil qilinsin.

III. So‘nggi raund kalitining har bir $K_q(1 \le q \le 32)$ bo‘laklari qabul qilishi mumkin bo‘lgan barcha (0 dan 255 gacha) qiymatlari uchun quyidagilar bajarilsin:

1. $Rejim = dsh$ uchun barcha T_i shifr matnlar uchun qism elementlari uchun $R_{iq} = Aralash(Sur(BaytAlmash(T_i)))$ qiymat hisoblansin.

2. Barcha R_{iq} qiymatlar XOR yig‘indisi hisoblansin, ya’ni:

$$XOR\_SUM = R_{1q} \oplus R_{2q} \oplus R_{3q} \oplus ... \oplus R_{mq}$$

3. Agar XOR_SUM=0 bo‘lsa, K_q to‘g‘ri kalitlar ro‘yxatiga kiritilsin.

4. Agar to‘g‘ri topilgan kalitlarning biror K_q bo‘lagi bir nechta variantga ega bo‘lsa I qadamga qaytilsin.

Quyida, ushbu ishlab chiqilgan kalit topishning 1-usul algoritmi hamda yuqorida keltirilgan xulosalar asosida 4 raundli O‘z DSt 1105:2009 algoritmiga integral kriptotahlil usulini qo‘llash uchun qanday ochiq matnlarni tanlash kerakligi keltirib o‘tiladi.

To‘rt raundli O‘z DSt 1105:2009 algoritmi uchun ochiq matnlar to‘plamini tanlash. To‘rt raundli O‘z DSt 1105:2009 algoritmiga integral kriptotahlil usulini qo‘llab so‘nggi raund kalitini topish uchun, holat massivining bir elementi aktiv bo‘ladigan to‘plamni tanlash kerak bo‘ladi. Mazkur holda ochiq matnlar soni 2^8 ta bo‘lib, 2.16-rasmda ushbu to‘plamni 4 raundli O‘z DSt 1105:2009 algoritmi orqali shifrlash jarayonida massiv elementlarining o‘zgarish sxemasi keltirilgan.

To‘rt raundli shifrlash algoritmi uchun tanlab olingan ochiq matnlarga mos shifr matnlar to‘plami T_i mavjud bo‘lgan holda ularni to‘rtinchi raundagi akslantirishlardan quyidagicha deshifrlanadi:

$$C_i = Qo'shBosqichKalit(Aralash\left(Sur\left(BaytAlmash(T_i)\right)\right), K^4)$$

C_i to‘plam to‘rtinchi raund kirishidagi to‘plamni ifodalaydi. K^4 kalitning K_q^4 $(1 \le q \le 32)$ bo‘laklari qabul qilishi mumkin bo‘lgan barcha (0 dan 255 gacha) mumkin bo‘lgan qiymatlari uchun C_i to‘plamni uchinchi raunddagi akslantirishlardan o‘tkaziladi:

$$R_{iq} = Aralash\left(Sur\left(BaytAlmash(C_i)\right)\right)$$

So‘ngra R_{iq} qiymatlar *XOR* yig‘indisi hisoblanadi:

$$XOR\_SUM=R_{1q} \oplus R_{2q} \oplus R_{3q} \oplus ... \oplus R_{mq}$$

XOR_SUM=0 bo‘lgan qiymatlariga mos K_q^4 $(1 \le q \le 32)$ nomzod kalitlar ro‘yxatiga qo‘shiladi.

O‘z DSt 1105:2009 algoritmiga integral kriptotahlil usulini qo‘llash natijalariga ko‘ra quyidagi xulosaga kelindi:

4 raundli O‘z DSt 1105:2009 shifrlash algoritmiga integral kriptotahlil usulini qo‘llab, tanlab olingan 2^8 ta ochiq matnlar asosida

2-raund so‘ngidagi $BaytAlmash()$ akslantirishining xossalariga muvofiq chiqishdagi kalitning K_2^4, K_3^4, K_4^4, K_6^4, K_7^4, K_8^4, K_9^4, K_{10}^4, K_{11}^4, K_{12}^4, K_{13}^4, K_{16}^4, K_{17}^4, K_{18}^4, K_{19}^4, K_{22}^4, K_{23}^4, K_{24}^4, K_{25}^4, K_{26}^4, K_{28}^4, K_{29}^4, K_{32}^4 - baytlarini (jami 184 bit) topish mumkin.

1-raund:

Qo`shBosqichKalit()

A	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P

Aralash()

A	A	A	A	P	A	P	P
P	P	A	P	P	P	P	A
P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P

Sur()

P	P	P	A	A	P	P	P
P	A	A	P	P	P	P	P
A	P	P	P	A	P	P	P
P	P	P	P	P	P	A	P

BaytAlmash()

P	P	P	A	A	P	P	P
P	A	A	P	P	P	P	P
A	P	P	P	A	P	P	P
P	P	P	P	P	P	A	P

2-raund:

Qo`shBosqichKalit()

P	P	P	A	A	P	P	P
P	A	A	P	P	P	P	P
A	P	P	P	A	P	P	P
P	P	P	P	P	P	A	P

Aralash()

A_1	D_0	D_0	D_0	D_0	D_0	D_0	D_0
D_0	A_1	D_0	A_1	A_1	A_1	A_1	A_1
A_1	A_1	A_1	A_1	A_1	A_1	A_1	A_1
A_1	A_1	A_1	A_1	A_1	A_1	A_1	A_1

Sur()

D_0	A_1	A_1	A_1	D_0	A_1	A_1	A_1
A_1	A_1	A_1	A_1	A_1	D_0	D_0	A_1
A_1	A_1	A_1	D_0	D_0	A_1	A_1	A_1
A_1	A_1	D_0	A_1	A_1	D_0	D_0	A_1

BaytAlmash()

D_1	D_0	D_0	D_0	D_1	D_0	D_0	D_0
D_0	D_0	D_0	D_0	D_0	D_1	D_1	D_0
D_0	D_0	D_0	D_1	D_1	D_0	D_0	D_0
D_0	D_0	D_1	D_0	D_0	D_1	D_1	D_0

3-raund:

Qo`shBosqichKalit ()

D_1	D_0	D_0	D_0	D_1	D_0	D_0	D_0
D_0	D_0	D_0	D_0	D_0	D_1	D_1	D_0
D_0	D_0	D_0	D_1	D_1	D_0	D_0	D_0
D_0	D_0	D_1	D_0	D_0	D_1	D_1	D_0

Aralash()

D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

Sur()

D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

BaytAlmash()

D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

4-raund:

Qo`shBosqichKalit()

D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

Aralash()

D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

Sur()

D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

BaytAlmash()

D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

2.16-rasm. **4 raundli O‘zDSt 1105:2009 algoritmi orqali shifrlash jarayonida to‘plam elementlarining o‘zgarish sxemasi**

Bunda, $rejim = dsh$ bo‘lganda $Aralash()$ akslantirishida diamatritsaviy ko‘paytirishdan foydalanilganda $K_{10}^4, K_{19}^4, K_{23}^4, K_{28}^4, K_{32}^4$ baytlarning har birini hisoblash uchun to‘rt baytning mumkin bo‘lgan barcha $(2^8)^4 = 2^{32}$ ta, K_2^4, K_3^4, K_4^4, K_6^4, K_7^4, K_8^4, K_9^4,K_{11}^4, K_{12}^4, K_{13}^4, K_{16}^4, K_{17}^4, K_{18}^4, K_{22}^4, K_{24}^4, K_{25}^4, K_{26}^4, K_{28}^4, K_{29}^4 baytlarning har birini hisoblash uchun yetti baytning mumkin bo‘lgan barcha $(2^8)^7 = 2^{56}$ ta qiymatlarini ko‘rib chiqish orqali so‘nggi raund kalitining 184 bit qiymatini aniqlash mumkin bo‘ladi.

Demak, ikkinchi raund kalitining 184 bit qiymatini hisoblash uchun 2^8 ta ochiq matnlar asosida $18 * 2^{56} + 5 * 2^{32} \approx 2^{60}$ variantlarini ko‘rib chiqish lozim.

Kriptotahlil natijasi 2-raund $BaytAlmash()$ akslantirishidan keyingi shifrlash kalitini topishda 2^{72} ta amal bajarish zarurligini ko‘rsatdi.

III BOB. TAKOMILLASHTIRILGAN O‘Z DST 1105:2009 SHIFRLASH ALGORITMINI ISHLAB CHIQISH

3.1-§. O‘rin almashtirish va aralashtirish akslantirish usullari uchun parametrlarni statik tanlash

O‘zDSt 1105:2009 shifrlash algoritmida *BaytAlmash()* akslantirishi uchun S jadvallar, *Aralash()* akslantirishi uchun diamatritsalar kiritilgan shifrlash va funksional kalitlar orqali dinamik hosil qilinadi. Ushbu bobda ularni statik tarzda tanlash masalalari bilan shug‘ullaniladi.

BaytAlmash() akslantirishi uchun statik S jadvallarni hosil qilish. O‘z DSt 1105:2009 shifrlash algoritmining $BaytAlmash()$ akslantirishi kalit asosida hosil qilingan S jadvallar bo‘yicha kiruvchi baytni chiqishda boshqa baytga almashtirib beradi. $BaytAlmash()$ akslantirishida uzunligi 256 ga teng bir baytli elementlardan iborat ikkita S jadvallardan foydalaniladi. Ushbu jadvallar kalitga bog‘liq ravishda hosil qilingani bois, algoritmga nisbatan aniq kriptotahlil bahosini berib bo‘lmaydi [124]. Bundan tashqari, Kerkxoffs prinsipiga ko‘ra kalitdan boshqa barcha ma’lumotlar kriptotahlilchiga ma’lum bo‘lishi kerak. Shu sababli, mazkur bo‘limda statik S jadvalni hosil qilish ketma-ketligi ko‘rib o‘tiladi.

S jadvallarni hosil qilishda ko‘plab yondashuvlar mavjud bo‘lib, ularga tasodifiy tanlash, tasodifiy tanlash va tekshirish, maxsus ishlab chiqish va matematik ishlab chiqish yondashuvlarini keltirish mumkin [35]. Ular orasida matematik ishlab chiqishga asoslangan S jadvallardan amalda keng foydalaniladi. Ushbu yondashuvga ko‘ra S jadval biror matematik qoida asosida ishlab chiqiladi. Shu bois mazkur yondashuv asosida hosil qilingan S jadvallar turli kriptotahlil usullariga nisbatan ishonarli bardoshlikka ega bo‘ladi. Mazkur yondashuv asosida AES shifrlash algoritmining S jadvali hosil qilingan. AES algoritmida S jadval uchun amallar $GF(2^8)$ maydonida amalga oshiriladi. Bunda maydon $m(x) = x^8 + x^4 + x^3 + x + 1$ yoki $\{11B\}$ ga teng bo‘lib, S jadvalni generatsiyalash quyidagi tenglik orqali amalga oshiriladi [100]:

$$y = (Ax^{-1} \oplus c) mod\ m(x) \qquad (3.1)$$

Bu yerda, y – chiquvchi bayt, A – affin matritsasi, x^{-1} – kiruvchi baytning inversi, c – o‘zgarmas qo‘shiluvchi, mod – qoldiqli bo‘lish funksiyasi.

Generatsiya qilingan S jadvallar orasidan eng mosini tanlash kriptobardoshlik masalasi bilan uzviy bog‘liq. Ma’lumki, chiziqli

kriptotahlil usuliga bardoshlikni ta’minlash S jadvalning umumiy chiziqsizlik qiymatini (non-linearity, $N(S)$) maksimal bo‘lishiga, differensial kriptotahlil usuliga bardoshli bo‘lishi S jadvalida ayirma matritsa jadvalidagi maksimal qiymat (δ) kichik bo‘lishiga, algebraik kriptotahlil usuliga bardoshlikni ta’minlash esa yuqori algebraik immunitetga (algebraic immunity, $AI(S)$) ega S jadvaldan foydalanishga bog‘liq. Boshqa tomondan, bir S jadval uchun $N(S)$ va $AI(S)$ ko‘rsatkichlarning maksimal bo‘lishi kuzatilmaydi. O‘z DSt 1105:2009 shifrlash algoritmida raundlarning juft yoki toqligiga ko‘ra kalitlardan hosil bo‘lgan ikkita turli S jadvallardan foydalaniladi. Yuqorida keltirilgan fikrlarni inobatga olgan holda, $BaytAlmash()$ akslantirishidagi ikkita S jadval o‘rniga quyidagi parametrli jadvallardan foydalanish talabi qo‘yildi:

1. $N(S)$ ko‘rsatkichi maksimal va δ ko‘rsatkichi minimal bo‘lgan 8×8 o‘lchamli jadval (S_1);
2. $AI(S)$ ko‘rsatkichi maksimal bo‘lgan 8×8 o‘lchamli jadval (S_2).

Odatda aksariyat simmetrik blokli shifrlarda qo‘yilgan birinchi talabni qanoatlantiruvchi S jadvallardan foydalaniladi. Masalan, AES, Camellia, SQUARE va [21] manbada keltirilgan O‘z DSt 1105:2009 algoritmlari uchun $N(S) = 112$ va $\delta = 4$ ga teng. Shuningdek, ularning barchasi uchun $AI(S) = 2$ ga teng.

Ikkinchi talabni qanoatlantiruvchi S jadvallar ham mavjud bo‘lib, ularga STB 34.101.31-2011 ($N(S) = 102$, $\delta = 8$ va $AI(S) = 3$), GOST R 34.12-2015 ($N(S) = 100$, $\delta = 8$ va $AI(S) = 3$) va [35] manbasini ($N(S) = 104$, $\delta = 8$ va $AI(S) = 3$) misol keltirish mumkin.

Birinchi talabni qanoatlantiruvchi S jadvalni yaratishda AES standartida foydalanilgan yondashuvdan foydalanildi. (3.1) tenglikning AES shifrlash standartidagi S jadvalni hosil qilishdagi ko‘rinishi quyida keltirilgan. Bu yerda, $(x_7, x_6, \dots, x_0)$ – S jadvalda kiruvchi baytning multiplikativ teskarisi va $(y_7, y_6, \dots, y_0)$ – S jadvaldan chiquvchi bayt. O‘zgarmas qo‘shiluvchi, $c = 0x63$ ga teng bo‘lib, kichik bitidan kattasiga tartibda (big endian) yozilgan. Affin matritsasining 7,...,1 - satrlari esa o‘zidan oldingi satrni (8-satr $0x1F$ ga teng va uni n shaklida belgilaylik) baytni siklik chapga bir bit surishdan hosil qilinadi.

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Yuqorida keltirilgan tenglikni bir baytli barcha kiruvchi qiymatlar uchun hisoblash bilan S jadvalni hosil qilish mumkin.

Yuqori chiziqsizlik ko‘rsatkichiga ega va δ ko‘rsatkichi minimal bo‘lgan 8×8 o‘lchamli S jadvallarni generatsiya qilish uchun AES shifrlash standartida foydalanilgan usulga asoslanildi. Buning uchun maxsus dasturiy vosita ishlab chiqildi. 8×8 o‘lchamga ega bo‘lgan jami affin matritsalarining soni 255 taga ($n \in [1,255]$) teng. Ulardan 160 tasi uchun teskari matritsa mavjud (n ning tegishli qiymatlari 1-ilovaga keltirilgan). Shuningdek, 160 ta affin matritsa va $c = 0x63$ bilan hosil qilingan S jadvallar ichidan o‘zgarmas nuqtalari (S jadvalga kiruvchi va chiquvchi qiymatlari bir xil bo‘lgan) mavjudlari soni 106 tani tashkil etdi. Masalan, $n = 53$ va $n = 98$ holatlarda affin matritsadan hosil qilingan o‘zgarmas nuqtalarga ega bo‘lgan S jadvallar 2-ilovada keltirilgan. O‘zgarmas nuqtalarda S jadvallar uchun n qiymatlari 3-ilovada keltirilgan.

Qolgan 54 affin matritsa va $c = 0x63$ bilan hosil qilingan S jadvallarda bir xil chiqish qiymatiga ega bo‘lganlari soni 5 taga teng ($n \in \{71,101,106,166,184\}$). $n = 71$ va $n = 184$ ga teng holatlar uchun generatsiya qilingan S jadvallar 4-ilovada keltirilgan. n ning qolgan 49 ta quyida keltirilgan qiymatlari uchun AES standartida foydalanilgan S jadvallarga o‘xshash jadvallarni generatsiya qilish mumkin:

$n \in \{1, 11, 19, 26, 31, 44, 49, 50, 52, 55, 56, 61, 62, 64, 69, 70, 74, 84, 87, 94, 100, 103, 104, 107, 109, 117, 121, 134, 138, 145, 146, 148, 152, 155, 161, 171, 181, 185, 186, 196, 199, 205, 206, 211, 213, 223, 224, 244, 248\}$.

Olib borilgan tahlil natijalari yuqorida keltirilgan n ning tegishli qiymatlari uchun 3.1-jadvaldagi xususiyatlarga ega bo‘lgan S jadvallarni hosil qilish imkoniyatini bergani aniqlandi.

3.1-jadval

Generatsiya qilingan S jadvallarning baholash natijalari

Baholash omillari		Qiymati
Balanslashganlik		True
Regulyarlik		True
Chiziqsizlik, $N(S)$		112
Korrelyatsion immunitet,(CI)		0
Minimal daraja, deg		7
Ayirma matritsa jadvalidagi maksimal qiymat, δ		4
$D(S)$		133120
Qat'iy lavin samaradorlik, SAC		False
Algebraik immunitet	AI(S)	2
	TS(S)	39

O‘z DSt 1105:2009 shifrlash algoritmida ikkita S jadvallardan foydalanilganini inobatga olib, $n = 244$ holat uchun hosil qilingan quyidagi S jadvalni birinchi jadval - $S_1(8 \times 8)$ shaklida qabul qilamiz:

$S_1(8 \times 8) =$ {99, 151, 153, 207, 158, 248, 53, 159, 29, 55, 174, 36, 200, 78, 157, 234, 92, 27, 201, 228, 5, 71, 192, 120, 182, 219, 117, 80, 156, 94, 39, 33, 252, 93, 95, 1, 54, 222, 32, 119, 208, 45, 241, 11, 178, 141, 110, 205, 137, 121, 191, 180, 232, 225, 250, 183, 28, 149, 253, 169, 65, 114, 66, 127, 172, 104, 124, 14, 125, 70, 210, 147, 73, 19, 61, 49, 194, 218, 233, 48, 58, 101, 68, 106, 42, 46, 215, 161, 139, 47, 20, 245, 229, 206, 52, 226, 22, 140, 238, 118, 13, 189, 136, 67, 38, 144, 162, 2, 175, 75, 9, 8, 220, 6, 152, 62, 44, 239, 134, 198, 242, 143, 107, 89, 115, 187, 237, 240, 4, 18, 230, 25, 108, 146, 85, 43, 236, 203, 113, 56, 59, 138, 155, 84, 246, 142, 91, 64, 204, 87, 202, 102, 179, 255, 63, 190, 166, 31, 74, 24, 79, 251, 96, 57, 112, 111, 231, 249, 199, 131, 197, 16, 185, 116, 130, 41, 23, 186, 69, 211, 216, 168, 40, 123, 160, 132, 181, 50, 72, 188, 35, 223, 217, 90, 148, 154, 37, 184, 105, 10, 212, 51, 12, 176, 150, 129, 243, 128, 193, 173, 26, 221, 3, 209, 83, 244, 133, 163, 247, 76, 214, 82, 86, 122, 60, 227, 81, 0, 30, 254, 77, 7, 196, 195, 165, 167, 145, 17, 177, 213, 171, 224, 21, 97, 103, 100, 126, 109, 235, 34, 15, 135, 164, 98, 170, 88 }.

Keltirilgan S_1 jadval yuqori chiziqsizlik darajasini taqdim etgan bo‘lib, bu algoritmning chiziqli kriptotahlil usuliga bardoshli bo‘lishini ta’minlaydi. Boshqa tomondan, algoritm algebraik tahlilga bardoshli bo‘lishi ham talab etiladi (bu ikki talab bir vaqtda bajarilmaydi). Shu bois, algoritmdagi ikkinchi - S_2 jadvalni hosil qilishda uning yuqori algebraik immunitetga ega bo‘lishiga e’tibor qaratiladi.

Yuqori algebraik immunitetga ega bo‘lgan S jadvallardan qator algoritmlarda foydalanilgan. Masalan, STB 34.101.31-2011 va GOST R 34.12-2015 standartlarida algebraik immuniteti $AI(S) = 3$ ga va S jadvalga nisbatan tuzilgan tenglamalar soni, $N_{TS} = 441$ teng bo‘lgan. Chiziqsizlik darajalari esa mos ravishda 102 va 100 ga teng bo‘lgan. Shuningdek, algebraik immuniteti yuqoridagi kabi bo‘lgan va chiziqsizligi 102 dan katta bo‘lgan S jadvallarni hosil qilish qo‘yilgan maqsadga muvofiq bo‘ladi. Mazkur muammoni hal qilishning ko‘plab o‘ziga xos usullari mavjud bo‘lib, ular orasidan tasodifiy tanlashga asoslangan usul muhim ahamiyat kasb etadi. Shuning uchun yaratiladigan S_2 jadval uchun quyidagi tasdiqni belgilab oldik [35]:

3.1.1-tasdiq. *AI* parametr qiymati maksimal bo‘lgan optimal $S(8 \times 8)$ – jadval uchun $AI(S) = 3$, $N_{TS} = 441$ va $N(S) \geq 104$ o‘rinli.

Yuqorida keltirilgan tasdiqqa mos keluvchi S jadvallarni yaratishda [35, 102] manbalarda quyidagi ikki bosqichdan iborat bo‘lgan ishlar amalga oshirilgan:

1. Chiziqsizlik darajasi yuqori $(N(S) = 112)$ bo‘lgan (8×8) jadvalni olish.

2. (8×8) jadvalni tasodifiy N ta elementini o‘zaro o‘rnini almashtirish.

Tanlangan N qiymati [35] ishda 39 ga teng deb olingan bo‘lsa, [99] ishda 22 ga teng deb olingan. Mazkur ishda ham [35] manbada keltirilgan yondashuvdan foydalanildi. Hosil qilingan S_2 jadval va uning xususiyatlari quyidagi keltirilgan (3.2-jadval).

$S_2(8 \times 8) = \{26, 168, 150, 161, 166, 151, 128, 38, 193, 242, 50, 127, 139, 201, 240, 195, 100, 121, 39, 16, 67, 76, 108, 155, 196, 172, 216, 234, 178, 158, 213, 142, 125, 2, 199, 14, 23, 131, 203, 7, 97, 224, 132, 250, 62, 3, 122, 36, 190, 140, 25, 111, 29, 247, 184, 104, 179, 230, 219, 120, 209, 205, 10, 167, 163, 180, 241, 252, 63, 93, 87, 79, 66, 141, 202, 113, 95, 171, 102, 217, 160, 114, 22, 173, 156, 44, 73, 48, 187, 153, 49, 206, 52, 60, 254, 211, 24, 208, 239, 207, 130, 54, 204, 109, 214, 183, 198, 92, 88, 134, 32, 228, 117, 126, 135, 65, 138, 83, 31, 33, 99, 103, 116, 55, 12, 45, 145, 72, 84, 223, 56, 115, 68, 177, 174, 64, 42, 98, 251, 197, 245, 28, 77, 175, 69, 112, 220, 149, 4, 236, 15, 188, 253, 107, 13, 162, 46, 147, 58, 235, 89, 170, 192, 85, 6, 237, 225, 80, 75, 215, 90, 101, 74, 227, 37, 169, 200, 181, 91, 118, 71, 5, 20, 34, 47, 129, 154, 11, 194, 119, 9, 53, 144, 30, 233, 61, 123, 244, 81, 146, 41, 51, 176, 157, 35, 210, 18, 106, 137, 43, 212, 40, 221, 246, 248, 143, 8, 105, 57, 0, 165, 229, 226, 136, 82,$

27, 249, 218, 191, 185, 243, 96, 19, 255, 86, 124, 222, 110, 94, 133, 59, 159, 232, 17, 78, 189, 148, 164, 70, 186, 238, 21, 152, 1, 182, 231}.

Hosil qilingan S_1 va S_2 jadvallar O‘z DSt 1105:2009 shifrlash algoritmidagi ikki jadvallar o‘rnida foydalaniladi va uning asosiy chiziqsiz akslantirishlari hisoblanadi.

3.2-jadval

Generatsiya qilingan S_2 jadvallarning baholash natijalari

Baholash omillari		Qiymati
Balanslashganlik		True
Regulyarlik		True
Chiziqsizlik, $N(S)$		104
Korrelyatsion immunitet,(CI)		0
Minimal daraja, deg		7
Ayirma matritsa jadvalidagi maksimal qiymat, δ		8
$D(S)$		194944
Qat’iy lavin samaradorlik, SAC		False
Algebraik immunitet	AI(S)	3
	TS(S)	441

***Aralash ()* akslantirishi uchun diamatritsalarni statik holatda tanlash.** $Aralash()$ akslantirishi O‘z DSt 1105:2009 shifrlash algoritmida tarqatish xususiyatiga ega bo‘lgan akslantirish hisoblanadi. Boshqacha aytganda, mazkur akslantirish qayta ishlanayotgan ma’lumot ixtiyoriy bitining o‘zgarishi undan chiquvchi ma’lumotning o‘rtacha yarmining (50 %) o‘zgarishiga asoslanadi. Boshqa algoritmlarda tarqatuvchi akslantirishlar sifatida davriy surish (GOST 28147-89), bitlar (baytlar) o‘rnini almashtirish (DES) yoki chekli maydonda biror matritsaga ko‘paytirish (AES) kabi funksiyalar kombinatsiyasidan foydalanilgan.

$Aralash()$ akslantirishi farqli ravishda maxsus tuzilmali diamatritsaga ko‘paytirish funksiyasiga asoslangan. Maxsus tuzilmali diamatritsalar dastlab murakkab elektron sxemalar sinteziga bag‘ishlangan tadqiqot natijalarida keltirilgan [36].

3.1.1-ta’rif. Agar berilgan $m \times m$ tartibli diamatritsaning barcha diagonal elementlari bir-biriga teng va birinchi satrdan boshlab, to $m - 2$ satrgacha, har bir satr boshidagi element shu satr diagonal elementidan o‘ngda shu satrda joylashgan barcha elementlarga teng bo‘lsa, unday diamatritsa maxsus tuzilmali diamatritsa, deb ataladi.

Xususan, 4×4 tartibli maxsus tuzilmali diamatritsa quyida keltirilgan bo‘lib, undagi barcha dioganal elementlar bir-biriga teng bo‘lib, 1-satrdagi nodioganal elementlar bir-biriga teng va 2-satr boshida va satr so‘ngida joylashgan elementlar bir-biriga teng. Keltirilgan maxsus tuzilmali diamatritsa 10 xil elementdan, a_0,a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, shakllangan.

$$\begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{vmatrix} a_7 & a_0 & a_1 & a_2 \\ a_8 & a_7 & a_8 & a_8 \\ a_9 & a_3 & a_7 & a_9 \\ a_4 & a_5 & a_6 & a_7 \end{vmatrix}$$

Aralash () akslantirishida ham ikkita (K_1 va K_2) 4×4 tartibli maxsus tuzilmali diamatritsadan foydalaniladi. K_1 va K_2 maxsus tuzilmali diamatritsalar *ShaklSeansKalit(K_{ST})* almashtirishida hosil qilinadi. *Aralash ()* akslantirishida esa maxsus tuzilmali diamatritsalar va $Holat$ massivi bilan esa diamatritsaviy ko‘paytirish amali bajariladi (mazkur ketma-ketlik [21] manbada batafsil keltirilgan).

Maxsus tuzilmali diamatritsalarni hosil qilishning umumiy talabi mavjud emas. Biroq, [32] manbada maxsus tuzilmali diamatritsalar quyidagi shartlar asosida hosil qilingan:

- agar $a_7 mod 2 = 0$ga teng bo‘lsa, u holda $a_7 = (a_7 - 1) mod p$ almashtirish amalga oshirilsin;
- agar $(a_7 + a_0 + a_5 + a_8 + a_3) mod 2 = 0$ga teng bo‘lsa, $a_5 = (a_5 - 1)\ mod p$ almashtirish amalga oshirilsin;
- agar $(a_7 + a_1 + a_8 + a_6 + a_4) mod 2 = 0$ ga teng bo‘lsa, $a_6 = (a_6 - 1)\ mod p$ almashtirish amalga oshirilsin.

Bu yerda, $p = 256$ ga teng.

Maxsus tuzilmali diamatritsalarni hosil qilishning qat’iy algoritmi mavjud emasligi bois, yuqoridagi shartlarni qanoatlantiruvchi diamatritsalarni tasodifiy hosil qilish mumkin. Biroq, hosil qilingan diamatritsalarning raundlar bo‘yicha tarqatish ko‘rsatkichlarini yuqori bo‘lishiga ahamiyat berish talab etiladi. Shu sababli, quyidagi ketma-ketlikdagi ishlar amalga oshirildi:

1. Tasodifiy tanlangan kalitlar asosida K_1 va K_2 diamatritsalarni hosil qilish.

2. Har bir K_1 va K_2 dimatritsalar jufti uchun bir bitning o‘zgarishini har bir raundda necha bitga ta’sir qilishini aniqlash.

Keltirilgan ketma-ketliklarni ko‘p sonli kalitlar va yagona ochiq matn/ boshlang‘ich vektor uchun amalga oshirish maqsadga muvofiqdir. Shu sababli, O‘z DSt 1105:2009 shifrlash algoritmining dasturiy vositasi ushbu maqsadda o‘zgartirildi. Tajribada 200 ta turli K_1 va K_2 dimatritsalar juftlari hosil qilindi. Har bir dimatritsalar juftlarining har raunddan keyingi tarqatish ko‘rsatkichlari (SAC - qat’iy lavin samaradorlik) aniqlandi (ushbu natijalar 5-ilovaga keltirilgan). Olingan natijalar O‘z DSt 1105:2009 shifrlash algoritmini barcha hosil qilingan diamatritsalar juftlari uchun 3 raunddan so‘ng maksimal tarqatish darajasiga erishishini ko‘rsatdi. Boshqa tomondan, hosil qilingan K_1 va K_2 dimatritsalar juftlaridan birini statik ravishda foydalanish mumkinligini ham ko‘rsatdi. Hosil qilingan dimatritsalar juftlarining ayrimlari 6-ilovaga keltirilgan bo‘lib, mazkur ishda ular orasidan quyidagi ikki dimatritsalar jufti statik ravishda foydalanish uchun tanlab olindi.

$$K_1 = \begin{vmatrix} 149 & 157 & 87 & 182 \\ 92 & 149 & 92 & 92 \\ 13 & 77 & 149 & 13 \\ 157 & 68 & 184 & 149 \end{vmatrix} \qquad K_2 = \begin{vmatrix} 157 & 150 & 197 & 66 \\ 52 & 157 & 52 & 52 \\ 86 & 233 & 157 & 86 \\ 184 & 241 & 69 & 157 \end{vmatrix}$$

Shifrlash va rasshifrovkalash jarayoni uchun ushbu ikki diamatritsalarga teskari bo‘lgan diamatritsalar aniqlanadi va ulardan foydalaniladi. Umumiy xulosa sifatida shuni aytish mumkinki, olib borilgan tajribalar ixtiyoriy kalit asosida hosil qilingan ikki diamatritsadan statik ravishda foydalanish uning tarqatish xususiyatiga salbiy ta’sir o‘tkazmaydi.

Ushbu bo‘limda taklif etilgan 2 ta akslantirish ishlab chiqiluvchi shifrlash algoritmida foydalaniluvchi asosiy akslantirishlar hisoblanadi. Ular asosida hosil qilingan raund kalit generatori va shifrlash/ rasshifrovkalash algoritmiga keyingi bo‘limlarda to‘xtalib o‘tiladi.

3.2-§. Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi uchun raund kalitlarini shakllantirish

Kriptografik algoritmlarning bardoshligi faqat kalitning maxfiyligiga asoslanishi blokli shifrlash algoritmlarida raund kalitlarini ishlab chiqishga yuqori talablar qo‘yadi. Xususan, shifrlash kalitidan raund kalitlarini generatsiyalash algoritmini ishlab chiqishda, amalga oshirishning qulayligiga va xotiradan unumli foydalanishga e’tibor berish lozim. Bunda raund kalitlarini generatsiyalash jarayonida shifrlash

algoritmidagi akslantirishlardan foydalanishda qulaylik va xotiradan unumli foydalanish kabi imkoniyatlarni taqdim etadi. Shu bois, aksariyat blokli shifrlash algoritmlari aynan shu yondashuvga asoslangan (masalan, AES). Mazkur bo‘limda ham O‘z DSt 1105:2009 shifrlash algoritmini takomillashtirishda ushbu yondashuvdan foydalaniladi.

Odatda raund kalitlarini ishlab chiqishda oldingi raund kalitidan foydalanishga asoslaniladi. Masalan, AES va O‘z DSt 1105:2009 shifrlash algoritmlarida. Bunga ko‘ra, birinchi raund kaliti keyingi raund kalitini hosil qilishda ishlatiladi va h.k. Bu esa o‘z navbatida raund kalitlarini saqlab turish uchun yuqori xotira hajmini talab etadi. Xususan, raund kalitlaridan teskari foydalanishga asoslangan rasshifrovkalash jarayonida dastlab kalitlarni generatsiyalash va ularni saqlash talab etiladi. Shu sababli, mavjud muammolarni oldini oluvchi va har bir raund kalitlarini mustaqil ravishda generatsiyalash imkoniyatiga ega bo‘lgan $\phi()$ – funksiyani shakllantirish talab etiladi:

$$K_i = \phi(K, i).$$

Bu yerda, K – shifrlash kaliti, i – raund soni va K_i esa i – raund kaliti. Boshqacha aytganda, har bir raund kaliti shifrlash kaliti va raund soni asosida hosil qilinadi. Bundan tashqari, ishlab chiqilayotgan raund kalit generatori quyidagi talablarga javob berishi talab qilinsin:

– raund kalitidan shifrlash kalitini hisoblashning imkonsizligi (bir tomonlamalik);

– turli uzunlikdagi shifrlash kalitlarini qabul qilishi va chiqishda ham belgilangan uzunlikdagi raund kalitlarini hosil qilish.

Yuqorida keltirilgan talablarning birinchisi AES va O‘z DSt 1105:2009 algoritmlarida amalga oshirilmagan [39,21]. Ikkinchi talab bo‘yicha ham aksariyat algoritmlar kirish va chiqish qiymatiga qat’iy talablar qo‘yadi. Bundan tashqari, raund kalitini generatsiyalash algoritmlari uchun xos bo‘lgan muammolardan yana biri bu – zaif kalitlarni generatsiyalashdir [101]. Ushbu muammoni oldini olishda aksariyat shifrlash algoritmlarida va xesh funksiyalarda o‘zgarmaslarni qo‘shishdan foydalanilgan (masalan, AES shifrlash algoritmi va MD4, MD5, SHA1 kabi xesh funksiyalarda) [109]. Bu esa raund kalitini generatsiyalash algoritmini yaratishda o‘zgarmas kattaliklardan foydalanishga e’tibor qaratish kerakligini ko‘rsatadi [102]. Shuningdek, ishlab chiqiladigan raund kaliti generatorida ham shifrlash akslantirishlaridan foydalanish talabini bajarish maqsad qilib olindi.

Yuqorida keltirilgan talablar va tavsiyalar asosida takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi uchun raund

kalitini generatsiyalash algoritmi ishlab chiqildi. Ishlab chiqilgan raund kalitini generatsiyalash algoritmining ketma-ketligi quyida keltirilgan (3.1-rasm):

1. Uzunligi L bayt ($L \in [128, 512]$) bo‘lgan shifrlash kaliti $K = \{k_0 \parallel k_1 \parallel k_2 \parallel \cdots \parallel k_{L-1}\}$ kalit 512 bit uzunlikka quyidagi tartibda to‘ldiriladi va K' hosil qilinadi:

$$K' = k'_0 \parallel k'_1 \parallel k'_2 \parallel k'_3 \parallel \cdots \parallel k'_{63} =$$
$$k_0 \parallel k_1 \parallel k_2 \parallel \cdots \parallel k_{L-1} \parallel 0x08 \parallel 0x08 \parallel \cdots \parallel 0x08.$$

Kiritilgan kalitni 512 bitga to‘ldirish uzunligi $[128, 512]$ oraliqdagi kalitni kiritish talabini qanoatlantiradi.

2. Hosil bo‘lgan K' dan $W_1(8 \times 4)$ va $W_2(8 \times 4)$ massivlar quyidagicha hosil qilinadi:

$$W_1(8 \times 4) = \begin{vmatrix} k'_0 & k'_1 & k'_2 & k'_3 \\ k'_4 & k'_5 & k'_6 & k'_7 \\ k'_8 & k'_9 & k'_{10} & k'_{11} \\ k'_{12} & k'_{13} & k'_{14} & k'_{15} \\ k'_{16} & k'_{17} & k'_{18} & k'_{19} \\ k'_{20} & k'_{21} & k'_{22} & k'_{23} \\ k'_{24} & k'_{25} & k'_{26} & k'_{27} \\ k'_{28} & k'_{29} & k'_{30} & k'_{31} \end{vmatrix},$$

$$W_2(8 \times 4) = \begin{vmatrix} k'_{32} & k'_{33} & k'_{34} & k'_{35} \\ k'_{36} & k'_{37} & k'_{38} & k'_{39} \\ k'_{40} & k'_{41} & k'_{42} & k'_{43} \\ k'_{44} & k'_{45} & k'_{46} & k'_{47} \\ k'_{48} & k'_{49} & k'_{50} & k'_{51} \\ k'_{52} & k'_{53} & k'_{54} & k'_{55} \\ k'_{56} & k'_{57} & k'_{58} & k'_{59} \\ k'_{60} & k'_{61} & k'_{62} & k'_{63} \end{vmatrix}$$

Izoh: Agar dastlabki kalit uzunligi 256 bitdan kichik bo‘lsa, W_2 massiv elementlari W_1 massiv elementlari tartibini teskari foydalanish natijasida hosil qilinadi. Masalan, $k'_{32} = k'_{31}$, $k'_{33} = k'_{30}$va h.k.

3. Hosil bo‘lgan $W_1(8 \times 4)$ va $W_2(8 \times 4)$ massivlar statik maxsus tuzilmali diamatritsalarga asoslangan $Aralash()$ akslantirishiga kiritiladi:

$$W_1(8 \times 4) = Aralash(W_1(8 \times 4));$$
$$W_2(8 \times 4) = Aralash(W_2(8 \times 4)).$$

$Aralash()$ akslantirishini to‘ldirishda foydalanilgan bir xil baytlarni yo‘q qilishda foydalaniladi.

4. $W_1(8 \times 4)$ massivining barcha elementlari ($w_{i,j}^1$) uchun quyidagi tarzda hosil qilinuvchi o‘zgarmaslar XOR amalida qo‘shiladi:

$$w_{i,j}^1 = w_{i,j}^1 \oplus S_1\big((11 * (i+1) + (j+1) * r + j)\%256\big).$$

Shunga o‘xshash, $W_2(8 \times 4)$ massivining barcha elementlari ($w_{i,j}^2$) uchun quyidagi tarzda hosil qilinuvchi o‘zgarmaslar XOR amalida qo‘shiladi:

$$w_{i,j}^2 = w_{i,j}^2 \oplus S\big((11 * (i+2) + (j+2) * r + j)\%256\big).$$

Bu yerda, $i = [0,7]$ va $j = [0,3]$lar $W_1(8 \times 4)$ va $W_2(8 \times 4)$ massivlarning satr va ustunlari. $r = [0,8]$ – esa raundlar sonini ko‘rsatadi. O‘zgarmaslarni hosil qilishda ularni raund ichida takrorlanmasligiga e’tibor berildi (Ularning umumiy natijalari 7-ilovaga berilgan). Bu esa hosil bo‘ladigan $W_1(8 \times 4)$ va $W_2(8 \times 4)$ massivlarning elementlarini ham takrorlanish darajasini kamaytiradi.

5. Hosil bo‘lgan $W_1(8 \times 4)$ va $W_2(8 \times 4)$ massivlari statik S jadvallar asosida hosil qilingan *BaytAlmash()* akslantirishiga kiritiladi:

$$W_1(8 \times 4) = BaytAlmash(W_1(8 \times 4), r),$$
$$W_2(8 \times 4) = BaytAlmash(W_2(8 \times 4), r).$$

6. Shundan so‘ng, $W_1(8 \times 4)$ va $W_2(8 \times 4)$ massivlari *Sur()* akslantirishiga kiritiladi:

$$W_1(8 \times 4) = Sur(W_1(8 \times 4)),$$
$$W_2(8 \times 4) = Sur(W_2(8 \times 4)).$$

7. $W_1(8 \times 4)$ va $W_2(8 \times 4)$ massivlari asosida $W(8 \times 8)$ massivi quyidagicha hosil qilinadi:

$$W(8\times 8)=\begin{vmatrix} w_{0,0}^1 & w_{0,1}^1 & w_{0,2}^1 & w_{0,3}^1 & w_{0,0}^2 & w_{0,1}^2 & w_{0,2}^2 & w_{0,3}^2 \\ w_{1,0}^1 & w_{1,1}^1 & w_{1,2}^1 & w_{1,3}^1 & w_{1,0}^2 & w_{1,1}^2 & w_{1,2}^2 & w_{1,3}^2 \\ w_{2,0}^1 & w_{2,1}^1 & w_{2,2}^1 & w_{2,3}^1 & w_{2,0}^2 & w_{2,1}^2 & w_{2,3}^2 & w_{2,0}^2 \\ w_{3,0}^1 & w_{3,1}^1 & w_{3,2}^1 & w_{3,3}^1 & w_{3,0}^2 & w_{3,1}^2 & w_{3,2}^2 & w_{3,3}^2 \\ w_{4,0}^1 & w_{4,1}^1 & w_{4,2}^1 & w_{4,3}^1 & w_{4,0}^2 & w_{4,1}^2 & w_{4,2}^2 & w_{4,3}^2 \\ w_{5,0}^1 & w_{5,1}^1 & w_{5,2}^1 & w_{5,3}^1 & w_{5,0}^2 & w_{5,1}^2 & w_{5,2}^2 & w_{5,3}^2 \\ w_{6,0}^1 & w_{6,1}^1 & w_{6,2}^1 & w_{6,3}^1 & w_{6,0}^2 & w_{6,1}^2 & w_{6,2}^2 & w_{6,3}^2 \\ w_{7,0}^1 & w_{7,1}^1 & w_{7,2}^1 & w_{7,3}^1 & w_{7,0}^2 & w_{7,1}^2 & w_{7,2}^2 & w_{7,3}^2 \end{vmatrix}$$

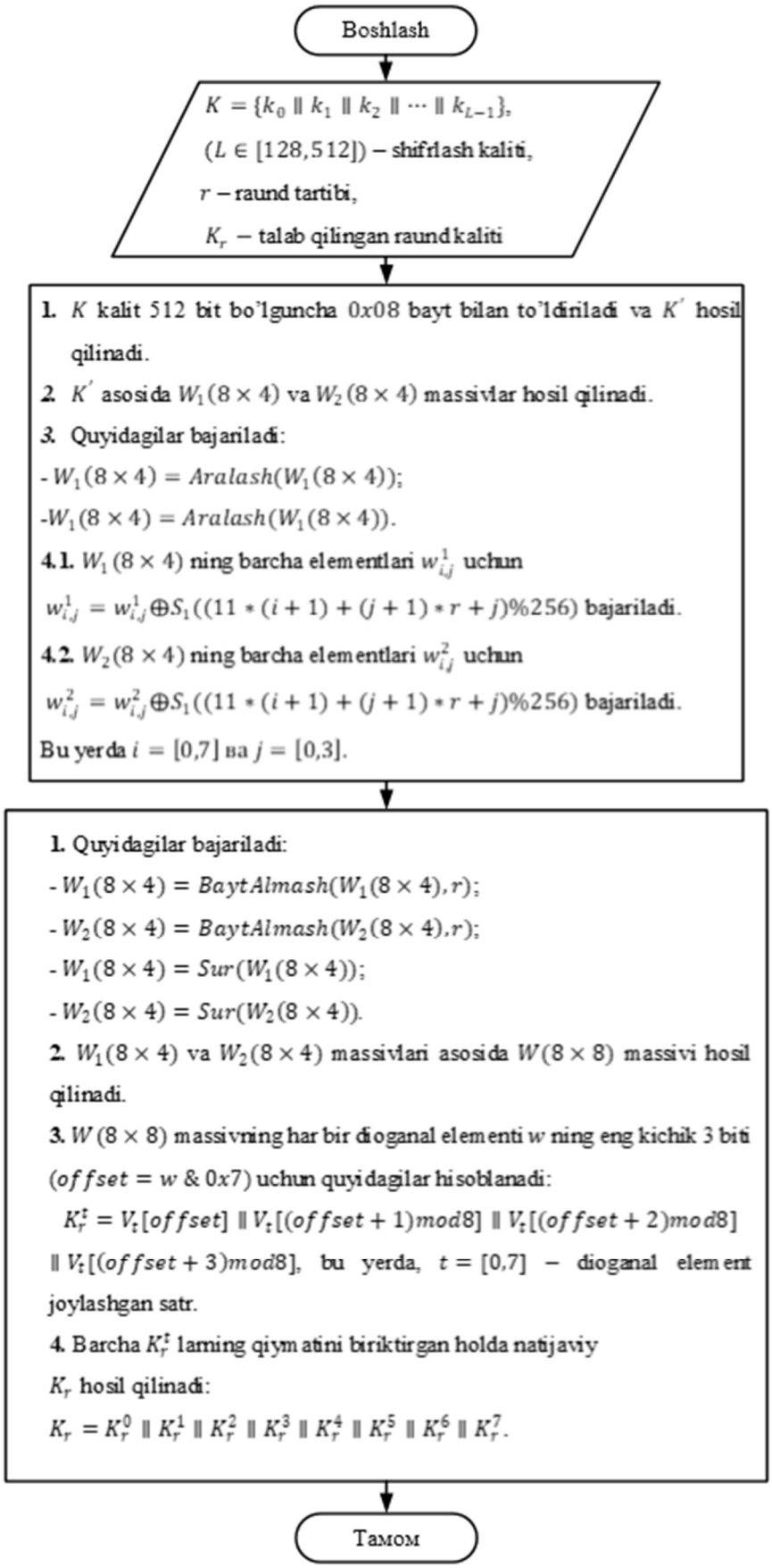
8. $W(8\times 8)$ massivning har bir diagonal elementi w ($w\in\{w_{0,0}^1, w_{1,1}^1, w_{2,2}^1, w_{3,3}^1, w_{4,0}^2,\ w_{5,1}^2, w_{6,2}^2, w_{7,3}^2\}$)ning eng kichik 3 biti ajratiladi: $offset = w\ \&\ 0x7$. Har bir diagonal elementga bog‘liq holda $W(8\times 8)$ massivning har bir satridan 64, 128, 192 va 256 bitli raund kalitlari holati uchun quyidagicha hosil qilinadi ($t=[0,7]$):

– 64 – bitli raund kaliti uchun: $K_r^t = V_t[offset]$;

– 128 – bitli raund kaliti uchun: $K_r^t = V_t[offset] \parallel V_t[(offset+1) mod 8]$;

– 192 – bitli raund kaliti uchun: $K_r^t = V_t[offset] \parallel V_t[(offset+1) mod 8] \parallel V_t[(offset+2) mod 8]$;

– 256 – bitli raund kaliti uchun: $K_r^t = V_t[offset] \parallel V_t[(offset+1) mod 8] \parallel V_t[(offset+2) mod 8] \parallel V_t[(offset+3) mod 8]$.



3.1-rasm. **Raund kalit generatsiyasi algoritmining blok sxemasi (256 bitli raund kaliti uchun)**

Bu yerda, V_t – bir o‘lchamli massiv bo‘lib, $W(8 \times 8)$ massivning w diagoanal elementi joylashgan t – satrini ko‘rsatadi. Tasodifiy baytlarni mazkur tartibda tanlab olish uni bir tomonlamalik xususiyatini ta’minlaydi.

9. $t = [0,7]$ shart uchun barcha K_r^t larning qiymatini biriktirgan holda natijaviy K_r kalit quyidagicha hosil qilinadi:

$$K_r = K_r^0 \parallel K_r^1 \parallel K_r^2 \parallel K_r^3 \parallel K_r^4 \parallel K_r^5 \parallel K_r^6 \parallel K_r^7.$$

Yuqorida keltirilgan ketma-ketliklarning [1-3] bosqichlari kiritilgan shifrlash kaliti uchun bir marta amalga oshiriladi. [4-9] bosqichlar raundlar soniga muvofiq ravishda takroriy amalga oshiriladi hamda talab etilgan raund kalitlarini taqdim etadi.

Ishlab chiqilgan kalit generatoridan hosil bo‘lgan psevdotasodifiy ketma-ketliklarni baholash uchun testlash amalga oshirildi. Testlashda dastlabki kiritiluvchi shifrlash kalitining uzunligi 128, 192, 256, 512 bitga teng bo‘lgan tasodifiy tanlangan hamda uzunligi 128 bitli zaif kalitlar (00, FF, 01, E1 va EF baytlardan iborat bo‘lgan) kiritilgan holat uchun amalga oshirildi. Testlashda har bir kalit uzunliklari uchun 5 martadan 2,048,000 bitdan va har bir zaif kalit uchun bir martadan psevdotasodifiy ketma-ketliklar hosil qilindi. Hosil bo‘lgan ketma-ketliklarni testlash uchun NIST statistik testlar to‘plamidan foydalanildi. Mazkur testlar to‘plami 16 ta turli testlash usullaridan iborat bo‘lib, ular asosida olingan natijalar qisqacha 3.3-jadvalda keltirilgan (natijalar batafsil ravishda 9-ilovaga keltirilgan).

3.3-jadval

Psevdotasodifiy ketma-ketliklarning statistik testlash natijalari

№	Dastlabki kalit uzunligi va tasodifiylik darajasi	Namunalar					%
		1	2	3	4	5	
1.	128 bit va tasodifiy	15/16	15/16	15/16	15/16	14/16	92,5
2.	192 bit va tasodifiy	15/16	15/16	15/16	15/16	15/16	93,75
3.	256 bit va tasodifiy	15/16	15/16	15/16	15/16	15/16	93,75
4.	512 bit va tasodifiy	15/16	15/16	14/16	14/16	15/16	91,25
5.	128 bit va zaif (0x00,0xFF,0x01,0xE1 va 0xEF iborat bo‘lgan)	15/16	13/16	13/16	15/16	15/16	88,75
						O‘rtacha:	**92**

O‘tkazilgan testlash natijalaridan kelib chiqib raund kalitlari generatorining o‘rtacha tasodifiylik darajasi 92 %ni qayd etganini bilish mumkin. Olingan testlash natijalari ishlab chiqilgan kalit generatorini turli uzunlikdagi va tasodifiylik darajasi turlicha bo‘lgan shifrlash kalitlari uchun bardoshli bo‘lgan raund kalitlarini hosil qilishini ko‘rsatdi. Bundan

tashqari, kalit generatorini har bir raund kalitini hosil qilish uchun mustaqil ravishda foydalanish mumkinligi hamda bir tomonlamalik xusisiyatlari mavjudlaridan afzalligini ko‘rsatadi.

3.3-§. O‘z DSt 1105:2009 shifrlash algoritmini takomillashtirish

Yuqorida keltirilgan takomillashtirilgan akslantirishlar va raund kaliti generatori asosida O‘z DSt 1105:2009 shifrlash algoritmini takomillashtirish tartibi bilan ushbu bo‘limda tanishib chiqiladi. O‘z DSt 1105:2009 shifrlash algoritmining raund funksiyasi: $Qo'shBosqichKalit() - Q$, $Aralash() - A$, $Sur() - S$ va $BaytAlmash() - B$, akslantirishlarning $Q \rightarrow$A$\rightarrow$S$\rightarrow$B tartibidan iborat.

Yuqoridagi bo‘limlarda $Aralash()$ va $BaytAlmash()$ akslantirishlari uchun maxsus tuzilmali diamatritsalar va S jadvallarni statik tarzda foydalanish talabi qo‘yilgan hamda zarur bo‘lgan maxsus tuzilmali diamatritsalar va S jadvallar yaratilgan.

Biroq, SP tarmoqqa asoslangan simmetrik blokli shifrlarni yaratish sohasida olib borilgan tadqiqotlar algoritmning bardoshligi nafaqat foydalanilgan akslantirishlarga, balki, ularning tartibiga ham bog‘liqligini ko‘rsatdi. Shu sababli, takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmini taqdim etishdan oldin raund akslantirishlar tartibi tanlash bo‘yicha kichik tajriba o‘tkazildi. Yuqorida keltirilgan to‘rtta akslantirishlar (Q, A, S, B)ning o‘rnini almashtirib hosil qilish mumkin bo‘lgan holatlari soni 24 ga teng (ya’ni, $4! = 24$). Shu sababli, har bir tartib uchun lavin samaradorligini aniqlash va unga asoslangan holda to‘g‘ri tartibni tanlash shart bo‘ladi.

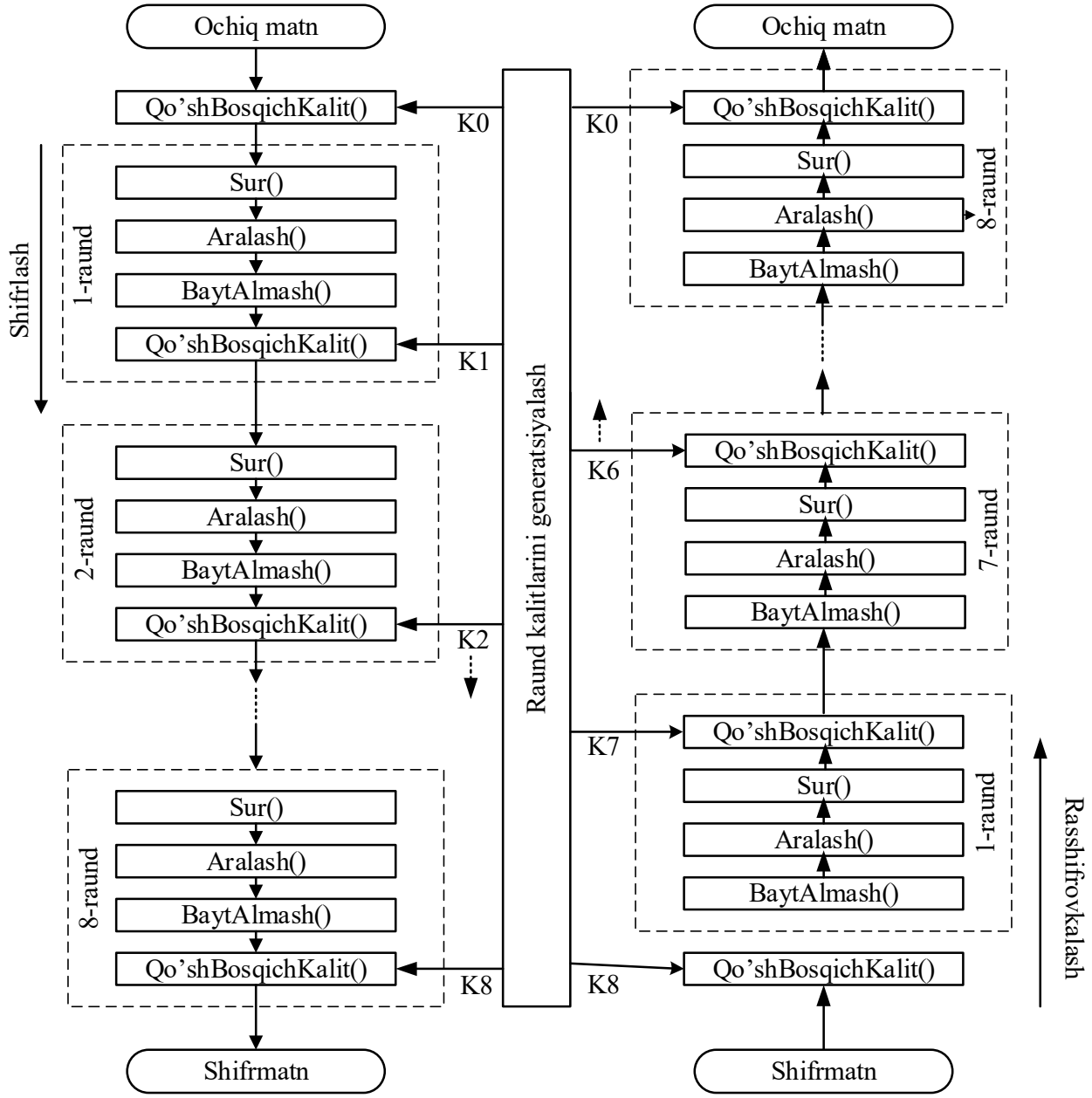
Ta’rif. Agar raund funksiyasiga kiritilgan ma’lumot bir bitining o‘zgarishi funksiyadan chiquvchi ma’lumot bitlarining o‘rtacha yarmini (50 %ini) o‘zgarishiga olib kelsa, u holda tanlangan tartib lavin samaradorligini qanoatlantiradi:

- $B \rightarrow$Q$\rightarrow$S$\rightarrow$A;
- Q$\rightarrow$S$\rightarrow$B$\rightarrow$A;
- Q$\rightarrow$S$\rightarrow$A$\rightarrow$B;
- S$\rightarrow$Q$\rightarrow$A$\rightarrow$B;
- S$\rightarrow$A$\rightarrow$B$\rightarrow$Q;
- S$\rightarrow$A$\rightarrow$Q$\rightarrow$B.

Ta’rifda keltirilgan qonuniyatni tekshirish uchun to‘rtta akslantirishlarning barcha 24 ta tartibi uchun lavin samaradorlikning 1, 2, 3 va 4-raundlar uchun qiymatlari 8-ilovaga keltirilgan. Tajriba natijasidan

ko‘rish mumkinki, akslantirishlardan quyidagi tartibda foydalanilganida 3-raunddan keyin lavin samaradorlik qiymati ≈50 %ga teng bo‘ladi.

Keltirilgan tartiblarning barchasidan foydalanish mumkin bo‘lib, olingan natijalarga ko‘ra va SP tarmoqlarda shifrlash/ rasshifrovkalash funksiyalarini qurishni osonlashtirish maqsadida $S \to A \to B \to Q$ tartibi tanlab olindi. Shu sababli, O‘z DSt 1105:2009 shifrlash algoritmida 8-raunddan keyin amalga oshirilgan $Qo'shBosqichKalit()$ akslantirishi 1-raund boshlanishidan oldin amalga oshiriladi. Bundan tashqari, 8-raunddan keyin amalga oshirilgan $Aralash()$ akslantirish olib tashlandi.



3.2-rasm. **Takomillashtirilgan O‘z DSt 1105:2009 algoritmi shifrlash/ rasshifrovkalash jarayonining tavsifi**

Rasshifrovkalash jarayoni uchun esa mos ravishda B→A→S→Q tartibdagi akslantirishlar ketma-ketligidan foydalanilib, bunda ham 1-raund boshlanishidan oldin $Qo'shBosqichKalit()$ akslantirishi amalga oshiriladi. Umumiy holda takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining shifrlash va rasshifrovkalash ketma-ketligi 3.2-rasmda aks ettirilgan.

Keltirilgan shifrlash va rasshifrovkalash sxemasidan ko‘rish mumkinki, talabga ko‘ra raundlar sonini osonlik bilan o‘zgartirish mumkin. Bundan tashqari, har bir raund uchun raund kalitlarini ham takrorlanmaydigan tarzda hosil qilish mumkin.

IV BOB. TAKOMILLASHTIRILGAN O‘Z DST 1105:2009 SHIFRLASH ALGORITMINI BAHOLASH

4.1. Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining integral kriptotahlili

3.3-bo‘limda keltirilgan takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmida akslantirish funksiyalari tartibini o‘zgartirilishi shifrlash algoritmining bardoshligiga ta’sir qilishi aytib o‘tilgan edi. To‘rtta akslantirish funksiyasining barcha variantlaridan qat’iy lavin samaradorligi bajarilgan 6 ta holati uchun integral tahlil natijalari quyidagi 4.1-jadvalda keltirilgan.

4.1-jadval

Akslantirish funksiyalarining turli tartibi uchun 2-raunddan so‘ng chiqish baytlariga ta’siri

№	Akslantirish tartibi	2-raunddan so‘ng chiqish baytlariga ta’siri
1.	B→Q→S→A	12
2.	Q→S→B→A	15
3.	Q→S→A→B	12
4.	S→Q→A→B	15
5.	S→A→B→Q	12
6.	S→A→Q→B	15

Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi mavjudligida foydalanilgan akslantirish funksiyalari o‘zgarmaganligi sababli, 2.3-bo‘limda qo‘llanilgan integral kriptotahlil strategiyasini ushbu algoritmga nisbatan ham qo‘llash mumkin. Quyida ushbu ketma-ketlik keltirilgan:

O‘z DSt 1105:2009 shifrlash algoritmi asosida takomillashtirilgan shifrlash algoritmining 4 raundi uchun integral kriptotahlil natijasi. $S \rightarrow A \rightarrow B \rightarrow Q$ akslantirish tartibi takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining to‘rt raundi uchun integral kriptotahlil usulini qo‘llab so‘nggi raund kalitini topishda, holat massivining bir elementi aktiv bo‘ladigan to‘plamni tanlash kerak bo‘ladi. Mazkur holda ochiq matnlar soni 2^8 ta bo‘lib, 4.1-rasmda ushbu to‘plamni 4 raundli takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi shifrlash jarayonida massiv elementlarining o‘zgarishi keltirilgan.

Aktiv bayt o‘rnini va akslantirish funksiyalarini almashtirilish kriptotahlil natijasiga ta’sir qiladi. Buni sinab ko‘rish uchun 4.1-jadvaldan bir baytning o‘zgarishi chiqishdagi 15 baytga ta’sir qiladigan boshqa bir akslantirishlar tartibidan foydalanish mumkin.

1-raund:

Sur()									*Aralash()*							
P	P	P	P	P	P	P	P		A	P	P	P	P	A	P	P
P	P	A	P	P	P	P	P		A	A	A	A	P	P	A	P
P	P	P	P	P	P	P	P		P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P		P	P	P	P	P	P	P	P
BaytAlmash()									*Qo‘shBosqichKalit()*							
A	P	P	P	P	A	P	P		A	P	P	P	P	A	P	P
A	A	A	A	P	P	P	A		A	A	A	A	P	P	P	A
P	P	P	P	P	P	P	P		P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P		P	P	P	P	P	P	P	P

2-raund:

Sur()									*Aralash()*							
P	P	P	A	P	P	P	P		A_1	A_1	A_1	A_1	D_0	A_1	D_0	D_0
P	A	A	P	P	A	P	P		A_1	A_1	A_1	A_1	D_0	D_0	D_0	A_1
A	P	P	A	P	P	P	P		A_1	D_0	D_0	D_0	A_1	A_1	A_1	A_1
P	P	P	P	P	A	P	P		A_1	A_1	A_1	A_1	D_0	D_0	D_0	A_1
BaytAlmash()									*Qo‘shBosqichKalit()*							
D_0	D_0	D_0	D_0	D_1	D_0	D_1	D_1		D_0	D_0	D_0	D_0	D_1	D_0	D_1	D_1
D_0	D_0	D_0	D_0	D_1	D_1	D_1	D_0		D_0	D_0	D_0	D_0	D_1	D_1	D_1	D_0
D_0	D_1	D_1	D_1	D_0	D_0	D_0	D_0		D_0	D_1	D_1	D_1	D_0	D_0	D_0	D_0
D_0	D_0	D_0	D_0	D_1	D_1	D_1	D_0		D_0	D_0	D_0	D_0	D_1	D_1	D_1	D_0

3-raund:

Sur()									*Aralash()*							
D_1	D_0	D_1	D_0	D_0	D_1	D_0	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_0	D_0	D_0	D_0	D_1	D_0	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_0	D_1	D_0	D_0	D_0	D_0	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_0	D_1	D_1	D_0	D_0	D_0	D_0	D_0		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
BaytAlmash()									*Qo‘shBosqichKalit()*							
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

4-raund:

Sur()									*Aralash()*							
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
BaytAlmash()									*Qo‘shBosqichKalit()*							
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1		D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

4.1-rasm. S→A→B→Q **tartibdagi 4 raundli takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi orqali shifrlash jarayonida massiv elementlarining o‘zgarishi**

Masalan, Q→S→B→A akslantirishlar tartibi uchun 4 raundli takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining integral kriptotahlil natijasi quyidagicha (4.2-rasm).

S→A→B→Q tartibdagi to‘rt raundli shifrlash algoritmi uchun tanlab olingan ochiq matnlarga mos shifr matnlar to‘plami T_i mavjud bo‘lganda, deshifrlash jarayoni ketma-ketligi quyidagicha:

$$C_i = Sur(Aralash(BaytAlmash(Qo'shBosqichKalit(T_i, K^4))))$$

Bu yerda, C_i massiv to‘rtinchi raund kirishidagi holatni ifodalaydi. K^4 kalitning K_q^4 $(1 \le q \le 32)$ baytlari qabul qilishi mumkin bo‘lgan barcha (0 dan 255 gacha) qiymatlarida C_i massivni uchinchi raunddagi akslantirishlardan o‘tkaziladi:

$$R_{iq} = Sur\left(Aralash\left(BaytAlmash(C_i)\right)\right)$$

Shundan so‘ng, R_{iq} qiymatlarning *XOR* yig‘indisi hisoblanadi:

$$XOR = R_{1q} \oplus R_{2q} \oplus R_{3q} \oplus R_{mq}$$

Agar $XOR = 0$ ga teng bo‘lsa, K_q^4 $(1 \le q \le 32)$ raund kaliti nomzod kalitlar ro‘yxatiga qo‘shiladi.

Xuddi shunday, Q→S→B→A tartibga ega to‘rt raundli shifrlash algoritmi uchun tanlab olingan ochiq matnlarga mos shifr matnlar to‘plami T_i mavjud bo‘lgan holda ularning to‘rtinchi raundagi deshifrlash holati quyidagicha bo‘ladi:

$$C_i = Qo'shBosqichKalit(Sur\left(BaytAlmash\left(Aralash(T_i)\right)\right), K^4)$$

Bu yerda, C_i massiv to‘rtinchi raund kirishidagi to‘plamni ifodalaydi. K^4 kalitning K_q^4 $(1 \le q \le 32)$ baytlarining qabul qilishi mumkin bo‘lgan barcha
(0 dan 255 gacha) qiymatlarida uchun C_i massivni uchinchi raunddagi akslantirishlardan o‘tkaziladi:

$$R_{iq} = Sur\left(BaytAlmash\left(Aralash(C_i)\right)\right)$$

Shundan so‘ng, R_{iq} qiymatlarning *XOR* yig‘indisi hisoblanadi:

$$XOR = R_{1q} \oplus R_{2q} \oplus R_{3q} \oplus R_{mq}$$

Agar $XOR = 0$ ga teng bo‘lsa, K_q^4 $(1 \le q \le 32)$ raund kaliti nomzod kalitlar ro‘yxatiga qo‘shiladi.

Yuqoridagi tahlil natijalaridan kelib chiqib shuni aytish mumkinki, S→A→B→Q tartibli akslantirishga ega 4 raundli O‘z DSt 1105:2009 shifrlash algoritmi asosida takomillashtirilgan shifrlash algoritmiga integral kriptotahlil usulini qo‘llab, tanlab olingan 2^8 ta ochiq matnlar

asosida 2-raund so‘ngidagi *BaytAlmash()* akslantirishining xossalariga muvofiq raund chiqishidagi kalitning K_2^4, K_4^4, K_5^4, K_7^4, K_9^4, K_{10}^4, K_{11}^4, K_{12}^4, K_{14}^4, K_{17}^4, K_{19}^4, K_{20}^4, K_{21}^4, K_{22}^4, K_{25}^4, K_{28}^4, K_{29}^4, K_{30}^4, K_{31}^4, K_{32}^4 baytlarini (jami 160 bit) topish mumkin.

1-raund:

Qo‘shBosqichKalit()							
A	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P

Sur()							
P	P	P	P	P	P	P	P
P	P	A	P	P	P	P	P
P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P

BaytAlmash()							
P	P	P	P	P	P	P	P
P	P	A	P	P	P	P	P
P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P

Aralash()							
A	P	P	P	P	A	P	P
A	A	A	A	P	P	P	A
P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P

2-raund:

Qo‘shBosqichKalit()							
A	P	P	P	P	A	P	P
A	A	A	A	P	P	P	A
P	P	P	P	P	P	P	P
P	P	P	P	P	P	P	P

Sur()							
P	P	P	A	P	P	P	P
P	A	A	P	P	A	P	P
A	P	A	P	P	P	P	P
P	P	P	P	A	P	P	P

BaytAlmash()							
A_1	A_1	A_1	D_0	A_1	A_1	A_1	A_1
A_1	D_0	D_0	A_1	A_1	D_0	A_1	A_1
D_0	A_1	D_0	A_1	A_1	A_1	A_1	A_1
A_1	A_1	A_1	A_1	D_0	A_1	A_1	A_1

Aralash()							
D_0	D_0	D_0	D_0	D_1	D_0	D_1	D_1
D_1	D_1	D_0	D_1	D_1	D_1	D_1	D_0
D_0	D_1	D_1	D_1	D_0	D_0	D_0	D_0
D_0	D_0	D_0	D_0	D_1	D_1	D_1	D_0

3-raund:

Qo‘shBosqichKalit()							
D_0	D_0	D_0	D_0	D_1	D_0	D_1	D_1
D_1	D_1	D_0	D_1	D_1	D_1	D_1	D_0
D_0	D_1	D_1	D_1	D_0	D_0	D_0	D_0
D_0	D_0	D_0	D_0	D_1	D_1	D_1	D_0

Sur()							
D_1	D_0	D_1	D_0	D_0	D_1	D_0	D_1
D_0	D_0	D_0	D_0	D_1	D_1	D_1	D_1
D_0	D_1	D_0	D_1	D_0	D_0	D_1	D_1
D_0	D_1	D_1	D_0	D_0	D_1	D_0	D_0

BaytAlmash()							
D_1	D_0	D_1	D_0	D_0	D_1	D_0	D_1
D_0	D_0	D_0	D_0	D_1	D_1	D_1	D_1
D_0	D_1	D_0	D_1	D_0	D_0	D_1	D_1
D_0	D_1	D_1	D_0	D_0	D_1	D_0	D_0

Aralash()							
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

4-raund:

Sur()							
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

Aralash()							
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

BaytAlmash()							
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

Qo‘shBosqichKalit()							
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1
D_1	D_1	D_1	D_1	D_1	D_1	D_1	D_1

4.2-rasm. Q→S→B→A **tartibdagi 4 raundli takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi orqali shifrlash jarayonida massiv elementlarining o‘zgarishi**

2-raund so‘ngidagi *BaytAlmash()* akslantirishining xossalariga muvofiq raunddagi kalitning qolgan K_1^4, K_3^4, K_6^4, K_8^4, K_{13}^4, K_{15}^4, K_{16}^4, K_{18}^4, K_{23}^4, K_{23}^4, K_{24}^4, K_{26}^4, K_{27}^4 baytlarini to‘liq tanlash usulidagi jami variantlar soni 2^{96} ga teng bo‘ladi.

Shuningdek, Q→S→B→A tartibli akslantirishga ega 4 raundli takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmiga integral kriptotahlil usulini qo‘llab, tanlab olingan 2^8 ta ochiq matnlar asosida 2-raund so‘ngidagi *BaytAlmash()* akslantirishining xossalariga muvofiq raund chiqishidagi kalitning K_{27}^4, K_1^4, K_2^4, K_2^4, K_3^4, K_4^4, K_6^4, K_{11}^4, K_{16}^4, K_{17}^4, K_{21}^4, K_{22}^4, K_{23}^4, K_{24}^4, K_{25}^4, K_{26}^4, K_{27}^4, K_{28}^4, K_{32}^4, K_{31}^4, K_{32}^4 baytlarini (jami 136 bit) topish mumkin. 2-raund so‘ngidagi *BaytAlmash()* akslantirishining xossalariga muvofiq raunddagi kalitning qolgan K_5^4, K_7^4, K_8^4, K_9^4, K_{10}^4, K_{12}^4, K_{13}^4, K_{14}^4, K_{15}^4, K_{18}^4, K_{19}^4, K_{20}^4, K_{29}^4, K_{30}^4, K_{31}^4 baytlarini to‘liq tanlash usulidagi jami variantlar soni 2^{120} ga teng bo‘ladi.

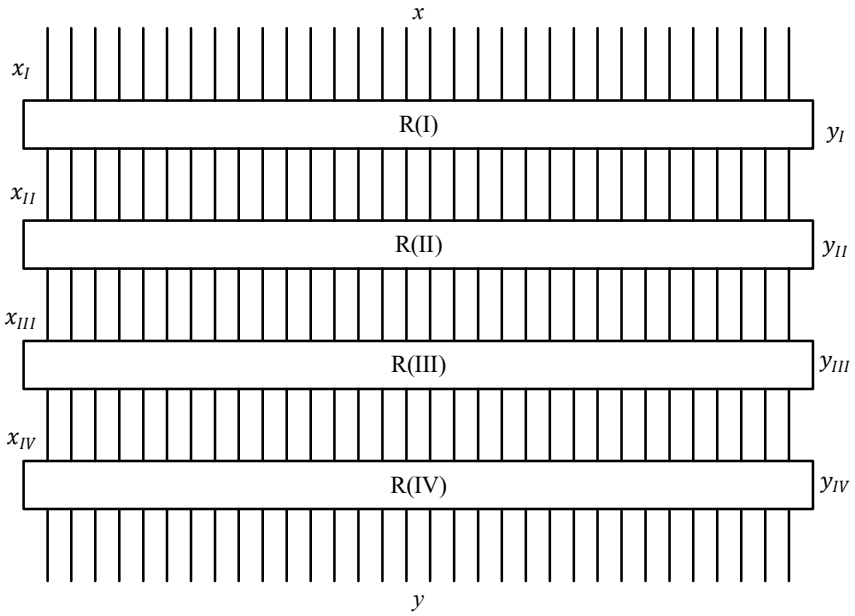
4.2. Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining algebraik kriptotahlili

2.2-bo‘limda keltirilgan ma’lumotlarga asosan, algebraik kriptotahlil usulini o‘tkazishda algoritm akslantirishlarining algebraik xususiyatlarini alohida o‘rganish talab etiladi. Takomillashtirilgan algoritmda akslantirishlarning xususiyatlari o‘zgarmaganligi sababli, ular uchun ham 2.2-bo‘limdagi xususiyatlar o‘rinli hisoblanadi. Quyida takomillashtirilgan shifrlash algoritmiga algebraik kriptotahlil usulini qo‘llashdagi natijalar algoritm akslantirishlarining ketma-ketligi va raund kalitlari generatsiyasining ta’siri nuqtayi nazaridan keltiriladi.

Algebraik kriptotahlil usuliga ko‘ra, har bir akslantirish uchun tenglamalar shakllantirilganidan so‘ng, ularni o‘zaro bog‘lash orqali har bir raund uchun tenglamalar sistemasi tuziladi. Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining raund elementlarini bog‘lash (ya’ni, algoritmga kirish va chiqish bitlari orqali ifodalanuvchi tenglamalarni shakllantirish) 2.2-paragrafdagi kabi *X, A, S, B* funksiyalar uchun tuzilgan tenglamalardan foydalanib amalga oshiriladi.

2.2-paragrafda *X, A, S, B* akslantirishlari uchun algebraik tenglamalar sistemasini qurish va ushbu akslantirishlarni bir-biri bilan bog‘lash masalasi ko‘rib chiqilgan. 4.3-rasmda algoritmning bir raundidagi akslantirishlar sxemasi keltirilgan bo‘lib, akslantirishlar ketma-ketligining raunddan chiqish massivlarini kirish massivlariga bog‘liq ravishda ifodalash mumkin.

Bu yerda, “x” raundga kiruvchi, “y” esa raunddan chiquvchi bitlar massivini anglatadi. $R(i)$ – $i-$ tartibli akslantirishni, $x_I, x_{II}, x_{III}, x_{IV}$ belgilashlar esa mos ravishda $i-$tartibli akslantirishlar *(X, A, S, B* akslantirishlardan biri*)*ga kirish bitlari massivini, $y_I, y_{II}, y_{III}, y_{IV}$ belgilashlar esa mos ravishda $i-$tartibli akslantirishlar (X, A, S, B akslantirishlardan biri)dan chiqish bitlari massivini bildiradi. Demak, quyidagi tengliklar o‘rinli: $x_I = x, x_{II} = y_I, x_{III} = y_{II}, x_{IV} = y_{III}, y = y_{IV}$.



4.3-rasm. **Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi uchun algebraik akslantirishlar sxemasi**

Takomillashtirilgan algoritm uchun akslantirishlar ketma-ketligini 3.3-paragrafda taklif qilingan variantlari uchun 2.2-paragrafda keltirilgan ma’lumotlarga asosan akslantirishlar o‘rtasidagi bog‘lanishlarni (2.2-paragrafdagi *BaytAlmash()* akslantirishiga nisbatan tenglamalar sistemasini tuzish usullariga bog‘liq ravishda) quyidagi 6 xil usulda qurish mumkin.

1. Raunddan chiqish massivlarini kirish massivlariga bog‘liq ravishda quyidagicha ifodalash mumkin:

$$y = B\left(X\left(S\left(A(x)\right)\right)\right)$$

$$y = X\left(S\left(B\left(A(x)\right)\right)\right)$$

$$y = X\left(S\left(A\left(B(x)\right)\right)\right)$$

$$y = S\left(X\left(A\left(B(x)\right)\right)\right)$$

$$y = S\left(A\left(B\left(X(x)\right)\right)\right)$$

$$y = S\left(A\left(X\left(B(x)\right)\right)\right)$$

2. Teskari (rasshifrovkalash) yo‘nalishida raundga kirish massivlarini raunddan chiqish massivlariga bog‘lanishini quyidagicha ifodalash mumkin:

$$x = A^{-}\left(S^{-}\left(X^{-}\left(B^{-}(y)\right)\right)\right)$$

$$x = A^{-}\left(B^{-}\left(S^{-}\left(X^{-}(y)\right)\right)\right)$$

$$x = B^{-}\left(A^{-}\left(S^{-}\left(X^{-}(y)\right)\right)\right)$$

$$x = B^{-}\left(A^{-}\left(X^{-}\left(S^{-}(y)\right)\right)\right)$$

$$x = X^{-}\left(B^{-}\left(A^{-}\left(S^{-}(y)\right)\right)\right)$$

$$x = B^{-}\left(X^{-}\left(A^{-}\left(S^{-}(y)\right)\right)\right)$$

3. Agar *BaytAlmash()* akslantirishiga nisbatan tuzilgan tenglamalar $F(x, y) = 0$ ko‘rinishidagi, ya’ni aralash (darajasi pasaytirilgan) tenglamalar bo‘lsa, akslantirishga kiruvchi va chiquvchi bitlar mustaqil ravishda ifodalanmagan quyidagi ko‘rinishdagi tenglamalar hosil bo‘ladi:

$$F\left(X\left(S\left(A(x)\right)\right), y\right) = 0$$

Shundan so‘ng, raundlarni o‘zaro bog‘lash jarayoni amalga oshiriladi. Ya’ni, ular asosida to‘liq shifrlash algoritmini ifodalovchi umumiy tenglamalar sistemasi shakllantiriladi.

O‘z DSt 1105:2009 algoritmining raundlarini bog‘lashni yuqoridagi xususiyatlarga muvofiq, uch xil yondashuv yordamida amalga oshirish mumkin:

1. Har bir raund chiqishidagi bitlarni mustaqil ifodalovchi tenglamalarni tuzish orqali.
2. Har bir raund kirishidagi bitlarni mustaqil ifodalovchi tenglamalarni tuzish orqali.
3. Har bir raund kirishida yangi o‘zgaruvchi kiritish usuli orqali.

Har bir raund uchun ushbu jarayon takrorlanadi. Bu usul yordamida tuzilgan tenglamalar sistemasida algoritmga kirish va chiqish bitlaridan tashqari nafaqat kalit bitlari, balki, har bir raundda kiritilgan yangi o‘zgaruvchilar noma’lum sifatida qatnashadi. Ushbu usulda tuzilgan

tenglamalar sistemasining darajasi 1- va 2-usulga nisbatan past bo‘lsada, noma’lumlar sonining yuqoriligi ushbu usulning kamchiligi hisoblanadi.

1 – va 2 – usullardan umumiy algoritm uchun tenglamalar sistemasini qurishda parallel ravishda foydalanish tenglamalar sistemasi darajasining oshib ketmasligini ta’minlaydi. Ya’ni, 1-usuldan foydalanib $1, 2, \ldots, n/2$ raundlar uchun tenglamalar tuziladi. Parallel ravishda 2-usuldan esa $n,\ n-1, \ldots, n/2+1$ raundlar uchun tenglamalar tuziladi.

Natijada $n/2$ – raunddan chiqish bitlari algoritmga kirish bitlari orqali, $n/2+1$– raundga kirish bitlari esa shifrlash algoritmidan chiqish bitlari orqali ifodalangan tenglamalar sistemasi hosil bo‘ladi. $x_{i+1} = y_i$ ekanligidan, hosil bo‘lgan tenglamalar bir-biriga tenglashtiriladi va darajasi faqat 1-usul yordamida tuzish mumkin bo‘lgan tenglamalar sistemasi darajasidan kichik bo‘lgan quyidagi ko‘rinishdagi tenglama hosil bo‘ladi:

$$F\left(x_{i+1}, k_1, k_2, \ldots, k_{\frac{n}{2}}\right) = F\left(y_i, k_{\frac{n}{2}+1}, \ldots, k_{n-1}, k_n\right)$$

Umumiy tenglamalar sistemasi hosil qilinganidan so‘ng, qiymati ma’lum bo‘lganlar noma’lumlar (ochiq va shifr matn bitlarini ifodalovchi noma’lumlar) qiymatlari bilan almashtiriladi. Qolgan noma’lumlarni esa, tenglamalar sistemasini yechish orqali aniqlanadi. Ushbu noma’lumlar keyinchalik maxfiy kalit bitlarini aniqlash imkonini beradi.

Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi akslantirishlariga nisbatan o‘tkazilgan sinov natijalari. Avvalgi bo‘limda o‘tkazilgan tajribalar O‘z DSt 1105:2009 shifrlash algoritmidagi 3-bobda keltirib o‘tilgan algoritm asosida tenglamalar sistemalari shakllantirildi. Quyidagi 4.2-jadvalda shakllantirilgan tenglamalar sistemalarining algebraik xususiyatlari bo‘yicha ma’lumotlar keltirilgan.

-

o‘yicha quyidagicha xulosalar qilish mumkin:

O

O

o

O

3 – darajali tenglamalar soni 441 tani tashkil qildi va bu ko‘rsatkich o‘zgarishsiz qoldi.

o

a

O‘z DSt 1105:2009shifrlash algoritmida taklif etilgan diamatritsalar diamatritsalarning diagonal elementlarni ifodalovchi tenglamalar sistemalarining algebraik xususiyatlari bo‘yicha ma’lumotlar keltirilgan (4.3-jadval).

’ -

o

‘

o

‘

o‘rish mumkinki, shifrlashda ishlatiladigan *K1*, *K2t* maxsus tuzilmali diamatritsalarga kirish va chiqish bitlarining bog‘liqligi tenglamalarida birhadlarning umumiy soni 14993 tani tashkil qildi.

Mazkur bo‘limda o‘tkazilgan eksperimentlar natijalaridan kelib chiqib, takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi akslantirishlari ketma-ketligi o‘zgargan holatlar uchun shakllantirilgan tenglamalar sistemalarining darajasi va noma’lumlar sonining raundlar bo‘yicha taqsimoti 4.4-jadvalda keltirilgan.

4.4-jadval

T

№	Akslantirishlardan	1raund	I	II	2raund	I	II

a

k

o

m

i

l

l

	foydalanish tartibi	TS	*Deg*	NS			TS	*Deg*	NS		
1.	XBAS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{74}
2.	ABSX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{74}
3.	ASXB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{74}
4.	BASX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{74}
5.	BAXS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{74}
6.	BXAS	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{74}

I

z

o

h

.

Yuqoridagi 4.4-jadvalga asosan quyidagilarni xulosa qilish mumkin:

h

– takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi akslantirishlaridan foydalanish ketma – ketligi faqat bir raundli algoritm uchun shakllantirilgan tenglamalar sistemasi parametrlariga sezilarli ta’sir etadi;

T

S

– ikkinchi raunddan boshlab akslantirishlardan foydalanish ketma – ketligi, *BaytAlmash()* akslantirishi uchun tuzilgan tenglamalar sistemasi darajasi *deg=8* bo‘lganligi sababli tenglamalar sistemasi parametrlariga sezilarli ta’sir etmaydi;

t

e

n

g

– yangi raund kalitlarini generatsiya qilish algoritmi tenglamalar sistemasini saqlash uchun talab qilinadigan xotira hajmining oshishiga olib keladi;

l

a

m

a

l

– takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi ikkinchi raunddan boshlab shakllantirilgan tenglamalar sistemasini saqlash uchun talab qilinadigan xotira hajmi mavjudiga nisbatan 2 marta ortishi uning algebraik kriptotahlilga bardoshligini ham 2 martaga oshiradi.

a

r

Mazkur bo‘limda O‘z DSt 1105:2009 shifrlash algoritmi asosida takomillashtirilgan shifrlash algoritmi *Aralash()* hamda *BaytAlmash()* akslantirishlari uchun tajribalar o‘tkazildi. O‘tkazilgan tajribalar natijasida quyidagi xulosalarni berish mumkin:

S

o

n

– algoritmdagi *Aralash()* hamda *BaytAlmash()* akslantirishlari tenglamalar darajasi hamda noma’lumlar sonining ortishiga xizmat qiladi;

i

– akslantirishlardan keltirilgan ketma-ketlikda foydalanilsa bir raundli shifrlash algoritmi uchun teskari yo‘nalishda 1-darajali 256 ta noma’lumli 256 ta tenglamalardan iborat sistemani shakllantirish mumkin;

D

e

g

–

d

– akslantirishlardan *Qo‘shBosqichKalit()* hamda *Aralash()* akslantirishlari o‘rinlari almashtirilgan ketma-ketlikda foydalanilsa, bir raundli shifrlash algoritmi to‘g‘ri yo‘nalishda shakllantirilgan tenglamalar sistemasi darajasi *BaytAlmash()* akslantirishi uchun tuzilgan tenglamalar sistemasi darajasiga, teskari yo‘nalishda shakllantirilgan tenglamalar sistemasi darajasi *Aralash()* akslantirishi uchun tuzilgan tenglamalar sistemasi darajasiga teng bo‘ladi;

– *Sur()* akslantirishi esa chiziqli akslantirish bo‘lganligi sababli tenglamalar darajasi va noma’lumlar soniga ta’sir qilmaydi, lekin bitlarni aralashtirish nuqtayi nazaridan ushbu akslantirish muhim hisoblanadi;

– raundlar soni oshib borishi bilan tenglamalar darajasi va noma’lumlar soni, shuningdek, tenglamalarni yechish murakkabligi oshib boradi;

– raund kalitlaridan takroriy foydalanish (masalan, O‘z DSt 1105:2009 shifrlash algoritmida ikkinchi raunddan boshlab har bir raund kaliti oldingi raund kalitidan 83 bitga farq qiladi) shifrlash algoritmining algebraik kriptotahlil usuliga bardoshligini kamaytiradi, taklif qilingan raund kalitlarini generatsiya qilish usuli esa algoritmning algebraik kriptotahlil usuliga bardoshligini oshiradi;

– raundlar sonining yuqori tanlash imkoniyatining yaratilganligi takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining algebraik kriptotahlil usuliga bardoshligini oshiradi;

– takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmida *S1* va *S2* jadvallar kriptografik talablar asosida tanlanganligi bois, shifrlash algoritmining algebraik kriptotahlil usuliga bardoshligini oshirgan;

– takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmida raund kalitlari uzunligi o‘lchamini yuqori tanlash imkoniyati algoritmning algebraik kriptotahlilga bardoshligini oshirgan;

– turli raundli takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmiga algebraik kriptotahlil usulini qo‘llashdan olingan tenglamalar sistemasini *Mutant XL* usuli orqali yechish imkoniyati nazariy mavjud;

– takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi ikkinchi raunddan boshlab shakllantiriladigan tenglamalar sistemasini saqlash uchun talab qilinadigan xotira hajmini ta’minlash imkoniyati mavjud emasligi sababli algebraik kriptotahlil usuliga bardoshli.

Ushbu xulosalardan kelib chiqib, takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining va umuman SP tarmog‘iga asoslangan shifrlash algoritmlarining algebraik kriptotahlil usuliga bardoshliligini oshirish bo‘yicha quyidagi tavsiyalar ishlab chiqildi:

– algoritmdagi chiziqsiz akslantirish, ya’ni *S* jadvallar o‘lchamini kriptografik talablar asosida tanlash;

– algoritmda raundlar sonining yuqori bo‘lishini ta’minlash;

– raund kalitlarining bir-biriga chiziqli bog‘liq bo‘lmasligi;

– raund kalitlarinining uzunligi yuqori bo‘lishi.

Ushbu tadqiqot davomida erishilgan ilmiy yutuqlar, ishlab chiqilgan algoritm va tegishli dasturiy ta’minotlar hamda turli sinovlar orqali olingan natijalardan quyidagi maqsadlarda foydalanish mumkin:

– takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi va shu kabi shifrlash algoritmlarini algebraik kriptotahlil usuliga baholashda hamda ushbu algoritmlarda foydalanilgan akslantirishlarning algebraik xususiyatlarini (immunitetini) aniqlashda (tadqiqot maqsadida);

– algebraik kriptotahlil usuliga bardoshli bo‘lgan shifrlash algoritmlarini ishlab chiqishda.

4.3-§. Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmini amaliyotda qo‘llash natijalari

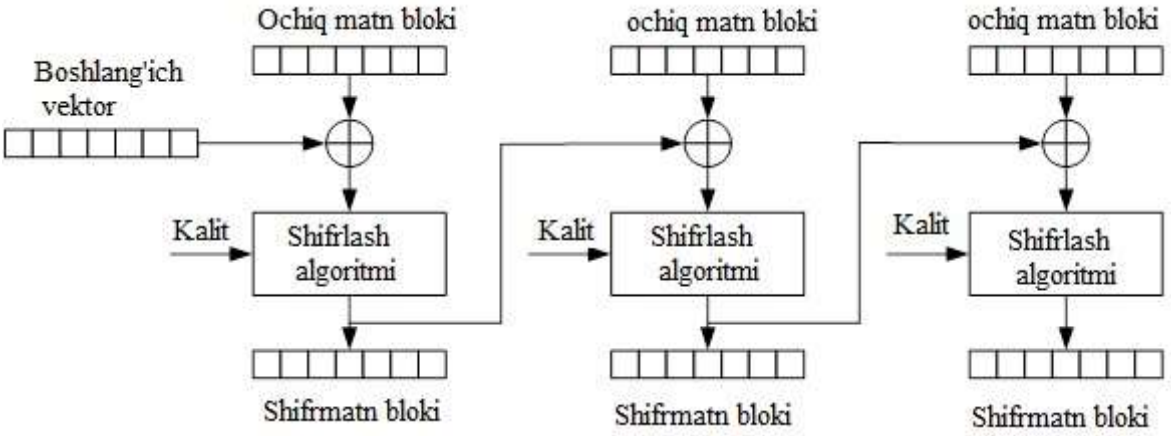
Shifrlash algoritmi uchun bardoshlik talabidan tashqari, yana bir muhim xususiyat bu – uning ishlash tezligidir. Chunki, katta hajmdagi ma’lumotlarni shifrlashda algoritmdan yuqori tezkorlik talab etiladi. Shu sababli, takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining dasturiy ta’minoti Mircosoft Visual Studio 2013 dasturlash muhitida C# dasturlash tilidan foydalanib yaratildi. Dasturiy vosita ishlatilgan shaxsiy EHM quyidagi ko‘rsatkichlarga ega: prosessor Intel® Core™ i5-4460 CPU @ 3.20GHz, 3.20 GHz, RAM 8.00 GB.

Tezlik bo‘yicha taqqoslash uchun mavjud va takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmlarining dasturiy vositalari ishlab chiqildi. Tezlik bo‘yicha taqqoslash nitijalari ishonchli bo‘lishi uchun taqqoslanayotgan shifrlash algoritmlarining raundlar soni bir xil bo‘lishi kerak. Shuning uchun yuqorida O‘z DSt 1105:2009 shifrlash algoritmini takomillashtirishda raundlar soni doimgidek “sakkizta” qilib belgilangan. Mavjud va takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmlarining dasturiy ta’minoti CBC (Cipher Block Chaining) rejimi uchun ishlab chiqilgan bo‘lib, ushbu rejimda ma’lumotni shifrlash jarayoni 4.4-rasmda aks ettirilgan. CBC rejimida ma’lumotni shifrlash bir xil ochiq matn bloklarini turli shifrmatn bloklari ko‘rinishida akslantirishga imkon beradi [113].

Har bir holat uchun quyidagi shaklda ma’lumotni shifrlash imkoniyatlari mavjud:

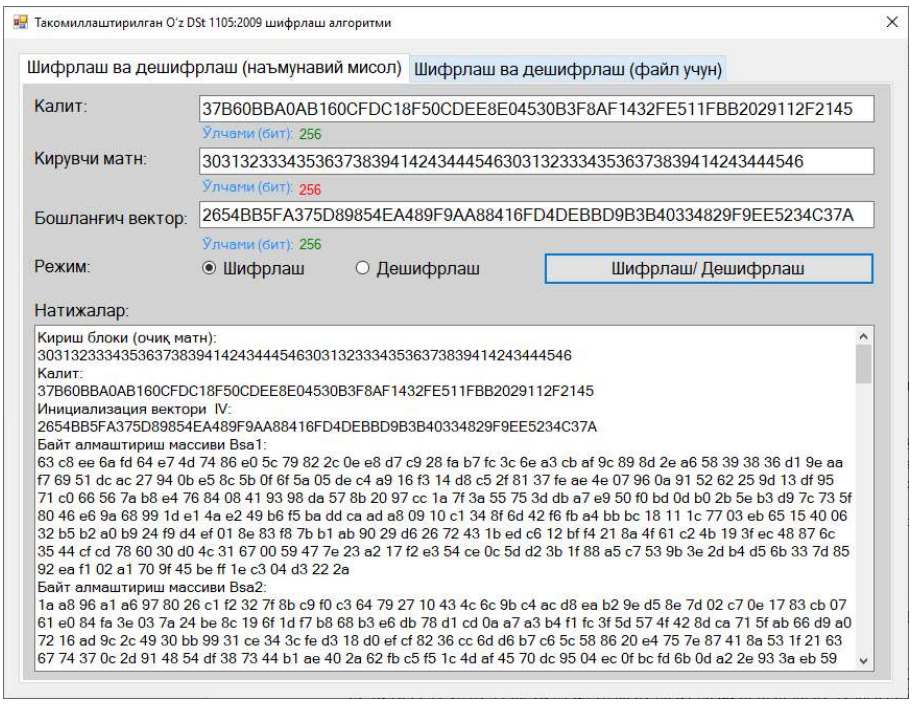
– *Ma’lumotlarni shifrlashning bosqichma-bosqich rejimi.* Ushbu ko‘rinish algoritmni tekshirish va o‘quv jarayoni uchun zarur bo‘ladi (4.5-rasm).

– *Fayllarni shifrlash rejimi.* Ma’lumotlarni shifrlashning mazkur usuli turli formatdagi va hajmdagi ma’lumotlarni shifrlash va rasshifrovkalash imkoniyatini taqdim etadi (4.6-rasm).

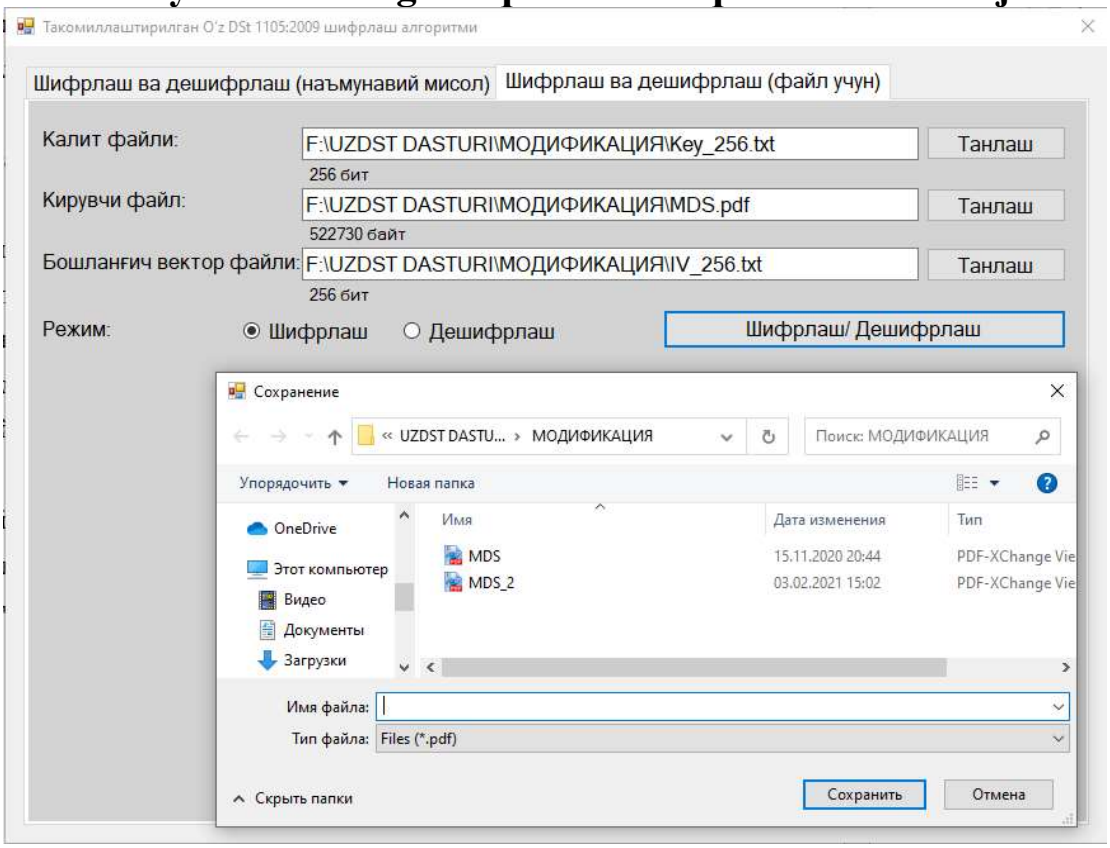


4.4-rasm. **CBC rejimida ma’lumotni shifrlash tartibi**

Dasturiy vositaning mazkur rejimi algoritmni ishlash ketma-ketligini o‘rganishda, algoritmni tahlil qilishda va o‘quv jarayonida na’munaviy misollarni ishlashda foydalaniladi. Xususan, mazkur rejimdan foydalanilganda shifrlashning har bir qadami natijalarini, hosil bo‘lgan raund kalitlarini va ishlatilgan statik parametrlarni bilish imkoniyati mavjud bo‘ladi [119]. Barcha ma’lumotlar tahlil qilishga oson bo‘lishi uchun 16 sanoq tizimida taqdim etilgan.



4.5-rasm. **Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi dasturiy vositasining bosqichma-bosqich shifrlash rejimi**



4.6-rasm. **Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi dasturiy vositasining fayllarni shifrlash rejimi**

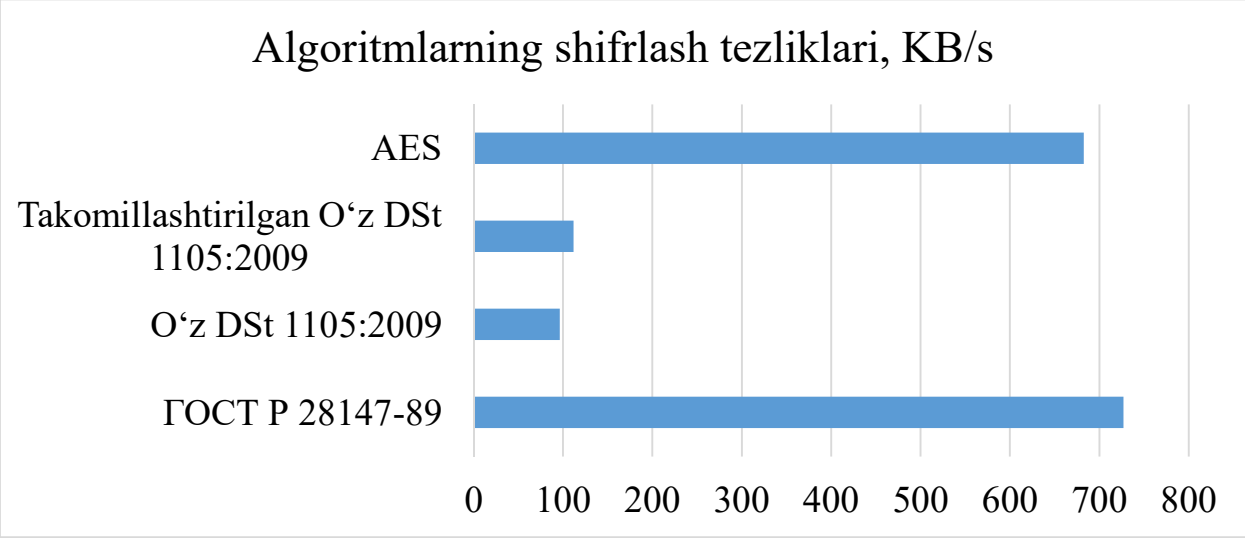
Dasturiy vositaning mazkur ko‘rinishi turli formatdagi va hajmdagi fayllarni shifrlash va rasshifrovkalash uchun ishlatiladi. Mazkur holatda foydalanuvchi shifrlanuvchi faylni, faylda saqlangan kalit va

boshlang‘ich vektorni tanlashi kerak bo‘ladi. Shifrlangan faylga qayta nom beriladi va ochiq matn fayli kengaytmasi bilan saqlanadi.

Tezlik omili bo‘yicha takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi quyidagi algoritmlar bilan taqqoslandi [111]:

– GOST 28147-89;
– O‘z DSt 1105:2009;
– AES.

Mavjud va takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi va GOST 28147-89 algoritmlari S# dasturlash tilidan foydalanib amalga oshirilgan bo‘lsa, AES shifrlash algoritmining S# dasturlash tilidagi kutubxonasidan foydalanildi. Shifrlash tezliklarini yuqori aniqlikda olish uchun NET muhiti dasturiy vositalariga mo‘ljallangan ANTS Performance Profiler dasturiy vositasidan foydalanildi [123]. Olingan tahlil natijalari 4.7-rasmda aks ettirilgan.



4.7-rasm. **Algoritmlarning ma’lumotni shifrlash tezliklari**

Yuqorida olingan natijalarni amalga oshirish tartibi, muhit, dasturlash tilining imkoniyatlariga bog‘liq bo‘lib, xususiy holat uchun olingan. Mavjud va takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmlarining ma’lumotlarni ishlashda past tezlik qayd etganining boisi esa, *Aralash()* akslantirishdagi maxsus tuzilmali diamatritsalarni ko‘paytirish amalidan foydalanilgani hisoblanadi.

Ishlab chiqilgan takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining dasturiy vositasi Toshkent shahri «SSP Maroqand» ko‘p funksiyali axborot markazi unitar korxonasida Savdo sanoat palatasining amaliy faoliyatida qo‘llanilayotgan CRM tizimida mijoz ma’lumotlarining konfidensialligini ta’minlashda test rejimida joriy etildi. Bunda, Savdo sanoat palatasining amaliy faoliyatida

qo‘llanilayotgan CRM tizimida mijoz ma’lumotlarining konfidensialligini ta’minlash jarayonida takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining dasturiy vositasi 300 Kbit/s tezlikni qayd etgan.

XULOSA

Ushbu monografiya simmetrik blokli shifrlash algoritmini takomillashtirish va kriptotahlil usullari yordamida baholashga qaratilgan bo‘lib, unda bajarilgan ishlar bo‘yicha quyidagi xulosalarni keltirish mumkin.

Zamonaviy simmetrik blokli shifr algoritmlari va ularning bardoshligini baholash usullari tahlil qilingan. Tahlil natijasida zamonaviy simmetrik blokli shifrlarning bardoshligini baholashda chiziqli, differensial, integral va algebraik kriptotahlil usullaridan keng foydalanilishi aniqlangan. Shuningdek, Amerika, Rossiya, Xitoy, Janubiy Koreya, Belorusiya, Ukraina, O‘zbekiston kabi davlatlarning shifrlash standartlariga bugungi kungacha amalga oshirilgan kriptotahlil natijalari o‘rganilgan. Ushbu ma’lumotlar simmetrik blokli shifrlash algorotmlarini zamonaviy kriptotahlil usullariga baholash imkonini beradi.

Monografiyada O‘zbekiston Respublikasining amaldagi shifrlash standarti bo‘lgan O‘z DSt 1105:2009 shifrlash algoritmi tarkibiy qismi va tuzilishi bo‘yicha tahlil qilingan. O‘z DSt 1105:2009 shifrlash algoritmidagi *BaytAlmash()* va *Aralash()* akslantirishlaridagi jadvallar, diamatritsalar seans kaliti asosida dinamik tarzda hosil qilinishi algoritmni aniq baholashga imkon bermasligi aniqlangan. Tahlillar natijasida O‘z DSt 1105:2009 shifrlash algoritmidagi $BaytAlmash()$ va $Aralash()$ akslantirishlaridagi jadvallar va diamatritsalar shifrlash va funksional kalitlar asosida dinamik tarzda hosil qilinishi algoritmni aniq baholashga imkon bermasligi aniqlangan. Shuningdek, O‘z DSt 1105:2009 shifrlash algoritmini algebraik kriptotahlil usuli yordamida baholash natijasi 2-raund kalitini topishda 2^{73} bayt xotira kerakligini ko‘rsatgan. Shuning uchun ikkinchi raunddan boshlab shakllantiriladigan tenglamalar sistemasini saqlash uchun talab qilinadigan xotira hajmini ta’minlashning imkonsizligi bois, MShA algebraik kriptotahlilga bardoshliligi aniqlangan. O‘z DSt 1105:2009 shifrlash algoritmining bardoshligi integral kriptotahlil usullari yordamida baholangan. Kriptotahlil natijasi 2-raund $BaytAlmash()$ akslantirishidan keyingi shifrlash kalitini topishda 2^{72} ta amal bajarish zarurligini ko‘rsatgan.

Ushbu monografiyada O‘z DSt 1105:2009 shifrlash algoritmini takomillashtirish va takomillashtirilgan algoritmni zamonaviy kriptotahlil usullari yordamida baholash masalasiga ham to‘xtalib o‘tilgan. Bunda statik bo‘lgan yuqori chiziqsizlik darajasiga ega S_1 va yuqori algebraik immunitetga ega S_2 jadvallar asosida O‘z DSt 1105:2009 shifrlash algoritmidagi *BaytAlmash()* akslantirishi, qat’iy lavin samaradorligini

ta’minlovchi statik 4×4 o‘lchamli maxsus tuzilmali diamatritsalar asosida $Aralash()$ akslantirishi takomillashtirilgan. Natijada algoritmga nisbatan yakuniy kriptotahlil bahosini berish imkoniyati yaratilgan. Raund kalitlarini bir-biriga bog‘liqsiz generatsiyalash algoritmi ishlab chiqildi. Ishlab chiqilgan algoritm NIST statistik testlar to‘plami asosida baholanganda 92 % tasodifiylik darajasini qayd etgan. Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi algebraik kriptotahlil usuli yordamida baholandi. Tahlil natijasida raund kalitlarini mustaqil ravishda generatsiyalash algoritmni algebraik kriptotahlilga bardoshligini
2-raunddan so‘ng ikki baravarga oshirishi aniqlangan. Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmi integral kriptotahlil usuli yordamida baholandi. Tahlil natijasida raund funksiyasi akslantirishlarini turli tartiblarda foydalanish algoritmni integral kriptotahlilga bardoshligiga ta’sir etishi aniqlandi. Takomillashtirilgan O‘z DSt 1105:2009 shifrlash algoritmining dasturiy vositasi ishlab chiqildi. Tahlil natijasida maxsus tuzilmali diamatritsalardan va S jadvallardan statik ravishda foydalanish algoritmning tezkorligini oshirishi aniqlangan.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Panasenko S.P. Algoritmы shifrovaniya. Spesialnыy spravochnik. – BXV-Peterburg, 2009.
2. D.Ye.Akbarov. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi”. Toshkent, 2008 – 394 bet.
3. Schneier B. Applied cryptography: protocols, algorithms, and source code in C. – john wiley & sons, 2007.
4. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.
5. Bellare M., Rogaway P. Introduction to modern cryptography //Ucsd Cse. – 2005. – T. 207. – S. 207.
6. Standard, NIST FIPS, Data Encryption Standard (DES). Federal Information Processing Standards Publication, 1999, 46-3.
7. Babenko L.K., Ищukova Ye.A. Analiz algoritma GOST 28147-89: poisk slabых blokov //Izvestiya Yujnogo federalnogo universiteta. Texnicheskiye nauki. – 2014. – №. 2 (151).
8. R.Beaulieu, S.Douglas, J.Smith, S.Treatman-Clark, B.Weeks, and L.Wingers, The SIMON and SPECK Families of Lightweight Block Ciphers, IACR Cryptology ePrint Archive, 2013, 404.
9. S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel, A practical attack on Keeloq, Advances in Cryptology - EUROCRYPT 2008, Springer, LNCS, 4965, 2008, pp.118.
10. FIPS P. U. B. 81: DES modes of operation, Federal Information Processing Standards Publication, December 2nd, 1980 //US Department of Commerce/National Institute of Standards and Technology.
11. Dworkin M. Recommendation for block cipher modes of operation. methods and techniques. – National Inst of Standards and Technology Gaithersburg MD Computer security Div, 2001. – №. NIST-SP-800-38A.
12. Dworkin M. J. Sp 800-38e. recommendation for block cipher modes of operation: The xts-aes mode for confidentiality on storage devices. – 2010.
13. Turner J. M. The keyed-hash message authentication code (HMAC) //Federal Information Processing Standards Publication. – 2008. – S. 198-1.

14. Dworkin M. Recommendation for cipher block modes of operation: the CMAC mode for authentication //National Institute of Standards and Technology. SP800-38B. – 2005.

15. Hall T. A., Keller S. S. The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS). – 2009.

16. Kohno T., Viega J., Whiting D. The CWC authenticated encryption (associated data) mode //ePrint Archives. – 2003.

17. Dworkin M. NIST Special Publication 800-38C: The CCM Mode for Authentication and Confidentiality //US National Institute of Standards and Technology,< http://csrc. nist. gov/publications/nistpubs/800-38C/SP800-38C.pdf. – 2007.

18. Bellare M., Rogaway P., Wagner D. A. EAX: A Conventional Authenticated-Encryption Mode //IACR Cryptology ePrint Archive. – 2003. – T. 2003. – S. 69.

19. Rogaway P. OCB mode: Parallelizable authenticated encryption. – 2000.

20. K.Inayah, B.E.Sukmono, R.Purwoko and S.Indarjani, "Insertion attack effects on standard PRNGs ANSI X9.17 and ANSI X9.31 based on statistical distance tests and entropy difference tests," 2013 International Conference on Computer, Control, Informatics and Its Applications (IC3INA), Jakarta, 2013, pp. 219-224, (DOI: 10.1109/IC3INA.2013.6819177).

21. O‘z DSt 1105:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi.// O‘zbekiston standartlashtirish, metrologiya va sertifikatlashtirish agentligi. Toshkent 2009 y.

22. Kerckhoffs A. La cryptographie militaire // Journal des sciences militaires, vol. IX. P. 5-38, Jan. 1883, (P. 161-191, Feb. 1883).

23. Knudsen L.R. Block Ciphers – Analysis, Design, Applicatons// Ph.D. dissertation, Aarhus Unversity, Nov 1994.

24. Sakiyama K., Sasaki Y., Li Y. Security of block ciphers: from algorithm design to hardware implementation. – John Wiley & Sons, 2016.

25. Kuryazov D.M., Sattarov A.B., Axmedov B.B. Blokli simmetrik shifrlash usullari bardoshliligini zamonaviy kriptotahlil usullari bilan baholash. O‘quv qo‘llanma. Toshkent “Aloqachi” 2017, 228 bet.

26. Babenko L.K., Iщukova Ye.A. Sovremennыye algoritmы blochnogo shifrovaniya i metodы ix analiza. - Moskva, «Gelios ARV», 2006. 376 bet

27. Key Lengths, Arjen K. Lenstra, The Handbook of Information Security, 06/2004.

28. Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018.

29. Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5, NIST, 05/2020.

30. Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI , 02/2014.

31. Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102-1 v2020-01, BSI, 03/2020.

32. Xasanov X.P. Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari. – Toshkent., 2008. – 200 bet.

33. Moldovyan A.A., Moldovyan N.A., Yeremeyev M.A Kriptografiya. Ot primitivov k sintezu algoritmov. – Sankt-Peterburg, Izd. «BXV-Peterburg», 2004. – 446 s.

34. Fomichev V.M.. Diskretnaya matematika i kriptologiya. – Moskva, “DIALOG-MIFI”, 2003. – 400 s.

35. Sattorov A.B. Gost 28147-89 algoritmi bardoshligini chiziqli-differensial va algebraik kriptotahlil usullari yordamida baholash va bardoshligi yuqori bo‘lgan shifr yaratish. Fizika-matematika fanlari bo‘yicha falsafa doktori (PhD) ilmiy darajasini olish uchun tayyorlangan dissertatsiya ishi. 2019 yil.

36. Xasanov X.P., Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari – Toshkent, 2008 – 208 bet.

37. Valea E. et al. Stream vs block ciphers for scan encryption //Microelectronics Journal. – 2019. – T. 86. – S. 65-76. (Scopus, IF=1.405, DOI :10.1016/j.mejo.2019.02.019).

38. Hatzivasilis G. et al. A review of lightweight block ciphers //Journal of Cryptographic Engineering. – 2018. – T. 8. – №. 2. – S. 141-184. (IF=1.61, DOI:10.1007/s13389-017-0160-y)

39. Standard A.E. Federal information processing standards publication 197 //FIPS PUB. – 2001. – S. 46-3.

40. J. Daemen, M. Peeters, G. Van Assche, and V. Rijmen, The NOEKEON Block Cipher, 2000, pp.1-30, http://gro.noekeon.org/.

41. F.X.Standaert, G.Piret, G.Rouvroy, J.Quisquater, and J.D.Legat, ICEBERG: An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware, Fast Software Encryption (FSE 2004), Springer, LNCS, 3017, 2004, pp.279-298.(DOI:10.1007/978-3-540-25937-4_18)

42. C.H. Lim and T. Korkishko, mCrypton - A lightweight block cipher for security of low-cost RFID tags and Sensors, Information Security Applications, Springer, LNCS, 3786, 2006, pp.243-258.(DOI:10.1007/11604938)

43. A.Bogdanov, L.R.Knudsen, G.Leander, C.Paar, and A.Poschmann, PRESENT: An Ultra-Lightweight Block Cipher, Cryptographic Hardware and Embedded Systems, CHES 2007, Springer, LNCS, 4727, 2007, pp.450-466. (DOI:https://doi.org/10.1007/978-3-540-74735-2_31)

44. K.Aoki, T. Ichikawa, M.Kanda, M.Matsui, S.Moriai, J.Nakajima, and T.Tokita, Camellia: a 128-bit block cipher suitable for multiple platforms design and analysis, Selected Areas in Cryptography (SAC'01), Springer, LNCS, 2001, pp.39-56.

45. F.X.Standaert, G.Piret, N.Gershenfeld, and J.Quisquater, SEA: A Scalable Encryption Algorithm for small embedded applications, Smart Card Research and Advanced Applications, Springer, LNCS, 3928, 2006, pp.222-236. (DOI:10.1007/11733447_16)

46. T.Shirai, K.Shibutani, T. Akishita, S.Moriai, and T.Iwata, The 128-bit blockcipher CLEFIA (extended abstract), Fast Software Encryption (FSE 2007), Springer, LNCS, 4593, 2007, pp. 181-195. (DOI: 10.1007/978-3-540-74619-5_12)

47. X. Lai and J.L.Massey, A proposal for a new block encryption standard, Advances in Cryptology EUROCRYPT '90, Springer, LNCS, 473, 1991, pp.389-404.(DOI: 10.1007/3-540-46877-3_35)

48. D. Hong et al., HIGHT: A New Block Cipher Suitable for Low-Resource Device. Cryptographic Hardware and Embedded Systems, CHES 2006, Springer, LNCS, 4249, 2006, pp.46-59. (DOI: 10.1007/11894063_4)

49. D. Hong, J.-K. Lee, D.-C. Kim, D. Kwon, K. H. Ryu, and D.-G. Lee, LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors, International Workshop on Information Security Applications (WISA 2013), Springer, LNCS, 8267, 2014, pp. 3-27. (DOI: 10.1007/978-3-319-12778-1_15)

50. C. D.E.Canniere, O.Dunkelman, and M.Knezevic, KATAN & KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers, Cryptographic Hardware and Embedded Systems, CHES 2009, Springer, LNCS, 5747, 2009, pp.272-288. (DOI: 10.1007/978-3-642-04138-9_20)

51. D.Engels, M.O.Saarinen, P.Schweitzer, and E.M.Smith, The Hummingbird-2 Lightweight Authenticated Encryption Algorithm, RFID Security and Privacy, Springer, LNCS, 7055, 2011, pp.19-31. (DOI: 10.1007/978-3-642-25286-0_2)

52. G.Bansod, N.Raval, and N.Pisharoty, Implementation of a New Lightweight Encryption Design for Embedded Security, IEEE Transactions on Information Forensics and Security, IEEE, vol. 10, issue 1, 2014, pp. 142-151. (Scopus, DOI: 10.1109/TIFS.2014.2365734)

53. Bellare M., Kilian J., Rogaway P. The security of the cipher block chaining message authentication code //Journal of Computer and System Sciences. – 2000. – Т. 61. – №. 3. – S. 362-399. (Scopus , IF=1.194, DOI: 10.1006/jcss.1999.1694)

54. Kohno T., Viega J., Whiting D. CWC: A high-performance conventional authenticated encryption mode //International Workshop on Fast Software Encryption. – Springer, Berlin, Heidelberg, 2004. – S. 408-426. (DOI: 10.1007/978-3-540-25937-4_26)

55. Jutla C.S. Encryption modes with almost free message integrity //International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 2001. – S. 529-544. (DOI:https://doi.org/10.1007/3-540-44987-6_32)

56. Kelsey J., Schneier B., Ferguson N. Yarrow-160: Notes on the design and analysis of the yarrow cryptographic pseudorandom number generator //International Workshop on Selected Areas in Cryptography. – Springer, Berlin, Heidelberg, 1999. – S. 13-33. (DOI:10.1007/3-540-46513-8_2)

57. Dodis Y. et al. How to eat your entropy and have it too: Optimal recovery strategies for compromised RNGs //Algorithmica. – 2017. – Т. 79. – №. 4. – S. 1196-1232. (DOI:10.1007/978-3-662-44381-1_3).

58. El-Emam E. et al. An Authentication Protocol Based on Kerberos 5 //IJ Network Security. – 2011. – Т. 12. – №. 3. – S. 159-170.

59. Avdoshin S.M., Savelyeva A.A. Kriptoanaliz: sovremennoye sostoyaniye i perspektivы razvitiya //Informasionnыye texnologii. – 2007. – №. S3. – S. 1-32.

60. Matsui M. Linear cryptanalysis method for DES cipher //Workshop on the Theory and Application of of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 1993. – S. 386-397. (DOI: 10.1007/3-540-48285-7_33).

61. 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. (Scopus, IF=1.17, DOI: 10.1007/3-540-45661-9_9).

62. Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal Of Cryptology, vol. 14, p. 255-293, 2001. (IF=1.021, DOI: 10.1007/s00145-001-0009-4).

63. Junod P. On the complexity of Matsui’s attack //International Workshop on Selected Areas in Cryptography. – Springer, Berlin, Heidelberg, 2001. – S. 199-211.

64. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems //Journal of CRYPTOLOGY. – 1991. – Т. 4. – №. 1. – S. 3-72. (IF=1.021, DOI: 10.1007/3-540-38424-3_1).

65. Moriai S., Yin Y.L. Cryptanalysis of Twofish (II). – 2000. (DOI: 10.1007/978-3-642-38519-3_2).

66. Ma C., Chandy J. A., Shi Z. Algebraic Side-Channel Attack on Twofish //J. Internet Serv. Inf. Secur. – 2017. – Т. 7. – №. 2. – S. 32-43

67. Wu W., Feng D. Differential-Linear Cryptanalysis of Camellia //Progress on Cryptography. – Springer, Boston, MA, 2004. – S. 173-180. (DOI: 10.1007/1-4020-7987-7_2)

68. Jia K., Wang N. Impossible Differential Cryptanalysis of 14-Round Camellia-192 //Australasian Conference on Information Security and Privacy. – Springer, Cham, 2016. – S. 363-378. (DOI:10.1007/1-4020-7987-7_2).

69. Liu Y. et al. Improved results on impossible differential cryptanalysis of reduced-round Camellia-192/256 //Journal of Systems and Software. – 2012. – Т. 85. – №. 11. – S. 2451-2458. (Scopus, IF=1.352, DOI:10.1016/j.jss.2012.05.051)

70. Duo L., Li C., Feng K. Square like attack on Camellia //International Conference on Information and Communications Security. – Springer, Berlin, Heidelberg, 2007. – S. 269-283. (DOI:10.1007/978-3-540-77048-0_21)

71. Sakamura, Kenichi, Wang Xiao Dong, and Hirofumi Ishikawa. "A study on the linear cryptanalysis of AES cipher." Journal of the Faculty

of Environmental Science and Technology, Okayama University Vo1.9, No.1, pp.19-26, February 2004.P.19-26.

72. Lu J. et al. New impossible differential attacks on AES //International Conference on Cryptology in India. – Springer, Berlin, Heidelberg, 2008. – S. 279-293. (DOI: 10.1007/978-3-540-89754-5_22)

73. N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D.Wagner, and D.Whiting. Improved cryptanalysis of Rijndael. In FSE 2000, volume 1978 of LNCS, pages 213–230. Springer-Verlag, f2001. (DOI: 10.1007/3-540-44706-7_15).

74. Biryukov A., Khovratovich D., Nikolić I. Distinguisher and related-key attack on the full AES-256 //Annual International Cryptology Conference. – Springer, Berlin, Heidelberg, 2009. – S. 231-249. (DOI: 10.1007/978-3-642-03356-8_14)

75. Tolomanenko Ye.A. Differensialnыy analiz trex raundov shifra" Kuznechik" //Dokladы Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. – 2018. – T. 21. – №. 2.

76. AlTawy R., Youssef A. M. A meet in the middle attack on reduced round Kuznyechik //IEICE transactions on Fundamentals of Electronics, Communications and Computer Sciences. – 2015. – T. 98. – №. 10. – S. 2194-2198.

77. Liu Y. et al. New Linear Cryptanalysis of Chinese Commercial Block Cipher Standard SM4 //Security and Communication Networks. – 2017. – T. 2017. (DOI:10.1155/2017/1461520)

78. Zhang J., Wu W., Zheng Y. Security of SM4 against (related-key) differential cryptanalysis //International Conference on Information Security Practice and Experience. – Springer, Cham, 2016. – S. 65-78.

79. Abdelkhalek A., Tolba M., Youssef A. M. Improved Linear Cryptanalysis of Round-Reduced ARIA //International Conference on Information Security. – Springer, Cham, 2016. – S. 18-34. (DOI:10.1007/978-3-319-45871-7_2)

80. Wu W., Zhang W., Feng D. Impossible Differential Cryptanalysis of ARIA and Camellia //IACR Cryptol. ePrint Arch. – 2006. – T. 2006. – S. 350.

81. Yi W., Ren J., Chen S. Multidimensional Differential-Linear Cryptanalysis of ARIA Block Cipher //ETRI Journal. – 2017. – T. 39. – №. 1. – S. 108-115. (Scopus, IF=1.094, DOI: 10.4218/etrij.17.0116.0544)

82. Li P., Sun B., Li C. Integral cryptanalysis of ARIA //International Conference on Information Security and Cryptology. –

Springer, Berlin, Heidelberg, 2009. – S. 1-14. (DOI: 10.1007/978-3-642-16342-5_1)

83. ElSheikh M., Abdelkhalek A., Youssef A.M. On MILP-Based Automatic Search for Differential Trails Through Modular Additions with Application to Bel-T //International Conference on Cryptology in Africa. – Springer, Cham, 2019. – S. 273-296. (DOI: 10.1007/978-3-030-23696-0_14)

84. ElSheikh M., Tolba M., Youssef A.M. Integral Attacks on Round-Reduced Bel-T-256 //International Conference on Selected Areas in Cryptography. – Springer, Cham, 2018. – S. 73-91. (DOI: 10.1007/978-3-030-10970-7_4).

85. Abdelkhalek A., Tolba M., Youssef A.M. Related-key differential attack on round-reduced Bel-T-256 //IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. – 2018. – T. 101. – №. 5. – S. 859-862. (IF=0.47, DOI:10.1587/transfun.E101.A.859).

86. Ruzhentsev V., Sokurenko V., Ulyanchenko Y. Analysis of probabilities of differentials for block cipher Kalyna" (DSTU 7624: 2014) //Vostochno-Yevropeyskiy jurnal peredovых texnologiy. – 2018. – №. 4 (9). – S. 14-19. (Csopus, IF=1.09, DOI:10.15587/1729-4061.2018.139682).

87. AlTawy R., Abdelkhalek A., Youssef A.M. A meet-in-the-middle attack on reduced-round Kalyna-b/2b //IEICE transactions on Information and Systems. – 2016. – T. 99. – №. 4. – S. 1246-1250. (IF=0.545, DOI:10.1587/transinf.2015EDL8174).

88. Fayzievich, A.B., Turakulovich, K.Z., Menglimuratovich, A.O., & Mardanakulovich, B. I. (2019, November). Analysis of algebraic properties of transformation of O'z DSt 1105:2009 algorithm. In 2019 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-3). IEEE. (Scopus, **DOI:** 10.1109/ICISCT47635.2019.9011917).

89. S.K.Langford, M.E.Hellman, Differential-Linear Cryptanalysis, in Y. Desmedt, editor, CRYPTO. LNCS, vol. 839 (Springer, 1994), pp. 17–25

90. Courtois N.T., Bard G.V. Algebraic cryptanalysis of the data encryption standard //IMA International Conference on Cryptography and Coding. – Springer, Berlin, Heidelberg, 2007. – S. 152-169.

91. Harris N. Algebraic Cryptanalysis of AES: An Overview. – 2004.

92. Knudsen L.R., Robshaw M.J.B. Brute force attacks //The Block Cipher Companion. – Springer, Berlin, Heidelberg, 2011. – S. 95-108. (DOI:10.1007/978-3-642-17342-4_5)

93. Schneier B. et al. The Twofish team's final comments on AES Selection //AES round. – 2000. – T. 2. – №. 1. – S. 1-13.

94. Allanov O. AES konkursi finalchilariga qaratilgan kriptotahlillar natijalari. Muhammad al-xorazmiy avlodlari. Ilmiy-amaliy va axborot-tahliliy jurnali 4(10)/2019 7-10 bet

95. Snell D.L. Advanced encryption standard (AES) hardware cryptographic engine : pat. 7295671 SShA. – 2007.

96. Agiyevich S.V. i dr. Algoritm blochnogo shifrovaniya BelT. – 2002.

97. Oliynykov R. et al. Results of Ukrainian national public cryptographic competition //Tatra Mountains Mathematical Publications. – 2010. – T. 47. – №. 1. – S. 99-113.

98. Rodinko M., Oliynykov R., Gorbenko Y. Optimization of the high nonlinear S-boxes generation method //Tatra Mountains Mathematical Publications. – 2017. – T. 70. – №. 1. – S. 93-105. (IF=0.5, DOI:10.1515/tmmp-2017-0020)

99. KAZYMYROV, O.V.: Methods and Techniques of Generation of Nonlinear Substitutions for Symmetric Encryption Algorithms. The thesis for the scholarly degree of candidate of technical sciences, speciality 05.13.21—Information security systems, Kharkiv National University of Radioelectronics, Kharkiv, 2014. (In Russian)

100. Mersaid A., Gulom T. The encryption algorithm AES-RFWKIDEA32-1 based on network RFWKIDEA32-1 //International Journal of Electronics and Information Engineering. – 2016. – T. 4. – №. 1. – S. 1-11.

101. Khudoykulov Z.T.,Islomov Sh.Z., Allanov O., Mardiyev U.R. A practical implementation of fingerprint based fuzzy commitment scheme. European Science Review. -Austria, Vienna- 2018. № (5-6). -P. 105-110. (IF=1.44).

102. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O, Boykuziyev I.M. A Novel Secure RNG Based On Three Entropy Sources. International Journal of Advanced Science and Technology. Vol. 29, No. 5, (2020), P. 12397-12412. (IF=0.41).

103. Abduraximov B.F., Allanov O., Shonazarov S.K. Teoreticheskiy analiz ustoychivosti sovremennых algoritmov blochnogo

shifrovaniya. «VЫISSShAYaShKOLA» Nauchno-prakticheskiyjurnal. №8, Ufa - 2018 g., -S. 69-72.

104. Abduraximov B.F. Primkulov B.Sh. Xudoyqulov Z.T., Allanov O. Simmetrik blokli shifrlash usullarining tahlili. “ToshDTU XABARLARI” jurnali, №2(99) 2017 y. -B. 30-35.

105. Irgasheva D.Ya., Xudoyqulov Z. T., Islomov Sh.Z., Allanov O. Barmoq iziga asoslangan autentifikatsiyalash usullarini tahlili. “Axborot kommunikatsiyalar: Tarmoqlar, Texnologiyalar, Yechimlar.” Har chorak ilmiy-texnik jurnal. № 4(48)/2018. –B. 45-54.

106. Xudoyqulov Z. T., Allanov O., Xolimtayeva I. U. Zamonaviy xesh funksiyalarining xavfsizlik va tezlik xususiyatlari asosidagi tahlili. “Axborot kommunikatsiyalar: Tarmoqlar, Texnologiyalar, Yechimlar.” Har chorak ilmiy-texnik jurnal. № 2(46)/2018. –B. 45-53.

107. Abduraximov B.F., Allanov O., Xudoyqulov Z. T., Islomov Sh.Z., DES algoritmining chiziqli kriptotahlili. “Axborotkommunikasiyalar: Tarmoqlar, Texnologiyalar, Yechimlar.” Har chorak ilmiy-texnik jurnal. № 3(51)/2019. –B. 56-61.

108. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O., Boykuziyev I.M. Algebraic Cryptanalysis of O‘z DSt 1105:2009 Encryption Algorithm. International Conference on Information Science and Communications Technologies (ICISCT). November 2020. 6p. (Csopus, **DOI:** 10.1109/ICISCT50599.2020.9351469).

109. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O., Boykuziyev I.M. Differential Collisions in SHA-1, International Conference on Information Science and Communications Technologies (ICISCT). November 2020. 5p. (Scopus, **DOI:** 10.1109/ICISCT50599.2020.9351441).

110. Abduraximov B.F., Allanov O., Xamidov Sh.J. Issledovaniye standarta shifrovaniya respubliki uzbekistan. Abstracts of III International Scientific and Practical Conferenc. London, United Kingdom -2020. –P. 196-176.

111. Abduraximov B.F., Allanov O., Yo‘ldoshov M. X. Zamonaviy blokli shifrlash algoritmlarining tezliklarining tahlili. International conference on importance of information-communication technologies in innovative development of sectors of economy. Tashkent -2018. -B. 421-424.

112. Xudoyqulov Z.T. Allanov O. Axborot xavfsizligini xavfsizligini ta’minlashda assimetrik shifrlash usullarining o‘rni. Respublikanskiy seminar: «Informasionnaya bezopasnost v sfere svyazi i

informatizasii. Problemы i puti ix resheniya». Sbornik tezisov i dokladov. Tashkent – 2016 g. - B. 26-28.

113. Allanov O. Unionpay xalqaro to‘lov kartalarining afzalliklari. Respublikanskiy seminar:«Informasionnaya bezopasnost v sfere svyazi i informatizasii. Problemы i puti ix resheniya». Sbornik tezisov i dokladov. Tashkent – 2016 g. - B. 81-82.

114. Allanov O. Tarmoq xavfsizligini ta’minlash usuli. “Iqtisodiyotning real tarmoqlarini innovatsion rivojlanishida axborot-kommunikatsiya texnologiyalarining ahamiyati” Respublika ilmiy-texnik anjumanining ma’ruzalar to‘plami. 3-qism. TOShKENT-2017 y. – B. 116-118.

115. Allanov O. Kriptografik xesh funksiyalarning axborot xavfsizligini ta’minlashdagi o‘rni. Iqtisodiyotning real tarmoqlarini innovatsion rivojlanishida axborot-kommunikatsiya texnologiyalarining ahamiyati” Respublika ilmiy-texnik anjumanining ma’ruzalar to‘plami. 3-qism. Toshkent-2017 y. –B. 116-118.

116. Allanov O., Asrorov A., Sodiqova D. Axborot konfidensialligini himoyalash usullari. Ta’lim, fan va ishlab chiqarish integratsiyasida innovatsion texnologiyalarni qo‘llash-mamlakat taraqqiyotining muhim omili” mavzusidagi XV respublika ilmiy-amaliy konferensiyasi materiallari, II qism. Samarqand-2018. –B. 241-243.

117. Abduraximov B.F., Allanov O., Karimov A.A. Kriptotahlil usullarining istiqbollari. “Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari” Respublika miqyosidagi ilmiy-texnik konferensiya. Toshkent-2018 y., -B. 13-16.

118. Abduraximov B., Allanov O., Djurabayev A. Kriptografik tizimlar tahlili. “Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari” Respublika miqyosidagi ilmiy-texnik konferensiya. Toshkent-2019 y., -B. 68-71.

119. Abduraximov B., Allanov O., Djurabayev A. Kalit va ma’lumotlarning inkapsulyatsiyasi mexanizmlariga asoslangan kombinatorli shifrlash algoritmlari. “Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari” Respublika miqyosidagi ilmiy-texnik konferensiya. Toshkent-2019 y. -B. 76-78.

120. BlueKrypt[sayt]:https://www.keylength.com/en/compare/#Biblio7(murojaat vaqti: 04.03.2021 y).

121. SM4 Block Cipher Algorithm [sayt]: http://www.codeofchina.com/standard/GMT0002-2012.html(murojaat vaqti:05.03.2021 y.)

122. O‘z DSt 1105:2009 [sayt’: http://stt.unicon.uz/ru/doc/2207 (murojaat vaqti:05.03.2021 y.)

123. Boost the performance of your applications with .NET profiling[sayt]:https://www.red-gate.com/products/dotnetdevelopment/ants-performance-profiler/ (murojaat vaqti: 05.03.2021 y.)

124. M.M.Aripov, D.M. Kuryazov. Analiz stoykosti S-bloka standarta algoritma O‘z DSt 1105:2009 //Sbornik materialov mejdunarodnoy konferensiy, Astana 12-13 sentyabrya 2013 goda, str. 109-116.

ILOVALAR

1-ilova

Teskarisigaega affinmatritsanihosilqilishdagi$n$ningqiymatlari

$n \in$ {1, 2, 4, 7, 8, 11, 13, 14, 16, 19, 21, 22, 23, 25, 26, 28, 29, 31, 32, 35, 37, 38, 41, 42, 43, 44, 46, 47, 49, 50, 52, 53, 55, 56, 58, 59, 61, 62, 64, 67, 69, 70, 71, 73, 74, 76, 77, 79, 81, 82, 83, 84, 86, 87, 88, 89, 91, 92, 93, 94, 97, 98, 100, 101, 103, 104, 106, 107, 109, 110, 112, 113, 115, 116, 117, 118, 121, 122, 124, 127, 128, 131, 133, 134, 137, 138, 139, 140, 142, 143, 145, 146, 148, 149, 151, 152, 154, 155, 157, 158, 161, 162, 163, 164, 166, 167, 168, 169, 171, 172, 173, 174, 176, 178, 179, 181, 182, 184, 185, 186, 188, 191, 193, 194, 196, 197, 199, 200, 202, 203, 205, 206, 208, 209, 211, 212, 213, 214, 217, 218, 220, 223, 224, 226, 227, 229, 230, 232, 233, 234, 236, 239, 241, 242, 244, 247, 248, 251, 253, 254}

2-ilova

O’zgarmasnuqtalarmavjudbo’lgan S jadvallarga misol

$S(n = 53) =$ {99, 86, 177, 255, 66, 23, 45, 210, 187, **12**, 89, 180, **12**, 39, 243, 63, 15, 216, 156, 216, 54, 51, 136, 95, 212, 180, 9, 201, 99, 46, 5, 102, 85, 159, 190, 116, 156, 102, 246, 40, 129, 160, 3, 209, 150, 250, 53, 222, 184, 207, 192, 245, 30, 10, 54, 68, 43, 119, 197, 170, 80, 250, 225, 172, 120, 86, 29, 3, 141, 163, 160, 20, 212, 92, 169, 111, 169, 36, 142, 255, 90, 0, 130, 119, 83, 17, 114, 46, 153, 129, 175, 65, 72, 111, 189, 187, 142, 106, 125, 184, 78, 225, 40, 113, 149, 165, 159, 197, 201, 245, 240, 96, 71, 135, 33, 24, 48, 237, 207, 235, 178, 219, 231, 221, 106, 130, 204, 147, 166, 204, 249, 249, 20, 132, 27, 195, 92, 189, 75, 123, 202, 9, 144, 139, 240, 75, 252, 192, 78, 58, 45, 177, 6, 228, 136, 80, 221, 154, 101, 105, 183, 166, 210, 235, 219, 165, 105, 135, 123, 29, 90, 237, 163, 153, 141, 226, 30, 18, 18, 48, 5, 58, 114, 238, 190, 238, 101, 222, 68, 113, 71, 246, 149, 108, 231, 0, 36, 51, 198, 65, 195, 78, 34, 183, 198, 60, 34, 172, 24, 232, 72, 215, 85, 17, 120, 209, 126, 15, 96, 6, 226, 232, 170, 126, 57, 43, 89, 228, 10, 116, 150, 23, 202, 57, 108, 77, 53, 125, 39, 83, 139, 154, 63, 66, 33, 144, 60, 132, 175, 215, 147, 95, 252, 243, 27, 77}

$S(n = 98) =$ {99, **1**, 170, 237, 127, 25, 36, 142, 149, 199, 94, 202, 56, 228, 109, 229, 24, 177, 201, 78, 5, 154, 183, 225, 206, 53, 88, 80, 156, 251, 216, 252, 222, 233, 10, 194, 54, 3, 13, 187, 168, 180, 103, 174, 9, 114, 218, 14, 181, 16, 176, 45, 6, 120, 250, 63, 100, 226, 47, 139, 190, 141, 172, 52, 189, 254, 38, 152, 215, 107, 75, 198, 49, 62, 171, 227, 84, 196, 247, 18, 126, 71, 136, 29, 97, 166, 125, 4, 86, 87, 235, 160, 191, 28, 213, 106, 8, 131, 34, 74, 138, 83, 68, 93, 41, 212, 22, 208, 175, 210, 77, 188, 224, 23, 91, 185, 69, 211, 239, 147, 117, 145, 236, 46, 124, 119, 48, 150, 244, 207, 173, 82, 57, 55, 102, 144, 193, 42, 159, 157, 143, 167, 73, 151, 178, 96, 205, 79, 255, 133, 219, 85, 248, 204, 72, 65, 209, 118, 35, 163, 21, 11, 113, 108, 110, 43, 92, 232, 98, 217, 129, 44, 148, 169, 40, 115, 249, 134, 121, 186, 39, 122, 130, 243, 245, 12, 220, 241, 192, 162, 31, 242, 214, 60, 19, 184, 59, 101, 15, 95, 111, 0, 123, 234, 240, 58, 132, 203, 70, 76, 64, 17, 33, 89, 66, 81, 253, 231, 67, 7, 140, 179, 116, 2, 90, 155, 161, 51, 135, 61, 246, 230, 112, 165, 195, 32, 37, 221, 27, 158, 104, 137, 26, 128, 164, 182, 197, 200, 20, 238, 105, 30, 50, 146, 153, 223}

3-ilova

O‘zgarmasnuqtalarda S jadvallaruchun$n$qiymatlari

$n \in$ {2, 4, 7, 8, 13, 14, 16, 21, 22, 23, 25, 28, 29, 32, 35, 37, 38, 41, 42, 43, 46, 47, 53, 58, 59, 67, 73, 76, 77, 79, 81, 82, 83, 86, 88, 89, 91, 92, 93, 97, 98, 110, 112, 113, 115, 116, 118, 122, 124, 127, 128, 131, 133, 137, 139, 140, 142, 143, 149, 151, 154, 157, 158, 162, 163, 164, 167, 168, 169, 172, 173, 174, 176, 178, 179, 182, 188, 191, 193, 194, 197, 200, 202, 203, 208, 209, 212, 214, 217, 218, 220, 226, 227, 229, 230, 232, 233, 234, 236, 239, 241, 242, 247, 251, 253, 254}

4-ilova

Takrorlanuvchichiqishqiymatlarigaega S jadvallarga misol

$S(n = 71) = \{$**99**, **36**, **160**, 30, 226, 72, 221, 34, 195, 92, 246, 17, 92, 190, 163, 197, 51, 65, 156, 65, 201, 120, 90, 40, 252, 17, 237, 54, **99**, 178, 80, 210, 75, 243, 114, 202, 156, 210, 18, 108, 86, 215, 142, 77, 255, 175, 166, 159, 172, 232, 58, 125, 68, 130, 201, 60, 3, 165, 139, 180, 250, 175, 187, 106, 119, **36**, 43, 142, 235, 184, 215, 39, 252, 71, 219, 222, 219, 209, 132, 30, 153, 225, 57, 165, 149, 150, 20, 178, 45, 86, 5, 141, 129, 222, 29, 195, 132, 111, 198, 172, 207, 187, 108, 123, 144, 102, 243, 139, 54, 125, 204, 12, 83, 136, 96, 154, 23, 6, 232, 216, 207, 46, 101, 240, 111, 57, 135, 78, 9, 135, 192, 192, 39, 231, 245, 85, 71, 29, 238, 24, 89, 237, 33, 53, 204, 238, 113, 58, 95, 116, 221, **160**, 63, 10, 90, 250, 240, 66, 189, 0, 126, 9, 34, 216, 46, 102, 0, 136, 24, 43, 153, 6, 184, 45, 235, 212, 68, 249, 249, 23, 80, 116, 20, 105, 114, 105, 189, 159, 60, 123, 83, 18, 144, 177, 101, 225, 209, 120, 228, 141, 85, 95, 15, 126, 228, 170, 15, 106, 154, 183, 129, 147, 75, 150, 119, 77, 169, 51, 12, 63, 212, 183, 180, 169, 27, 3, 246, 10, 130, 202, 255, 72, 89, 27, 177, 48, 166, 198, 190, 149, 53, 66, 197, 226, 96, 33, 170, 231, 5, 147, 78, 40, 113, 163, 245, 48}

$S(n = 184) = \{$**99**, **219**, 160, 30, 29, 183, 221, 34, 195, 163, 9, 17, 163, 190, 92, 58, 51, 65, 156, 65, 201, 120, 90, 40, 3, 17, 18, 54, **99**, 77, 80, 210, 75, 12, 114, 53, 156, 210, 237, 108, 169, 215, 113, 178, 255, 175, 89, 96, 83, 23, 197, 125, 68, 130, 201, 60, 252, 165, 116, 180, 250, 175, 187, 149, 119, **219**, 212, 113, 235, 71, 215, 39, 3, 184, 36, 33, 36, 46, 123, 30, 153, 225, 57, 165, 106, 150, 20, 77, 45, 169, 5, 141, 126, 33, 226, 195, 123, 144, 198, 83, 48, 187, 108, 132, 111, 102, 12, 116, 54, 125, 204, 243, 172, 136, 159, 101, 232, 249, 23, 216, 48, 209, 154, 240, 144, 57, 135, 78, 246, 135, 63, 63, 39, 24, 245, 85, 184, 226, 238, 231, 166, 18, 222, 202, 204, 238, 142, 197, 95, 139, 221, 160, 192, 10, 90, 250, 240, 189, 66, 0, 129, 246, 34, 216, 209, 102, 0, 136, 231, 212, 153, 249, 71, 45, 235, 43, 68, 6, 6, 232, 80, 139, 20, 105, 114, 105, 66, 96, 60, 132, 172, 237, 111, 177, 154, 225, 46, 120, 228, 141, 85, 95, 15, 129, 228, 170, 15, 149, 101, 72, 126, 147, 75, 150, 119, 178, 86, 51, 243, 192, 43, 72, 180, 86, 27, 252, 9, 10, 130, 53, 255, 183, 166, 27, 177, 207, 89, 198, 190, 106, 202, 189, 58, 29, 159, 222, 170, 24, 5, 147, 78, 40, 142, 92, 245, 207}

5-ilova

Tasodifiyhosilqilingandiamatritsalarjuftlari (K_1 vaK_2) uchunkirishdagibirbitningo'zgarishiniraundlardata'siretganbitlarsoni

№	Raundlarsoni								№	Raundlarsoni							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1.	13	85	131	113	124	132	114	133	**2.**	12	49	98	126	130	128	129	123
3.	22	96	129	124	122	136	139	128	**4.**	13	61	128	127	124	134	119	122
5.	19	68	137	118	127	134	122	106	**6.**	22	104	125	127	119	124	134	116
7.	4	30	78	148	125	119	130	129	**8.**	14	47	93	133	125	131	127	139
9.	9	59	128	118	135	101	126	132	**10.**	14	51	101	134	131	134	123	127
11.	19	83	124	131	132	123	136	132	**12.**	20	93	134	133	125	120	121	116
13.	7	35	98	124	132	135	125	132	**14.**	23	92	126	110	119	131	120	128
15.	6	20	99	132	131	127	135	136	**16.**	21	103	131	116	138	135	135	138
17.	19	95	130	133	132	137	141	133	**18.**	12	38	95	137	140	119	126	133
19.	16	63	134	122	129	129	118	130	**20.**	7	22	108	122	118	133	128	124
21.	9	73	132	132	117	140	138	125	**22.**	4	37	105	124	133	134	116	132
23.	10	33	112	132	135	151	129	125	**24.**	8	37	110	122	112	123	120	141
25.	16	69	121	105	133	136	126	125	**26.**	7	61	130	126	121	128	136	127
27.	17	92	134	129	138	123	131	121	**28.**	22	76	132	122	135	130	121	124
29.	14	73	145	134	129	127	126	142	**30.**	8	43	118	139	129	136	129	125
31.	14	81	104	122	125	122	120	112	**32.**	12	42	120	128	118	143	127	142
33.	15	88	125	133	130	116	135	127	**34.**	12	67	137	128	135	134	132	128
35.	9	40	117	135	141	135	130	119	**36.**	15	48	92	130	150	141	118	115
37.	18	104	135	120	142	134	135	118	**38.**	14	55	106	138	121	135	122	138
39.	5	22	101	127	135	133	129	121	**40.**	23	92	124	126	128	144	125	131
41.	21	70	117	123	122	146	125	110	**42.**	12	90	134	112	123	127	133	135
43.	21	77	142	132	137	136	142	114	**44.**	19	73	115	138	133	133	128	130
45.	13	88	115	114	139	124	119	125	**46.**	19	89	121	138	133	128	131	126
47.	12	43	96	129	130	122	121	137	**48.**	19	99	116	124	128	132	130	120
49.	8	45	115	114	134	128	120	114	**50.**	6	43	114	113	134	133	130	125

51.	22	104	125	127	119	124	134	116	**52.**	12	62	132	122	133	142	129	118
53.	26	75	134	129	118	134	134	128	**54.**	15	45	97	124	118	129	116	122
55.	8	38	121	129	123	122	132	127	**56.**	14	68	119	133	130	125	137	131
57.	18	100	129	131	129	129	138	121	**58.**	20	79	124	135	141	142	127	119
59.	3	23	95	123	131	117	134	131	**60.**	9	41	113	131	122	138	129	112
61.	23	98	132	118	121	133	119	123	**62.**	15	89	135	136	123	123	120	135
63.	13	56	118	127	129	125	116	136	**64.**	4	21	92	127	129	133	135	115
65.	5	26	100	123	128	129	125	141	**66.**	16	49	116	126	134	114	129	121
67.	14	47	106	129	121	114	130	129	**68.**	19	110	139	128	132	122	131	128
69.	18	80	119	117	111	129	134	138	**70.**	13	52	114	135	130	124	133	128
71.	16	68	122	132	128	131	138	122	**72.**	9	47	108	136	120	132	125	127
73.	7	39	111	127	133	113	125	131	**74.**	6	20	102	118	125	121	122	122
75.	19	73	143	129	139	134	134	133	**76.**	4	26	88	130	136	128	121	121
77.	14	46	96	146	134	131	136	127	**78.**	20	75	130	116	135	128	132	131
79.	9	46	115	126	106	126	124	122	**80.**	19	68	118	130	138	121	126	145
81.	19	78	130	122	133	121	125	123	**82.**	23	81	115	117	133	116	122	115
83.	4	26	96	125	139	131	141	115	**84.**	12	48	98	137	129	139	143	131
85.	4	19	90	125	129	135	135	130	**86.**	4	24	97	123	121	136	127	131
87.	18	87	126	123	109	127	142	127	**88.**	12	58	120	111	127	132	130	137
89.	21	67	129	125	132	127	142	129	**90.**	25	72	139	122	123	122	144	133
91.	14	57	131	136	122	123	121	132	**92.**	31	96	129	126	132	129	129	129
93.	22	71	130	127	131	123	143	138	**94.**	26	100	132	127	133	132	119	142
95.	11	57	121	126	132	129	133	148	**96.**	3	25	109	132	127	116	124	123
97.	13	48	90	132	127	116	124	123	**98.**	10	65	128	140	133	134	130	24
99.	13	64	116	130	129	137	132	126	**100.**	14	73	111	131	141	124	131	123
101.	11	53	120	122	147	134	120	131	**102.**	10	50	116	123	125	146	125	115
103.	6	24	109	134	118	129	130	125	**104.**	11	58	139	128	127	115	120	122
105.	23	96	133	116	128	119	121	122	**106.**	20	71	128	131	138	131	122	114
107.	15	47	97	121	127	122	135	134	**108.**	10	60	121	128	127	127	135	121
109.	11	76	121	121	129	127	126	134	**110.**	17	44	92	129	134	114	126	135

111.	7	35	94	135	116	118	121	131	**112.**	20	110	119	118	136	127	133	133
113.	14	66	124	132	137	142	120	126	**114.**	11	87	135	125	125	117	135	136
115.	15	50	113	118	131	121	131	122	**116.**	20	90	125	129	135	113	134	132
117.	9	39	103	149	144	133	119	126	**118.**	15	80	119	128	135	123	136	129
119.	13	24	98	128	139	125	123	131	**120.**	1	22	98	129	137	113	139	126
121.	18	90	133	119	129	124	122	140	**122.**	5	23	105	134	142	119	139	121
123.	11	40	112	129	138	129	131	116	**124.**	11	40	103	132	119	119	128	139
125.	12	62	131	118	123	134	119	141	**126.**	15	84	105	130	130	135	133	121
127.	12	52	107	127	132	131	145	128	**128.**	5	24	96	136	124	124	136	130
129.	11	53	130	128	124	124	131	123	**130.**	11	87	141	137	135	111	127	129
131.	8	43	128	120	130	114	133	116	**132.**	10	42	105	115	140	130	129	133
133.	19	87	125	117	116	131	105	113	**134.**	4	21	104	114	122	126	123	127
135.	10	41	122	117	118	129	120	124	**136.**	12	48	100	123	129	119	143	131
137.	15	93	118	140	125	118	126	126	**138.**	15	56	119	123	122	116	115	143
139.	5	25	115	139	122	131	130	121	**140.**	9	38	110	126	143	120	137	130
141.	20	83	116	129	132	145	122	134	**142.**	18	81	118	134	126	122	121	120
143.	14	44	98	134	130	138	142	128	**144.**	2	24	97	127	128	126	132	137
145.	17	79	130	145	111	145	130	125	**146.**	2	24	95	123	127	140	125	132
147.	17	64	130	129	132	116	118	133	**148.**	24	96	117	129	125	126	126	125
149.	14	82	124	130	122	126	120	110	**150.**	18	92	117	114	131	123	132	134
151.	21	77	117	125	131	139	137	135	**152.**	17	95	141	129	124	128	126	128
153.	27	104	118	127	114	130	138	125	**154.**	10	62	130	141	125	121	124	123
155.	27	104	139	139	123	135	123	128	**156.**	26	96	111	127	127	125	132	127
157.	8	39	118	133	129	129	133	137	**158.**	13	40	102	130	114	128	134	138
159.	10	49	110	124	121	129	128	132	**160.**	26	72	140	137	129	131	131	135
161.	15	68	127	114	130	124	121	128	**162.**	16	83	131	128	120	127	123	128
163.	12	54	98	130	124	136	125	116	**164.**	8	43	104	127	128	134	147	127
165.	9	35	124	131	139	135	125	122	**166.**	23	66	145	126	145	131	129	121
167.	12	86	114	126	135	126	128	132	**168.**	17	77	115	132	137	115	129	137
169.	3	25	92	130	122	122	129	130	**170.**	12	61	131	144	125	133	131	129

171.	13	37	104	134	124	121	115	117	**172.**	18	84	127	132	111	125	117	108
173.	18	76	120	115	133	122	129	125	**174.**	18	86	131	125	134	125	125	130
175.	20	88	111	130	124	126	132	135	**176.**	25	114	126	134	128	125	131	129
177.	12	33	104	145	114	121	144	133	**178.**	12	46	93	133	141	124	125	127
179.	5	22	98	127	118	135	150	121	**180.**	20	63	136	136	117	121	128	136
181.	8	38	108	10	112	129	135	133	**182.**	11	41	97	124	129	134	130	126
183.	9	34	114	124	133	136	131	130	**184.**	12	41	97	116	117	133	138	125
185.	16	70	138	121	121	133	118	124	**186.**	21	104	136	132	148	128	135	133
187.	13	48	100	127	23	137	118	128	**188.**	21	69	127	113	121	132	129	119
189.	12	66	129	125	125	139	126	127	**190.**	14	62	127	124	118	128	120	130
191.	20	71	121	130	131	139	122	127	**192.**	11	39	110	119	123	129	137	125
193.	17	86	127	124	133	133	125	130	**194.**	11	65	135	120	113	127	127	133
195.	10	48	93	126	115	125	134	128	**196.**	21	109	138	120	118	112	127	126
197.	24	84	138	135	112	123	107	135	**198.**	3	25	97	127	128	129	131	135
199.	10	47	105	134	127	136	139	129	**200.**	19	86	127	118	125	135	130	140

6-ilova

Hosilqilingandiamatritsalarjuftlarigamisollar (16-sanoqtizimida)

K_1 ={05, 3b, 93, 0c, 67, 05, 67, 67, 77, 09, 05, 77, c6, 4f, 79, 05}	K_2 ={93, cc, ab, af, 99, 93, 99, 99, c9, af, 93, c9, d5, 78, 5b, 93}
K_1 ={79, 31, 13, 8e, f8, 79, f8, f8, 01, e7, 79, 01, 45, da, 24, 79}	K_2 ={a9, d4, f2, fd, 1c, a9, 1c, 1c, d8, 37, a9, d8, 8d, 1b, 5e, a9}
K_1 ={a1, 0c, c6, 58, c9, a1, c9, c9, 83, 42, a1, 83, fe, 9d, aa, a1}	K_2 ={73, 6f, a7, 2b, b2, 73, b2, b2, 87, 8f, 73, 87, 14, 68, 7c, 73}
K_1 ={23, 92, b3, ed, 90, 23, 90, 90, eb, 64, 23, eb, c6, 56, c0, 23}	K_2 ={cd, 46, e4, b9, b2, cd, b2, b2, 5c, 91, cd, 5c, 21, 5d, 64, cd}
K_1 ={e7, 66, c3, f8, c3, e7, c3, c3, 32, 80, e7, 32, 61, 25, f4, e7}	K_2 ={ed, d5, 45, b0, 50, ed, 50, 50, ad, 82, ed, ad, 67, 11, c2, ed}
K_1 ={55, 84, 4d, b1, b0, 55, b0, b0, 2e, 72, 55, 2e, 5f, f6, 99, 55}	K_2 ={e9, c9, 09, fa, 05, e9, 05, 05, 70, 78, e9, 70, 29, a6, 7a, e9}
K_1 ={f1, c0, 53, a6, 9c, f1, 9c, 9c, 57, 33, f1, 57,	K_2 ={91, 55, 71, 42, 53, 91, 53, 53, 11, 12, 91, 11,

79, ed, 2c, f1}	e0, e2, a9, 91}
K_1 ={4f, 90, 42, 16, d2, 4f, d2, d2, 4b, c2, 4f, 4b, bf, 08, 5f, 4f}	K_2 ={77, 07, 8b, bd, 37, 77, 37, 37, c2, 54, 77, c2, 56, 46, 9c, 77}
K_1 ={bf, bc, cd, 8c, 63, bf, 63, 63, 2d, ec, bf, 2d, 84, cb, 9f, bf}	K_2 ={a1, c6, c8, 09, b6, a1, b6, b6, 34, 58, a1, 34, c5, 50, 88, a1}
K_1 ={ab, 97, a1, 2c, de, ab, de, de, 25, fa, ab, 25, 8f, a1, 70, ab}	K_2 ={11, 42, de, 15, 70, 11, 70, 70, 03, bb, 11, 03, 96, 4b, 19, 11}
K_1 ={d5, 37, 45, 5d, 5b, d5, 5b, 5b, 40, 3b, d5, 40, 44, df, 2e, d5}	K_2 ={1b, 9a, 6f, 63, d3, 1b, d3, d3, 18, 9a, 1b, 18, 3c, ad, 98, 1b}

7-ilova

$w_{i,j}^{1}$ningbarcharaundlaruchunqiymatlari

$w_{i,j}$	**Raundlarsoni, *k***								
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
i=0, j=0	92	121	130	44	14	232	215	201	40
i=0, j=1	121	44	232	201	250	252	110	203	156
i=0, j=2	130	232	40	252	163	156	46	57	209
i=0, j=3	44	201	252	203	141	57	158	81	148
i=1, j=0	252	60	110	163	203	175	156	137	141
i=1, j=1	60	163	175	137	46	88	56	209	170
i=1, j=2	110	175	141	88	54	170	81	39	229
i=1, j=3	163	137	88	209	105	39	140	90	169
i=2, j=0	88	57	56	54	209	158	170	247	105
i=2, j=1	57	54	158	247	81	172	148	229	91
i=2, j=2	56	158	105	172	11	91	90	196	243
i=2, j=3	54	247	172	229	111	196	20	129	78
i=3, j=0	172	39	148	11	229	140	91	15	111
i=3, j=1	39	11	140	15	90	222	169	243	216
i=3, j=2	148	140	111	222	22	216	129	174	150
i=3, j=3	11	15	222	243	47	174	10	37	149
i=4, j=0	222	196	169	22	243	20	216	197	47
i=4, j=1	196	22	20	197	129	254	78	150	145
i=4, j=2	169	20	47	254	7	145	37	223	192
i=4, j=3	22	197	254	150	98	223	102	228	65
i=5, j=0	254	174	78	7	150	10	145	82	98
i=5, j=1	174	7	10	82	37	19	149	192	86
i=5, j=2	78	10	98	19	113	86	228	8	152
i=5, j=3	7	82	19	192	184	8	218	151	58
i=6, j=0	19	223	149	113	192	102	86	122	184
i=6, j=1	223	113	102	122	228	132	65	152	87
i=6, j=2	149	102	184	132	147	87	151	127	117
i=6, j=3	113	122	132	152	32	127	61	80	176

i=7, j=0	132	8	65	147	152	218	87	139	32
i=7, j=1	8	147	218	139	151	26	58	117	219
i=7, j=2	65	218	32	26	85	219	80	13	94
i=7, j=3	147	139	26	117	233	13	179	95	154

$w_{i,j}^2$ningbarcharaundlaruchunqiymatlari

$w_{i,j}$	**Raundlarsoni, *k***								
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
i=0, j=0	252	110	203	156	141	166	57	54	158
i=0, j=1	60	203	137	166	56	158	105	172	11
i=0, j=2	110	156	166	54	247	172	229	111	196
i=0, j=3	163	141	56	247	39	91	222	20	55
i=1, j=0	88	56	209	170	105	220	39	11	140
i=1, j=1	57	209	247	220	148	140	111	222	22
i=1, j=2	56	170	220	11	15	222	243	47	174
i=1, j=3	54	105	148	15	196	216	254	10	157
i=2, j=0	172	148	229	91	111	5	196	22	20
i=2, j=1	39	229	15	5	169	20	47	254	7
i=2, j=2	148	91	5	22	197	254	150	98	223
i=2, j=3	11	111	169	197	174	145	19	102	118
i=3, j=0	222	169	243	216	47	55	174	7	10
i=3, j=1	196	243	197	55	78	10	98	19	113
i=3, j=2	169	216	55	7	82	19	192	184	8
i=3, j=3	22	47	78	82	223	86	132	218	204
i=4, j=0	254	78	150	145	98	157	223	113	102
i=4, j=1	174	150	82	157	149	102	184	132	147
i=4, j=2	78	145	157	113	122	132	152	32	127
i=4, j=3	7	98	149	122	8	87	26	61	240
i=5, j=0	19	149	192	86	184	118	8	147	218
i=5, j=1	223	192	122	118	65	218	32	26	85
i=5, j=2	149	86	118	147	139	26	117	233	13
i=5, j=3	113	184	65	139	127	219	189	179	128

i=6, j=0	132	65	152	87	32	204	127	85	61
i=6, j=1	8	152	139	204	58	61	233	189	43
i=6, j=2	65	87	204	85	167	189	94	115	230
i=6, j=3	147	32	58	167	13	217	70	29	182
i=7, j=0	26	58	117	219	233	240	13	43	179
i=7, j=1	127	117	167	240	176	179	115	70	104
i=7, j=2	58	219	240	43	124	70	153	226	186
i=7, j=3	85	233	176	124	230	225	245	168	143

8-ilova

4 taakslantirishlarningturlitartibiuchunlavinsamaradorligiiningqiymatlari

№	Akslantirishtartibi	Lavin samaradorlik			
		128 – bitkalit			
		1-raund	2-raund	3-raund	4-raund
1.	B→Q→S→A	0,0906	0,3356	0,4904	0,5004
2.	B→Q→A→S	0,1005	0,3588	0,4858	0,5008
3.	B→S→Q→A	0,0897	0,3340	0,4884	0,4997
4.	B→S→A→Q	0,0891	0,3332	0,4894	0,4996
5.	B→A→Q→S	0,0995	0,3590	0,4860	0,5002
6.	B→A→S→Q	0,1011	0,3596	0,4856	0,4981
7.	Q→B→S→A	0,0898	0,3347	0,4892	0,5012
8.	Q→B→A→S	0,0995	0,3593	0,4854	0,5001
9.	Q→S→B→A	0,0910	0,3351	0,4907	0,4990
10.	Q→S→A→B	0,0775	0,3374	0,4980	0,5007
11.	Q→A→B→S	0,0311	0,1563	0,4356	0,5005
12.	Q→A→S→B	0,0306	0,1564	0,4350	0,5007
13.	S→B→Q→A	0,0914	0,3344	0,4900	0,5021
14.	S→B→A→Q	0,0912	0,3324	0,4906	0,4998
15.	S→Q→B→A	0,0909	0,3349	0,4913	0,5004
16.	S→Q→A→B	0,0778	0,3392	0,4989	0,4997
17.	S→A→B→Q	0,0778	0,3399	0,4998	0,5000
18.	S→A→Q→B	0,0778	0,3384	0,4979	0,4996
19.	A→B→Q→S	0,0312	0,1559	0,4345	0,5000
20.	A→B→S→Q	0,0309	0,1561	0,4350	0,5007
21.	A→Q→B→S	0,0310	0,1565	0,4343	0,4992
22.	A→Q→S→B	0,0309	0,1557	0,4336	0,4995
23.	A→S→B→Q	0,0309	0,1555	0,4346	0,4987
24.	A→S→Q→B	0,0314	0,1562	0,4342	0,4999

NISTstatistiktestlashnatijalari

128 bitlikalit – 1 - na'muna

monobit_test 0.3710933695226976 7 PASS
frequency_within_block_test 0.9517593636072188 PASS
runs_test 0.7180059159426126 PASS
longest_run_ones_in_a_block_test 0.03117654174000522 PASS
binary_matrix_rank_test 0.8636096275247119 PASS
dft_test 1.2242009827814287e-05 FAIL
non_overlapping_template_matching_test 0.9999980235757895 PASS
overlapping_template_matching_test 0.05662774869592887 PASS
maurers_universal_test 0.9981849128506057 PASS
linear_complexity_test 0.6538551861170803 PASS
serial_test 0.5248438832758395 PASS
approximate_entropy_test 0.5833680418567758 PASS
cumulative_sums_test 0.41812503598942485 PASS
random_excursion_test 0.23458315457603654 PASS
random_excursion_variant_test 0.03639276222842889 PASS

128 bitlikalit – 2 - na'muna

monobit_test 0.23212656184359673 PASS
frequency_within_block_test 0.9139345352935897 PASS
runs_test 0.29761121025177956 PASS
longest_run_ones_in_a_block_test 0.7349290758278089 PASS
binary_matrix_rank_test 0.3026522383026931 PASS
dft_test 4.050851623545979e-10 FAIL
non_overlapping_template_matching_test 0.9999999605905411 PASS
overlapping_template_matching_test 0.2542443353898376 PASS
maurers_universal_test 0.9994710007055765 PASS
linear_complexity_test 0.46950573741504636 PASS
serial_test 0.12189470300761339 PASS
approximate_entropy_test 0.2229181360537875 PASS
cumulative_sums_test 0.21117016618921136 PASS
random_excursion_test 0.0843247013164315 PASS
random_excursion_variant_test 0.35201486942213317 PASS

128 bitlikalit – 3 - na'muna

monobit_test 0.7531815191389909 PASS
frequency_within_block_test 0.8625319608518368 PASS
runs_test 0.7352605476695402 PASS
longest_run_ones_in_a_block_test 0.781400209186321 PASS
binary_matrix_rank_test 0.2520883248219178 PASS
dft_test 3.8427225604824335e-05 FAIL
non_overlapping_template_matching_test 0.9999998188652189 PASS
overlapping_template_matching_test 0.4074468929895905 PASS
maurers_universal_test 0.9999128501184967 PASS
linear_complexity_test 0.3976002641750591 PASS
serial_test 0.05098701412544494 PASS
approximate_entropy_test 0.2015541920707594 PASS
cumulative_sums_test 0.8084137450768241 PASS
random_excursion_test 0.12379429466083483 PASS
random_excursion_variant_test 0.06614786610425866 PASS

128 bitlikalit – 4 - na'muna

monobit_test 0.7362618386421997 PASS
frequency_within_block_test 0.888525343385874 PASS
runs_test 0.9197867594890975 PASS
longest_run_ones_in_a_block_test 0.5646979830484062 PASS
binary_matrix_rank_test 0.6080433833183277 PASS
dft_test 1.8737961731441276e-09 FAIL
non_overlapping_template_matching_test 0.9994203840032165 PASS
overlapping_template_matching_test 0.9315674401728546 PASS
maurers_universal_test 0.9976633015079981 PASS
linear_complexity_test 0.2796176148804707 PASS
serial_test 0.13911316301434126 PASS
approximate_entropy_test 0.4551869770630015 PASS
cumulative_sums_test 0.4344732031596017 PASS
random_excursion_test 0.014963036284841724 PASS
random_excursion_variant_test 0.16390750941244592 PASS

128 bitlikalit – 5 - na'muna

monobit_test 0.8591251721171266 PASS
frequency_within_block_test 0.6869738124615308 PASS
runs_test 0.42892585984432186 PASS
longest_run_ones_in_a_block_test 0.10137046272065502 PASS
binary_matrix_rank_test 0.10055415395970421 PASS
dft_test 7.2965353634402870e-09 FAIL
non_overlapping_template_matching_test 0.9999977988251526 PASS
overlapping_template_matching_test 0.7385569209912617 PASS
maurers_universal_test 0.9996783042347573 PASS
linear_complexity_test 0.8148376147882189 PASS
serial_test 0.0073112431673581935 FAIL
approximate_entropy_test 0.04478831902334479 PASS
cumulative_sums_test 0.8090418601478795 PASS
random_excursion_test 0.019833109962644556 PASS
random_excursion_variant_test 0.020251713468705097 PASS

192bitlikalit –1 - na'muna

monobit_test 0.2781462826959445 PASS
frequency_within_block_test 0.8822584229745166 PASS
runs_test 0.7138189032156856 PASS
longest_run_ones_in_a_block_test 0.581403684840445 PASS
binary_matrix_rank_test 0.050475664231082976 PASS
dft_test 0.00041054164296551183 FAIL
non_overlapping_template_matching_test 1.000101796994085 PASS
overlapping_template_matching_test 0.15707276870268716 PASS
maurers_universal_test 0.9990322152177363 PASS
linear_complexity_test 0.07888773514592222 PASS
serial_test 0.6378195489174414 PASS
approximate_entropy_test 0.6372107375069958 PASS
cumulative_sums_test 0.0945536968646652 PASS
random_excursion_test 0.2057850859902828 PASS
random_excursion_variant_test 0.06825898811407623 PASS

192bitlikalit –2 - na'muna

monobit_test 0.9376193426792672 PASS
frequency_within_block_test 0.9999103253744537 PASS
runs_test 0.13738935196517418 PASS
longest_run_ones_in_a_block_test 0.41792846441257103 PASS
binary_matrix_rank_test 0.8970250086901314 PASS
dft_test 1.259267472552782e-09 FAIL
non_overlapping_template_matching_test 0.9999710033408832 PASS
overlapping_template_matching_test 0.6040061028566835 PASS
maurers_universal_test 0.9994922037876685 PASS
linear_complexity_test 0.18292521304692994 PASS
serial_test 0.17490422867627345 PASS
approximate_entropy_test 0.1749457532663562 PASS
cumulative_sums_test 0.9551412636473311 PASS
random_excursion_test 0.19917346093369964 PASS
random_excursion_variant_test 0.08887267098693304 PASS

192bitlikalit –3 - na'muna

monobit_test 0.2489216512238181 PASS
frequency_within_block_test 0.8322674868919058 PASS
runs_test 0.9372465364626711 PASS
longest_run_ones_in_a_block_test 0.9214326362641231 PASS
binary_matrix_rank_test 0.3210190180939391 PASS
dft_test 4.5811687968652013e-10 FAIL
non_overlapping_template_matching_test 1.0000339213348954 PASS
overlapping_template_matching_test 0.5647008566490621 PASS
maurers_universal_test 0.9992770436883103 PASS
linear_complexity_test 0.48783842427845536 PASS
serial_test 0.5335003145994045 PASS
approximate_entropy_test 0.5331831481784685 PASS
cumulative_sums_test 0.4349910480342043 PASS
random_excursion_test 0.036724767576959486 PASS
random_excursion_variant_test 0.18341265185025787 PASS

192bitlikalit –4 - na'muna

monobit_test 0.2166714219388558 PASS
frequency_within_block_test 0.3698878108907941 PASS
runs_test 0.9507038377410943 PASS
longest_run_ones_in_a_block_test 0.5701357754911165 PASS
binary_matrix_rank_test 0.3696869346919205 PASS
dft_test 9.712418953053711e-14 FAIL
non_overlapping_template_matching_test 1.0000007170146878 PASS
overlapping_template_matching_test 0.4578576899073186 PASS
maurers_universal_test 0.9997530557847102 PASS
linear_complexity_test 0.5408495683428005 PASS
serial_test 0.8207343847169889 PASS
approximate_entropy_test 0.8579115191276894 PASS
cumulative_sums_test 0.2484333410857833 PASS
random_excursion_test 0.15878150189616216 PASS
random_excursion_variant_test 0.042191839410739056 PASS

192bitlikalit –5 - na'muna

monobit_test 0.7017741573991256 PASS
frequency_within_block_test 0.9592221590542728 PASS
runs_test 0.6079509066798632 PASS
longest_run_ones_in_a_block_test 0.3933128618971442 PASS
binary_matrix_rank_test 0.31544223464135307 PASS
dft_test 1.0729710883299393e-09 FAIL
non_overlapping_template_matching_test 1.0017571824724898 PASS
overlapping_template_matching_test 0.03222205220367096 PASS
maurers_universal_test 0.9990633327094991 PASS
linear_complexity_test 0.8344280451811533 PASS
serial_test 0.03982211111854489 PASS
approximate_entropy_test 0.1294786231813478 PASS
cumulative_sums_test 0.4381069659319232 PASS
random_excursion_test 0.11336999506869137 PASS
random_excursion_variant_test 0.03464794643376185 PASS

256bitlikalit –1 - na'muna

monobit_test 0.7820001724131037 PASS
frequency_within_block_test 0.235331322217485 PASS
runs_test 0.7351681689603489 PASS
longest_run_ones_in_a_block_test 0.621939251826269 PASS
binary_matrix_rank_test 0.8429451095154354 PASS
dft_test 7.874252289770167e-09 FAIL
non_overlapping_template_matching_test 0.999957309459021 PASS
overlapping_template_matching_test 0.8040212731660688 PASS
maurers_universal_test 0.9983162601648017 PASS
linear_complexity_test 0.6189208261830953 PASS
serial_test 0.19340808378153954 PASS
approximate_entropy_test 0.20897758002604194 PASS
cumulative_sums_test 0.6001453452004988 PASS
random_excursion_test 0.040162540927182085 PASS
random_excursion_variant_test 0.12635334150137517 PASS

256bitlikalit – 2 - na'muna

monobit_test 0.3636655441955544 PASS
frequency_within_block_test 0.4737266212820048 PASS
runs_test 0.14401294157958372 PASS
longest_run_ones_in_a_block_test 0.5671790813005558 PASS
binary_matrix_rank_test 0.5656386885055672 PASS
dft_test 4.042518159580746e-08 FAIL
non_overlapping_template_matching_test 1.000051313263019 PASS
overlapping_template_matching_test 0.6453795657944845 PASS
maurers_universal_test 0.9991073584383567 PASS
linear_complexity_test 0.4168090331152054 PASS
serial_test 0.30954096905600403 PASS
approximate_entropy_test 0.30948905874209987 PASS
cumulative_sums_test 0.3385088988774694 PASS
random_excursion_test 0.1896581264573567 PASS
random_excursion_variant_test 0.10102241332659927 PASS

256bitlikalit –3 - na'muna

monobit_test 0.18107639338498233 PASS
frequency_within_block_test 0.7923842283584159 PASS
runs_test 0.2737689200294277 PASS
longest_run_ones_in_a_block_test 0.6091295506829709 PASS
binary_matrix_rank_test 0.3269966443495426 PASS
dft_test 1.1207019125939086e-05 FAIL
non_overlapping_template_matching_test 0.9998360813441503 PASS
overlapping_template_matching_test 0.5169620979328121 PASS
maurers_universal_test 0.9993503037982964 PASS
linear_complexity_test 0.1391863457718615 PASS
serial_test 0.5048748001561789 PASS
approximate_entropy_test 0.5040186074523779 PASS
cumulative_sums_test 0.17431233859223383 PASS
random_excursion_test 0.14199174873854534 PASS
random_excursion_variant_test 0.04784333039445718 PASS

256bitlikalit –4 - na'muna

monobit_test 0.23818884632901322 PASS
frequency_within_block_test 0.6925354835786088 PASS
runs_test 0.3346799017128671 PASS
longest_run_ones_in_a_block_test 0.8276042101397326 PASS
binary_matrix_rank_test 0.5529560971378986 PASS
dft_test 0.00017596683120572974 FAIL
non_overlapping_template_matching_test 0.9999998957330569 PASS
overlapping_template_matching_test 0.34303767873766167 PASS
maurers_universal_test 0.9991686467133676 PASS
linear_complexity_test 0.6077162050258621 PASS
serial_test 0.7655083326149356 PASS
approximate_entropy_test 0.7652218780919076 PASS
cumulative_sums_test 0.26276594936037867 PASS
random_excursion_test 0.15609211851930616 PASS
random_excursion_variant_test 0.01421338109037403 PASS

256bitlikalit –5 - na'muna

monobit_test 0.28313087066234666 PASS
frequency_within_block_test 0.694483159545546 PASS
runs_test 0.7708359901058804 PASS
longest_run_ones_in_a_block_test 0.35775659348323585 PASS
binary_matrix_rank_test 0.32231734241589244 PASS
dft_test 1.1887275314776766e-05 FAIL

non_overlapping_template_matching_test 0.9999976133719408 PASS
overlapping_template_matching_test 0.7090410766218178 PASS
maurers_universal_test 0.9989005510533575 PASS
linear_complexity_test 0.950665114457174 PASS
serial_test 0.313721167018862 PASS
approximate_entropy_test 0.48209393679480206 PASS
cumulative_sums_test 0.14817914710921265 PASS
random_excursion_test 0.014068661322363663 PASS
random_excursion_variant_test 0.07211809342878084 PASS

512bitlikalit –1 - na'muna

monobit_test 0.4864437610201667 PASS
frequency_within_block_test 0.7760207089538866 PASS
runs_test 0.08304385919246365 PASS
longest_run_ones_in_a_block_test 0.3329573026417528 PASS
binary_matrix_rank_test 0.7929493130499903 PASS
dft_test 2.0896945763128018e-08 FAIL
non_overlapping_template_matching_test 0.9999836069407184 PASS
overlapping_template_matching_test 0.0407135681870612 PASS
maurers_universal_test 0.9999295601845891 PASS
linear_complexity_test 0.1662290374683726 PASS
serial_test 0.2517709530922548 PASS
approximate_entropy_test 0.25239661978955846 PASS
cumulative_sums_test 0.4136050904083872 PASS
random_excursion_test 0.11289935568621036 PASS
random_excursion_variant_test 0.1703008057139401 PASS

512bitlikalit –2 - na'muna

monobit_test 0.5905398672847959 PASS
frequency_within_block_test 0.8366421225428272 PASS
runs_test 0.6167071635039107 PASS
longest_run_ones_in_a_block_test 0.10273944652206958 PASS
binary_matrix_rank_test 0.6007186071231131 PASS
dft_test 1.0996379901689999e-07 FAIL
non_overlapping_template_matching_test 0.9999993851635168 PASS
overlapping_template_matching_test 0.5645398966326612 PASS
maurers_universal_test 0.9992096210773789 PASS
linear_complexity_test 0.5944285760641836 PASS
serial_test 0.1429216401960604 PASS
approximate_entropy_test 0.3106897423352451 PASS
cumulative_sums_test 0.7171167634881552 PASS
random_excursion_test 0.1442757405379839 PASS
random_excursion_variant_test 0.023671895351299918 PASS

512bitlikalit –3 - na'muna

monobit_test 0.5321669942362957 PASS
frequency_within_block_test 0.6348869126289941 PASS
runs_test 0.08607876149077438 PASS
longest_run_ones_in_a_block_test 0.16788479512714802 PASS
binary_matrix_rank_test 0.6004234296240798 PASS
dft_test 2.362119201968142e-11 FAIL
non_overlapping_template_matching_test 0.9999998843850203 PASS
overlapping_template_matching_test 0.6918725394085885 PASS
maurers_universal_test 0.9999533696348322 PASS
linear_complexity_test 0.16265759280602402 PASS
serial_test 0.32696856637063626 PASS
approximate_entropy_test 0.32736994495424526 PASS
cumulative_sums_test 0.23178719097176148 PASS
random_excursion_test 0.3067597059407578 PASS
random_excursion_variant_test 0.0 FAIL

512bitlikalit –4 - na'muna

monobit_test 0.6011963391515139 PASS
frequency_within_block_test 0.8394742648580571 PASS
runs_test 0.03425252863874708 PASS
longest_run_ones_in_a_block_test 0.4917300113192189 PASS
binary_matrix_rank_test 0.007431773552013385 FAIL
dft_test 0.00019987729016825254 FAIL
non_overlapping_template_matching_test 1.0000000290750706 PASS
overlapping_template_matching_test 0.8046086184637246 PASS
maurers_universal_test 0.9998464146638257 PASS
linear_complexity_test 0.08548434359401508 PASS
serial_test 0.3885370767595971 PASS
approximate_entropy_test 0.38796326287774635 PASS
cumulative_sums_test 0.824594605713862 PASS
random_excursion_test 0.30594431330731875 PASS
random_excursion_variant_test 0.015469056098486707 PASS

512bitlikalit –5 - na'muna

monobit_test 0.6346697671049808 PASS
frequency_within_block_test 0.8695773434128986 PASS
runs_test 0.9374938396968943 PASS
longest_run_ones_in_a_block_test 0.856582139141071 PASS
binary_matrix_rank_test 0.4293564158941799 PASS
dft_test 4.042518159580746e-08 FAIL
non_overlapping_template_matching_test 0.9999983986770911 PASS
overlapping_template_matching_test 0.7850991979177968 PASS
maurers_universal_test 0.9999602924174762 PASS
linear_complexity_test 0.23274422110792287 PASS
serial_test 0.6584889209039524 PASS
approximate_entropy_test 0.935331970239308 PASS
cumulative_sums_test 0.32444585128711645 PASS
random_excursion_test 0.028324688499308096 PASS
random_excursion_variant_test 0.06131863864322428 PASS

128bitlizaifkalit –1 – na'muna (0x00 daniborat)

monobit_test 0.7852216119165469 PASS
frequency_within_block_test 0.5980117356801798 PASS
runs_test 0.7372765261772061 PASS
longest_run_ones_in_a_block_test 0.8224851639483036 PASS
binary_matrix_rank_test 0.7290840845200594 PASS
dft_test 2.515461389484617e-15 FAIL
non_overlapping_template_matching_test 0.9999986065840362 PASS
overlapping_template_matching_test 0.32409952211025284 PASS
maurers_universal_test 0.9995340313315269 PASS
linear_complexity_test 0.63157485997919 PASS
serial_test 0.45235498917026057 PASS
approximate_entropy_test 0.8369936449476212 PASS
cumulative_sums_test 0.47777545484308725 PASS
random_excursion_test 0.2301408825734448 PASS
random_excursion_variant_test 0.05292561240249631 PASS

128bitlizaifkalit –2 – na'muna (0xFFdaniborat)

monobit_test 0.6476736381742034 PASS
frequency_within_block_test 0.9729597665953549 PASS
runs_test 0.450532788663954 PASS
longest_run_ones_in_a_block_test 0.0082827405964489 FAIL
binary_matrix_rank_test 0.9982781601264766 PASS
dft_test 6.827003083463316e-12 FAIL
non_overlapping_template_matching_test 1.0001207341033838 PASS
overlapping_template_matching_test 0.7401100166428962 PASS
maurers_universal_test 0.999375617230823 PASS
linear_complexity_test 0.18411293996849676 PASS
serial_test 0.38927668000478816 PASS
approximate_entropy_test 0.3886853551358627 PASS
cumulative_sums_test 0.49845602241750897 PASS
random_excursion_test 0.039282150195671356 PASS
random_excursion_variant_test 0.0 FAIL

128bitlizaifkalit –3 – na'muna (0x01 daniborat)

monobit_test 0.7723584735683581 PASS
frequency_within_block_test 0.8753430577587222 PASS
runs_test 0.7564119389425068 PASS
longest_run_ones_in_a_block_test 0.6872633184012372 PASS
binary_matrix_rank_test 0.011328966827666983 PASS
dft_test 1.259267472552782e-09 FAIL
non_overlapping_template_matching_test 0.9998400648742272 PASS
overlapping_template_matching_test 0.29179468977576034 PASS
maurers_universal_test 0.9998581151937869 PASS
linear_complexity_test 0.7945519646232208 PASS
serial_test 0.0031002078314147493 FAIL
approximate_entropy_test 0.011229241018273889 PASS
cumulative_sums_test 0.7472797953788002 PASS
random_excursion_test 0.009513528037869534 FAIL
random_excursion_variant_test 0.2921887223517532 PASS

128bitlizaifkalit –4 – na'muna (0xE1daniborat)

monobit_test 0.5591040869812358 PASS
frequency_within_block_test 0.9894547762434537 PASS
runs_test 0.6874972209598063 PASS
longest_run_ones_in_a_block_test 0.3041166583580004 PASS
binary_matrix_rank_test 0.2813140631895416 PASS
dft_test 3.676159826321767e-07 FAIL
non_overlapping_template_matching_test 1.000005434563388 PASS
overlapping_template_matching_test 0.400080120783165 PASS
maurers_universal_test 0.9993664586617641 PASS
linear_complexity_test 0.23124737792818156 PASS
serial_test 0.2724506714060732 PASS
approximate_entropy_test 0.6711380039230356 PASS
cumulative_sums_test 0.6382476795550129 PASS
random_excursion_test 0.05877836479050916 PASS
random_excursion_variant_test 0.017127205135811088 PASS

128bitlizaifkalit –5 – na'muna (0xEFdaniborat)

monobit_test 0.5838040676176302 PASS
frequency_within_block_test 0.8661118044579389 PASS
runs_test 0.35063990724382554 PASS
longest_run_ones_in_a_block_test 0.07048874996763387 PASS
binary_matrix_rank_test 0.5837660534012311 PASS
dft_test 9.382145064467882e-06 FAIL
non_overlapping_template_matching_test 0.9999994264112613 PASS
overlapping_template_matching_test 0.02456669994157126 PASS
maurers_universal_test 0.9989586644420327 PASS
linear_complexity_test 0.9307927715638428 PASS
serial_test 0.04652587073398401 PASS
approximate_entropy_test 0.20991978126271282 PASS
cumulative_sums_test 0.3312087936940331 PASS
random_excursion_test 0.11269746821043446 PASS
random_excursion_variant_test 0.26137207438963944 PAS

10-ilova

Na’munaviy misol
Shifrlash jarayoni

Kirishbloki (Ochiqmatn):
30313233343536373839414243444546303132333435363738394142434445 46

ShifrlashkalitiK:
37B60BBA0AB160CFDC18F50CDEE8E04530B3F8AF1432FE511FBB2029112F2145

Inisializasiyavektori IV:
2654BB5FA375D89854EA489F9AA88416FD4DEBBD9B3B40334829F9EE5234C37A

Baytalmashtirishmassivi Bsa1:
63 c8 ee 6a fd 64 e7 4d 74 86 e0 5c 79 82 2c 0e e8 d7 c9 28 fa b7 fc 3c 6e a3 cb af 9c 89 8d 2e a6 58 39 38 36 d1 9e aa f7 69 51 dc ac 27 94 0b e5 8c 5b 0f 6f 5a 05 de c4 a9 16 f3 14 d8 c5 2f 81 37 fe ae 4e 07 96 0a 91 52 62 25 9d 13 df 95 71 c0 66 56 7a b8 e4 76 84 08 41 93 98 da 57 8b 20 97 cc 1a 7f 3a 55 75 3d db a7 e9 50 f0 bd 0d b0 2b 5e b3 d9 7c 73 5f 80 46 e6 9a 68 99 1d e1 4a e2 49 b6 f5 ba dd ca ad a8 09 10 c1 34 8f 6d 42 f6 fb a4 bb bc 18 11 1c 77 03 eb 65 15 40 06 32 b5 b2 a0 b9 24 f9 d4 ef 01 8e 83 f8 7b b1 ab 90 29 d6 26 72 43 1b ed c6 12 bf f4 21 8a 4f 61 c2 4b 19 3f ec 48 87 6c 35 44 cf cd 78 60 30 d0 4c 31 67 00 59 47 7e 23 a2 17 f2 e3 54 ce 0c 5d d2 3b 1f 88 a5 c7 53 9b 3e 2d b4 d5 6b 33 7d 85 92 ea f1 02 a1 70 9f 45 be ff 1e c3 04 d3 22 2a
Baytalmashtirishmassivi Bsa2:
1a a8 96 a1 a6 97 80 26 c1 f2 32 7f 8b c9 f0 c3 64 79 27 10 43 4c 6c 9b c4 ac d8 ea b2 9e d5 8e 7d 02 c7 0e 17 83 cb 07 61 e0 84 fa 3e 03 7a 24 be 8c 19 6f 1d f7 b8 68 b3 e6 db 78 d1 cd 0a a7 a3 b4 f1 fc 3f 5d 57 4f 42 8d ca 71 5f ab 66 d9 a0 72 16 ad 9c 2c 49 30 bb 99 31 ce 34 3c fe d3 18 d0 ef cf 82 36 cc 6d d6 b7 c6 5c 58 86 20 e4 75 7e 87 41 8a 53 1f 21 63 67 74 37 0c 2d 91 48 54 df 38 73 44 b1 ae 40 2a 62 fb c5 f5 1c 4d af 45 70 dc 95 04 ec 0f bc fd 6b 0d a2 2e 93 3a eb 59 aa c0 55 06 ed e1 50 4b d7 5a 65 4a e3 25 a9 c8 b5 5b 76 47 05 14 22 2f 81 9a 0b c2 77 09 35 90 1e e9 3d 7b f4 51 92 29 33 b0 9d 23 d2 12 6a 89 2b d4 28 dd f6 f8 8f 08 69 39 00 a5 e5 e2 88 52 1b f9 da bf b9 f3 60 13 ff 56 7c de 6e 5e 85 3b 9f e8 11 4e bd 94 a4 46 ba ee 15 98 01 b6 e7
K1[4x4]:
95 9d 57 b6
5c 95 5c 5c
0d 4d 95 0d
9d 44 b8 95
K2[4x4]:
9d 96 c5 42
34 9d 34 34
56 e9 9d 56
b8 f1 45 9d
K1D[4x4]:
bd 40 14 69
6c bd 6c 6c
43 83 bd 43
dc f3 45 bd
K2D[4x4]:
b5 9b 05 98
3c b5 3c 3c
86 43 b5 86
d2 f2 55 b5
Qo`shHolat (Holat, Holatn):
16 65 89 6c 97 40 ee af 6c d3 09 dd d9 ec c1 50 cd 7c d9 8e af 0e 76 04 70 10 b8 ac 11 70 86 3c
Boshlang’ichbosqichkalit K[0]:
36 6d 33 2b 76 ee 69 4b ae 0f 32 55 17 7d 24 22 80 e4 3b 2c ac 15 0e 68 06 4d 04 55 15 5f 49 da
Qo`shBosqichKalit (Holat, K[0]):
20 08 ba 47 e1 ae 87 e4 c2 dc 3b 88 ce 91 e5 72 4d 98 e2 a2 03 1b 78 6c 76 5d bc f9 04 2f cf e6

1 –bosqich
Kalit K[1]:
62 6b 46 c8 f1 a6 98 06 da 9b 43 6e 29 83 19 2e 40 17 22 83 fc 6c 80 65 32 6b a8 0b d5 0d c4 63
Sur(Holat):
a2 04 5d 78 bc 6c 20 2f 08 cf f9 e1 c2 ae ba e6 47 ce dc 87 3b e4 4d 91 98 e5 88 03 76 1b e2 72
Aralash(Holat, K1D&K2):

2d 4d 52 39 18 47 e1 9b 20 fa 3c 29 02 e6 8a 31 e9 83 c9 bf 77 e0 8b 8d 1e 89 ab e9 ba 46 0d 74
BaytAlmash(Holat, Ba):
27 13 66 a9 6e 0a 3b eb a6 1e 14 69 ee 53 09 8c 2d b6 44 61 5f d2 10 34 8d a8 83 2d bf 96 82 d9
Qo`shBosqichKalit (Holat, K):
45 78 20 61 9f ac a3 ed 7c 85 57 07 c7 d0 10 a2 6d a1 66 e2 a3 be 90 51 bf c3 2b 26 6a 9b 46 ba

2 –bosqich
Kalit K[2]:
c8 ff 04 8f bf 9c 9a e9 bd ff 47 93 b9 fc d7 a5 7b 17 8f 51 a5 53 a7 76 49 95 4d 2c d3 3b 22 14
Sur(Holat):
e2 6a c3 90 2b 51 45 9b 78 46 26 9f 7c ac 20 ba 61 c7 85 a3 57 ed 6d d0 a1 10 07 a3 bf be 66 a2
Aralash(Holat, K1D&K2):
9a 65 92 78 d1 e3 e3 41 fe 6f 56 f5 60 30 94 f2 91 ab e4 f1 13 52 a4 ac c1 7e 8a 03 c5 1e 47 f2
BaytAlmash(Holat, Ba):
0d 36 dc 63 2b da da b4 b6 e4 49 bd 18 be 04 e8 70 65 bf 9f 10 16 06 4a 1e 91 fb a1 f4 d5 4f e8
Qo`shBosqichKalit (Holat, K):
c5 c9 d8 ec 94 46 40 5d 0b 1b 0e 2e a1 42 d3 4d 0b 72 30 ce b5 45 a1 3c 57 04 b6 8d 27 ee 6d fc

3 –bosqich
Kalit K[3]:
d5 88 7f f9 8a 6b 27 00 5c 98 10 c6 9b b9 55 a6 45 91 d2 01 dd 28 15 c6 35 4f 9a 2b 6f da 88 2d
Sur(Holat):
ce 27 04 a1 b6 3c c5 ee c9 6d 8d 94 0b 46 d8 fc ec a1 1b 40 0e 5d 0b 42 72 d3 2e b5 57 45 30 4d
Aralash(Holat, K1D&K2):
29 a6 0f 8d 61 19 f4 19 66 c5 46 c1 ac 97 a7 f7 e4 9c 34 c0 88 16 51 3c b2 aa 19 55 85 1b ad 65
BaytAlmash(Holat, Ba):
69 f9 0e 34 97 a3 a1 a3 55 48 96 4b f8 11 d4 45 a5 65 6f c2 ad fc c0 14 d6 8e a3 b8 ba af 7b 3a
Qo`shBosqichKalit (Holat, K):
bc 71 71 cd 1d c8 86 a3 09 d0 86 8d 63 a8 81 e3 e0 f4 bd c3 70 d4 d5 d2 e3 c1 39 93 d5 75 f3 17

4 –bosqich
Kalit K[4]:
c8 f1 91 b3 2f d8 e3 8e 13 6a 63 7f fd ea b5 f2 6c d5 91 c7 9d c6 d9 49 a0 aa fa db af 87 0f 47
Sur(Holat):
c3 d5 c1 d5 39 d2 bc 75 71 f3 93 1d 09 c8 71 17 cd 63 d0 86 86 a3 e0 a8 f4 81 8d 70 e3 d4 bd e3
Aralash(Holat, K1D&K2):
03 3d f5 40 a0 88 d3 1c 1b 65 9f 07 dd 5f 44 17 f1 2d 08 ce 36 21 b6 98 d4 af 93 d0 e7 2e b5 c7
BaytAlmash(Holat, Ba):
a1 cd bd a3 59 2a 28 b2 ea 36 eb 26 e5 d3 3f 9b 9f 03 c1 12 b8 02 14 fd dd a9 95 89 60 7a 05 92
Qo`shBosqichKalit (Holat, K):
69 3c 2c 10 76 f2 cb 3c f9 5c 88 59 18 39 8a 69 f3 d6 50 d5 25 c4 cd b4 7d 03 6f 52 cf fd 0a d5

5 –bosqich
Kalit K[5]:
a9 ac 66 75 a6 15 c3 2b 3d 4d 95 82 82 62 87 e5 a9 d0 52 79 ab ac f2 22 da 63 15 00 4c c6 07 f2
Sur(Holat):
d5 cf 03 cd 6f b4 69 fd 3c 0a 52 76 f9 f2 2c d5 10 18 5c cb 88 3c f3 39 d6 8a 59 25 7d c4 50 69
Aralash(Holat, K1D&K2):
76 1d 65 15 e5 77 09 13 7e 3a a7 98 78 e1 75 76 62 13 f4 11 c6 d2 c4 97 1a 81 56 49 23 58 c9 db
BaytAlmash(Holat, Ba):
73 89 3a b7 c7 5f 86 28 1d 16 d4 1c 80 3b 7c 73 cc 28 a1 d7 87 67 ec 11 cb e2 e4 52 38 84 44 e3
Qo`shBosqichKalit (Holat, K):
da 25 5c c2 61 4a 45 03 20 5b 41 9e 02 59 fb 96 65 f8 f3 ae 2c cb 1e 33 11 81 f1 52 74 42 43 11

6 –bosqich
Kalit K[6]:
da 2f ef 1d 6e 38 1f c0 0c 99 90 27 53 98 b8 27 ff ee d2 a4 d8 a4 8e 24 fe 50 d9 83 db ca ad f5
Sur(Holat):
ae 74 81 1e f1 33 da 42 25 43 52 61 20 4a 5c 11 c2 02 5b 45 41 03 65 59 f8 fb 9e 2c 11 cb f3 96
Aralash(Holat, K1D&K2):
5a 9f 4c c7 f2 50 06 f3 23 61 f3 9f 2c 80 9a cd 7e 5a 14 6b f5 77 a1 0d a2 bc d6 56 f1 8e 70 d2
BaytAlmash(Holat, Ba):

31 eb 5f 92 e8 a0 80 11 0e d0 11 eb 3e 54 0d d2 91 31 43 5c bd 21 aa c9 c0 c2 f8 49 9f 4d 75 d4
Qo`shBosqichKalit (Holat, K):
eb c4 b0 8f 86 98 9f d1 02 49 81 cc 6d cc b5 f5 6e df 91 f8 65 85 24 ed 3e 92 21 ca 44 87 d8 21

7 –bosqich
Kalit K[7]:
1d a9 38 2f 2b b7 3a c9 29 a5 b7 60 4c 30 22 a8 48 d3 ca ad 86 f0 16 cd 5c dd fc 80 83 82 73 b7
Sur(Holat):
f8 44 92 24 21 ed eb 87 c4 d8 ca 86 02 98 b0 21 8f 6d 49 9f 81 d1 6e cc df b5 cc 65 3e 85 91 f5
Aralash(Holat, K1D&K2):
8a 6a 2c 85 af c6 4b 35 7d 3b 53 9f d8 8e 32 e3 7d c7 15 27 2b 82 39 d6 9d a6 fc e3 e0 e9 6a a3
BaytAlmash(Holat, Ba):
09 a7 ac ba ab 87 25 5a 99 f3 56 06 a2 8f 5b 88 99 6c b7 aa dc 49 a9 7e 15 f9 04 88 d2 2d a7 a0
Qo`shBosqichKalit (Holat, K):
14 0e 94 95 80 30 1f 93 b0 56 e1 66 ee bf 79 20 d1 bf 7d 07 5a b9 bf b3 49 24 f8 08 51 af d4 17

8 –bosqich
Kalit K[8]:
7c 48 4d 5f d7 71 bf b9 78 df a5 b7 8b 1a 81 63 4a 0e 9d c2 38 38 13 80 47 6d bf ae a7 b3 e1 14
Sur(Holat):
07 51 24 bf f8 b3 14 af 0e d4 08 80 b0 30 94 17 95 ee 56 1f e1 93 d1 bf bf 79 66 5a 49 b9 7d 20
Aralash(Holat, K1D&K2):
98 ea 65 d8 80 bc fd 07 fc b8 cd ce d0 93 81 a8 ab 75 d5 f7 dd 33 87 7b 79 9b 1d 74 45 b2 e6 96
BaytAlmash(Holat, Ba):
fd 56 36 08 54 c2 01 26 98 2f d2 12 89 95 df 4b 65 53 f6 a4 e5 6f 40 37 67 a2 9e 8a 5d 5b f3 0f
Qo`shBosqichKalit (Holat, K):
81 1e 7b 57 83 b3 be 9f e0 f0 77 a5 02 8f 5e 28 2f 5d 6b 66 dd 57 53 b7 20 cf 21 24 fa e8 12 1b

Shifrmatn:
81 1e 7b 57 83 b3 be 9f e0 f0 77 a5 02 8f 5e 28 2f 5d 6b 66 dd 57 53 b7 20 cf 21 24 fa e8 12 1b

Rasshifrovkalash jarayoni

Kirishbloki (shifrmatn):
811e7b5783b3be9fe0f077a5028f5e282f5d6b66dd5753b720cf2124fae8121b
ShifrlashkalitiK:
37B60BBA0AB160CFDC18F50CDEE8E04530B3F8AF1432FE511FBB2029112F2145
Inisializasiyavektori IV:
2654BB5FA375D89854EA489F9AA88416FD4DEBBD9B3B40334829F9EE5234C37A
Baytalmashtirishmassivi Bsa1:
d3 a9 f3 9a fc 36 9f 45 59 8a 47 2f de 6f 0f 33 8b 97 b9 4d 3c 9d 3a d9 96 c2 63 b6 98 7e fa e2 60 bc fe d7 a5 4b b3
2d 13 b1 ff 71 0e e9 1f 3f ce d1 a0 ed 8d c8 24 41 23 22 65 e1 17 68 e8 c3 9e 5a 90 b5 c9 f7 79 d5 c5 82 80 c1 d0
07 44 be 6c 2a 49 e6 dc 66 53 5e 21 d4 35 32 0b df 72 77 cd bf 4a 00 05 9c 52 d2 7c 29 03 ec c7 8f 18 34 f5 50 b4
76 08 67 57 99 cc 0c 54 ad 75 ee d6 64 78 40 0d ab 58 ef 09 c6 e3 1d bd 5f 31 1e aa 8e b0 48 f0 5b 2e 4f 46 61 5c
7d 7b e7 1c 4c 26 f6 a3 f4 d8 19 93 e4 20 6a 89 39 27 af 2c 88 43 1b 70 ae a2 73 ea a1 83 15 55 a4 85 94 95 6e f8
ba 51 8c c0 fb 38 3e b8 e5 01 12 87 1a 62 cb dd ca cf 25 e0 fd a7 eb b2 11 3d 74 5d 69 2b 86 37 4e 0a 7f 81 db 56
30 7a 06 10 6b f1 9b c4 b7 02 a8 6d f2 da 3b bb 84 91 28 ac a6 14 92 16 04 42 f9
Baytalmashtirishmassivi Bsa2:
db fd 21 2d 94 b5 a4 27 d8 be 3e bb 7c 9a 23 96 13 f3 ce e8 b6 fb 52 24 60 32 00 e1 8d 34 c1 76 6e 77 b7 cc 2f ae
07 12 d3 c8 88 d1 55 7d 9c b8 57 5a 0a c9 5c bf 65 7b 82 da 9e f0 5d c3 2c 44 87 73 48 14 84 90 f8 b4 7f 56 ac a8
15 8e f4 47 a7 c6 e0 75 80 a3 ea 46 6c a0 aa b2 6b 45 ee 4c e7 28 89 78 10 ab 4e 79 37 d9 cf 99 16 67 ed 33 91 4b
51 83 7a 70 b3 bd 3b 11 2e c4 eb 20 71 0b 06 b9 64 25 2a ef 6d 72 df d0 74 0c 31 49 1f d7 c0 7e c7 9d f6 93 02 05
fc 59 ba 17 54 cb 1d f1 50 03 9b 40 f7 dc 04 3f 01 af a1 4d 19 53 86 8f ca 85 1c 38 41 b1 fe 69 36 e5 f9 58 97 f5 30
e4 a2 08 bc 0f 18 8b 6a 22 b0 0d 4a 26 66 3d 5b 63 61 3c cd 5f d2 1e 68 a9 1a 4f e3 3a 92 d4 ec 81 29 a6 de ad 6f
dd 39 ff f2 c2 1b 9f 95 a5 fa 62 0e 42 09 e6 c5 8c d5 35 d6 e2 2b 8a 43 98 5e e9
Boshlang'ichbosqichkalit K[0]:
7c 48 4d 5f d7 71 bf b9 78 df a5 b7 8b 1a 81 63 4a 0e 9d c2 38 38 13 80 47 6d bf ae a7 b3 e1 14
Qo'shBosqichKalit(Holat, K[0]:)
fd 56 36 08 54 c2 01 26 98 2f d2 12 89 95 df 4b 65 53 f6 a4 e5 6f 40 37 67 a2 9e 8a 5d 5b f3 0f

1- bosqich
Kalit K[1]:
1d a9 38 2f 2b b7 3a c9 29 a5 b7 60 4c 30 22 a8 48 d3 ca ad 86 f0 16 cd 5c dd fc 80 83 82 73 b7

BaytAlmash(Holat, Ba):
98 ea 65 d8 80 bc fd 07 fc b8 cd ce d0 93 81 a8 ab 75 d5 f7 dd 33 87 7b 79 9b 1d 74 45 b2 e6 96
Aralash(Holat, K1&K2D):
07 51 24 bf f8 b3 14 af 0e d4 08 80 b0 30 94 17 95 ee 56 1f e1 93 d1 bf bf 79 66 5a 49 b9 7d 20
Sur(Holat):
14 0e 94 95 80 30 1f 93 b0 56 e1 66 ee bf 79 20 d1 bf 7d 07 5a b9 bf b3 49 24 f8 08 51 af d4 17
Qo‘shBosqichKalit(Holat, K):
09 a7 ac ba ab 87 25 5a 99 f3 56 06 a2 8f 5b 88 99 6c b7 aa dc 49 a9 7e 15 f9 04 88 d2 2d a7 a0

2 - bosqich
Kalit K[2]:
da 2f ef 1d 6e 38 1f c0 0c 99 90 27 53 98 b8 27 ff ee d2 a4 d8 a4 8e 24 fe 50 d9 83 db ca ad f5
BaytAlmash(Holat, Ba):
8a 6a 2c 85 af c6 4b 35 7d 3b 53 9f d8 8e 32 e3 7d c7 15 27 2b 82 39 d6 9d a6 fc e3 e0 e9 6a a3
Aralash(Holat, K1&K2D):
f8 44 92 24 21 ed eb 87 c4 d8 ca 86 02 98 b0 21 8f 6d 49 9f 81 d1 6e cc df b5 cc 65 3e 85 91 f5
Sur(Holat):
eb c4 b0 8f 86 98 9f d1 02 49 81 cc 6d cc b5 f5 6e df 91 f8 65 85 24 ed 3e 92 21 ca 44 87 d8 21
Qo‘shBosqichKalit(Holat, K):
31 eb 5f 92 e8 a0 80 11 0e d0 11 eb 3e 54 0d d2 91 31 43 5c bd 21 aa c9 c0 c2 f8 49 9f 4d 75 d4

3 - bosqich
Kalit K[3]:
a9 ac 66 75 a6 15 c3 2b 3d 4d 95 82 82 62 87 e5 a9 d0 52 79 ab ac f2 22 da 63 15 00 4c c6 07 f2
BaytAlmash(Holat, Ba):
5a 9f 4c c7 f2 50 06 f3 23 61 f3 9f 2c 80 9a cd 7e 5a 14 6b f5 77 a1 0d a2 bc d6 56 f1 8e 70 d2
Aralash(Holat, K1&K2D):
ae 74 81 1e f1 33 da 42 25 43 52 61 20 4a 5c 11 c2 02 5b 45 41 03 65 59 f8 fb 9e 2c 11 cb f3 96
Sur(Holat):
da 25 5c c2 61 4a 45 03 20 5b 41 9e 02 59 fb 96 65 f8 f3 ae 2c cb 1e 33 11 81 f1 52 74 42 43 11
Qo‘shBosqichKalit(Holat, K):
73 89 3a b7 c7 5f 86 28 1d 16 d4 1c 80 3b 7c 73 cc 28 a1 d7 87 67 ec 11 cb e2 e4 52 38 84 44 e3

4 - bosqich
Kalit K[4]:
c8 f1 91 b3 2f d8 e3 8e 13 6a 63 7f fd ea b5 f2 6c d5 91 c7 9d c6 d9 49 a0 aa fa db af 87 0f 47
BaytAlmash(Holat, Ba):
76 1d 65 15 e5 77 09 13 7e 3a a7 98 78 e1 75 76 62 13 f4 11 c6 d2 c4 97 1a 81 56 49 23 58 c9 db
Aralash(Holat, K1&K2D):
d5 cf 03 cd 6f b4 69 fd 3c 0a 52 76 f9 f2 2c d5 10 18 5c cb 88 3c f3 39 d6 8a 59 25 7d c4 50 69
Sur(Holat):
69 3c 2c 10 76 f2 cb 3c f9 5c 88 59 18 39 8a 69 f3 d6 50 d5 25 c4 cd b4 7d 03 6f 52 cf fd 0a d5
Qo‘shBosqichKalit(Holat, K):
a1 cd bd a3 59 2a 28 b2 ea 36 eb 26 e5 d3 3f 9b 9f 03 c1 12 b8 02 14 fd dd a9 95 89 60 7a 05 92

5 - bosqich
Kalit K[5]:
d5 88 7f f9 8a 6b 27 00 5c 98 10 c6 9b b9 55 a6 45 91 d2 01 dd 28 15 c6 35 4f 9a 2b 6f da 88 2d
BaytAlmash(Holat, Ba):
03 3d f5 40 a0 88 d3 1c 1b 65 9f 07 dd 5f 44 17 f1 2d 08 ce 36 21 b6 98 d4 af 93 d0 e7 2e b5 c7
Aralash(Holat, K1&K2D):
c3 d5 c1 d5 39 d2 bc 75 71 f3 93 1d 09 c8 71 17 cd 63 d0 86 86 a3 e0 a8 f4 81 8d 70 e3 d4 bd e3
Sur(Holat):
bc 71 71 cd 1d c8 86 a3 09 d0 86 8d 63 a8 81 e3 e0 f4 bd c3 70 d4 d5 d2 e3 c1 39 93 d5 75 f3 17
Qo‘shBosqichKalit(Holat, K):
69 f9 0e 34 97 a3 a1 a3 55 48 96 4b f8 11 d4 45 a5 65 6f c2 ad fc c0 14 d6 8e a3 b8 ba af 7b 3a

6 - bosqich
Kalit K[6]:
c8 ff 04 8f bf 9c 9a e9 bd ff 47 93 b9 fc d7 a5 7b 17 8f 51 a5 53 a7 76 49 95 4d 2c d3 3b 22 14
BaytAlmash(Holat, Ba):
29 a6 0f 8d 61 19 f4 19 66 c5 46 c1 ac 97 a7 f7 e4 9c 34 c0 88 16 51 3c b2 aa 19 55 85 1b ad 65

Aralash(Holat, K1&K2D):
ce 27 04 a1 b6 3c c5 ee c9 6d 8d 94 0b 46 d8 fc ec a1 1b 40 0e 5d 0b 42 72 d3 2e b5 57 45 30 4d
Sur(Holat):
c5 c9 d8 ec 94 46 40 5d 0b 1b 0e 2e a1 42 d3 4d 0b 72 30 ce b5 45 a1 3c 57 04 b6 8d 27 ee 6d fc
Qo‘shBosqichKalit(Holat, K):
0d 36 dc 63 2b da da b4 b6 e4 49 bd 18 be 04 e8 70 65 bf 9f 10 16 06 4a 1e 91 fb a1 f4 d5 4f e8

7 - bosqich
Kalit K[7]:
62 6b 46 c8 f1 a6 98 06 da 9b 43 6e 29 83 19 2e 40 17 22 83 fc 6c 80 65 32 6b a8 0b d5 0d c4 63
BaytAlmash(Holat, Ba):
9a 65 92 78 d1 e3 e3 41 fe 6f 56 f5 60 30 94 f2 91 ab e4 f1 13 52 a4 ac c1 7e 8a 03 c5 1e 47 f2
Aralash(Holat, K1&K2D):
e2 6a c3 90 2b 51 45 9b 78 46 26 9f 7c ac 20 ba 61 c7 85 a3 57 ed 6d d0 a1 10 07 a3 bf be 66 a2
Sur(Holat):
45 78 20 61 9f ac a3 ed 7c 85 57 07 c7 d0 10 a2 6d a1 66 e2 a3 be 90 51 bf c3 2b 26 6a 9b 46 ba
Qo‘shBosqichKalit(Holat, K):
27 13 66 a9 6e 0a 3b eb a6 1e 14 69 ee 53 09 8c 2d b6 44 61 5f d2 10 34 8d a8 83 2d bf 96 82 d9

8 - bosqich
Kalit K[8]:
36 6d 33 2b 76 ee 69 4b ae 0f 32 55 17 7d 24 22 80 e4 3b 2c ac 15 0e 68 06 4d 04 55 15 5f 49 da
BaytAlmash(Holat, Ba):
2d 4d 52 39 18 47 e1 9b 20 fa 3c 29 02 e6 8a 31 e9 83 c9 bf 77 e0 8b 8d 1e 89 ab e9 ba 46 0d 74
Aralash(Holat, K1&K2D):
a2 04 5d 78 bc 6c 20 2f 08 cf f9 e1 c2 ae ba e6 47 ce dc 87 3b e4 4d 91 98 e5 88 03 76 1b e2 72
Sur(Holat):
20 08 ba 47 e1 ae 87 e4 c2 dc 3b 88 ce 91 e5 72 4d 98 e2 a2 03 1b 78 6c 76 5d bc f9 04 2f cf e6
Qo‘shBosqichKalit(Holat, K):
16 65 89 6c 97 40 ee af 6c d3 09 dd d9 ec c1 50 cd 7c d9 8e af 0e 76 04 70 10 b8 ac 11 70 86 3c

Holatn:
26 54 bb 5f a3 75 d8 98 54 ea 48 9f 9a a8 84 16 fd 4d eb bd 9b 3b 40 33 48 29 f9 ee 52 34 c3 7a
Qo`shHolat(Holat, Holatn):
30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46

Ochiqmatn:
30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46

11-ilova

O‘z DSt 1105:2009 algoritmi bardoshligini algebraik kriptotahlil usuli yordamida baholash jarayonida $BaytAlmash()$ akslantirishi uchun qurilgan algebraik tenglamalardan biri

$$y_1 \oplus x_8x_7x_6x_5x_4x_3x_2 \oplus x_8x_7x_6x_5x_4x_2x_1 \oplus x_8x_7x_6x_5x_4x_2 \oplus x_8x_7x_6x_5x_4x_1 \oplus x_8x_7x_6x_5x_2 \oplus x_8x_7x_6x_5x_1 \oplus x_8x_7x_6x_5 \oplus x_8x_7x_6x_4x_3x_2x_1 \oplus x_8x_7x_6x_4x_3x_2 \oplus x_8x_7x_6x_4x_3x_1 \oplus x_8x_7x_6x_4x_3 \oplus x_8x_7x_6x_4x_2x_1 \oplus x_8x_7x_6x_4 \oplus x_8x_7x_6x_4x_3x_1 \oplus x_8x_7x_6x_3x_2 \oplus x_8x_7x_6x_3x_1 \oplus x_8x_7x_6x_3 \oplus x_8x_7x_6x_2 \oplus x_8x_7x_6x_5 \oplus x_8x_7x_5x_4x_3x_1 \oplus x_8x_7x_5x_4x_3 \oplus x_8x_7x_5x_4 \oplus x_8x_7x_5x_4 \oplus x_8x_7x_5x_3x_2x_1 \oplus x_8x_7x_5x_4x_3x_1 \oplus x_8x_7x_5x_3 \oplus x_8x_7x_6x_5x_2 \oplus x_8x_7x_5x_1 \oplus x_8x_7x_4x_3x_1 \oplus x_8x_7x_4x_3 \oplus x_8x_7x_4x_2 \oplus x_8x_7x_4x_1 \oplus x_8x_7x_4 \oplus x_8x_6x_5x_4x_3x_2 \oplus x_8x_6x_5x_4x_3x_1 \oplus x_8x_6x_5x_4x_3 \oplus x_8x_6x_5x_4x_2x_1 \oplus x_8x_6x_5x_4x_2 \oplus x_8x_6x_5x_4x_1 \oplus x_8x_6x_5x_3x_1 \oplus x_8x_6x_5x_2x_1 \oplus x_8x_6x_5x_2 \oplus x_8x_6x_5x_1 \oplus x_8x_6x_4x_2 \oplus x_8x_6x_4x_1 \oplus x_8x_6x_3x_2 \oplus x_8x_6x_3x_1 \oplus x_8x_6x_3 \oplus x_8x_6 \oplus x_8x_5x_4x_3x_2 \oplus x_8x_5x_4x_3 \oplus x_8x_5x_4x_2x_1 \oplus x_8x_5x_4x_2 \oplus x_8x_5x_4 \oplus x_8x_5x_3x_1 \oplus x_8x_5x_3 \oplus x_8x_5x_2x_1 \oplus x_8x_5x_1 \oplus x_8x_4x_3x_2x_1 \oplus x_8x_4x_3x_2 \oplus x_8x_4x_3x_1 \oplus x_8x_4x_2x_1 \oplus x_8x_4x_2 \oplus x_8x_3 \oplus x_7x_6x_5x_4x_3x_2 \oplus x_7x_6x_5x_4x_3x_1 \oplus x_7x_6x_5x_4x_3 \oplus x_7x_6x_5x_4x_2 \oplus x_7x_6x_5x_4 \oplus x_7x_6x_5x_3x_1 \oplus x_7x_6x_5x_2x_1 \oplus x_7x_6x_5x_1 \oplus x_7x_6x_5 \oplus x_7x_6x_4x_3x_2 \oplus x_7x_6x_4x_3 \oplus x_7x_6x_4x_2 \oplus x_7x_6x_4x_1 \oplus x_7x_6x_3x_2x_1 \oplus x_7x_6x_2x_1 \oplus x_7x_6 \oplus x_7x_5x_4x_3x_2x_1 \oplus x_7x_6x_4x_3 \oplus x_7x_5x_4x_2x_1 \oplus x_7x_5x_4 \oplus x_7x_5x_3x_2x_1 \oplus x_7x_5x_3x_2 \oplus x_7x_5x_2x_1 \oplus x_7x_5x_1 \oplus x_7x_4x_3x_2 \oplus x_7x_4x_3x_1 \oplus x_7x_4x_3 \oplus x_7x_4x_2x_1 \oplus x_7x_3x_2 \oplus x_7x_2x_1 \oplus x_7x_2 \oplus x_7x_1 \oplus x_6x_5x_4x_3x_1 \oplus x_6x_5x_4x_3x_2x_1 \oplus x_6x_5x_3x_2 \oplus x_6x_5x_2 \oplus x_6x_5x_1 \oplus x_6x_5 \oplus x_6x_4x_3x_2x_1 \oplus x_6x_4x_3x_2 \oplus x_6x_4x_3x_1 \oplus x_6x_4x_2x_1 \oplus x_6x_4 \oplus x_6x_3x_2 \oplus x_6x_2x_1 \oplus x_6x_1 \oplus x_5x_4x_3x_2 \oplus x_5x_4x_2x_1 \oplus x_5x_4x_2 \oplus x_5x_4x_1 \oplus x_5x_4 \oplus x_5x_3x_2 \oplus x_5x_3 \oplus x_5x_2x_1 \oplus x_5x_1 \oplus x_4x_3x_2 \oplus x_4x_3x_1 \oplus x_4x_2 \oplus x_4x_1 \oplus x_4 \oplus x_3x_2x_1 \oplus x_3x_2 \oplus x_2x_1 \oplus x_2 = 0.deg=7$$

MUNDARIJA

O. Allanov, I. Boyquziyev, N. Safoyev

SIMMETRIK SHIFRLASH ALGORITMINI TAKOMILLASHTIRISH VA KRIPTOTAHLIL USULLARI YORDAMIDA BAHOLASH

MONOGRAFIYA

Muharrir: Sh. Bazarova
Badiiy muharrir: K. Boyxo‘jayev
Kompyuterda sahifalovchi: K. Boyxo‘jayev

Nashr. lits. AI № 305.
Bosishga ruxsat 22.04.2022-yilda berildi.
Bichimi 60x84/16. Ofset qog‘ozi.
«New Times Roman» garniturasi.
Shartli b.t.14,7. Nashr hisob t.15,3.
Adadi 100 dona. 3-buyurtma.

“IQTISOD-MOLIYA” nashriyoti.
100000, Toshkent, Amir Temur, 60«A».

“HUMO-ISTIQLOL PRESS” MChJ
bosmaxonasida chop etildi.
100198, Toshkent, Amir temur, 60 “A”.