O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKASIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

A.O.Po‘latovna, X.P.Hasanov,
M.H. Nazarova, I.U.Xolimtayeva, O.D.Nuritdinov.

AXBOROT XAVFSIZLIGI PROTOKOLLARI

(O‘quv qo‘llanma)

Toshkent – 2019

UO'K: 003.26:004.057.4
KBK: 32.973.202-018.2
A 90

A.O.Po'latovna, X.P.Hasanov, M.H. Nazarova, I.U.Xolimtayeva, O.D.Nuritdinov. Axborot xavfsizligi protokollari. O'quv qo'llanma. – T.: 2018 – 168 bet.

ISBN 978–9943–5570–2–4

Ushbu o'quv qo'llanmada axborot xavfsizligini ta'minlashda foydalaniladigan kriptografik protokollar, ularda qo'llaniladigan asosiy atamalar va ta'riflar, kriptografik protokollar nazariyasi asoslari, kriptografik protokollar funksiyalari va protokol xavfsizligiga oid talablar bayon etilgan.

O'quv qo'llanmada autentifikasiya protokollari, kalitlarni taqsimlash protokollari va ularning xossalari, e'lon qilinganligi nolga tengligi tushunchasi, matematik masalalarni yechish protokollari va shartnoma imzolash protokollari haqidagi ma'lumotlar keltirilgan.

Ushbu o'quv qo'llanma Muhammad al-Xorazmiy nomidagi TATU axborot xavfsizligi yo'nalishida ta'lim olayotgan bakalavrlar uchun mo'ljallangan. Shuningdek ushbu o'quv qo'llanmadan axborot xavfsizligi va kriptografiya yo'nalishida ilmiy-tadqiqot olib borayotgan tadqiqotchilar, ilmiy xodimlar va soha mutaxassislari foydalanishlari mumkin.

O'quv qo'llanma Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti ilmiy-uslubiy kengashining qarori bilan chop etishga tavsiya etildi.

UO'K: 003.26:004.057.4
KBK: 32.973.202-018.2

Taqrizchilar: B.F.Abdurahimov;
K.A.Tashev.

Mas'ul muharrir: O.P.Ahmedov.

ISBN 978–9943–5570–2–4

BELGILASHLAR VA QISQARTMALAR

1.	**A**	Alisa - barcha protokollarning birinchi ishtirokchisi.
2.	**AP**	Autentifikasiya protokoli.
3.	**V**	Bob - barcha protokollarning ikkinchi ishtirokchisi.
4.	**VB**	Vaqt belgisi.
5.	**D**	Deyv - to'rt tomonli protokollar ishtirokchisi.
6.	**E**	Yeva – passiv buzg'unchi.
7.	**JERI**	Jamoaviy elektron raqamli imzo.
8.	**K**	Kerol - uch va to'rt tomonli protokollar ishtirokchisi.
9.	**KP**	Kriptografik protokol.
10.	**KROM**	Kalitlarni ro'yxatga olish markazi.
11.	**IM**	Ishonchli manba
12.	**M**	Mellori - yomon niyatli aktiv buzg'unchi.
13.	**R**	Isbotlovchi ishtirokchi.
14.	**V**	Tekshiruvchi ishtirokchi.
15.	**ERI**	Elektron raqamli imzo.
16.	**EECh**	Elliptik egri chiziq.
17.	**T**	Trent - ishonchli vositachi.
18.	**TSh**	To'lov shlyuzi
19.	**XOR**	2 modul bo'yicha qo'shish.

KIRISH

So‘nggi yillarda O‘zbekiston Respublikasida axborot xavfsizligini ta’minlashga, dasturiy va apparat-dasturiy vositalarni mahalliylashtirishga davlatimiz rahbariyati tomonidan katta ahamiyat berilmoqda. Bunga qabul qilingan bir nechta qonun va normativ hujjatlar, jumladan, «Axborotlashtirish to‘g‘risida»gi, «Elektron hujjat aylanishi to‘g‘risida»gi, «Elektron raqamli imzo to‘g‘risida»gi Qonunlar misol bo‘lishi mumkin.

Hozirgi kunga qadar axborot xavfsizligini ta’minlashda eng ishonchli vositalardan biri axborotni kriptografik muhofazalash vositalari hisoblanadi. O‘zbekiston Respublikasi Prezidentining 2007 yil 3- apreldagi «O‘zbekiston Respublikasida axborotning kriptografik muhofazasini tashkil etish chora-tadbirlari to‘g‘risida»gi [1] PQ-614–son qarorining asosiy vazifalaridan biri axborotning kriptografik muhofazasi sohasida yuqori malakali kadrlarni tayyorlashdan iborat. Shuningdek O‘zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida” gi PF-4947- son farmoyishida beshta ustuvor yo‘nalishdan biri sifatida axborot xavfsizligini ta’minlash bo‘yicha ishlarni jadallashtirish ko‘zda tutilgan. Buning uchun axborot xavfsizligi va kriptografiya yo‘nalishida davlat tilida ta’lim olayotgan talabalar, tadqiqotchilar va ilmiy xodimlar uchun mo‘ljallangan o‘quv va uslubiy qo‘llanmalar, darsliklar va kitoblar ishlab chiqish muhim ahamiyat kasb etadi.

Bitiruvchilarning bilimi, malaka va ko‘nikmalariga qo‘yilgan talablarni, mamlakatdagi ijtimoiy-iqtisodiy o‘zgarishlarni va axborot xavfsizligini intensiv rivojlanishini inobatga olgan holda va 5330500 – «Axborot xavfsizligi» yo‘nalishida tayyorlanayotgan kadrlarning bilim, malaka va ko‘nikmalarini yanada mustahkamlash maqsadida o‘zbek tilidagi «Axborot xavfsizligi protokollari» o‘quv qo‘llanmasini ishlab chiqish maqsadga muvofiq hisoblanadi. Hozirgi kunda ««Axborot xavfsizligi protokollari» fanidan o‘zbek tilidagi o‘quv qo‘llanmasi nashr etilmaganligi mazkur o‘quv qo‘llanmani ishlab chiqish vazifasi dolzarbligidan dalolat beradi.

O‘zbek tilida «Axborot xavfsizligi protokollari» o‘quv qo‘llanmasini ishlab chiqishdan maqsad talabalarni asosiy axborot xavfsizligini ta’minlashga xizmat qiluvchi kriptografik protokollar va ularning vazifalari, protokollarga oid xavfsizlik talablari, kalitlarni taqsimlash protokollari va protokollarga qilinadigan hujum turlari bilan tanishtirishdan iborat.

O‘quv qo‘llanmasini ishlab chiqish jarayonida ko‘zlangan maqsadga erishish uchun quyidagi vazifalar bajarildi: axborot xavfsizligi va kriptografiya yo‘nalishidagi mavjud ta’lim standartlari va o‘quv-metodik hujjatlarni hamda shu yo‘nalishda ishlab chiqilgan o‘quv qo‘llanmalar, darsliklar, kitoblar, sohada qilingan ilmiy ishlar o‘rganib tahlil qilib chiqildi.

O‘quv qo‘llanmasini ishlab chiqish uchun dastlabki ma’lumotlar bo‘lib O‘zbekiston Respublikasining Qonun hujjatlari, davlat standartlari, shu jumladan axborot xavfsizligi va kriptografiya yo‘nalishidagi mavjud ta’lim standartlari va o‘quv-metodik hujjatlar xizmat qildi. Ushbu o‘quv qo‘llanma «5330500 – Axborot xavfsizligi ta’lim yo‘nalishi bo‘yicha bakalavrlarning tayyorgarlik darajasi va zaruriy bilimlar mazmuniga qo‘yiladigan TALABLAR» O‘zbekiston davlat ta’lim standarti [2] va o‘quv dasturiga muvofiq ishlab chiqildi.

O‘quv qo‘llanmaning birinchi “Axborot xavfsizligini ta’minlash protokollari” bo‘limida kriptografik protokollarda qo‘llaniladigan asosiy atamalar va ta’riflar, kriptografik protokollar nazariyasi asoslari, kriptografik protokollar vazifalari va protokol xavfsizligiga oid talablar bayon etildi.

O‘quv qo‘llanmaning ikkinchi “Autentifikasiya protokollari” bo‘limida autentifikasiyaga oid asosiy tushunchalar, protokollarga qilinadigan hujum turlari, parol yordamidagi autentifikasiya va xavfsizlikni ta’minlaydigan autentifikasiya protokollari bayon etildi.

O‘quv qo‘llanmaning uchinchi “Kalitlarni taqsimlash protokollari” bo‘limida kalitlarni taqsimlash protokollarining xossalari, simmetrik kriptotizimlarga asoslangan kalitlarni taqsimlash protokollari, nosimmetrik kriptotizimlarga asoslangan kalitlarni taqsimlash protokollari va kalitlarni taqsimlash protokollarini tahlillash usullari yoritildi.

O‘quv qo‘llanmaning to‘rtinchi “E’lon qilinganligi nolga teng bo‘lgan protokollar” bo‘limida e’lon qilinganligi nolga tengligi tushunchasi, matematik masalalarni yechish protokollari va kontrakt imzolash protokollari haqidagi ma’lumotlar bayon etildi.

Har bir bo‘limdan keyin nazorat savollari keltirildi.

Taqdim etilayotgan o‘quv qo‘llanma axborot xavfsizligi yo‘nalishida ta’lim olayotgan bakalavrlar uchun mo‘ljallangan. Shuningdek, ushbu o‘quv qo‘llanmadan axborot xavfsizligi va kriptografiya yo‘nalishida ilmiy-tadqiqot olib borayotgan tadqiqotchilar, ilmiy xodimlar va soha mutaxassislari foydalanishlari mumkin.

1. AXBOROT XAVFSIZLIGINI TA'MINLASH PROTOKOLLARI

1.1. Boshlang'ich tushunchalar

Har qanday soha va yo'nalish haqida to'liq ma'lumotga ega bo'lish uchun dastlab shu soha va yo'nalishning asosiy tushunchalari bilan tanishmoq lozim [3]. Kriptologiya haqida to'liqroq ma'lumotga ega bo'lish uchun quyidagi keltirilgan atamalar va ularning ta'riflari muhim ahamiyatga ega.

Axborotning, unga bo'ladigan tabiiy yoki sun'iy tusdagi tahdidlarning ta'siri sharoitida, uning yaxlitligini, konfidensialligini, ishonchliligini, haqiqiyligini va undan foydalana olishni ta'minlovchi usullar va vositalarning yig'indisi *axborotni muhofaza qilish* deyiladi [3].

Kriptologiya kriptografik almashtirishlarni o'rganuvchi bilimlar sohasi bo'lib, u ikki yo'nalishni – kriptografiya va kriptotahlilni o'z ichiga oladi [3]. Kriptologiya grekchada *kryptos* - "sirli" va *logos* -"so'z" degan ma'noni bildiradi [3-6].

Kriptografiya axborot mazmunidan ruxsat etilmagan tarzda foydalanishdan muhofaza qilish, uni soxtalashtirish imkoniyatini yo'qqa chiqarish maqsadida axborotni almashtirish tamoyillari, vositalari va usullarini o'rganadigan bilimlar sohasidir [3].

Kriptotahlil shifrni yoki istalgan boshqa shakldagi kriptografiya obyektining sirini ochish san'ati va ilmi bo'lib, kalitni bilmasdan turib shifrlangan matndan dastlabki matnni olish yoki dastlabki matn va shifrlangan matn bo'yicha kalitni hisoblash jarayonidir [3].

Kalitdan foydalangan holda alohida qoidalar bo'yicha ochiq (dastlabki) ma'lumotlar to'plamini shifrlangan ma'lumotlar to'plamiga almashtirish uchun amalga oshiriladigan qaytar almashtirishlar majmui *shifr* deb ataladi [3].

Dastlabki ochiq matnni uning ma'nosini berkitish maqsadida shifrlangan ma'lumotga o'girish natijasi *shifrmatn* (shifrma'lumot) deb ataladi [3].

Shifrmatnga o'girish yoki dastlabki matnga o'girish jarayoni *axborotni shifrlash* deyiladi [3].

Dastlabki ma'lumotlar (axborotlar)ni shifr (kalit) yordamida shifrlangan ma'lumotlarga almashtirish jarayoni *ma'lumotlarni shifrmatnga o'girish (yoki tor ma'noda shifrlash) jarayoni* deyiladi [3-6].

Dastlabki matnni shifrlangan matndan shifrlash kalitini bilmasdan turib tiklash bilan tugaydigan kriptotahlil jarayoni *shifrni kalitsiz ochish (keng ma'noda deshifrlash)* deb ataladi [3-6].

Nosimmetrik shifr deb shifrlashning maxfiy kaliti dastlabki matnga o'girishning ochiq kaliti bilan mos tushmaydigan va ochiq kalit asosida hisoblab chiqarilishi murakkab bo'lgan shifrga aytiladi.

Simmetrik shifr esa shifrlash va dastlabki matnga o'girish uchun aynan bir kalitdan yoki turli kalitlardan foydalaniladigan, ularning biri bo'yicha boshqasi oson topiladigan shifrdir.

Muhofaza qilinadigan axborot deganda mulkka egalik predmeti hisoblanadigan va huquqiy hujjatlar talablariga yoki axborot mulkdori tomonidan belgilanadigan talablarga muvofiq muhofaza qilinishi zarur bo'lgan axborot tushuniladi [3].

Axborotni yo'qolishdan muhofaza qilish deb muhofaza qilinadigan axborotning oshkor bo'lishi natijasida nazorat qilib bo'lmaydigan darajada tarqalishining, axborotdan ruxsat etilmagan tarzda foydalanish va muhofaza qilinadigan axborotning razvedka tomonidan qo'lga kiritilishini bartaraf etishga qaratilgan faoliyatga aytiladi [3-6].

Axborotni ruxsat etilmagan ta'sirdan muhofaza qilish deganda muhofaza qilinadigan axborotga axborotni o'zgartirishga belgilangan huquqlarni va/yoki qoidalarni buzgan holda, axborotning buzilishiga, yo'q qilinishiga, undan nusxa ko'chirilishiga, axborotdan foydalanishga to'sqinlik qilish, shuningdek axborot eltuvchisining yo'qolishiga, yo'q qilinishiga yoki ishida uzilishga olib keladigan ta'sirni bartaraf qilishga qaratilgan faoliyat tushuniladi [3-6].

Axborotni oshkor qilishdan muhofaza qilish esa muhofaza qilinadigan axborotning bu axborotdan foydalanish huquqiga ega bo'lmagan iste'molchilarga ruxsat etilmagan tarzda yetkazilishini bartaraf qilishga qaratilgan faoliyatdir [3].

Axborotni muhofaza qilish tizimi deganda axborotni muhofaza qilish sohasiga tegishli huquqiy, tashkiliy-tartibiy va me'yoriy hujjatlar bilan belgilangan qoidalar bo'yicha tashkil qilingan va faoliyat ko'rsatadigan organlar va/yoki ijro etuvchilar, ular tomonidan foydalaniladigan axborotni muhofaza qilish texnikasining yig'indisi tushuniladi.

Axborotni muhofaza qilish usuli deb axborotni muhofaza qilishning muayyan qoidalari (tamoyillari) va vositalarini qo'llash tartibi hamda qoidalariga aytiladi [3].

Axborotni muhofaza qilish samaradorligini nazorat qilish uchun mo'ljallangan yoki foydalaniladigan texnik va dasturiy vosita, buyum va/yoki material *axborotni muhofaza qilish vositasi* hisoblanadi.

Algoritm deganda masalani cheklangan qadamlarda yechish uchun aniq belgilangan qoidalarning tartiblangan chekli to'plami tushuniladi [3].

Axborotni soxtalashtirish imkoniyatini yo'qqa chiqarish va undan ruxsat etilmagan tarzda foydalanishdan muhofaza qilish maqsadida axborotni almashtirishning matematik algoritmi *kriptografik algoritm* deb ataladi [3].

Ma'lum bir natijaga erishish maqsadida ikki va undan ko'p subyekt tomonidan berilgan ketma-ketlikda bajariladigan harakatlar (yo'riqnomalar, buyruqlar, hisoblashlar, algoritmlar) to'plami *protokol* deyiladi.

Kriptoalgoritmdan va shifrlash kalitlaridan foydalanishni belgilab beradigan qoidalar va proseduralar to'plami *kriptografik protokol* deb ataladi [3].

Kriptografik tizim deganda kriptoalgoritmlar, protokollar va kalitlarni boshqarish tartibotlarining to'plami tushuniladi.

Kriptografik almashtirishlar algoritmlari yordamida axborotni ruxsat etilmagan tarzda foydalanish va almashtirishdan muhofaza qilish *kriptografik muhofaza* hisoblanib, masalan uzoqdan bank xizmatini ko'rsatish tizimlarida kriptografik muhofaza qilish uchun elektron raqamli imzo (ERI)dan va uzatiladigan axborotni shifrlashdan foydalaniladi.

Ochiq kalitli kriptotizim (nosimmetrik kriptotizim) ikkita - maxfiy va oshkora kalitdan foydalaniladigan kriptografik tizim bo'lib, kalitlardan hyech birini maqbul tushadigan vaqt ichida boshqasidan hisoblab chiqarish

mumkin bo'lmaydi. Maxfiy kalit sir saqlanishi zarur, oshkora kalit esa, o'zaro hamkorlikni amalga oshiruvchi barcha abonentlarga tarqatilishi mumkin [3].

Simmetrik kriptotizim (maxfiy kalitli kriptotizim) shunday kriptografik tizimki, bunda bitta kriptografik kalitdan axborotni shifrmatnga o'girish va shifrmatnni dastlabki matnga o'girish uchun foydalaniladi. Bunday kriptotizimlar bir kalitli yoki klassik deb ham ataladi [3].

Parametrlarning bir qismi maxfiy holda bo'lgan kriptografik algoritm bo'yicha ma'lumotlarni almashtirish *kriptografik almashtirish* deyiladi. Ma'lumotlarni shifrlash, ma'lumotlarni xeshlash yoki ERIni shakllantirish, imitoqistirmalar, maxsus kriptografik nazorat yig'indilarini hisoblashlar kabi kriptografik masalalardan birini hal etish uchun axborotni maxsus almashtirish tartiboti hisoblanadi [3].

Axborotni muhofaza qilishni shifrlash va/yoki ERI qoidalariga asoslangan usuli *axborotni muhofaza qilishning kriptografik usuli* deyiladi. Kriptografik usul ham dasturiy, ham apparat vositalari orqali amalga oshirilishi mumkin.

Dastlabki matnni shifrlangan matnga va/yoki aksincha, almashtirish bo'yicha kalitli o'zgaruvchi (shifrlash kaliti)ga bog'liq bo'lgan amallar mazmuni va ketma-ketligini belgilovchi kriptografik algoritm *ma'lumotlarni shifrlash algoritmi* deyiladi [3].

ERI algoritmi bu muhofaza qilinmaydigan umumiy foydalanishdagi telekommunikasiya kanallari orqali uzatiladigan xabar (elektron hujjat) ostidagi ERIni shakllantirish va uning haqiqiyligini tasdiqlash uchun mo'ljallangan kriptografik algoritmdir [3].

Chekli uzunlikdagi bitlarning dastlabki ketma-ketligini belgilangan uzunlikdagi bitlarning ketma-ketligiga almashtiruvchi kriptografik algoritm *xeshlash algoritmi* deyiladi.

Xesh-funksiya bitlar satrini belgilangan uzunlikdagi bitlar satriga aylantirish funksiyasi bo'lib, ixtiyoriy o'lchamdagi ma'lumotlar massivini matematik almashtirish va u uchun uncha uzun bo'lmagan belgilangan yagona ketma-ketlikni hisoblaydi. Xesh funksiyalar bir tomonlama funksiya deb ham ataladi [3-6].

Berilgan argument x bo'yicha $f(x)$ funksiyaning qiymatini hisoblash oson, lekin x ni $f(x)$ dan topish qiyin bo'lgan funksiya *bir tomonlama funksiya* deb ataladi [3].

Autentifikasiya (haqiqiylikni tasdiqlash) deganda foydalanuvchining (tarmoq abonentining, xabar jo'natuvchining), dastur, qurilma yoki ma'lumotlarning (axborotning, olinadigan xabarning, kalitning) haqiqiyligini belgilash tartiboti tushuniladi [3].

Axborotni uzatishda, saqlashda yoki qayta ishlashda, raqobatchi oldida muayyan foyda olish yoki unga ziyon yetkazish maqsadida ataylab, axborotni ruxsat etilmagan tarzda o'zgartirish *axborotni soxtalashtirish* deyiladi.

Kriptotizimni buzish deganda muayyan vaqtda zamonaviy hisoblash vositalaridan foydalanib kriptotahlil masalalarini hal etish usulini topish tushuniladi.

Kriptoalgoritmning kriptotahlilga bardoshliligi, ya'ni kriptotizimning turli hujumlarga dosh bera olish qobiliyati *kriptobardoshlilik* deb ataladi [3].

Axborotni muhofaza qilish tizimining bir qismini yoki butun tizimni buzishga bo'lgan muvaffaqiyatli yoki muvaffaqiyatsiz urinish *hujum* deb ataladi [3-6].

Hujumning quyidagi turlari mavjud:

1. Aktiv (faol) hujum - tizimga yolg'on axborot o'rnashtirish yoki mavjud axborotni o'zgartirish yo'li bilan qilinadigan hujum.

2. Lug'at bo'yicha hujum - to'g'ridan-to'g'ri qilinadigan turli ko'rinishli hujumning biri bo'lib, bu hujum paytida maxfiy so'z (parol)lar qayta saralanadi va/yoki oldindan tuzilgan maxfiy so'zlar ro'yxatiga murojaat etiladi.

3. Shifrmatn bo'yicha hujum - faqat berilgan shifrmatnga asoslangan kriptotahlil usuli. Bunda mavjud shifrmatnga mos keladigan ochiq matnlarni imkoniyat darajasida ko'plab topish nazarda tutiladi.

4. Qo'pol kuch hujumi, to'liq tanlash - mumkin bo'lgan qiymatlarning barchasini yoki salmoqli miqdorini haqiqiy qiymat topilguncha tanlashga asoslangan hujum.

Yolg'on xabarlar o'rnashtirishga, xabarlarni tutib olish va o'zgartirishga, ma'lumotlar bazasidan foydalanishga, o'z vakolatini kengaytirishga, yolg'on ochiq kalitni o'rnashtirishga, soxta hujjatlar tayyorlashga, imzodan bosh tortishga va shu kabilarga urinayotgan buzg'unchi *aktiv (faol) buzg'unchi* hisoblanadi [3].

Kriptografik bayonnomani izdan chiqarish bo'yicha harakat qilmaydigan buzg'unchi *passiv (sust) buzg'unchi* deyiladi.

Elektron hujjat bu - elektron shaklda qayd etilgan, ERI bilan tasdiqlangan, hamda elektron hujjatning uni identifikasiya qilish imkonini beradigan boshqa rekvizitlariga ega bo'lgan axborot.

Elektron raqamli imzo – elektron hujjatdagi mazkur elektron hujjat axborotini ERIning yopiq (maxfiy) kalitidan foydalangan holda maxsus almashtirishlar natijasida hosil qilingan hamda ERIning ochiq kaliti yordamida elektron hujjatdagi axborotda buzilish yo'qligini aniqlash va ERI yopiq kalitining egasini identifikasiya qilish imkoniyatini beradigan imzo [3].

ERI vositalari deganda elektron hujjatda ERI yaratish va ERIning haqiqiyligini tasdiqlash, ERIning yopiq va ochiq kalitlarini yaratishni ta'minlaydigan barcha texnikaviy va dasturiy vositalar majmui tushuniladi [3].

ERI kalitlarini ro'yxatga olish markazi maxsus vakolatli organda davlat ro'yxatidan o'tgan va qonun hujjatlarida nazarda tutilgan vazifalarni bajaruvchi va muayyan ERI kalitining mansubligini tasdiqlashga qonuniy huquqi bo'lgan yuridik shaxsdir.

Elektron hujjat aylanishi deganda elektron hujjatlarni axborot tizimi orqali jo'natish va qabul qilib olish jarayonlari to'plami tushuniladi.

Elektron tijorat axborot tizimlaridan foydalangan holda amalga oshiriladigan tovarlarni sotish, ishlarni bajarish va xizmatlar ko'rsatishga doir tadbirkorlik faoliyatidir.

Axborot xavfsizligini ta'minlash uchun uni kriptografik almashtirishni amalga oshiruvchi apparat, dasturiy yoki apparat-dasturiy vosita *axborotni kriptografik muhofaza qilish vositasi* deyiladi [3].

Axborotni muhofaza qilishning apparat vositasi deganda axborotdan ruxsat etilmagan foydalanishdan, nusxa ko'chirishdan, uni o'g'irlash yoki o'zgartirishdan muhofaza qilish uchun mo'ljallangan mexanik, elektr mexanik, elektron, optik, lazer, radio, radiotexnik, radiolokasion va boshqa qurilmalar, tizimlar va inshootlar tushuniladi [3].

Dasturiy ta'minot majmuasiga kiruvchi va axborotni muhofaza qilish uchun mo'ljallangan maxsus dastur *axborotni muhofaza qilishning dasturiy vositasi* deb ataladi [3].

Meynfreym (meynfreym) deganda katta sig'imdagi ma'lumotlarni markazlashtirilgan holda saqlashni tashkillashtirishga va jadal hisoblash ishlarini bajarishga mo'ljallangan katta hajmli tezkor va tashqi xotiraga ega bo'lgan samaradorligi yuqori kompyuter tushuniladi.

Axborot-kommunikasiya tarmoqlarida axborot xavfsizligi muammosini yechish uchun kriptografik usullarga asoslangan protokollardan foydalaniladi. Xavfsizlikni ta'minlashning kriptografik usullari ko'pgina Internet tizimlarini qurishning asosi hisoblanadi. Bu axborot almashinuv tizimi yoki to'lovlar o'tkazish tizimi bo'lishi mumkin. Ularni tashkil etish uchun xavfsizlik masalalarining muhimligi ahamiyatlidir. Tadqiqotlarga ko'ra bugungi kunda xaridorlar Internet orqali hisob kitob qilishlarida mablag'larining ishonchliligi to'g'risida tashvishlanishlari elektron tijorat sekin rivojlanishining asosiy sabablaridan biri bo'lib qolmoqda.

Tashvishlanishlarning asosiy sabablari quyidagi omillarga bog'liq.

- Konfidensiallik kafolatining yo'qligi – uzatiladigan ma'lumotlarni kimdir tutib olishi va qimmatli axborotni, masalan kredit kartalar to'g'risidagi ma'lumotlarni olishga urinishi mumkin. Bu axborotni uzatish vaqtida sodir bo'lishi mumkin bo'lgani kabi xarid yakunlanganidan so'ng ham savdo qiladigan Veb-saytlar orqali ham sodir bo'lishi mumkin.
- Operasiya ishtirokchisini tasdiqlash (autentifikasiya qilish) darajasining pastligi, xaridor do'konga tashrif buyura turib, unda taqdim etilgan kompaniya o'zini tanishtirayotgan kompaniya ekanligiga, sotuvchida esa buyurtma bergan xaridor kredit kartaning qonuniy egasi ekanligiga ishonch xosil qilmasligidir.
- Ma'lumotlar butunligiga kafolat yo'qligi – agar ma'lumotlar jo'natuvchisi identifikasiya qilinishi mumkin bo'lsa ham, uchinchi tomon uzatish vaqtida ularni o'zgartirishi mumkin.

Ko'rsatilgan omillarni bartaraf etish va Internet orqali elektron tranzaksiyalarni himoya qilishning eng ko'p tarqalgan usuli SSL (Secure Socret Layer) protokoli orqali uzatiladigan axborot shifrlanishini ta'minlovchi ma'lumotlar almashinuvidir.

SSL protokoli ochiq kalitlarga ega kriptografiyaga asoslangan standart hisoblanadi. Protokol TSR/TR tarmoqlarida ilovalar protokollari bo'yicha serverlar va mijozlarni shifrlash va autentifikasiya qilish hisobiga uzatiladigan ma'lumotlar himoyasini ta'minlaydi. Bu Veb-brauzer tomonidan uzatiladigan va qabul qilinadigan barcha ma'lumot, jumladan URL-adresi, barcha jo'natiladigan ma'lumotlar (kredit kartalar nomerlari kabi), yopiq Veb-saytlardan foydalanish uchun ma'lumotlar (foydanuvchining nomi va paroli), shuningdek, Veb-serverlardan kelib tushadigan barcha ma'lumotlar shifrlanishini bildiradi.

1999 yili SSL protokolining 3.0 versiyasi o'rniga, SSL protokoliga asoslangan va hozirgi kunda Internet standarti hisoblangan TLS protokoli yaratildi. SSL 3.0 va TLS protokollari orasidagi farq juda ham jiddiy emas.

SSL va TLS protokollarining kamchiligi - o'zlarining xabarlarini tashishda tarmoq sathidagi faqat bitta – IP protokolidan foydalanishlari va faqat IP tarmoqlarda ishlay olishlari. Undan tashkari, SSL/TLSning amalda qo'llanishi tatbiqiy protokollar uchun to'la shaffof emas. Undan tashqari, SSLda autentifikasiyalashda va shifrlashda bir xil kalitdan foydalaniladi. Bu esa ma'lum bir holatlarda zaiflikka olib kelishi mumkin. Bunday yechim turli kalitlar ishlatilganiga nisbatan ko'p statistik ma'lumotlarni yig'ishga imkon beradi.

SSL protokoliga muvofiq o'zaro aloqadagi tomonlarni autentifikasiyalashda va umumiy maxfiy kalitni shakllantirishda ko'pincha RSA algoritmidan foydalaniladi.

Shunday qilib, SSL protokoli aytib o'tilgan xavfsizlik muammolarining bir qismini yechish imkonini beradi, biroq uning vazifasi uzatiladigan ma'lumotlarni shifrlashni ta'minlash bilan cheklanadi.

Yuqorida aytib o'tilgan muammolarni kompleks ravishda hal etish uchun protokollar spesifikasiyasi va to'plami, SET standarti (Secure Electronic Transactions) kabi xavfsiz elektron taranzaksiyalar yaratilgan. 1996 yil 1 fevralda Visa International va Master Card International bir qator texnologik kompaniyalar bilan birgalikda Internet orqali plastik kartalardan foydalanib himoyalangan hisob-kitoblarning yagona ochiq standarti bo'lgan SET standartini ishlab chiqilganligi to'g'risida e'lon qildilar.

Raqamli sertifikatlardan va shifrlashdan foydalanish tufayli SET xaridorlar va sotuvchilar uchun ham shartnomaning barcha ishtirokchilarini autentifikasiya qilish imkonini beradi. Bundan tashqari SET kredit kartalar nomerlarini va Internet orqali uzatiladigan boshqa maxfiy axborotning ishonchli himoya qilinishini ta'minlaydi, standartning ochiqligi esa, ishlab chiqaruvchilarga o'zaro hamkorlik qila oladigan yechimlarni yaratish imkonini beradi. Shuningdek, SETni rivojlantirishning mumkin bo'lgan muhim omili uning tanish moliyaviy vositasi bo'lib qolgan mavjud kartochkali tizimlarga suyanishi hisoblanadi. SET foydalanadigan xavfsizlik tizimining asosida kriptografik DES va RSA standartlari yotadi. SET infrastrukturasi ISO standartlashtirish

bo'yicha tasdiqlangan X.509 standartiga mos keladigan sertifikatlar bazasida ochiq kalit infrasturkturasiga muvofiq qurilgan.

SETning asosiy o'ziga xos xususiyati – xalqaro to'lov tizimlari tomonidan belgilanadigan xavfsizlik tizimidan foydalanishni reglamentga solishdir. Xulosa qilib aytganda SET protokoli elektron xizmat turlarining quyidagi talablarini ta'minlaydi:

- xizmat ma'lumotlarining maxfiyligi va axborot konfidensialligini;
- elektron raqamli imzo yordamida ta'minlanadigan to'lovlar ma'lumotlari butunligi saqlanishini;
- autentifikasiyani o'tkazish uchun ochiq kalitga ega maxsus kriptografiyani;
- elektron raqamli imzoni va karta egasini sertifikatlarini qo'llash bilan ta'minlanadigan kredit karta egasining autentifikasiya qilinishini;
- sotuvchi va sotuvchi seritifikatlarini qo'llagan holda plastik kartalar bo'yicha qabul qilish imkoniyatini autentifikasiya qilish.

IPSec protokoli (Internet Protocol Security) asosan IP tarmoqlarda ma'lumotlarni xavfsiz uzatishni ta'minlashga atalgan. IPSecning ishlatilishi quyidagilarni kafolatlaydi:

- uzatilayotgan ma'lumotlarning butunligini, ya'ni ma'lumotlar uzatilishida buzilmaydi, yo'qolmaydi va takrorlanmaydi;
- jo'natuvchining haqiqiyligini, ya'ni ma'lumotlar haqiqiy jo'natuvchi tomonidan uzatilgan;
- uzatiladigan ma'lumotlarning konfidensialligini, ya'ni ma'lumotlar shunday shaklda uzatiladiki, ularni ruxsatsiz ko'zdan kechirishning oldi olinadi.

Ta'kidlash lozimki, ma'lumotlar xavfsizligi tushunchasiga odatda, yana bir talab - ma'lumotlarning foydalanuvchanligi kiritiladi. Ma'lumotlarning foydalanuvchanligi deganda, ma'lumotlar yetkazilishining kafolati tushuniladi. IPSec protokollari bu masalani hal etmaydi va IPSec protokollar steki tarmoq sathida axborot ximoyasini ta'minlaydi.

IPSecdagi barcha protokollarni ikkita guruhga ajratish mumkin:

- uzatiluvchi ma'lumotlarni bevosita ishlovchi (ularning xavfsizligini ta'minlash uchun) protokollar;
- birinchi guruh protokollariga kerakli himoyalangan ulanishlar parametrlarini avtomatik tarzda muvofiqlashtirishga imkon beruvchi protokollar.

Internet uchun tarmoq himoya vositalarini dasturiy ta'minoti bozorini o'rganish shu faktni aniqladiki, ma'lumotlarga qaraganda masofadan ta'sir ko'rsatadigan barcha turlarini aniqlaydigan kompleks vositalar mavjud emas, borlari esa bitta muayyan turdagisini aniqlash uchun mo'ljallangan. Bugungi kunda Internet tarmoqlari orqali amalga oshiriladigan xizmatlarning xavfsizligini ta'minlashda eng ishonchli usul sifatida axborot xavfsizligini ta'minlashning kriptografik usullari tan olingan. Shularni inobatga olgan holda quyida asosan kriptografik protokollarga e'tibor qaratilgan.

1.2. Kriptografik protokollar nazariyasi asoslari

1.2.1. Protokol va uning vazifalari

Ikki yoki undan ortiq tomonlar bajaradigan, biror-bir masalani yechish uchun loyihalashtirilgan harakatlar ketma-ketligi protokol hisoblanib, "harakatlar ketma-ketligi" so'zi protokol boshidan to oxiriga qadar ketma-ket bajarilishini bildiradi. Har bir harakat navbatma-navbat bajariladi, shuningdek keyingi harakatlar oldingi harakatlar tugagandan keyingina bajarilishni boshlaydi. "Ikki yoki undan ortiq tomonlar bajaradigan" so'zi protokol bajarilishi uchun kamida ikki tomonning ishtiroki kerakligini bildiradi. Protokolni yakka tartibda bajarib bo'lmaydi. Nihoyat "biror-bir masalani yechish uchun loyihalashtirilgan" so'zi protokol qandaydir natijaga olib borishi kerakligini anglatadi [7-8].

Protokolga o'xshash, ammo biror-bir natijaga olib bormaydigan harakatlar ketma-ketligi – bu protokol emas, aksincha bekorga ketkazilgan vaqt hisoblanadi.

Protokollar quyidagi hususiyatlarga ega bo'lishi kerak [7-8]:

- amallar boshidan oxirigacha tartibga ega, ya'ni hyech bir amal undan oldingisi tugamaguncha boshlanmasligi kerak;
- protokolning har bir ishtirokchisi protokolga bo'ysunishi shart;
- har bir amal aynan aniqlangan bo'lib, ikki xil ma'no kasb etmasligi kerak, har bir vaziyatdan aniq chiqish yo'li bo'lishi kerak;
- protokol uchun bitta ishtirokchining bo'lishi yetarli emas (ikki yoki undan ortiq bo'lishi kerak);
- protokolning barcha ishtirokchilari avvaldan bajariladigan amallar ketma-ketligi bilan tanish va uni bajarishga rozi bo'lishlari kerak;

- tomonlar biror bir aniq vazifani bajaradilar – bu maqsadsiz amallar bo‘lmasligi kerak.

- protokol to‘liq bo‘lishi lozim – unda aniq harakatlar keltirilishi kerak.

Har kunlik hayotimizda formal bo‘lmagan protokollar deyarli hamma joyda ishlatiladi: masalan, telefon orqali tort buyurish, saylovlarda ovoz berish va h.z. Odamlar bu protokollar haqida uncha o‘ylashmaydi. Ular uzoq vaqt mobaynida evolyusiyalashgan, ulardan qanday foydalanishni hamma biladi va ular ishonchli ishlaydi.

Hozir ko‘pgina odamlar shaxsiy muloqot uchun kompyuter tarmog‘ini ma’qul ko‘radilar. Ammo odamlar ko‘p o‘ylamay qiladigan ishlarni qilishlari uchun kompyuterlar uchun formal protokollar kerak bo‘ladi. Masalan, odamlar bir joydan boshqa joyga ko‘chib ketsa, ular u yerdagi o‘zgarishlarga moslashadi, ammo kompyuterlar bunday moslashuvchanlik qobiliyatiga ega emaslar.

Kompyuter tarmog‘idan foydalanuvchilar va kompyuter tarmog‘i yaratuvchilarining rostgo‘yligiga har doim ham ishonib bo‘lmaydi. Albatta ularning ko‘pchiligi to‘g‘ri so‘z odamlar, ammo ularning orasida bir nechta buzg‘unchisi bo‘lsa ham katta talofot keltirishi mumkin. Protokollar formalizasiyasi buzg‘unchilar tomonidan protokolni ochish uchun ishlatiladigan usullarni aniqlash imkonini beradi. Buning natijasida bardoshli protokollarni ishlab chiqish imkoniyati tug‘iladi.

Harakatlarni formalizasiya qilishdan tashqari protokollar vazifani yechish jarayonini mexanizmni yechish jarayonidan ajratib olish imkonini beradi. Masalan, IBM shaxsiy kompyuteri va VAX meynfreymlarida bir xil aloqa protokollari ishlatiladi [7-8].

Protokollar ishlashini namoyish qilish uchun bir-nechta ishtirokchilar yordamidan foydalanamiz (1.1-jadval).

1.1- jadval

Protokol ishtirokchilari

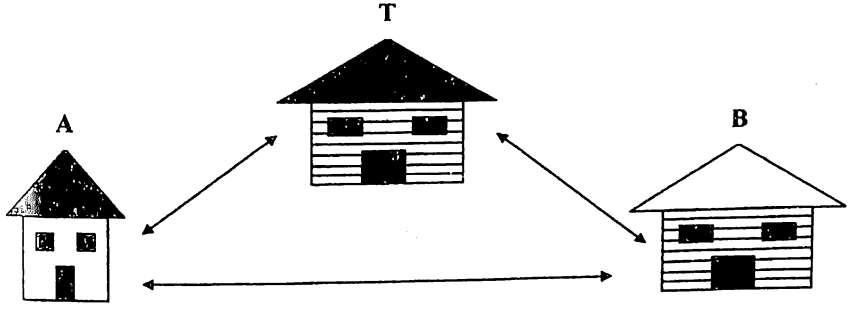
Ishtirokchilar	Faoliyati	Belgilanishi
Alisa	Barcha protokollarning birinchi ishtirokchisi	A
Bob	Barcha protokollarning ikkinchi ishtirokchisi	V
Kerol	Uch va to‘rt tomonli protokollar ishtirokchisi	K

Deyv	To‘rt tomonli protokollar ishtirokchisi	**D**
Trent	Ishonchli vositachi	**T**
Yeva	Passiv buzg‘unchi	**E**
Mellori	Yomon niyatli aktiv buzg‘unchi	**M**

Jarayondagi asosiy ishtirokchilar – **A** va **V** bo‘lib, ular umumiy qabul qilingan barcha ikki tomonlama protokollarni bajaradilar. Qoida bo‘yicha barcha protokollarni **A** inisializasiya qiladi, **B** esa javob beradi. Agar protokol 3 va 4 tomonlar ishtirokini talab qilsa, o‘yinga **K** va **D** qo‘shiladilar. Boshqa ishtirokchilar maxsus yordamchi rolni bajarishadi [7-8].

Vositachi yordamidagi protokollar

Vositachi deb protokolni bajarilishini yakuniga yetkazishga ishonch bildirilgan manfaatdor bo‘lmagan uchinchi tomonga aytiladi (1.1- rasm). Vositachining “manfaatdor bo‘lmasligi” protokol bajarilishining natijasi hamda protokol ishtirokchisining hyech biri u uchun ahamiyatga ega emasligini bildiradi. “Ishonch bildirish” so‘zi protokolning barcha ishtirokchilari vositachining so‘zlarini haqiqat deb qabul qilishini, uning hamma harakatlarini to‘g‘ri deb bilishligini, bundan tashqari vositachi protokoldagi o‘zining qismini bajarishiga ishonishligini bildiradi. Vositachilar bir-biriga ishonchi bo‘lmagan 2 tomonga protokolni bajarilishiga yordam beradilar [7-8].



1.1- rasm. Vositachi yordamidamidagi protokollar

Real hayotda vositachi sifatida ko‘p hollarda advokatlarni tanlashadi.

Masalan, **A** unga begona bo‘lgan **B** ga avtomobil sotyapti. **B** chek yordamida pulini to‘lamoqchi, ammo **A** da chekning haqiqiyligini tekshirish imkoni yo‘q. Shuning uchun **B** ga mulkka egalik huquqini berishdan oldin **A** chek orqali pulini olmoqchi. **B** ham **A** ga o‘xshab egalik huquqini olmasdan turib chekni berishni xohlamaydi.

Bu ishda advokatning ishtiroki ikkala tomonni ham qoniqtiradi. U **A** va **B** ga bir-birini alday olmasligini kafolatlovchi quyidagi protokolni bajarilishiga yordam beradi:

1 **A** egalik xuquqini advokatga beradi.

2 **B** chekni **A** ga beradi.

3 **A** chekni depozitga qo‘yadi.

4 Chekni to‘lash uchun kerakli vaqt o‘tgandan keyin advokat **B** ga egalik huquqini beradi. Agar ma’lum vaqt mobaynida chek to‘lanmasa, **A** bu faktni advokatga isbotlab beradi va u egalik huquqini **A** ga qaytarib beradi.

Bu protokolda **A** chek to‘langunga qadar advokat egalik huquqini **V** ga bermasligiga va agar chek bo‘yicha to‘lov amalga oshmasa egalik huquqini **A** ga qaytarib berishiga ishonadi. **V** chek to‘lanmasdan turib egalik huquqini advokatda turishiga ishonadi va u chek to‘langandan keyin shu zahoti egalik huquqini **V** ga beradi. Advokatni chekning to‘lovi qiziqtirmaydi. Ixtiyoriy holatda u protokoldagi o‘zining qismini bajaradi, chunki ishning qanday yakunlanishiga qaramay o‘zining xizmat haqini oladi [7-8].

Bu misolda advokat vositachi rolini o‘ynaydi. Advokatlar ko‘pincha shaxs rolida ishtirok etishadi, bunda ikki shaxs orasidagi munosabatlar tartibga solingunga qadar hisob ularning qo‘lida turadi. Bundan tashqari, advokatlar ko‘pincha vasiyatnoma yozilganda, ba’zan esa savdo-sotiq shartnomasi tuzilganda vositachi sifatida ishtirok etadilar. Sotuvchi va oluvchi orasida ba’zan vositachi sifatida turli birjalar ham ishtirok etadi.

Quyidagi misolda vositachi sifatida bank ham ishtirok etishi mumkin. **A** dan avtomobil sotib olish uchun **V** kafolatlangan chekni ishlatishi mumkin:

1 **V** chekni yozib bankka beradi.

2 **V** ning hisobida chekni to‘lash uchun yetarli miqdordagi pullarni rezervlab, bank chekni tasdiqlaydi va uni **V** ga qaytaradi.

3 A egalik huquqini V ga beradi, V esa A ga kafolatlangan chekni beradi.

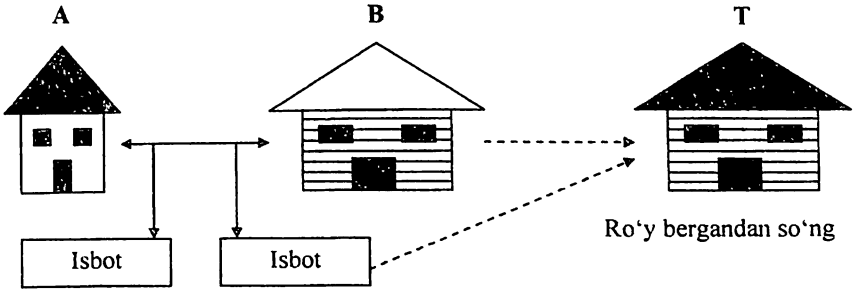
4 A chekni depozitga o'tkazadi.

A bankning kafolatlariga ishonganligi uchun bu protokol ishlaydi. A bank u uchun V ning pullarini ushlab qolishiga va ularni xavfli operasiyalarni bajarishda mablag' bilan ta'minlashga ishlatmasligiga ishonadi.

Yana bir bo'lishi mumkin bo'lgan vositachi – notarius. Qachonki V A dan notariusda tasdiqlangan hujjatni olsa, u A hujjatga o'z ixtiyori va o'z qo'li bilan imzo chekkaniga ishonadi. Kerak bo'lganda notarius bu faktni sudda tasdiqlashi mumkin [7-8].

Arbitrli protokollar

Vositachini yollash katta mablag' talab etganligi uchun, vositachi ishtirok etgan protokollarni hiyla pastroq darajali ikkita qism protokolga ajratish mumkin. Birinchisi vositachisiz protokol hisoblanadi, bunda tomonlar protokolni bajarish niyatida bo'lgan hollardagina ishlaydi. Ikkinchisi, faqat ayrim hollarda ijro etiladigan – qachon tomonlar orasida kelishmovchilik kelib chiqsa, vositachi yordamidagi protokollar hisoblanadi. Bu protokolda maxsus turdagi vositachi ishtirok etadi – bu arbitr (1.2-rasm) [7-8].



1.2- rasm. Atributli protokil

Arbitr xuddi vositachi kabi qiziqmaydigan va ishonchli protokolning uchinchi tomoni hisoblanadi. Vositachidan farqli ravishda u har bir protokolning bajarilishida ishtirok etishi shart emas. Arbitr faqat protokolning to'g'ri bajarilganligini tekshirish uchun taklif qilinadi.

Professional arbitrlarga misol qilib hakamlarni (sudya) keltirish mumkin. Notariuslardan farqli ravishda hakamlarga faqat kelishmovchilik kelib chiqqanda murojaat qilinadi. **A** va **V** hakam ishtirokisiz shartnoma tuzishlari mumkin, agar ixtiyoriy bir tomon ikkinchi tomonni sudga bermasa, hakam shartnoma haqida hyech qachon bilmaydi [7-8]. Shartnoma imzolash protokolini quyidagicha ifodalash mumkin:

Vositachisiz protokol (har doim bajariladi):

1 **A** va **V** shartnoma shartlariga rozilik bildirishadi;

2 **A** shartnomani imzolaydi;

3 **V** shartnomani imzolaydi.

Arbitr ishtirokidagi protokol (kelishmovchilik kelib chiqqanda bajariladi):

1 **A** va **V** sudda ishtirok etishadi;

2 **A** o'zining dalillarini keltiradi;

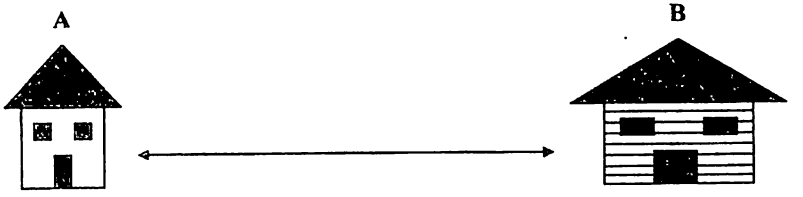
3 **V** o'zining dalillarini keltiradi;

4 Dalillarga tayanib hakam o'z qarorini chiqaradi.

Arbitrli kompyuter protokollari ham ma'lum. Bu protokollar tomonlarning rostgo'yligi taxminiga tayanishadi. Biroq agar kimdir firibgarlikni sezsa, uchinchi ishonchli tomon **T** mavjud ma'lumotlar massivi asosida aldovni fosh qilishi mumkin. Bundan tashqari yaxshi arbitrajli protokol arbitrga firibgarning shaxsini xam aniqlash imkonini beradi. Shunday qilib arbitrajli protokollar firibgarlikni oldini olmaydi, balki uni aniqlaydi [7-8].

O'ziga yetarli protokollar

O'ziga yetarli protokollar - eng yaxshi protokol turi hisoblanadi (1.3-rasm). Tomonlar to'g'riligi protokollarning o'zi bilan kafolatlanadi. Protokolning bajarilishi uchun vositachi kerak emas, kelishmovchiliklarni bartaraf etish uchun esa – arbitr (hakam). Kelishmovchiliklarning yo'qligini (mavjud emasligini) protokol konstruksiyasining o'zi ta'minlaydi. Agar tomonlarning biri g'irromlik qilishga harakat qilsa, boshqa tomon shu zahoti aldovni aniqlaydi va protokol bajarilishi to'xtatiladi [7-8].



1.3- rasm. O'ziga yetarli protokol

1.2.2. Kriptografik protokollar nazariyasi

Kriptografik protokol tushunchasi kriptografiyaning asosiy tushunchalaridan biri hisoblanadi va u maxfiylik, haqiqiylikni tekshirish, yaxlitlik va insonlar tomonidan qilinadigan buzg'unchilik muammolarini hal etishda muhim ahamiyat kasb etadi [7-10]. Kriptografik algoritmlar va usullarni aniq bir muammolarni yechishda qo'llay olish uchun kriptografik protokollar haqida to'liq ma'lumotga ega bo'lish talab etiladi.

Kriptografik protokol kriptoalgoritmdan va shifrlash kalitlaridan foydalanishni belgilab beradigan qoidalar va proseduralar to'plamidir. Tomonlar bir-biriga ishonib do'st bo'lishi mumkin yoki aksincha bir-biriga ishonmasligi, ya'ni buzg'unchi bo'lishi mumkin. Kriptografik protokol tarkibiga ma'lum bir kriptografik algoritm kiradi, ammo protokollar faqatgina maxfiylikni ta'minlash uchun mo'ljallanmagan. Protokollarda kriptografiyani ishlatishdan maqsad firibgarlik va noqonuniy eshitishni aniqlash yoki unga yo'l qo'ymaslik [7-10].

Umumiy qoida shunday:

Protokolda keltirilgandan tashqari ko'proq narsa bilish yoki o'zgartirish mumkin emas.

Ba'zi protokollarda ishtirokchilardan biri ikkinchisini aldashi mumkin. Boshqa protokollarda esa buzg'unchi protokolni buzishi yoki undagi maxfiy ma'lumotni bilib olishi mumkin.

Kriptografik protokollar (KP) quyidagi bir necha ishtirokchilardan tarkib topgan taqsimlangan algoritmdir:

- odamlar;
- kompyuter dasturlari;
- kompyuterlar va hisoblash komplekslari;

- ma'lumotlar bazasi;
- aloqa tarmoqlari;
- autentifikasiya vositalari;
- va boshqalar.

KPning har bir ishtirokchisi ma'lum algoritmlar ketma-ketligiga mos ravishda ish bajaradi. Har bir ishtirokchi tomonidan bajariladigan amal quyidagicha bo'lishi mumkin [11-12]:

- boshqa ishtirokchiga (yoki ishtirokchilar guruhiga) *xabarni yuborish;*
- boshqa ishtirokchidan *xabar qabul qilish;*
- *ichki amal,* ya'ni ishtirokchilar amalga oshiradigan ba'zi hisoblash ishlari.

KP ishtirokchilari 3 sinfga bo'linadi [11-14]:

1. *Odatdagi (qonuniy) ishtirokchilar* (**A, V** va hakozo belgilar ko'rinishida ifodalanadi, indekslar bilan ham kelishi mumkin).
2. *Ishonchli vositachi* (**T** belgisi ko'rinishida ifodalanadi, indeks bilan ham kelishi mumkin).
3. Quyidagi ikki sinfga bo'linuvchi *buzg'unchilar:*

a) *Passiv buzg'unchilar* (**Ye** belgisi ko'rinishida ifodalanadi, indeks bilan ham kelishi mumkin).

Passiv buzg'unchi boshqa ishtirokchilarga yuborgan xabarni ushlab olishi, o'g'irlashi va tahlil qilishi mumkin.

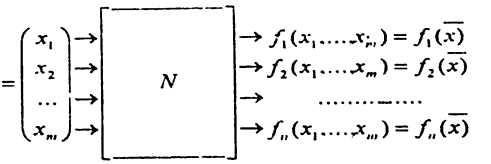
b) *Aktiv buzg'unchilar* (**M** belgisi ko'rinishida ifodalanadi, indeks bilan ham kelishi mumkin).

Aktiv buzg'unchi quyidagi amallarni bajarishi mumkin:

- boshqa ishtirokchilarga yuborilgan xabarni ushlab olishi va tahlil qilishi;
- yuborilgan xabarni o'zgartirishi yoki o'chirishi;
- yangi xabarni hosil qilib, boshqa ishtirokchilarga yuborishi;
- o'zini boshqa ishtirokchi qilib ko'rsatishi (bunday aktiv buzg'unchilarni *firibgar* deb nomlashadi).

Shunday qilib KP – bu shunday protokolki, unda kriptografik algoritmlar qo'llaniladi, va u biror bir kriptografik masalani yechish uchun xizmat qiladi.

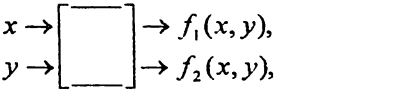
Nazariy kriptografiyada protokol m ta kirish va $n \le m$ ta chiqishga ega bo'lgan "qora quti" sifatida qaraladi (1.4-rasm) [10, 15]:



1.4- rasm. Nazariy kriptografiyada protokol sxemasi

Ravshanki, N kriptotizimni barcha ishtirokchilar to'liq va so'zsiz ishonadigan ishtirokchisi mavjud bo'lsa, ixtiyoriy protokolni trivial loyihalashtirish ham mumkin bo'ladi. Ammo amaliyotda bunday holatlar deyarli uchramaydi. Kriptografik protokollarni loyihalashtirish masalalari quyida keltiriladi. Kriptotizim qisman va to'la bir biriga ishonmaydigan ishtirokchilaridan iborat bo'lsa, bunday kriptografik protokolda ishonchli tomon T umumiy kuch bilan hosil qilinishi kerak [15].

Xususan, kriptografik protokolda agar faqat ikki tomon ishtirok etayotgan bo'lsa, u holda ikkita kirish va ikkita chiqish yo'liga ega bo'lgan qora quti qaraladi:



$$F(x,y) = (f_1(x,y); f_2(x,y)).$$

Agar ikkala ishtirokchi ham protokol bajarilishi natijasida bir xil ma'lumot hosil qilsa, u holda:

$$F(x,y) = (g(x,y); g(x,y)).$$

Avval ta'kidlab o'tilganidek, protokol – bu kriptografik algoritm va boshlang'ich elementlariga (primitivlarga) nisbatan yuqori darajadagi struktura. Bitta protokolda turli elementlar va algoritmlar ishlatilishi mumkin. Ulardan bittasining yoki bir nechtasining noto'g'ri qo'llanilishi butun protokol xavfsizligini yo'qolishiga olib kelishi mumkin. Shunday vaziyatga oddiy misol keltirishimiz mumkin: protokolda uzatilayotgan ma'lumotlarni yopish uchun biror shifrlash algoritmidan foydalanilayotgan, ammo uning kaliti protokol bajarilish jarayonida ochiq holda uzatilayotgan bo'lsin. Ma'lumki, bu yerda protokolning noto'g'ri tuzilishi shifr qanchalar turg'un bo'lmasin xavfsizlikning yo'qolishiga olib keladi.

Kriptografik protokollarning berilgan talablarga ko'ra to'g'ri tuzilishi odatda ikki maqsadni ko'zlaydi: tashqaridagi buzg'unchidan

himoya qilishni va o'zaro bir birini aldashdan himoya qilishni. Kriptografik protokollar – bu ishtirokchilar qrasidagi shunday o'zaro bog'lanish prosedurasiki, uning natijasida qonuniy ishtirokchilar o'z maqsadlariga erishadilar, buzg'unchi esa maqsadiga yeta olmaydi.

Bardoshli protokol – uni "sindirish" uchun urinishlarga nisbatan "ichki" konstruktiv turg'unlikka ega bo'lgan protokol. Protokolni ko'pchilik ishtirokchilar unga to'g'ri amal qilganda, ishonchli natija oladigan qilib tuzish mumkin.

Turg'un protokol – buzg'unchi ishtirokchilarning maxfiy ma'lumotining biror qismini bilganda ham xavfsizlikni saqlay oladigan protokol [15].

Bitta protokol aynan bitta ishtirok etuvchi shaxslar tomonidan biror vaqt oralig'ida bir necha marta bajarilishi mumkin. Seans – bu protokolning bir marta bajarilishi. Protokol raundi – bu bir martali ikki tomonlama xabar yuborish. Raund kontekstiga bog'liq holda ikki yoki undan ortiq xabarlarni jo'natishni o'z ichiga olishi mumkin. Ba'zan protokolning ichida siklik konstruksiyalar ham uchraydi: bunda bir martali siklning bajarilishi raund deb ataladi.

Kriptografik protokollarning tavsifi, odatda ishtirokchilarning hatti-harakati tavsifidan tashqari talab qilinayotgan algoritmlarning xarakteristikalarini, protokolning to'g'ri ishlashi uchun talab qilinadigan boshlang'ich shartlarni o'z ichiga oladi.

Umumiy holda protokol ishtirokchilari ikki guruhga bo'linadi:

1. protokol masalasini bevosita yechuvchilar;
2. birinchi guruh ishtirokchilariga xizmat ko'rsatuvchilar.

Birinchi guruhga kiruvchi ishtirokchilar soniga bog'liq ravishda protokollar ikki tomonlama va ko'p tomonlama bo'ladi. O'z navbatida bunday ishtirokchilar vijdonli va vijdonsizga bo'linadi. Vijdonsizlarga protokol masalalarini yechishga atayin xalaqit beruvchilar kiradi, ya'ni bular dushmanlar, buzg'unchilar, qasddan bo'lmasada xato o'tkazishga sabab bo'lganlardir.

Amaliyotda odatda biror bir ishtirokchining protokolda keltirilgan amallardan chetlashishi atayinmi yoki tasodifiymi ekanligini aniqlash juda ham qiyin. Shuning uchun amaliyotda protokolda buzg'unchi ishtirok etmoqda degan yetarlicha kuchli taxmin qabul qilinadi va bu xavfni amalga oshirilishini hisobga olgan holda protokol tuziladi. Buzg'unchi turli masalalarda turli imkoniyatlarga ega bo'lishi mumkin: abonentlar

bilan boshqa ishtirokchilar nomidan bog'lanish, axborot almashinuviga aralashish. Buzg'unchi abonentlardan biri yoki u bilan til biriktirgan bir necha kishi bo'lishi mumkin [15].

Yuqorida bayon qilinganlarga asoslanib *quyidagi xulosaga kelish* mumkin: Protokolga hujum qilish usuliga ko'ra buzg'unchi passiv yoki aktiv (faol) bo'lishi mumkin. Passiv buzg'unchi faqat aloqa kanallarini eshitishi va bu kanallar orqali yuborilayotgan axborotlarni to'laligicha yoki saralab saqlashi mumkin. Faol buzg'unchi aloqa kanalida xabarlarni qo'shib qo'yishi, o'zgartirishi, olib tashlashi va xattoki protokol ishtirokchilarining maxfiy kalitining bir qismini qo'lga kiritishi mumkin.

Kriptografik protokollar nazariyasining paydo bo'lish tarixi kishilar amaliyotining tomonlar o'rtasida ishonchsizlik mavjud bo'lgan, qiziqishlar ustma-ust tushmay bir-birini aldash ehtimolligi mavjud bo'lgan sohalarida yuzaga kelgan. Bunday sohalarga avvalam bor bank ishlari, notarial ishlar, savdo-sotiq, moliyaviy bitimlar, xizmat yozishmalari, hujjat aylanishi va hokazolar kiradi [15].

1.2.3. Kriptografik protokolning xossalari

KPning xossalari bir necha sinflarga bo'linadi. Quyidagi sinfdagi xossalar eng dolzarb hisoblanadi.

1. *Aniqlik,* ya'ni:

- KP ishtirokchilari tomonidan amalga oshiriladigan hisoblashlarning to'g'riligi;
- ishtirokchilar tomonidan hisoblangan natijalarning berilgan o'zaro nisbatga mos kelishi;
- va hokazo.

Aniqlik xossasi asosiy hisoblanadi, chunki ularning buzilishi natijasida, hattoki KP qolgan hamma xossalarga ega bo'lsa ham, KPni ishlatib bo'lmaydi [16].

2. *Xavfsizlik.*

Ushbu xossalar sinfi bir necha qismiy sinflarga bo'linadi. Ulardan eng dolzarblari quyidagilar:

- *Yaxlitlik,* ya'ni qonuniy ishtirokchilar almashinadigan xabarni buzg'unchi tomonidan o'zgartirish harakatlari KPni bajarish jarayonida aniqlanishidan iborat;

• *Maxfiylik,* ya'ni KP ishi jarayonida axborotning mualliflashtirilmagan tarzda chiqib ketishining oldi olinganligidan iborat: KP ishlab turgan ixtiyoriy paytda buzg'unchi shifrlangan xabarni tarkibi bilan tanishish imkoni bo'lmasligi kerak.

3. *Turg'unlik* (quyidagi hollarda):

• ma'lum hatti-harakatlardan ishtirokchining hatti-harakatlarini rad etishda;

• KP bajarilib turgan muhitda kutilmagan hatti-harakati holatida.

Shuningdek ushbu xossalar sinfiga KP ishlab turgan kompyuter tizimida nosozlikdan so'ng normal ishlashini tezda ta'minlash qobiliyati kiradi.

4. *Samaradorlik* - KP ishlashi jarayonida xotira va vaqt resurslaridan samarali foydalanish. KPdagi amalga oshirilgan algoritmlarning optimalligi.

5. *Adaptasiya* – ichki strukturasini o'zgartirmasdan uni sozlagichi yordamida o'zgartirish yo'li bilan KP muhitining ozgina o'zgarishiga moslashuvchanligi.

6. *Hujjatlashtirilganlik* - uni ishlatish shartida muhim o'zgarish bo'lganda KPga tezda o'zgartirish kiritishga imkon beruvchi KP tavsifining tiniq va aniq hujjatlashtirilganligi (Masalan, juda ko'p mumkin bo'lgan kirish ma'lumotlarini kengaytirish yoki toraytirish holatida).

7. *Mobillilik va moslashuvchanlik,* ya'ni KPning turli konfigurasiya va platformalarda yaxshi ishlash qobiliyati [16].

1.2.4. Kriptografik protokollarning sinflanishi

Kriptografik protokollarni sinflashda turli yondashuvlar mavjud. Quyida ulardan ba'zi birlari keltiriladi [17].

1. *Ishtirokchilar soniga ko'ra sinflanish*:

– ikki tomonlama;

– uch tomonlama;

– ko'p tomonlama.

2. *Yuboriladigan xabarlar soniga ko'ra sinflanish:*

– interaktiv (o'zaro xabarlar almashinuvi);

– nointeraktiv (faqat bir tomonlama yuborish). Nointeraktiv protokollar ko'pincha sxema deb nomlanadi.

3. *Protokolning belgilangan maqsadiga ko'ra sinflanishi:*

– xabar yaxlitligini ta'minlovchi protokol:
  - manbani autentifikasiya qilib;
  - manbani autentifikasiya qilmasdan.

– ERI protokoli (sxemasi):
  - jamoaviy/shaxsiy ERI protokoli;
  - xabarni qayta tiklashli/qayta tiklashsiz;
  - ko'r-ko'rona ERI protokoli;
  - maxfiy ERI protokoli;
  - soxtalashtirilganligini isbotlovchi (yoki soxtalashtirilganligini isbotlash sifatiga ega bo'lgan) ERI protokoli.

– Identifikasiyalash protokoli (ishtirokchilarni autentifikasiya qilish):
  - bir tomonlama autentifikasiya;
  - ikki tomonlama (o'zaro) autentifikasiya.

– Maxfiy yuborish:
  - xabarlarni odatiy almashinishi;
  - keng qamrovli/sirkulyar yuborish;
  - sirlarning haqqoniy almashinuvi;
  - unutiladigan yuborish;
  - bitga (satr) bog'lanuvchi protokol.

– Kalitlarni taqsimlash protokoli:
  - kalitlarni avvaldan taqsimlash protokoli (sxemasi);
  - kalitni yuborish protokoli (kalitlar almashinish);
  - kalitni birgalikda ishlab chiqish protokoli;
  - juftli/jamoaviy protokol;
  - sirni bo'lishish protokoli (sxemasi);
  - telekonferensiya protokoli;
  - va hokazolar [17].

1.3. Kriptografik protokollarning vazifalari

Xavfli ochiq kompyuter tarmoqlarida va taqsimlangan kompyuter tarmoqlarida o'zaro xavfsiz ma'lumot almashinuvini tashkillashtirish

muhim vazifalardan biri bo'lib, uni hal qilish uchun KPdan foydalanish mumkin [17].

Kriptografik protokollar quyidagi asosiy vazifalarni bajaradi:

- Ma'lumotlar manbasining autentifikasiyasi;
- Tomonlar autentifikasiyasi;
- Ma'lumotlar maxfiyligi;
- Rad etishning mumkin bo'lmasligi;
- Qabul qilganlikning isboti bilan rad etishning mumkin bo'lmasligi;
- Manbaning isboti bilan rad etishning mumkin bo'lmasligi;
- Ma'lumotlar yaxlitligi;
- Qayta tiklashsiz ulanishning yaxlitligini ta'minlash;
- Qayta tiklashli ulanishning yaxlitligini ta'minlash;
- Foydalanishni chegaralash.

1.2-paragrafda bayon etilganlarga asoslanib kriptografik protokollarni bajaradigan asosiy vazifalariga qarab umumiy holda quyidagicha sinflash mumkin:

- shifrlash/shifrni ochish protokollari;
- ERI protokoli;
- identifikasiya/autentifikasiya protokoli (AP);
- kalitlarni autentifikasiya qilib tarqatish protokoli.

Shifrlash/shifrni ochish protokollari. Bu sinfdagi protokol asosini shifrlash/shifr ochishning simmetrik yoki nosimmetrik algoritmi tashkil etadi. Shifrlash algoritmi jo'natuvchi xabarni yuborayotganda amalga oshiriladi, natijada xabar ochiq holatdan shifrlangan holatga almashtiriladi. Shifrni ochish algoritmi qabul qiluvchi xabarni olayotganda amalga oshiriladi, natijada xabar shifrlangan holatdan ochiq holatga almashtiriladi. Shu tarzda maxfiylik xususiyati ta'minlanadi [18].

Odatda simmetrik shifrlash/shifrni ochish algoritmlarida uzatilayotgan xabarlarning yaxlitlik xossasini saqlash uchun, uzatishda va qabul qilishda shifrlash kaliti qo'llaniladigan imitohimoya qo'shimchalarini tekshirishni imitohimoya qo'shimchalarini hisoblovchi algoritmlar bilan birga qo'llaniladi. Nosimmetrik shifrlash/shifrni ochish algoritmlarini qo'llaganda yaxlitlik xossasi alohida ERIni hisoblash orqali, uzatishda va qabul qilishda qabul qilingan xabarni rad eta olmaslik va haqiqiylikni ta'minlovchi ERIni tekshirish yordamida amalga oshiriladi.

ERI protokoli. Bu sinfdagi protokol asosini yuborishda yuboruvchining yopiq kaliti yordamida ERIni hisoblash, qabul qilishda ochiq ma'lumotnomadan olinadigan va o'zgartirishdan himoyalangan yopiq kalitga mos ochiq kalit yordamida ERIni tekshirish algoritmlari tashkil etadi. Protokolni tekshirish natijasi ijobiy bo'lganda, qabul qilingan xabar, uning ERIsi va mos ochiq kalitlarni arxivlash amali bilan tugallanadi. Agar ERI rad qila olmaslik xususiyati uchun emas, balki faqat yaxlitlik va qabul qilingan xabarning haqiqiyligini ta'minlash uchun qo'llanilsa, arxivlash amali bajarilmasligi mumkin. Bu holda tekshiruvdan so'ng ERI o'sha zahotiyoq yoki kutish davri chegarasi tugashi bilan o'chirib tashlanadi [18].

Identifikasiya/autentifikasiya protokoli. Bu sinfdagi protokol asosini identifikatorga ega bo'lgan identifikasiya qilinuvchi obyektning faqatgina qayd etilgan obyektga ma'lum bo'lgan maxfiy axborotni bilishligini tekshiradigan ba'zi algoritm tashkil etadi. Bunda tekshirish usuli bilvosita hisoblanadi, ya'ni bu maxfiy axborotni taqdim qilmasdan amalga oshiriladi.

Odatda har bir obyektning nomi (identifikatori) himoyalangan ma'lumotlar bazasiga yozilgan tizimdagi huquq va vositalar ro'yxati bilan bog'lanadi. Bu holatda identifikasiya protokoli identifikasiya qilingan obyekt buyurtirgan xizmatning vakolatli ekanligini tekshiradigan APgacha kengaytirilishi mumkin [18].

Agar identifikasiya protokolida ERI ishlatilsa, u holda maxfiy axborot sifatida ERIning maxfiy kaliti ishlatiladi. ERIni tekshirish yopiq kalitni aniqlashga yo'l qo'ymaydigan, lekin bu yopiq kalitni ERI muallifiga ma'lum bo'lishiga ishonch hosil qiladigan ma'lumot bo'lgan unga mos ochiq kalit yordamida amalga oshiriladi.

Autentifikasiya qilingan kalitlarni taqsimlash protokoli. Bu sinfdagi protokol ishtirokchilarni autentifikasiya qilishni generasiyalash va kanal bo'yicha kalitlarni taqsimlash protokoli bilan qo'shilib ketadi. Protokol ikki yoki uch ishtirokchilardan iborat: uchinchi ishtirokchi bo'lib, kalitlarni taqsimlash va generasiyalash markazi xizmat qiladi (*s* server). Protokol 3 bosqichdan iborat: generasiya, qayd etish (registrasiya) va kommunikasiya. Generasiya bosqichida *s* server tizimning parametrlari qiymatlarini, shuningdek o'zining ochiq va yopiq kalitini ham generasiyalaydi. Qayd qilish bosqichida *s* server hujjatlar bo'yicha ishtirokchilarni (shaxsan o'zining kelishi yoki vakolatli shaxslar orqali)

identifikasiya qiladi. Buning uchun *s* server har bir obyekt uchun kalit va/yoki identifikasiyalovchi axborotni generasiya qiladi va kerakli tizim konstantalari va *s* serverining ochiq kalitidan (zaruriy holatda) iborat bo'lgan xavfsizlik markerini shakllantiradi. Kommunikasiya bosqichida umumiy seans kalitini shakllantirish bilan yakunlanadigan o'zining autentifikasiya qilingan kalitlar almashinuvi protokolini amalga oshiradi [18].

Yuqorida keltirilgan funksiyalardan kriptografik protokollarning asosiy vazifalari kelib chiqadi. Bu vazifalar quyidagilardan iborat:

- Autentifikasiyaning turli rejimlarini ta'minlash;
- Kriptografik kalitlarni hosil qilish, taqsimlash va o'zaro moslash;
- Ishtirokchilarning o'zaro aloqasini himoyalash;
- Ishtirokchilar orasidagi javobgarlikni taqsimlash.

1.4. Protokol xavfsizligiga oid talablar

Protokol xavfsizligi tushunchasi xavfsizlikni tavsiflaydigan foydalana olishlik, konfidensiallik, yaxlitlik va boshqa xususiyatlarni bajarish kafolatini ta'minlash bilan ifodalanadi. Kriptografik protokollar turli hujumlarga nisbatan bardoshli bo'lsa, bunday protokollar xavfsiz deyiladi. Hujumlar protokollarda ishlatiladigan kriptografik algoritmlarga, algoritm va protokollarni tadqiq qilishda ishlatiladigan kriptografik usullarga yoki protokollarning o'ziga yo'naltirilgan bo'lishi mumkin. Kriptografik protokollarga qilinadigan asosiy hujumlarning tasnifini keltiramiz.

1. *Ma'lum kalitlar bo'yicha hujum* – bu hujumda buzg'unchi protokolning avvalgi seanslarida qo'llanilgan bir qancha kalitlarga ega bo'lib, bu ma'lumotdan keyingi seanslarda yangi kalitlarni aniqlash maqsadida foydalanadi, masalan kalitlarni o'zgarishi qonunini aniqlashi mumkin [19].

2. *Seansni takrorlash usuli bo'yicha hujum* – bu hujumda buzg'unchi protokol seansini qisman yoki to'laligicha yozib oladi va keyingi seansda takroran qo'llaydi, ya'ni seansni yoki uning qismini bir oz vaqtdan so'ng "qaytadan o'ynaydi" [19].

3. *O'zini boshqa shaxs nomidan ko'rsatish usuli bo'yicha hujum* – buzg'unchi o'ziga protokolning qonuniy ishtirokchilaridan birining o'xshashligini oladi [19].

4. *Lug'at bo'yicha hujum* – protokolda ishlatilish ehtimolligi katta bo'lgan kattaliklar yoki xabarlarni tanlash orqali hujum (masalan, parollarni tanlash, chunki odatda ular uchun oson topiladigan ma'lumotlar: familiya, ism, otasining ismi, telefon raqami, manzili va hokazolar olinadi) [19].

5. *Oldindan qidirish usuli bo'yicha hujum* – bajarilishiga ko'ra lug'at bo'yicha hujumga o'xshab ketadi, ammo bunda biror bir kattalikning mumkin bo'lgan barcha qiymatlarni to'la tanlash orqali amalga oshiriladi va odatda xabarlarni shifrini ochish uchun ishlatiladi. Masalan, bank tomonidan tarnzaksiya bajarilayotgan bo'lib, ochiq shifrlash sxemasiga ko'ra shifrlangan tranzaksiya kattaligi 32 bitli maydonda ko'rsatilgan bo'lsin. Buzg'unchi ochiq shifrlash xususiyatidan kelib chiqib 2^{32} ta ochiq matin olib ularni shifrlashi mumkin. So'ngra 2^{32} shifrmatinning har birini buzg'unchi tomonidan kuzatilayotgan tarnzaksiya kattaligi bilan solishtirib, unga mos keluvchi ochiq matinni aniqlashi mumkin [19].

6. *Kanalga suqilib kirish usuli bo'yicha hujum* – buzg'unchi **M** qonuniy **A** va **V** ishtirokchilar orasidagi aloqa kanaliga shunday "suqilib" kiradiki, u **A** ishtirokchiga **V** bilan bog'lanayotganlik illyuziyasini va aksincha **V** ishtirokchiga **A** bilan bog'lanayotganlik illyuziyasini hosil qiladi. Haqiqatda esa ularning har biri **M** bilan bog'lanayotgan bo'lib, **M** har bir xabarni "o'zi orqali o'tkazib", ularni o'zgartirishi, ushlab qolishi, o'rnini almashtirishi va hokazo qilishi mumkin. Ma'lumki, bu hujumda buzg'unchi faol bo'ladi [19].

Protokolning obro'sizlantirilishi (kompromentasiya) – bu protokol oldiga qo'yilgan maqsadlarga erishishga qodir bo'lmay, buzg'unchi protokol asosida yotadigan kattaliklarni va algoritmlarni "ochmasdan" turib faqt protokolni boshqarish yo'li bilangina ustunlikka ega bo'ladigan vaziyat.

Masalan, oqimli shifrlash qo'llanilayotgan bo'lsin. Protokolda uzatilayotgan xabarlar maxsus ko'rinishga egaligi ma'lum bo'lsin, ya'ni: boshlang'ich 20 bitda bir hisob raqamidan boshqa hisob raqamiga o'tkazilayotgan pul miqdorini ifodalovchi ma'lumot shifrlangan holda uzatilayotgan bo'lsin. Faol buzg'unchi boshlang'ich 20 bitni biron bir

kattalik bilan bitma bit qo'shib, pul miqdorini bilmasdan turib o'zgartirishi mumkin.

Kriptografik protokol xavfsizligini tavsiflaydigan xususiyatlar yetarli darajada ko'p bo'lib, odatda protokollarning turli hujumlarga bardoshligi xususiyati xavfsizlik talablarini shakllanishiga olib keladi [19]. Quyida protokol xavfsizligiga oid asosiy talablar keltirildi.

1. Autentifikasiya (noommaviy):
   - Subyekt autentifikasiyasi;
   - Xabar autentifikasiyasi;
   - Takrorlanishdan himoya.
2. Ko'p adreslarga jo'natish yoki yozilish/ma'lum qilish xizmatiga ulanish paytida autentifikasiya:
   - Ishtirokchini oshkor bo'lmagan tarzda (maxfiy) autentifikasiya qilish;
   - Manbani autentifikasiya qilish.
3. Mualliflashtirish (ishonchli uchinchi tomon).
4. Kalitni hamkorlikda generasiyalash xususiyati:
   - Kalitni autentifikasiyalash;
   - Kalit haqiqiyligini tasdiqlash;
   - Orqaga o'qishdan himoyalash;
   - Yangi kalitlarni shakllantirish;
   - Xavfsizlik parametrlari haqida kelishishning himoyalangan imkoni.
5. Konfidensiallik.
6. Anonimlik:
   - Identifikatorlarni eshitishdan himoya qilish (bog'liq bo'lmaslik);
   - Identifikatorlarni boshqa ishtirokchilardan himoya qilish.
7. "Xizmat ko'rsatishni rad etish" hujumidan chekli himoyalanish.
8. Yuboruvchining invariantligi.
9. Avvalgi qilingan amallarni rad eta olmaslik:
   - Hisob berishlik;
   - Manbaning isboti;
   - Qabul qiluvchining isboti.
10. Xavfsiz vaqtinchalik xususiyat.

Xavfsizlik talablariga javob beradigan protokollarni yaratish uchun quyidagi asosiy yondashuvlar ham mavjud [20]:

1. *Hisoblanishi murakkab bo'lgan masalalarga reduksiya prinsipi.* KP larning xavfsizligi protokolda foydalanilgan kriptografik algoritmlar bardoshliligini ta'minlashga asos bo'lgan murakkab muammo (masala) turiga bog'liq bo'ladi. Birgina murakkab bo'lgan masalani yechish kriptografik algoritmni buzish kabi qiyin bo'lgan hisoblashlarni talab etadi. Keyingi yillarda mavjud kriptografik algoritmlar bardoshliligini ta'minlashga asos bo'lgan sonlar nazariyasining mashhur va eng ko'p qo'llaniladigan hisoblash murakkab bo'lgan masalalar tasnifi quyidagi 1.2-jadvalda keltirildi [20].

1.2- jadval

Hisoblash murakkab bo'lgan masalalar tasnifi

Shartli belgilash	***Muammoning nomi***	***Berilishi***	***Topish kerak***
FACTORING	Butun sonlarni faktorlash	butun musbat n son	$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, bunda p^i - o'zaro tub sonlar, $e_i \geq 1$.
RSA	RSA muammosi	$n=p*q$, $ye:EKUB(e,(p-1)(q-1))=1$, $s \in Z$	$m: m^e \equiv c(\text{mod } n)$
SRA	Kuchaytirilgan RSA muammosi	$n=p*q$, $z \in Z_n^*$	$r=r(z)>1$, $y \in Z_n^*: y^r=z$
QRP	Kvadratik chegirma muammosi	n - toq murakkab butun son, $a \in Z: \left(\frac{a}{n}\right)=1$	$a \in QR_n$
SQROOT	n moduli bo'yicha kvadrat ildiz muammosi	n - murakkab butun son $a \in QR_n$	$x: x^2 \equiv a(\text{mod } n)$
DLP	Diskret logarifmlash muammosi	p - tub con, α hosil qiluvchi element Z_p^*, $\beta \in Z_p^*$	$x: 0 \leq x \leq p-2$ $\alpha^x \equiv \beta (mod\ p)$

GDLP	Umumlashgan diskret logarifmlash muammosi	G - n tartibli chekli siklik gruppa, α G ning hosil qiluvchisi, $\beta \in G$	x: $0 \le x \le n-1$, $\alpha^x = \beta$
DHP	Diffi- Xellman muammosi	p- tub son, α - Zp^* hosil qiluvchisi, $\alpha^a \pmod p$, $\alpha^b \pmod p$	$\alpha^{ab} \pmod p$
GDHP	Umumlashgan Diffi- Xellman muammosi	G - chekli siklik gruppa, α - G ni hosil qiluvchisi, α^a, α^b.	α^{ab}
DDHP	Diffi- Xellman muammosini aniqlash	p- tub son, α - Zp^* hosil qiluvchisi, $\alpha^a \pmod p$, $\alpha^b \pmod p$, $\alpha^s \pmod p$	$\alpha^{ab} \equiv \alpha^s \pmod p$
SUBSET	"Ryukzak muammosi"	$\{a_1, a_2, ..., a_n\}$ - butun musbat sonlar to'plami, S - butun musbat son	$\sum_{j \in \{1,...,n\}} a_j = S$
	Daraja parametri muammosi	*1-ta'rif.* $(F_n; \circledR)$-parametrli gruppa, y F_n ning elementi. *2-ta'rif.* $(F_n; \circledR)$-parametrli gruppa, y, a F_n ning elementlari. *Bunda* F_n –n ta butun sonlardan tuzilgan chek-li to'plam, $y \equiv a^{ye} \pmod n$,	R - parametr, ye - daraja ko'rsatkichi, a –element R - parametr, ye - daraja ko'rsatkichi.

Mavjud nosimmetrik kriptotizimlar bardoshliligini ta'minlashga asos bo'lgan hisoblash murakkab bo'lgan masalalar asosan quyidagicha tasniflanadi (1.2-jadval):

- faktorlash muammosining murakkabligiga asoslangan kriptotizimlar [20-22];
- diskret logarifmlash muammosining murakkabligiga asoslangan kriptotizimlar [23-24];
- EEChda diskret logarifmlash muammosining murakkabligiga asoslangan kriptotizimlar [25-26];
- boshqa muammolarga asoslangan kriptotizimlar [27-30].

Mavjud nosimmetrik kriptoalgoritmlar orasida xalqaro va davlat standartlari maqomiga ega bo'lgan algoritmlarning ko'pchiligi faktorlash, diskret logarifmlash, EEChda diskret logarifmlash va daraja parametri muammolarining murakkabligiga asoslangan algoritmlardir.

Simmetrik kriptotizimlar uchun shifrlash kalitini ochiq kanal bo'yicha taqsimlash algoritmlari asosida Diffi-Xellman muammosining murakkabligi yotadi. Shu bois, faktorlash, diskret logarifmlash, EEChda diskret logarifmlash, Diffi-Xellman va daraja parametri muammolarini hal etish ko'pchilik kriptotahlilchilarning e'tiborini o'ziga tortadi.

2. *Buzg'unchining harakatlarini modellash prinsipi.* Protokolni loyihalashda buzg'unchi tomonidan kuzatilgan barcha axborotlar va uni protokol ishtirokchisi sifatidagi (agar buzg'unchi faol bo'lsa) barcha harakatlari aniqlanadi. Shundan keyin esa buzg'unchi protokolda kuzatilishi mumkin bo'lgan barcha axborotlarni ko'rib chiqishni mustaqil ravishda modellash imkoni bo'lgan formal isboti yaratiladi. Boshqa so'z bilan aytganda buzg'unchi mustaqil holda bu protokolni modellash asosida haqiqiy ishtirokchilar protokolni bajarishda oladigan axborotdan ko'p bo'lmagan axborotni oladi [20].

Nazorat savollari

1. Nosimmetrik shifrning simmetrik shifrdan farqi nima?
2. Muhofaza qilinadigan axborotga ta'rif bering va uni qanday muhofaza qilish turlarini bilasiz?
3. Elektron raqamli imzo, xesh-funksiya va autentifikasiyadan nima maqsadda foydalaniladi?
4. Qanday hujum turlari majud? Ularni tushuntirib bering.
5. Protokol nima? U qanday xususiyatlarga ega?
6. Protokolning vazifasi nimadan iborat?
7. Qanday protokol turlarini bilasiz? Ularga misollar keltiring.

8. Kriptografik protokolga ta'rif bering.

9. Kriptografik protokoli ishtirokchilari qanday sinflarga bo'linadi.

10. Kriptografik protokol necha guruhga bo'linadi? Ularning ta'rifi va belgilanishi keltirib o'ting.

11. KPning eng dolzarb xossalarini keltiring.

12. KPning xossalaridan qaysi biri muhim ahamiyatga ega va nima uchun?

13. KPning adaptasiya va mobillilik xossalari orasida qanday farq bor?

14. KPni sinflanishida qanday yondashuvlar mavjud? Ularning har birini sinflab bering.

15. KPlar qanday funksiyalarni bajaradi? KPlar funksiyasiga ko'ra necha turga bo'linadi?

16. Shifrlash protokoli bilan ERI protokoli jarayonlarining farqi nimada?

17. Identifikasiya/autentifikasiya protokoliga izoh bering.

18. Kriptografik protokollarning asosiy vazifalari nimalardan iborat?

19. KPga qilinadigan qanday hujumlarni bilasiz?

20. Protokol xavfsizligiga qanday asosiy talablar qo'yiladi?

21. Xavfsizlik talablariga javob beradigan protokollarni yaratishda qanday yondashuvlardan foydalaniladi?

22. Nosimmetrik kriptotizimlar bardoshliligini ta'minlashda asosan qanday murakkab masalalarga asoslaniladi?

2. AUTENTIFIKASIYA PROTOKOLLARI

2.1. Autentifikasiyaga oid asosiy tushunchalar

Autentifikasiya deganda ishtirokchining dastur, qurilma yoki ma'lumotlarning haqiqiyligini belgilash tartiboti tushuniladi. Autentifikasiya ishtirokchi haqiqatan aynan o'zi ekanligiga ishonch hosil qilishga imkon beradi. Autentifikasiya o'tkazishda tekshiruvchi tomon tekshiriluvchi tomonning haqiqiy ekanligiga ishonch hosil qilish bilan birga tekshiriluvchi tomon ham axborot almashinuv jarayonida faol ishtirok etadi. Odatda ishtirokchi tizimga o'zi haqida maxfiy, boshqalarga ma'lum bo'lmagan axborotni (masalan parol yoki sertifikat) kiritish orqali identifikasiyani tasdiqlaydi. Identifikasiya va autentifikasiya ishtirokchilarning haqiqiy ekanligini aniqlash va tekshirishning o'zaro bog'langan jarayonidir. Muayyan ishtirokchi yoki jarayonning tizim resurslaridan foydalanishga tizimning ruxsati aynan shularga bog'liq [31].

Ishtirokchi o'zining haqiqiyligini tasdiqlash uchun turli asoslarni taqdim etishi mumkin. Ishtirokchi ko'rsatgan asoslarga bog'liq holda autentifikasiya jarayonlari quyidagi kategoriyalarga bo'linishi mumkin: biror narsani bilish asosida, biror narsaga egaligi asosida va qandaydir daxlsiz xarakteristikalar asosida.

AP autentifikasiyalash prosedurasi bo'lib, unda bir-biri bilan o'zaro muloqotga kirishayotgan ikki tomondan biri (yoki ikkalasi ham) boshqasining haqiqiyligini tekshiradi.

Autentifikasiya protokollarining maqsadi o'zini boshqa ishtirokchi qilib tanitish bo'lgan potensial buzg'unchilardan himoyani ta'minlashdir. Shuningdek, AP tekshiruvchiga o'zining haqiqiyligini isbotlovchi tomondan keyinchalik o'zini uning nomidan chiqishiga yordam beruvchi axborotni olish imkoniyatini bermasligi lozim.

Autentifikasiyani uch turga ajratish mumkin: ma'lumotlar manbai autentifikasiyasi (data – origin authentication), mohiyat autentifikasiyasi (entity authentication) va autentifikasiyalangan kalitlarni generasiyalash (authenticationed key establishment). Autentifikasiyaning birinchi turi ma'lumotning e'lon etilgan xossasini tekshirishni bildiradi, ikkinchisi ko'proq e'tiborni ma'lumot jo'natuvchi haqidagi xabarlarning

haqiqiyligiga qaratadi, uchinchisi esa maxfiy ma'lumotlar almashish uchun himoyalangan kanalni tashkil etish uchun mo'ljallangan [31-32].

Ma'lumotlar manbai autentifikasiyasi

Ma'lumotlar manbai autentifikasiyasi (avvallari, ma'lumotlar autentifikasiyasi (message authentication) deb ham atalib kelingan) ma'lumotlar yaxlitligi bilan uzviy bog'langan. Zero, ataylab o'zgartirilgan axborotni qabul qilib olishdagi tavakkalchilik (xavfi) ishonchli bo'lmagan manbadan axborot qabul qilish tavakkalchiligiga (xavfiga) yaqin. Ammo aslida ma'lumotlar manbai autentifikasiyasi va ma'lumotlarni yetishmasligidan himoyalash tushunchalari farqli tushunchalardir. Chunki ma'lumotlar manbai autentifikasiyasi albatta aloqa kanali bilan bog'liq holda qaralib, manba identifikasiyasi (manbani uning identifikatori (nomi, simvollarning noyob satri) bo'yicha aniqlash jarayoni) va ma'lumotlarning yangiligi bilan aloqador bo'lsa, ma'lumotlar yaxlitligini himoyalashda aytilgan belgilar asosiy hisoblanmaydi.

Ma'lumotlar manbai autentifikasiyasi quyidagi amallarni bajarishni nazarda tutadi [31-32].

1. Ma'lumot uni qabul etuvchiga shunday tarzda jo'natiladiki, ma'lumotning haqiqiyligini uni qabul qilishdan avval tekshirib chiqishga imkoniyat bo'lsin.
2. Ma'lumot jo'natuvchisini identifikasiyalash.
3. Jo'natuvchi yuborgan ma'lumotlarning yaxlitligini tekshirish.
4. Ma'lumot jo'natuvchisining kimligini (realligini) tekshirish.

Mohiyat autentifikasiyasi

Mohiyat autentifikasiyasi axborot almashuv jarayoni, ya'ni protokoli bo'lib, uning davomida ishtirokchi boshqa ishtirokchining haqiqiyligiga (lively correspondence) amin bo'ladi.

Aslida AP davomida ma'lumotning haqiqiyligi yoki haqiqiy emasligi ayon bo'ladi. Bunday hollarda ma'lumot va uni muallifining haqiqiyligiga ishonch hosil qilish uchun ma'lumotlar manbai autentifikasiyasi mexanizmlaridan foydalanish lozim.

Tarmoqlangan tizimlarda quyidagi mohiyat autentifikasiyasi ssenariylari amal qiladi. Ulardan ikkitasiga to'xtalamiz.

Ikkita bosh kompyuterlararo (xost-xost tipida, inglizchada - host-host type) ma'lumotlar almashuvi.

Protokol ishtirokchilari kompyuterlar bo'lib, ular tarmoqlangan tizimning tugunlari yoki platformalari deb yuritiladi. Kompyuterlar ishi o'zaro moslashgan bo'lishi zarur. Masalan, agar uzoqlashgan platformalardan biri "qayta yuklanmoqchi bo'lsa" (takroriy inisializasiyalanish), u haqiqiy serverni identifikasiya qilishi lozim va unga kerakli axborotni jo'natishi lozim, masalan, operasion tizimning haqiqiy nusxasini, taymerni yoki atrof-muhitni to'g'ri o'rnatish. Axborot haqiqiyligini aniqlash odatda AP yordamida amalga oshiriladi. Qoida tarzida, ikki bosh kompyuterlararo ma'lumotlar almashuv kliyent-server tizimi sifatida bo'lib, biriga (kliyent) ikkinchisi (server) tomonidan xizmat ko'rsatiladi.

Ishtirokchi va bosh kompyuterlararo (ishtirokchi-xost tipida, inglizchada - user-host type) ma'lumotlar almashinuvi. Ishtirokchi bosh kompyuterda ro'yxatdan o'tib, kompyuter tizimiga kirishga ruxsat oladi. Odatda mijoz bosh kompyuterda tarmoqqa uzoqdan kirish (telnet) orqali ro'yxatdan o'tadi yoki o'z faylini fayl uzatish protokoliga (ftp-file transfer protocol) muvofiq bosh kompyuterga jo'natadi. Ikkala holda ham parolni autentifikasiyalash protokoli ishga tushadi. Ayrim hollarda, masalan, kredit kartochkalar bo'yicha to'lovlarda, o'zaro autentifikasiyalash (mutual authentication) zarur bo'ladi.

Subyekt o'zining haqiqiyligini tasdiqlash uchun tizimga turli ma'lumotlarni taqdim etishi mumkin, masalan, parol, shaxsiy identifikasiya kodi, shaxsiy kalit bilan shifrlangan xabar, smart-karta, biometrik belgi, barmoq izi, so'rovga javob, raqamli sertifikat, imzo va shunga o'xshashlar [31].

Autentifikasiyalangan kalitlarni generasiyalash

Odatda axborot almashuvchi tomonlar muloqotni yanada yuqsakroq pog'onaga ko'tarish maqsadida mohiyat autentifikasiyasi protokolini ishga tushiradilar. Zamonaviy kriptografiyada himoyalangan aloqa kanallarini tashkil etishda kriptografik kalitlardan foydalaniladi. Binobarin, mohiyat autentifikasiyasi protokoli himoyalangan aloqa kanallari orqali axborot almashish uchun tarkibiy qism sifatida *autentifikasiyalangan kalitlarni generasiyalash* yoki *kalit almashish* (key exchange) yoki *kalitlarni muvofiqlashtirish* (key agreement) mexanizmlarini o'z ichiga olishi lozim.

Autentifikasiyalangan kalitlarni generasiyalash protokolida protokol ma'lumotlari o'zida kalitlar parametrlarini aks ettirgani bois, ularning manbaini ham autentifikasiyadan o'tkazish lozim.

Adabiyotlarda autentifikasiyalangan kalitlarni generasiyalash protokoli, mohiyat autentifikasiyasi protokoli, ma'lumotlarni himoyalash protokoli, hattoki kriptografik protokollar ham ko'pincha aloqa protokollari deb nomlanadi.

Barcha autentifikasiyalash protokollarini uch sinfga bo'lish mumkin [33]:

1.Biron narsani bilish asosida. Eng keng tarqalgan varianti – parollar;

2.Biron narsaga egalik qilish asosida (magnit kartalar, smart-kartalar va hokazo);

3.Ajralmas xususiyatlar asosida (ovoz, ko'zning to'r pardasi, barmoq izlari). Bu kategoriyada kriptografik usullar odatda qo'llanilmaydi.

Autentifikasiyalash protokollarini taqqoslashda va tanlashda quyidagi xarakteristikalarni hisobga olish zarur [33]:

- o'zaro autentifikasiyaning mavjudligi. Ushbu xususiyat autentifikasiyali almashinuv taraflari o'rtasida ikkiyoqlama autentifikasiyalashning zarurligini aks ettiradi;
- hisoblash samaradorligi. Protokolni bajarishda zarur bo'lgan amallar soni;
- kommunikasion samaradorlik. Ushbu xususiyat autentifikasiyalashni bajarish uchun zarur bo'lgan xabarlar soni va uzunligini aks ettiradi;
- ikkinchi tarafning mavjudligi. Ushbu tarafga misol tariqasida simmetrik kalitlarni taqsimlovchi ishonchli serverni yoki ochiq kalitlarni taqsimlash uchun sertifikatlar daraxtini amalga oshiruvchi serverni ko'rsatish mumkin;
- xavfsizlik kafolat asosi. Misol sifatida nollik bilim bilan isbotlash xususiyatiga ega bo'lgan protokollarni ko'rsatish mumkin;
- sirni saqlash. Jiddiy kalitli axborotni saqlash usuli ko'zda tutiladi.

2.2. Protokollarga qilinadigan hujum turlari

Kriptografik hujumlar protokollarda ishlatiladigan kriptografik algoritmlarga, algoritm va protokollarni tadqiq qilishda ishlatiladigan

kriptografik usullarga yoki protokollarning o'ziga yo'naltirilgan bo'lishi mumkin. Bu bo'limda protokollar haqida gap ketar ekan, kriptografik algoritm va usullar ishonchli deb xisoblanadi. Bu yerda faqat protokollarga qilinadigan hujumlar ko'rib o'tiladi.

Protokollarga qaratilgan hujumlarda odamlar ko'pgina usullarni qo'llashi mumkin. Ba'zi jinoyatkorlar protokolda ishtirok etmay turib protokolni to'liq yoki qisman "eshitishi" mumkin. Bu usul *passiv hujum* deb ataladi, chunki buzg'unchi protokolga hyech qanday ta'sir ko'rsatmaydi. U faqat protokolni kuzatishi va axborot olishga urinishi mumkin. Bu turdagi hujumlar faqat shifrmatn asosidagi hujumlarga mos keladi. Chunki passiv ochilishlarni aniqlash qiyin, protokollar ularni aniqlashga emas, balki qaytarishga urinishadi. Bizning protokollarda "eshituvchi" rolini Ye bajaradi.

Boshqa holatda esa buzg'unchi protokolni o'zining foydasiga moslab o'zgartirishga urinishi mumkin. Shu maqsadda u o'zini boshqa odam sifatida ko'rsatishi, protokolga yangi axborotlar kiritishi, bir axborotni boshqa axborotga almashtirishi, qaytadan eski axborotlarni jo'natishi, aloqa liniyasini uzishi yoki kompyuterda saqlanadigan axborotni modifikasiya qilishi (o'zgartirishi) mumkin. Bunday harakatlar *aktiv hujum* deb ataladi. Bunday hujumlarning shakli tarmoq standartiga bog'liq [33].

Passiv buzg'unchilar protokol ishtirokchilari haqidagi ma'lumotni olishga urinishadi. Ular turli tomonlardan yuborilgan xabarlarni yig'adilar va kriptotahlil qilishga urinadilar. Aktiv ta'sir qiluvchilarning urinishlari kengroq maqsadni ko'zlaydi. Buzg'unchi axborot olishdan, tizim tezligining pasayishidan yoki resurslardan ruxsatsiz foydalana olishdan manfaatdor bo'lishi mumkin.

Aktiv hujumlar passivlarga nisbatan ancha xavfli. Ayniqsa bu tomonlar bir-biriga ishonishi shart bo'lmagan protokollarga tegishli. Buzg'unchi sifatida har doim ham mutlaqo begona odam ishtirok etmaydi. U tizimning registrasiya qilingan ishtirokchisi yoki tizim administratori yoki kelishgan holda ishlovchi jinoyatkorlar guruhi bo'lishi mumkin. Bu yerda g'arazli aktiv buzg'unchi rolini M o'ynaydi.

Buzg'unchi sifatida protokol ishtirokchilaridan biri bo'lishi mumkin. Protokolni bajarib u hamkasblarini aldashi yoki umuman protokolga rioya etmasligi mumkin. Bunday buzg'unchi *firibgar* deb aytiladi. Passiv firibgarlar protokolni bajaradilar, ammo, protokolda mo'ljallangan

axborotdan tashqari yana ko'proq axborot olishga urinishadi. Aktiv firibgarlar protokolning normal bajarilishini buzadilar.

Agar protokol ishtirokchilarining ko'pi – aktiv firibgarlar bo'lishsa, u holda protokolning ishonchliligini ushlab turish qiyin. Ammo ba'zan qonuniy ishtirokchilar aktiv firibgarlarni aniqlashi mumkin. Albatta, protokollarni passiv firibgarlardan ham himoyalash kerak.

Autentifikasiya protokollariga qo'llaniladigan namunaviy hujum turlari asosan sakkiz turda bo'lib ular quyidagilardan iborat [33]:

1. *Xabarni qayta yuborish hujumi* - bu hujumda buzg'unchi avvaldan protokolning oldingi seansida tutib olingan eski xabarni yozib qo'yadi va uni yangi seansda qayta yuboradi.

2. *"O'rtadagi odam" hujumi* - bu hujum asosan o'zaro autentifikasiya qilishni ko'zda tutmaydigan protokollarga qo'llaniladi. Bunday hujum asnosida buzg'unchi protokol ishtirokchilaridan birining qiyin savollarini boshqa ishtirokchiga jo'natishi va unga javob olishi keyin so'rovchiga yuborishi mumkin va aksincha.

3. *Parallel seans yordamidagi hujum* - bu hujumda buzg'unchi boshchiligida bir nechta protokol bajariladi. Parallel seanslar buzg'unchiga biror seansdagi qiyin savollarga javob uchun boshqa seanslarda olingan axborotdan foydalanish imkonini beradi.

4. *Xabarlarni akslantirish yordamida hujum* - xabarlarni akslantirish yordamida hujumda buzg'unchi qonuniy ishtirokchini keyingi kriptografik ishlov berish uchun o'zining sherigiga yuborgan xabarni tutib qoladi va uni orqaga qaytarib yuboradi. Bunda akslantirilgan xabar "orqaga qaytarilgan xabarning" aynan o'zi bo'lmaydi, chunki buzg'unchi quyi darajali protokol bilan ismi va manzilini o'zgartiradi, shuning uchun xabarning muallifi o'z matnini tanimaydi.

5. *Xabar almashinuvi yordamida hujum* – bu hujum vaqtida buzg'unchi bir nechta protokollarning xabarlarni almashtirib amalga oshiradi. Buzg'unchi xabar tuzadi va uni protokol ishtirokchilaridan biriga yuboradi va javobini kutadi. So'ngra u olingan javobni ikkinchi ishtirokchiga boshqa protokol doirasida yuboradi, uning javobini olgandan so'ng keyingi ishtirokchiga jo'natadi va hokazo.

6. *Noto'g'ri talqin etish asosidagi hujum* – bu hujumda buzg'unchi qonuniy ishtirokchining xabarni yoki xabarlar to'plamini ma'nosini aniqlay olmaganidan foydalanadi. Ko'pincha noto'g'ri talqin etish ishtirokchiga tasodifiy sonni, vaqt belgisi (VB)ni, ism, shifrlangan

kalitni aldash yo'li bilan noto'g'ri talqin etishiga majburlaganda paydo bo'ladi.

7. *Nomsiz xabarlar asosidagi hujum* - Autentifikasiyalash protokollarida xabar muallifi ismini va shifrlash kalitini kontekstdan aniqlash mumkin. Ammo ba'zan bunday qilish mumkin bo'lmasligi, ya'ni ismining yo'kligi katta muammolarni keltirib chiqaradi.

8. *Kriptografik amallarni noto'g'ri bajarishga asoslangan hujum* – bu hujum protokollardagi eng keng tarqalgan nuqson hisoblanib, bu kamchilak ikki holatda paydo bo'ladi:

1) ma'lumotlar yaxlitligi himoyasining mavjud emasligi oqibatidagi hujum. Bunda buzg'unchi ma'lumotlar yaxlitligi himoyasining mavjud emasligi oqibatida zaiflashgan protokolga hujum qiladi.

2) "ma'noga ega turg'unlik" mavjud emasligi oqibatidagi maxfiylikning buzilishi. Protokol nuqsonidan foydalangan buzg'unchi shifrlangan matndagi maxfiy xabar haqidagi qisman ma'lumotni olishi mumkin va kriptoprotokolni buzmagan holatda "hammasi yoki hyech narsa" prinsipidagi hujumni tashkil etishi mumkin.

Yuqorida keltirilgan hujumlarni bartaraf qilish uchun autentifikasiyalash protokollarini qurishda quyidagi usullardan foydalaniladi [34]:

– «so'rov-javob», vaqt belgilari, tasodifiy sonlar, indentifikatorlar, raqamli imzolar kabi mexanizmlardan foydalanish;

– autentifikasiya natijasini ishtirokchilarning tizim doirasidagi keyingi harakatlariga bog'lash. Shunday yondashish misol tariqasida autentifikasiyalash jarayonida ishtirokchilarning keyingi o'zaro aloqalarida ishlatiluvchi maxfiy seans kalitlarini almashishni ko'rsatish mumkin;

– aloqaning o'rnatilgan seansi doirasida autentifikasiya muolajasini vaqti-vaqti bilan bajarib turish va hakozo.

«So'rov-javob» mexanizmi quyidagicha. Agar **A** ishtirokchi **V** ishtirokchi dan oladigan xabari yolg'on emasligiga ishonch hosil qilishni istasa, u **V** ishtirokchi uchun yuboradigan xabarga oldindan bilib bo'lmaydigan element – X so'rovini (masalan, qandaydir tasodifiy sonni) qo'shadi. **V** ishtirokchi javob berishda bu amal ustida ma'lum amalni (masalan, qandaydir $f(X)$ funksiyani hisoblash) bajarishi lozim. Buni oldindan bajarib bo'lmaydi, chunki so'rovda qanday tasodifiy son X kelishi **V** ishtirokchiga ma'lum emas. **V** ishtirokchi harakati natijasini olgan **A** ishtirokchi **V** ishtirokchining haqiqiy ekanligiga ishonch hosil

qilishi mumkin. Ushbu usulning kamchiligi – so'rov va javob o'rtasidagi qonuniyatni aniqlash mumkinligi.

Vaqtni belgilash mexanizmi har bir xabar uchun vaqtni qaydlashni ko'zda tutadi. Bunda tarmoqning har bir ishtirokchisi kelgan xabarning qanchalik eskirganini aniqlashi va uni qabul qilmaslik qaroriga kelishi mumkin, chunki u yolg'on bo'lishi mumkin. Vaqtni belgilashdan foydalanishda seansning haqiqiy ekanligini tasdiqlash uchun *kechikishning joiz vaqt oralig'i* muammosi paydo bo'ladi. Chunki "vaqt belgisi"li xabar, umuman, bir lahzada uzatilishi mumkin emas. Undan tashqari, qabul qiluvchi va jo'natuvchining soatlari mutlaqo sinxronlangan bo'lishi mumkin emas [33].

2.3. Parol yordamidagi autentifikasiya

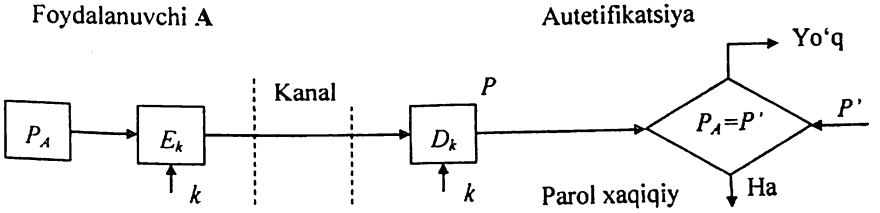
Autentifikasiyalashning keng tarqalgan sxemalaridan biri oddiy autentifikasiyalash bo'lib, u an'anaviy ko'p martali parollarni ishlatishga, ya'ni parollar va raqamli sertifikatlardan foydalanishga asoslangan [31]. Tarmoqdagi ishtirokchini oddiy autentifikasiyalash jarayonini quyidagicha tasavvur etish mumkin. Tarmoqdan foydalanishga uringan ishtirokchi kompyuter klaviaturasida o'zining identifikatori va parolini teradi. Bu ma'lumotlar autentifikasiya serveriga ishlash uchun tushadi. Autentifikasiya serverida saqlanayotgan ishtirokchi identifikatori bo'yicha ma'lumotlar bazasidan mos yozuv topiladi. Undan parolni topib ishtirokchi kiritgan parol bilan taqqoslanadi. Agar ular mos kelsa, autentifikasiyalash muvaffaqiyatli bo'lgan hisoblanadi va ishtirokchi legal (qonuniy) maqomini va mualliflashgan tizimi orqali uning maqomi uchun aniqlangan huquqlarni va tarmoq resurslaridan foydalanishga ruxsatni oladi.

Parol – ishtirokchi hamda uning axborot almashuvidagi sherigi biladigan narsa.

Paroldan foydalangan holda oddiy autentifikasiya sxemasi 2.1-rasmda keltirilgan.

Ma'lumki, ishtirokchining parolini shifrlamasdan uzatish orqali autentifikasiya varianti xavfsizlikning hatto minimal darajasini kafolatlamaydi. Parolni himoyalash uchun uni himoyalanmagan kanal orqali uzatishdan oldin shifrlash zarur. Buning uchun sxemaga shifrlash E_k va shifrni ochish D_k vositalari kiritilgan. Bu vositalar bo'linuvchi maxfiy

kalit k orqali boshqariladi. Ishtirokchining haqiqiyligini tekshirish ishtirokchi yuborgan parol P_A bilan autentifikasiya serverida saqlanuvchi dastlabki qiymat P'_A ni taqqoslashga asoslangan. Agar P_A va P'_A qiymatlar mos kelsa, P_A parol haqiqiy, A ishtirokchi esa qonuniy hisoblanadi.



2.1- rasm. Paroldan foydalangan holda oddiy autentifikasiyalash

Oddiy autentifikasiyani tashkil etish sxemalari nafaqat parollarni uzatish, balki ularni saralash va tekshirish turlari bilan ajralib turadi. Eng keng tarqalgan usul – ishtirokchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o'qish va yozishdan himoyalash atributlari o'rnatiladi (masalan, operasion tizimdan foydalanishni nazoratlash ro'yxatidagi mos imtiyoztarni tavsiflash yordamida). Tizim ishtirokchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funksiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi – niyati buzuq odamning tizimning ma'mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan, parol fayllaridan foydalanish imkoniyatidir [14, 32].

Xavfsizlik nuqtai nazaridan parollarni bir tomonlama funksiyalardan foydalanib uzatish va saqlash qulay hisoblanadi. Bu holda ishtirokchi parolning ochiq shakli o'rniga uning bir tomonlama funksiyadan foydalanib olingan tasvirini yuborishi shart. Bu o'zgartirish g'anim tomonidan parolni uning tasviri orqali oshkor qila olmaganligini kafolatlaydi, chunki g'anim yechilmaydigan sonli masalaga duch keladi.

Ko'p martali parollarga asoslangan oddiy autentifikasiyalash tizimining bardoshligi past, chunki ularda autentifikasiyalovchi axborot ma'noli so'zlarning nisbatan katta bo'lmagan to'plamidan jamlanadi. Ko'p martali parollarning ta'sir muddati tashkilotning xavfsizligi siyostida

belgilanishi va bunday parollarni muntazam ravishda almashtirib turish lozim. Parollarni shunday tanlash lozimki, ular lug'atda bo'lmasin va ularni topish qiyin bo'lsin.

Bir martali parollarga asoslangan autentifikasiyalashda foydalanishga har bir so'rov uchun turli parollar ishlatiladi. Bir martali dinamik parol faqat tizimdan bir marta foydalanishga yaroqli. Agar hatto kimdir uni ushlab qolsa ham, parol foyda bermaydi. Odatda bir martali parollarga asoslangan autentfikasiyalash tizimi masofadagi ishtirokchilarni tekshirishda qo'llaniladi.

Bir martali parollarni generasiyalash apparat yoki dasturiy usul orqali amalga oshirilishi mumkin. Bir martali parollar asosidagi foydalanishning apparat vositalari tashqaridan to'lov plastik kartochkalariga o'xshash mikroprosessor o'rnatilgan miniatyur qurilmalar ko'rinishda amalga oshiradi. Odatda, kalitlar deb ataluvchi bunday kartalar klaviaturaga va katta bo'lmagan displey darchasiga ega.

Ishtirokchilarni autentifikasiyalash uchun bir martali parollarni qo'llashning quyidagi usullari ma'lum [14, 32]:

1. Yagona vaqt tizimiga asoslangan vaqt belgilari mexanizmidan foydalanish;
2. Qonuniy ishtirokchi va tekshiruvchi uchun umumiy bo'lgan tasodifiy parollar ro'yxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanish;
3. Ishtirokchi va tekshiruvchi uchun umumiy bo'lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanish.

Birinchi usulni amalga oshirish misoli sifatida SecurID autentifikasiyalash texnologiyasini ko'rsatish mumkin. Bu texnologiya SecurID Dynamics kompaniyasi tomonidan ishlab chiqilgan qator kompaniyalarning, xususan SecurID kompaniyasining serverlarida amalga oshirilgan. Vaqt sinxronizasiyasidan foydalanib autentifikasiyalash sxemasi tasodifiy sonlarni ma'lum vaqt oralig'idan so'ng generasiyalash algoritmiga asoslangan. Autentifikasiyalash sxemasi quyidagi ikkita parametrdan foydalanadi:

- har bir ishtirokchiga atalgan va autentifikasiya serverida hamda ishtirokchining apparat kalitida saqlanuvchi noyob 64 bitli sondan iborat maxfiy kalit;
- joriy vaqt qiymati.

Masofadagi ishtirokchi tarmoqdan foydalanishga uringanida undan

shaxsiy identifikasiya nomeri PINni kiritish taklif etiladi. PIN to'rtta o'nli raqamdan va apparat kaliti displeyida akslanuvchi tasodifiy sonning oltita raqamidan iborat. Server ishtirokchi tomonidan kiritilgan PIN koddan foydalanib, ma'lumotlar bazasidagi ishtirokchining maxfiy kaliti va joriy vaqt qiymati asosida tasodifiy sonni generasiyalash algoritmini bajaradi. So'ngra server generasiyalangan son bilan ishtirokchi kiritgan sonni taqqoslaydi. Agar bu sonlar mos kelsa, server ishtirokchiga tizimdan foydalanishga ruxsat beradi [14, 32].

Autentifikasiyalashning bu sxemasidan foydalanishda apparat kalit va serverning qat'iy vaqti sinxronlanishi talab etiladi. Chunki apparat kalit bir necha yil ishlashi va demak, server ichki soati bilan apparat kalitining muvofiqligi asta-sekin buzilishi mumkin.

Ushbu muammoni hal etishda Security Dynamics kompaniyasi quyidagi ikki usuldan foydalanadi:

- apparat kaliti ishlab chiqilayotganida uning taymer chastotasining me'yoridan chetlashishi aniq o'lchanadi. Chetlashishning bu qiymati server algoritmi parametri sifatida hisobga olinadi;
- server muayyan apparat kalit generasiyalagan kodlarni kuzatadi va zaruriyat tug'ilganida ushbu kalitga moslashadi.

Autentifikasiyaning bu sxemasi bilan yana bir muammo bog'liq. Apparat kalit generasiyalagan tasodifiy son katta bo'lmagan vaqt oralig'i mobaynida haqiqiy parol hisoblanadi. Shu sababli. umuman, qisqa muddatli vaziyat sodir bo'lishi mumkinki, xaker PIN kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizasiyasiga asoslangan autentifikasiya sxemasining eng zaif joyi hisoblanadi [14, 32].

Bir martali paroldan ishtirokchi autentifikasiyalashni amalga oshiruvchi yana bir variant – «so'rov-javob» sxemasi bo'yicha autentifikasiyalash. Ishtirokchi tarmoqdan foydalanishga uringanida server unga tasodifiy son ko'rinishidagi so'rovni uzatadi. Ishtirokchining apparat kaliti bu tasodifiy sonni, masalan. DES algoritmi va ishtirokchining apparat kaliti xotirasida va serverning ma'lumotlar bazasida saqlanuvchi maxfiy kaliti yordamida shifrni ochadi. Tasodifiy son - so'rov shifrlangan ko'rinishda serverga qaytariladi. Server ham o'z navbatida o'sha DES algoritmi va serverning ma'lumotlar bazasidan olingan ishtirokchining maxfiy kaliti yordamida o'zi generasiyalagan tasodifiy sonni shifrlaydi. So'ngra server shifrlash natijasini apparat kalitidan kelgan son bilan

taqqoslaydi. Bu sonlar mos kelganida ishtirokchi tarmoqdan foydalanishga ruxsat oladi. Ta'kidlash lozimki, «so'rov-javob» autentifikasiyalash sxemasi ishlatishda vaqt sinxronizasiyasidan ishtirokchi autentifikasiya sxemasiga qaraganda murakkabroq.

Ishtirokchini autentifikasiyalash uchun bir martali paroldan foydalanishning ikkinchi usuli ishtirokchi va tekshiruvchi uchun umumiy bo'lgan tasodifiy parollar ro'yxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanishga asoslangan. Bir martali parollarning bo'linuvchi ro'yxati maxfiy parollar ketma-ketligi yoki to'plami har bir parol faqat bir marta ishlatiladi. Ushbu ro'yxat autentifikasiyalash almashinuvi taraflari o'rtasida oldindan taqsimlanishi shart. Ushbu usulning bir variantiga binoan so'rov-javob jadvali ishlatiladi. Bu jadvalda autentifikasiyalash uchun taraflar tomonidan ishlatiluvchi so'rovlar va javoblar mavjud har bir juft faqat bir marta ishlatilishi shart [32].

Ishtirokchini autentifikasiyalash uchun bir martali paroldan foydalanishning uchinchi usuli ishtirokchi va tekshiruvchi uchun umumiy bo'lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanishga asoslangan. Bu usulni amalga oshirishning quyidagi variantlari mavjud:

- o'zgartiriluvchi bir martali parollar ketma-ketligi. Navbatdagi autentifikasiyalash seansida ishtirokchi aynan shu seans uchun oldingi seans parolidan olingan maxfiy kalitda shifrlangan parolni yaratadi va uzatadi;
- o'zgarmas parolli (bir tomonlama funksiyaga asoslangan parollar ketma-ketligi). Ushbu usulning mohiyatini bir tomonlama funksiyaning ketma-ket ishlatilishi (Lamportning mashhur sxemasi) tashkil etadi. Xavfsizlik nuqtai nazaridan bu usul ketma-ket o'zgartiriluvchi parollar usuliga nisbatan afzal hisoblanadi [32].

Quyidagi misollarda isbotlovchi ishtirokchi **P** belgisi bilan belgilanadi, Prover so'zidan olingan. Tekshiruvchi ishtirokchi **V** belgisi bilan belgilanadi, Verifier so'zidan olingan.

O'zgartiriluvchi bir martali parolli AP

1. Bunday sxemalardan biri shundan iboratki, **P** va **V** $\pi_1, \ldots \pi_n$ parollarning umumiy ro'yxatiga ega bo'ladi va autentifikasiya KPdagi parollarni almashtirish tartibini kelishib olishadi.

2. Boshqa sxema quyidagi algoritm bo'yicha yangi parollarni hosil qiladi.

Avval **P** va **V** π_0 bitta umumiy paroliga ega bo'lishadi. **P** va **V** autentifikasiyasining har bir seansida o'zining $i=0,1\ldots$ tartib raqamiga egadirlar. i raqamli autentiqikasiya seansida π_i paroli ishlatiladi. $\pi_1,\ldots$ parollari **P** tomonidan hosil qiladi. Taxmin qilinadiki, **P** va **V** har bir π_i paroli bo'yicha K_{π_i} shifrlash kalitini hosil qiladigan algoritmni qo'llaydi. **P** ni **V** bilan autentifikasiyasining i-seansi quyidagi jo'natmadan iborat

$$P \to V : K_{\pi_i}(\pi_{i+1}).$$

Bunda **P** **V** ga autentifikasiyaning navbatdagi seansida ishlatiladigan parolni yuboradi.

3. Yana bir sxema h xesh-funksiyasini ishlatadi.

P va **V** ular amalga oshirmoqchi bo'lgan maksimal sonli autentifikasiya seansini aks ettiruvchi n sonini tanlab olishadi. **P** tasodifiy N satrini tanlaydi va parollar ketma-ketligini hosil qiladi.

$$\pi_0 := N,$$

$$\pi_1 := h(N),$$

$$\ldots$$

$$\pi_{n+1} := h^{(n+1)}N.$$

V esa qandaydir yo'l bilan π_{n+1}ni oladi.

Autentifikasiyaning i-seansi (bu yerda i=1,...,n) quyidagi amalni o'z ichiga oladi:

$$P \to V : P, i, \pi_{n-i+1}.$$

π_{n-i+1} belgisi ushbu seansda ishlatilgan parolni ifodalaydi.

Har bir autentifikasiya seansida **V** ishtirokchi

- $h(\pi) = \pi'$ tengligini tekshiradi, bu yerda π - bu seansdagi **P** yuborgan parol, π' - avvalgi seansda ishlatilgan parol (agar $i=1$, $\pi' = \pi_{n+1}$);
- navbatdagi seansda tekshirishda foydalaniladigan π parolini eslab qoladi.

4. Parollar ketma-ketligini hosil qilishning yana bir sxemasini keltirish mumkin. Bunda har bir yangi parol hosil qilinganda avvalgi parol generasiyasida qo'llanilgan bitli satr ishlatiladi.

O'zgarmas parolli (bir tomonlama funksiyaga asoslangan parolli) AP

O'zgarmas parolli AP birgina xabarni yuborishdan iborat bo'lib, u quyidagi ko'rinishga ega:

$P \rightarrow V : (P, пароль, ресурс)$

Parolni tutib olish yoki saralash yo'li bilan buzib ochishdan himoyalanish uchun "tuzlangan" ("podsolenniye"), ya'ni katta tasodifli bitli satrlar qo'shilgan oddiy parollardan iborat bo'lgan parolni qo'llasa bo'ladi. Bu holatda **P** ishtirokchi parolni o'rniga quyidagi satrni yuboradi

h(parol tuz)

Bu yerda h – qaysidir xesh-funksiya.

Keng tarqalgan bir martali paroldan foydalanishga asoslangan autentifikasiyalash protokollaridan biri Internetda standartlashtirilgan S/Key (RFC1760) protokolidir. Ushbu protokol masofadagi ishtirokchilarning haqiqiyligini tekshirishni talab etuvchi ko'pgina tizimlarda, xususan, Cisco kompaniyasining TACACS+ tizimida amalga oshirilgan [32].

2.4. Xavfsizlikni ta'minlaydigan autentifikasiya

Autentifikasiya protokollari xavfsizlikni ta'minlash darajasiga ko'ra quyidagicha tasniflanadi:

1. Oddiy autentifikasiyalash, ya'ni parollar va raqamli sertifikatlardan foydalanishga asoslangan autentifikasiya protokollari. Xavfsizlik nuqtai nazaridan bunday usul juda zaif, chunki fayl parollar bilan buzg'unchi tomonidan o'g'irlanishi mumkin. Shuning uchun maxsus faylda parollarning faqat xeshlarini saqlash ishonchliroq bo'ladi.

2. Kriptografik usullar va vositalarga asoslangan qatiy autentifikasiya protokollari. Qat'iy autentifikasiyalashda ko'p xollarda ishtirokchi ma'lum yopiq kalitga egalik qilish belgisi asosida identifikasiyalanadi, lekin kalitning o'zi protokol davomida oshkor etilmaydi.

3. E'lon qilinganligi nolga teng bo'lgan bilim bilan isbotlanadigan autentifikasiya protokollari.

4. Biometrik autentifikasiya protokollari.

Xavfsizlik nuqtai nazaridan yuqorida keltirilganlarning har biri o'ziga xos masalalarni yechishga imkon beradi. Shu sababli autentifikasiya jarayonlari va protokollari amalda faol ishlatiladi. Shu bilan bir qatorda ta'kidlash lozimki nollik bilim bilan isbotlash xususiyatiga ega bo'lgan autentifikasiyaga qiziqish amaliy xarakterga nisbatan ko'proq nazariy xarakterga ega.

Qat'iy autentifikasiyada isbotlovchi tomon qandaydir sirni bilishini namoyon etgan holda tekshiruvchiga o'zining haqiqiy ekanligini isbotlaydi. Masalan bu sir autentifikasiyali almashish tomonlari o'rtasida oldindan xavfsiz usul bilan taqsimlangan bo'lishi mumkin. Sirni bilishlik isboti kriptografik usullar va vositalardan foydalanilgan holda so'rov va javob ketma-ketligi yordamida amalga oshiriladi. Eng muhimi, isbotlovchi tomon faqat sirni bilishligini namoyish etadi, sirni o'zi esa autentifikasiyali almashuv mobaynida ochilmaydi. Bu tekshiruvchi tomonning turli so'rovlariga isbotlovchi tomonning javoblari yordami bilan ta'minlanadi. Bunda yakuniy so'rov faqat ishtirokchi siriga va protokol boshlanishida ixtiyoriy tanlangan katta sondan iborat boshlang'ich so'rovga bog'liq bo'ladi [14].

Xalqaro X.509 standarti tavsiyalariga binoan qat'iy autentifikasiyalashning quyidagi tartibotlari farqlanadi [30]:

- bir tomonlama autentifikasiya;
- ikki tomonlama autentifikasiya;
- uch tomonlama autentifikasiya.

Bir tomonlama autentifikasiyalash bir tomonga yo'naltirilgan axborot almashinuvini ko'zda tutadi. Bir tomonlama APda ishtirokchilardan faqat bittasi o'zining haqiqiyligini boshqa ishtirokchiga isbotlaydi. Bunday KPning ishi bir necha raunddan iborat bo'ladi. Har bir raundda quyidagilar amalga oshiriladi:

1. Isbotlovchi ishtirokchi **P** tekshiruvchi ishtirokchiga o'zining haqiqiyligining dalilini taqdim qiladi va
2. Tekshiruvchi ishtirokchi **V** dalilni tekshiradi va qaror qabul qiladi: taqdim qilingan dalilni tan oladi yoki yo'q.

Masalan, **R** sifatida kredit kartochka va **V** sifatida bankomat bo'lishi mumkin.

Qoidaga ko'ra har bir raundda

- **V** ishtirokchi **R** ishtirokchiga qandaydir savol yuboradi va,
- Bu raunddagi **R** tomonidan **V** ga yuboriladigan o'z haqiqiyligining isboti sifatidagi xabar bu savolga javob hisoblanadi.

Bu raunda unga **V** yuborgan javobni **V** har bir raundda to'g'ri deb topgan holda **P** autentifikasiyadan o'tadi.

Qayta yuborish hujumidan himoyalanish uchun har bir savol va javobga tasodifiy satr yoki VBni qo'shib qo'yish mumkin. Bu holatda

javobni tekshirish jarayonida quyidagicha qo'shimcha qayta tekshirish ishi amalga oshiriladi [32]:

Javob tarkibidagi tasodifiy satr savol tarkibidagi tasodifiy satr bilan solishtiriladi yoki javobdagi VB berilgan $[t_{min}, t_{max}]$ oraliqqa tegishliligi tekshiriladi.

Bir tomonlama autentifikasiyalash quyidagilarga imkon yaratadi:

- uzatiladigan axborot yaxlitligini buzilishini aniqlash;
- uzatishning takroriy tipdagi hujumni aniqlash;
- uzatilayotgan autuntifikasion ma'lumotlardan faqat tekshiruvchi tomon foydalanishini kafolatlash.

Ikki tomonlama autentifikasiyalashda bir tomonliligiga nisbatan isbotlovchi tomonga tekshiruvchi tomonning qo'shimcha javobi bo'ladi. Bu javob tekshiruvchi tomonni alokaning aynan autentifikasiya ma'lumotlari mo'ljallangan tomon bilan o'rnatilayotganiga ishontirishi lozim.

Quyida ikki tomonlama APga bir qancha sodda misollar ko'riladi.

1. Simmetrik shifrtizim va tasodifiy satrni qo'llaydigan KPlar [32]

:

- $B \rightarrow A: N_B$
- $A \rightarrow B: K_{AB}(N_A, N_B, B)$
- $B \rightarrow A: K_{AB}(N_A, N_B)$

2. ERI va vaqt tasodifiy satrni qo'llaydigan KPlar:

- $B \rightarrow A: N_B$
- $A \rightarrow B: S_A(N_A, N_B, B)$
- $B \rightarrow A: S_B(N_B, N_A, A)$

3. Xesh-funksiya va tasodifiy satrni qo'llaydigan KPlar:

- $B \rightarrow A: N_B$
- $A \rightarrow B: N_A, h(A, N_A, N_B)$
- $B \rightarrow A: h(N_A, B)$

Uch tomonlama autentifikasiyalash tarkibida isbotlovchi tomondan tekshiruvchi tomonga qo'shimcha ma'lumotlar uzatish mavjud. Bunday yondashish autentifikasiya o'tkazishda vaqt belgilaridan foydalanishdan voz kechishga imkon beradi.

Quyida qatiy autentifikasiya protokollaridan biri sifatida sertifikat va ERIdan foydalanishga asoslangan AP bayon etilgan [33].

Xalqaro X.509 standarti ERI, VB va tasodifiy sonlardan foydalanib, quyidagi bir tomonlama autentifikasiyalash protokollarini tavsiya etadi.

B *ishtirokchi tomonidan* **A** *ishtirokchini bir tomonlama autentifikasiyalash.*

1. **A** ishtirokchi o'z shaxsiy kaliti bilan shifrmatn $S_A(t_A, B)$ ni shakllantiradi va uni o'z ichiga olgan quyidagi xabarni **B** ishtirokchi manziliga jo'natadi:

$$A \rightarrow B: cert_A, t_A, B, S_A(t_A, B),$$

bu yerda $\rightarrow$ - jo'natma yo'nalishi belgisi, $cert_A$ - A ishtirokchining sertifikati, B - ishtirokchining identifikatori, t_A - VB.

B ishtirokchi xabar $(cert_A', t_A', B', S_A'(t_A, B))$ ni olgandan so'ng $cert_A'$ dagi oshkora kalitdan foydalanib shifrmatn $S_A'(t_A, B)$ ni t_A, **B** ga aylantiradi va ularni xabardagi VB t_A', o'zining identifikatori B' bilan taqqoslaydi. Agar taqqoslanuvchi qiymatlar teng bo'lmasa, unda **A** haqiqiy emas, aks holda haqiqiy degan xulosa chiqariladi va keyingi qadamga o'tiladi.

2. **B** ishtirokchi r_B ni generasiyalab **A** ga jo'natadi:

$$B \rightarrow A: r_B.$$

A ishtirokchi r_B ni qabul qilib o'ziga tegishli tasodifiy son r_A ni generasiyalaydi va shifrmatn $S_A(r_A, r_B, B)$ ni o'z ichiga olgan quyidagi xabarni **B** ishtirokchiga jo'natadi:

$$A \rightarrow B: cert_A, r_A, B, S_A(r_A, r_B, B),$$

bu yerda, r_A, r_B mos tarzda **A** va **B** generasiyalagan tasodifiy sonlar.

B ishtirokchi xabar $(cert_A', r_A', B', S_A'(r_A, r_B, B))$ ni olgandan so'ng $cert_A'$ dagi oshkora kalitdan foydalanib shifrmatn $S_A'(r_A, r_B, B)$ ni r_A, r_B, B ga aylantiradi va ularni xabardagi r_A', o'zi jo'natgan r_B va o'zining identifikatori B' bilan taqqoslaydi. Agar taqqoslanuvchi qiymatlar teng bo'lmasa, unda **A** haqiqiy emas, aks holda haqiqiy degan xulosa chiqariladi.

A *va* **B** *ishtirokchilar tomonidan ikki tomonlama autentifikasiyalash* quyidagi jo'natmalar ketma-ketligidan iborat :

$$B \rightarrow A: r_B.$$

$$A \rightarrow B: cert_A, r_A, B, S_A(r_A, r_B, B),$$

$$B \rightarrow A: cert_B, A, S_B(r_A, r_B, A),$$

Prosedura tasodifiy sonlarni generasiyalash va ularni tomonlarga tegishli identifikatorlar bilan birgalikda shaxsiy kalit bilan shifrlash va shifrmatnlarni oshkora kalit bilan ochish va natijalarni taqqoslash

amallarini bajarish natijasida tomonlarning haqiqiy yoki aksinchaligi haqida xulosa chiqarishni nazarda tutadi.

ERI axborot-kommunikasiya tarmog'ida almashinadigan hujjatli ma'lumotlar va ularning manbalarini haqiqiy yoki haqiqiy emasligini aniqlash masalasini, ya'ni ma'lumotlar autentifikasiyasi masalasining yechimini ta'minlovchi kriptografik vosita hisoblanadi [32].

Har qanday qog'ozli yozma xat yoki hujjatning oxirida shu hujjatni tuzuvchisi yoki tuzish uchun javobgar bo'lgan shaxsning imzosi bo'lishi tabiiy holdir. Imzo quyidagi ikkita maqsaddan kelib chiqib qo'yiladi. Birinchidan, ma'lumotni olgan tomon o'zida mavjud imzo namunasiga olingan ma'lumotdagi imzoni solishtirib, imzoning haqiqiy yoki soxtaligiga ko'ra shu ma'lumotning haqiqiy yoki soxta ekanligini aniqlaydi. Ikkinchidan, shaxsiy imzo ma'lumot hujjatining yuridik maqomini ta'minlaydi. Bunday kafolat esa savdo–sotiq, ishonchnoma, majburiyat va shu kabi bitimlarda alohida muhimdir.

Qog'ozli hujjatlarga qo'yilgan shaxsiy imzolarni soxtalashtirish nisbatan murakkab. Chunki shaxsiy imzo faqat uning muallifi tafakkurining o'ziga xos bo'lgan ko'p qirrali tomonlari mahsulidir. Shuning uchun bunday imzo muallifini hozirgi zamonaviy ilg'or kriminalistika uslublaridan foydalanish orqali aniqlash mumkin.

Axborot-kommunikasiya tarmog'ida almashinadigan elektron hujjatli ma'lumotlar ham qog'ozli hujjat almashinuvidagi an'anaviy shaxsiy imzo vazifasini bajaruvchi kabi ERI bilan ta'minlanib, elektron hujjat va uning manbaini haqiqiy yoki haqiqiy emasligini aniqlash masalasi yechimini hal etilishini talab etadi.

Tasodifiy sonlar asosida qat'iy bir tomonlama autentifikasiyalash. Ikki tomon (ularga ma'lum bo'lgan) umumiy kalit k ni va shifrlashning simmetrik algoritmini tanlashdi.

1. **V** tomon (tekshiruvchi) tasodifiy son r ni generasiya qiladi va uni **A** tomonga yuboradi.

2. **A** tomon qabul qilgan r sonini va ismini o'z ichiga olgan xabar tuzib, K kalit bilan shifrlaydi va **V** tomonga yuboradi.

3. **V** tomon xabarni shifrini ochib **A** ism va r sonning bir xilligiga ishonch hosil qiladi.

Agar buzg'unchi tarmoqda yuboriladigan xabarlarni tutib qoladigan bo'lsa, u bu xabarlardan o'zini **A** yoki **V** sifatida ko'rsatish uchun

foydalana olmaydi, chunki k kalit ochiq xolatda uzatilmaydi va har bir autentifikasiyalash seansida yangi tasodifiy sondan foydalaniladi.

Tasodifiy sonlar asosida qat'iy ikki tomonlama autentifikasiyalash. Ikki tomonlamalik, autentifikasiyalash seansi jarayonida ikki ishtirokchi bir birining haqiqiyligiga ishonch hosil qilishini bildiradi. Bunda xabar almashish quyidagi sxema asosida boradi:

V ishtirokchi **A** ga r_1 tasodifiy sonni yuboradi.

A ishtirokchi **V** ga k kalit bilan shifrlangan r_1 , **V** ism va tasodifiy son r_2 ni o'z ichiga olgan xabarni jo'natadi.

V ishtirokchi **A** ga k kalit bilan shifrlangan r_1 va r_2 ni o'z ichiga olgan xabarni yuboradi.

Nosimmetrik algoritm asosida autentifikasiyalash.

1. **V** (tekshiruvchi) ishtirokchi tasodifiy son r ni tanlaydi va **A** ishtirokchiga quyidagilarni yuboradi: $H(r), B, P_A(r, B)$. Bu yerda N – xesh funksiya, R_A – nosimmetrik shifrlash algoritmi (shifrlash **A** ning ochiq kaliti yordamida amalga oshiriladi).

2. **A** ishtirokchi $P_A(r, B)$ ni shifrini ochar ekan xesh r qabul qilingan $H(r)$ bilan ustma-ust tushishiga ishonch hosil qiladi va **V** ishtirokchiga r sonini yuboradi.

3. **V** ishtirokchi qabul qilgan sonni tekshiradi va agar u r bilan ustma-ust tushsa, **A** ning haqiqiyligiga ishonch hosil qiladi (ya'ni, **A** ni yopiq kalitni bilishiga).

Autentifikasiya jarayonida uchinchi tomonni jalb etish bilan ishtirokchilarni autentifikasiyalashni ta'minlovchi protokollarning mashhur namunalaridan biri sifatida simmetrik algoritmlarga asoslangan qat'iy autentifikasiyalash protokollaridan biri Kerberos protokolini ko'rsatish mumkin [32-33].

Kerberos protokolining asosida Nidxeym-Shreder protokoli yotadi. Bu protokol 1987 yilda Massachusset texnologiya institutida "Afina" loyihasining qismi sifatida ishlab chiqilgan. Kerberos protokolining modifikasiyalangan rusumi *Windows 2000* operasion tizimida qo'llanilgan.

Kompyuter tarmog'i ishtirokchilardan va serverdan tashkil topgan bo'lib, ishtirokchilar sifatida ishtirokchilar, dasturlar yoki maxsus xizmatlar bo'lishi mumkin. Kerberos ishtirokchilar va ularning maxfiy kalitlarini o'z ichiga oluvchi markaziy ma'lumotlar bazasini saqlaydi. Agar tizimga n ta ishtirokchi kiradigan bo'lsa, ularning kalitlari fazosining

o'lchami $O(n)$ tartibli bo'ladi. Kerberos protokolining maqsadi ishtirokchilarni identifikasiya qilish va ular uchun seans kalitlarini generasiya qilishdan iborat.

Bundan tashqari Kerberos protokoli turli xizmatlar va resurslarga kirish huquqini beruvchi tizim sifatida ham xizmat qilishi mumkin. Identifikasiya qilish va kirish huquqini berish funksiyalariga ajratish muhim amaliy ahamiyatga ega. Masalan, korxonada biror bo'limning xodimi sizning shaxsingizni aniqlasa, boshqa bo'lim sizning korxona resurslariga kira olish darajangizni aniqlaydi.

Faraz qilaylik, **A** ishtirokchi **V** ishtirokchining resurslaridan foydalanmoqchi. U holda **A** ishtirokchi o'zining parolidan foydalanib autentifikasiyalash serveriga kiradi. Server unga shu parol yordamida shifrlangan sertifikat beradi. Sertifikat shuningdek seans kaliti k_{as} ni ham o'z ichiga oladi. **A** ishtirokchi k_{as} kalitini **V** ishtirokchining resurslariga kirish huquqini beruvchi sertifikat olish uchun qo'llaydi. So'nggi sertifikat k_{ab} kalitdan, kalitning yaroqlilik muddati l dan va VB t_s dan iborat bo'ladi. Berilgan sertifikat **A** ishtirokchining **V** ga keyinga murojaatlarida "shaxsini tasdiqlash" uchun ishlatiladi.

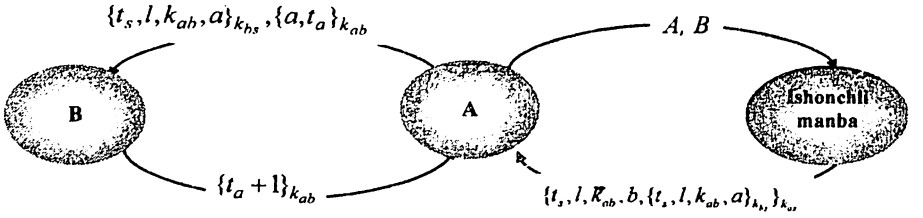
Kerberos protokoli quyidagi bosqichlardan iborat (2.2-rasm):

$$A \rightarrow S : A, B,$$

$$S \rightarrow A : \{t_s, l, k_{ab}, b, \{t_s, l, k_{ab}, a\}_{k_{bs}}\}_{k_{as}},$$

$$A \rightarrow B : \{t_s, l, k_{ab}, a\}_{k_{bs}}, \{a, t_a\}_{k_{ab}},$$

$$B \rightarrow A : \{t_a + 1\}_{k_{ab}}.$$



2.2- rasm. Kerberos protokoli

– Birinchi xabarida A ishtirokchi ishonchli manba (IM) S ga V ishtirokchi bilan bog'lanmoqchiligini xabar qiladi.

– Agar IM S bu bog'lanishga ruxsat beradigan bo'lsa, k_{bs} kalit bilan shifrlangan $\{t_s, l, k_{ab}, a\}$ sertifikat hosil qilinib, A ga V ga uzatish uchun yuboriladi. A ishtirokchi bu kalitning o'zi o'qiy oladigan shaklining nusxasini oladi.

– A ishtirokchi sertifikatning yaroqliligini tekshirish va V ishtirokchining resursidan foydalanish imkoniyatini bilish maqsadida shifrlangan VB t_a ni V ishtirokchiga yuboradi.

– V ishtirokchi VBning yangiligini tekshirib, bu bilan seans kalitini bilishini va bog'lanishga tayyorligini bildirib, $t_a + 1$ shifrlangan kattalikni ortiga qaytarib yuboradi.

Bu protokolda Nidxeym-Shreder protokoliga xos bo'lgan kamchiliklar vaqtning majburiy sinxronlashtirish hisobiga yo'qotilgan [32-33].

Kerberos xavfsizligi

Kerberos, kriptografik himoyalashning boshqa har qanday dasturiy vositasi kabi ishonchsiz dasturiy muhitda ishlaydi. Ushbu muhitning hujjatlashtirilmagan imkoniyatlari yoki noto'g'ri konfigurasiyasi jiddiy axborotning chiqib ketishiga olib kelishi mumkin. Hatto kalitlar ishtirokchi ishlash seansida faqat tezkor xotirada saqlansa ham, operasion tizimdagi buzilish kalitlarning qattiq diskda nusxalanishiga olib kelishi mumkin.

Kerberos dasturiy ta'minoti o'rnatilgan ishchi stansiyasidan ko'pchilik ishtirokchi rejimning ishlatilishi yoki ishchi stansiyalardan foydalanishning nazorati bo'lmasligi dastur-zakladkani kiritish yoki kriptografik dasturiy ta'minotni modifikasiyalash imkoniyatini tug'diradi.

Shu sababli, Kerberos xavfsizligi ko'p jihatdan ushbu protokol o'rnatilgan ishchi stansiyasi himoyasining ishonchligiga bog'liq. Kerberos protokolining o'ziga quyidagi qator talablar qo'yiladi:

– Kerberos xizmati xizmat qilishdan voz kechishga yo'naltirilgan hujumlardan himoyalanishi shart;

– VB autentifikasiya jarayonida qatnashishi sababli, tizimdan ishtirokchilarining barchasi uchun tizimli vaqtni sinxronlash zarur;

– Kerberos parolni saralash orqali hujum qilishdan himoyalamaydi. Muammo shundaki, kalitlarni taqsimlash markazida

saqlanuvchi ishtirokchi kaliti uning parolini xesh-funksiya yordamida qayta ishlash natijasidir. Parolning bo'shligida uni saralab topish mumkin.

– Kerberos xizmati ruxsatsiz foydalanishining barcha turlaridan ishonchli himoyalanishi shart;

– mijoz olgan mandatlar hamda maxfiy kalitlar ruxsatsiz foydalanishdan himoyalanishi shart.

Yuqorida keltirilgan talablarning bajarilmasligi muvaffaqiyatli hujumga sabab bo'lishi mumkin.

Hozirda Kerberos protokoli autentifikasiyalashning keng tarqalgan vositasi hisoblanadi. Kerberos turli kriptografik sxemalar, xususan, ochiq kalitli shifrlash bilan birgalikda ishlatilishi mumkin.

Nazorat savollari

1. Autentifikasiya va autentifikasiya protokoli nima?
2. Autentifikasiya necha turga bo'linadi va ular nima maqsadda qo'llaniladi?
3. Autentifikasiya protokollarini taqqoslashda qanday xarakteristikalarni hisobga olinadi?
4. Aktiv va passiv hujumlarning farqi nimadan iborat?
5. Autentifikasiya protokollariga qo'llaniladigan qanday namunaviy hujumlarni bilasiz?
6. Xabar almashinuvi yordamida hujum nimadan iborat?
7. Autentifikasiya protokollarini qurishda qanday usullardan foydalaniladi?
8. Parol yordamidagi autentifikasiya qilish qanday amalga oshiriladi?
9. Parollarni qanday holda uzatish xavfsiz hisoblanadi?
10. Bir martali parollar bilan ko'p martali parollarning farqi nima?
11. Bir martali parollardan foydalanishda qanday usullar qo'llaniladi? Ularning har birini tushuntirib bering.
12. O'zgaruvchan parolli APda parolning yangilanishi qanday sxemalar bo'yicha amalga oshiriladi?
13. Xavfsizlikni ta'minlash darajasiga ko'ra AP qanday tasiflanadi?
14. Bir va ikki tomonlama autentifikasiyaga misollar keltiring.
15. Kerberos protokoli qanday protokol va u qanday bosqichlardan iborat?
16. Kerberos protokoliga qanday talablar qo'yiladi?

3. KALITLARNI TAQSIMLASH PROTOKOLLARI

3.1. Kalitlarni taqsimlash protokollarining xossalari

3.1.1. Kalitlarni boshqarish tushunchasi

Hozirgi kunda kriptografik tizimlar axborot xavfsizligini ta'minlashda eng ishonchli vositalardan biri bo'lib, elektron hujjat aylanish va elektron to'lov tizimlarida ERI shakllantirish va autentifikasiya masalalarini yechish uchun foydalaniladi [8-11]. Axborot-kommunikasiya tizimida ma'lumotlarni maxfiy yoki konfidensial almashuv jarayoni uchun kriptografik tizimlar yaratish bilan bir qatorda shu tizimda kalitlarni boshqarish masalasini ishonchli hal etish muhim o'rin tutadi. Chunki tanlangan kriptotizim qanchalik murakkab va ishonchli bo'lmasin, undan amalda foydalanish jarayonlari kalitlarni boshqarish masalasi bilan bog'liqdir. Agar ma'lumotlarning maxfiy almashinuvi oz sonli ishtirokchilar bilan bo'lsa, kalitlar almashinuvi jarayonida noqulayliklar tug'ilmaydi. Ammo axborot-kommunikasiya tizimida ma'lumotlarning maxfiy almashinuvi yuzlab, minglab va hatto millionlab ishtirokchilar bilan bo'lsa, kalitlarni boshqarishning o'ziga xos alohida muhim masalalari kelib chiqadi.

Kriptografik tizimlarda asosiy tushunchalardan biri kalit tushunchasi hisoblanadi. Kriptografik kalitlar nosimmetrik kriptotizimlar uchun ochiq va maxfiy kalitlarning umumiy nomi bo'lib, ERIni hisoblash yoki tekshirish, shuningdek shifrlash va dastlabki matnga o'girish uchun qo'llaniladigan simvollar ketma-ketligini ifodalaydi. Kriptografik almashtirishlarni amalga oshiruvchi shaxsgagina tegishli va ma'lum bo'lgan kalit maxfiy kalit deb ataladi [3].

Kalitlar haqidagi ma'lumot deganda, axborot-kommunikasiya kriptotizimida mavjud bo'lgan barcha kalitlar to'plami va ularning muhofazasi bilan bog'liq ma'lumotlar tushuniladi. Agarda kalitlar haqidagi ma'lumotlarni yetarli darajadagi ishonchli muhofazali boshqaruvi ta'minlanmasa, tabiiyki, raqib tomonga axborot-kommunikasiya tizimidagi deyarli ixtiyoriy ma'lumotni olish uchun to'la imkoniyat tug'iladi. Kalitlarni boshqarish kriptografik kalitlar va xavfsizlik bilan bog'liq boshqa parametrlar (masalan, inisializasiyalash vektorlari va parollar)ni boshqarishni, shuningdek, ularni generasiya qilish, saqlash,

o'rnatish, kiritish, chiqarish va nollashni o'z ichiga oladigan kalitlar hayotining to'liq sikli davomida bajariladigan amallarni o'z ichiga oladi.

Kriptografik kalitlarni boshqarish sohasida asosiy xalqaro standart sifatida 3 qismdan iborat ISO/IEC 11770 standartidan foydalaniladi [34-36].

Kalitlarni boshqarish jarayoni quyidagi uchta muhim bo'lgan jarayonlarga ahamiyat berishni talab etadi:

- kalitlar generasiyasi;
- kalitlarning to'planishi;
- kalitlarning taqsimlanishi.

Kalitlarni oson eslab qolish maqsadida tasodifiy tanlanmagan kalitlardan foydalanish xavfsizlikni ta'minlay olmaydi. Axborot-kommunikasiya tizimlarida tasodifiy kalitlarni generasiyalashning maxsus apparat va dasturiy usullaridan foydalaniladi.

Kalitlarning to'planishi deganda, ularni saqlash, hisobga olish va yo'qotishni tashkillashtirish tushuniladi. Kalit buzg'unchi uchun o'ziga eng jalb etuvchi obyekt hisoblanib, unga konfidensial axborot uchun yo'l ochadi, shuning uchun ham kalitlar to'plamiga katta ahamiyat berish talab etiladi. Maxfiy kalitlar hyech qachon oshkora holda axborot tashuvchilarga yozilmasligi, ya'ni uni o'qib va ko'chirib bo'lmaslik kerak. Yetarli darajada murakkab axborot-kommunikasiya tizimlarida bitta ishtirokchi katta hajmdagi kalit axborotlar bilan ishlashi mumkin va ba'zida esa kalit axborotlar bo'yicha kichik ma'lumotlar bazasi tashkil etish zaruriyati paydo bo'ladi. Bunday ma'lumotlar bazasi foydalanilgan kalitlarni qabul qilishga, saqlashga, hisobga olishga va yo'qotishga javobgar hisoblanadi. Shunday qilib ishlatilgan kalitlar haqidagi barcha axborotlar shifrlangan holda saqlanishi kerak. Axborot tizimlaridagi kalit axborotlarni muntazam ravishda yangilab turish axborot xavfsizligining muhim sharti hisoblanadi.

Kalitlarni taqsimlash kalitlarni boshqarish jarayonidagi eng ma'suliyatli jarayon hisoblanadi. Kalit tarqatish protokollarining uch turi mavjud: (generasiyalangan) kalitlarni uzatish protokollari, birgalikda umumiy kalitni ishlab chiqarish protokollari (kalitlarni ochiq taqsimlash) va dastlabki kalit taqsimlash sxemalari.

Dastlabki kalit tarqatish sxemalari ikkita algoritmdan tashkil topgan: boshlang'ich kalitga oid axborotni taqsimlash va kalitni shakllantirish. Birinchi algoritm yordamida kalitga oid axborotning ochiq

qismi va maxfiy qismi (har bir tomon uchun) generasiya qilinadi, ochiq kalit hamma kirishi mumkin bo'lgan ochiq serverga joylashtiriladi. Ikkinchi algoritm abonentlarda mavjud bo'lgan maxfiy va boshlang'ich kalit ma'lumotining umumiy ochiq qismi yordamida, ular orasidagi o'zaro bog'lanishni amaldagi kalitini hisoblash uchun mo'ljallangan. Saqlanadigan va taqsimlanadigan maxfiy kalitli axborotning hajmini kamaytirish uchun qo'llaniladi. Dastlabki kalit taqsimlash sxemasi turg'un bo'lishi, ya'ni kompromentasiyada, firibgarlikda yoki ba'zi abonentlarning maxfiy kelishuvida kalitning bir qismini ochilishini e'tiborga olinishi va tez moslashuvchan – ya'ni obro'sizlantirilgan kalitlarni chiqarib tashlash orqali tezlikda tiklash va yangi abonentlarni ulashi imkoniyatini berishi kerak.

3.1.2. Kalit taqsimoti muammosi

Kalit taqsimoti - kriptografiyaning asosiy masalalaridan biri bo'lib, uning bir qancha yechimlari mavjud, ulardan mosi vaziyatga bog'liq holda tanlanadi [3-5].

Fizik taqsimot. Ishonchli kuryerlar yoki qurollangan soqchilar yordamida kalitlar an'anaviy fizik usul bilan yuborilishi mumkin. XX asrning yetmishinchi yillariga qadar tarmoq o'rnatishda bu haqiqatan ham kalit taqsimotining yagona xavfsiz usuli edi. Buning o'ziga xos qiyinchiliklari ham mavjud bo'lib, ulardan eng asosiysi kriptotizimlarning kriptobardoshliligi faqat kalitga bog'liq bo'lmay, kuryerga ham bog'liq bo'ladi. Agar kuryerni sotib olish, o'g'irlash yoki o'ldirish mumkinligi e'tiborga olinsa, u holda tizim obro'sizlanishi mumkin.

Maxfiy kalitli protokollar yordamida taqsimlash. Agar uzoq muddatli maxfiy kalitlar ishtirokchilar va biror ishonch markazi orasida taqsimlangan bo'lsa, u holda undan kalitlarni generasiya qilishda va ixtiyoriy ikkita ishtirokchi orasida almashinuv zarurati tug'ilganda foydalaniladi.

Ochiq kalitli protokollar yordamida taqsimlash. Ochiq kalitli kriptotizimlardan ishtirokchi sheriklar vositachiga ishonmasa va uchrashish imkoniga ega bo'lmasalar, kalit taqsimlash protokoliga muvofiq onlayn rejimida umumiy maxfiy kalit to'g'risida kelishib olishlari mumkin. Bu ochiq kalitli shifrlash texnikasining eng ko'p tarqalgan ilovasidir. Katta hajmdagi ma'lumotni ochiq kalit yordamida bevosita

shifrlash o'rniga tomonlar oldindan maxfiy kalitni kelishib olishadi. Keyin aniq ma'lumotlarni shifrlash uchun kelishilgan kalit bilan simmetrik shifr qo'llaniladi.

Muammoning ko'lamini tushuntirish uchun o'zaro bir-birlari bilan maxfiy axborot almashinuvchi n ta ishtirokchiga xizmat ko'rsatish uchun $\frac{n(n-1)}{2}$ ta turli maxfiy kalit kerak bo'ladi. n oshishi bilan katta miqdordagi kalitlarni boshqarish muammosi paydo bo'ladi. Masalan, 20 000 talaba bo'lgan universitetga 199 milliondan ko'p alohida maxfiy kalitlar kerak bo'ladi. Katta miqdordagi maxfiy kalitlarning hosil qilinishi ularning boshqaruvida katta muammolarni keltirib chiqaradi.

Bunday muammoning yechimlaridan biri shundaki, har bir ishtirokchiga faqat bitta kalit biriktirib qo'yiladi va bu kalitdan foydalanib u IM bilan bog'lanadi. Bu holda n ishtirokchili tizim n ta kalit talab etadi. Agar ikki ishtirokchi maxfiy axborot almashmoqchi bo'lsa, ular faqat shu axborotni uzatishda qo'llash uchun kalit generasiya qilishadi. Bu kalitni seans kaliti deb ataladi.

Maxfiy kalit to'la ma'noda tasodifiy bo'lishi kerak, chunki buzg'unchi avvaldan kalit va xabarlarning taqsimlanish ehtimolligini bilsa, kalit haqida ham ma'lumotga ega bo'lishi mumkin. Barcha kalitlar bir xil ehtimollikka ega bo'lishi va tasodifiy sonlarning haqiqiy generatori yordamida hosil qilinishi kerak. Lekin butunlay tasodifiy sonlar manbaini yaratish juda ham qiyin. Bundan tashqari haqiqiy tasodifiy kalit amaliyot uchun qulay bo'lgani bilan uni inson miyasida saqlab turish murakkabdir. Shuning uchun ko'pgina tizimlar maxfiy kalitni generasiya qilishda parol yoki mos iboralardan foydalanadi. PIN kodga o'xshaydigan parol, ya'ni 0 dan 9999 oralig'ida yotuvchi oddiy sonni to'g'ridan-to'g'ri hujum bilan oson topish mumkin.

Quyidagi 3.1-jadvalda kalitlarni ishlatilayotgan simvollarning uzunligi va tipiga bog'liqligi ko'rsatilgan. Agar kalit uzunligi 4 simvoldan iborat bo'lgan son 10 lik sanoq sistemasi (s.s.) ko'rinishida bo'lsa, u taxminan 10^4 .(4 xonali sonni) sonini, 2 lik sanoq sistemasi ko'rinishida bo'lsa 2^{13} (13 xonali sonni) sonini ifodalaydi.

Agar kalit uzunligi 4 simvoldan iborat bo'lgan harf 10 lik sanoq sistemasi (s.s.) ko'rinishida bo'lsa, u taxminan 10^7 (7 xonali sonni) sonini, 2 lik sanoq sistemasi ko'rinishida bo'lsa 2^{23} (23 xonali sonni) sonini ifodalaydi (3.1-jadval).

3.1-jadval

Kalitlarni ishlatilayotgan simvollarning uzunligi va tipiga bog'liqligi

Kalitning uzunligi (simvollar soni)	Kalit tipi			
	Sonlar		Harflar	
	O'nlik s.s.	Ikkilik s.s.	O'nlik s.s.	Ikkilik s.s.
4	10^4	2^{13}	10^7	2^{23}
8	10^8	2^{26}	10^{15}	2^{50}

Yuqorida bayon etilganlar asosida shunday xulosa qilish mumkin: 8 xonali sonlardan iborat paroldan foydalanish ham hozirgi kunda yetarli xavfsizlikni ta'minlamaydi. Chunki zamonaviy kompyuterlar yordamida kalitlarni to'liq tanlash asosida ularni qisqa vaqt ichida topish imkoniyati oshib bormoqda. Shularni hisobga olgan holda kalit tanlashda ma'lum qoidalarga amal qilish talab etiladi.

Kalitlarni tanlashda 20-30 simvolli uzun iboralardan foydalanish mumkin, biroq bu ham yechim bo'lmaydi, sababi tabiiy tildagi harflar ketma-ketligi butunlay tasodifiy emas.

Ismlarga yoki iboralarga asoslangan qisqa parollar ko'plab katta korxonalarning umumiy muammosidir. Ulardan ko'pchiliga parolda

- hyech bo'lmaganda bitta bosh harf ishtirok etishini;
- hyech bo'lmaganda bitta katta harf ishtirok etishini;
- hyech bo'lmaganda bitta raqam ishtirok etishini;
- hyech bo'lmaganda bitta raqam va harfdan boshqa belgi ishtirok etishini;
- parolning uzunligi 8 simvoldan kam bo'lmasligini talab etishadi.

Lekin keltirilgan qoidalar lug'at bo'yicha hujumdan tashqari sakkizta simvolni haqiqatan tasodifiy tanlagandagi mumkin bo'lgan maksimal parollar sonini ta'minlamaydi.

Kalitlarni generasiyalaganda va saqlaganda kalitlarning yaroqlilik muddatiga ahamiyat berish kerak. Foydalanilayotgan kalit qancha ko'p muomalada bo'lsa, buzg'unchiga uni ochish shunchalik oson bo'ladi va u shunchalar katta qiymatga ega bo'ladi. Bu asosiy qoida bo'lib kalitning yaroqlilik muddati tugashi bilan uni to'g'ri yo'qotish kerak. Muammoni

"del" yoki "rem" komandasi orqali operasion tizim zimmasiga yuklash buzg'unchining qattiq diskdagi axborotni qayta tiklay olmasligini kafolatlamaydi. Chunki faylni yo'qotishda uning ichidagi narsalar yo'qolmaydi, balki tizimga faqat xotiraning unga ajratilgan yacheykalari endi boshqa yangi ma'lumotlarni yozish uchun bo'shligini bildiradi.

Asosiy muammolardan biri maxfiy kalit taqsimotining xavfsiz boshqaruvidir. IM ishlatilganda ham uning har bir ishtirokchisi uchun qandaydir kalit olish usuli kerak bo'ladi.

Bu muammoni yechish yo'llaridan biri kalitni parchalash (yoki maxfiylikni bo'lish) bo'lib, bunda kalit bir necha bo'laklarga bo'linadi [3-4, 6]:

$$k = k_1 \oplus k_2 \oplus \ldots \oplus k_r .$$

Uning har bir qismi o'zining kanali bo'yicha yuboriladi. Kalitni aniqlashi uchun buzg'unchi barcha kanallarga bir vaqtda ulanishi kerak bo'ladi. Bunda agar buzg'unchi kalit qismi uzatiladigan kanallardan biriga kirishga muvaffaq bo'lsa, u kalitning qonuniy tiklanishiga to'sqinlik qilishi mumkin.

Nisbatan murakkabroq usul maxfiylikni chegaraviy bo'lish sxemalaridan birini qo'llash keltirilgan muammoning oldini oladi. Kalit avvalgidek bir necha qismga bo'linadi. Qonuniy ishtirokchi bu qismlarni qanchadir miqdorini, ya'ni aniqlangan chegaraviy qiymati Q dan ko'prog'ini olib kalitni butunlay tiklashi mumkin. Lekin buzg'unchi *(Q-1)* qismni bilib olgani bilan kalitni ocha olmaydi.

Shamirning maxfiylikni bo'lish sxemasi chegaraviy bo'lish sxemalarining namunaviy misoli bo'ladi [3-4]. Faraz qilaylik, k kalit W ta bo'lakka shunday bo'linganki, ulardan Q tasini birga yig'ish natijasida kalit bir qiymatli tiklanadi. Bunday qiymatli sxema *(Q, W)* - chegaraviy sxema deyiladi.

$W+1$ katta bo'lgan tub p sonini olamiz. k kalit F_P maydonning elementi bo'lsin. Ishonchli shaxs bittadan kalitning har bir qismi uchun $i=1,\ldots,W$ da $X_i \in F_P$ qiymatlarni tanlaydi. Maxfiylikni bo'lishning har bir ishtirokchisi boshqa ishtirokchilarga ham ma'lum bo'lgan o'zining X_i qiymatini oladi. k kalitni ishtirokchilar orasida bo'lish uchun mas'ul shaxs maydonning $Q-1$ elementini $a_1,\ldots,a_{T-1}$ tanlaydi va

$$F(X) = k + \sum_{j=1}^{Q-1} a_j X^j$$

ko'phadni tuzadi. So'ngra uning qiymatlari hisoblanadi:

$$y_i = F(X_i) \text{ bunda } 1 \le i \le W$$

va kalit bo'linish ishtirokchilariga tarqatiladi.

Kalitni tiklash uchun ishtirokchilar ko'phadni interpolyasiya qilish jarayonini qo'llashadi. Faraz qilaylik, L ta maxfiylik saqlovchi birga to'planishdi va $y_i (i = 1,..., L)$ qiymatlarni almashishdi. Bunda ular tenglamalar sistemasini yechishga harakat qilib ko'rishadi:

$$\begin{cases} y_1 = k + a_1 X_1 + ... + a_{T-1} X_1^{T-1} \\ \cdots \\ y_L = k + a_1 X_L + ... + a_{T-1} X_L^{T-1} \end{cases}$$

Agar $L \ge Q$ bo'lsa, sistema bitta yechimga ega bo'ladi va u $F(X)$ ni va demak kalitni tiklash imkonini beradi. Agar $L < Q$ bo'lsa, u holda sistema aniqlanmagan bo'lib qoladi va zarur ko'phadni tiklashga yordam bera olmaydi. Shunday qilib, k kalit to'g'risida hyech qanday ma'lumot olish imkoni bo'lmaydi.

Amaliyotda bu sistemani Lejandrning interpolyasion ko'phadi yordamida qisqa yechish usuli qo'llaniladi. Bu ko'phadning tafsilotlariga berilmagan holda, faqat kalit tiklanish sxemasini keltiramiz. Koeffisentlar quyidagicha hisoblanadi:

$$B_j = \prod_{1 \le \alpha \le T, \alpha \ne j} \frac{X_\alpha}{X_\alpha - X_j},$$

va ular orqali kalit tiklanadi:

$$k = \sum_{j=1}^{T} B_j y_j.$$

Yuqorida aytib o'tilgandek, n ta ishtirokchi o'zaro bir-birlari bilan maxfiy axborot almashinishi uchun $\frac{n(n-1)}{2}$ ta uzoq muddatli turli maxfiy kalit kerak bo'ladi. Ta'kidlab o'tilganidek, bu o'z navbatida katta miqdordagi kalitlarni boshqarish va ularni taqsimlash muammosini keltirib chiqaradi. Avval aytilgandek bunda seans kalitlaridan va bir nechta statik kalitlardan foydalanish afzalroq.

Bu masalani yechish uchun ko'plab protokollar ishlab chiqilgan, ularda seans kalitini taqsimoti uchun simmetrik kalitli kriptografiyadan foydalaniladi.

3.1.3. Kalitlarni taqsimlash protokollarining xossalari

Kalitlarni taqsimlash tartib va qoidalari (protokoli) quyidagicha [37]:

1. Kalitlarni ro'yxatga olish markazi (KROM) muhofazalangan aloqa tarmog'i orqali barcha $i=1,2,...,S$ ishtirokchilarga maxfiy Z_i kalitlarni taqdim etadi.

2. Ishtirokchi i ishtirokchi j bilan maxfiy aloqa o'rnatmoqchi bo'lsa, u umumiy aloqa tarmog'i orqali (ochiq matn bilan bo'lishi mumkin) KROMga murojaat qilib, ishtirokchi j bilan maxfiy aloqa qilish kalitini so'raydi.

3. KROM maxfiy aloqa uchun ochiq matnning biror qismini tashkil etuvchi Z_{ij} maxfiy kalitni tanlab oladi. Qolgan qismini i va j ishtirokchilar ko'rsatilgan "bosh qism" ("zagolovka") yoki "nomlanish qismi" deb ataluvchi bo'lak tashkil etadi. KROM bu ochiq matnni kriptotizimda qabul qilingan shifrlash algoritmiga ko'ra Z_i va Z_j kalitlar bilan shifrlab, umumiy aloqa tarmog'i orkali Z_i kalit bilan shifrlangan kriptogrammani i ishtirokchiga va Z_j kalit bilan shifrlangan kriptogrammani j ishtirokchiga jo'natadi.

4. Olingan kriptogrammalarni i va j ishtirokchilar shifrini ochib, keyingi olingan ma'lumotlarni shifrini ochishning maxfiy kalitiga ega bo'ladilar.

Kalitlarni taqsimlashning bunday protokoli oddiy bo'lib, uning bardoshliligi shifrlash algoritmining bardoshliligi bilan belgilanadi. Haqiqatdan ham 3-qadamda keltirilganidek, kriptotahlilchiga har xil kalitlar bilan shifrlangan bir xil ochiq matnning kriptogrammasi ma'lum bo'lib, bunday holat unga kriptotahlil qilishda qo'l keladi. Shunday qilib, ochiq matnni shifrlash algoritmi kriptotahlilga bardoshli bo'lsa, kalitlarni taqsimlash protokoli ham bardoshli bo'ladi. Bu yerda shuni ham unutmaslik kerakki, kalitlarni taqsimlashda shifrlash algoritmidan foydalanish shu taqsimlash tartib va qoidalarining buzilishiga, kriptobardoshsizlikka va shu kabi nomutonosibliklarga olib kelmasligi kerak.

Kalit taqsimlash protokollarining asosiy xossalariga kalitni autentifikasiya qilish, kalitni tasdiqlash va kalitni aniq autentifikasiya qilish xossalari kiradi.

Kalitning (noaniq) autenitfikasiyasi – bu shunday xossaki, buning vositasida protokol ishtirokchilaridan biri maxsus identifikasiyalangan

protokolning ikkinchi ishtirokchisidan (ishonch markazi bo'lishi mumkin) boshqa hyech qaysi tomon protokolda olingan maxfiy kalitlarni olish imkoniga ega bo'lmasligiga ishonch hosil qiladi [37].

Bu ta'rifni tushuntirib beramiz. Bu yerda ikkinchi ishtirokchi haqiqatan ham kalitga kirish huquqini olganligiga kafolat yo'q, ammo undan boshqa hyech kim bu huquqni olaolmaydi. Kalitning noaniq autentifikasiyasi boshqa ishtirokchining kalitga aniq egaligidan bog'liq bo'lmaydi va ikkinchi tomondan hyech qayday amaliyotni talab qilmaydi.

Kalitlarni haqiqiy taqsimlash protokoli – bu kalitlarni oldingi ta'rifda kelitirlgan ma'nodagi autentifikasiyasini ta'minlaydigan kalit taqsimlash protokoli.

Kalitni tasdiqlash – bu xossa yordamida protokolning bitta ishtirokchisi boshqa ishtirokchining haqiqatan ham protokolda olingan maxfiy kalitga egalik qilishiga ishonch hosil qiladi.

Protokollarda kalit tasdiqlashning to'rt usuli qo'llaniladi:

1. kalitning xesh-kodini hisoblash;
2. kalitni xesh-funksiyali kalit bilan qo'llash;
3. kalitni qo'llab ma'lum kattaliklarni shifrlash;
4. e'lon qilinganligi nolga teng bo'lgan bilishni isbotlash.

Oxirigisidan boshqa, birinchi uchta xususiyat kalit to'g'risidagi ozgina ma'lumotni oshkor qiladi, ammo bu deyarli hyech qanday amaliy ahamiyatga ega emas.

Kalitni aniq autentifikasiya qilish – kalitni autentifikasiya qilish va kalitni tasdiqlash bir vaqtda sodir bo'lganda bajariladigan xususiyat. Bu holda protokoldagi identifikasiyalangan tomon tasniflangan kalitga ega bo'lishi ma'lum.

Kalitni autentifikasiyalash tushunchasi protokol ishtirokchi-sub-yektining autentifikasiyasi tushunchasi bilan bir xil emas. Avval kiritilgan tushunchalar ma'nosida ishtirokchilarni autentifikasiya qilish ko'pgina protokollarda talab qilinmaydi. Masalan, kalit taqsimotining mashhur Diffi-Xellman protokoli kalit autentifikasiyasini ham, kalit tasdiqlashni ham, protokol ishtirokchilari autentifikasiyasini ham ta'minlamaydi.

Ammo ishtirokchilarni autentifikasiyalash bilan kalit taqsimlash protokolida autentifikasiyalash natijasi aynan bir xilligini kafolatlashi juda muhim.

3.1.4. Kriptografik kalitlarni taqsimlash usullari va sxemalari

Kalit taqsimlash kriptografiyaning asosiy masalalaridan biri hisoblanib, kalit taqsimlash qanday vaziyatda amalga oshirilayotganiga qarab uni yechishning bir qancha usullari mavjud [5-7]. 3.1.2-paragrafda kalitni taqsimlashning fizik usuli va uning asosiy kamchiliklari bayon etilgan edi. Bugungi kunda kalitlarni taqsimlashda bir qancha usullardan foydalaniladi, bu usullarni quyidagi sinflarga jamlash mumkin:

1. Oshkora e'lon qilish;
2. Oshkora foydalanish mumkin bo'lgan katalog;
3. Ochiq kalitlarning IM;
4. Ochiq kalitlar sertifikatlari.

Ochiq kalitlarni oshkora e'lon qilish

Ma'lumot almashinuvida ishtirok etuvchi ixtiyoriy tomon o'zining ochiq kalitini kommunikasiya vositalari orqali barcha ishtirokchilarga taqdim etishi mumkin. Bunday yondashuvning qulay bo'lishi bilan birga, zaif tomoni ham mavjud: ixtiyoriy kishi bunday oshkora e'lonni berishi mumkin. Ya'ni, ixtiyoriy kishi (buzg'unchi) o'zini **A** ishtirokchi deb tanishtirib, ochiq kalitini tarmoqdagi boshqa ishtirokchiga yuborishi mumkin yoki ochiq kalitini barchaning foydalanishi uchun taqdim etishi mumkin. Firibgarligi ochilgunga qadar buzg'unchi **A** ishtirokchiga kelgan barcha shifr matnlarni o'qish va ochiq kalit yordamida autentifikasiyalash (tekshirish va haqiyqiyligini tasdiqlash) imkoniga ega bo'ladi (3.1-rasm).

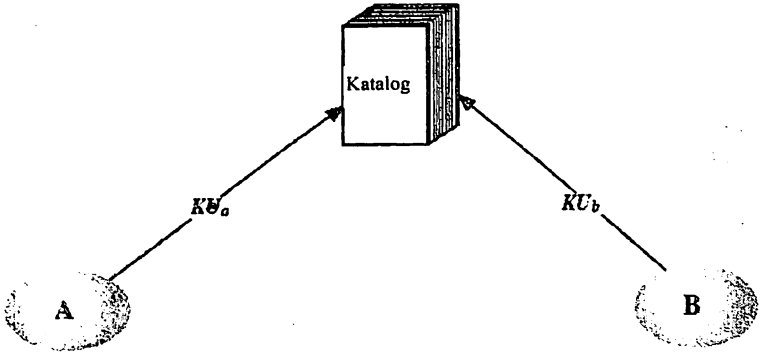
3.1- rasm. Ochiq kalitlarni oshkora e'lon qilish

Oshkora foydalanish mumkin bo'lgan katalog

Ochiq kalitlarning oshkora foydalanish mumkin bo'lgan biror dinamik katalogini yaratish, himoyalanish darajasini nisbatan oshishini ta'minlashi mumkin. Ochiq kalitlarning oshkora foydalanish mumkin bo'lgan dinamik katalogini kuzatish va tarqatish javobgarligi biror bir ishonchli markaz yoki tashkilot zimmasida bo'lishi lozim.

Bu jarayon quyidagi bosqichlarni o'z ichiga oladi [38]:

- vakolatlangan tashkilot har bir ishtirokchining ismi va ochiq kaliti qayd etilgan katalogni shakllantiradi;
- har bir ishtirokchi o'zining ochiq kalitini vakolatlangan tashkilot yordamida ro'yxatdan o'tkazadi. Bunday ro'yxatdan o'tkazish ishtirokchining shaxsan kelishini yoki himoyalangan kommunikasiya kanallari orqali bajarilishini talab etadi;
- har bir ishtirokchi ochiq kalitdan katta hajmdagi ma'lumotni yuborish uchun foydalangani uchun yoki kalitning obro'si tushgani bois ixtiyoriy vaqtda mavjud kalitni boshqa yangisi bilan almashtirishi mumkin;
- vaqti-vaqti bilan vakolatlangan tashkilot katalogni to'laligicha yoki unga qo'shimchalarni e'lon qilib boradi;
- ishtirokchilar shuningdek katalogning elektron ko'rinishiga kirish huquqiga ham ega bo'lishi mumkin. Buning uchun ma'lumot almashuvchi ishtirokchilar va vakolatlangan tashkilot orasida autentifikasiya vositalari qo'llanilgan aloqa kanali talab qilinadi (3.2-rasm).



3.2- rasm. Oshkora foydalanish mumkin bo'lgan katalog

Bu sxema yakka tartibda oshkora e'lon qilishga nisbatan ancha himoyalangan bo'lsada, uning ham zaif tomonlari mavjud. Agar buzg'unchi vakolatlangan tashkilotning maxfiy kalitini olishga yoki hisoblab topishga muvaffaq bo'lsa, u qat'iy ishonch bilan soxtalashtirilgan ochiq kalitni berishi, demakki, ma'lumot almashinuvida ixtiyoriy ishtirokchi nomidan ishtirok etishi va ixtiyoriy ishtirokchiga mo'ljallangan ma'lumotni o'qishi mumkin bo'ladi. Katalogda saqlanuvchi qaydlarni o'zgartirish yordamida ham buzg'unchi shunday natijaga erishishi mumkin.

Ochiq kalitlarning ishonchli manbai

Bu sxemada ma'lumotlar almashinuvida qatnashuvchi barcha ishtirokchilar ochiq kalitlarining dinamik katalogini ta'minlovchi biror bosh vakolatlangan obyekt borligini faraz qiladi. Bundan tashqari har bir ishtirokchiga markazning ochiq kaliti ma'lum, lekin faqatgina markaz unga mos maxfiy kalitni biladi. Bunda quyidagilar bajariladi (3.3-rasm):

1. **A** boshlab beruvchi sana/VB qo'yilgan xabarni ochiq kalitlarning IMga **V** ishtirokchining joriy ochiq kaliti so'rovnomasi bilan yuboradi.

2. IM o'z maxfiy kaliti yordamida shifrlangan xabar bilan javob beradi. Bu xabarning shifrini **A** boshlab beruvchi IMning ochiq kalitidan foydalanib ochishi mumkin.

Bu xabar quyidagilarni o'z ichiga olishi lozim:

– **A** ishtirokchi **V** ishtirokchiga yuboradigan xabarlarni shifrlashi uchun V ishtirokchining ochiq kalitini;

– **A** tomonga javobni avvalgi yuborilgan so'rovnoma bilan taqqoslashi va IMga yuborilganda yo'lda o'zgartirib qo'yilmaganiga ishonch hosil qilishi uchun o'ziga xos so'rovnomani;

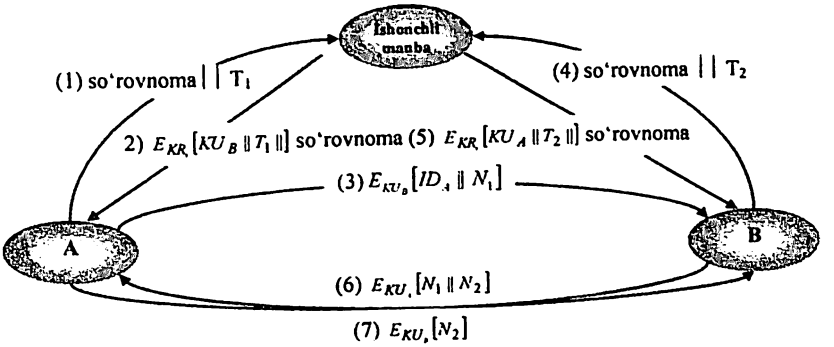
– maxsus sana/VBni, **A** ishtirokchi xabar IMning **V** ishtirokchini joriy kalitidan farq qiluvchi kalitli eski xabarlardan biri emasligiga inonmog'i uchun;

3. **A** boshlab beruvchi **V** ishtirokchining ochiq kalitini saqlab qo'yadi va undan **V** ishtirokchiga yuboriladigan xabarlarni shifrlashda foydalanadi, bu xabarda **A** ishtirokchining identifikatori va ushbu xabarning maxsus belgisi bo'lgan sana ham qayd etiladi;

4. V javob yo'llovchi A ishtirokchining ochiq kalitini IMdan A yuboruvchi V qabul qiluvchining ochiq kalitini olgan usul bilan oladi;

5. V javob yo'llovchi A boshlab beruvchiga V ning kaliti bilan shifrlangan xabarni va A yuboruvchining qo'ygan sanasini, shuningdek qabul qilingan ma'lumotning yuboruvchisi V ekanligiga ishontirish uchun, V ishtirokchi tomonidan generasiyalangan yangi sanani ham qo'shib yuboradi;

6. A boshlab beruvchi, V ishtirokchini javob yuboruvchi A ishtirokchi ekanligiga ishonishi uchun, uning ochiq kaliti bilan shifrlangan sanani qaytarib yuboradi.



3.3- rasm. Ochiq kalitlarning ishonchli manbai

Shunday qilib, oltita xabar yuborish talab qilinar ekan, lekin boshidagi to'rttasini yuborish ko'pincha talab qilinmaydi, chunki ikkala tomon ham bir-birining ochiq kalitini keyinchalik foydalanish uchun saqlab qo'yishi mumkin, buni keshlash deyiladi. Vaqti-vaqti bilan ishtirokchi kafolatlangan xavfsiz ma'lumot almashinish imkoniyatiga ega bo'lishi uchun o'z adresatlarining yangi ochiq kalit nusxalarini so'rashi lozim. Ochiq kalitning IM tarmoqning cheklangan qismi bo'lib, ishtirokchi unga yozishma olib bormoqchi bo'lgan har bir yangi adresatning ochiq kalitini olish uchun murojaat qilishi lozim. IM tomonidan yuritiluvchi ismlar va ochiq kalitlar katalogi ruxsatsiz kirishga nisbatan zaif bo'lib qoladi.

Ochiq kalitlar sertifikatlari

Sertifikatlar ishtirokchilar tomonidan ochiq kalitlarning IM bilan aloqasiz kalit almashinuvi uchun ishlatilishi mumkin bo'lib, almashinuv usuli xuddi ochiq kalitlarning IMining o'zidan olish usulidek ishonchli usulni ta'minlashi zarur. Har bir sertifikat ochiq kalit va boshqa ma'lumotni o'z ichiga olgan bo'lib, sertifikatlarning IM tomonidan ishlab chiqiladi va ishtirokchiga mos maxfiy kaliti bilan birga beriladi. Bir ishtirokchi o'zining kaliti to'g'risidagi ma'lumotni boshqa ishtirokchiga o'zining sertifikatini berish orqali yetkazadi. Boshqa ishtirokchilar esa sertifikat IM tomonidan berilganligini tekshirishlari mumkin. Keltirilgan sxemaga quyidagi talablar qo'yiladi [38-39]:

- har bir ishtirokchi sertifikat egasining ismi va ochiq kalitini aniqlashi uchun sertifikatni o'qish imkoniyatiga ega bo'lishi kerak;
- har bir ishtirokchi sertifikat sertifikatlarning IM tomonidan berilganligiga va u soxta emasligini tekshirish imkoniyatiga ega bo'lishi kerak;
- faqatgina sertifikatlarning IM gina sertifikatlarni yaratish va o'zgartirish imkoniyatiga ega bo'lishi kerak.

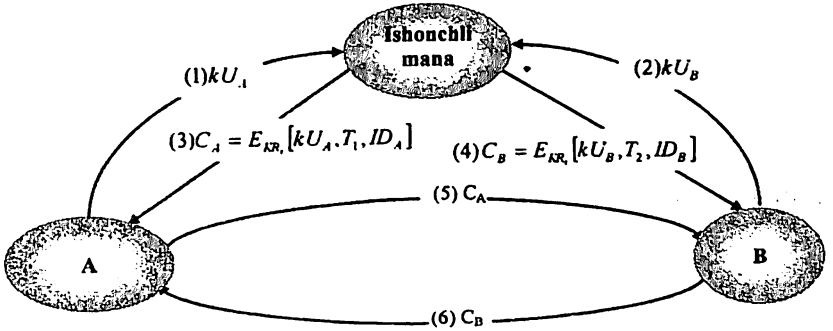
Sertifikatni ishlatilish sxemasi quyidagicha (3.4-rasm). Har bir ishtirokchi sertifikatlarning IMga ochiq kalitni taqdim etgan holda o'ziga sertifikat so'rab murojaat qiladi. So'rovnoma shaxsan yoki biror himoyalangan aloqa vositasi orqali murojaat qilishni talab etadi. **A** ishtirokchi uchun ishonch manbai $C_A = E_{KR_{im}}[T,\ ID_A,\ KU_B]$ sertifikat beradi, bunda kR_{im} – IMning maxfiy kaliti; kU_B – **V** ishtirokchining ochiq kaliti; ID_A – **A** ishtirokchining identifikatori; T – yuborilgan sana/vaqt. **A** ishtirokchi bu sertifikatni ixtiyoriy boshqa ishtirokchiga o'qishi va qabul qilishi uchun yuborishi mumkin:

$$D_{kU_{im}}[C_A] = D_{kU_{im}}[E_{kR_{im}}[T, ID_A, kU_A]] = (T, ID_A, kU_A),$$

bunda, kU_{im} – IMning ochiq kaliti; kU_A – **A** ishtirokchining ochiq kaliti.

Sertifikatni sertifikatlar IMning ochiq kaliti bilan o'qish mumkinligi, sertifikat aynan sertifikatlar IMdan kelganligini kafolatlaydi. ID_A, kU_A elementlar oluvchiga sertifikat egasining ismi va ochiq kalitini bildiradi. Sana/VB T sertifikatning qo'llanilish muddatini aniqlaydi. Sana/VB quyidagi ta'sirlar ketma-ketligidan muhofazalangan bo'lishi

kerak. Buzg'unchi A ishtirokchining maxfiy kalitini bilib olgan bo'lsin. U holda A ishtirokchi yangi (maxfiy va ochiq) kalitlar juftini generasiyalaydi va sertifikatlarning IMga yangi sertifikat olish uchun murojaat qiladi. Bu vaqtda buzg'unchi eski sertifikat asosida xabar ishlab, uni V ishtirokchiga yuboradi. Agar V ishtirokchi xabarni eski ochilgan kalit bilan shifrlasa, buzg'unchi bu xabarni o'qiy oladi. Bunda vaziyat mumkin bo'lgan tizimlarni eski tizim bekor qilingani to'g'risida xabardor qilinmaguncha qaltisligicha qoladi.



3.4- rasm. Ochiq kalitlar sertifikatlari

Ochiq kalitlar taqsimlangandan keyin xabarlarni qo'lga kiritish va buzishdan himoyalangan aloqani tashkil etish mumkin bo'ladi. Lekin ochiq kalitli shifrlashni qo'llanilganda ma'lumotlarni uzatish tezligi nisbatan sekinlashadi, bu ko'pincha ishtirokchilar uchun to'g'ri kelmaydi. Shuning uchun asosan Merkel tomonidan taklif etilgan maxfiy kalitlarning taqsimlash sxemasidan foydalaniladi [38-39].

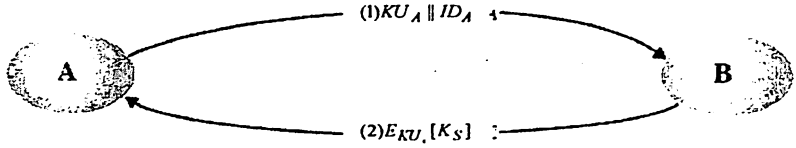
Taklif etilgan sxema quyidagidan iborat (3.5-rasm). Agar A boshlab beruvchi V ishtirokchi bilan ma'lumot almashmoqchi bo'lsa, quyidagi jarayon taklif etiladi:

1. A ishtirokchi (ochiq/maxfiy) kalitlar juftini generasiyalaydi va V ishtirokchiga kU_A va A ishtirokchining identifikatori bo'lgan ID_A ni o'z ichiga olgan xabarni yuboradi.

2. Qabul qiluvchi V maxfiy kalit k ni generasiyalaydi va bu kalitni A ishtirokchining ochiq kaliti bilan shifrlab, A ishtirokchiga yuboradi.

3. **A** ishtirokchi $D_{kU_A}[E_{kU_A}[k_S]]$ ni maxfiy kalitni tiklash uchun hisoblaydi. Faqatgina **A** ishtirokchi bu xabarning shifrini ochishi mumkin bo'lgani sababli faqat shu ikki ishtirokchi **A** va **V** k_A ning qiymatni biladi.

4. **A** ishtirokchi kR_A kalitni, **V** ishtirokchi esa kU_A ni yo'q qiladi.



3.5- rasm. Maxfiy kalitlar taqsimlashning Merkel sxemasi

Ikkala **A** va **V** ishtirokchi k_A seans kalitini qo'llab an'anaviy shifrlash yordamida himoyalangan aloqadan foydalanishi mumkin. Ma'lumot almashinuvi so'ngida **A** ishtirokchi ham, **V** ishtirokchi ham k_A ni yo'q qiladi. Sodda tuzilishiga qaramay, bu protokol e'tiborga loyiq. Aloqa boshlangunga qadar ham, aloqa tugagandan so'ng ham, hyech qanday kalit mavjud bo'lmaydi. Shuning uchun kalitning kompromentasiyalanish (obro'sizlanish) xavfi juda kichik va bu vaqtda aloqa himoyalangan bo'ladi. Lekin bu protokol faol hujumga nisbatan zaif. Agar **Ye** buzg'unchining aloqa kanaliga suqilib kirish imkoniyati mavjud bo'lsa, u aniqlangunga qadar aloqaga quyidagicha putur yetkazishi mumkin:

1. **A** ishtirokchi bir juft ochiq/maxfiy (kU_A, kR_A) kalitlarni generasiyalaydi, so'ngra kU_A ni va **A** ishtirokchining identifikatori ID_A mavjud bo'lgan xabarni **V** ishtirokchiga yuboradi.

2. **Ye** buzg'unchi xabarni tutib qoladi, o'zining xususiy bir juft ochiq/maxfiy (kU_{Ye}, kR_{Ye}) kalitlarini hosil qiladi va kU_{Ye}, ID_A mavjud bo'lgan xabarni **V** ishtirokchiga yuboradi.

3. **V** ishtirokchi k_s maxfiy kalitni generasiya qiladi va $E_{kU_A}[k_S]$ ni yuboradi.

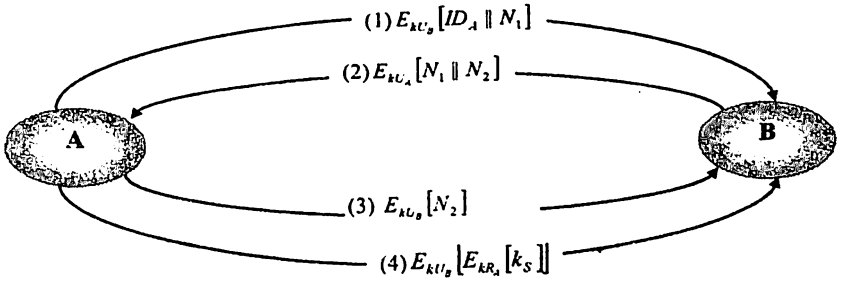
4. **Ye** buzg'unchi xabarni tutib qoladi va $D_{kU_Y}[E_{kU_Y}[k_S]]$ hisoblash yordamida k_s ning qiymatini topadi.

5. Buzg'unchi **A** ishtirokchiga $E_{kU_A}[k_S]$ ni yuboradi.

A ishtirokchi ham V ishtirokchiga ham k_s ma'lum bo'ladi, lekin ular Ye buzg'unchiga ham k_s ma'lumligini bilishmaydi. Shuning uchun A va V ishtirokchilar k_s dan foydalanib xabar almashinishlari mumkin. Ye buzg'unchi aloqa kanalida boshqa faol suqilib kirmaydi, faqatgina xabarlarni tutib qoladi. k_s ni bilgan holda buzg'unchi ixtiyoriy xabarni shifrini ochishi mumkin, ammo A va V ishtirokchilar bu muammodan bexabar bo'lishadi. Demak, bu protokol faqatgina xabarlarni passiv tutib qolish mumkin bo'lganida foyda beradi.

3.1.5. Maxfiy kalitlarni konfidensialligini va autentifikasiyasini ta'minlab taqsimlash sxemasi

Quyidagi 3.6-rasmda keltirilgan sxema faol va passiv hujumlardan himoyani ta'minlaydi.



3.6- rasm. Faol va passiv hujumlardan himoyani ta'minlash sxemasi

A va V yuqorida keltirilgan sxemalardan biri yordamida ochiq kalitlarini almashinishgan bo'lsin. Bunda quyidagi amallar bajariladi:

1. A ishtirokchi V ishtirokchiga shifrlangan axborot jo'natish uchun A ishtirokchining ID_A identifikatorini va N_1 psevdotasodifiy sonni o'z ichiga olgan xabarni V ning ochiq kaliti kU_V yordamida shifrlanb V ishtirokchiga yuboradi.

2. V ishtirokchi A ishtirokchiga undan olingan N_1 psevdotasodifiy sonni va yangi V ishtirokchi tomonidan generasiyalangan N_2 psevdotasodifiy sonni o'z ichiga olgan, hamda kU_A yordamida shifrlangan

xabarni jo'natadi. N_1 ning xabarda mavjudligi **A** ishtirokchini xabar yuboruvchi **V** ishtirokchi ekanligiga ishontiradi.

3. **A** ishtirokchi xabarni **V** ishtirokchining ochiq kaliti bilan shifrlab N_2 ni qaytarishi xabar yuboruvchi **A** ekanligiga **V** ni ishontiradi.

4. **A** ishtirokchi k_s maxfiy kalitni tanlab **V** ishtirokchiga $M = E_{kU_B}\left[E_{kR_A}[k_S]\right]$ xabarni yuboradi. **V** ishtirokchining ochiq kaliti bilan shifrlangan matnni faqatgina **V** ishtirokchigina o'qiy olishini, **A** ishtirokchi xabarini maxfiy kaliti bilan shifrlashi esa xabarni faqatgina **A** ishtirokchi yuborganini kafolatlaydi.

5. **V** ishtirokchi esa $D_{kU_A}\left[E_{kU_B}[M]\right]$ ni hisoblab maxfiy kalitni tiklaydi.

Bu sxemaning boshidagi uchta amal IMdagi ochiq kalit tarqatishining uchta so'nggi amaliga mos keladi. Natijada, maxfiy kalitlar almashinishda bu sxema konfidensiallik va autentifikasiyani kafolatlaydi.

3.1.6. Gibrid sxema

Maxfiy kalit tarqatishidagi ochiq kalit bilan shifrlashning yana bir sxemasi gibrid yondashuvi bo'lib, u IBM firmasining super kompyuterlarida qo'llaniladi [39-40]. Bu sxema kalit tarqatish markazi ishtirokini ko'zda tutadi.. Bunday uch bosqichli yondashuvning asosida quyidagi mantiq yotadi:

– *proseduralarning bajarilish tezligi.* Bu mantiqqa tranzaksiyalarni uzatishga ixtisoslashgan ilovalar (prilojeniye) moslangan bo'lib, bunda seans kalitlari tez-tez almashtirib turilishi lozim. Seans kalitlarini oshkora kalitli sxema yordamida tarqatilishi, bu sxemada shifrlash va shifrni ochish jarayonida ishlatiladigan hisoblash resurslariga qo'yiladigan katta talablar hisobiga tizimning unumdorligini juda ham pasaytirib yuborishi mumkin edi. Uch bosqichli iyerarxiyada ochiq kalit bilan shifrlash ishtirokchilar bilan kalit tarqatuvchi markaz orasida taqsimlanuvchi asosiy kalitni o'zgartirish kabi ba'zi hollardagina ishlatiladi;

– *qaytariluvchi moslik (obratnaya sovmestimost).* Gibrid sxemani mavjud sxemaning kalit tarqatish markazi prosedura va dastur ta'minotida

minimal o'zgartirishlar ko'zda tutgan kengaytmasi ko'rinishida osongina tadbiq etish mumkin.

Oshkora kalit bilan shifrlash bosqichini qo'shish asosiy kalit taqsimoti vositasini muhofazasini va samaradorligini ta'minlaydi. Bu esa bitta kalit taqsimoti markazining ko'plab bir-biridan yetarlicha uzoq masofada joylashgan ishtirokchilarga xizmat ko'rsatgandagi afzalligidir.

3.2. Simmetrik kriptotizimlarga asoslangan kalitlarni taqsimlash protokollari

3.2.1. Simmetrik shifrlash algoritmi yordamida kalit uzatishning sodda protokollari

Simmetrik kriptotizimlardan muvaffaqiyatli foydalanish uchun maxfiy kalit to'g'risida kelishib olish, ya'ni turli ishtirokchilar o'rtasida kalitlar taqsimlangan bo'lishi kerak. Taqsimlangan kalitlarga taqsimlashning tezkorligi va aniqligi, taqsimlanadigan kalitlarning maxfiyligi kabi talablar qo'yiladi [40].

Statik (uzoq vaqtli) kalit. Uzoq vaqt davomida ishlatiladigan kalit statik kalit deyiladi. "uzoq" so'zining ma'nosi kalitning qayerda va qancha vaqt davomida (bir necha soatdan bir necha yilgacha) ishlatilishga bog'liq. Statik kalitni ochilishi odatda asosiy muammoning halokatli oqibati hisoblanadi.

Seans (qisqa muddatli) kalitidan qisqa vaqt (bir necha soniyadan bir kungacha) oralig'ida foydalaniladi. Odatda undan bir martali aloqada maxfiylikni ta'minlash uchun foydalaniladi. Seans kalitining ochilishi faqat seansning maxfiyligini buzilishiga olib keladi, lekin bu butun kriptotizimning kriptobardoshliligiga hyech qanday ta'sir ko'rsatmasligi kerak.

Ushbu paragrafda simmetrik shifrlash algoritmi yordamida generasiya qilingan kalitni almashish protokollari ko'rib chiqiladi. Bu protokollarda axborot almashinuvi subyektlari bo'lgan **A** va **B** ishtirokchilar umumiy k_{AB} - kalitga ega deb qabul qilinadi. Bu protokollar, uchinchi ishonchli tomonning ishtirok etishi yoki etmasligiga bog'liq ravishda ikki turga bo'linadi. Avvalo uchinchi ishonchli tomon ishtirok etmagan protokollarni ko'rib o'tiladi. Buning uchun quyidagi belgilashlar kiritiladi:

Ye – shifrlash algoritmi;

t_A – VB;

r_A – **A** ishtirokchining tasodifiy soni;

n_A – **A** ishtirokchining generasiya qilish tartib raqami;

V – **B** ishtirokchining identifikasion raqami;

k_{AB} – ikkala ishtirokchiga ham ma'lum bo'lgan kalit.

Simmetrik kalitli kriptotizimda ishtirokchilardan tashqari kalitlarni tarqatuvchi tomon, ya'ni kalitlarni tarqatish markazi ham ishtirok etadi. Simmetrik kriptotizim yordamida kalitlarni almashish protokoli quyidagicha amalga oshiriladi:

1. **A** ishtirokchi **V** ishtirokchi bilan aloqa o'rnatish uchun kalit tarqatuvchiga murojaat qiladi va seans kalitini so'raydi.

2. Kalit tarqatuvchi seans kalitni generasiya qiladi va bu kalitini ikki nusxada shifrlab, **A** ishtirokchiga uzatadi.

3. **A** ishtirokchi o'ziga tegishli shifrlangan seans kalitini deshifrlaydi.

4. **A** ishtirokchi shifrlangan seans kalitining ikkinchi nusxasini **V** ishtirokchiga uzatadi.

5. **V** ishtirokchi o'zining shifrlangan kalitini shifrini ochadi.

6. **A** va **V** ishtirokchilar maxfiy aloqa uchun yuqorida hosil qilingan seans kalitidan foydalanadilar.

Bu protokolda seans kalitlar tarqatuvchini ishonchli tomon deb qabul qiladilar. Agar kriptotahlilchi aktiv hujum yordamida yoki boshqa qandaydir usul bilan seans kalitlarini qo'lga kiritsa, u holda kriptotahlilchi aloqa tarmog'iga ulanib, tarmoqdagi barcha almashinuvchi maxfiy ma'lumotlarni kuzatish yoki eshitish imkoniyatiga ega bo'ladi.

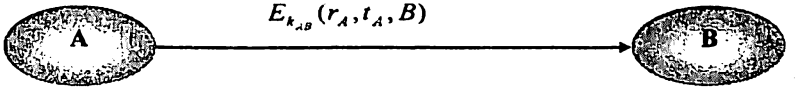
Yuqorida bayon qilingan tizimning yana bir kamchiligi shundaki, har bir kalit almashishda qatnashuvchi uchinchi tomon, ya'ni kalitlarni tarqatish markazi, mazkur tizimning nozik nuqtasi hisoblanadi. Agar unda biror kamchilik kuzatilsa, butun tizimga ta'sir etadi. Quyida shu kabi bir nechta protokollar haqida to'xtalib o'tiladi.

1 – protokol

Simmetrik shifrlash algoritmi yordamida generasiya qilingan kalitni uzatish protokolining sodda ko'rinishi – seans kalitni bir raundda uzatish (3.7-rasm). Butun protokol yagona ma'lumotdan tashkil topgan:

$$A \rightarrow V: E_{k_{AB}}(r_A, t_A, B).$$

V ishtirokchi umumiy kalit yordamida bu ma'lumotning shifrini ochadi. Bu holda r_A seans kalit vazifasini bajaradi.



3.7- rasm. Simmetrik shifrlash algoritmi yordamida generasiya qilingan kalitni uzatish protokoli

Agar ko'rib chiqilgan protokolda :

1) Baqt belgisi uzatilmasa, kriptotahlilchi aynan shu ma'lumotni qayta uzatishi mumkin.

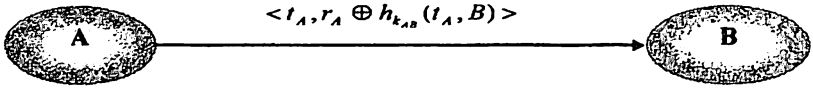
2) **V** ishtirokchining identifikasiya raqami ko'rsatilmasa, kriptotahlilchi bu ma'lumotni **A** ishtirokchining o'ziga uzatishi mumkin va natijada **A** ishtirokchi ma'lumotni **V** ishtirokchidan kelgan yoki kelmaganligini aniqlay olmaydi.

3) Seans kalit $f(r_A, r_B)$ funksiya yordamida hisoblab topilishi mumkin. Agar f funksiya sifatida bir tomonlama funksiyadan foydalanilsa, tomonlarning hyech biri natijaviy kalitni nazorat qila olmaydi.

Yuqorida keltirilgan protokolda shifrlash algoritmi o'rniga kalit yordamidagi xesh-funksiyadan foydalanish mumkin:

$$A \rightarrow V: <t_A, r_A \oplus h_{k_{AB}}(t_A, B)>.$$

V ishtirokchi ma'lumotni qabul qiladi. U ham kalit orqali bajariladigan xesh-funksiyani biladi. Qabul qilingan ma'lumotdan VBni ajratib oladi. Uning keyingi vazifasi VB va o'zining identifikasiya raqamini birlashtirib kalitli xesh-funksiya yordamida xeshlashdir. Chiqqan $h_{k_{AB}}(t_A, B)$ natija qolgan $r_A \oplus h_{k_{AB}}(t_A, B)$ ma'lumotga XOR amali bo'yicha qo'shiladi. Natijada r_A, ya'ni seans kalit hosil bo'ladi (3.8-rasm).



3.8- rasm. Kalit yordamidagi xesh-funksiyadan foydalanib generasiya qilingan kalitni uzatish protokoli

Agar tizim umumiy sinxron vaqtga ega bo'lmasa, lekin kalitning yangiligiga ishonch hosil qilish talab qilinsa, u holda VBni tartib raqami bilan almashtirilishi mumkin. U holda protokol quyidagi ko'rinishga keladi:

2 – protokol

V ishtirokchi o'zining n_B tasodifiy sonini hosil qilib uni **A** ishtirokchiga uzatadi:

$$V \rightarrow A : n_B.$$

A ishtirokchi bu tasodifiy sonni qabul qilib, unga o'zi hosil qilgan seans kalitni va **V** ishtirokchining identifikasiya raqamini birlashtirib ikkala ishtirokchi uchun umumiy bo'lgan kalit yordamida shifrlaydi hamda **V** ishtirokchiga uzatadi:

$$A \rightarrow V: E_{k_{AB}}(r_A, n_B, B).$$

V ishtirokchi n_B va **V** ni tekshirib, r_A seans kalitning to'g'ri ekanligiga ishonch hosil qiladi. Xesh-funksiyadan foydalanilsa protokolning ko'rinishi quyidagicha bo'ladi:

$$\text{V} \rightarrow \text{A} : n_B,$$

$$\text{A} \rightarrow \text{V}: r_A \oplus h_{k_{AB}}(n_B, B).$$

Ushbu protokolni shunday o'zgartirish mumkinki, natijada $k = r_A$ - seans kalitni bir tomon emas, balki ikkala tomon birgalikda generasiya qiladilar.

A va **V** ishtirokchilar r_A va r_B sonlaridan boshqa tasodifiy n_A va n_B sonlarni generasiya qiladilar. Bu yerda r_A va r_B sonlari kalit materiallari sifatida foydalaniladi, n_A va n_B sonlari esa kalitning yangi kalit ekanligini ta'minlaydi. U holda protokol quyidagi ko'rinishga keladi:

Yuqorida keltirilgan protokol kabi **V** ishtirokchi o'zining n_B tasodifiy sonini **A** ishtirokchiga uzatadi:

$$V \rightarrow A : n_B.$$

A ishtirokchi bu tasodifiy sonni qabul qiladi. O'zaro

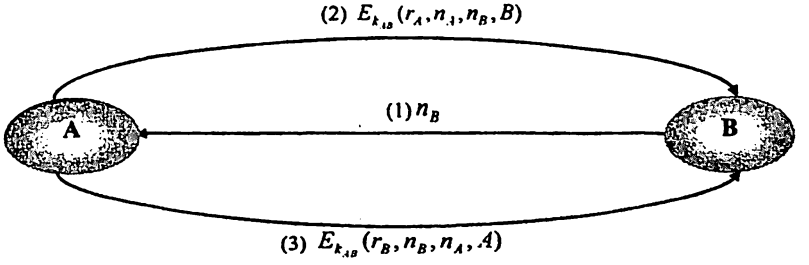
autentifikasiyani ta'minlash hamda seans kalitni birgalikda hosil qilish uchun quyidagi ma'lumotni **V** ishtirokchiga uzatadi.

$$A \rightarrow V: E_{k_{AB}}(r_A, n_A, n_B, B).$$

V ishtirokchi ma'lumotning shifrini ochib, n_B tasodifiy sonni tekshiradi. Natija to'g'ri bo'lsa, **A** ishtirokchiga r_B, n_B, n_A, A ni umumiy kalit bilan shifrlab uzatadi.

$$V \rightarrow A: E_{k_{AB}}(r_B, n_B, n_A, A).$$

Natijada har bir tomon umumiy kalitni oldindan kelishib olingan biror funksiya yordamida $k = f(r_A, r_B)$ qonuniyat bilan hisoblab topishi mumkin (3.9-rasm).



3.9- rasm. Xesh-funksiyadan foydalanib kalitni uzatish protokoli

3.2.2. Shamir protokoli

Quyida esa Shamir protokoli deb ataluvchi (kalitsiz) umumiy maxfiy ma'lumotdan foydalanmagan holda kalitni uzatish protokolini ko'rib chiqamiz. Bu protokol qadamlariga muvofiq kalitning maxfiylik masalasi ta'minlanadi [10].

Shunday shifrlash va shifrni ochish o'zgartirishlari mavjudki, barcha x ma'lumotlar, k_1 va k_2 lar uchun quyidagi

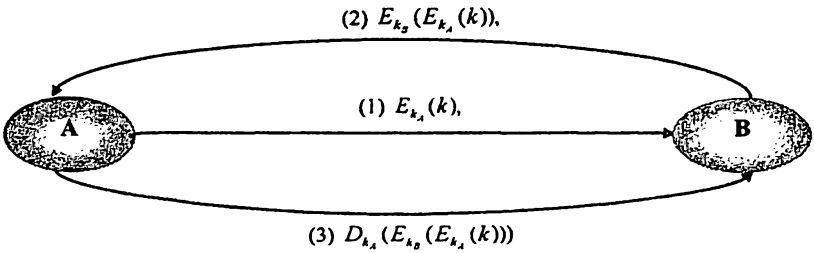
$E_{k_1}(E_{k_2}(x)) = E_{k_2}(E_{k_1}(x))$ shart bajariladi.

U holda **A** va **V** ishtirokchilar k seans kalitni uzatuvchi quyidagi 3-bosqichli protokoldan foydalanishlari mumkin (3.10-rasm):

(1) $A \rightarrow V: E_{k_A}(k)$,

(2) $V \rightarrow A: E_{k_B}(E_{k_A}(k))$,

(3) $\underline{A \to V: D_{k_A}(E_{k_B}(E_{k_A}(k)))}$.



3.10- rasm. Shamir protokoli

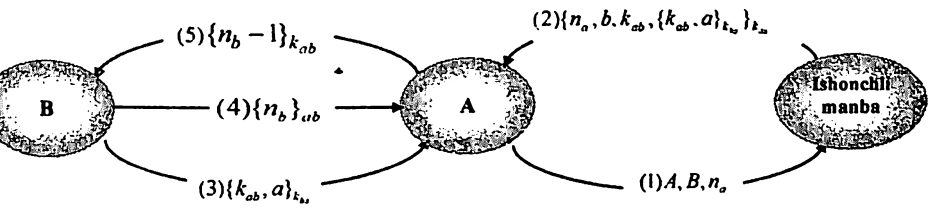
Xususan, Shamir protokolida modul bo'yicha darajaga ko'tarish amalidan foydalanish taklif etilgan, ya'ni $E_{k_A}(k) = k^{k_A} \bmod p$. Shunday qilib, bu protokolning kriptobardoshligi diskret logarifmlash masalasining murakkabligiga asoslangan. Shamir protokolining kamchiligi shundaki, bu protokolda autentifikasiya masalasi hal etilmagan.

3.2.3. Nidxeym-Shreder protokoli

Bu protokol 1978 yilda ishlab chiqilgan bo'lib, bugungi kunda eng ko'p o'rganiladigan protokol hisoblanadi [3-7]. Bu protokolning mashhur bo'lishiga sabab, hattoki eng oddiy protokol ham axborot himoyasidagi kamchiliklarni uzoq vaqt berkitishi mumkin.

Xabar almashinuvi quyidagi sxema bo'yicha boradi (3.11-rasm):

$$A \to S : A, B, n_a,$$
$$S \to A : \{n_a, b, k_{ab}, \{k_{ab}, a\}_{k_{bs}}\}_{k_{as}}$$
$$A \to B : \{k_{ab}, a\}_{k_{bs}},$$
$$B \to A : \{n_b\}_{ab}$$
$$A \to B : \{n_b - 1\}_{k_{ab}}$$



3.11- rasm. Nidxeym-Shreder protokoli

Endi protokolning batafsil bayonini keltiramiz:

– **A** boshlab beruvchi *S* IMga **V** ishtirokchining kalitini u bilan yozishma olib borish uchun so'rab xabar yuboradi. Bunda xabarga **A** tomonidan yaratilgan maxsus sonli qo'shimcha qo'shib yuboriladi;

– *S* IM k_{ab} kalitni generasiya qiladi va uni **A** ishtirokchiga yuboradi. Unga **A** ishtirokchi xabar uning so'rovnomasiga javob sifatida kelganini bilishi uchun sonli qo'shimcha n_a qo'shiladi. Seans kaliti k_{bs} yordamida shifrlanadi va xabarga qo'shib yuboriladi.

– Uchinchi xatda seans kaliti **V** ishtirokchiga yuboriladi.

– **V** ishtirokchi bu xabarning jo'natuvchisi **A** ishtirokchi ekanligini tekshirib ko'rishi kerak, ya'ni **A** ishtirokchi hali ham faolligiga ishonch hosil qilishi kerak. Buning uchun **V** ishtirokchi to'rtinchi xabarda o'zining sonli qo'shimchasini **A** ishtirokchiga shifrlangan holda yuboradi.

– **V** ishtirokchiga o'zining ishga layoqatligini ko'rsatish uchun **A** ishtirokchi n_b ga bog'liq bo'lgan oddiy iborani shifrlaydi va **V** ishtirokchiga yuboradi.

Nidxeym-Shreder protokolining asosiy kamchiligi uni qo'llash natijasida **V** ishtirokchi olgan kalitni yangi deb hisoblashga asos yo'q. Bu dalil protokol e'lon qilingandan keyin bir oz vaqt o'tgandan keyingina ma'lum bo'ldi. Buzg'unchi avvalgi xabarlarni va seans kalitini topib eski xatlarni **V** ishtirokchi eslatilgan xabarlarni oxirigi uchta xabar o'rnida ishlatishi mumkin. Shunday qilib buzg'unchi **V** ishtirokchini u **A** ishtirokchi bilan so'zlashuv olib borayotganiga ishontirib, o'zining kalitini olishga majbur qilib aldashi mumkin.

3.2.4. Otvey-Riis protokoli

Otvey-Riis protokoli 1987 yildan boshlab deyarli ishlatilmaydi, ammo u tarixiy nuqtai nazardan muhim o'rin tutadi [3-7]. Nidxeym-Shreder protokoliga o'xshab, unda ham vaqtni sinxronlashtirish talab etilmaydi.

Xuddi avvalgi protokollardagidek ikkita ishtirokchi ishonch manbaining S vositachiligida kalit to'g'risida kelishib olishadi. Bunda n_a va n_b sonli qo'shimchalar xabarning barcha shifrlangan komponentalarining yangiligini tasdiqlash uchun ishtirok etadi. Bundan tashqari M sonli qo'shimchasi bitta seansga tegishli xabarlarni o'zaro bog'laydi. Otvey-Riis protokoli Nidxeym-Shreder protokoliga nisbatan qisqa, u faqat to'rtta xabardan iborat. Ammo bu xabarlar umuman boshqacha ko'rinishga ega. Avvalgidagi kabi ishonch manbai ikki ishtirokchi uchun k_{ab} kalitni generasiyalaydi.

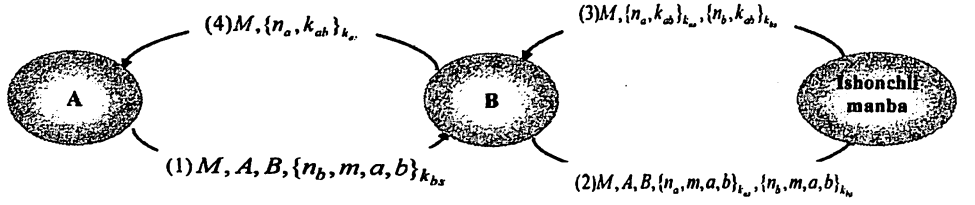
Otvey-Riis protokoli quyidagi bosqichlardan iborat (3.12-rasm):

$$A \to B: M, A, B, \{n_a, m, a, b\}_{k_{as}},$$

$$B \to S: M, A, B, \{n_a, m, a, b\}_{k_{as}}, \{n_b, m, a, b\}_{k_{bs}},$$

$$S \to B: M, \{n_a, k_{ab}\}_{k_{as}}, \{n_b, k_{ab}\}_{k_{bs}},$$

$$B \to A: M, \{n_a, k_{ab}\}_{k_{as}}.$$



3.12- rasm. Otvey-Riis protokoli

Protokol k_{ab} kalitni xabarni shifrlash uchun ishlatmagani tufayli, ikkala tomon ham bu kalit boshqa ishtirokchiga ayonmi yo'qmi xabarsiz. Bundan Otvey-Riis protokoli kalitni tasdiqlashni o'z ichiga olmaydi degan xulosa keladi. Kelishuvni amalga oshirayotgan tomonlarga nimalar

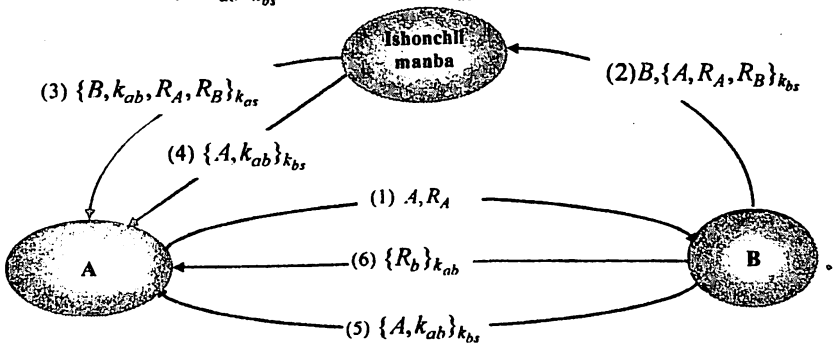
ma'lumligini ko'ramiz. **A** ishtirokchi **V** ishtirokchi n_a sonli qo'shimchali xabar yuborganini biladi, **V** ishtirokchi bu sonli qo'shimchaning yaratuvchisi bo'lgani uchun **A** ishtirokchi bu sonli qo'shimcha yangiligiga ishonadi. Demak, **V** ishtirokchi o'z xabarini yaqinda yuborgan bo'lishi kerak. Boshqa tarafdan server **V** ishtirokchini **A** ishtirokchi tomonidan xabarga qo'shilgan sonli qo'shimcha haqida xabardor qilyapti, ammo **V** ishtirokchi olgan xabari eski xabarlardan birining qayta yuborilmasi bo'lishini tahmin qilishga hyech qanday asos yo'q.

3.2.5. Yahalom protokoli

Yahalom (Yaxalom) protokoli kalit taqsimotining IM ishtirokidagi simmetrik protokolidir [10]. Katta halqumli qurbaqa protokolidan farqli tomoni shundaki, bu protokolda ikki ishtirokchi IMning faqat ular ikkisi uchungina umumiy maxfiy kalit generasiya qilganiga ishonch hosil qilishlari mumkin.

Yaxalom protokolining xabar almashinuv sxemasi quyidagicha (3.13-rasm):

$$A \to B: A, R_A,$$
$$B \to S: B, \{A, R_A, R_B\}_{k_{bs}},$$
$$S \to A: \{B, k_{ab}, R_A, R_B\}_{k_{as}},$$
$$S \to A: \{A, k_{ab}\}_{k_{bs}},$$
$$A \to B: \{A, k_{ab}\}_{k_{bs}},\ A \to B: \{R_B\}_{k_{ab}}.$$



3.13- rasm. Yahalom protokoli

Quyida protokolning batafsil bayoni keltiriladi:

– **A** ishtirokchi **V** ishtirokchiga tasodifiy tanlangan son R_A ni va o'z identifikatorini yuboradi.

– **V** ishtirokchi xabarni o'zining tasodifiy tanlagan R_B soni bilan to'ldirib, so'ngra k_{bs} kalit bilan shifrlab va o'z identifikatorini qo'shib IMga uzatadi.

– IM **V** ishtirokchining identifikatori, seans kaliti k_{ab} va tasodofiy R_A va R_B sonlarni k_{as} kalit bilan shifrlab **A** ishtirokchiga 1-xabarni yuboradi.

– Ikkinchi xabarda esa IM **A** ishtirokchining identifikatori va umumiy seans kaliti k_{ab} ni k_{bs} kalit bilan shifrlab **A** ishtirokchiga uzatadi.

– **A** ishtirokchi 1-xabarni shifrini ochib, R_A ning avval yuborilganiga mosligiga ishonch hosil qilib, IM yuborgan 2-xabarni **V** ishtirokchiga yuboradi.

– **A** ishtirokchi **V** ning seans kaliti bilan shifrlangan R_B tasodifiy sonini **V** ishtirokchiga uzatadi. **V** ishtirokchi 2 ta qabul qilgan xabarlardagi R_B va k_{ab} ning qiymatini olib uni avvalgilari bilan solishtiradi.

3.2.6. Nyuman-Stabblbayn protokoli

Nyuman-Stabblbayn protokoli kalit taqsimoti va autentifikasiyasining IM ishtirokidagi simmetrik protokoli bo'lib, Yaxalom protokolining takomillashtirilgan rusumi hisoblanadi [10]. Nyuman - Stabblbayn protokolining o'ziga xos xususiyati shundan iboratki, unda tomonlararo vaqtni sinxronlashtirish zarurati va IMni ishtirokisiz takroriy autentifikasiya qilish imkoniyati mavjud.

Nyuman - Stabblbayn protokolining sxemasi quyidagicha (3.14-rasm):

$$A \to B : A, R_A,$$

$$B \to S : B, R_b, \{A, R_A, t_B\}_{k_{bs}},$$

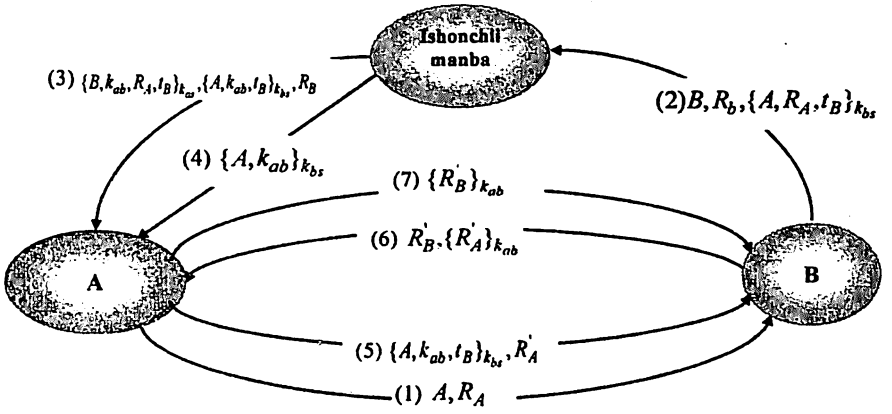
$$S \to A : \{B, k_{ab}, R_A, t_B\}_{k_{as}}, \{A, k_{ab}, t_B\}_{k_{bs}}, R_B$$

$$A \to B : \{A, k_{ab}\}_{k_{bs}}, \{R_B\}_{k_{ab}}$$

$$A \to B : \{A, k_{ab}, t_B\}_{k_{bs}}, R_A^{'}$$

$$B \to A : R_B^{'}, \{R_A^{'}\}_{k_{ab}},$$

$A \rightarrow B : \{R_B^{'}\}_{k_{ab}}$.



3.14- rasm. Nyuman-Stabblbayn protokoli

A ishtirokchi **V** ishtirokchiga tasodifiy tanlangan son R_A ni va o'z identifikatorini yuboradi.

– **V** ishtirokchi xabarni o'zining VB t_V bilan to'ldiradi, so'ngra k_{bs} kalit bilan shifrlab, o'z identifikatorini va tasodifiy tanlagan R_B sonni qo'shib IMga uzatadi.

– IM **V** ishtirokchi identifikatorini, **A** ishtirokchining tasodifiy tanlangan son R_A ni, seans kaliti k_{ab} ni va t_V ni k_{as} kalit bilan, A ishtirokchidan identifikatorini, seans kaliti k_{ab} ni va t_V ni k_{bs} kalit bilan shifrlab, so'ngra tasodifiy tanlagan R_B sonni qo'shib **A** ishtirokchiga yuboradi.

– A ishtirokchi R_A ni 1-xabarda o'zi yuborgani bilan taqqoslab, bir xilligiga ishonch hosil qilib, so'ngra o'z idantifikatorini va seans kaliti k_{ab} ni k_{bs} kalit bilan shifrlab, unga R_B sonini seans kaliti k_{ab} bilan shifrlanganini qo'shib **V** ishtirokchiga uzatadi.

– V ishtirokchi o'z navbatida t_V va R_B qiymatlarni tekshirib, o'zgarmaganligiga ishonch hosil qiladi.

Yuqorida aytib o'tganimizdek, bu protokolda IMning ishtirokisiz, yangi tasodifiy tanlangan sonlardan foydalanib takroriy autentifikasiya qilish imkoniyati mavjud, ya'ni

– **A** ishtirokchi o'z identifikatorini, seans kaliti k_{ab} ni va t_V ni k_{bs} kalit bilan shifrlab uni yangi tasodifiy tanlangan son $R_A^{'}$ bilan to'ldirib **V** ishtirokchiga yuboradi.

– **V** ishtirokchi yangi tasodifiy tanlangan son $R_A^{'}$ ni seans kaliti k_{ab} bilan shifrlab, uni o'zi tasodifiy tanlagan yangi $R_B^{'}$ bilan to'ldirib **A** ishtirokchiga qaytaradi.

– **A** ishtirokchi esa o'z navbatida **V** tasodifiy tanlagan yangi $R_B^{'}$ ni seans kaliti k_{ab} bilan shifrlab **V** ishtirokchiga yuboradi.

Bunda yangi tasodifiy tanlangan $R_A^{'}$ va $R_B^{'}$ sonlardan foydalanish qayta yuborishga bo'ladigan hujumdan himoya qiladi.

3.2.7. SKID protokoli

SKID protokoli simmetrik kriptografiya asosida qurilgan identifikasiya masalasini ta'minlashga qaratilgan bo'lib, uning SKID2 va SKID3 turlari mavjud. Quyida **V** ishtirokchiga o'zining haqiqiyligini ko'rsatish imkonini beruvchi SKID2 protokoli ko'rib chiqiladi [10-11].

1) **A** ishtirokchi tasodifiy R_A - sonini **V** ishtirokchiga uzatadi.

2) **V** ishtirokchi tasodifiy R_B - sonini oladi. U $R_B, H_k(R_A, R_B, B)$ ni **A** ishtirokchiga uzatadi. Bu yerda H_k – MAS kod.

3) **A** ishtirokchi $H_k(R_A, R_B, B)$ ni xisoblaydi va qabul qilgani bilan solishtiradi. Agar natijalar teng bo'lsa, u holda **A** ishtirokchi **V** ishtirokchi bilan to'g'ri bog'langaniga ishonch hosil qiladi.

SKID3 protokoli esa **A** va **V** ishtirokchilarning to'liq autentifikasiyasini ta'minlaydi. 1, 3 - bosqichlar SKID2 protokoli kabi bajariladi:

4) **A** ishtirokchi $N_K(R_V, A)$ ni **V** ishtirokchiga uzatadi.

5) **B** ishtirokchi $H_k(R_B, A)$ ni hisoblaydi va qabul qilgani bilan solishtiradi. Agar natijalar teng bo'lsa, **V** ishtirokchi aynan **A** ishtirokchi bilan bog'langaniga ishonch hosil qiladi.

Ushbu protokol "O'rtadagi kishi" hujumiga bardoshli emas.

3.2.8. Vaqt belgisi protokoli

Ba'zi hollarda yuborilayotgan xabarlarga VB biriktiriladi. Bu quyidagi sabablarga ko'ra qilinadi [10-11]:

- qabul qilingan xabarlar va ularning manbalarining autentifikasiyalanganligiga nisbatan ishonchni kuchaytirish;
- yuborilgan xabarni qayta yuborishga asoslangan hujumga qarshi turish.

Xabardagi VB yolg'on yoki soxta bo'lishi mumkin. Shuning uchun ba'zi KPlarda VBni qo'yish yuboruvchi tomonidan emas ishonchli vositachi T tomonidan amalga oshiriladi. Masalan m xabariga VBni qo'shib qo'yish quyidagicha bo'ladi:

1. $A \rightarrow T : m$
2. $T \rightarrow A : S_T(n, t)$

T tomon A bilan kelishgan holda yolg'on VBni xabarga qo'shib yuborishi imkoni bo'lsa, u holda bunday VBni qo'shish usuli yordam bermaydi. Qo'shilayotgan VBlari bir-biri bilan aloqada bo'ladigan quyidagi KP bunday turdagi hujumlarga bardosh bera oladi. Agar A ishtirokchisi uchun m xabarga VBni qo'yish zarur bo'lsa, u quyidagi amallarni bajaradi:

1. $A \rightarrow T : h(m), A$, бу ерда h – Қайсидир хэш – функция
2. $T \rightarrow A : S_T(A, n, h_n, t_n, A_{n-1}, h_{n-1}, t_{n-1}, H_n)$

Bu yerda:

- n – qo'shilayotgan VBning tartibli raqami,
- $h_n := h(m)$,
- t_n – qo'shilgan VB,
- A_{n-1} – unga T avvalgi VBni qo'shib yuborgan ishtirokchi,
- h_{n-1} - A_{n-1} ishtirokchi xabarining xesh-funksiya qiymati,
- t_{n-1} – avvalgi VB,
- $H_n := h(A_{n-1}, h_{n-1}, t_{n-1}, H_{n-1})$.

T $n+1$ tartibli VBni qo'shgach, u quyidagi amalni bajaradi:

$T \rightarrow A : A_{n+1}$

bu yerda A_{n+1} - VBni qo'shish maqsadida T ga murojaat qilgan A ishtirokchidan keyingi ishtirokchi.

Agar t_n VB haqiqiyligiga shubha tug'ilsa, u holda A ishtirokchi t_n ni haqiqiyligini tasdiqlovchi axborotni olish maqsadida A_{n-1} va A_{n+1}

bilan bog'lanadi. Agar bu axborotlarni haqiqiyligiga ham shubha tug'ilsa, u holda A ishtirokchi A_{n-2} va A_{n+2} bilan bog'lanadi va hokazo.

Mazkur qo'shilayotgan t_n VBni avvalgi k va navbatdagi k bilan bog'lab qo'yish orqali avvalgi KPni kuchaytirish mumkin. Ushbu KPda A_n ishtirokchi t_{n+1} VBni xotirada saqlaydi ($i = \pm 1, \ldots, \pm k$).

T ishonchli vositachi bo'lmagan holda, VB qo'yish uchun oddiy ishtirokchilarni jalb etish mumkin. Bu holda A ishtirokchining m xabariga VBni qo'yish quyidagicha bo'ladi. A ishtirokchi tasodifiy tarzda $A_1, \ldots, A_k$ ishtirokchilar to'plamini tanlaydi va $S_{A_i}(h(m), t_i)$ ERIni unga jo'natishni so'ragan holda ularning har biriga $h(m)$ satrini jo'natadi, bu yerda t_i - joriy vaqt momentida A_i ishtirokchining vaqt ko'rsatkichi. m xabarning VB quyidagi ko'rinishga ega

$$\{S_{A_i}(h(m), t_i) \mid i = 1, \ldots, k\}$$

3.3. Nosimmetrik kriptotizimlarga asoslangan kalitlarni taqsimlash protokollari

3.3.1. Diffi-Xellman algoritmi va protokoli

Kalit tarqatishning eng birinchi algoritmlaridan biri bo'lgan Diffi-Xellman algoritmi nosimmetrik shifrlashga asoslangan bo'lib, u ikki ishtirokchi uchun ma'lumotlarni shifrlashda bir-biriga kalitini muhofazalangan holda xabar qilish imkonini beradi [4-6].

Diffi-Xellman sxemasiga asosan kalit tarqatish quyidagicha amalga oshiriladi. Bu sxemada ikkita oshkora son mavjud bo'lib: tub son q va q ning boshlang'ich ildizi bo'lgan butun son α. Faraz qilaylik, A va V ishtirokchilar kalit almashmoqchi bo'lsin. A ishtirokchi tasodifiy $X_A < q$ butun son tanlaydi va $Y_A \equiv \alpha^{X_A} \bmod q$ qiymatni hisoblaydi. Xuddi shuningdek V ishtirokchi ixtiyoriy $X_V < q$ butun son tanlaydi va $Y_V \equiv \alpha^{X_B} \bmod q$ hisoblaydi. Har bir ishtirokchi X ning qiymatini sir saqlaydi va Y ning qiymati boshqa ishtirokchi uchun erkin bo'ladi. A ishtirokchi kalitni $k \equiv (Y_B)^{X_A} \bmod q$ formula bilan, V ishtirokchi esa $k \equiv (Y_A)^{X_B} \bmod q$ formula bilan hosil qiladi. Bu ikki formulalar orqali hisob-kitob bir xil natija beradi:

$k \equiv (Y_B)^{X_A} \bmod q \equiv (\alpha^{X_B} \bmod q)^{X_A} \bmod q \equiv (\alpha^{X_B})^{X_A} \bmod q \equiv \alpha^{X_B X_A} \bmod q \equiv$

$\equiv (\alpha^{X_A})^{X_B} \bmod q \equiv (\alpha^{X_A} \bmod q)^{X_B} \bmod q \equiv (Y_A)^{X_B} \bmod q$

Ikki ishtirokchi maxfiy kalit almashishadi. Bunda X_A va X_V sir saqlangani uchun, buzg'unchiga faqat q, α, Y_A, Y_V lar ma'lum bo'ladi. Shuning uchun buzg'unchi kalitni topishi uchun diskret logarifmni hisoblashi kerak bo'ladi: $X_B = ind_{\alpha,q}(Y_B)$. So'ngra u k kalitni V ishtirokchi hisoblagandek hisoblaydi.

Kalit taqsimlashning Diffi-Xellman sxemasi xavfsizligi katta tub sonning diskret logarifmini aniqlash masalasining yechilishi murakkabligiga asoslangan. Quyida bunga misol keltiramiz.

Modul sifatida $q=113$ tub sonini tanlaymiz. Uning birga aylantiruvchi ildizi $\alpha=3$. A va V ishtirokchilar mos ravishda $X_A=42$ va $X_V=86$ maxfiy kalitlarni tanlagan bo'lsin. U holda har biri ochiq kalitni quyidagicha hisoblaydi:

$Y_A = 3^{42} \equiv 69 \ (mod\ 113), \quad Y_V = 3^{86} \equiv 22 \ (mod\ 113).$

Ochiq kalitlarni almashganlaridan so'ng ularning har biri umumiy maxfiy kalitni hisoblashi mumkin:

$k \equiv (Y_B)^{X_A} \bmod q \equiv 22^{42} \equiv 98 \ (mod\ 113),$

$k \equiv (Y_A)^{X_B} \bmod q \equiv 69^{86} \equiv 98 \ (mod\ 113).$

Faqatgina 69 va 22 ga ega bo'lgan buzg'unchi uchun 98 ni hisoblab topish mushkul bo'ladi.

Kriptografik kalitlarni taqsimlash protokoli deganda, protokolni bajarish jarayonida umumiy maxfiylik ikki va undan ortiq tomonlarga kriptografik maqsadlarda keyinchalik foydalanish uchun erkin bo'ladigan protokol tushuniladi [3]. Kalitlarni taqsimlash protokoli ikkita sinfga ajraladi:

- kalitlarni transportirovkalash protokollari;
- kalitlarni almashish protokollari.

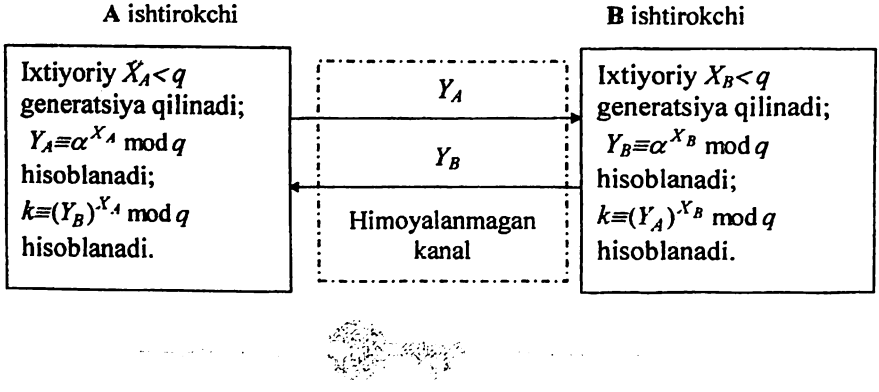
Kalitlarni transportirovkalash protokoli shunday protokolki, unda bitta ishtirokchi maxfiylikni ishlab chiqadi yoki boshqa yo'l bilan qo'lga kiritadi va xavfsiz yo'l bilan boshqa ishtirokchilarga uzatadi.

Kalitlarni transportirovkalash protokoliga xorijiy davlatlarda ishlab chiqilgan Nidxeym-Shreder, Otvey-Riis, Kerberos, Beller-Yacobi, SSL, uch bosqichli Shamir, X.509 protokollari misol bo'ladi.

Kalitlarni almashish protokolida esa umumiy maxfiylik ikkita yoki undan ko'proq ishtirokchilarning har biri tomonidan olib chiqilgan axborotning funksiyasi sifatida ishlab chiqarilishi natijasida boshqa hyech qanday tomon ularning umumiy maxfiyligini aniqlay olmaydi.

Kalitlarni almashish protokollariga esa Diffi-Xellman, Sharadi Merkl, Blom sxemasi, El Gamal, MTI, STS va boshqa protokollar kiradi [10-11].

Quyidagi 3.15-rasmda Diffi-Xellman sxemasini qo'llashga doir oddiy protokol keltirilgan.



3.15- rasm. Diffi-Xellman sxemasini qo'llashga doir protokol

Faraz qilaylik, **A** ishtirokchi **V** ishtirokchi bilan aloqa o'rnatib, bu aloqa orqali maxfiy kalit yordamida shifrlangan xabar jo'natmoqchi. **A** ishtirokchi X_A ning bir martalik maxfiy qiymatini generasiya qilib, Y_A ning qiymatini hisoblaydi va uni **V** ishtirokchiga yuboradi. Bunga javoban **V** ishtirokchi X_V ning maxfiy qiymatini generasiya qiladi va Y_V ni hisoblab, uni **A** ishtirokchiga yuboradi. Ikkala ishtirokchi ham umumiy maxfiy kalitni hisoblab topadi. Bunda modul va uni birga aylantiruvchi ildiz qiymati avvaldan ma'lum bo'lishi kerak. Shuningdek, **A** ishtirokchi ularni hohlagancha tanlab birinchi xabarida jo'natishi ham mumkin.

Diffi-Xellman sxemasini lokal tarmoqning bir guruh ishtirokchilari uchun qo'llash mumkin. Bunda har bir ishtirokchi X ning maxfiy qiymatini generasiya qilishi va unga mos Y ning ochiq qiymatini hisoblab topishi

kerak. Bu usulda topilgan barcha ochiq qiymatlar, modul hamda modulning birga aylantiruvchi ildiz qiymati markazlashgan biron bir katalogda saqlanadi. Ixtiyoriy vaqtda **V** ishtirokchi **A** ishtirokchining ochiq qiymatlaridan foydalanib, umumiy maxfiy kalitni hisoblashi va undan **A** ishtirokchi bilan shifrlangan xabar almashinuvida foydalanishi mumkin.

Agar markazlashgan katalog ishonchli bo'lsa, u holda bunday aloqa usuli konfidensiallikni va qandaydir bir miqdorda autentifikasiyani ham ta'minlaydi. Faqatgina **A** va **V** ishtirokchilarga kalit ma'lum bo'lgani uchun boshqa ishtirokchilar xabarni o'qiy olishmaydi, bu esa axborotning konfidensialligini ta'minlaydi. **A** ishtirokchi faqat **V** ishtirokchigina bu kalitdan foydalanib xabar yuborishi mumkinligini biladi, bu esa autentifikasiyani ta'minlaydi.

Quyida bundan buyon protokollar bayonida kerak bo'ladigan bir qancha belgilashlarni keltiramiz.

Ishtirokchilar/administrator: A,B,S. Maxfiy xabar almashinuvida ikki kishi qatnashayapti deb faraz qilamiz: **A** ishtirokchi va **V** ishtirokchi. Ular IMning xizmatiga murojaat qiladi, IMni S bilan belgilaymiz.

Uzoq muddatli maxfiy kalitlar: k_{ab},k_{bs},k_{as}. k_{ab} faqat **A** va **V** ishtirokchilarga ma'lum bo'lgan kalit.

Sonli qo'shimchalar: n_a,n_b. Bular tasodifiy bir martali sonlar bo'lib, protokolning har bir xabari uchun yagona bo'ladi. n_a son **A** ishtirokchi tomonida hosil qilingan sonli qo'shimcha.

Vaqt belgisi: t_a,t_b,t_s. VB bo'lgan t_a kattalik **A** ishtirokchi tomonidan hosil qilingan. VBni ishlatayotganda ishtirokchilar boshqa protokol yordamida vaqtning sinxronligini ta'minlashi kerak.

Quyidagi yozuv

$$A \rightarrow B: M,A,B,\{n_a,m,a,b\}_{k_{as}}$$

A ishtirokchi **V** ishtirokchiga quyidagilarni o'z ichiga olgan xabar yuboradi:

– son qo'shimchasi M,

– xabar jo'natuvchining ismi A,

– xabar qabul qiluvchining ismi V,

– k_{as} kalit yordamida shifrlangan xabar matni $\{n_a,m,a,b\}$.

V ishtirokchi esa bu xabarning shifrlangan qismini o'qiy olmaydi.

Endi protokollarning bayonini keltiramiz. Faraz qilaylik **A** va **V** ishtirokchilar ishonch markazi bilan k_{as} va k_{bs} kalitlardan foydalanib bog'lanishadi, protokol ishining natijasida ular o'zaro ma'lumot almashishadi.

3.3.2. Hughes protokoli

Hughes algoritmi Diffi-Xellman algoritmining o'zgartirilgan varianti hisoblanadi [11-12]. Hughes algoritmi quyidagi tartibda amalga oshiriladi (3.16-rasm) :

(1) **A** ishtirokchi katta tub son x ni generasiya qiladi va quyidagini hisoblaydi:

$$k = g^x \bmod n$$

(2) **V** ishtirokchi katta tub son **y** ni generasiya qiladi va quyidagini hisoblab, uni **A** ishtirokchiga jo'natadi:

$$Y = g^y \bmod n$$

(3) **A** ishtirokchi **V** ishtirokchiga quyidagini jo'natadi:

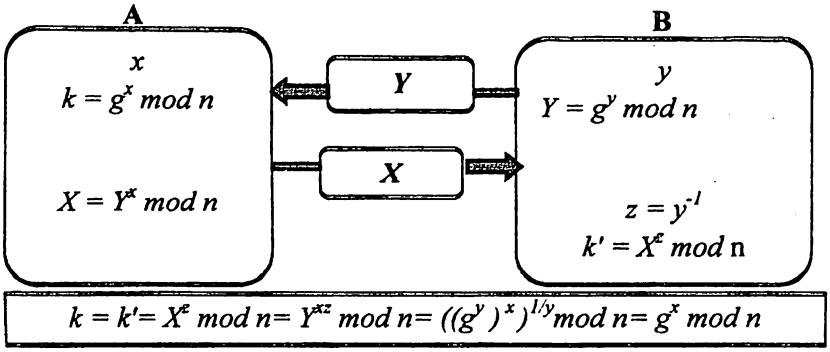
$$X = Y^x \bmod n$$

(4) **V** ishtirokchi hisoblaydi:

$$z = y^{-1}$$

$$k' = X^z \bmod n$$

Agar hammasi to'g'ri bajarilgan bo'lsa, $k = k'$ bo'ladi.



3.16- rasm. Hughes protokoli

Hughes protokolining Diffi-Xellman protokolidan afzalligi shundaki, k maxfiy seans kalitini bog'lanish bo'lmasdan avval hisoblab

qo'yish mumkin va bu orqali **A** ishtirokchi ma'lumotlarni bu kalit orqali shifrlab qo'yish mumkin bo'ladi, ya'ni **V** ishtirokchi bilan bog'lanmasdan turib amalga oshirishi mumkin.

U shifrlangan ma'lumotni bir vaqtning o'zida bir necha kishiga jo'natishi mumkin, kalitni esa keyinroq har biriga alohida – alohida jo'natishi mumkin.

3.3.3. Katta halqumli qurbaqa protokoli

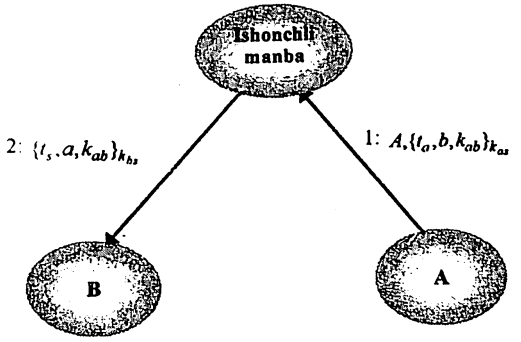
Birinchi protokol bu Barrouz tomonidan taklif etilgan katta halqumli (Wide-Mouth Frog) qurbaqa protokolidir [10-12]. Protokol **A** ishtirokchi **V** ishtirokchiga S vositachi orqali faqat ikkita ma'lumotlardan foydalanib k_{ab} kalitni yuboradi, lekin bu protokolning kamchiliklari bor. Xususan, uni amalga oshirishda vaqtni sinxronlashtirish kerak bo'ladi, bu esa o'z navbatida qo'shimcha muammolarni keltirib chiqaradi.

A ishtirokchi seans kalitini k_{ab} tanlaydi va uni **V** ishtirokchiga yuboradi. Bu degani **V** ishtirokchi **A** ishtirokchining puxta (turg'un) kalit yarata olishiga va uni maxfiy saqlay olishiga ishonadi. Bunday kuchli talab bu protokolning amaliyotda kam qo'llanilishining asosiy sababi bo'lib hisoblanadi. Endi protokolning o'zi ko'rib chiqiladi.

Protokol ikkita ma'lumot almashinuvidan iborat bo'ladi (3.17-rasm):

$$A \to S: A, \{t_a, b, k_{ab}\}_{k_{as}},$$

$$S \to B: \{t_s, a, k_{ab}\}_{k_{bs}}.$$



3.17- rasm. Katta halqumli qurbaqa protokoli

Birinchi xabarni olib ishonchli S manba uning oxirigi qismi shifrini ochadi va VB joriy vaqtga yaqinligini tekshiradi. Shifrning ochilgan qismi S ga k_{ab} kalitni V ishtirokchiga yuborish kerakligini xabarlaydi. Agar VB yaqindagi vaqtga mos kelsa, S talab etilayotgan kalitni o'zining VB bilan birga shifrlaydi va shifrmatnni V ishtirokchiga yuboradi. V ishtirokchi S dan ma'lumot olganidan so'ng uning shifrini ochadi va VBning yangiligini tekshiradi. So'ngra u k_{ab} kalitni va unga shifrlangan xabar yubormoqchi bo'layotgan A ishtirokchining nomini o'qiydi.

VBning aniqligi seans kaliti yaqinda yaratilganini bildiradi. Lekin A ishtirokchi bu kalitni avval generasiya qilib, keyin qattiq diskda saqlagan bo'lishi va undan buzg'unchi nusxa olgan bo'lishi mumkin.

Yuqorida ta'kidlaganimizdek, bu protokol barcha ishtirokchilarning vaqtini sinxronizasiya qilingandagina to'g'ri ishlaydi. Ammo bu uncha katta murakkablik tug'dirmaydi, chunki ishonchli shaxs protokolda ishlatiladigan barcha vaqt belgilarini tekshirib, generasiya qilib turadi. Shuning uchun boshqa ishtirokchilar o'zlarining soatlari va ishonchli shaxsning soati ko'rsatishi orasidagi farqni yozib olishlari kerak. Bunda protokol agar bu ishtirokchilardan birortasining soati tezroq yoki sekinroq ishlagandagina yoki soat ko'rsatishi majburan o'zgartirilgandagina noto'g'ri ishlaydi.

3.3.4. MTI protokoli

MTI protokolining nomi uning mualliflari hisoblangan *T. Masumoto I. Takashima va X. Imailar* sharafiga qo'yilgan. Bu protokol ham Diffi-Xellman protokoliga o'xshash bo'lib, uning kriptobardoshliligi chekli maydonda diskret logarifmlashga asoslangan [14, 20]. Biroq undan farqli tomoni shundaki, MTI protokolida kriptobardoshlilikni oshirish maqsadida qo'shimcha a va b o'zgaruvchilardan foydalaniladi. Ushbu protokolning amallar ketma-ketligi quyidagicha bajariladi. Eng avvalo A va V ishtirokchilar katta tub son p va uning primitiv ildizi α ning qiymati haqida kelishib oladilar (3.18-rasm).

A ishtirokchi o'z maxfiy kaliti a, $1 \le a \le p-2$ ni generasiya qiladi va bu kalit yordamida

$$z_A = \alpha^a \bmod p$$

ifodani hisoblaydi. A ishtirokchi hosil bo'lgan qiymatni V ishtirokchiga uzatadi:

$$A \rightarrow V:\ z_A = \alpha^a \bmod p,$$

V ishtirokchi bu ma'lumotni qabul qiladi. U o'zining yopiq kaliti b, $1 \le b \le p-2$ ni generasiya qiladi. Bu yopiq kalit yordamida

$$z_B = \alpha^b \bmod p$$

ifodani hisoblaydi va natijani A ishtirokchiga uzatadi:

$$V \rightarrow A:\ z_B = \alpha^b \bmod p.$$

A ishtirokchi z_B ni qabul qiladi. A va V ishtirokchilar umumiy maxfiy kalitni generasiya qilish uchun mos holda o'zlarining x, $1 \le x \le p-2$ va y, $1 \le y \le p-2$ tasodifiy sonlarini generasiya qilishlari zarur. A ishtirokchi o'zining tasodifiy x sonini generasiya qilib,

$$\alpha^x \bmod p$$

ifodani hisoblaydi va uni V ishtirokchiga uzatadi:

$$A \rightarrow V:\ \alpha^x \bmod p.$$

V ishtirokchi bu ma'lumotni qabul qiladi. U o'zining tasodifiy y sonini generasiya qilib, $\alpha^y \bmod p$ ifodani hisoblaydi. Hosil bo'lgan natijani A ishtirokchiga uzatadi. Shu vaqtdan boshlab, V ishtirokchi α^x va z_A ma'lumotlarga ega. Endi u o'zining tasodifiy soni va yopiq kalitidan foydalanib quyidagi ifodani hisoblaydi:

$$k = (\alpha^x)^b \cdot z_A^y,$$

$$V \rightarrow A:\ \alpha^y \bmod p.$$

A ishtirokchi bu ma'lumotni qabul qiladi. Endi A ishtirokchi α^y va z_B ma'lumotlarga ega. U o'zining tasodifiy soni va yopiq kalitidan foydalanib ushbu ifodani hisoblaydi: $k = (\alpha^y)^a \cdot z_B^x$.

Natijaviy kalitning umumiy ko'rinishi esa quyidagicha:

$$k = (\alpha^y)^a \cdot z_B^x = (\alpha^x)^b \cdot z_A^y = \alpha^{xb+ya} \bmod p.$$

MTI protokoli shu tartibda amalga oshiriladi. Unda kriptotahlilchining ixtiyoriy almashtirishi tomonlardagi kalitning qiymati turlicha bo'lishiga olib keladi. Bu esa uzatilayotgan ma'lumotni o'qish imkoniyatini butunlay yo'qotadi.

Quyida MTI protokoli uchun ham misol keltiriladi.

$p = 9531$

$\alpha = 1647$

A: $a = 126$

$A: Z_a = \alpha^a \bmod p = 1647^{126} \bmod 9531 = 3375$

$A \rightarrow B: Z_a = 3375$

$B: b = 98$

$B: Z_B = \alpha^b \bmod p = 1647^{98} \bmod 9531 = 8775$

$B \rightarrow A: Z_B = 8775$

$A: x = 8643$

$A: X = \alpha^x \bmod p = 1647^{8643} \bmod 9531 = 972$

$A \rightarrow B: X = 972$

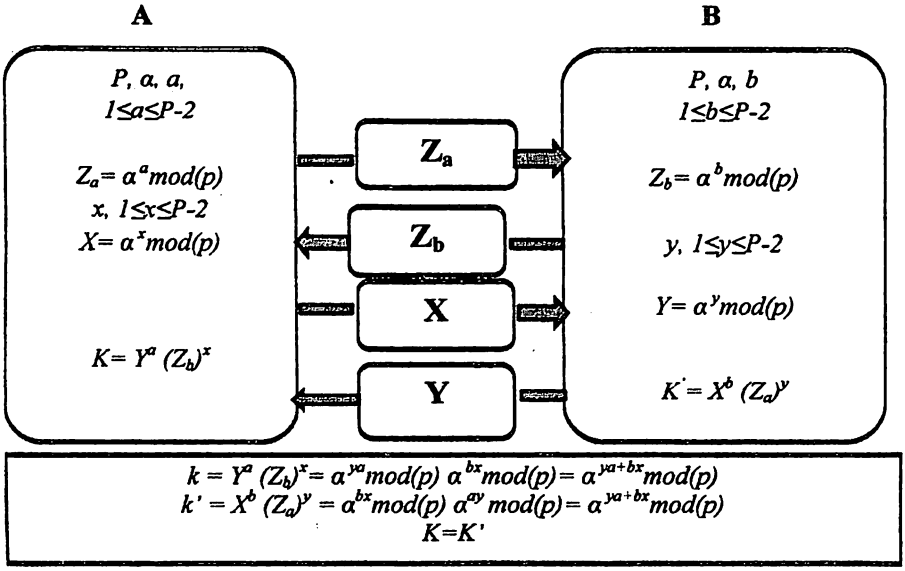
$B: k_1 = (\alpha^x)^b Z_A^y \bmod p = X^b Z_A^y \bmod p = 972^{98} \cdot 3375^{6983} \bmod 9531 = 3564$

$B: y = 6983$

$B: Y = \alpha^y \bmod p = 1647^{6983} \bmod 9531 = 4131$

$B \rightarrow A: Y = 4131$

javob: $k_1 = k_2 = k = 3564$.



3.18- rasm. MTI protokoli

3.3.5. DASS protokoli

DASS protokoli kalit taqsimoti va autentifikasiyasining IM ishtirokidagi simmetrik va nosimmetrik algoritmlarga asoslangan protokoldir [10-12]. Bunda **A** va **V** ishtirokchilar hamda IM S o'zlarining ochiq va yopiq kalitlari juftiga egalar, ya'ni k_a, k_b, k_s o'zaro mos holatda. Bu kalitlar bilan mos ravishda xabarlarni imzolash s_a, s_b, s_S.

DASS protokoli sxemasini keltiramiz (3.19-rasm):

$A \rightarrow S : B,$

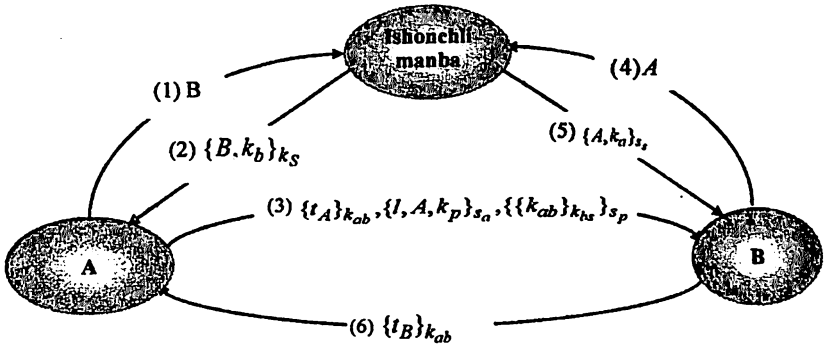
$S \rightarrow A : \{B, k_b\}_{k_s},$

$A \rightarrow B : \{t_A\}_{k_{ab}}, \{l, A, k_p\}_{s_a}, \{\{k_{ab}\}_{k_{bs}}\}_{s_p},$

$B \rightarrow S : A,$

$S \rightarrow B : \{A, k_a\}_{s_s},$

$B \rightarrow A : \{t_B\}_{k_{ab}}.$



3.19- rasm. DASS protokoli

Endi DASS protokolining to'liq bayonini keltiramiz:

– A ishtirokchi IMga **V** ishtirokchining ochiq kalitini olish uchun so'rovnoma yuboradi.

– IM V ishtirokchining kaliti $k_b$ni o'zining kaliti bilan imzolab uzatadi.

– **A** ishtirokchi ma'lumotlarni IMning avvaldan ma'lum bo'lgan ochiq kaliti bilan tekshiradi, so'ngra seans kaliti k_{ab} ni va tasodifiy seans

katiti k_p ni generasiya qiladi, VB t_a ni va kalitning yaroqlilik muddati l ni qo'shib, bir qismini shifrlab, bir qismini imzolab V ishtirokchiga yuboradi.

– V ishtirokchi IMga A ishtirokchining identifikatorini olish uchun so'rovnoma yuboradi.

– IM V ishtirokchining kalitini o'zining kaliti bilan imzolab yuboradi.

– A ishtirokchining va IMning xabarlaridagi ma'lumotlardan foydalanib, V ishtirokchi A ishtirokchining imzosini tekshiradi, tasodifiy seans kaliti k_p ni, seans kaliti k_{ab} ni chiqarib oladi va t_A ning shifrini ochib takrorlanganidan emas, balki shu vaqtdagi xabardan foydalanilayotganiga ishonch hosil qiladi.

– Zaruratga ko'ra protokol tomonlarni o'zaro identifikasiyasini ta'minlash maqsadida davom ettirilishi mumkin.

3.3.6. Denning – Sakko protokoli

Denning–Sakko protokoli oshkora kalitli autentifikasiyalash va kalit taqsimlash protokoli bo'lib, DASS protokolidagi kabi IM barcha ochiq kalitlarning ma'lumotlar bazasini tutib turadi [10-12].

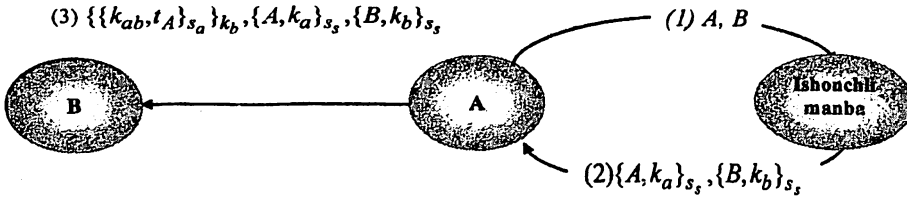
Denning–Sakko protokolining zaifligi shundan iboratki, tomonlardan biri seans tugagandan so'ng o'zini boshqa tomondan deb ko'rsatish imkoniyatiga ega.

Denning– Sakko protokolining sxemasi (3.20-rasm) :

$A \rightarrow S : A, B,$

$S \rightarrow A : \{A, k_a\}_{s_s}, \{B, k_b\}_{s_s},$

$A \rightarrow B : \{\{k_{ab}, t_A\}_{s_a}\}_{k_b}, \{A, k_a\}_{s_s}, \{B, k_b\}_{s_s},$



3.20- rasm. Denning – Sakko protokoli

– A ishtirokchi IMga o'zining va V ishtirokchining identifikatorini yuboradi.

– IM A ishtirokchiga o'zining maxfiy kaliti bilan imzolagan A va V ishtirokchilarning ochiq kalitlarini va identifikatorlarini uzatadi.

– A ishtirokchi seans kaliti va VBni o'zining kaliti bilan imzolab, so'ngra uni V ishtirokchining ochiq kaliti bilan shifrlab va IMning xabari bilan to'ldirib V ishtirokchiga yuboradi.

– V ishtirokchi xabarni shifrini ochib, IMning ochiq kalitidan foydalanib kalitlardagi imzoni tekshiradi, A ishtirokchining ochiq kalitidan foydalanib seans kalitidagi imzoni tekshiradi, bunda seans kaliti k_{ab} dan A ishtirokchi bilan xavfsiz ma'lumot almashinuvida foydalanishi mumkin bo'ladi.

A ishtirokchidan kelgan xabarda $\{\{k_{ab}, t_A\}_{s_a}\}_{k_b}$ oluvchining identifikatori qatnashmasligi, V ishtirokchiga A ishtirokchidan olgan ma'lumotlarni boshqa ishtirokchi bilan bo'ladigan yangi seansda o'zini A ishtirokchi deb ko'rsatishi imkonini beradi. Bu muammoni xabarga A va V ishtirokchilarning identifikatorini qo'shib, ya'ni bu xabarni ishlatilishini faqat shu seans bilan chegaralab oson hal qilish mumkin.

3.3.7. Vu – Lama protokoli

Vu – Lama protokoli ham Denning – Sakko protokoli kabi oshkora kalitli autentifikasiyalash va kalit taqsimlash protokoli bo'lib [10-12], DASS protokolidagi kabi IM barcha ochiq kalitlarning ma'lumotlar bazasini saqlab turadi.

Vu – Lama protokoli sxemasi 3.21-rasmda keltirilgan:

$A \rightarrow S: A, B,$

$S \rightarrow A: \{k_b\}_{s_s},$

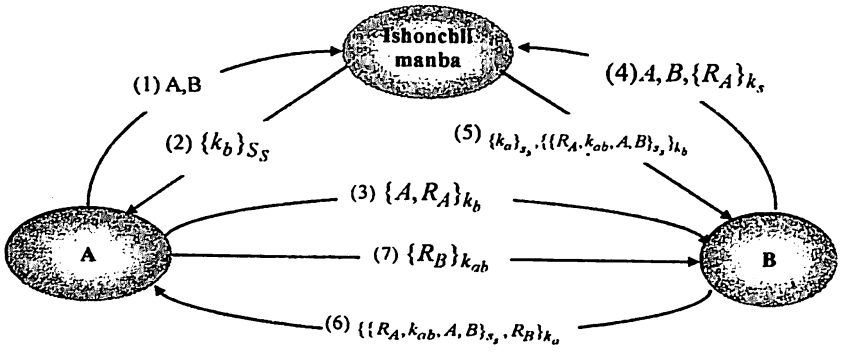
$A \rightarrow B: \{A, R_A\}_{k_b},$

$B \rightarrow S: A, B, \{R_A\}_{k_s},$

$S \rightarrow B: \{k_a\}_{s_s}, \{\{R_A, k_{ab}, A, B\}_{s_s}\}_{k_b},$

$B \rightarrow A: \{\{R_A, k_{ab}, A, B\}_{s_s}, R_B\}_{k_a},$

$A \rightarrow B: \{R_B\}_{k_{ab}}.$



3.21- rasm. Vu – Lama protokoli

Quyida Vu – Lama protokolining to'liq bayoni keltiriladi:

– **A** ishtirokchi IMga o'zining va **V** ishtirokchining identifikatorini yuboradi.

– IM **A** ishtirokchiga o'zining maxfiy kaliti bilan imzolagan **V** ishtirokchining ochiq kalitlarini uzatadi.

– **A** ishtirokchi imzoni tekshiradi, so'ngra **V** ishtirokchiga o'zining identifikatori va tasodifiy tanlangan sonni **V** ishtirokchining ochiq kaliti bilan shifrlab yuboradi.

– **V** ishtirokchi esa IMga o'zining va **A** ishtirokchining identifikatorini va tasodifiy tanlangan sonni IMning ochiq kaliti bilan shifrlab uzatadi.

– IM **V** ishtirokchiga ikkita xabar yuboradi. Birinchisida **A** ishtirokchining IMning kaliti yordamida imzolangan ochiq kaliti bo'lsa, ikkinchisida IM kaliti bilan imzolangan va **V** ishtirokchining ochiq kaliti bilan shifrlangan **A** ishtirokchining tasodifiy tanlagan soni, tasodifiy tanlangan seans kaliti va **A** va **V** ishtirokchilarning identifikatori bo'ladi.

– **V** ishtirokchi IM ochiq kaliti yordamida xabarning haqiqiyligini tekshiradi, so'ngra **A** ishtirokchiga IM xabarining ikkinchi qismini, uning imzosi hamda o'zining tasodifiy tanlagan soni bilan to'ldirib, so'ng **A** ishtirokchining ochiq kaliti bilan shifrlab yuboradi.

– **A** ishtirokchi IM imzosini va o'zining tasodifiy tanlagan sonining tengligini tekshiradi, so'ngra **V** ishtirokchiga **V** tasodifiy tanlagan sonni uning seans kaliti bilan shifrlab qayta yuboradi.

– V ishtirokchi sonning shifrini ochib uning o'zgarmaganligiga ishonch hosil qiladi.

3.3.8. EEChlarga asoslangan kalitlarni taqsimlash algoritmlari va protokollari

Elliptik egri chiziqlar

Ko'plab oshkora kalitli kriptografik mahsulotlar va standartlar deyarli an'anaviy mavqyega erishgan RSA va El Gamal algoritmlariga asoslangan [21-23]. So'nggi vaqtlarda kriptotahlil usullarining va hisoblash texnikasining keskin rivojlanishi tizimlarning ishonchli himoyasi uchun kalit bitlari sonining ham katta bo'lishiga olib keldi, bu esa an'anaviy tizimlarni qo'llovchi tizimlar ilovasini yuklanish vaqtining ortishiga olib keldi. Bu o'z navbatida katta tranzaksiyalarni himoyalash talab etiladigan, elektron tijoratga ixtisoslashgan aloqa tugunlarida ko'plab muammolarni keltirib chiqardi. Shu bois an'anaviy mavqyega erishgan tizimlarga raqib – EEChlarga asoslangan kriptografiya vujudga keldi [20. 25-26].

EEChlarga asoslangan kriptografik tizimlarning an'anaviy tizimlarga nisbatan afzalligi shundaki, ularda foydalaniladigan kalit uzunligi razryadi kichik bo'lganda ham, ekvivalent himoya bilan ta'minlashidadir. Bu esa qabul qiluvchi va uzatuvchi moslama prosessorlarining yuklanish vaqtini kamaytiradi.

EECh xossalari. EEChlar quyidagi ko'rinishdagi tenglamalar yordamida beriladi:

$$y^2 + axy+by=x^3+cx^2+dx+g,$$

bunda *a, b, c, d* butun sonlar.

EECh *O* deb belgilangan maxsus bo'lmagan (cheksizlikdagi nuqta, nol element) elementni o'z ichiga oladi.

EECh ta'rifidan agar uchta nuqta bir to'g'ri chiziqda yotsa, ularning yig'indisi *O* ekanligi kelib chiqadi. Bu ta'rifdan EECh nuqtalarining qo'shishni quyidagi qoidalari kelib chiqadi:

1. Qo'shishda *O* nol elementi sifatida qatnashadi, ya'ni $O=-O$ bo'lib, EEChning ixtiyoriy nuqtasi uchun $R+O=R$.

2. Vertikal chiziq EEChni bir xil *x* absissali ikkita nuqtada kesib o'tadi. Bu chiziq egri chiziqni cheksizlik nuqtasida ham kesib o'tadi. Shuning uchun $P_1+P_2+O=O$ va $P_1=-P_2$, bunda $P_1=(x,y)$, $P_2=(x,-y)$.

"Manfiy" ishorali nuqta bu x koordinatasi xuddi o'sha qiymatga, u koordinatasi esa ishorasi bo'yicha qarama-qarshi qiymatga ega bo'lgan nuqtadir.

3. Turli x koordinatali Q va R nuqtalarni qo'shish uchun, bu ikki nuqta orqali to'g'ri chiziq o'tkaziladi va bu to'g'ri chiziqning EECh bilan kesishgan uchinchi nuqtasi P_1 topiladi. Agar bu nuqtalarning birortasida to'g'ri chiziq EEChqa urinma bo'lmaydigan bo'lsa, u holda bu to'g'ri chiziqning EECh bilan faqat bitta kesishish nuqtasi topiladi. Bunda $Q+R=-P_1$.

4. Q nuqtani ikkilantirish uchun Q nuqtadan urinma o'tkazish kerak va boshqa S kesishish nuqtasini topish kerak. Bunda $Q+Q=2Q=-S$.

Qo'shishning yuqorida keltirilgan xossalari qo'shishning barcha oddiy xossalariga, masalan, kommutativlik va assosiativlik qonunlariga bo'ysunadi. EEChning R nuqtasini k songa ko'paytirish R nuqtaning k ta nusxasining yig'indisi shaklida aniqlangan. $2P=P+P$, $3P=P+P+P$ va hokazo.

r - tub sonli modul bo'yicha elliptik gruppa kriptografiyada alohida qiziqish kasb etadi. Bunday gruppa quyidagicha aniqlanadi. Ikkita manfiy bo'lmagan va p dan kichik bo'lgan butun a va b sonlarni tanlaymiz, bunda

$$4a^3+27b^2 \bmod p \neq 0$$

shart bajarilsin, u holda $E_p(a,b)$ r modul bo'yicha elliptik gruppani bildiradi. Bu gruppaning elementlari manfiy bo'lmagan r dan kichik (x,u) sonlar juftligi bo'lib, cheksizlikdagi O nuqta bilan $y^2 \equiv (x^3+ax+b)(\bmod p)$ shartni qanoatlantiradi.

Elliptik gruppa uchun $(0,0)$ dan (r,r) gacha bo'lgan, kvadrati manfiy son bo'lmagan r modul bo'yicha tenglamani qanoatlantiradigan faqat butun qiymatlar qaraladi.

EEChda nuqtani topish quyidagi algoritm yordamida amalga oshiriladi:

1. x ning $0 \le x < p$ shartni qanoatlantiruvchi har bir qiymati uchun $(x^3+ax+b) \bmod p$ hisoblanadi.

2. Avvalgi qadamda hosil qilingan har bir qiymat uchun bu qiymatning r modul bo'yicha kvadrat ildizi mavjudligi tekshiriladi. Agar kvadrat ildiz mavjud bo'lmasa, u holda $E_p(a,b)$ to'plamda x ning bu qiymatiga mos nuqta mavjud emas. Agar ildiz mavjud bo'lsa, u holda u

ildizdan chiqarishga mos keluvchi (nol bo'lmagan holda) ikkita qiymatga ega bo'ladi. (x,u) ning bu qiymatlari $E_p(a,b)$ ning nuqtalari bo'ladi.

$E_p(a,b)$ da qo'shish qoidasini geometrik formulalarga mos holda quyidagicha yozish mumkin:

1. $P+O=P$.

2. Agar $P=(x,y)$ bo'lsa, u holda $P+(x,-y)=O$. $(x,-u)$ nuqta R nuqtaning manfiy qiymati deyiladi va $(-R)$ kabi belgilanadi. $(x,-u)$ nuqta EEChda yotadi va demak, $E_p(a,b)$ ga tegishli bo'ladi.

3. Agar $P=(x_1,y_1)$ va $Q=(x_2,y_2)$ bo'lsa, bunda $P\neq Q$, u holda $P+Q=(x_3,y_3)$ quyidagi qoidalar asosida aniqlanadi:

$$x_3\equiv(\lambda^2-x_1-x_2)\bmod p,$$

$$y_3\equiv(\lambda\,(x_1-x_2)-y_1)\bmod p,$$

bunda

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}\Rightarrow P\neq Q\\[2ex]\dfrac{3x_1^2+a}{2y_1}\Rightarrow P=Q\end{cases}.$$

EECh nuqtalari qo'shish amaliga nisbatan kommutativ va assosiativ, ya'ni nuqtalar to'plami cheksizlik nuqtasi O bilan birga abel gruppasini tashkil qiladi.

3.3.9. EEChlarga asoslangan kalitlar taqsimotida

Diffi- Xellman sxemasi analogi

Kalit taqsimotining EEChlardagi analogi quyidagi ko'rinishda bo'ladi: avval katta tub r son va EECh uchun a, b parametrlar tanlanadi [20, 25-26]. Bu elliptik nuqtalar guruhi $Ye_r(a, b)$ ni beradi. So'ngra $Ye_r(a, b)$ da generasiyalovchi nuqta $G=(x,y)$ tanlanadi. G ni tanlaganda $nG=0$ shartni qanoatlantiruvchi n ning eng kichik qiymati juda ham katta tub son bo'lishi muhim. Kriptotizimning G va $Ye_r(a, b)$ parametrlari barcha ishtirokchilarga ma'lum parametr hisoblanadi.

A va **V** ishtirokchilar orasidagi kalit taqsimoti quyidagi sxema bo'yicha amalga oshiriladi:

1. **A** ishtirokchi butun $n_A< n$ sonni tanlaydi. Bu son **A** ishtirokchining maxfiy kaliti bo'ladi. So'ngra **A** ishtirokchi ochiq kaliti

$R_A = G \times n_A$ generasiya qiladi. Ochiq kalit $Ye_r(a, b)$ ga tegishli nuqta bo'ladi.

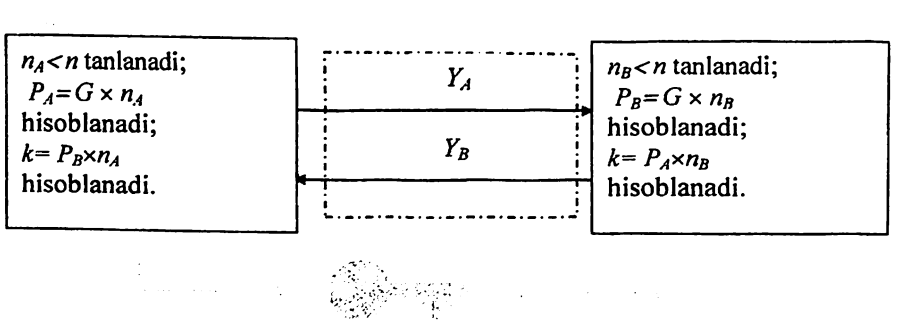
2. **V** ishtirokchi ham xuddi shunday n_V maxfiy kalitni tanlaydi va $R_V = G \times n_V$ ochiq kalitni hisoblaydi.

3. **A** ishtirokchi $k = R_V \times n_A$ maxfiy kalitni, **V** ishtirokchi esa $k = R_A \times n_V$ maxfiy kalitni generasiya qiladi.

3-qadamdagi ikkala formula ham bir xil qiymatni beradi

$$R_V \times n_A = (G \times n_V) \times n_A = (G \times n_A) \times n_V = R_A \times n_V.$$

Bu sxemani buzishi uchun buzg'unchi G va G k ning qiymatlaridan k ni hisoblab topishi kerak bo'ladi (3.22-rasm). Bu esa qiyin yechiladigan masala hisoblanadi.



3.22- rasm. EEChlarga asoslangan Diffi- Xellman sxemasining analogi

Modul $r=211$ va elliptik nuqtalar to'plami $Ye_{211}(0,-4)$ ni tanlaymiz. Ularga mos keluvchi EECh $u^2=x^3-4$ va $G=(2,2)$. Hisoblashlar $241\ G=0$ ekanini ko'rsatadi. **A** ishtirokchining maxfiy kaliti $n_A = 121$ bo'lsin, u holda **A** ishtirokchining ochiq kaliti $P_A = 121(2,2) = (115,48)$ bo'ladi. **V** ishtirokchining maxfiy kaliti $n_B = 203$ bo'lsin, u holda **V** ishtirokchining ochiq kaliti $P_B = 203(2,2) = (130,203)$ bo'ladi. U holda umumiy maxfiy kalit $121(130,203)=203(115,48)=(161,169)$ bo'ladi.

EEChlarga asoslangan kriptografiyada maxfiy kalit sifatida sonlar juftligi qaraladi. Agar bu kalitdan an'anaviy shifrlashda foydalanilmoqchi bo'lsa, u holda bu ikkita sondan mos bitta qiymat generasiya qilinadi. Yoki bo'lmasa x yoki u koordinatalardan birini ishlatish mumkin.

3.3.10. Messi – Omur sxemasi bo'yicha kalit taqsimlash protokoli

Faraz qilaylik *Ye - n* tartibli EECh, *ye* esa $(ye, n)=1$, $1<ye<n$ shartni qanoatlantiruvchi son. Invertlash algoritmidan foydalanib $d \equiv e^{-1} \bmod n$ ni topamiz. Butun sonlar ustidagi modul arifmetikasi qonunlari bilan EECh nuqtalari ustidagi modul arifmetikasi qonunlari bir xil bo'lgani uchun, EEChning ixtiyoriy R nuqtasini quyidagi formulalar yordamida hisoblash mumkin:

$$Q = eP,$$

$$R = dQ.$$

Messi – Omur protokoli EEChning berilgan nuqtasini bazaviy nuqtaga nisbatan skalyar ko'paytuvchisini aniqlash muammosining yechilishiga, ya'ni EEChlarda diskret logarifm masalasini yechishga asoslangan [10-12].

A va **V** ishtirokchilar orasida kalit taqsimotini quyidagi sxema yordamida amalga oshiriladi (3.23-rasm):

1. **A** ishtirokchi $e_A < n$ butun sonni tanlaydi va $d_A \equiv e^{-1}{}_A \bmod n$ ni hisoblaydi. e_A son **A** ishtirokchining maxfiy kaliti bo'ladi. d_A esa **A** ishtirokchining shaxsiy shifrni ochish kaliti bo'ladi. So'ngra **A** ishtirokchi o'zining m xabarini P_m EEChning biror nuqtasiga joylashtiradi va o'zining maxfiy e_A ga ko'paytirib, (ochiq kalit generasiya qiladi): ya'ni

$P_A = e_A P_m$ nuqtani hosil qiladi.

2. **V** ishtirokchi ham o'zi uchun xuddi shunday shaxsiy shifrlash va shifrni ochish kalitlari e_B va d_B kalitlarni hosil qiladi. So'ngra **V** ishtirokchi o'zining maxfiy kaliti qiymatini **A** ishtirokchining oshkora P_A kalitiga ko'paytirib (oshkora kalitni generasiya qiladi): ya'ni

$$P_B = e_B P_A$$

nuqtani hqsil qiladi.

3. Bu qiymatni **A** ishtirokchiga jo'natadi.
4. **A** ishtirokchi

$P_O = d_A P_B$ ni hisoblaydi.

5. Hisoblab topilgan qiymatni **V** ishtirokchiga yuboradi.
6. **V** ishtirokchi yuborilgan qiymatni o'zining maxfiy shifrni ochish kalitiga d_B ko'paytirib, **A** ishtirokchining m xabariga mos P_m nuqtani topadi:

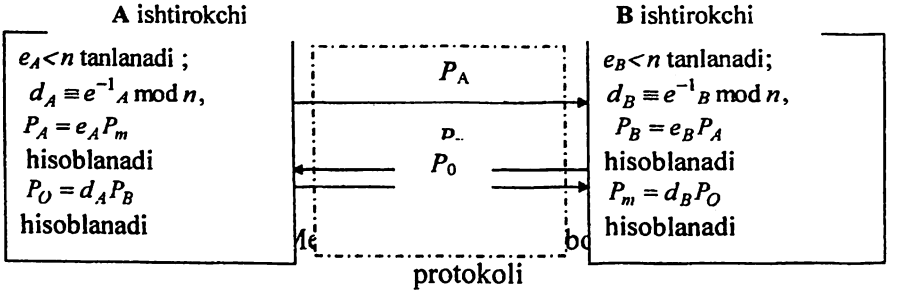
$$P_m = d_B P_O .$$

P_O ni hisoblab **A** ishtirokchi o'zining shifrlash kalitining faoliyatini bartaraf qiladi:

$$P_O = d_A P_B = d_A(e_B P_A) = d_A(e_B(e_A P_m)) = e_B(d_A(e_A P_m)) = e_B P_m .$$

Demak, **V** ishtirokchi quyidagini oladi:

$$d_B P_O = d_B(d_A P_m) = P_m$$



m xabar an'anaviy kriptotizimlar uchun kalit o'rnida ishlatilishi mumkin. Bu holda EEChning o'zidan boshqa protokol parametrlari to'g'risida hyech qanday axborotni e'lon qilish talab etilmaydi. Buning evaziga ochiq kanal bo'ylab uch marta uzatish amalga oshiriladi.

3.3.11. Menezes-Kyu-Vanstonning kalit taqsimlash sxemasi

Menezes-Kyu-Vanstonning kalit taqsimlash sxemasi, ya'ni -*MQV* - protokoli avval keltirilganlaridan farq qiladi [12, 18]. Avvalgi keltirilgan protokollar "vositachi" hujumidan himoyalanmagan edi. Vositachi deganda, **A** va **V** ishtirokchilarning ochiq aloqa kanalini boshidan boshqarib turuvchi va ularning normal muloqotiga halaqit beruvchi kriptotahlilchi nazarda tutiladi. Vositachi ochiq kanal orqali o'tuvchi

xabarlarni tutib qolish, **A** va **V** ishtirokchilarga o'zining xabarlarini yuborish, qonuniy ishtirokchilarda ularning har biri vositachi bilan bevosita muloqot qilayotgan bo'lsada, protokolning normal ishlayotgan taassurotini hosil qilish imkoniyatiga ega.

Faol kriptotahlilchining faoliyatini yo'qotish uchun masalan, Messi-Omur protokolida qisqa muddatli $e_A P$, $e_B P$ kalitlarning autentifikasiyasi zarur. Buning uchun $d_A P$ va $d_B P$ kalitlarni ochiq e'lon qilishdan foydalaniladi. Bunda begona shaxs diskret logariflash masalasi qiyin yechiladigan muammo bo'lgani sababli vositachi bo'la olmaydi. Protokolda qisqa muddatli ochiq kalit uzoq muddatlisi bilan funksional bog'langan holda tashkil etiladi, bu esa uchinchi shaxsning ikkita ishtirokchi orasida vositachi bo'lishining oldini oladi. Maqsadiga erishish uchun vositachi ham qisqa vaqtli ham uzoq vaqtli kalitlarning uzatilish jarayoniga suqilib kirishi, **A** va **V** ishtirokchilar orasida uzatilgan uzoq muddatli kalitlarning to'g'riligini tekshirishga mone'lik qilishi zarur.

Bu protokolning matematik asosini modul arifmetikasi asosida, tatbiq qilish jarayonini EECh nuqtalari qismgruppasining siklik xossasiga asoslanib amalga oshirish mumkin [20].

Ikkala holatda ham EECh nuqtalari koordinatalarining ikki xil talqini qo'llaniladi: a) egri chiziq yasalayotgan kengaytirilgan maydon elementi sifatida; b) butun sonning kodi sifatida.

Sonlar ustida modul arifmetikasi qo'llanilganda EECh tartibi n modul bo'yicha qo'shish va ko'paytirish amallari bajarilishi mumkin, EECh arifmetikasini qo'llaganda bunday sonlarga EECh nuqtalari ko'paytiriladi. Bunda sikl EECh nuqtalari qism gruppasining tartibi bilan aniqlanadi va EECh yoki qismgruppasi tartibini bilish talab etilmaydi.

$\mathbb{A}$ va $\mathbb{V}$ ishtirokchilar n tartibli EEChning barcha amallar bajariladigan P nuqtasiga ega bo'lsinlar. Ular bir-birlarining qisqa muddatli va uzoq muddatli kalitlarini ham bilsinlar.

1. $\mathbb{V}$ ishtirokchining kaliti **A** ishtirokchiga ma'lum bo'lsin:

$$Q_B = d_B P = (a_B, b_B),$$
$$R_B = k_B P = (x_B, y_B).$$

2. **A** ishtirokchining kaliti **V** ishtirokchiga ma'lum bo'lsin:

$$Q_A = d_A P = (a_A, b_A),$$
$$R_A = k_A P = (x_A, y_A).$$

3.3.12. EEChlarga asoslangan kriptotizimlar uchun El Gamal protokoli

RSA kriptotizimida El Gamal protokolining qo'llanilishi quyidagicha bo'ladi. n tub son va ixtiyoriy $p<n$ va $q<n$ sonlar tanlanadi. Ochiq kalit sifatida $(n, p, p^q \bmod n = y)$ uchlik, maxfiy kalit sifatida esa q dan foydalaniladi.

Ochiq m matnni shifrlash uchun $a \equiv p^k (\bmod n), b(m) \equiv (y^k m) (\bmod n)$ hisoblash kerak bo'ladi, bunda k - ixtiyoriy n bilan o'zaro tub bo'lgan son. $a, b(m)$ juftlik shifrmatn bo'ladi. Ravshanki, matnni shifrini ochish uchun $m = (b(m)/a^q) \bmod n$ hisoblanadi.

EEChning multiplikativ gruppasini qo'llovchi El Gamal protokolining modifikasiyasi quyidagicha:

Faraz qilaylik, M ochiq matn *Ye* EEChning nuqtasi bo'lsin. Agar ochiq matn bir qancha nuqtalar to'plamidan iborat bo'lsa, quyida keltiriladigan almashtirishlar har bir nuqta uchun alohida bajariladi.

Kriptotizimning **A** va **V** ishtirokchilari Diffi-Xellman protokoli bo'yicha $k_A Q$ va $k_B Q$ kalit qismlarini almashtirishdi. **A** ishtirokchi **V** ishtirokchiga M xabarni yubormoqchi bo'lsa, l maxfiy sonni tanlaydi va **V** ishtirokchiga EEChning $E = (lQ, M + l(k_B Q))$ nuqtalar juftini yuboradi. Olingan axborotni shifrini ochish uchun **V** ishtirokchi $T = k_B(lQ)(l(k_B Q))$ ni hisoblashi kerak. Bunda $M = M + l(k_B Q) - T$.

E'tiborli jihati shundaki, lQ nuqta shifrni yig'ish funksiyasini bajaradi va demak, biron bir Q nuqta ikki marta ishlatilishi mumkin emas. Agar ikki marta ishlatilsa, ikki xil shifrmatnni taqqoslash natijasida nafaqat shifrmatnning shifrini sindirish, balki tizimning maxfiy komponentalarini aniqlashning ham imkoni tug'iladi.

3.3.13. Modul arifmetikasiga asoslangan protokollar

Modul arifmetikasiga asoslangan kalitlarni taqsimlash protokoli har ikkala tomondan simmetrik bajaraladigan uch bosqichdan iborat [9-11].

Birinchi bosqichda **A** va **V** ishtirokchilar o'zining maxfiy k_A, d_A hamda k_B, d_B ma'lumotlaridan foydalanib, quyidagilarni hisoblaydi:

$$s_A = (k_A + x_A a_A d_A) \bmod n,$$

$$s_B = (k_B + x_B a_B d_B) \bmod n.$$

Ikkinchi bosqichda ular EEChning nuqtalarini hisoblashadi:

$$U_A = R_B + x_B a_B Q_B,$$

$$U_B = R_A + x_A a_A Q_A.$$

Uchinchi bosqichda ular EECh nuqtasini hisoblashadi:

$$W = s_A U_A,$$

$$W = s_B U_B.$$

Chap tarafidagi belgilashning bir xilligi bu ikkala tenglikning qiymati tengligini bildiradi. Buni esa quyidagicha isbotlash mumkin.

A ishtirokchi uchun

$$\begin{aligned} s_A U_A &= ((k_A + x_A a_A d_A) \bmod n)(R_B + x_B a_B Q_B) = \\ &= ((k_A + x_A a_A d_A) \bmod n)(k_B P + x_B a_B d_B P) = \\ &= ((k_A + x_A a_A d_A) \bmod n)(k_B + x_B a_B d_B) P = \\ &= ((k_A + x_A a_A d_A)(k_B + x_B a_B d_B) \bmod n) * P. \end{aligned}$$

V ishtirokchi uchun

$$\begin{aligned} s_B U_B &= ((k_B + x_B a_B d_B) \bmod n)(R_A + x_A a_A Q_A) = \\ &= ((k_B + x_B a_B d_B) \bmod n)(k_A P + x_A a_A d_A P) = \\ &= ((k_B + x_B a_B d_B) \bmod n)(k_A + x_A a_A d_A) P = \\ &= ((k_B + x_B a_B d_B)(k_A + x_A a_A d_A) \bmod n) * P. \end{aligned}$$

Qarab chiqilayotgan protokolning talqinida modul arifmetikasi EEChlar arifmetikasi bilan uyg'unlashtirilgan.

Modul arifmetikasidan foydalanilmagan va s_A, s_B sonlar avvaldan hisoblanmagan holdagi talqinini quyida ko'rib chiqiladi.

A ishtirokchi Q_B nuqtani a_B konstantaga va x_B konstantaga ko'paytirib, so'ngra hosil bo'lgan nuqtani R_B nuqta bilan qo'shib EEChning U_A nuqtasini hisoblab topishi mumkin. Xuddi shunday **V** ishtirokchi ham U_B nuqtani hisoblab topishi mumkin.

W nuqtani olish uchun **A** va **V** ishtirokchilar olingan nuqtalarni s_A, s_B konstantalarga ko'paytirish lozimligini ko'zda tutgan holda, quyidagi algoritm bo'yicha amalga oshirishlari mumkin (**A** ishtirokchi uchun):

1) EECh nuqtasini konstantaga ko'paytirish natijasida $k_A U_A$ ni hisoblash.

2) Mos kattaliklarni ketma-ket ko'paytirish yo'li bilan $x_A(a_A(d_A U_A))$ ni aniqlash.

3) 1) va 2) punktlarda topilgan EEChning ikkita nuqtasi qo'shiladi.

Protokol tugallanishida **A** va **V** ishtirokchilar an'anaviy shifrlash tizimlarida koordinatalari maxfiy kalitning binar kodini quruvchisi sifatida qo'llanilishi mumkin bo'lgan EEChning maxfiy W nuqtasiga ega bo'ladilar.

3.4. Kalitlarni taqsimlash protokollarini tahlillash usullari

3.4.1. Kalitlarni taqsimlash bo'yicha mavjud protokollarning bardoshliligini ta'minlovchi muammolar

U. Diffi va M. Xellman oshkora kalitlar kriptografiyasi asoschilari hisoblanib, kalitlarni taqsimlash sohasiga oid ulkan ahamiyatga molik ixtirolari AQSh patenti [41] hisoblanadi. Unda tomonlar o'rtasida maxfiy yo'lli bir tomonlama funksiyadan foydalanib maxfiy kalitlarni bevosita almashish muammosi hal qilib berildi. Ular bir tomonlama funksiya sifatida maxfiy ko'rsatkichda tub modul bo'yicha diskret darajaga oshirish funksiyasidan foydalandilar. Modul arifmetikasida bir tomonlama funksiya f ning maxfiy argumenti sifatida diskret daraja ko'rsatkichi x tanlandi. Funksiya qiymati y bo'yicha katta qiymatli tub modul p arifmetikasida x ni topishning samarali hisoblash algoritmi hanuz topilmagan diskret logarifm muammosi bilan bog'liq. Internet sahifalarida nemis olimlari *530* bitli tub modul bo'yicha diskret logarifm muammosini yechganliklari yoritilgan. Bu esa diskret logarifm muammosiga asoslangan algoritmlarning kriptografik bardoshliligi va xavfsizlik parametrlariga bo'lgan talablarni kuchaytirishga olib keladi.

Kalitlarni taqsimlash bo'yicha mavjud xorijiy algoritmlarning tahlili shuni ko'rsatdiki, ularning bardoshliligini ta'minlashga asos bo'lgan murakkab muammolar quyidagilardan iborat:

- diskret logarifm muammosining murakkabligiga asoslangan;
- Diffi-Xellman muammosining murakkabligiga asoslangan;
- EEChda diskret logarifm muammosining murakkabligiga asoslangan;
- boshqa muammolarga asoslangan algoritm va protokollardir.

Diskret logarifm muammosiga quyidagicha ta'rif beriladi:

Ta'rif. Tub con p uchun, chekli maydon Z_p^* da hosil qiluvchi (generator) element α hamda $\beta \in Z_p^*$ berilgan bo'lsa, shunday $0 \le x \le p-2$ bo'lgan butun x son topilsinki, unda $\alpha^x \equiv \beta \pmod p$ bo'lsin, bu yerda x – daraja ko'rsatkichi.

U. Diffi va M. Xellman o'zlari nomida ta'riflangan diskret logarifm muammosiga teng kuchli muammoni ham ilgari surdilar:

Ta'rif. Agar tub modul p, $GF(p)$ chekli maydonning hosil qiluvchi (generator) elementi a va diskret darajaga oshirish funksiyalari qiymatlari $y_1 \equiv a^e \pmod p$, $y_2 \equiv a^d \pmod p$ berilgan bo'lsa, $(a^e)^d \pmod p \equiv (a^d)^e \pmod p$ topilsin.

Bu yerda $y_1 \equiv a^e \pmod p$ birinchi ishtirokchining oshkora kaliti vazifasini, $y_2 \equiv a^d \pmod p$ ikkinchi ishtirokchining oshkora kaliti vazifasini o'taydi. Daraja ko'rsatkichi e birinchi ishtirokchining maxfiy kaliti vazifasini, daraja ko'rsatkichi d ikkinchi ishtirokchining maxfiy kaliti vazifasini o'taydi. Natural son a va tub modul p dan tarkib topgan juftlik (a, p) ikkala yoki undan ortiq ishtirokchilar uchun umumiy oshkora parametrlardir.

EEChda diskret logarifm muammosi quyidagi ta'rifga ega:

Ta'rif. K chekli maydon va G nuqtada tartibi n bo'lgan G nuqta, $Q \in E(K)$ nuqtada E EECh berilgan. $Q=[d]G$ shartni qanoatlantiruvchi d, $0 \le d \le n-1$ butun sonni topish talab etiladi, agarda u mavjud bo'lsa.

Kalitlarni taqsimlash bo'yicha mavjud algoritmlar va protokollarning ko'pchiligi diskret logarifmlash va EEChda diskret logarifmlash muammolarining murakkabligiga asoslangandir.

Simmetrik kriptotizimlar uchun shifrlash kalitini oshkora kanal bo'yicha taqsimlash algoritmlari asosida Diffi-Xellman muammosining murakkabligi yotadi. Shu bois, EEChda diskret logarifmlash va Diffi-Xellman muammolarini hal etish ko'pchilik kriptotahlilchilarning e'tiborini o'ziga tortadi.

3.4.2. Kalitlarni taqsimlash protokollarini tahlillash usullari

Kalitlarni taqsimlash jarayonida taqsimlangan kalitlarga taqsimlashning tezkorligi va aniqligi, taqsimlanadigan kalitlarning yashirinligi kabi talablar qo'yiladi. Kalitlarni taqsimlash protokollarini qo'yilgan talablarga muvofiqligini tahlil etish ancha murakkab masala

bo'lib, bardoshliligini tahlil etishning quyidagi usullari mavjud: evristik, formal va xavfsizlikni isbotlash [10].

1. Evristik tahlil – bu an'anaviy usul bo'lib klassik kriptografiyaga xos. Uning mohiyati shundan iboratki, tayyor protokoldan amaliyotda foydalanish jarayonida undan xato va kamchiliklar topib uni yo'qqa chiqarishga harakat qilinadi. Boshqacha aytganda bu usul "sinov va xato" deb ham nomlanadi.

2. Tahlillashning formal usullari. Bu usullar guruhi shu bilan xarakterlanadiki, tayyor protokollar maxsus matematik va mantiqiy usullar yordamida tahlillillashga tayyorlanadi. Ammo protokolning mohiyat mazmuni emas, balki uning formal tomonlari, ya'ni uning tuzilishi, prokolning har bir qadamini bajarishda namoyon bo'ladigan belgilari va xususiyatlari tahlil qilinadi. Bu usullarning afzalligi ularning yaxshi algoritmlashtirilishida bo'lib, u kriptografik protokollarda avtomatik dasturiy analizatorlarni yaratish imkonini beradi. Ammo ularni cheklashning sababi – ular tahlil qilayotgan protokollardagi barcha xatolarni aniqlamaydi. Agar formal tahlilda protokolda xatolar aniqlangan bo'lsa, demak ular haqiqatan ham protokolda bor va bu buzg'unchiga protokolga mos hujum uyushtirish imkonini beradi. Formal tahlilda protokolda xato aniqlanmaganligi ham hali bu protokolda xato yo'q degani emas.

3. Xavfsizlikni isbotlash usullari. Bu guruhdagi usullar umumiy yondashuvning xususiy holi bo'lib, kriptografik xavfsizlikning zamonaviy isboti unga asoslangan. Oldingi keltirilgan usullardan farqli holda bu usul avvaldan berilgan xavfsizlik xossalari asosida kriptografik protokollarni loyihalashtirish imkonini beradi.

3.2-jadval

Hujumlarning kalitlarni taqsimlash protokollariga ta'siri

№	Protokol nomi	Hujum turlari
1	**Shamir protokoli**	Kriptotahlilchi kriptotahlil usuli orqali kalitni aniqlashi mumkin

2	**Nidxeym-Shreder protokoli**	**V** ishtirokchi kalitni kim tomonidan yuborilganini bilmaydi Kriptotahlilchi bu kalitni ma'lum vaqtdan so'ng qayta uzatishi mumkin Arbitr ma'lumotni kimdan kelganini va kimga yuborish kerakligi haqida hyech narsa bilmaydi **A** ishtirokchi ma'lumotni arbitrdan kelganiga to'la ishonch hosil qilmaydi
3	**Yahalom protokoli**	Ishtirokchilar o'rtasida o'zaro identifikasiya ta'minlanmaydi
4	**Diffi- Xellman protokoli**	"O'rtadagi kishi " hujumiga bardoshli emas. Kriptotahlilchi bu ma'lumotlarni ma'lum vaqtdan keyin **V** ishtirokchiga qayta jo'natishi mumkin
5	**Hughes protokoli**	"O'rtadagi kishi " hujumiga bardoshli emas
6	**Katta halqumli qurbaqa protokoli**	Kriptotahlilchi bu ma'lumotni **V** ishtirokchiga takroran uzatishi mumkin Ishtirokchilar ma'lumotni kimdan kelganini bilmaydi
7	**DASS protokoli**	**V** ishtirokchi ERIni tekshirish imkoniga ega bo'lmaydi Tomonlar o'rtasida o'zaro identifikasiya ta'minlanmaydi
8	**Vu – Lama protokoli**	**A** ishtirokchi arbitrni identifikasiya qilmaydi Ishtirokchilar bir-birini identifikasiya qilmaydilar
9	**Denning – Sakko protokoli**	Protokol yakunlangandan so'ng **V** ishtirokchi boshqa **S** ishtirokchi bilan aloqa o'rnatishi uchun **A** ishtirokchining nomidan ish ko'rishi mumkin

Kriptografik protokollarning bardoshliligini tahlillashda BAN-mantiqdan foydalanish mumkin. **Berrouz – Abadi – Nidxem mantiqi** (inglizchada *Burrows-Abadi-Needham logic*) yoki **BAN-mantiqi** (inglizchada *BAN logic*) – axborot almashish protokollarini aniqlash va tahlillash uchun foydalaniladigan qoidalar to'plamidir [62]. Xususan, BAN-mantiq almashish jarayonida ishtirok etayotgan axborot haqiqiymi, eshitishdan himoyalanganmi va boshqalarni aniqlashda foydalanuvchilarga yordam beradi. Birinchidan, BAN-mantiq – bu istalgan muhitda (bu mis o'tkazgich, optik tola yoki havo bo'lishi mumkin) uzatiladigan axborotning konfidensialligi va haqiqiyligiga tahdid mavjud bo'lishi mumkinligidir. BAN-mantiqning oddiy ketma-ketligi uch qadamdan iborat:

1. Xabar manbasini tekshirish.
2. Xabarning yangiligini tekshirish.
3. Manbaning ishonchliligini tekshirish.

Autentifikasiya protokollarini tahlillashda BAN-mantiq boshqa barcha formal nazariyalar kabi aksioma va ta'riflardan foydalanadi. BAN-mantiq ko'pincha axborot muhofazasi protokollarining formal bayoniga ilova qilinadi.

BAN-mantiq hal qilinadiganlar sirasiga kiradi: ya'ni gipotezadan BAN-mantiq yordamida keltirilgan xulosalarning to'g'riligini tekshiruvchi algoritm mavjud. BAN-mantiq boshqa formal tizimlarning asosi bo'lib, ularning ba'zilari BAN-mantiqning zaif joylarini bartaraf etishga harakat qiladi.

Asosiy qoidalar va ularning xulosalari quyida keltirilgan (**P** va **Q** – tizim mijozlari, X - uzatiladigan xabar, K - shifrlash kaliti):

– **P** X ga ishonadi: **R** X haqiqat bo'lgandagidek harakat qiladi, va X ni boshqa xabarlarda ham tasdiqlamog'i mumkin.

– **P** X ga haqqi bor: **P** ning X to'g'risidagi tasdiqlariga ishonish kerak.

– **P** X deydi: bir vaqtda **P** X (ga ishonib) xabar yuboradi, shuningdek **P** X ga boshqa ishonmasligi mumkin.

– **P** X ni ko'radi: **P** X xabarni qabul qiladi, X ni o'qishi va uzatishi mumkin.

– $\{X\}_K$: X K kalit bilan shifrlangan.

– Yangi (X): shu vaqtgacha X hyech bir xabarda yuborilmagan.

– Kalit (K, **P**↔**Q**): **P** va **Q** K kalit yordamida bog'lanishi mumkin.

Bu ta'riflarning mohiyatini quyidagi mantiqiy ifodalardan tushunish mumkin: Agar **R** kalit (K, **P**↔**Q**) ga ishonsa, va **R** $\{X\}_K$ ni ko'radi, u holda **R** (**Q** X deganiga) ishonadi. Agar **R** (**Q** X deganiga) va yangi (X) ga ishonsa, u holda (**Q** X ga ishonishiga) ishonadi. Bunda **R** X ning yangiligiga ishonishi lozim, aks holda X eski xabar bo'lib, hujum qiluvchi tomonidan qayta yuborilgan bo'ladi.

Agar **R** (**Q** ni X da haqqi borligiga) ishonsa va **R** (**Q** X ga ishonishiga) ishonsa, u holda **R** X ga ishonadi. Shuningdek, xabarlar kompozisiyasi bilan ishlash uchun foydalaniladigan yana bir qancha texnik tasdiqlar mavjud. Masalan, agar **P** **Q** ning $\langle X, Y \rangle$ (X va Y ning konkatensiyasi)ga ishonsa, u holda **R** **Q** X deganiga va **Q** Y deganiga ishonadi. Ushbu belgilashlardan foydalanib, autentifikasiyalash protokollari tavsifini shakllantirish mumkin. Shuningdek bu tasdiqlar yordamida, mazkur mijozlar aloqa uchun berilgan kalitlardan foydalanishga ishonishini tekshirish mumkin.

Quyida BAN-mantiq yordamida "Qurbaqa protokolining" tahlili keltiriladi [62]. Autentifikasiyalash protokolining juda sodda protokoli bo'lgan, "Qurbaqa protokoli" ikkita **A** va **V** ishtirokchilar uchun ular ikkisi ham ishongan S serverdan foydalanib himoyalangan aloqa o'rnatish va vaqtni sinxronlash imkonini beradi. Standart belgilashlardan foydalanib, protokol quyidagicha yozilishi mumkin:

$$A \rightarrow S : A, \{T_A, K_{ab}, B\}_{Kas}$$
$$S \rightarrow B : \{T_S, K_{ab}, A\}_{Kbs}$$

A va **V** ishtirokchilar S server bilan bog'lanish uchun mos ravishda K_{as} va K_{bs} kalitlarga ega. Bundan quyidagi natijalarni keltirish mumkin:

A ishonadi kalit (K_{as}, $A \leftrightarrow S$)
S ishonadi kalit (K_{as}, $A \leftrightarrow S$)
B ishonadi kalit (K_{bs}, $B \leftrightarrow S$)
S ishonadi kalit (K_{bs}, $B \leftrightarrow S$)

A ishtirokchi **V** ishtirokchi bilan himoyalangan yozishmalar olib bormoqchi. Buning uchun u K_{as} kalitni generasiya qiladi. **A** ishtirokchi bu

kalitni o'zi generasiyalagani uchun xavfsiz deb biladi, ya'ni: **A** kalit (K_{as}, $A \leftrightarrow S$) ga ishonadi.

B ishtirokchi bu kalitning **A** ishtirokchidan kelganiga ishonar ekan, bu kalitdan foydalanishga tayyor, ya'ni: **B** ishtirokchi (**A** ishtirokchining ishonchli kalit (K, $A \leftrightarrow B$)ga) ishonadi.

Bundan tashqari, **V** ishtirokchi S ni **A** ishtirokchining kalitini xatosiz uzatishiga ham ishonishga tayyor, ya'ni: **V** ishtirokchi (S ishonchli (**A** ishtirokchining ishonchli kaliti (K, $A \leftrightarrow B$))) ishonadi.

Bu degani, **V** ishtirokchi S ning **A** ishtirokchini **V** ishtirokchi bilan aloqa qilishi uchun o'zining kalitidan foydalanishni hohlashiga ishonishi, S ga ishonishi va unga suyana olishiga ishonishi kerak.

A ishtirokchi soatdan joriy vaqt t ni oladi, so'ngra quyidagi xabarni yuboradi: 1 A->S: {t, kalit (K_{ab}, $A \leftrightarrow B$)}K_{as}.

Bu shunday deganiki, **A** ishtirokchi seans kalitini va joriy vaqtni S serverda o'zining autentifikasiyalash kaliti bo'lgan K_{as} bilan shifrlab, S serverga yuboradi. S yangi (t) ga ishonishi bilan, va S (A {t, kalit (K_{ab}, $A \leftrightarrow B$)} deganiga) ishonadi, S **A** ishtirokchining kalit (K_{ab}, $A \leftrightarrow B$) ga ishonishiga ishonadi. (Shuningdek, S xabarni hujum qiluvchi tomonning avval tutib olgan xabarni qayta yuborilgani emasligiga ishonadi). So'ngra, S **V** ishtirokchiga kalit yuboradi 2 S->B: {t, A, **A** ishonchli kalit (K_{ab}, $A \leftrightarrow B$)}K_{bs}. 2 xabar K_{bs} kaliti bilan shifrlangani uchun **V** ishtirokchi ham kalit (K_{bs}, $B \leftrightarrow S$) ga ishonadi, endi **B** ishtirokchi S {t, A, **A** ishonadi kalit (K_{ab}, $A \leftrightarrow B$)}deganiga ishonadi. Vaqt sinxronlashtirilgani uchun **B** ishtirokchi yangi (t) ga ishonadi, va demak, yangi (**A** ishonadi kalit (K_{ab}, $A \leftrightarrow B$)) ga ishonadi. **B** ishtirokchi S ning tasdiqlari yangiligiga ishonishi, **B** ishtirokchi S ning (**A** ishonadi kalit (K_{ab}, $A \leftrightarrow B$)) ga ishonishiga ishonadi. **V** ishtirokchi S ni **A** ishtirokchining nimaga ishonishini bilishiga ishongani uchun **V** ishtirokchi (**A** ishonadi kalit (K_{ab}, $A \leftrightarrow B$)) ga ishonadi. **V** ishtirokchi **A** ishtirokchining **V** va **A** ishtirokchilar orasidagi seans kaliti haqida bilishiga ishongani uchun, **V** ishtirokchi kalit (K_{ab}, $A \leftrightarrow B$) ga ishonadi. Endi **V** ishtirokchi **A** ishtirokchi bilan K_{ab} dan maxfiy seans kaliti sifatida foydalanib to'g'ridan to'g'ri aloqada bo'lishi mumkin.

3.4.3. Kriptografik kalitlarni taqsimlash usullarining tasnifi

Kriptografik kalitlarni taqsimlash usullarini tasniflash mumkin bo'lgan asosiy belgilar to'plamiga quyidagilar kiradi:

1. Vaziyatga bog'liq holda tanlash darajasi;
2. Kalit xavfsizligini ta'minlash usuli;
3. Kalitlarni taqsimlash protokoli sinflari.
4. Kalitlarni taqsimlash protokoli bardoshliligini tahlil etish usuli.
5. Kalitlarni taqsimlash protokoli bardoshliligini ta'minlovchi muammo turlari.

Kriptografik kalitlarni taqsimlashning bir qancha yechimlari mavjud bo'lib, ulardan mosi vaziyatga bog'liq holda 3 xil darajada tanlanadi: fizik, maxfiy va ochiq kalitli protokollar yordamida.

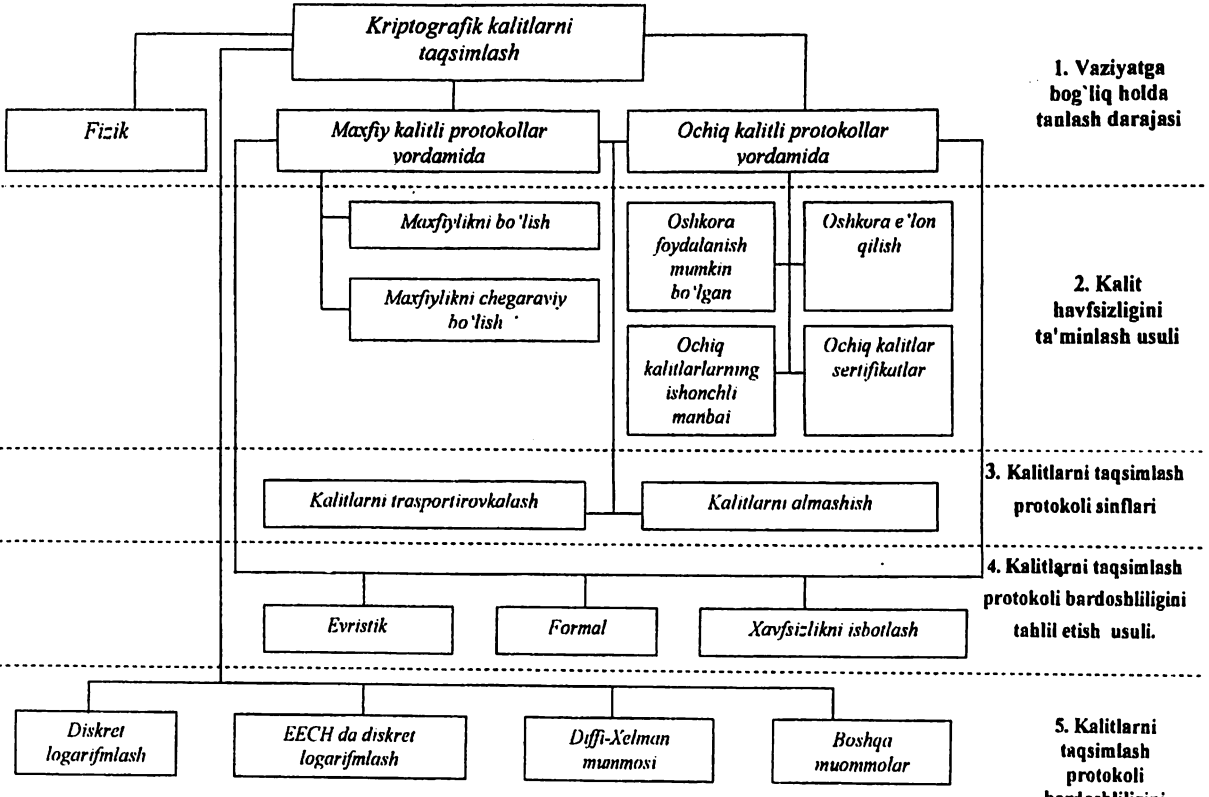
Ikkinchi belgi - kalit xavfsizligini ta'minlash usuli bo'yicha ma'lumotlar yuqoridagi paragraflarda to'liq bayon etilgan.

Kalitlarni taqsimlash protokoli ikkita sinfga kalitlarni transportirovkalash va kalitlarni almashish protokollariga ajraladi.

Taqsimlangan kalitlarga taqsimlashning tezkorligi va aniqligi, taqsimlanadigan kalitlarning yashirinligi kabi talablar qo'yiladi. Bu talablarga protokollar muvofiqligini tahlil etish ancha murakkab masaladir. Kalitlarni taqsimlash protokoli bardoshliligini tahlil etishning 3 ta ma'lum usullari mavjud: evristik, formal va xavfsizlikni isbotlash.

Beshinchi belgi bo'yicha kalitlarni taqsimlash protokolini ta'minlovchi muammolar turlariga diskret logarifmlash muammosi, EECh gruppasida diskret logarifmlash muammosi, Diffi-Xellman muammosi va boshqa turdagi muammolar kiradi. Eng ko'p foydalaniladigan logarifmlash muammolari va EECh gruppasida diskret logarifmlash sinflariga oid algoritmlar va protokollar yuqoridagi paragraflarda to'liq bayon etilgan.

Quyidagi 3.24-rasmda kriptografik kalitlarni taqsimlash usullarining tasnifi keltirilgan.



3.24- rasm. Kriptografik kalitlarni taqsimlash usullari tasnifi

Nazorat savollari

1. Kalitlarni boshqarish qanday tizimlarda juda muhim hisoblanadi?
2. Kriptografik kalitlar deganda nima nazarda tutiladi? Bu kalitlar nima uchun ishlatiladi?
3. Kalitlarni boshqarish qanday amallarni o'z ichiga oladi?
4. Kriptografik kalitlarni boshqarish sohasida qaysi xalqaro standartdan foydalaniladi?
5. Kalitlarni boshqarish qanday jarayonlardan iborat va ularni izohlab bering.
6. Kalit tarqatish protokollarining uchta turini tushuntiring.
7. Kalit taqsimotining qanday yechimlari mavjud?
8. Tasodifiy sonlar qanday hosil qilinadi va u nima uchun kerak?
9. Kalitlarning yaroqlilik muddati deganda nimani tushunasiz?
10. Chegaraviy bo'lish sxemalari qaday amalga oshiriladi? Unga misol keltiring.
11. Kalitlarni taqsimlash tartib va qoidalarini qadamma-qadam gapirib bering.
12. Kalit taqsimlash protokollarining asosiy xossalariga nimalar kiradi?
13. Kalit tasdiqlashning to'rtta usulini izohlang.
14. Kalitlarni taqsimlash usullari qanday sinflarga bo'linadi? Ularning kamchiligi va afzalligi nimalardan iborat?
15. Ochiq kalitlarning IM jarayonini yoritib bering.
16. Sertifikat nima vazifani bajaradi va unga qanday talablar qo'yiladi?
17. Maxfiy kalitlarni konfidensialligini va autentifikasiyasini ta'minlab taqsimlash sxemasini tushuntirib bering.
18. Gibrid sxema nima va u qanday mantiqqa asoslanadi?
19. Statik kalitdan seansli kalitni nima farqi bor?
20. Simmetrik kriptotizim yordamida kalitlarni almashish protokolini tushuntirib bering.
21. Simmetrik kriptotizim yordamida kalitlarni almashish protokoliga misol keltiring.
22. Shamir protokoli qanday bosqichlardan tashkil topgan? U qanday masalaning murakkabligiga asoslangan va uning kamchiliklari?

23. Nidxeym-Shreder protokolining afzalligi va kamchiligi nimadan iborat?

24. Otvey-Riis protokolining Nidxeym-Shreder protokolidan asosiy farqi nimadan iborat?

25. Yahalom protokolining sxemasini mohiyati nimada?

26. Nyuman-Stabblbayn protokoli qanday asosiy xususiyatlarga ega?

27. SKID protokoli qanday amalga oshiriladi?

28. Vaqt belgisi nima maqsadda qo'llaniladi?

29. Yolg'on vaqt belgisi deganda nimani tushunasiz?

30. Biror xabarga vaqt belgisini qo'yish qanday amalga oshiriladi?

31. Diffi-Xellman 'sxemasiga asosan kalit tarqatish qanday bajariladi?

32. Kriptografik kalitlarni taqsimlash protokoli deganda nimani tushunasiz va u qanday sinflarga bo'linadi?

33. Kalitlarni transportirovkalash protokoliga izoh bering va misol keltiring.

34. Hughes protokoli qanday amalga oshiriladi?

35. Katta halqumli qurbaqa protokoli mazmunini tushuntirib bering.

36. MTI protokolining o'ziga xos xususiyatlari nimadan iborat?

37. DASS protokolini yoritib bering.

38. Denning – Sakko protokoli qanday kamchilikka ega?

39. Vu – Lama protokolining Denning – Sakko protokolidan farqi nimada?

40. EEChlarga asoslangan kriptografik tizimlarning an'anaviy tizimlarga nisbatan afzalligi nima?

41. EEChlar qanday tenglama bilan ifodalanadi va u qanday xossalarga ega?

42. EEChda nuqta qanday topiladi?

43. Kalit taqsimotining EEChlardagi analogi qanday ko'rinishda bo'ladi?

44. EEChlarga asoslangan Diffi-Xellman sxemasining analogini yoritib bering.

45. Messi – Omur' protokolining kalit taqsimoti sxemasi qanday amalga oshiriladi?

46. Menezes-Kyu-Vanstonning kalit taqsimlash sxemasini izohlab bering.

47. EEChlarga asoslangan kriptotizimlar uchun El Gamal protokoli qanday qo'llaniladi?

48. Modul arifmetikasiga asoslangan kalitlarni taqsimlash protokoli qanday bosqichlardan iborat va ularni izohlab bering?

49. Kalitlarni taqsimlash bo'yicha bardoshlilikni ta'minlashga asos bo'lgan qanday murakkab muammolar mavjud?

50. Kalitlarni taqsimlash protokollarini tahlillashda qanday usullardan foydalaniladi?

51. BAN-matiqining mohiyatini tushuntiring.

52. BAN-mantiqi yordamida "Qurbaqa protokolining" tahlili qanday amalga oshiriladi?

53. Kriptografik kalitlarni taqsimlash usullarini tasniflab bering.

4. E'LON QILINGANLIGI NOLGA TENG BO'LGAN PROTOKOLLAR

4.1. E'lon qilinganligi nolga tengligi tushunchasi

Kriptografik protokollarning sinflaridan biri e'lon qilinganligi nolga tengligi isboti deb nomlanadi. Bunday protokollar agar bir **R** ishtirokchi boshqa bir **V** ishtirokchiga u ba'zi bir sirlardan xabardor ekanligiga ishontirmoqchi bo'lgan hollarda ishlatiladi. Bu sir quyidagilar bo'lishi mumkin: ba'zi bir son yoki ba'zi bir tasdiqning isbotini bilish [7-10]. E'lon qilinganligi nolga tengligi isboti interfaol va interfaol bo'lmagan holda bo'lishi mumkin.

Faraz qilaylik, interfaol isbotlash tizimi $\langle P,V,S\rangle$ berilgan bo'lsin. Interfaol isbotlash tizimining ta'rifida avval **V** ni buzg'unchi bo'lishi ko'zda tutilmagan edi. Ammo **V** **R** dan S tasdiq to'g'risidagi biron bir foydali ma'lumotni bilib olmoqchi bo'lgan buzg'unchi bo'lishi mumkin. Bunda **R** interfaol isbotlash tizimi $\langle P,V,S\rangle$ protokolining ishlash jarayonida bunday bo'lishini istamasligi mumkin. Shunday qilib, xabardorlikni e'lon qilishning nolga teng bo'lgan isbotlash protokoli fikriga kelinadi. Bilishlikni e'lon qilishning nolga teng bo'lishi deganda interfaol isbotlash tizim protokolining ishlashi natijasida **V** S tasdiq to'g'risidagi bilganini ko'paytira olmaydi, ya'ni S ning nima uchun haqiqatligi to'g'risida hyech qanday ma'lumot ololmaydi.

Xuddi avvalgidek protokolda biror bir S tasdiq shakllantiriladi, masalan biron bir w obyekt L xossaga ega degan, ya'ni $w\in L$. Protokol davomida **V** va **R** xabarlar almashishadi. Ularning har biri biron bir tasodifiy son generasiya qilishi va undan o'z hisoblashlarida foydalanishlari mumkin. Protokol so'nggida esa **V** o'zining S haqiqiy yoki soxtaligi to'g'risidagi qat'iy fikrini berishi kerak.

R ning maqsadi **V** ni har doim S ning haqiqiy yoki qalbakiligidan qat'iy nazar uning haqiqiyligiga ishontirishdan iborat, ya'ni **R** faol buzg'unchi bo'lib, **V** ning vazifasi **R** ning dalilini tekshirishdir. **V** ishtirokchining maqsadi Sning haqiqiy yoki soxtaligi to'g'risida xulosa chiqarish. **V** polinomli chegaralangan hisoblash imkoniyatiga ega, ya'ni uning ishlash vaqti isbotlanayotgan tasdiq uzunligi kattaligining biron bir polinomi bilan chegaralangan: $t\le p(|w|)$. Shuning uchun u **R** ning yordamisiz mustaqil ravishda S tasdiqning haqiqiyligini aniqlay olmaydi. **R** ni hisoblash imkoniyatlari hyech qanday chegaralanmaydi [8-10].

Bilishni e'lon qilinganligi nolga teng bo'lgan isbotlash protokollariga misollar ko'rib chiqamiz.

1. "Ali Boboning g'ori masalasi". 4.1-rasmda keltirilgan reja ko'rinishidagi g'or mavjud bo'lsin. Bu g'orning F va J nuqtalar orasida maxfiylikka ega bo'lgan eshigi bor bo'lsin. Har bir bu maxfiy so'zni bilgan odam bu eshikni ochib, F dan J ga va aksincha o'tishi mumkin. Qolgan barcha uchun g'orning ikkala yo'nalishi ham boshi berk yo'lga olib keladi.

Faraz qilaylik, **R** g'orning sirini biladi. **U** **V** ga maxfiy so'zni aytmasdan turib sirni bilishini isbotlamoqchi. Bu ularning aloqasi protokoli:

1) **V** G nuqtada bo'lsin;

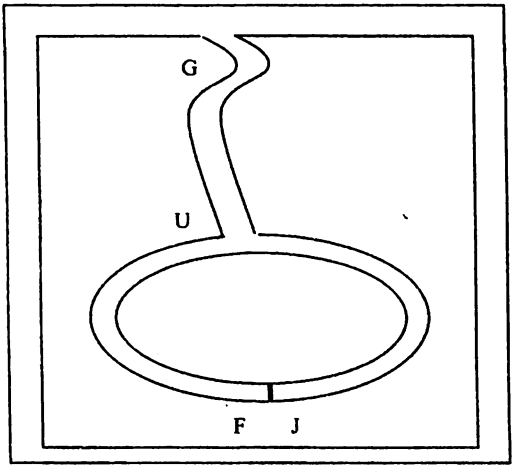
2) **R** g'orga kiradi va yo F nuqtaga yoki J nuqtaga yetib boradi;

3) **R** g'orga kirib ketgandan so'ng **V** U nuqtaga keladi va **R** ni qayerga ketganini bilmaydi;

4) **V** **R** ni chaqiradi va **V** ning hohishiga qo'ra g'orning chap tomonidan yoki o'ng tomonidan kelishini so'raydi;

5) **R** bu iltimosni kerak bo'lsa eshikni ochib, albatta, bunda u maxfiy so'zni bilsa bajaradi.

6) **R** va **V** 1)-5) qadamni n marta bajaradi.



4.1- rasm. "Ali Boboning g'ori haqidagi masala"

Agar **R** eshikning sirini bilmasa, u holda V ni uni kirgan yo'lidan qaytib chiqishini so'rash ehtimolligi $1/2$ ga teng. Protokolning n ta raundidan keyin ehtimollik $1/2^n$ gacha kamayadi.

2. *Graflarning izomorfligini isbotlash.* **R** **V** ga G_0 va G_1 graflarning izomorfligini isbotlamoqchi. Faraz qilaylik, $G_1 = \varphi(G_0) : G_0 = G_1$, bunda φ - izomorf almashtirish; m - graf uchlari to'plami N ning quvvati.

Bu protokolning tuzilishini ko'rib chiqamiz [10]. (1) qadamda **R** ishtirokchi tasodifiy G_1 ga izomorf bo'lgan N grafni yaratadi. (2) qadamda **V** ishtirokchi tasodifiy bit $\alpha = \{0,1\}$ tanlaydi va shu bilan $H \approx G_0$ yoki $H \approx G_1$ ekanini isbotlashni so'raydi. (3) qadamda **R** ishtirokchi **V** ishtirokchiga Ψ almashtirishni yuboradi. Bu Ψ almashtirishni $\alpha = 1$ da G_α grafiga qo'llaganda $F^{-1} = \pi G_1 = H$ graf hosil bo'ladi. $\alpha = 0$ da esa bu almashtirishni G_α grafiga qo'llaganda $F^0 = \pi(\varphi(G_0)) = \pi G_1 = H$ graf hosil bo'ladi. (4) qadamda **V** ishtirokchi graflarni tenglikka tekshirar ekan, $H = F^\alpha$ shartining bajarilish yoki bajarilmasligini aniqlaydi. (1) – (4) qadamlar m marta takrorlanadi. Agar bu protokolning barcha m raundida natija ijobiy bo'lsa, V isbotni qabul qiladi.

4.1-jadval

Graflarning izomorfligini tasdiqlovchi protokol

	R		**V**	
1	π - uchlarni tasodifiy o'rnini almashtirish, $H = \pi G_1$ hisoblaydi	$\rightarrow$		m марта
2		$\leftarrow$	$\alpha = \{0,1\}$ - tasodifiy	
3	Ψ quyidagicha aniqlangan akslantirishni yuboradi $\Psi = \begin{cases} \pi, agar \alpha = 1 \\ \pi \circ \varphi, agar \alpha = 0 \end{cases}$	$\rightarrow$		
4			ΨG_α grafni hisoblang va taqqoslang: $H = \Psi G_\alpha$.	
5			Isbotni faqat va faqat $\forall m$ uchun $H^{(m)} = \Psi G_\alpha^{(m)}$ bo'lgandagina qabul qilinadi	

Bu protokol haqiqatan ham xabardorlikni e'lon qilishning nolga teng bo'lgan protokoli, chunki izomorf $G_0 \approx G_1$ da **V** ishtirokchi G_0 va G_1 graflarni qandaydir bir raqamlangandagi qiymatining izomorfligidan boshqa ma'lumot ola olmaydi, ammo bu raqamlashni uni o'zi mustaqil α ga tasodifiy bit berib va G_α grafni tasodifiy raqamlash orqali hosil qilishi ham mumkin edi (4.1-jadval).

3. *X sonining diskretlogarifmi x ni bilishning isboti.* Protokol ish jarayonining boshlanishidan oldin ochiq kattaliklar beriladi: p,q - shunday tub sonlarki, $q|(p-1)$, $g \in Z_p^*$ element, X son. **R** isbot qiluvchiga maxfiy kattalik $x: x \in Z_q, g^x = X$ ma'lum bo'lib, maxfiy kattalikni aytmasdan turib, u **V** ga maxfiy ma'lumotni bilishini isbotlashi kerak. Quyidagi 4.2-jadvalda bu masalaning yechimi keltirilgan.

4.2-jadval

Diskret logarifmni bilishini isbotlash protokoli

	R		**V**
1	$r \in_R Z_q, M = g^r (\mathrm{mod} p)$	$\rightarrow$	
2		$\leftarrow$	$R \in_R Z_q$
3	$m = r + xR (\mathrm{mod} q)$	$\rightarrow$	
4			$g^m = X^R \cdot M (\mathrm{mod}\ p)$

4. *Y sonini bazisdagi ko'rinishini bilishning isboti.* Protokol ish jarayonini boshlanishidan oldin barcha ishtirokchilarga ochiq kattaliklar beriladi: p,q - tub sonlar, $y, g_1, g_2, \ldots, g_k \in G_q$ elementlar. **R** isbot qiluvchiga maxfiy kattalik $\alpha_1, \alpha_2, \ldots \alpha_k \in Z_q : y = g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \ldots \cdot g_k^{\alpha_k}$ ma'lum bo'lib, maxfiy kattalikni aytmasdan turib u **V** ga maxfiy ma'lumotni bilishini isbotlashi kerak [10]. Protokol quyidagi 4.3-jadvalda keltirilgan.

4.3-jadval

Sonning bazisdagi ko'rinishini bilishini isbotlash protokoli

	R		**V**
1	$r_1, r_2, \ldots r_k \in_R Z_q$, $M = g_1^{r_1} \cdot g_2^{r_2} \cdots g_k^{r_k}$	$\rightarrow$	
2		$\leftarrow$	$R \in_R Z_q$
3	$m_i = r_i + \alpha_i R, i = \overline{1,k}$	$\rightarrow$	
4			$g_1^{m_1} \cdot g_2^{m_2} \cdots g_k^{m_k} = y^R \cdot M$

5. *Sonlar to'plamining mos bazislardagi ko'rinishlarini bilishining isboti.* Protokol ish jarayonini boshlanishidan oldin barcha ishtirokchilarga ochiq kattaliklar beriladi: p,q - tub sonlar, $y^{(j)}, g_1^{(j)}, g_2^{(j)}, \ldots, g_k^{(j)} \in G_q$ elementlar berilgan (j) uchun. **R** isbot qiluvchiga maxfiy kattalik $\alpha_1, \alpha_2, \ldots, \alpha_k \in Z_q$ va $\forall j : y^{(j)} = (g_1^{(j)})^{\alpha_1} \cdot (g_2^{(j)})^{\alpha_2} \cdot \ldots \cdot (g_k^{(j)})^{\alpha_k}$ ma'lum bo'lib, maxfiy kattalikni aytmasdan turib u **V** ga maxfiy ma'lumotni bilishini isbotlashi kerak [10]. Bu masalaning yechilish protokoli quyidagi 4.4-jadvalda keltirilgan.

4.4-jadval

Sonlar to'plamining mos bazislardagi ko'rinishlarini bilishini isbotlash protokoli

	R		**V**
1	$r_1, r_2, \ldots r_k \in_R Z_q, \forall j$ $M^{(j)} = (g_1^{(j)})^{r_1} \cdot (g_2^{(j)})^{r_2} \cdots (g_k^{(j)})^{r_k}$	$\rightarrow$	
2		$\leftarrow$	$R \in_R Z_q$
3	$m_i = r_i + \alpha_i R, i = \overline{1,k}$	$\rightarrow$	
4			$\forall j$ $(g_1^{(j)})^{m_1} \cdot (g_2^{(j)})^{m_2} \cdots (g_k^{(j)})^{m_k} = (y^{(j)})^R \cdot M^{(j)}$

6. *"Deponirlangan" kattaliklarning multiplikativ bog'liqligini bilishning isboti.* Diskret logarifmlash murakkab hisorblanadigan masala hisoblanadigan, tartibi tub son bo'lgan siklik qismgruppaning $X = g^x$ elementi maxfiy x kattalikni ifodalovchi "deponirlangan" kattalik deyiladi. Faraz qilaylik, d - noma'lum element bo'lib, $h = g^d$ bo'lsin. Protokol ish jarayonini boshlanishidan oldin ochiq kattaliklar beriladi: p,q - tub sonlar, $A,E,C \in G_q$ elementlar. **R** isbot qiluvchiga $c=ae$, $A=g^a h^{\hat{a}}$, $E=g^e h^{\hat{e}}$, $C=g^c h^{\hat{c}}$ shartlarni qanoatlantiruvchi maxfiy kattaliklar a, $\hat{a}$, e, $\hat{e}$, c, $\hat{c}$ ma'lum bo'lib, maxfiy kattalikni aytmasdan turib u **V** ga maxfiy ma'lumotni bilishini isbotlashi kerak [10]. Protokol quyidagi 4.5-jadvalda keltirilgan.

4.5-jadval

"Deponirlangan" kattaliklarning multiplikativ bog'liqligini bilishini isbotlash protokoli

	R		V
1	$d,x,s,s_1,s_2 \in_R Z_q$, $M = g^d \cdot h^s$, $M_1 = g^x \cdot h^{s_1}$, $M_2 = B^x \cdot h^{s_2}$	→	
2		←	$R \in_R Z_q$
3	$y=d+eR$, $z=x+aR$, $w=s+\hat{e}R$, $w_1=s_1+\hat{a}R$, $w_2=s_2+(\hat{c}-a\hat{e})R$	→	
4			$g^y \cdot h^w = B^R \cdot M$, $g^z \cdot h^{w_1} = A^R \cdot M_1$, $B^z \cdot h^{w_2} = C^R \cdot M_2$

Keltirilgan misollarni umumlashtirib bir qator ta'riflar keltiramiz. Umumiy holda e'lon qilinganligi nolga teng bo'lgan interfaol isbotlash protokoli to'rt qadamdan iborat bo'ladi (4.6-jadval).

4.6-jadval

E'lon qilinganligi nolga teng bo'lgan bilishni isbotlash protokolining tuzilishi

	R	$S: x \in L$ - isbotlanadigan tasdiq, h-boshqa ochiq parametrlar va kattaliklar, s S ning nima uchun haqiqat ekanligini isbotlovchi maxfiy ma'lumot, r- tasodifiy son	V
1	r_p - tasod. s., $W = f_1(x, r_p)$	→	
2		←	r_v - tasod. s., $C = f_2(r_v)$
3	$R = f_3(C, x)$	→	
4			$R \approx W$

1) isbot qiluvchi tekshiruvchiga uni bilishini isbotlovchi "dalil" (*W - witness*) – maxfiy kattalikning bir tomonlama funksiyasini hisoblab topilgan natijasi;

2) tekshiruvchi unga tasodifiy so'rovnoma yuboradi;

3) isbotlovchi bu so'rovnomaga javob beradi, bunda javob tasodifiy so'rovnoma bilan birga maxfiy kattalikka ham bog'liq bo'ladi, ammo javobdan o'sha maxfiy kattalikni hisoblashning imkoni bo'lmaydi;

4) javobni olib, **V** uning 1 – qadamda yuborgan "dalil"i bilan taqqoslaydi.

E'lon qilinganligi nolga teng bo'lgan bilishning asosiy tamoyillarini ko'rib chiqamiz: e'lon qilinganligi nolga teng bo'lgan bilish nimani anglatadi.

E'lon qilinganligi nolga teng bo'lgan bilishni isbotlash nazariyasida **R** va **V** qora quti sifatida qaraladi (4.2-rasm).

Faraz qilaylik, $\{m_P\},\{m_V\}$ - **R** dan **V** ga (**V** dan **R** ga) uzatilayotgan barcha xabarlar to'plami bo'lib, ularning har biri tasodifiy kattalik va shuning uchun $\{x,h,r_V,\{m_P\},\{m_V\}\} = view_{P,V}(x,h)$ - protokolning tashqi kuzatuvchi uchun tasodifiy kattaliklari majmui. $\{x,h,r_V,\{m_P\},\{m_V\}\} = M_V(x,h)$ - buzg'unchi tomonidan mustaqil ravishda bajarilgan polinomial modellashtiruvchi algoritm ishining natijasi sifatida olingan tasodifiy kattaliklari majmui [10].

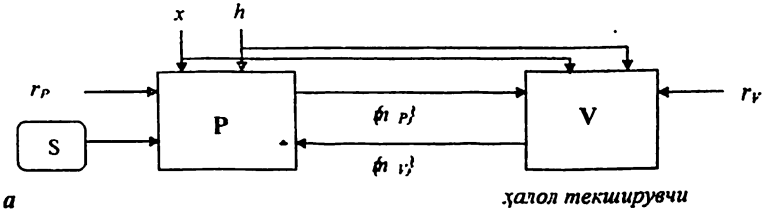
Agar $view_{P,V}(x,h) \overset{c}{\approx} M_V(x,h)$ kattaliklar polinomial vaqt oralig'ida hisoblanishlari ajratilmaydigan (ya'ni bu ikki tasodifiy kattaliklar majmuini polinomial vaqt oralig'ida tanib oladigan algoritm mavjud emas) bo'lsa, u holda protokol e'lon qilinganligi nol hisoblanishga teng bo'lgan bilishni ta'minlaydi deyiladi (4.2-rasm).

Agar $view_{P,V}(x,h) \overset{c}{\approx} M_V(x,h)$ kattaliklar tasodifiy kattaliklar ustida tekis taqsimlangan bo'lsa, u holda protokol e'lon qilinganligi absolyut nolga teng bo'lgan bilishini ta'minlaydi deyiladi.

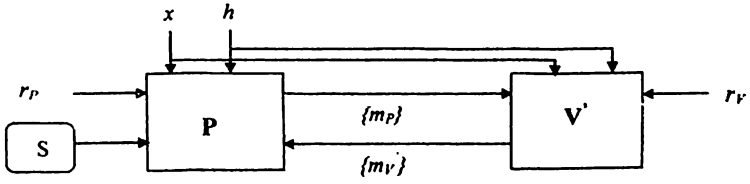
$\langle P,V,S\rangle$ tizim L tilda e'lon qilinganligi nolga teng bo'lgan bilishni interfaol isbotlash tizimi deyiladi, agar:

1) L til uchun interfaol isbotlash tizimi (ya'ni to'lalik va korrektlik xossalariga ega) bo'lsa;

2) e'lon qilinganligi nolga teng bo'lgan bilish xususiyatiga ega bo'lsa.



а *ҳалол текширувчи*



б **М** *бузғунчи*

4.2- rasm. E'lon qilinganligi nolga teng bo'lgan bilish protokolidagi kuzatiladigan tasodifiy kattaliklar: ***а*** – buzg'unchi protokolni chetdan kuzatadi; ***b*** – buzg'unchi o'zi mustaqil protokol modellashtiradi.

Faraz qilaylik, S - tasdiq ko'rinishi $w \in L$, bunda w - so'z, L- ikkilik alifbosidagi til bo'lsin. L til e'lon qilinganligi nolga teng bo'lgan bilishni interfaol isbotlash tizimiga ega deyiladi, agar:

1) L til uchun interfaol isbotlash tizimi $\langle P,V,S\rangle$ mavjud bo'lsa;

2) ixtiyoriy polinomial cheklangan ishtirokchi V' uchun $\langle P,V',S\rangle$ interfaol protokoli L tilda e'lon qilinganligi nolga teng bo'lgan bilishni interfaol isbotlash tizimi bo'lsa.

E'lon qilinganligi absolyut nolga teng bo'lgan bilishni isbotiga ega bo'lgan tillar sinfini PZK deb, nol hisoblanishga ega bo'lganini - ZK deb belgilanadi.

Quyida e'lon qilinganligi nolga teng bo'lgan protokolga misol sifatida Fiat-Shamir protokoli keltiriladi.

Bu protokolda **P** ishtirokchisi **V** ishtirokchiga isbotlaydigan bilim (sir) sifatida quyidagi sonni keltirish mumkin:

$$s \in_r \{2,\ldots,n-2\}$$

Bu yerda:

- $n = pq$ ko'rinishidagi ochiq son, p, q – uzunligi ≥ 512 bit bo'lgan maxfiy tub sonlar;
- **V** ishtirokchi $v := s^2$ sonni biladi.

Kriptografik protokol har biri quyidagi ko'rinishga ega bo'lgan t raunddan iborat (quyidagi barcha amal va taqqoslashlar *mod n* bo'yicha bajariladi):

1. $P \to V : x := z^2$, bu yerda $z \in_r \{1, \ldots, n-1\}$
2. $V \to P : b$, bu yerda $z \in_r \{0,1\}$ (b - bu savol)
3. $V \to P : y := z \cdot s^b$

(ta'kidlash kerakki, **P** ishtirokchi s qiymatini oshkor qilmaydi, chunki z tasodifiy son va uni **P** dan boshqa hyech kim bilmaydi)

4. Agar $y^2 = x \cdot v^b$ bo'lsa, **V P** ning javobini qabul qiladi

P ning s ni bilmasdan autentifikasiyadan muvaffaqiyatli o'tish ehtimolligi 2^{-t} dan oshmaydi, chunki

- Agar **P** s ni bilsa, u hamma savollarga to'g'ri javob beradi.
- Agar **P** s ni bilmasa, u holda **P** ning muvaffaqiyatli javob berish ehtimolligi bir raundda 1/2 ga teng va modomiki, har bir raund mustaqil ekan, u holda **P** ning hamma raundda xato qilmaslik ehtimolligi bir raundda **P** ning muvaffaqiyatli javobining ehtimolliklari ko'paytmasiga teng, ya'ni 2^{-t}.

Shuni aytish lozimki, hatto KP ish jarayonida **P** va **V** ishtirokchilari almashinadigan xabar buzg'unchi tomonidan qo'lga kiritilsa ham, undan s qiymatining qaysi maydonda yotishi haqida xech qanday axborot olib bo'lmaydi. Bu $n=pq$ uchun $\sqrt{x}$ funksiyasini Z_n da hisoblash murakkabligini isbotlaydi, bu yerda p va q – noma'lum tub sonlar (agar p va q ma'lum bo'lganda edi, u holda bu funksiyani hisoblash oson bo'lar edi).

Bunday turdagi kriptografik protokollar *nolinchi oshkoralikning isbotini* ifodalaydi.

4.2. Matematik masalalarni yechish protokollari

4.2.1. Kompyuterlarni sotish bo'yicha kriptografik protokollar

A ishtirokchida kompyuter bor, V ishtirokchida esa pul bor. V ishtirokchi A ishtirokchidan kompyuter sotib olmoqchi. Mazkur maqsadga erishish uchun bajarilishi lozim bo'lgan amallar quyidagi ko'rinishga ega bo'lishi mumkin [32]:

1. $A \rightarrow B$: kompyuter;
2. $B \rightarrow A$: pul.

Modomiki A ishtirokchi va B ishtirokchi bir-biriga ishonmas ekan, u holda

- A ishtirokchi avval 2, keyin 1 bo'lishini hohlaydi;
- V ishtirokchi esa avval 1, keyin 2 bo'lishini hohlaydi.

Bu muammoning yechimlaridan biri sifatida A ishtirokchi va V ishtirokchidan tashqari T ishonchli vositachi tomon qatnashadigan KP bo'lishi mumkin. Talab qilinayotgan KP quyidagi ko'rinishga ega bo'lishi mumkin:

- $A \rightarrow T$: kompyuter;
- $B \rightarrow A$: pul;
- $A \rightarrow T$: quyidagilar haqida tasdiq yoki raddiya:
  - V ishtirokchidan olingan pul kompyuter narxiga mosligi;
  - pul haqiqiyligi;
- $T \rightarrow B$: (A ishtirokchidan tasdiq keldimi) ? kompyuter;
- $T \rightarrow A$: (A ishtirokchidan raddiya keldimi) ? kompyuter.

Bu KP A ishtirokchi va V ishtirokchi uchun quyidagi sabablarga ko'ra ma'qul keladi:

- A ishtirokchi ishonadiki:
  - A pulni tekshirguncha T kompterni V ishtirokchiga berib yubormaydi;
  - T kompyuterni A ishtirokchiga qaytarib beradi, agar V ishtirokchi A ishtirokchiga yetarli pul bermasa yoki pul haqiqiy bo'lmasa.
- V ishtirokchi ishonadiki:
  - A ishtirokchi T ga tasdiqni yuborguncha, kompyuter T da bo'ladi.

– A ishtirokchi T ga tasdiqni yuborishi bilan T V ishtirokchiga kompyuterni berib yuboradi.

4.2.2. Tushlik qilayotgan kriptograflar

Keyingi misolni ko'rib chiqamiz.

Stol atrofida uchta kriptograf tushlik qilishmoqda. Ular tushlik qilib, pulini to'lashmoqchi bo'lishganda ofisiant tushlik uchun to'liq pul to'langanligi aytadi, lekin aynan kim to'laganligini aytmaydi [32].

Ikki variantdan biri bo'lishi mumkin:

1. Tushlik pulini kriptograflardan biri to'lagan.
2. Tushlik pulini vakolatli organ to'lagan.

Kriptograflar variantlardan qaysi biri ekanligiga ravshanlik kiritish niyatida bo'lsalar, birinchi varint bo'lgan holda pul to'lamagan ishtirokchilar kim pul to'laganini bilmasliklari kerak bo'ladi.

Bu masalani yechish uchun quyidagi protokolni taklif etish mumkin:

Madomiki, ishtirokchilar stol atrofida o'tirishar ekan yonma–yon o'tirgan juftlik o'zaro tanga tashlashi mumkin. Natija esa faqat ikkisiga ma'lum bo'lishi kerak.

Uchta juftlik tanga tashlab bo'lganidan keyin har bir ishtirokchi ikki marta tanga tashlash natijasini (reshka yoki orel) biladi. Bu natijalar quyidagilar bo'lishi mumkin:

- bir xil (tanga tashlanganda ikki marta ham tanganing bir tomoni tushgan bo'lishi);
- turlicha (tanga tashlanganda ikki marta tanganing ikki tomoni tushgan bo'lishi).

Har bir ishtirokchi boshqalarga "bir xil" yoki "turlicha" gapiradi, bunda kim pul to'lagan bo'lsa o'sha teskarisini tasdiqlaydi (ya'ni agar "bir xil" gapirish kerak bo'lsa, u "turlicha" gapiradi va teskarisi).

4.2.3. Qabul qilinganlik haqida tasdiq protokoli

Keyingi misolni ko'rib chiqamiz: A va V ishtirokchilar xabarni shifrlash uchun simmetrik shifrlash tizimini ishlatishmoqda, bu holda har bir qabul qilinadigan xabarni to'g'ri yuborishni boshqarish uchun xabar

yuboruvchiga qayta uzatiladi (yuboruvchi xabarning buzilmagan holda yetib borganligini aniq bilishi uchun) [32].

Ishtirokchilar buning uchun quyidagi KPdan foydalanadilar.

1. $A \to B$: $K_B^+(K_A^-(m))$.
2. $V \to A$: $K_A^+(K_B^-(m))$.

(Olingan xabar qabul qilinganlik sifatida tasdig'i yuboriladi).

Afsuski, bu KP quyidagi hujumlarga zaifdir. Aktiv buzg'unchi **M** birinchi xabarni ushlab olishi mumkin.

- $M \to B$: $K_B^+(K_A^-(m))$,
- $V \to M$: $K_M^+(K_B^-(K_M^+(K_A^-(m))))$.

Natijada **M** *m* xabarini qo'lga kritadi.

4.2.4. Matematik masalalarni yechish protokollari

O'rtacha qiymatni hisoblash protokoli

$\mathbf{A_1},\ldots, \mathbf{A_n}$ ishtirokchilar mos ravishda $a_1,\ldots, a_n$ sonlariga ega. Ular $\frac{1}{n}\sum_{i=1}^{n} a_i$ ni hisoblashmoqchi va bu holda har bir $\mathbf{A_i}$ ishtirokchi o'zining a_i sonini oshkor qilishni xohlamaydi.

Bunday masalani navbatdagi KP yordamida yechish mumkin:

1. $A_1 \to A_2 : K_{A_2}^+(a_1 + N)$, bunda $N \underset{r}{\in} Z$,

("$\underset{r}{\in}$" simvol elementning ixtiyoriy tanlanganligini bildiradi, ya'ni $x \underset{r}{\in} X$ belgilar birikmasidagi x ixtiyoriy bo'lib, X to'plamining teng ehtimollik bilan tanlangan elementidir).

2. $A_2 \to A_3 : K_{A_3}^+(a_2 + a_1 + N)$.
3. $A_3 \to A_4 : K_{A_4}^+(a_3 + a_2 + a_1 + N)$.
4. ...
5. $A_n \to A_1 : K_{A_1}^+(a_n + \ldots + a_1 + N)$.
6. $\mathbb{A}_1$ olingan natijadan N ni ayiradi va n ga bo'ladi.

Ikki sonni taqqoslash protokoli

Ushbu KP quyidagi masalani yechish uchun mo'ljallangan: **A** va **V** ishtirokchilar mos ravishda a va b sonlarga ega. Ular a va b sonlarini

oshkor qilmasdan (ma'lum qilmasdan) turib $a \le b$ shartini to'g'riligini tekshirishmoqchi.

Quyida shu masalani kriptografik protokoli bayon qilingan. $a,b \in \{1,...,100\}$ deb faraz qilamiz.

1. $A \to B: c - a$, bunda $c = K_B^+(x)$ va $x \in Z$.
2. **B** tub bo'lgan p sonni generasiyalaydi va quyidagini hisoblaydi:

$$\{c_i := K_B^-(c - a + i)\%p \mid i = 1,...,100\}$$

B quyidagi shartlarni tekshiradi:

- $\forall i \ne j$ uchun $|c_i - c_j| \ge 2$;
- $\forall i$ uchun $0 < c_i < p - 1$.

Agar bu shartlar bajarilmasa, u holda qadam (boshqa p bilan) takrorlanadi.

3. $B \to A: c_1,..... c_b, c_{b+1} + 1,.... c_{100} + 1, p$,

(bu sonlar hammasi turlicha).

Agar $c_i = c_j$ bo'lsa, u holda $i \le b < j$ va **A** uni bilib oladi.

4. $A \to B$: javobi $= (a \le b)$ bo'ladi, agar $x = a$, ya'ni bu ketma-ketlikning a-chi elementi bo'lsa.

Kamchilgi: ishtirokchilarning haqqoniyligi boshqarilmaydi.

Bu KPni sirli auksion KP ishlab chiqish uchun ishlatish mumkin.

4.2.5. O'ziga xos protokollar

Autentifikasiyalash protokollari va kalit almashish protokollari – kriptografik protokollarning ayniqsa ko'p sonli sinflaridir. Shuningdek, boshqa maxsus masalalarni yechishga qaratilgan boshqa bir qator protokollar ham mavjud:

Ovoz berish protokollari. Bu protokollar saylovlarni o'tkazishni ta'minlash uchun mo'ljallangan bo'lib, uning davomida har bir ishtirokchi o'z ovozini anonim xolda berishi mumkin. Bunda hyech qaysi ishtirokchi o'z ovozini ikki marta berishi mumkin emas; faqat ro'yxatga olingan ishtirokchilar ovoz berishi mumkin; har bir ishtirokchi o'zining ovozi to'g'ri hisobga olinganligini tekshirishi mumkin.

Xavfsiz ovoz berish protokoli ikkita ishonchli ishtirokchi – ovoz beruvchini tekshirish agentligi T_1 va ovoz berish natijalarini chiqarish agentligi T_2 ni qo'llashga asoslanadi. Ovoz berishdan avval T_1 ishtirokchi

T_2 ga barcha ruxsat berilgan ishtirokchilar identifikatori ro'yxatini yuborishi kerak. Har bir ovoz beruvchi (i) T_1 ga biron bir uni identifikasiyalovchi ma'lumotni yuboradi, so'ngra, agar ovoz beruvchiga ovoz berishga ruxsat berilgan bo'lsa, T_1 unga ovoz beruvchining identifikasiyasi - $E_1(i)$ ni yuboradi va saylovda ishtirok etish faktini qayd qiladi. So'ngra ovoz beruvchi maxfiy identifikator $E_2(i)$ ni va ovoz berish natijasi $E_3(i)$ ni hisoblaydi va T_2 ga $(E_1(i), E_2(i), E_3(i))$ to'plamni yuboradi. T_2 $E_1(i)$ ni ovoz berishi ruxsat berilgan identifikatorlar ro'yxatida bor yo'qligini tekshiradi; agar bor bo'lsa, $E_2(i)$ ni $E_3(i)$ ga ovoz beruvchilar ro'yxatiga qo'shib qo'yadi. $E_1(i)$, $E_2(i)$ va $E_3(i)$ almashtirishlar nosimmetrik algoritmlarga yoki bir tomonlama funksiyalarga asoslangan.

Bir vaqtda imzolash protokollari. Ishtirokchilarning maqsadi: har bir ishtirokchi agar u biror bir hujjatni imzolasa boshqa ishtirokchi ham shunday qilishi kafolatiga ega bo'lishi kerak. Bunda ishtirokchilar bir biridan ma'lum masofada bo'lishi va hujatni ERI yordamida imzolashi mumkin.

Jamoaviy imzolash protokoli. Faqat jamoa a'zolarigina xabarni imzolashlari mumkin, bunda imzoni qabul qiluvchi xabar jamoa a'zosi tomonidan imzolanganiga ishonch hosil qilishi mumkin, ammo kim tomonidanligini aniqlay olmaydi. Shunday bo'lsada, munozara vaqtida imzo imzolovchining shaxsini aniqlash maqsadida ochilishi mumkin.

Rad qilib bo'lmaydigan imzo. Uni tekshirish uchun imzolovchining ruxsati kerakligi bilan oddiy elektron raqamli imzodan farq qiladi.

Ko'r-ko'rona imzo. ERI ning xususiyatlariga ega bo'lib, imzolanayotgan hujjatning mazmuni bilan tanishi mumkin bo'lmay imzolash (masalan: merosni notariusda tasdiqlash).

Maxfiylikni bo'lish protokoli. Xabarni jamoa a'zolari orasida bir necha qismga shunday taqsimlanadiki, bunda jamoaning har bir a'zosi o'zining qismidan hyech qanday ma'lumot ola olmaydi, faqat jamoa a'zolari o'zaro birga yig'ilibgina, xabarni o'qiy olishadi.

Maxfiylikni bo'lishning eng keng tarqalgan protokoli XOR amali bilan qo'shilgandagina dastlabki xabarni beradigan mazmunsiz xabarlar to'plamini generasiya qiluvchi arbitr qatnashishini talab qiladi. Masalan, ikki ishtirokchi orasidagi xabarni bo'lish uchun arbitr o'sha dastlabki xabar M uzunlikdagi tasodifiy sonni R generasiya qiladi, so'ngra

$R \oplus M = S$ ni hisoblaydi. R va S qismlar ishtirokchilarga tarqatiladi. Boshlang'ich xabarni olish uchun esa $R \oplus S = M$ amali bajariladi.

4.3. Shartnoma imzolash protokollari

4.3.1. Shartnoma imzolash protokollarining turlari

Shartnoma imzolash protokollaridan **A** va **V** ishtirokchilar bir-biriga ishonch bildirmagan, ammo ba'zi bir shartnomalarga birgalikda imzolashi lozim bo'lgan holatlarda foydalaniladi. Bu masalaning oddiy yechimi quyidagicha amalga oshirilishi mumkin [32]:

- ishtirokchilardan biri shartnomani imzolaydi;
- imzolangan shartnoma boshqa ishtirokchiga shartnomani yana imzolash uchun yuboriladi.

Bu yechim ikkala ishtirokchini ham qanoatlantirmaydi, chunki olingan shartnoma hamkori tomonidan imzolanmay qolishi mumkinligini oldini olmaydi.

Shartnoma imzolash protokollarining ishonchli vositachi va vositachisiz turlaridan foydalaniladi.

Ishonchli vositachi bilan shartnoma imzolash protokoli

Bu protokol quyidagi bosqichlarni o'z ichiga oladi:

1. $A \to T : S_A(m)$ (t- shartnoma) yuboradi;
2. $B \to T : S_B(m)$ yuboradi;
3. $T \to A$: $S_B(m)$ ni olganligi to'g'risidagi ma'lumotni yuboradi;
4. $T \to B$: $S_A(m)$ ni olganligi to'g'risidagi ma'lumotni yuboradi;
5. $A \to B : S_A(m)$ yuboradi;
6. $B \to A : S_B(S_A(m))$ ni o'zida ikkinchi imzolangan nus'hasini olib qolib yuboradi;
7. $A \to T$: ikkita ishtirokchi tomonidan imzolangan shartnoma olganligi to'g'risidagi ma'lumotni yuboradi;
8. $B \to T$: ikkita ishtirokchi tomonidan imzolangan shartnoma qo'lida borligi to'g'risidagi ma'lumotni yuboradi;
9. T: o'zida mavjud bo'lgan ikkita nusxani yo'qotadi.

Vositachisiz shartnoma imzolash protokoli

Bu KP da simmetrik shifrlash tizimi qo'llaniladi. Protokol quyidagi bosqichlardan iborat:

1. **A** p ta kalitlar juftligini $\{(KA_i^L, KA_i^R) \mid i = 1,...n\}$ va p ta $\{(MA_i^L, MA_i^R) \mid i = 1,...n\}$ ko'rinishdagi xabarlar juftligini generasiyalaydi, bunda har bir xabar $S_A(m)$ ga ega;

2. **V** p ta kalitlar juftligini $\{(KB_i^L, KB_i^R) \mid i = 1,...n\}$ va p ta $\{(MB_i^L, MB_i^R) \mid i = 1,...n\}$ ko'rinishdagi xabarlar juftligini generasiyalaydi, bunda har bir xabar $S_B(m)$ ga ega;

3. $A \to B: \{\begin{pmatrix} KA_i^L(MA_i^L) \\ KA_i^R(MA_i^R) \end{pmatrix} \mid i = 1,...,n\}$ yuboradi;

4. $B \to A: \{\begin{pmatrix} KB_i^L(MB_i^L) \\ KB_i^R(MB_i^R) \end{pmatrix} \mid i = 1,...,n\}$ yuboradi;

5. $\forall i = 1,...,n \quad A \to B: \frac{1}{2}\{KA_i^L, KA_i^R\}$ yuboradi;

6. $\forall i = 1,...,n \quad B \to A: \frac{1}{2}\{KB_i^L, KB_i^R\}$ yuboradi;

7. **A** va **V** ishtirokchilar juftlikning komponentasi shifrini ochishga harakat qiladi, har bir juftlikda bitta komponentasining shifri ochiladi;

8. $\forall i = 1,...,n \quad \forall j = 1,...,n$
   - $A \to B$: i–bit KA_j^L, i–bit KA_j^R
   - $B \to A$: i–bit KB_j^L, i–bit KB_j^R;

9. **A** va **V** ishtirokchilar juftliklarning qolgan komponentasining shifrini ochishadi;

10. **A** va **V** ishtirokchilar protokolda qo'llanilgan yopiq kalitlar bilan almashishadi (haqqoniylikni tekshirish uchun).

Shartnoma imzolangan deyiladi, agar

$$\begin{cases} \exists i: \ A \ \text{эга} \ (MB_i^L, MB_i^R) \\ \exists j: \ B \ \text{эга} \ (MA_j^L, MA_j^R) \end{cases} \text{bo'lsa.}$$

4.3.2. Jamoaviy elektron raqamli imzo protokollari

4.2.5-paragrafda keltirilgan o'ziga xos protokollarning orasida jamoaviy elektron raqamli imzo (JERI) protokollaridan elektron hujjat aylanish, elektron to'lov tizimlarida va shartnomalar tuzishda foydalaniladi.

Elektron hujjat aylanish tizimlarining jadal sur'atlar bilan rivojlanishi jamoaviy elektron hujjatlar yuridik kuchini ta'minlashning

yangi mexanizmlarini ishlab chiqishni taqozo etadi. Shu jumladan jamoaviy loyihalarni ishlab chiqishda, elektron ovoz berishda, pasport haqiqiyligini ta'minlashda JERI protokollaridan foydalanish muhim ahamiyat kasb etadi.

Hozirgi paytda elektron hujjat aylanish tizimlarining xavfsizligini ta'minlash asosini ERI tizimlari bilan belgilanadi. ERIlar ikki asosiy kategoriya bo'yicha tasniflanadi: shaxsiy ERI va jamoaviy ERI. Bitta hujjatga bir ishtirokchi imzo qo'ysa, shaxsiy ERI deyiladi. Agar hujjatga bir necha ishtirokchi imzo qo'ysa, bunday ERI JERI deyiladi.

ERIning eng ko'p foydalaniladigan turi [33] shaxsiy imzo bo'lib, undan zamonaviy elektron hujjat aylanish tizimlarida foydalanilganda faqat birgina mushtariy imzolovchi sifatida qatnashadi, bu esa bir necha imzolovchi an'anaviy tarzda qatnashganda ERI o'lchami imzolovchilar soniga proporsional sur'atda ortib ketishiga olib keladi. Shuningdek imzoni tekshirish jarayoni ham har bir imzolovchining imzosini alohida tekshirishni talab etadi.

Shu kungacha ma'lum bo'lgan an'anaviy elektron raqamli imzo protokollari "karrali imzo" (direktor, buxgalter, yetakchi muhandis va sh.k.) yaratishga imkon beradi. Imzolovchi jamoa a'zolari qancha ko'p bo'lsa, imzo o'lchami ham shuncha ko'p bo'ladi va bunda imzo qo'yuvchilar va tekshiruvchilar ketma-ketliklarining tartiblari bir xil bo'lishi shart.

Amaliyotda ERIdan bunday taxlitda foydalanish usuli har qachon ham zarur bo'lavermaydi. Ayniqsa, ERI biror jamoa ishtirokchilaridan shakllantirilishi lozim bo'lganda, jamoaviy oshkora kalit tushunchasidan foydalanib, ERI hosil etish qulaydir. Bunda ERI protokoli soddalashadi, ERI o'lchami va uni shakllantirish, hamda tekshirish jarayonlariga vaqt sarfi an'anaviy ERIdan foydalanilganidan ortiq bo'lmaydi.

Ko'rsatib o'tilgan kamchiliklarni bartaraf etish uchun [42-45]da yangi protokollar taklif etilgan. JERI protokollari bir vaqtning o'zida shartnomalarni va hujjatlar paketini imzolash muammosini hal etish uchun eng samarali vosita bo'lib, imzolangan hujjatlardan amalda tezroq foydalanish imkoniyatini yaratadi.

JERI protokolining afzalliklari quyidagilardan iborat :

- JERI o'lchami oddiy ERIniki bilan teng bo'lib, ishtirokchilar soniga bog'liq bo'lmaydi;

- protokol ishtirokchilarining maxfiy kalitidan xabardor bo'lgan ishonchli shaxs mavjud emas;
- qisqartirilgan va kengaytirilgan JERIni hisoblash mumkin emas.

JERI protokollarida shaxsiy oshkora kalitlar asosida shakllantiriladigan jamoaviy umumiy oshkora kalitdan foydalaniladi. Bu holda Internetda e'lon qilinadigan standart ma'lumotnomalaridan va oshkora kalit sertifikatlaridan foydalanish nazarda tutiladi.

1983 yilda Itakura va Nakamura [46] birinchi bo'lib JERIni taklif qilishgan. Unda bir qancha imzolovchilar tomonidan bitta xabarga jamoa tarzida imzo qo'yiladi va hosil bo'lgan ERI tekshiruvchilar guruhi tomonidan haqiqiylikka tekshiriladi. Shundan keyin bir qancha JERIlar taklif qilingan [46-55].

JERIdan foydalanishda imzoni soxtalashtirishni oldini olish maqsadida qog'ozli formatda shtrix-kod ko'rinishida yozishda imzo o'lchamini minimallashtirish ham muhim ahamiyatga ega. Bu maqsadda JERIning yangicha protokollarini ishlab chiqish lozim bo'ladi.

JERI protokollariga quyidagi talablar qo'yiladi:

1. Yaxlitlik:
   - JERIdan biror bir kengaytirilgan va boshqa to'g'ri ERIni hisoblab topish mumkin bo'lmasligi;
   - JERIni generasiyalashning oraliq bosqichlarida hosil bo'ladigan qiymatlar biror bir hujjat uchun to'g'ri kelmasligi.
2. ERI algoritmining kriptografik yadrosi o'zgarmas bo'lishi:
   - JERI mavjud standartlar asosida shakllantiriladi.

JERI jamoaviy maxfiy kalitlar haqidagi bilim yordamida ko'p sonli imzolovchilar tomonidan imzolanadi va hamma imzolovchilarning oshkora kalitlari asosida tekshiriladi.

Samarali JERI sxemasi muayyan xabarga qo'yilgan ko'plab shaxsiy ERIlarini yagona JERIda mujassamlashtiradi va bunday ERI samarali tekshirilishi mumkin.

JERI sxemasi bu ichki siyosatni samarali amalga oshirishni ta'minlaydi. Masalan, kompaniya siyosati bir qancha menejerlardan ixtiyoriy savdo shartnomasini imzolashni talab etishi mumkin. Har bir menejer kompaniya siyosatiga mos shartnomani imzolash uchun o'zining maxfiy kalitidan foydalanishi shart va hamma individual ERIlarni yagona JERIga birlashtirish mumkin. Biroq, ixtiyoriy tashqi ERI tekshiruvchilari

uchun bu JERI kompaniyaning oshkora kaliti yordamida tekshirilishi mumkin bo'lgan oddiy ERI hisoblanadi. Kompaniyaning oshkora kaliti - hamma imzolovchilarning oshkora kalitlari mahsulidir.

Xarn [56-58] hamma shaxsiy ERIlarni ma'lumotlar hajmi ortmaydigan yagona JERIga birlashtiradigan El Gamal tipidagi ikkita variantni taklif qilgan. Unda jamoaviy imzoning uzunligi har bir individual imzoning uzunligiga teng.

Bu natija jamoaviy imzolarning hajmi jalb qilingan imzolovchilarning soniga emas, faqat imzo sxemasining xavfsizlik parametrlariga bog'liq bo'lgandagina o'rinlidir. Ko'p imzolovchilar ko'p yopiq kalitlar haqidagi bilimi yordamida doimiy uzunlikdagi raqamli imzoni shakllantirishi mumkin.

JERI sxemasi quyidagi xususiyatlarga ega:

1.JERI uzunligi o'zgarmas.

2.JERIni har birini alohida tekshirishni o'rniga bir marta tekshirish mumkin.

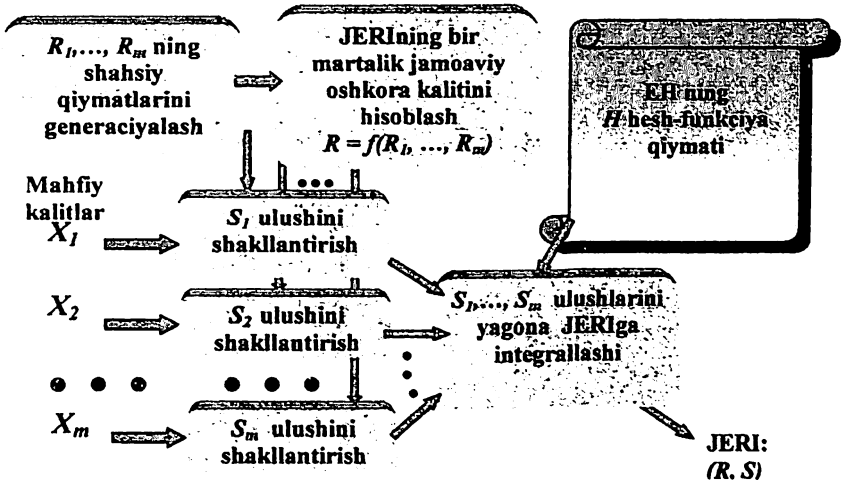
3.JERIga biriktirilgan oshkora kalit barcha alohida oshkora kalitlarning natijasidir.

(1) xususiyat JERIlarning aloqa va xotiraga zarur sarf-harajatlarni minimallashtiradi. (2) xususiyat tekshirish jarayoni tezligini ko'p marta oshiradi. (3) xususiyat shu paytgacha har bir imzolovchining oshkora kalitini o'zida saqlashi kerak bo'lgan oshkora kalitning hajmini kamaytiradi.

Mavjud JERI algoritmlari asosan quyidagi muammolarni yechish murakkabligiga asoslangan:

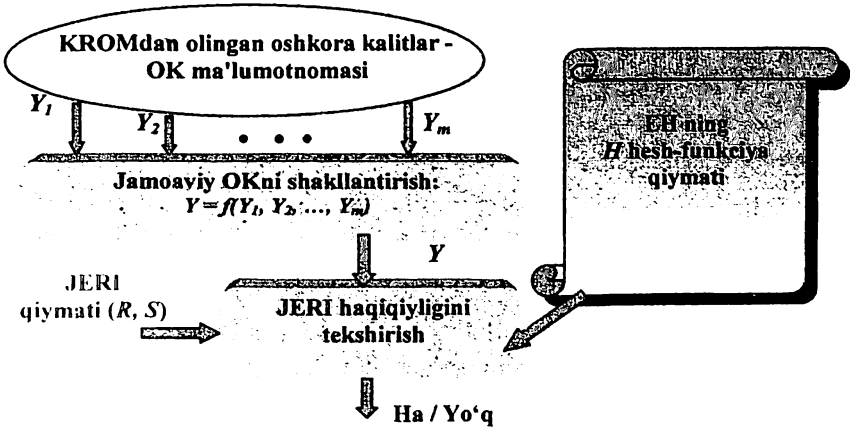
- katta tub modul bo'yicha katta tub ko'rsatkichli ildizdan chiqarish;
- katta tub tartibli multiplikativ gruppada diskret logarifmlash;
- maxsus ko'rinishdagi elliptik egri chiziq nuqtalari gruppasida diskret logarifmlash.

JERI shakllantirishning umumiy sxemasi quyidagi 4.3-rasmda keltirilgan. Bu yerda $R_1, ..., R_m$ - shaxsiy oshkora kalitlar, $X_1, X_2, ..., X_m$ - maxfiy kalitlar, $S_1, ..., S_m$ - ishtirokchilarning JERI ulushlari, *(R, S)* juftligi – JERI, EH – elektron hujjat.



4.3- rasm. JERI shakllantirishning umumiy sxemasi

JERI haqiqiyligini tekshirishning umumiy sxemasi quyidagi 4.4-rasmda keltirilgan.



4.4- rasm. JERI haqiqiyligini tekshirishning umumiy shemasi

Bu yerda Y - jamoaviy oshkora kalit, Y_1, Y_2, ..., Y_m - shaxsiy oshkora kalitlar, (R, S) juftligi – JERI, KROM – kalitlarni ro'yxatga olish markazi, OK – oshkora kalit.

4.3.3. Hujjatlar paketiga jamoaviy imzo shakllantirish

ERIni shakllantirish jadal hisoblashlarni talab qilganidek, maxsus qurilma yoki samarali dastur algoritmini qo'llash yordamida bu hisoblashlarni tezlashtirish maqsadga muvofiqdir. Hujjatlar paketiga jamoaviy imzo qo'yish bir qancha qabul qiluvchilar uchun mo'ljallangan xabarlarga imzolovchining bir vaqtda imzo qo'yishiga imkon beradi. Shunday qilib, bu imzo qo'yish vaqtini ko'p marta kamaytiradi. Endi hujjatlar paketiga jamoaviy imzo qo'yish sxemasining muhim xossalarini umumlashtiramiz:

1. Hujjatlar paketiga jamoaviy imzo qo'yish sxemasi bir vaqtda ko'p xatlarni imzolashga imkon yaratadi.

2. Hujjatlar paketiga qo'yilgan jamoaviy imzo haqiqiylikka har bir qabul qiluvchi ishtirokchi tomonidan alohida tekshirilishi mumkin.

3. Jamoaga taalluqli bo'lmagan xabarlar aloqador bo'lmagan tekshiruvchi ishtirokchilarga ochilishi mumkin emas.

1-xossa hujjatlar paketiga jamoaviy imzo qo'yish sxemasining yutug'ini kafolatlaydi. 2-xossa shuni ta'kidlaydiki, hujjatlar paketining jamoaviy imzosi har bir qabul qiluvchi uchun odatdagidek alohida ERI kabidir. 3-xossa esa xabarlarning shaxsiyligini kafolatlaydi. Hujjatlar paketiga jamoaviy imzo qo'yish sxemasini ko'pincha ko'p sonli xabarlarni imzolashni talab qiladigan himoyalangan elektron tranzaksiyalar protokolida ishlatiluvchi to'lov shlyuzlariga (TSh) o'xshash dasturlarga qo'llasa bo'ladi.

Keltirilgan algoritmni ixtiyoriy ERI sxemasiga qo'llash mumkin. Keyingi misol ushbu algoritmni o'zida aks ettiradi.

Faraz qilaylik, to'lov tizimida TSh uchta har xil M_1, M_2, M_3 savdogarlar uchun mos ravishda uchta har xil m_1, m_2, m_3, xabarlarni imzolashi kerak. TShning oshkora kalitini e va yopiq kalitini d, yopiq kalit d va m xabarning bir ishtirokchi tomonidan xesh-qiymati $h(m)$ yordamida hosil qilingan m xabarning ERIsini $Imzo\{h(m)\}d$ deb belgilash kiritamiz.

TSh quyidagi qadamlarni amalga oshiradi:

1-qadam: $h(m_1)$, $h(m_2)$, va $h(m_3)$ lar hisoblanadi.

2-qadam: $h(h(m_1) \,||\, h(m_2) \,||\, h(m_3))$ hisoblanadi, bunda " || " ma'lumot konkatenasiyasi jarayonini ifodalaydi.

3-qadam: $Imzo\{h(h(m_1) \,||\, h(m_2) \,||\, h(m_3))\}d$ hisoblanadi.

4-qadam: $\{Imzo\{h(h(m_1) \,||\, h(m_2) \,||\, h(m_3))\}d,\ m_1,\ h(m_2),\ h(m_3)\}\ M_1$ qabul qiluvchiga yuboriladi.

$\{Imzo\{h(h(m_1) \,||\, h(m_2) \,||\, h(m_3))\}d,\ m_2,\ h(m_1),\ h(m_3)\}\ M_2$ qabul qiluvchiga yuboriladi.

$\{Imzo\{h(h(m_1) \,||\, h(m_2) \,||\, h(m_3))\}d,\ m_3,\ h(m_1),\ h(m_2)\}\ M_3$ qabul qiluvchiga yuboriladi.

M_1 TShdan $\{Imzo\{h(h(m_1) \,||\, h(m_2) \,||\, h(m_3))\}d,\ m_1,\ h(m_2),\ h(m_3)\}$ qabul qilib olinganidan so'ng quyidagilar amalga oshiriladi:

1-qadam: $h(m_1)$ ni hisoblanadi.

2-qadam: $h(m_1)$, $h(m_2)$, va $h(m_3)$ larni birlashtirish orqali $h(h(m_1) \,||\, h(m_2) \,||\, h(m_3))$ hisoblanadi.

3-qadam: 2-qadamda olingan $h(h(m_1) \,||\, h(m_2) \,||\, h(m_3))$ va TShning oshkora kaliti yordamida qabul qilingan $Imzo\{h(h(m_1) \,||\, h(m_2) \,||\, h(m_3))\}d$ ning haqiqiyligi tekshiriladi.

M_2 va M_3 ham xuddi yuqoridagi qadamlarni mos ravishda o'ziga tegishli xabarning shaxsiy imzosini tekshirishi mumkin.

Yuqorida jamoa uchta savdogardan iborat hol uchun usul bayon etildi. Bu usuldan ixtiyoriy jamoa n ta a'zoga ega bo'lgan holda ham foydalanilishi mumkin.

$h(m_2)$ va $h(m_3)$ lar M_1 ga m_1 xabarning ERIsini tekshirish uchun yuborilgan bo'lsada, m_2 va m_3 xabarlar M_1 muallifiga hyech qachon ma'lum bo'lmaydi. Bu xavfsizlik talabiga javob beradi, chunki maxfiy hujjatlar taalluqsiz qabul qiluvchiga ma'lum bo'lmasligi lozim. Boshqa tarafdan, xabarlar uchun to'g'ri imzoni generasiya qilish uchun d yopiq kalit kerak bo'ladi. Bu ERIning xavfsizlik talabini qondiradi.

Har bir maxfiy xabarni alohida imzolash o'rniga, bu algoritm to'lash shlyuziga uchta xabarni bir vaqtda imzolanilishiga imkon beradi. Umuman olganda, xesh-funksiyani hisoblash vaqti imzoni hosil etishga nisbatan juda oz farq qiladi. Shuning uchun bu algoritm jamoaviy imzoni generasiyalash vaqtini tejaydi. Agar to'lov shlyuzi bir vaqtda $n>2$ ta xabarga imzo shakllantirsa, unda ko'proq tejamkorlikka erishish mumkin. Lekin tarmoq orqali uzunroq xesh-qiymatni tarqatish kerak bo'ladi.

4.3.4. Xarnning hujjatlar paketiga jamao tomonidan qo'yilgan imzo haqiqiyligini tasdiqlash

Hujjatlar paketiga qo'yilgan jamoaviy imzo haqiqiyligini tasdiqlash bitta imzolovchi tomonidan imzolangan ko'p ERIlarni tasdiqlashga imkon beradi. Bu ERI haqiqiyligini tasdiqlash vaqtini ko'p marta kamaytiradi. Hujjatlar paketiga qo'yilgan jamoaviy imzo haqiqiyligini tasdiqlash xossalari quyidagicha umumlashtiriladi:

1. Ko'p sonli imzolar bir vaqtda haqiqiylikka tekshirilishi mumkin.
2. Hujjatlar paketiga qo'yilgan jamoaviy imzo haqiqiyligini tekshirish vaqti o'zgarmas songa teng.

Hujjatlar paketiga qo'yilgan jamoaviy imzo haqiqiyligini tasdiqlash dasturi sertifikatlashtirish markazi tomonidan imzolanadigan X. 509 oshkora kalit sertifikatini [59] haqiqiyligini tekshirishni talab qiladigan trafigi yuklangan shlyuzlarda topilishi mumkin.

Nakache va boshqalar tomonidan interaktiv DSAga aoslangan hujjatlar paketining jamoaviy imzosi haqiqiyligini tasdiqlash protokoli taklif etilgan. Unda imzolovchi bir paytda tekshiruvchi bilan o'zaro aloqada bo'lgan holda t ta ERIlarni generasiya qiladi, keyin esa tekshiruvchi hujjatlar paketining jamoaviy imzosi haqiqiyligini tasdiqlash xususiyatiga asoslanib t. ta ERI haqiqiyligini tekshiradi. Nakache tomonidan taklif etilgan interaktiv DSAga aoslangan hujjatlar paketining jamoaviy imzosi haqiqiyligini tasdiqlash protokolini Lim va Li [60] xavfsiz emas deb ko'rsatib o'tishgan. Xarn [61] xavfsiz DSA tipli hujjatlar paketining jamoaviy imzosi haqiqiyligini tasdiqlash algoritmini taklif etgan.

4.3.5. Jamoaviy elektron raqamli imzoning umumlashgan sxemasi

Quyida GOST R. 34.10-2001 va Shnorr sxemalari asosida shakllantirish va tekshirish usulining umumlashgan sxemasi bayon etilgan (4.5-rasm).

Bayon etilayotgan usul uch bosqichni o'z ichiga oladi:

I bosqich - JERI shakllantirish, quyidagi qadamlardan tarkib topgan:

1. JERI birinchi qismi R ni shaxsiy parametr R_i lar asosida yaratib, unga jamoaviy parametr R ga akslantirish funksiyasini amalga oshirishdan iborat.

2. Shaxsiy kalitlarni yaratib, JERI ikkinchi qismi S ning ulushlarini shakllantirish.

3. Yagona JERI ikkinchi qismi S ga integrallash.

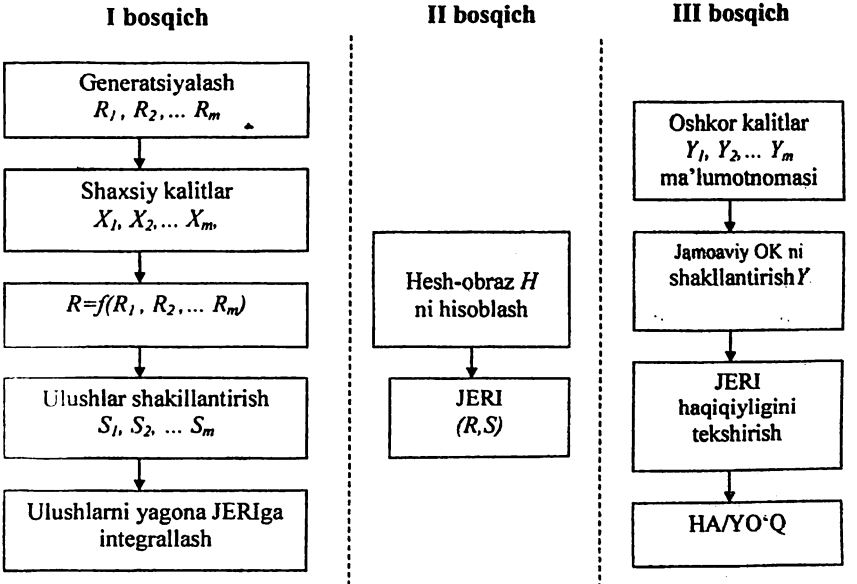
II bosqich - xesh-obrazni hisoblab, ikki qism *(R, S)* dan tarkib topgan JERI bilan imzolangan hujjatni tekshiruvchilarga jo'natish.

III bosqich - JERI xaqiqiyligini tekshirish:

1. Oshkora kalitlar ma'lumotnomasidan JERIni shakllantirishda qatnashgan foydalanuvchilarning oshkora kalitlari Y_i tanlanadi.

2. Tanlangan oshkora kalitlar asosida jamoaviy oshkora kalit Y shakllantiriladi.

3. JERI haqiqiyligi tekshiriladi va u haqikiy yoki haqiqiy emas deb qabul etiladi.



4.5- rasm. GOST R. 34.10-2001 va Shnorr shemalari asosida JERI shakllantirish va tekshirish usuli

An'anaviy va jamoaviy ERIlarni xarakteristikalarini taqqoslash shuni ko'rsatadiki, ularni generasiyalash murakkabligi bir xil bo'lib, JERIni tekshirish murakkabligi an'anaviy ERInikiga nisbatan m marta oson.

JERIni shakllantirish shartnomalarni imzolashda va imzolash huquqini boshqalarga berishda foydalaniladi. JERI bir necha muammolarni keng ma'noda yechishga imkoniyat beradi. Masalan, bir paytda shartnomalar paketini imzolash muammosini yechishda; bunda turli shartnomalar turli imzolovchilar guruhi tomonidan imzolanadi deb qaraladi. Buning afzalligi shundaki, JERIdan foydalanishda ERI o'lchami shaxsiy imzodagidek va imzolangan elektron aktlar va imzolovchilar soniga bog'liq emas. Bunday protokollar diskret logarifmlashning yoki maxsus strukturali tub modul bo'yicha ildiz chiqarish masalasining murakkabligiga asoslanadi. Bunda har bir ishtirokchi umumiy imzoda o'z ulushini shakllantirib, bu ulushlar o'ramasini JERI sifatida qabul etiladi. Shunday qilib, JERIni shakllantirish jarayonida barcha imzolovchilar bir paytda qatnashadilar.

JERI multiimzo (multisignature) deb ham ataladi. Ko'pchilik faktorlash va chekli katta tub tartibli gruppalarda diskret logarifmlash masalalarining murakkabligiga asoslangan ma'lum protokollarning kamchiligi shundaki, imzo ketma-ket shakllantiriladi. Bu o'z navbatida imzoni shakllantirish va tekshirishdagi oraliq bosqichlarda to'la bo'lmagan imzolovchilar qismiga taalluqli imzo shakllanadi. Bu esa protokollarga turli maxsuslashgan hujumlarni amalga oshirish imkoniyatini yuzaga keltiradi. Bunday kamchilikdan holi bo'lgan imzoni parallel shakllantirishga asoslangan JERI protokoli shartnomalar paketini bir vaqtda imzolashga, imzolovchilar tarkibini har xil qilib belgilashga imkon beradi.

Faktorlash masalasining murakkabligiga asoslangan JERIni bir vaqtda imzolash protokoli JERI shakllantirishda foydalaniladigan primitivlar sinfining kengayishiga olib kelib, JERIni buzish uchun ikkita bir-biriga bog'liq bo'lmagan masalalar juftligini yechishga to'g'ri keladi. Bunda n sonini va uncha katta bo'lmagan tub son k ga teng daraja ko'rsatkichi sonini Ro'yxatga Olish Markazi generasiyalaydi deb qaraladi.

JERI sxemalarining va protokollarining bardoshligi bir vaqtda o'zaro mustaqil bo'lgan ikkita masalaning, ya'ni diskret logarifmlashni chekli maydonda va elliptik egri chiziqlarda hal etish murakkabligiga

asoslansa, yakuniy bardoshlilik ortishiga erishilishi kriptograflar tomonidan asoslanganligi JERI protokollari uchun alohida ahamiyat kasb etadi.

Nazorat savollari

1. E'lon qilinganligi nolga tengligi isboti nima uchun ishlatiladi?
2. E'lon qilinganligi nolga teng bo'lgan bilishni isbotlashning qanday protokollarini bilasiz?
3. Graflarning izomorfligini tasdiqlovchi protokolini tushuntirib berng.
4. X sonining diskretlogarifmi x ni bilishning isboti protokolida sir sifatida nima ishtirok etadi?
5. Y sonini bazisdagi ko'rinishini bilishning isboti xususiyatlari nimadan iborat?
6. Sonlar to'plamining mos bazislardagi ko'rinishlarini bilishining isboti protokoli bilan "Deponirlangan" kattaliklarning multiplikativ bog'liqligini bilishning isboti protokoli orasida qanday farq bor?
7. Umumiy holda e'lon qilinganligi nolga teng bo'lgan interfaol isbotlash protokoli necha qadamdan iborat? Ularni yoritib bering.
8. Qachon L til e'lon qilinganligi nolga teng bo'lgan bilishni interfaol isbotlash tizimiga ega deyiladi?
9. E'lon qilinganligi nolga teng bo'lgan protokolga misol sifatida Fiat-Shamir protokolini izohlang.
10. Kompyuterlarni sotish bo'yicha kriptografik protokollar deganda nimani tushunasiz? U qanday jarayonlardan iborat?
11. Tushlik qilayotgan kriptograflar protokoli mohiyati nimadan iborat?
12. Qabul qilinganlik haqida tasdiq protokolining boshqa protokollardan afzalligi nimada?
13. Matematik masalalarni yechish protokollariga misollar keltiring va ularni tushuntirib bering.
14. Ikki sonni taqqoslash protokoli nima maqsadda qo'llaniladi?
15. O'ziga xos protokollarga qanday protokollarni misol sifatida keltira olasiz?
16. Jamoaviy imzolash protokoli nima?
17. Ko'r imzodan nima maqsadda foydalaniladi?

18. Maxfiylikni bo‘lish protokolining afzalligi nimada?
19. Shartnoma imzolash protokollarining qanday turlari mavjud?
20. JERI qayerda ishlatiladi?
21. ERI bilan JERIning nima farqi bor?
22. JERI protokollariga qanday talablar qo‘yiladi?
23. JERI sxemasi qanday xususiyatlarga ega?
24. JERI algoritmlari asosan qaysi muammolarni yechish murakkabligiga asoslanadi?
25. Hujjatlar paketiga jamoaviy imzo shakllantirish sxemasi qanday qulayliklarga ega?
26. Hujjatlar paketiga qo‘yilgan jamoaviy imzo haqiqiyligini tasdiqlash qanday imkoniyatni beradi? U qanday xossalarga ega?
27. EC-DSAH hujjatlar paketining jamoaviy imzosini haqiqiyligini tasdiqlash jarayonini tushuntirib bering.
28. JERI shakllantirish va tekshirish usuli qanday bosqichlardan iborat?

XULOSA

Ming yilliklar davomida davlat qurilishida, harbiy va diplomatik aloqalarni muhofazalashda foydalanib kelingan kriptologiya axborot asrining boshlanishi bilan jamiyatda va xususiy sektorda foydalanish uchun ham zarur bo'lib qoldi.

Hozirgi kunda O'zbekiston Respublikasida axborotning kriptografik muhofazasi sohasida yuqori malakali kadrlarni tayyorlashga katta ahamiyat berilmoqda. Bu o'z navbatida "Axborot xavfsizligi" yo'nalishi bo'yicha davlat tilida ta'lim olayotgan talabalarni zarur o'quv qo'llanma va darsliklar bilan ta'minlashni taqozo etadi.

Ushbu o'quv qo'llanmada kriptografik protokollarda qo'llaniladigan asosiy atamalar va ta'riflar, kriptografik protokollar nazariyasi asoslari, kriptografik protokollar funksiyalari va protokol xavfsizligiga oid talablar bayon etilgan.

O'quv qo'llanmada autentifikasiya protokollari, kalitlarni taqsimlash protokollari va ularning xossalari, e'lon qilinganligi nolga tengligi tushunchasi, matematik masalalarni yechish protokollari va shartnoma imzolash protokollari haqidagi ma'lumotlar keltirilgan.

Taqdim etilayotgan o'quv qo'llanma axborot xavfsizligi yo'nalishida ta'lim olayotgan bakalavrlar uchun mo'ljallangan. Shuningdek, ushbu o'quv qo'llanmadan axborot xavfsizligi va kriptografiya yo'nalishida ilmiy-tadqiqot olib borayotgan tadqiqotchilar, ilmiy xodimlar va soha mutaxassislari foydalanishlari mumkin. Ushbu o'quv qo'llanma «Axborot xavfsizligi» ta'lim yo'nalishining o'quv ta'lim standarti va o'quv dasturiga muvofiq ishlab chiqildi.

Mazkur «Axborot xavfsizligi protokollari» o'quv qo'llanmasining chop etilishi kelgusida tegishli o'quv darsliklarining yuzaga kelishi uchun zamin yaratadi.

GLOSSARIY – ГЛОССАРИЙ - GLOSSARY

Algoritm – amallarning cheklangan soni yordamida masala echimini belgilovchi buyruqlarning cheklangan to'plami.

Алгоритм - упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.

Algorithm - an ordered finite set of clearly defined rules for solving a finite number of steps.

Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm.

Алгоритм шифрования - алгоритм криптографический, реализующий функцию зашифрования.

Encryption algorithm - a cryptographic algorithm that implements the encryption function.

Kriptografik algoritm – kriptografik funksiyalarning birini xisoblashni amalga oshiruvchi algoritm.

Алгоритм криптографический - алгоритм, реализующий вычисление одной из функций криптографических.

Cryptographic algorithm - the algorithm that implements the computation of one of the cryptographic functions.

Rasshifrovkalash algoritmi – rasshifrovkalash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.

Алгоритм расшифрования - алгоритм криптографический, обратный к алгоритму зашифрования и реализующий функцию расшифрования.

Decryption algorithm – a cryptographic algorithm, the inverse of the algorithm encryption and decryption function implements.

Autentifikator– foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo'shimcha kod so'zlari, biometrik ma'lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo'lishi mumkin.

Аутентификатор - средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации

пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.

Authenticator - authentication means representing the hallmark of the user. Means of user.

Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul qilish uchun foydalanuvchining (xakikiyligini), qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikatsiyasini tekshirish; saqlanuvchi va uzatiluvchi ma'lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.

Аутентификация - проверка идентификации пользователя (проверка подлинности), устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.

Authentication - checking user authentication (authentication), device or other component in the system, usually to make a decision about granting access to system resources; checking the integrity of stored or transmitted data to detect unauthorized modification.

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.

Аутентификация двухфакторная – аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Two-factor **authentication**- user authentication based on two different factors are usually based on what the user knows, and what he owns (eg password-based and physical identifier).

Ko'p faktorli autentifikatsiya- bir necha mustaqil faktorlar asosida foydalanuvchini identifikatsiyalash orqali foydalanish nazoratini amalga oshirish.

Аутентификация многофакторная – реализация контроля доступа, представляющая собой идентификацию пользователя на основе нескольких независимых факторов.

Multifactor Authentication - implementing access control, which is a user identification based on several independent factors.

Ma'lumotlar bazasi - tatbiqiy dasturlarga bog'liq bo'lmagan xolda ma'lumotlarni tavsiflashning, saqlashning va manipulyatsiyalashning umumiy prinsiplarini ko'zda tutuvchi ma'lum qoidalar bo'yicha tashkil etilgan ma'lumotlar majmui.

База данных - совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ.

Database - a set of data organized according to certain rules, general principles providing descriptions, storing and manipulating data, regardless of the application.

Axborot xavfsizligi - axborot xolati bo'lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta'sir etishga yoki uning olinishiga yo'l qo'yilmaydi. Yana - axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarining (xususiyatlarining) saqlanishini ta'minlovchi axborotning himoyalanish sathi xolati.

Безопасность информации - состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение, еще - состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность /конфиденциальность/, целостность и доступность.

Information security - state information , which prevents accidental or intentional tampering or unauthorized information to receive it, also - state -level data protection during processing technologies to support the preservation of its qualitative characteristics (properties) as privacy / confidentiality / integrity and availability.

Tarmoq xavfsizligi - axborot tarmog'ini ruxsatsiz foydalanishdan, me'yoriy ishlashiga tasodifan yoki atayin aralashishdan yoki tarmoq komponentlarini buzishga urinishdan extiyot qiluvchi choralar. Asbob-uskunalarni, dasturiy ta'minotni, ma'lumotlarni himoyalashni o'z ichiga oladi.

Безопасность сетевая – меры, предохраняющие сеть информационную от доступа несанкционированного, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Включает защиту оборудования, программного обеспечения, данных.

Network Security - measures that protect the network information from unauthorized access, accidental or intentional interference with normal activities or attempts to destroy its components. Includes the protection of hardware, software, data.

Verifikatsiya – hisoblash vositalari yoki ularning kompleksi spetsifikatsiyasining ikki sathini tegishli moslikka taqqoslash jarayoni. Yana- dasturlashda – dastur to'g'riligining tasdig'i. Verifikatsiyaga ikkita yondashish farqlanadi: statik va konstruktiv usullar.

Верификация - процесс сравнения двух уровней спецификации средств вычислительной техники или их комплексов на надлежащее соответствие. Еще - в программировании доказательство правильности программ. Различают два подхода к верификации: статические и конструктивные методы.

Verification - the process of comparing two levels of specification of computer equipment or systems for proper alignment. Also - programming proof of the correctness of programs. There are two approaches to verification: static and constructive methods.

Генератор ключей – техническое устройство или программа, предназначенные для выработки массивов чисел или других данных, используемых в качестве ключей (криптосистемы), последовательности ключевой, векторов инициализации и т. п.

Key generator- technical device or program designed to generate arrays of numbers or other data to be used as keys (cryptographic) key sequence, initialization vectors, and so on.

Foydaluvchanlik - avtorizatsiyalangan mantiqiy obekt so'rovi bo'yicha mantiqiy ob'ektning tayyorlik va foydalanuvchanlik holatida bo'lish xususiyati.

Доступность – свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

Availability - property of an object in a state of readiness and usage upon request authorized entity.

Kalit uzunligi (o'lchovi) - kalitni ifodalovchi ma'lum alfavitdagi so'z uzunligi. Ikkili kalit uzunligi bitlarda o'lchanadi.

Длина (размер) ключа – длина слова в определённом алфавите, представляющего ключ. Длина ключа бинарного измеряется в битах.

Key length - word length in a certain alphabet, representing the key. The key length is measured in binary bits.

Axborotni kriptografik himoyalash - axborotni kriptografik o'zgartirish yordamida himoyalash.

Защита информации криптографическая – защита информации с помощью ее криптографического преобразования.

Cryptographic protection of information - information security by means of its cryptographic transformation.

Identifikator – sub'ekt yoki ob'ektning farqlanuvchi alomatidan iborat foydalanishning identifikatsiya vositasi. Foydalanuvchilar uchun asosiy identifikatsiya vositasi parol hisoblanadi.

Идентификатор - средство идентификации доступа, представляющее собой отличительный признак субъекта или объекта доступа. Основным средством идентификации доступа для пользователей является пароль.

Identifier - means of identification of the access, representing a distinctive sign of the subject or object of access. The main means of identification of access for users is the password.

Identifikatsiya – foydalanish sub'ektlari va obyektlariga identifikator berish va/yoki taqdim etilgan identifikatorni berilganlari ro'yhati bilan taqqoslash.

Идентификация- присвоение субъектам и объектам доступа

идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Identification -assignment to subjects and objects of access of the identifier and/or comparison of the shown identifier with the list of the appropriated identifiers.

Ochiq kalitlar infrastrukturasi – asimmetrik shifrtizim kalitlari tizimining qismtizimi. Qonuniy foydalanuvchilarning kalitlarning xaqiqiyligiga, kalitlarning foydalanuvchilarga va ular oldindan kelishilgan ishlatish shartlariga mosligiga ishonishlarini (kalitlar sertifikatlari yordamida) ta'minlashga mo'ljallangan.

Инфраструктура ключей открытых – подсистема системы ключевой шифрсистемы асимметричной. Предназначена для обеспечения (с помощью сертификатов ключей) доверия пользователей законных к подлинности ключей, соответствия ключей пользователям и оговоренным условиям их применения.

Public Key Infrastructure (PKI) – subsystem of system key cipher system of asymmetric. It is intended for providing (by means of certificates of keys) trust of users of lawful keys to authenticity, compliance of keys to users and the stipulated conditions of their application.

Mojaro – ruxsatsiz foydalanish xuquqiga ega bo'lishga yoki kompyuter tizimiga xujum o'tkazishga urinishning qayd etilgan xoli.

Инцидент – зафиксированный случай попытки получения несанкционированного доступа или проведения атаки на компьютерную систему.

Incident– the recorded case of attempt of receiving unauthorized access or carrying out attack to computer system.

Ma'lumotlarni uzatuvchi kanal - fizik muhit, u orqali axborot bir qurilmadan ikkinchisiga uzatiladi.

Канал передачи данных – физическая среда, по которой передается информация из одного устройства в другое.

Data transmission channel – the physical environment on which information from one device is transferred to another.

Ochiq kalit –asimetrik shifrtizimning maxfiy bo'lmagan kaliti.

Ключ открытый – несекретный ключ шифрсистемы асимметричной.

Public key – unclassified key the asymmetric cryptosystem.

Deshifrlash kaliti - deshifrlashda ishlatiluvchi kalit.

Ключ расшифрования – ключ, используемый при расшифровании.

Decryption key – the key used for decryption.

Seans kaliti - ikkita qatnashchilar (protokol qatnashchilari) orasidagi bitta aloqa seansi uchun maxsus generatsiyalangan kalit.

Ключ сеансовый – ключ, специально сгенерированный для одного сеанса связи между двумя участниками (протокола).

Session key – the key which has been specially generated for one communication session between two participants (protocol).

Maxfiy kalit - ma'lum simmetrik shifrtizim kalitlaridan yoki ma'lum asimmetrik shifrtizimning ba'zi funksiyalaridan foydalanish huquqiga ega bo'lmagan shaxslardan maxfiy sanaluvchi kalit.

Ключ секретный – ключ, сохраняемый в секрете от лиц, не имеющих допуска к ключам данной шифрсистемы симметричной или к использованию некоторых функций данной шифрсистемы асимметричной.

Secret key – the key kept in a secret from persons, not having the admission to keys given symmetric cryptosystem or to use of some functions given the asymmetric cryptosystem.

Kriptografik tizim –axborotni kriptografik o'zgartirishni va kalitlarni taqsimlash jarayonini boshqarishni ta'minlovchi texnik va/yoki dasturiy vositalar, tashkiliy usullar majmui.

Криптографическая система - совокупность технических и /или программных средств, организационных методов, обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей.

Cryptographic system, Cryptosystem - set technical and/or software, the organizational methods providing cryptographic transformation of information and management process of distribution of keys.

Parol –tizimdan, dasturdan yoki ma'lumotlardan foydalanishga ruxsat olish uchun kompyuter so'rovi bo'yicha kiritiladigan simvollarning noyob ketma-ketligi.

Пароль – уникалная последовательноеть символов, которую необходимо ввести по запросу компьютера, чтобы исключить доступ к системе, программе или данным.

Password - a password is an unspaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user.

Raqamli imzo - xabarga yoki hujjatga va faqat imzo chekuvchi sub'ektga ma'lum qandaydir maxfiy kalitga bog'liq qandaydir alfavitdagi qatordan (masalan raqamli qatordan) iborat. Raqamli imzoning, maxfiy kalitdan foydalanmasdan osongina tekshirilishi lozimligi faraz qilinadi.

Подпись цифровая – представляет собой строку в некотором алфавите (например, цифровую), зависящую от сообщения или документа и от некоторого ключа секретного, известного только подписывающему субъекту. Предполагается, что п. ц. должна быть легко проверяемой без получения доступа к ключу секретному.

Digital signature - is a string in some alphabet (eg, digital), depending on the message or document and from a secret key known only to the signatory subject. It is assumed that digital signatur should be easily verified without access to the secret key.

Elektron imzo - boshqa elektron shakldagi axborotga (imzolanuvchi axborotga) birlashtirilgan yoki boshqa tarzda shunday axborot bilan bog'langan va axborotni imzolovchi shaxsni aniqlashda ishlatiladigan elektron shakldagi axborot.

Подпись электронная – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Electronic signature - information in electronic form which is attached to the other information in electronic form (signed information) or otherwise relating to such information and is used to determine the person signing the information.

Protokol - qurilmalar, dasturlar, ma'lumotlarlarni ishlash tizimlari, jarayonlar yoki foydalanuvchilarning o'zaro harakati algoritmini belgilovchi qoidalar majmui.

Протокол - совокунность правил, определящих алгоритм взаимодействия устройств, программ, систем обработки данных, процессов или пользователей.

Protocol - a set of rules that define the algorithm of interaction devices, software, data processing systems, processes or users.

Taxdid (axborot xavfsizligiga taxdid) - axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug'diruvchi sharoitlar va omillar majmui.

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Threat - set of conditions and factors that create potential or actual violations of the existing danger of information security.

Xesh-funksiya - chekli alfavitdagi uzunligi chekli kirish yo'li so'zini berilgan, odatda, qat'iy uzunlikdagi, so'zga akslantirish funksiyasi.

Хеш-функция - функция, отображающая входное слово конечной длины в конечном алфавите в слово заданной, обычно фиксированной длины.

Hash function - function mapping input word of finite length over a finite alphabet in a given word, usually a fixed length.

Axborot yaxlitligi - tasodifan va/yoki atayin buzilish hollarida hisoblash texnikasi vositalarining yoki avtomatlashtirilgan tizimning axborotini o'zgartirmasligini ta'minlovchi xususiyati.

Целостность информации - способность средства вычислительной техники или системы автоматизированной обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Information Integrity - the ability of computers and automated systems to provide consistent information in a casual and / or intentional distortion (destruction).

FOYDALANILGAN ADABIYOTLAR

1. Ўзбекистон Республикасини янада ривожлантириш бўйича ҳаракатлар стратегияси тўғрисида. Ўзбекистон Республикаси Президентининг ПФ-4947- сон фармони. Тошкент, 2017 йил 7 феврал.

2. «Ўзбекистон Республикасида ахборотнинг криптографик муҳофазасини ташкил этишга доир чора-тадбирлари тўғрисида» ги Ўзбекистон Республикаси Президентининг ПҚ-614-сон қарори. – Тошкент, 3 апрел 2007 йил.

3. «5523500 – Ахборот хавфсизлиги таълим йўналиши бўйича бакалаврларнинг тайёргарлик даражаси ва зарурий билимлар мазмунига қўйиладиган ТАЛАБЛАР» Ўзбекистон давлат таълим стандарти. Тошкент, 2008.

4. O'z DSt 1109:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар».

5. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005.

6. Чмора А.Л. Современная прикладная криптография. Изд.:Гелиос, 2001.- 256 с.

7. Аграновский А.В., Хади Р.А. Практическая криптография. Алгоритмы и их программирование. Изд.:Лори СОЛОН-Пресс, 2002. – 226 с.

8. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ – Москва: ТРИУМФ, 2002.

9. А.В. Черемушкин, "Криптографические протоколы: основные свойства и уязвимости", ПДМ, 2009.

10. Криптографические протоколы. Программа. – Ставрополь: издательство СГУ, 2009.

11. С. В. Запечников Криптографические протоколы и их применение в финансовой и коммерческой деятельности , Москва Горячая линия - Телеком 2007.

12. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие/ Изд.:Гелиос АРВ, 2001. – 480 с.

13. Акбаров Д.Е. «Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши» - Т.: «Ўзбекистон маркаси», 2009. - 424 б.

14. Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. Тошкент, ФТМТМ, 2008.

15. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. Т., "Aloqachi". 2008, 382бет.

16. Арипов М.М., Пудовченко Ю.Е. Основы криптологии.- Ташкент: 2004. – 136 с.

17. Новые алгоритмы и протоколы для аутентификации информации в АСУ / А. А. Молдовян, Н. А. Молдовян // Автоматика и телемеханика. - 2008. - N 7.

18. Классификация криптографических протоколов. www.boolevar.ru/wp-content.

19. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc. 2004.-456 pp.

20. А.В. Черемушкин, "Криптографические протоколы: основные свойства и уязвимости". Учебное пособие для вузов. 2009.

21. Отчет о НИР «Разработка алгоритма электронной цифровой подписи на эллиптических кривых на основе алгебры параметров», ГУП «UNICON.UZ», 2009.

22. Молдовян А.А., Молдовян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005г.

23. Мирин А. Ю., Заболотный А. П., Молдовян У. А. Протокол коллективной подписи на основе сложности задачи факторизации // Материалы VI Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2009)». Санкт-Петербург, 28-30 октября. СПб.: СПОИСУ, 2009. С. 117.

24. T. El Gamal, A Public-key Cryptosystem and a Signature Based on Discrete Logarithms. IEEE Trans. Inform. Theory, Vol. IT-31,pp.469-472, July 1985.

25. "Digital Signature Standard (DDS)", Federal Information Processing Standards Publication 186, May 19, 1994, pp.1-18.

26. Miller V. Use of elliptic curves in cryptography // Advances in cryptology – CRYPTO'85 (Santa Barbara, Calif., 1985). 1986. (Lecture Notes in Comput. Sci.; V. 218).

27. Koblitz N. and Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography, 19 (2000).

28. Изотов Б.В., Молдовян Н.А. Новые возможности технологии PKI: Коллективная и композиционная ЭЦП. // www.cobra.ru.

29. Хасанов П.Ф., Хасанов Х.П. Стойкость Государственного стандарта ЭЦП Республики Узбекистан // «Сервисы удостоверяющих центров. Новые области применения PKI»: Тез. докл. международной научно –

практической конференции PKI Forum- 2006, Санкт-Петербург, 7-10 ноября 2006.

30. Ахмедова О.П. Параметрлар алгебраси асосида носимметрик криптотизимлар яратиш усули ва алгоритмлари // Номзодлик диссертация иши, Тошкент-2007.

31. Хасанов Х.П. Диаматрицалар алгебраси элементлари асосида ахборотларни криптографик ҳимоялаш усуллари ва алгоритмлари // Номзодлик диссертация иши, Тошкент-2010.

32. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. Санкт-Петербург-2004.

33. Миронов А.М. Криптографические протоколы PDF. Учебное пособие для студентов. intsys.msu.ru.

34. Акбаров Д., Хасанов П., Хасанов Х., Ахмедова О. Криптографиянинг математик асослари – Тошкент, 2010 – 210 бет.

35. ISO/IEC 11770 -1. "Key management – Introduction".

36. ISO/IEC 11770 -2. "Key management – Symmetric techniques".

37. ISO/IEC 11770 -3. "Key management – Asymmetric techniques".

38. The Secure Sockets Layer Protocol. http://www.netscape.com/info/security-doc.html.

39. Масленников М., Практическая криптография. - М.:Лори BHV - Санкт - Петербург, 2003.- 464 с.

40. «Криптографик тизимларни криптотаҳлиллашнинг истиқболли усулларини ишлаб чиқиш ва уларни тадқиқ этиш» мавзуси бўйича бажарилган илмий-тадқиқот ишининг 1-4-босқич ҳисоботлари. – ЎзААА «UNICON.UZ» ДУК, Тошкент, 2009-2010.

41. Menezes A.J. Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

42. US Patent, Hellman, et al. Cryptographic apparatus and method, 4.200.770, April 29,1980.

43. Min-Shiang Hawng, Cheng-Chi Le. Research issues and challenges for multiple digital signature // Int. J. of Network Security. – 2005. – Vol. 1, No 1. – P. 1-7.

44. Молдовян Н.А., Молдовян П.А. Новые протоколы слепой подписи // Безопасность информационных технологий. – М.:МИФИ. –2007. – № 3. – С. 17–21.

45. Артамонов А.В., Маховенко Е.Б. Применение алгоритма Шнорра в протоколе коллективной подписи //Материалы XIV Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы». – 2007. – С. 17–18.

46. Гортинская Л.В., Молдовян Н.А., Козина Г.Л. Реализация протоколов коллективной подписи на основе стандартов ГОСТ 34.310–95 и ДСТУ 4145-2002 //Правове, нормативне та метрологичне забезпечення системи захисту информации в Украини. – Киев: НТУУ «КПІ». – 2008. – № 1. – С.21–25.

47. K. Itakura and K. Nakamura, "A public-key cryptosystem suitable for digital multisignature", NEC Research and Development, Vol. 71, October 1983, pp. 1-8.

48. Anna Nelasa, Victor Dolgov, Anatolij Pogorily. Digital Signature Protocol for corporate network // Proceedings of International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2008). – Lviv-Slavsko (Ukraine). – 2008. –Pp. 396–397.

49. Дернова Е.С. Механизмы аутентификации информации, основанные на двух вычислительно трудных задачах. Автореферат диссертации на соискание ученой степени кандидата технических наук. Санкт-Петербург–2009.

50. Аникевич Е.А. Метод формирования электронной цифровой подписи на основе открытого коллективного ключа для электронного документооборота проедприятия. Автореферат диссертации на соискание ученой степени кандидата технических наук. Санкт-Петербург – 2010.

51. Аль-Маджмар Н.А. Методы аутентификации информации и обеспечения защищенности документов от подделки. Автореферат диссертации на соискание ученой степени кандидата технических наук. Санкт-Петербург – 2009.

52. Аль-Маджмар Н.А. Реализация системы выдачи паспортов с повышенной защищенностью от подделки. Санкт-Петербургский государственный электротехнический университет, ЛЭТИ, 2008.

53. Протоколы слепой коллективной подписи на основе стандартов цифровой подписи / Фахрутдинов Р. Ш., Костин А. А., Молдовян Н. А. // Вопросы защиты информации. – 2010. – № 1. – С. 14–23.

54. Протоколы слепой коллективной подписи на основе задачи дискретного логарифмирования / Галанов А. И., Костина А. А., Молдовян Д. Н., Цехановский В. В. // Вопросы защиты информации. – 2009. – № 4. С. 7–11.

55. Коллективная ЭЦП – специальный криптографический протокол на основе новой трудной задачи / Молдовян А. А., Молдовян Н. А. // Вопросы защиты информации. – 2008. – № 1.

56. Неласая А.В., Козина Г.Л., Молдовян Н.А. Протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривых. ISSN 1607-3274 "Радиоэлектроника. Информатика. Управление" № 1, 2008.

57. L. Harn. A New Digital Signature Based on the Discrete Logarithm. In Electronics Letters, Vol. 30, No. 5, March 1994, pp. 193-195.

58. L. Harn. Group-oriented (*t, n*) Threshold Signature and Multisignature. In IEE Proceedings-Computers and Digital Techniques, Vol. 141, No. 5, Sep. 1994, pp. 307-313.

59. L. Harn. Batch Verifying Multiple DSA-type Digital Signatures. In Electronics Letters, Vol. 34, No. 9, April, 1998, pp. 870-871.

60. CCITT, Recommendation X.509. The Directory-Authentication Framework. Consultation Committee, International Telephone and Telegraph, International Telecommunications Union, Geneva, 1989.

61. C.-Y. Lin, T.-C. Wu and J.-J. Hwang, "ID-based Structured Multisignature Schemes", Advancesin Network and Distributed Systems Security, Kluwer Academic Publishers (IFIP Conference Proceedings 206), Boston, 2001, pp. 45-59.

62. L. Harn and Y. Xu. Design of Generalized ElGamal type digital signature schemes based on discrete logarithm. In Electronics Letters, Vol. 30, No. 24, Nov. 1994, pp. 2025-2026.

63. David Monniaux, Decision Procedures for the Analysis of Cryptographic Protocols by Logics of Belief, in Proceedings.

MUNDARIJA

Oydin Po‘latovna Ahmedova,
Xislat Po‘latovich Hasanov,
Mahmuda Husnuddinovna Nazarova,
Iqbol Ubaydullayevna Xolimtayeva,
Oybek Djalalitdinovich Nuritdinov

AXBOROT XAVFSIZLIGI PROTOKOLLARI

(O‘quv qo‘llanma)

Тошкент – «Aloqachi» – 2019

Муҳаррир: М. Миркомилов
Тех. муҳаррир: А. Тоғаев
Мусаввир: Б. Эсанов
Мусаҳҳиҳа: Ф. Тоғаева
Компьютерда саҳифаловчи: Ш. Тўхтамуродов

Нашр. лиц. ii № 176, 11.06. 2010.
Босишга рухсат этилди 1.02.2019. Бичими 60x84 $^{1}/_{16}$.
«Times Uz» гарнитураси. Офсет усулида босилди.
Шартли босма табоғи 11,0. Нашр босма табоғи 10,5 .
Адади 100. Буюртма № 5.

«Nihol print» ОК да чоп этилди.
Тошкент шаҳри, Мухтор Ашрафий кўчаси, 99./101.