ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА
ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ГУЛИСТОН ДАВЛАТ УНИВЕРСИТЕТИ

«АХБОРОТЛАРНИ ХИМОЯЛАШ»
фанидан методик кўрсатмалар

Гулистон – 2019

Кудратов А.Н. «Ахборотларни химоялаш» фанидан методик кўрсатмалар . - Гулистон, 2019. - 43 бет.

Ушбу методик ишланма Олий таълимнинг 5110700 – информатика ўқитиш методикаси мутахассислиги буйича мутахассислик фанлари блокига тегишли «Ахборотларни химоялаш» махсус курсидан тасдиқланган ўқув дастури (ГулДУ, 2018) асосида тайёрланган бўлиб, унда амалий ва лаборатория ишларини бажариш бўйича тавсиялар берилган.

Методик ишланма Гулистон давлат университети Илмий Кенгаши - баённома 28.08.2018 й.) тамонидан тавсия килинган.

Тақризчи: Абдурахимов Д.Б. - педагогика фанлари номзоди

AMALIY MAShG'ULOTLAR:

1-amaliy mashg'ulot

Mavzu: KOMPYuTERLARGA TEXNIK XIZMAT KO'RSATISh.

Darsning maqsadi: Talabalarga zamonaviy shaxsiy kompyuterlarga xizmat ko'rsatuvchi dasturlarning qo'llanilishi haqida ma'lumot berish, UNEraze dasturi va uning ishlash printsipi, disklarga xizmat ko'rsatuvchi dasturlar bilan ishlash malakalarini oshirish.

Kerakli jixoz va materiallar: Shaxsiy kompyuter (ShK), Windows operatsion tizimi, magnit disklar, ma'ruza matni, ma'ruza daftari, xar-xil adabiyotlar.

Ishni bajarish tartibi:

1. Disk *bilan* ishlash jarayonida o'chib ketgan katalog va fayllarni qayta tiklash uchun quyidagi dasturlarni ishlash printsiplarini tushuntirish.
   - MS — DOS tarkibida kiruvchi Undelete dasturi;
   - Norton Utilites servis dasturi majmuasiga kiruvchi Unerase dasturi;
   - PCTOOLS dasturi.
2. O'chib ketgan axborotni tiklashni muvaffaqiyatli amalga oshirish uchun disklarga ko'rsatiladigan amallarni izohlang.
3. Uneraze dasturi va uning ishlash tamoyili.
4. Buzilgan fayllar va disklarni tiklashda e'tibor qaratish kerak bo'lgan qoidalarni izohlang.
5. Diskka xizmat ko'rsatuvchi dasturlar ish jarayonini ko'rsatib, izohlab bering.

Tekshirish uchun savollar:

1. Magnit disklar qanday sabablarga ko'ra ishdan chiqadi?
2. O'chgan axborotlar qanday dasturlar yordamida qayta tiklanadi?
3. O'chgan axborotlarni qanday xollarda qisman yoki to'la tiklash mumkin?
4. Fizikaviy kamchiliklar qanday paydo bo'ladi?
5. Mantiqiy defektlar kanday paydo bo'ladi?
6. Buzilgan fayllarni qaysi dasturlar yordamida tiklash mumkin?

ADABIYoTLAR:

1. Informatika. Bazovo'y kurs. Pod redaktsiey S.V.Simonovicha Sank — Peterburg. 2001 g.
2. V. Passikov. Zahita kompyuternoy informatsii. M.: Nauka 2001g.
3. Informatika. Pod redaktsiey prof. N.V.Makarovoy M.: 1997 g.
4. Axborot tizimlari va texnologiyalari. Akad. S. G'ulomov va boshqalar, T. "Shark", 2000 y.
5. S.S.G'ulomov va boshq. Iqtisodiy informatika. T.:"O'zbekistan", 1999 y.

2-amaliy mashg'ulot

Mavzu: KOPYuTERLARNI VIRUSLARDAN HIMOYaLASh.

Darsning maqsadi: Kompyuter viruslari va ularning turlari, kompyuter viruslaridan ximoyalanish usullari va ularga qarshi ximoya vositalari, antivirus dasturlar va ular bilan ishlash texnologiyalari haqida ko'nikma va malakalarni xosil qilish.

Kerakli jixoz va materiallar: Shaxsiy kompyuter, Windows operatsion tizimi, antivirus dasturlar, magnit disklar, ma'ruza matni, ma'ruza daftari, xar-xil adabiyotlar

Ishni bajarish tartibi:

1. Kompyuterni ishga tushiring.
2. Kompyuterga antivirus dasturini o'rnating.
3. Antivirus dasturini ishga tushiring va quyidagi amallar ketma-ketligini bajaring:
   - Biror faylni virusga tekshiring.
   - Biror papkani virusga tekshiring.
   - Moi dokumento' papkasini virusga tekshiring.
   - Zararlangan fayllarni o'chiring.
   - S diskni virusga tekshiring.
   - D diskni virusga tekshiring.
4. Disketadagi ma'lumotlarni kompyuterga ko'chirishdan oldin uni virusga tekshiring.
5. Dastur hisoboti (otchyot) bilan tanishib chiqing.
6. Kompyuterni virusga tekshiring.
7. Kompyuter ishini yakunlang.

Tekshirish uchun savollar:

1. Kompyuter virusi nima?
2. Viruslar kompyuterga qanday zarar etkazadi?
3. Yuklanuvchi virusning ta'sirini tushuntirib bering.
4. Makroviruslar kanday axborotlarga ta'sir kiladi?
5. "Troyanno'y kon" dasturlari nima uchun ishlatiladi?
6. Kompyuter viruslaridan ximoyalanish usullari nimalardan iborat?
7. Viruslardan ximoyalanishning kanday vositalari ishlatiladi?
8. Antivirus dasturlari kanday turlarga bulinadi?
9. Apparat ximoya vositasi kanday amalga oshiriladi?

ADABIYoTLAR:

1. Informatika. Bazovo'y kurs. Pod redaktsiey S.V. Simonovicha Sank—Peterburg, 2001 g.
2. V. Passikov. Zahita kompyuternoy informatsii. M.: Nauka, 2001 g.
3. Informatika. Pod redaktsiey prof. N.V. Makarovoy M.: 1997 g.
4. Axborot tizimlari va texnologiyalari. Akad. S. G'ulomov va boshkalar. T.: "Sharq", 2000 y.
5 S.S. G'ulomov va boshq. Iktisodiy informatika. T.:"O'zbekistan", 1999 y.

3-amaliy mashg'ulot

Mavzu: ARXIVATORLAR BILAN IShLASh.

Darsning maqsadi: Arxivatorlar, ularning vazifalari, arxivda joylashtirilgan fayllar, arxivli faylga yangi fayllarni qo'shish yoki olib tashlash xaqida ma'lumotlar berish va ular bilan ishlash malakasini hosil qilish.

Kerakli jixoz va materiallar: Shaxsiy kompyuter, Windows operatsion tizimi, arxivator dasturlari, ma'ruza matni, ma'ruza daftari, xar-xil adabiyotlar.

Ishni bajarish tartibi:

1. Kompyuterni ishga tushiring.
2. MS DOS operatsion tizimi bilan ishlash rejimiga o'tkazing.
3. Arxiv nomli papka yarating va unga 6 ta fayl nusxasini ko'chiring.
4. ARJ arxivator dasturida quyidagilarni bajaring:
    - Fayllarni ARJ arxivatori yordamida arxivlang;
    - Arxivlangan fayllarni himoyalash maqsadida unga parol o'rnating;
    - O'zi ochiladigan arxiv fayl hosil qiling;
    - ARJ arxivator dasturida maksimal darajada tezroq siqish amalini bajaring;
    - ARJ arxivator dasturida fayllarni bo'laklab arxivlash amalini bajaring;
    - ARJ arxivator dasturida fayllarni qirqib arxivlash amalini bajaring;
    - Bir nechta arxiv fayllarni birlashtiring;
    - Arxivdagi fayllar mundarijasini ko'rib chiqing;
    - Arxivlangan fayllarni oching.
5. MS DOS operatsion tizimi ishini yakunlang.
6. Windows operatsion tizimida ishchi stolda o'z ismingiz bilan ataluvchi papka yarating va unga ixtiyoriy 10 ta fayl nusxasini ko'chiring.

1. WINZIP arxivatori yordamida fayllarni arxivlang.
2. Arxivlangan fayllar necha foizga siqilganini aniqlang.
3. O'zi ochiluvchi (.exe) arxiv fayllarni hosil qiling.
4. RAR arxivatorida quyidagi amallarni bajaring:
    - Yangi papkaga 10 ta fayl nusxasini ko'chiring;
    - Fayllarni RAR arxivatori yordamida arxivlang;
    - Arxivlangan fayl necha foizga siqilganini aniqlang va ZIP arxivatorida siqilgan fayl bilan taqqoslang;
    - Arxivlangan faylni himoyalash maqsadida parol o'rnating;
    - Arxivlangan faylni oching.

Tekshirish uchun savollar:

1. Fayllarni arxivlash deganda nimani tushunasiz?
2. Fayllarni arxivlashda ularni xajmi kanchaga kiskaradi?

3. Winrar dasturi yordamida fayllar kanday arxivlanadi?
4. Arxivlangan faylga boshka fayllarni kushish mumkinmi?
5. Arxiv faylini yangilash nima va kanday amalga oshiriladi?
6. Nima uchun fayllar bo'laklab arxivlanadi?
7. Faylni kirkib arxivlash deganda nimani tushunasiz?
8. Mavjud arxiv fayliga yangi fayllarni birlashtirish imkoniyatini tushuntiring?
9. Arxiv fayli ichidagi ma'lumotlarni kanday kurish mumkin?
10. Arxivda joylashgan fayllar xakidagi ma'lumotlarni faylga yozish va qog'ozga chop etish qanday amalga oshiriladi?
11. Winrar dasturining imkoniyatlari.
12. Winrar dasturida necha formatda fayllarni arxivlash mumkin?

ADABIYoTLAR:

1. Informatika. Bazovo'y kurs. Pod redaktsiey S.V.Simonovicha Sank—Peterburg, 2001 g.
2. V. Passikov. Zahita kompyuternoy informatsii. M.: Nauka, 2001 g.
3. Informatika. Pod redaktsiey prof. N.V. Makarovoy M.: 1997 g.
4. Axborot tizimlari va texnologiyalari. Akad. S. G'ulomov va boshkalar T.: "Shark", 2000 y.
5 S.S. G'ulomov va boshq. Iqtisodiy informatika. T.:"Uzbekistan", 1999 y.

4-amaliy mashg'ulot.

Mavzu: MA'LUMOTLAR BAZASINI HIMOYaLASh.

Darsning maqsadi: Ma'lumotlar bazasi axborot tizimlari, Ma'lumotlar bazasi, Ma'lumotlar ombori, MBBT, maydon, yozuv, indekslash, kalit, universallik, mustakillik haqida tushuncha xosil qilish va ularda ishlash malakasini oshirish.

Kerakli jihoz va materiallar: Shaxsiy kompyuter, Windows operatsion tizimi, ACCESS ma'lumotlar bazasi dasturi, ma'ruza matni, ma'ruza daftari, xar-xil adabiyotlar.

Ishni bajarish tartibi:

1. Kompyuterni ishga tushirish tartibi bo'yicha ishga tushiring.
2. Kompyuter avtomatik ravishda biror dastur bilan ishlashga o'tsa undan Windows tizimi bilan ishlash rejimiga o'tkazing.
3. ACCESS dasturini ishga tushiring.
4. ACCESS dasturi ishchi oynasi tashkil etuvchilariga tavsif bering va ularni ekrandan olish va joylashtirish ishlarini bajaring.
5. ACCESS dasturida jadvallar bilan ishlash rejimida guruhingiz talabalari haqidagi ma'lumotni tayyorlang.
6. Guruhingiz talabalari haqidagi ma'lumotlar omborini yarating.
7. Siz tahsil olayotgan oliygohingiz haqidagi ma'lumotlar omborini yarating.

8. Kiritilgan barcha ma’lumotlarni kompyuterning qattiq diskiga o’zingizning ismingiz bilan nomlangan papkaga saqlab qo’ying.

Tekshirish uchun savollar:

1. Ma’lumotlar ombori deganda nimani tushunasiz?
3. Qanday ma’lumotlar omborlarini bilasiz?
4. Ma’lumotlar bazasining strukturasi qanday tashkil topgan?
5. Maydon va yozuv deganda nimalarni tushunasiz?
6. Indekslash qanday jarayon?
7. Ma’lumotlar bazasini boshqarish tizimi qanday vazifalarni bajaradi?
8. MBBT ni ishlab chiqishda qanday tamoyillarga asoslaniladi?
9. Ma’lumotlar bazasini xavfsizligini saqlash usullari.
10. Ma’lumotlar bazasi boshqa fayllardan qanday farq qiladi?

ADABIYoTLAR:

1. Informatika. Bazovo’y kurs. Pod redaktsiey S.V.Simonovicha Sank — Peterburg, 2001 g.
2. V. Passikov. Zahita kompyuternoy informatsii. M.: Nauka, 2001 g.
3. Informatika. Pod redaktsiey prof. N.V. Makarovoy, M.: 1997 g.
4. Axborot tizimlari va texnologiyalari. Akad. S. G’ulomov va boshqalar. T.:"Sharq", 2000 y.
5 S.S. G’ulomov va boshq. Iqtisodiy informatika. T.:"O’zbekiston", 1999 y.

5-amaliy mashg’ulot

Mavzu: WINDOWS NT NING AXBOROTLARNI XIMOYa QILISh VA XAVFSIZLIK SISTEMASI.

Darsning maqsadi: FAT, NIFS, NRFS—fayl tizimlari, registry (registr), SAM (himoyaning byudjet menedjeriga), Welcome oynasi, himoyaning S2 darajasi, himoyalash Milliy Markazining (WCSC), "Zarg’aldoq kitob", Windows NT da turli fayl tizimlarni qo’llash kabilar haqida ma’lumotlar berish.

Kerakli jihoz va materiallar. Shaxsiy kompyuter, Windows NT operatsion tizimi, ma’lumotlar bazasi dasturi, ma’ruza matni, ma’ruza daftari, xar-xil adabiyotlar.

Ishni bajarish tartibi:

1. Windows NT da turli fayl tizimlarni qo’llash.
2. MS DOC, Windows va OSG’2 operatsion tizimlarida ishlatiladigan FAT, NTFS, HPFS fayl tizimlari haqida ma’lumot.
3. *Windows NT* ni o’rganish.
4. *Windows* ning boshka versiyalarini o’rnatish va sozlash.
5. Windows NT da Registry (registr) deb ataluvchi baza va uning ilovalarini sozlash parametrlari.
6. *Windows NT* Workstation — ishchi stantsiyasi va Windows N*T* Server — Server versiyalarini fayl, bosmaga chiqarish, ilovalar, domenlarni tekshiruvchisi, uzoqlashgan kompyuterlarga kirish, ma’lumotlar xavfsizligini ta’minlash,

ma’lumotlar nusxalarini yaratish, aloka, yordamchi xizmatlar serveri sifatida bo’lishini o’rganish.

7. Ro’yxatdan o’tish jarayoni. Ximoya qilish sistemasining S2 darajasi. S2 Ximoya darajasi talabalarini aniqlash.

Tekshirish uchun savollar:

1. Windows operatsion tizimlarida kanday fayllar tizimlari ishlatiladi?

2. Windows NT da Registry (registr) deb ataluvchi baza qanday vazifani bajaradi?

3. Ro’yxatdan o’tish jarayoni qanday amalga oshiriladi?

4. Domin deganda nima tushuniladi?

5. Axborotlarni himoya qilishning S2 darajasiga qanday talablar qo’yilgan?

6. "Zarg’aldoq kitob" nima xaqida?

Adabiyotlar:

1. Informatika. Bazovo’y kurs. Pod redaktsiey S.V. Simonovicha Sank-Peterburg, 2001 g.

2. V. Passikov. Zahita kompyuternoy informatsii. M.: Nauka, 2001 g.

3. Informatika. Pod redaktsiey prof. N.V. Makarovoy M.: 1997 g.

4. Axborot tizimlari va texnologiyalari. Akad. S.G’ulomov va boshqalar. T.: "Sharq", 2000 y.

5. S.S. G’ulomov va boshq. Iqtisodiy informatika. T.:"O’zbekiston", 1999 y.

6-amaliy mashg’ulot.

Mavzu: Internetda axborotlarni himoyalash.

Darsning maqsadi: Talabalarga butun jaxon Internet tarmog’ida ishlovchilar uchun qo’yilgan talablar, Elektron tijorat, elektron konvert, elektron otkritka, elektron imzo, elektron sertifikat va boshqalarda axborotlarni himoyalash haqida ko’nikmalar berish.

Kerakli jihoz va materiallar: Shaxsiy kompyuter, Internet tarmoqlari, Intranet, login parol, ma’ruza matni, ma’ruza daftari, xar-xil adabiyotlar.

Ishni bajarish tartibi:

1. Butun jaxon Internet tarmog’ida ishlovchilar uchun qo’yilgan talablar mazmunini aniqlang.

2. Axborotlarni nosimmetrik shifrlashtirish.

3. Himoyaning etarlilik tamoili, elektron imzo haqida ma’lumot.

4. Elektron sertifikatlar haqida ma’lumot.

5. Web-tugunlarni sertifikatsiyalash va uning talablari.

6. Pochta aloqasi, internetda tijorat ishlarida axborotlarni himoyalash.

7. Simmetrik shifrlashtirish, nosimmetrik shifrlashtirish, kriptochidamlik va elektron imzolardagi himoyalar.

Tekshirish uchun savollar:

1. Internetda ishlaganda nimalarga rioya qilish kerak?
2. Pochta aloqasi va internet o’rtasida qanday o’xshashlik bor?
3. Internetda tijorat ishlari qanday amalga oshiriladi?
4. Axborotlar qanday usullar yordamida kodlashtiriladi?

5. Simmetrik shifrlashtirish qanday amalga oshiriladi?
6. Simmetrik shifrlashning qanday kamchiligi bor?
7. Nosimmetrik shifrlashtirish va uning qulayliklari nimalardan iborat?
8. Himoyaning etarlik tamoilli nima?
9. Kriptochidamlik nima?
10. Elektron imzo qanday amalga oshiriladi?

Adabiyotlar:

1. Informatika. Bazovo'y kurs. Pod redaktsiey S.V. Simonovicha Sank-Peterburg, 2001 g.
2. V. Passikov. Zahita kompyuternoy informatsii. M.: Nauka, 2001 g.
3. Informatika. Pod redaktsiey prof. N.V. Makarovoy M.: 1997 g.
4. Axborot tizimlari va texnologiyalari. Akad. S. G'ulomov va boshqalar. T.: "Sharq", 2000 y.
5. S.S. G'ulomov va boshqalar, Iqtisodiy informatika. T.:"O'zbekiston", 1999 y.

7-amaliy mashg'ulot.

Mavzu: Axborotlarni oddiy almashtirish usuli bilan shifrlash.

Darsning maqsadi: Talabalarni axborotlarni oddiy almashtirish usuli bilan shifrlash haqida ma'lumotlar berish va axborotlarni himoyalashning shifrlash usullari haqida ko'nikmalar hosil qilish.

Kerakli jihoz va materiallar: Shaxsiy kompyuter, ma'ruza matni, ma'ruza daftari, xar-xil adabiyotlar.

Ishni bajarish tartibi:

1. «Internet» so'zini almashtirish uslubi bilan shifrlash va shifrni ochish
2. «Algoritm» so'zini almashtirish uslubi bilan shifrlash va shifrni ochish.
3. « Direktor» so'zini almashtirish uslubi bilan shifrlash va shifr ochish.
4. «Redaktor» so'zini almashtirish uslubi bilan shifrlash va shifr ochish.
5. «Mexanizm» so'zini almashtirish uslubi bilan shifrlash va shifr ochish.
6. «Katalog» so'zini almashtirish uslubi bilash shifrlash va shifr ochish.

Adabiyotlar:

1. Informatika. Bazovo'y kurs. Pod redaktsiey S.V. Simonovicha Sank-Peterburg, 2001 g.
2. V. Passikov. Zahita kompyuternoy informatsii. M.: Nauka, 2001 g.
3. Informatika. Pod redaktsiey prof. N.V. Makarovoy M.: 1997 g.

1 – Лаборатория машғулотлари.

Ўрин алмаштириш шифрлари. Алмаштириш (подстановка) усулларининг мохияти бир алфавитда ёзилган ахборот символларини бошка алфавит символлари билан маълум коида буйича алмаштиришдан иборатдир. Энг содда усул сифатида тугридан тугри ўрин алмаштиришни курсатиш мумкин. Дастлабки ахборот ёзилувчи A_0 алфавитнинг s_{oi} символларига шифрловчи Aj

алфавитнинг символлари мое куйилади. Оддий холда иккала алфавит хам бир хил символлар тупламига эга булиши мумкин.

Иккала алфавитдаги символлар уртасидаги мослик маълум алгоритм буйича К символлар узунлигига эга бўлган дастлабки матн T_0 символларининг рақамли эквивалентларини ўзгартириш орқали амалга оширилади.

Моноалфавитли алмаштириш алгоритми қуйидаги қадамлар кетма-кетлиги кўринишда ифодаланиши мумкин

1- кадам. [lxR] ўлчамли дастлабки A_0 алфавитдаги хар бир символ s_0 € T i=1k) ни A_0 алфавитдаги s_{0l} символ тартиб ракдмига мое келувчи h_0 (s_0j) сонга алмаштириш йули билан ракамлар кетма- кетлиги L_0h ни шакллантириш.

2- кадам. L_0h кетма-кетлигининг хар бир сонини hji= (k_1xh_0i(s_0i)+k_2)(modR) формула оркали хисобланувчи $L_{,h}$ кетма-кетликнинг мос сони h_{ji} га алмаштириш йўли билан L_{lh} сон кетма-кетлигини шакллантириш, бу ерда к1-ўнлик коэффицент; $к_2$-силжитиш коэффициенти. Танланган $к_ь$ $к_2$ коэффицентлар h_{oi}, h_{ij} сонларнинг бир маъноли мослигини таъминлаши лозим, hij=0 олинганида эса hij=R алмашинуви бажарилиши керак.

3- кадам. Lih кетма-кетликнинг хар бир сони $h_{,j}$(s_{li}) ни [lxR] ўлчамли шифрлаш алфавитнинг мос Sji, € Ti($i^{=1k}$) символи билан алмаштириш йули билан Ti шифрматнни хосил қилиш.

4- қадам. Олинган шифрматн ўзгармас В узунликдаги блокларга ажратилади. Агар охирги блок тўлиқ бўлмаса блок оркасига махсус символ-тулдирувчилар жойлаштирилади (масалан:*).

Шифрловчи жадвал усулида калит сифатида куйидагилар кулланилади:

— жадвал ўлчовлари;

— сўз ёки сўзлар кетма-кетлиги;

— жадвал таркиби хусусиятлари.

Масалан:

T_0=КАДРЛАР ТАЙЁРЛАШ МИЛЛИЙ ДАСТУРИ

К=4х7; В=4;

Ушбу ахборот устун бўйича кетма-кет жадвалга киритилади:

К	л	А	Л	и	и	т
А	А	Й	А	л	д	У
д	Р	Е	Ш	л	А	р
р	Т	Р	м	и	С	и

Натижада, 4х7 ўлчовли жадвал ташкил килинади. Энди шифрланган матн каторлар буйича аникланади, яъни ўзимиз учун 4 тадан белгиларни ажратиб ёзамиз.

У	К	О	Л	Г	ю	В
З	И	Н	А	И	к	Л
Б	С	К	Ж	Б	д	А
Е	Т	Е	А	У	А	Т

Энди калит оркали 7х6 жадвал тузиб калитдаги харфларни алфавит буйича ракамлаб чикамиз.

КЛАЛ_ИЙТА_АЙАЛ_ДУДР_ЁШЛА_РРТР_МИСИ Бу ерда калит сифатида жадвал ўлчовлари хизмат килади. Оддий ўрин алмаштириш усулидан ташкари калит ёрдамида ўрин алмаштириш усули хам мавжуд. Шифрлаш жадвалидан калит оркали фойдаланилади.

Бу ерда калит символларига мое холда жадвалнинг ўлчамига караб МхМ жадвали тузилади ва очиқ матнни ($Т_0$) устун буйича жойлаштирилиб чикилади. Сўнгра калит символлари алфавит тартибида тартибланиб, устун буйича ўрин алмаштирилади, қатор буйича ўқилиб шифрланган матнга (Т,) эга булинади ва блокларга булинади.

$Т_0$= Ўзбекистан келажаги буюк давлат;

К = Тошкент;

В=4;

Матнда 28-та ва калитда 7-та харфлар борлиги учун 7х7 жадвал тузамиз.

Т	0	ш	к	е	н	т
5	4	7	2	1	3	6
У	К	О	Л	Г	ю	В
З	И	н	А	И	к	Л
Б	С	к	Ж	Б	Д	А
Е	т	Е	А	У	А	Т

Ракам буйича устунларни узгартириб чикамиз.

е	к	н	0	т	т	ш
1	2	3	4	5	6	7
Г	Л	Ю	К	У	В	О
И	А	К	И	З	Л	Н
Б	Ж	д	С	Б	А	К
У	А	А	т	Е	Т	Е

Катор буйича 4 тадан блокларга булиб, символлар кетма-кетлигидаги шифрланган матнни оламиз.

Кетма- кераки агар қаторда иккита бир хил символлар кетма —кетлиги келса, чап тарафдан келаётган биривчи ракамланади, кйин эса иккинчисиракамланади ва шифрланган матн хосил қилинади.

T_1= ГЛЮК_ УВОИ_АКИЗ_ЛНБЖ_ДСБА_КУУА_ТЕТЕ

Шифрни очишда тескари жараён a_Mалга оширилади. Шифрланиш жараёни қадамма қадам амалга оширила мақадга муфофиқ бўлар эди.

Икки томонлама ўрин алмаштириш усули.

Бу усулда калит сифатида устун ва қатордагихарфлар тартибдаги сонлардан ойдаланилади.

Аввалом бор калит символларига қараб жадвал тузилади ва очиқ То матн жайлаштириб чиқиқилади, сўнграэса рақамлар навбатма навбат тартибланиб, аввал устун, сўнгра эса қаторлар ўрни алмаштирилади ва жадвалдаги маълумот қатор бўйича ўқилиб T_1 га эга бўлинади. Масалан: “Малакали хизматчи” очиқ матнни шифрлаш талаб этилсин. Бу ерда калитбўлиб 1342 ва 2314 хизмат қилади. Яхшироқ изохланиши учун К1=1342 ва К2=2314, В=4 деб белгилаб оламиз.

4х4 жадвал яратиб T_0 қатор бўйича ёзамиз(1-жадвал). 2-жадвалдаги кўриниш бўйича қатор ва устунлар тартиббилан ўринлари алмаштирилади.

2	3	1	4
М	а	л	а
к	а	л	и
х	и	з	М

1-жадвал

а	т	ч	и

2-жадвал

м	а	л	а
а	т	ч	и
к	а	л	и
х	и	з	м

а	м	а	л
и	а	т	ч
и	к	а	л
м	х	и	з

3-жадвал

3 -жадвалга асосан шифрлачган матни ёзамиз ва блокларга булиб чикамиз.

Т1 =АМАЛ_ИАТЧ_ИКАЛ_МХИЗ

Икки томонлама алмаштиришда жадвал катталигига караб вариантлар хам ортиб боради. Жадвал ўлчамининг катталиги шифр чидамлилигини оширади,

Сехрли квадрат деб, катакчаларига 1 дан бошлаб сонлар ёзилган, ундаги хдр бир устун, сатр ва диагонал буйича сонлар йигиндиси битга сонга тенг булган квадрат шаклидаги жадвалга айтилади. Сехрли квадратга сонлар тартиби буйича белгилар киритилади ва бу белгилар сатрлар буйича укилганда матн хосил булади.

Сехрли квадрат - кадимги Хитой тарихига бориб такалади. Афсоналарга кура Ю императори бошкаруви вактида (бизнинг асримиздан 2200 йил илгари) Хуанхэ (Сарик дарё) суви остидан тошбака сузиб чикади ва бу тошбакд устидаги тоши(панцири)да махфий иероглифлар чизилган бўлиб, кейинчалик бу белгилар «ло-шу» атамаси билан номланган (1(6) - расм).

XI асрга келиб сехрли квадрат билан Хиндистон, кейинчалик эса Япония олимлари шугилланишган. Европага сехрли квадрат хакида маълумотлар XV асрдан етиб келган.

4	9	2
3	5	7
8	1	6

Сехрли квадрат йигиндисини топиш куйидаги тартибда амалга оширилди: $1 + 2 + ... + n = n^2 + 1)/2$. Шунинг учун диоганаллар (қатор ва устун хам) йигиндиси M(n)=n(n2+1)2. га тенг. Қуйидаги жадвалда мумкин бўлган n*n жадвалларнинг йигиндиси курсатилган.

n тартиби	3	4	5	6	7	8	9	10	11	12	13
M(n)	15	34	65	111	175	260	369	505	671	870	1105

Мисол.

4_X4 ўлчовли сехрли квадратни оламиз, бу ерда сонларнинг 880

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

Бошлангич матн сифатида куйидаги матнни оламиз:

T_0=Д А С Т У Р Л А Ш Т И Л Л А Р И

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

Шифрланган матн жадвал элементларини сатрлар бўйича ўқиш натижасида ташкил топади:

T1=ИСАЛ_УТИА_ШРЛЛ_ТРАД

Классик махфий криптотизимларга хам олишимиз мумкин. Силжитиш шифри икки турга бўлинади. Улар

оддий ва мураккаб силжитиш шифрларидир. Оддий силжитиш шифрида алфавит буйича силжиган харфлар билан шифрланаётган матн харфлари алфавитга мос равишда алмаштириш оркали шифрлаш амалга оширилади. Бир турли алмаштириш шифри оддий силжитиш шифрининг бир кисми хисобланади.

Оддий алмаштиришли шифр. Алмаштириш усуллари сифатида қуйидаги усулларни келтириш мумкин: Цезар усули, Аффин тизимидаги Цезар усули, таянч сўзли Цезар усули ва бошкалар.

Цезар шифри оддий силжитиш шифрининг бир кисми хисобланади. Бу шифрни римлик император Голе Юлий Цезар ўйлаб топтан. Шифрлашда матннинг хар бир харфи бошқа харф билан куйидаги қоида асосида алмаштирилади. Харфларни алмаштиришда келаётган ёзув харфларини К-га силжитиб алмаштирилади. Бу эрда К-бутун сон хисобланиб уни куйидагича ифодалаш мумкин. *К=К (modm), m* -алфавит сони. Юлий Цезар бевосита к = 3 бўлганда ушбу усулдан фойланган.

Цезар усулининг камчилиги бу бир хил харфларнинг ўз навбатида, бир хил харфларга алмашишидир.

Масалан, матн сифатида T_0=KOMPUTER сузини ва К=3 деб оладиган булсак Цезар усули натижасида куйидаги шифрланган ёзув хосил бўлади:

T, =NRPSXWHU.

Аффин тизимидаги Цезар усулида хар бир харфга алмаштирилувчи харфлар махсус формула' буйича аникланади: *at+b, (modm),* бу ерда a, b - бутун сонлар, 0<a, b<m.

m=26, a=3, b=5

бўлганда Шунга мое равишда қилинади:

қуйидагича алмашади:

т	3t+5		A	F
0	5		B.	J
1	8		C	N
2	11		D	R
3	14		E	S
4	17		. F	V
5	20		G	Z
6	23		H	D
7	26		1	H
8	29		J	L
9	32		K	, P
10	35		L	T
11	38		м	X
12	41		N	B
13	44		0	F
14	47		p	J
15	50		Q	N
16	53		R	R
17	56		S	V
18	59		T	Z
19	62		и	D
20	65		V	H
21	68		W	L
22	71		x	P
23	74		Y	T
24	77		Z	X
25	80			
26	83			

харфлар

T1=PFXJDZSR

Калит сузли Цезар тизими. Цезарнинг калит сўзли шифрлаш тизими битта алфавитли алмаштириш тизими хисобланади. Бу усулда калит сўзи оркали хдрфларнинг суришда ва тартибини ўзгартиришда фойдаланади. Лотин алифбоси

асосида шифрлаш. Калит сузини танлашда такрорланмайдиган хар хил харфлардан иборат булган сузни танлаш максадга мувофикдир. Бу усул амалиётда кулланилмайди.Чунки калит сўзли Цезар шифрини кириптотахлил асосида очиш мумкин.

Мураккаб алмаштиришли шифр. Мураккаб алмаштиришли шифр кўп алфавитли бўлиб, шифрлашда келувчи матннинг хар бир харфи узининг оддий алмаштириш шифри каби шифрланади. Куп алфавитли алмаштиришда алфавит кетма-кетлиги ва циклидан фойдаланилади.

А-алфавитли алмаштиришда кирувчи ахборотнинг X_0-харфи Во-алфавитнинг $У_0$-харфи билан алмаштирилади, Х,-харфи эса В,- алфавитнинг $У_г$-харфи билан алмаштирилади, $X_р$.,-харфи $B_{р.г}$ алфавитнинг $Y_р$.,-харфи билан алмаштирилади ва хоказо.

Куп алфавитли алмаштиришнинг р=4.булган хол учун умумий кўриниши куйидаги жадвалда келтирилган.

Кирувчи харфлар	Х О	XI	Х 2	Х З	Х 4	Х 5	Х 6	*XI*	Х 8	Х 9
Алфавит алмаштириш	В О	В1	В 2	В З	В О	В 1	В 2	В З	В О	В 1

Бу усул билан шифрланган матнни очишда етарли кийинчиликлар тугдиради, энди k-калит бир-неча маротаба узгаради. Гамма шифри ихтиёрий кўринишда хар бир шифрланаётган булакни узгартиради. Бунда душман хар бир матн булагини кандай килиб очишни бундай шифрлашда химояланганлик даражаси фойдаланиётган Bj-алфавит кетма-кетлигига богликдир. Куп алфавитли алмаштириш шифрини Леон Батист Алъберт криптографияга киритди.

Вижинернинг шифрлаш тизими. Биринчи булиб Вижинер тизими 1586-йилда чоп этилган ва у куп алфавитли тизимга нисбатан юкорирок ўрин да туради. Блеза Вижинера узини XVI асрнинг француз дипломата деб хисоблайди. У криптография тизимига, яъни унинг ривожланишига уз хиссасини кушган. Вижинер тизими Цезар шифрлаш тизимига Караганда мукаммалрок х,исобланиб, унда калит хдрфидан хдрфга алмаштирилади. Бундай куп алфавитли алмаштириш шифрини шифрлаш жадвали оркали ифодалаш мумкин. Куйидаги жадвалда Вижинернинг инглиз алфавита учун мое келувчи жадвал курсатилган.

Бу жадвалдан матнни шифрлаш ва уни очиш учун ишлатилади. Жадвалнинг иккита кириши булиб: Юкори қатор даги харфлардан кирувчи очик ёзув учун фойдаланилади.

Чап устундан эса калит харфларидан фойданилади. Мисол учун калит кетма-кетлигини р-деб олайлик, у холда калит р-алфавитли р-сатрдан иборат булади.

Ж=(л$_0$, 7t$_b$...,7t$_r$.i);

Вижинернинг шифрлаш тизимида очик матн х=(х$_0$,х$_ь$...,х$_{Г]\cdot 1}$) ва шифрланганп матн у=(Уо,Уь---,Уп-0 кўринишга эга. 7t=(*о, я$_ь$...,тг$_г$.,) калит ёрдамида куйидагича муносабатда булади.

х$^{=}$(х0,хі,... ,х$_n$_i) у=(уо,уи---,уп-і);

(Уо,У Ь • • • ,Уп-1)=(7Іо(Хо),7І,(Х,),... ,Я,,.1 (Хп-1)); Юкоридаги ифодадан маълумки Вижинер жадвали оркали шифрлашда матннинг (ахборотнинг) хар бир харфига мое келувчи калитнинг хар бир харфи оркали уларнинг устун ва сатрлари кесишмасига мое келувчи харфлар олинади. Агар узбек - кирил алфавити ишлатилса, Вижинер матрицаеи [36х36] ўлчамга эга булади. Масалан, Агар калит сифатида <КУЗА> сузи танланган булса, шифрлаш матрицаеи бешта қатор дан иборат булади.

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯУКГХ_

КЛМНОПРСТУФХЦЧШЬЪЭЮЯУК,ЕХ^_АБВГДЕЁЖЗИЙ

ЎҚҒҲ_АБИГГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯ

ЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯУКГ^АБВГДЕЁЖ

УКЕ^АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯ

ЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯУКГ^АБВГДЕЁЖ

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯУКГ^ Мисол. К=<КУЗА> калити ёрдамида Т=<БАЙРАМ КУНИ> дастлабки матни шифрлансин.

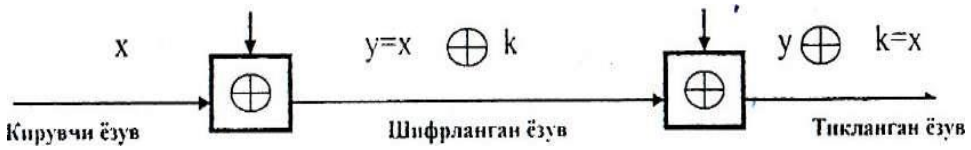
Очик матн	Б	А	Й	Р	А	М	_	К	У	Н	И
Калит	К	У	З	А	К	У	З	А	К	У	З
Шифрланган матн	Л	У	С	Р	К	З	Ж	К	У	И	Р

Т1=ЛЎСР_КЗЖК_ЎИР.

Вернамнинг шифрлаш усули. Вернамнинг шифрлаш тизими модул киймати т-2 булган Вижинер шифрлаш тизимининг бир кием и хисобланиб, 1926-йилда бу усулнинг аник кўриниши ишлаб чикилади.Гилбэртом Вернам АТ&США фирмаси хомийлиги остида кирувчи матн сифатида иккилик санок системасидан фойдаланди. Шифрлашда биринчи инглиз алфавитидаги(А,В---2) матннинг хдр бир харфи 5-бит булакли ((b$_0$,b$_1$...b$_4$) Бадо раками билан кодланади. Ихтиёрий кетма-кетликдаги иккилик калитлар к$_0$, к$_ь$ к$_2$, аввал китобсимон лентага ёзилади. Куйидаги раемда узатилаётган ахборотни Вернам усули оркали шифрлаш курсатилган.

I Калит кетма - кстлигн I

к к



Кирувчи матнни шифрлашда Х-кирувчи матн иккилик кўринишига утказилади ва иккилик модул остида иккилик кетма- кетликдаги k-калит билан шифрлаш амалга оширилади. У шифрланган ёзув: у=х 0 к

Шифрни очишда ёзувдаги хар бир иккилик модул остидаги белгилар k-калит кетма-кетлиги билан тузилади.

Уф к=х ф кф к=х;

Вернам ишлаб чиккан бу тизимни айланали лента ёрдамида текширган, узатгич ва кабул килгичларни кўринишда бир хил ёки шунга ухшаган калит кетма-кетлигидан фойдаланган. Вернам шифрлаш тизимининг камчилиги узатувчи оркали кабул килиш томонига калит кетма-кетлигини кандай узатиш эди. Чунки душман калитни олса, у юборган шифрланган матнни бемалол очиб укий олади. Шунинг учун хам Вернамнинг шифрлаш тизими етарли эмаслиги сабабли буни хал килиш учун шифрлашни гаммалаштириш усулига утилган.

Гаммалаш усули билан шифрлаш. Гаммалаштириш хам криптографии акслантиришда кенг кулланилади. Аслида гаммалаштириш, Вижинер шифри хамда чексиз калитдан фойдаланиш бир-бирига жуда ўхшаш.

Гаммалаштиришда тасодифий сонлар генератори ёрдамида гамма генерация килинади ва у очик матнга кайта тикланадиган усулда (масалан, 2 га модуль бўйича кушиш) қўшилади.

Маълумотларни дешифрлаш жараёни шифр гаммасини маълум калит ёрдамида кайтадан генерация килиш ва бу гаммани шифрланган маълумотдан олиб ташлаш билан амалга оширилади.

Агар шифр гаммасида такрорланувчи битли кетма-кетлик мавжуд бўлмаса шифрланган матнни очиш жуда кийин. Умуман олганда, шифр гаммаси хар бир шифрланадиган суз учун тасодифий равишда узгариши керак. Агар гамма узунлиги бутун шифрланадиган матн узунлигидан ошиб кетса ва очик матннинг хеч кандай кисми маълум бўлмаса, у холда шифрни факат мумкин булган калитларни тула куриб чикиш билан очиш мумкин. Бу холда криптобардошлилик калит узунлиги билан ўлчанади.

Агар ракибга очик матннинг булаги ва унга мос келувчи шифрограммаси маълум булса гаммалаштириш усули кучеиз булиб колади. Модуль буйича оддий айириш оркали тасодифий сонлар кема-кетлиги кисми олинади ва бу кием буйича бутун кетма-кетлик тикланади. Ракиблар буни очик матннинг ташкил этувчилари

асосида тахмин билан топишлари хам мумкин. Куйида амалиётда куллаш мумкин булган гамма генерациясининг кенг таркалган усуллари каралади. Гамма шифри куйидаги кўринишдаги кетма-кетликда олинади.

$Г^{(,)}ш$

Шифрлашни куйидаги кўринишда ёзиш мумкин.

$T^{(}W^{(i)}$ ϕ$T^{0)}$o , i=l..m;

Б. .....

$T^{(0}$ш і-шифрланган матн;

$Г^{(П}$ш і-гамма шифри булади;

$T^{(\circ}$0 і-очик матн булади;

М-(очик) матнни сифат даражаси.

Шифрни очиш да кайта гамма шифридан фойдаланилади**:**

$To=Г_{ш}$ 0 'Ги, /.

Бу усул билан шифрланган матнни очишда етарли кийинчиликлар тугдиради, энди k-калит бир-неча маротаба узгаради. Гамма шифри ихтиёрий кўринишда хар бир шифрланаётган булакни узгартиради. Бунда душман хар бир матн булагини кандай килиб очишни билмайди. Чунки душман хар бир турдаги калитни топиши учун анча вакт кетади. Бу холатда шифрланган матн бардошлилиги куплигига боглик булади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильяме», 2005г.-424с.
2. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
3. Коблиц Н. Курс теории чисел в криптографии. - М., Научное издательство ТВП, 2001 й.
4. Ященко В.В. Введение в криптографию. МЦМО, 2003Й.
5. Масленников А. Практическая криптография BHV - СПб 2003Й.
6. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002й.
8. С.К.Ганиев, М.М. Каримов, К.А. Тошев «Ахборот хавфсизлиги. Ахборот - коммуникацион тизимлари хавфсизлиги», «Алокачи» 2008 йил, 378

СИММЕТРИК КРИПТОТИЗИМЛАР

PES алгоритмининг асог.ий ишлаш тартиби. DES алгоритму 64-битли маълумотлар блокини турли ўрин алмаштириш ва акслантиришлар комбинациясига асосланиб 56 битли к калит билан шифрлашни амалга оширади. DES шифрлаш алгоритмининг схемаси 2.1.-расмда келтирилган. Шифрлаш жараёни, хамда охирги битларни бошлангич ўрин алмаштириш, 16марта шифрлаш циклини такрорланиши хамда охирги битларни ўрин алмаштиришдан иборат.

Алгоритмда келтирилган барча ўрин алмаштириш ва акслантиришлар жадваллари стандарт кабул килинган, алгоритм бажарилишида булар хеч кандай узгартиришларсиз уз холича
сакданади.

Фойдаланилган белгилашлар:

Lj BaRi -64битли блоклни чап ва унг кисмлари;

+-2 модул буйича кушиш амали;

Kj - 48битли i-цикллар калити;

f-шифрлаш функцияси;

f

IP -бошлангич ўрин алмаштириш.

Маълумотнинг T блокини шифрлашда унинг барча битлари

2.1.-жадвалга кура IP бошлангич ўрин алмаштирилади.

Бунда 58-бит T блокнинг 1-бити, 50-бит, 2-бити ва хдк. кўринишда алмаштириш бажарилади.Ўрин алмаштиришдан кейин х,осил булган 1P(T) блок мое равишда икки: L_0 1 битдан 32- битгача ва R_0 33-битдан 64-битгача булган блокларга ажралади.Кейин Фейстел акслантиришларига асосланган 16марта такрорланувчи итератив шифрлаш жараёни бажарилади.

T| ,=Li.iRj-r(i-$^{}$) ~ итерация натижаси булсин. У \олда, i- итерация натижаси T,=L,R, куйидаги формуладан аникланади. *Li=Rj.i*

RrL$_{hl}$+f(R,M, i=l,2,--l

f шифрлаш функцияси дейилади.Функция аргумента 32 битли R_M вектор ва 56 битли шифрлаш к калитдан акслантиришлар асосида олинган 48 битли К, калитдир.T_{16}=К,$_6$Ь$_{16}$ охирги итерация натижаси. Шифрлаш тугаши билан битларнинг уз жойларини кайта тиклаш максадидаT_{16} га IP''' кайта ўрин алмаштиришлар Килинади.Маълумотни кайта шифрлаш учун юкоридаги килинган ишлар тескари тартибда бажарилади, шунга кура (1) муносабат урнига куйидаги муносабатни куллашгатугри келади.

R,-i=Lj

L ,_i=R,+f(L,, к,), i=16....1

F(R,.i,kJ шифрлаш функциясини кийматини хисоблаш схемаси.

F(Rj-i,ki) шифрлаш функциясининг схемаси / шифрлаш функциясининг кийматини хисоблашда Е «кенгайтма» функцияси, *SI, S2...S8* блоклардан иборат 5 ва *P* ўрин алмаштиришлардан фойдаланилади. R*i-1* (32 бит) вектор ва *ki* (48 бит) калитлар/ функцияси аргументи хисобланади.

E «кенгайтма» функцияси 32 битли R*i-1* векторни 2.2. - жадвалга кура бир хил битларни такрорлаш йули билан *E(Ri-JJ* 48 битли вектор **хосил** килади.

2.2.-жадвал.

32	1	2	о J)	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

E(R*i-1)* векторнинг биринчи учта бити мое равшида R/-7 векторни 32,] ва 2-битлар, охирги учта. бити эса *Ri-1* векторни 31, 32,1-битлардир.

Хосил булган нагижа мавжуд *ki* калитга 2 модули буйича битма-бит кушилади ва 6 битлик 8 та *B1.B2 B8* блоклар кетма-кетлигини хосил килинади.

E(Ri-1)+ ki= B1.B2 B8.

Сўнгра хар бир *Bj* блок 4-битли *B'j* блока мое келган *Sj* S - блоклар жадвали ёрдамида узгартирилади, S-блоклар руйхати 2.3.- жадвалда келтирилган.

2.3.-жадвал.

S(l)

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

S(2)

5	1	8	14	6 11	o J	4	9	7 ! 2 1 .	13	12	0	5	10

3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	o J	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S (3)

10	0	9	14	6	J	15	5	1	13	12	7	11	4	2	3
13	7	0	9	o J	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	•*i* J	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S(4)

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	o *J*	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	O *J*	14	5	2	8	4
o J	15	0	6	10	1	13	8	9	4	*5*	11	12	7	2	14

В,- блокнинг Bj га у^{ЗГА}Р^{ТИ}Р^{ИЛ}ишини битта мисол оркали келтирамиз. Масалан B_2 блок 111010 дан иборат булсин. B_2 блокни биринчи разряди а,=1 $a=a_1a_6$ сонининг иккилик санок системасидаги ёзуви булса, бу соннинг унлик сонок

системасидаги киймати 4 дан катта булмайди, яъни 0<a<4. Орадаги 4 та Ь=a_2аза4a_5=1101 дан ташкил топган b сони эса 0<Ь<16 муносабатни каноатлантиради. Бизнинг мисолда а=2, Ь=13.

S_2 блокнинг сатрлари 0 дан а гача булган сонлар билан устунлари эса 0 дан b гача булган сонларда ракамлаб чикилган. Шундай килиб, (а,Ь) сонлар жуфтлиги жадвалдаги а-сатр ва Ь- устуннинг кесишмасидаги бирор сонини аниклайди. Ушбу холатда кесишмада турган сон 3. Бу сонни иккилик санок системасига утказиб B_2ни хосил киламиз.(0011)

F(Rj.[к,) киймати Р битли ўрин алмаштиришларни 2.4,- жадвалдан фойдаланиб куллаган холда хосил килинади.

2.4-жадвал

16	7	20	21
24	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	->	9
19'	13	30	6
22	П	4 /	25

Х,ар бир итерация к, (48 бит) калитнинг айни пайтдаги киймати фойдаланилади. Ушбу кийматлар дастлабки к калитдан куйидагича олинади. Дастлаб фойдалануви 56 та ихтиёрий битли калитни танлайди. 8.16....64 ўринларда турган 8 та бит калитга шундай куйиладики, ундаги х,ар бир байт ток сондаги бирлик ракамларни уз ичига олеин. Лекин бу битлар шифрлашда катнашмайди. Бу калитларни узатиш ва саклашда учрайдиган айрим хатоликларни топишда жуда кул келади. 56 бит калит 2.5.-жадвалга кура ўрин алмаштиришлар асосида олинади.

2.5.-жадвал.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Бу ўрин алмаштириш хар бир 28 битдан иборат булган иккита C_0 ва D_0 блоклар билан аникданади (улар мое равишда жадвалнинг

юкори ва пастки кисмларни эгаллаган). C_0 *ни* учта олдинги битлари калитнинг 57,49,41 учта битларига мое келади ва жадвал асосида давом эттириладй. Кейин индуктив йул билан С, ва Д (i=l,....16) блоклар аникланади. Агар *Ci-1* ва *Di-1* лар аникланган булса, у холда *Ci* ва *Di* лар улардан 2.6.-жадвалга асосан бир ёки иккита чапга циклик сураш билан хосил килинади.

2.6.-жадвал.

. 1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Суришлар сони	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Энди, *к, (l< г< 16)* калитни аниклаймиз. *ki* калит 48 битдан ташкил топган булиб, улар 2.7.-жадвалга асосан С, *D,* блок битларидан танлаб олинган. Такидлаш жоизки, С, Д даги 56 битдан 8 таси (9,18,22,25,35,38,43,54 ракамли) *к,* да йук-

2.7.-жадвал.

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильяме», 2005г.-424с.
2. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
3. Коблиц Н. Курс теории чисел в криптографии. - М., Научное издательство ТВП, 2001 й.
4. Ященко В.В. Введение в криптографию. МЦМО, 2003й.
5. Масленников А. Практическая криптография BHV — СПб 2003й.
6. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком,2002Й.

8. С.К.Ганиев, М.М. Каримов, К.А. Тошев «Ахборот хавфсизлиги. Ахборот - коммуникацион тизимлари хавфсизлиги», «Алокачи» 2008 йил, 378 бет.

3 – Лаборатория машғулотлари.

ОЧИҚ; КАЛИТЛИ ШИФРЛАШ АЛГОРИТМЛАРИ

Очик калитли RSA криптоалгоритми. RSA бир томонли функцясига асосланган тартиб ва коидаларни бошкариш криптотизими хисобланади. Бу криптотиз'имини калитларни таксимлаш тартиб ва коидаларини бошкариш криптотизими учун хам куллаш мумкин. Тартиб ва коидаларни бошкариш масалалари, криптотизимиларига дойр криптологик илмий изланишлар хозирда, замонавий, бардошли криптографик тизимларни яратишда кенг ва жадал ривожланиб бормокда. Бу сохада RSA бир томонли функциясидан фойдаланишнинг кулайлиги ўзини хар томонлама оклаб келмокда.

RSA алгоритмини кулланишига дойр кичик бир мисол келтирамиз.

Мисол: Учта харфдан иборат булган "САВ" маълумотини шифрлаймиз.

Биз кулайлик учун кичик туб сонлардан фойдаланамиз Амалда эса мумкин кадар каттатуб сонлар билан иш курилади.

1. Туб булган p=3 ва $д$= 11 сонларини танлаб оламиз.
2. Ушбу $n=pq$=3*11=33 сонини аниклаймиз.

Су игра, (0(33) = *{p-\){q-\)* = 2-10 = 20 сонини топамиз, хамда бу сон билан 1 дан фаркли бирор умумий булувчига эга булмаган d сонини, мисол учун d= 3 сонини, оламиз.

3. Юкорида келтирилган (24) шартни каноатлантирувчи е сонини Зе=1 (mod 20) тенгликдан топамиз. Бу сон e= 7
4. Шифрланиши керак булган «САВ» маълумотини ташкил этувчи харфларни: А—И, В-»2, С-»3 мосликлар билан сонли кўринишга утказиб олиб, бу маълумотни мусбат бутун сонларнинг, кетма-кетлигидан иборат деб караймиз. У холда маълумот (3,1,2)кўринишда булади ва уни {е;п}={7;33} очик калит билан /. (х) = ,\-^{7}(mod33) бир томонли функция билан шифрлаймиз:

х=3да ШМ1=(3^{7})(тоёЗЗ)=2187(mod33)=9,
х=1 да ШМ2=(1^{7}) (mod33)=l,
д:=2да ШМЗ=(2^{7}) (mod33)=128(mod33)=29

5. Бу олинган шифрланган (9,1,29) маълумотни махфий {^;и}={3;33} калит билан /.'"= $У^{3}$(^{тос13}3;ифода оркали дешифрлаймиз:

у=9 да ОМ1=(9^{3}) (mod33)=729(mod33)=3,
у=\ да ОМ2=(1^{3}) (mod33)=l(mod33)=l,
у-29 да ОМЗ=(29^{3}) (mod33)=24389(mod33)=2.

Шундай килиб, криптотизимиларда RSA алгоритмининг кулланиши куйидагича: х,ар бир фойдаланувчи иккита етарли даражада катта булмаган p ва q туб сонларни танлайдилар ва юкорида келтирилган алгоритм буйича d ва e туб сонларини х,ам танлаб олади. Бунда $n=pq$ булиб, $\{e;n\}$ очик калитни $\{d;ri\}$эса махфий калитни ташкил этади. Очик калит очик маълумотлар китобига киритилади. Очик калит билан шифрланган шифрматнни шу калит билан дешифрлаш имконияти йук булиб, дешифрлашнинг махфий калити факат шифр маълумотининг хаки кий эгасигагина маълум.

Эль - Гамал криптотизими. Эль - Гамал тизими RSA тизимига мукобил (алтернатив) булиб, бу криптотизимиларнинг калитларининг ўлчов узунлнклари тенг булганда бир - хил криптобардошлиликга эга буладилар.

Эль - Гамал криптотизими Диффи-Хеллман алгоритмига ухшаш булиб, дискрет логарифмларни хисоблаш масаласи ечимининг мураккаблигига асосланган. Бу криптотизими асосини туб булган р ва ва бутун булган g сонлари ташкил этади. куйида ушбу тизимнинг мохиятини очиб берувчи мисолни келтирамиз.

Бирор фойдаланувчи (А) махфий калит а сонини танлаб олади ва $y = g''' \bmod p$. булган очик калитни хисоблайди. Агарда мана шу фойдаланувчи (А) билан бирор бошка фойдаланувчи (Б) махфий маълумотни жунатмокчи булса, у х,ол,а,а (Б) р сонидан кичик булган бирор криптотизими сонини танлаб олиб

$V, = g^k$ тоф ва $y_2 = m$ ® y^{κ}, сонларини хисоблайди, бу ерда ® белгиси 2 модул буйича битларни кушиш амалини билдиради, яъни m ва y^{κ} сонлари иккилик санок тизимида, деб тушинилади. Сўнгра (Б) 0'i'>'2) маълумотларини (А)га жунатади. уз навбатида (А) бу шифрланган маълумотни кабул килиб, куйидаги

$\{y''' \bmod p)$ ® $y_2 = m$ булган хисоблаш билан маълумотнинг очик матнини тиклайди.

Шифрлашни комбинацион усули. Шифрлашнинг комбинацияланган усуллари. Кудратли компьютерлар, тармок технологиялари ва нейронли хисоблашларнинг пайдо булиши хозиргача умуман фош килинмайди деб хисобланган криптографик тизимларни обрусизлантирилишига сабаб булди. Бу эса уз навбатида юкори бардошликка эга криптографик тизимларни яратиш устида ишлашни +акозо этди. Бундай криптографик тизимларни яратиш усулларидан бири шифрлаш усулларини комбинациялашдир. К^/йида энг кам вакт сарфида криптобардошликни жиддий. ошишини таъминловчи шифрлашнинг комбинацияланган усули устида суз боради. Шифрлашнинг ушбу комбинацияланган усулига биноан маълумотларни шифрлаш икки боскичда амалга оширилади. Биринчи боскичда маълумотлар стандарт усул (масалан, DES усул) ёрдамида шифрланса, иккинчи боскичда шифрланган маълумотлар махсус усул буйича кайта шифрланади. Махсус усул сифатида маълумотлар векторини

элементлари нолдан фаркли булган сон матрицасига купайтир'ишдан фойдаланиш мумкин.

Гаммалашни куллашда агар шифр гаммаси сифатида ракамларнинг такрорланмайдиган кетма-кетлиги ишлатилса шифрланган матнни фош килиш жуда кийин. Одатда шифр гаммаси хар бир шифрланувчи суз учун тасодифий узгариши лозим. Агар шифр гаммаси шифрланган суз узунлигидан катта булса ва дастлабки матннинг хеч кандай кисми маълум бўлмаа, шифрни факат тугридан-тугри саралаш оркали фош этиш- мумкин. Бунда криптобардошлик калит ўлчами оркали аникланади. Шифрлашнинг бу усулидан купинча химоя тизимининг дастурий амалга оширилишида фойдаланилади ва шифрлашнинг бу усулига асосланган тизимларда бир секундда маълумотларнинг бир неча юз ЬСбайтини шифрлаш имконияти мавжуд. Расшифровка жараёни-калит маълум булганида шифр гаммасини кайта генерациялаш ва уни шифрланган маълумотларга сингдиришдан иборат.

Шифрланган маълумотлар векторини матрицага купайтиришни куллашда шифрланган матн бйр байт узунликдаги векторларга

, *"mL* -

ажратилади ва хар бир вектор квадрат матрица [1] "• га купаитирилади

ва шифрланган векторлар шакллантирилади:

G'.' •.G'. -w„

Бу усулнинг асосий афзаллиги сифатида унинг маълумотлар ишланишининг турли жабхаларидаги мосланувчанлигини курсатиш мумкин. X^p бир вектор алохида шифрланган лиги сабабли маълумотлар блоки ни узатиш ва дастурланган маълумотлардан ихтиёрий фойдаланиш имконияти тугилади. Ушбу усулни аппарат ёки дастурий усулда амалга ошириш мумкин.

Дешифрлаш жараёнида шифрланган / векторларни тескари

(Ki) •• -

матрица " * 1'га купаитирилади.

G'. - G'.' • m „ "

Комбинацияланган усулларнинг юкори самарадорлигига унинг иккала боскичини аппарат усулда амалга ошириш оркали эришиш мумкин. Аммо бу ускуна харажатларининг жиддий ошишига олиб келади. Дастурий усулда амалга оширилишида эса маълумотларни шифрлаш ва, Дешифрлаш вакти ошиб кетади. Шу сабабли комбинацияланган усуларни аппарат-дастурий усулда, яъни усулнинг бир боскичи аппарат усулда, иккинчи боскичи дастурий усулда амалга оширилиши максадга мувофик хисобланади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильяме», 2005г.-424с.
2. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
3. Коблиц Н. Курс теории чисел в криптографии. - М., Научное издательство ТВП, 2001 й.
4. Масленников А. Практическая криптография BHV - СПб 2003Й.
5. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
6. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002Й.
9. С.К.Ганиев, М.М. Каримов, К.А. Тошев «Ахборот хавфсизлиги. Ахборот — коммуникацион тизимлари хавфсизлиги», «Алокачи» 2008 йил, 378 бет.

4 – Лаборатория машғулотлари.

ЭЛЕКТРОН РАКАМЛИ ИМЗО

Электрон хужжатларни тармок оркали алмашишда уларни ишлаш ва саклаш харажатлари камаяди, кидириш тезлашади. Аммо, электрон хужжат муаллифини ва хужжатнинг узини аутентификациялаш, яъни муаллифнинг хакикийлигини ва олинган электрон хужжатда узгаришларнинг йуклигини аниклаш муаммоеи пайдо булади.

Электрон хужжатларни ауентификациялашдан максад уларни мумкин булган жинояткорона харакатлардан химоялашдир. Бундай харакатларга куйидагилар киради:

- фаол ушлаб колиш - тармокка уланган бузгунчи хужжатларни (файлларни) ушлаб колади ва узгартиради.
- маскарад - абонент С хужжатларни абонент В га абонент А номидан юборади;
- ренегатлик - абонент А абонент В га хабар юборган булсада, юбормаганман дейди;
- алмаштириш - абонент В хужжатни узгартиради, ёки янгисини шакиллантирадива уни абонент А дан олганман дейди;
- такрорлаш - абонент А абонент В га юборган хужжатни абонент С такрорлайди.

Жинояткорона харакатларнинг бу турлари уз фаолиятида компьютер ахборот технологияларидан фойдаланувчи банк ва тижорат структураларига, давлат корхона ва ташкилотларига хусусий шахсларга анча- мунча зарар етказиши мумкин.

Электрон ракамли имзо методологияси хабар яхлитлигини ва хабар муаллифининг хакикийлигини текшириш муаммосини самарали хал этишга имкон беради.

Электрон ракамли имзо телекоммуникация каналлари оркали узатилувчи матнларни аутентификациялаш учун ишлатилади. Ракамли имзо ишлаши буйича оддий кулёзма имзога ухшаш булиб, куйидаги афзалликларга эга:

- имзо чекилган матн имзо куйган шахсга тегишли эканлигини тасдиклайди;
- бу шахсга имзо чекилган матнга боглик мажбуриятларидан тониш имкониятини бермайди;
- имзо чекилган матн яхлитлигини кафолатлайди.

Электрон ракамли имзо - имзо чекилувчи матн билан бирга узатилувчи кушимча ракамли хабарнинг нисбатан катта булмаган еонидир.

Электрон ракамли имзо асимметрик шифрларнинг кайтарувчанлигига хамда хабар таркиби, имзонинг узи ва калитлар жуфтининг узаро богликлигига асосланади. Бу элементларнинг хатто биринин узгариши ракамли-имзонинг хакикийлигини тасдиклашга имкон бермайди. Электрон ракамли имэо шифрлашнинг асимметрик алгоритмлари ва хеш-функциялари ёрдамида амалга оширилади.

Электрон ракамли имзо тизимининг кулланишида бир- бирига имзо чекилган электрон хужжатларни жунатувчи абонент тармогининг мавжудлиги фараз килинади. Х,ар бир абонент учун жуфт - махфий ва очик калит генерацияланади. Махфий калит абонентда сир сакланади ва ундан абонент электрон ракамли имзони шакллантиришда фойдаланади.

Очик калит бошка барча фойдаланувчиларга маълум булиб, ундан имзо чекилган электрон хужжатни кабул килувчи электрон ракамли имзони текширишда фойдаланади.

Электрон ракамли имзо тизими иккита асосий муолажани амалга оширади:

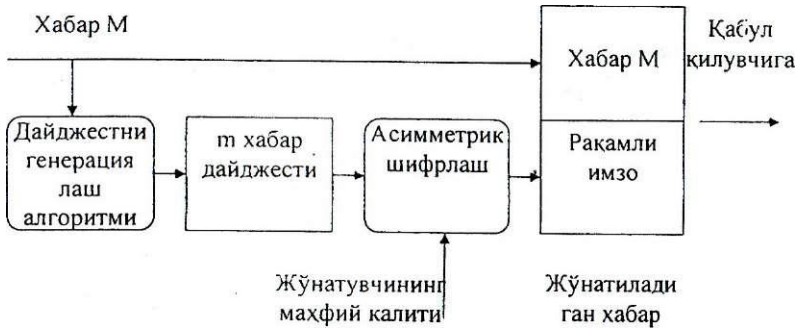
- ракамли имзони шакллантириш муолажаси;
- ракамли имзони текшириш муолажаси.

Имзони шакллантириш муолажасида хабар жунатувчисининг махфий калити ишлатилса, имзони текшириш муолажасида жунатувчининг очик калитидан фойдаланилади.

Ракамли имзони шакллантириш муолажаси. Ушбу муолажани тайёрлаш боскичида хабар жунатувчи абонент А иккита калитни генерациялайди: махфий калит $к_А$ ва очик калит $К_А$. Очик калит $К_А$ унинг жуфти булган махфий калити $к_А$ дан хисоблаш оркали олинади. Очик калит $К_Л$ тармокнинг бошка абонентларига имзони текширишда фойдаланиш учун таркатилади.

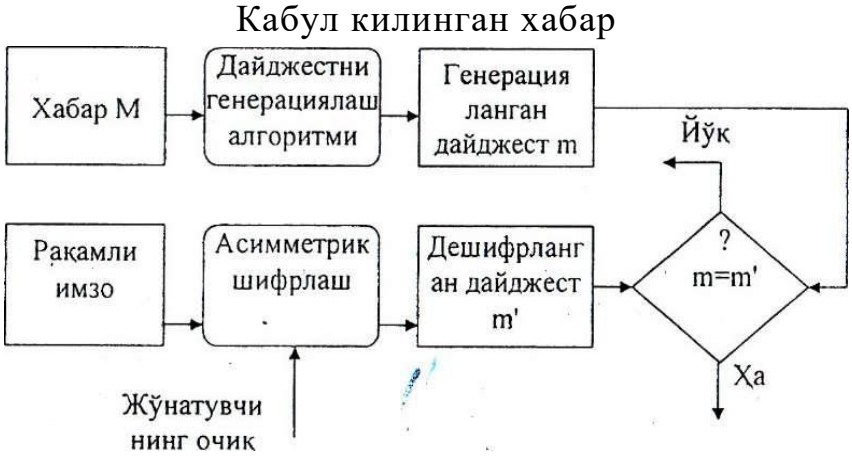
Ракамли имзони шакллантириш учун жунатувчи А аввало имзо чекилувчи матн М нинг хеш функцияси L(M) кийматини хисоблайди (4.1 .-раем).

Хеш-функция имзо чекилувчи дастлабки матн "М" ни дайджест "т" га зичлаштиришга хизмат килади. Дайджест М-бутун матн "М" ни характерловчи битларнинг белгиланган катта булмаган сонидан иборат нисбатан киска сондир. Сўнгра жунатувчи А узининг махфий калити $к_A$ билан дайджест "т" ни шифрлайди. Натижада олинган сонлар жуфти берилган "М" матн учун ракамли имзо хисобланади. Хабар "М" ракамли имзо билан биргаликда кабул килувчининг адресига юборилади.



$к_A$

Электрон ракамли имзони шакллантириш схемаси Ракамли имзони текшириш муолажаси. Тармок абонентлари олинган хабар "И" нинг ракамли имзосини ушбу хабарни жунатувчининг очик калити $К_A$ ёрдамида текширишлари мумкин.



4.2.-расм. Электрон ракамли имзони текшириш схемаси.

Электрон ракамли имзони текширишда хабар "М"ни кабул килувчи "В" кабул килинган дайджестни жунатувчининг очик калити "$К_A$" ёрдамида дешифрлайди. Ундан ташкари, кабул килувчини узи хеш-функция h(M) ёрдамида кабул килинган хабар "М" нинг дайджести "т" ни хисоблайди ва уни дешифрлангани билан таккослайди. Агар иккала дайджест "т" ва "т"' мое келса ракамли имзо хакикий хисобланади. Акс холда имзо калбакилаштирилган, ёки ахборот мазмуни узгартирилган булади.

Электрон ракамли имзо тизимининг принципиал жихати- фойдаланувчининг электрон ракамли имзосини унинг имзо чекишдаги махфий калитини билмасдан калбакилаштиришнинг мумкин эмаслигидир. Шунинг учун имзо чекишдаги махфий калитни рухсатсиз фойдаланишдан химоялаш зарур. Электрон ракамли имзонинг махфий калитини, симметрик шифрлаш калитига ухшаб, шахеий калит элитувчисида, химояланган холда саклаш тавфеия этилади.

Электрон ракамли имзо имзо чекилувчи хужжат ва махфий калит оркали аникланувчи ноёб сондир. Имзо чекилувчи хужжат сифатида хар кандай файл ишлатилиши мумкин. Имзо чекилган файл имзо чекилмаганига бир ёки бир нечта электрон имзо кушилиши оркали яратилади.

Имзо чекилувчи файлга жойлаштирилувчи электрон ракамли имзо имзо чекилган хужжат муаллифини идентификацияловчи кушимча ахборотга эга. Бу ахборот хужжатга электрон ракамли имзо хисобланмасидан олдин кушилади. Х,ар бир имзо куйидаги ахборотни уз ичига олади:

- имзо чекилган сана;
- ушбу имзо калити таъсирининг тугаши муддати;
- файлга имзо чекувчи шахе хусусидаги ахборот (Ф.И.Ш., мансаби, иш жойи);
- имзо чекувчининг индентификатор и (очик калит номи);
- ракамли имзонинг узи.

Асимметрик шифрлашга ухшаш, электрон ракамли имзони текшириш учун ишлатиладиган очик калитнинг алмаштирилишига йул куймаслик лозим. Фараз килайлик, нияти бузук одам "п" абонент "В" компьютерида сакланаётган очик калитлардан, хусусан, абонент А нинг очик калити $К_А$ дан фойдалана блади. Унда у куйидаги харакатларини амалга ошириши мумкин:

- очик калит $К_А$ сакланаётган файлдан абонент А хусусидаги инденцификация ахборотини укиши;
- ичига абонент А хусусидаги индентификация ахборотини ёзган холда шахеий жуфт калитлари к,, ва $К_п$ ни генерациялаши;
- абонент Вда сакланаётган очик калит $К_А$ни ^зининг очик калити $К_п$ билан алмаштириши.

Сўнгра нияти бузук одам "п" абонент В га хужжатларни узининг махфий калити к,, ёрдамида имзо чекиб жунатиши мумкин. Бу хужжатлар имзосини текширишда абонент В абонент А имзо чеккан хужжатларни ва уларнинг электрон ракамли имзоларини тугри ва хеч ким томонидан модификацияланмаган деб хисоблайди. Абонент А' билан муносабатларини бевосита ойдинлаштирилишигача В абонентда олинган хужжатларнинг хакикийлигига шубха тугилмайди.

Электрон ракамли имзонинг қатор алгоритмлари ишлаб чикилган. 1977 йилда АКШ да яратилган[3]RSA тизими биринчи ва дунёда машхур электрон

ракамли имзо тизими хисобланади ва юкорида келтирилган принципларни амалга оширади. Аммо ракамли имзо алгоритми RSA жиддий камчиликка эга. У нияти бузук одам га махфий калитни билмасдан, хешлаш натижасини имзо чекиб булинган хужжатларнинг хешлаш натижаларини купайтириш оркали хисоблаш мумкин булган хужжатлар имзосини шакллантиришга им кон беради.

Ишончлилигининг юкорилиги ва/ шахсий компьютерларда амалга оширилишининг кулайлиги билан ажралиб турувчи ракамли имзо алгоритмли 1984 йилда Эль Гамал томонидан ишлаб чикилди. Эль Гамалнинг ракамли имзо алгоритми (EGSA) RSA ракамли имзо алгоритмидаги камчиликлардан холи булиб, АКШ нинг стандартлар ва технологияларнинг Миллий университета томонидан ракамли имзонинг миллий стандартига асос каби кабул килинди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильяме», 2005г.-424с.
2. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
3. Коблиц Н. Курс теории чисел в криптографии. - М., Научное издательство ТВП, 2001 й.
4. Масленников А. Практическая криптография BHV - СПб 2003Й.
5. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
6. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002Й.
7. С.К.Ганиев, М.М. Каримов, К.А. Тошев «Ахборот хавфсизлиги. Ахборот - коммуникацион тизимлари хавфсизлиги», «Алокачи» 2008 йил, 378 бет.

- **5– Лаборатория машғулотлари.**

КВАНТ КРИПТОГРАФИЯСИНИНГ МАЪЛУМОТ КАЛИТИ ТАКСИМОТИ ТИЗИМИНИ ПРОТОКОЛЛАРИ

Квантли объектлар билан ахборотларни сохталаштириш ва рухсат этилмаган киришдан химоя килиш фикрини биринчи булиб 1970 йил Стефан Вейснер томонидан айтилган. 10 йилдан сунг, Вейснер билан таниш булган Беннет ва Брассард Вейснернинг ишини давом этиб, квантли обектлар ёрдамида махфий калитларни юборишда ишлатган. 1984 йили IBM фирмаси ходими Чарлз Беннет ва Монрела университета олими Жил Брассор фотонларнинг криптография сохасида фундаментал химояланган алока каналини ташкил килиши мумкинлигини аниклашган. 0 ва 1 ларни ташкил килиш учун фотонларни олишга карор килишди, бу фотонларнинг турли кутблари оркали ташкил килинади. BB84 деб номланувчи квантли шифрлаш калитларини аниклаш схемасини тузиб

чикишди. Кейин рок, 1991 йилда бу гоя Экерт томонидан шакллантирилди. Бу схема квантли канални куллайди, кайсики алокани химояланган сеанси иштирокчилари бир бирлари билан маълумот алмашиш учун уларни кутбланган фотонлар кўринишида юборади.

Квантли криптография технологияси квант тизимининг куйидаги хоссасига асосланган - бир вактнинг узида кордината ва импулс кисмларини кабул кила олмайди ва фотоннинг бир параметрини бошка бир фотонни бузмасдан узгартириб булмайди. Бу табиатнинг фундаментал хусусияти физикада Гейзенберг ноаниклик принципи билан маълум. Бу принцип 1927 йилда ишлаб чикилган. Бу принципга асосан, квант тизимидаги параметрларнинг узаро богликлигини аниклаш ' унинг бузилишига олиб келади ва бу узгартириш натижасида кабул килинадиган ахборот дезинформация шаклида аникланади.

Агар фотонни бирор бир хусусиятини узгартирсак, масалан дейлик кутбланиш даражаси ёки ёруглик узунлигини ўзгартириш натижасида фотоннинг тузилиши узгаради. Бир вакднинг узида квантнинг иккита катталигини берилган аниклик буйича узгартириб булмайди ва кутбланиш даражасининг узгариши иккинчисининг хам мое равишда узгаришига олиб келади. Агар маълумотни юборувчи ва кабул килувчи томонлар кутбланишнинг бирор бир усулини танлаб олишмаган булса, кабул килувчи юборувчи томонидан берилган маълумотлардан хеч кандай фойдали маълумот олиша олмайди.

Шунга асосланиб, ахборотни узатишда бошка кимсалар томонидан ушлаб колинишида'химоя килиш учун маълумот узатиш каналлари курилади. Кабул килувчи келаётган ахборотни бошка одамлар томонидан ушлаб колинганлигини аниклаши мумкин ва бу аникланганидан кейин узатувчи томонга маълумотларни бошка калит буйича кайта узатишни сурайди.

Юборувчи маълумотларни бирор бир квантли тузилиш буйича кодлаштиради. Кабул килувчи эса, бу тузилишларни руйхатдан утказади. Кейин юборувчи ва кабул килувчи томонлар биргаликда кузатиш натижаларини тахлил килишади. Натижада, юборилган ва кабул килинган маълумотларнинг бир хиллилига ишонч хосил килинади. Натижаларни тахлил килишда куйидагиларга эътибор берилади: хатоликлар, шовкин ва бузгунчилар келтириб чикарган хатоликлар. Маълумотларни аниклиги тахлил килинади, лекин бит буйича тахлил килинмайди. Маълумотларни узатиш вактида фотонларнинг жойлашуви назорат килинади.

Ёругликни кутбланишини улчаш учун у кайси кутб системаси буйича узатилганлигини олдиндан билишимиз керак. Агар бизга ёруглик вертикал ёки горизонтал узатилган булса, уни горизонтал фильтрдан утказганимизда у 0 ёки 90 градусда кутбланганлигини аниклашимиз мумкин. Агар кутбланиш диоганал ва фильтрни горизонтал куйган булса, у холда ёруглик +45 ёки -45 градусда утканлигини аниклай олмаймиз.

Шунинг учун ёруглик импульелари оркали шакллантирилган каналда бошка шахслар томонидан ушлаб колинмайди. Нотугри фильтр урнатилганда канал бузилади. Квант криптографиясидан фойдаланиш жараёнида куйидаги квантли протоколлардан фойдаланилади:

1. Квантли протокол BB84

Бу система узида кабул килгич ва узаткичдан ташкил топган. Узаткич узида фотонларни турт кутбдан бирига жунатишда генератор ишлата олади.О, 45, 90 ёки 135 градуслар танланаётган битга боглик. Кабул килгич эса, кутбланишни улчайдиган фиксаторни ишлатади. Квант механикасини конунларига кура кабул килгич, тугридан-тугри кутбланиш(0,..,90) ёки диоганал кутбланиш(45,..,135)ларни фарклаи олади, лекин иккалсини биргаликда хеч качон фарклай олмаиди. Калитларни таксимлаш бир неча кадамларда иборат:

1- кадам: Узаткич фотонларни ихтиёрий танланган 4 кутблардан

1тасига юборади.

2- кадам: Хар бир кабул килинган фотон учун кабул килувчи ихтиёрий типдаги кутбланиш ?лчамини танлайди: тугри ёки диоганал. Кабул килувчи улчанган натижани ёзиб олади ва уларни махфий равишда саклайди.

3- кадам: Кабул килувчи (очик канал) ошкора фотонларни улчашда ишлатиладиган типларни эълон килади (натижани эълон килмайди).

4- кадам: Узатувчи юборувчига (очик канал буйича) тугри типдаги улчашларни хабар килади.

5- кадам: Фойдаланувчилар (кабул килувчи ва узатувчи) улчашлар хакида хамма тугри типдаги ходисаларни танлайди.

Бу ходисаларни битларга у™риб, калитларни олади. Хабарни угирламокчи булган бузгунчи, албатта шу хатоликни бажаради чунки у олдиндан фотоннинг кутбланиш типини билмайди. Квант механикаси эса, бу иккита номаълум бир-бирига боглик булмаган кутб типларини улчаш имконини бермайди (тугри ва диоганал кутблар) Иккита конуний фойдаланувчи квантли каналда эшитиш имконияти, **очик** канал оркали ихтиёрий битли калитлар ва хатоликларни теетдан ўтказади.

ололмаса хдм, бузгунчилар томонидан алданмайди, чунки каналга хар бир уланиш аникланади.

Масалан, бузгунчи кабелни кесиб ускуналар ёрдамида адресатни аналогик жихозлари хакида улчашларни олиб боради. Шундан сунг, у улчашлар натижасига кура кабул килувчига фотон жунатади. Шунда бузгунчи холатнинг 50% да нотугри анализатор танлайди ва адресатга тасодифан танланган холда жунатади. Натижада 25% мухим хабарлар битлари юборувчи томонидан адресатн и ки дан фарк килади.

Энди фойдаланувчилар ярим битли сатр калитини танлаш оркали ва ошкора уларни маъносини эълон килиш оркали бузгунчи борлигини била олади. Агар эълонларнинг хамма маъноси бир-бирига мое тушеа, фойдаланувчилар уларни хеч ким эшитмаётганини ишонч хосил килиши мумкин. Чунки, уларни эшитиб туриш эхтимоллиги (3/4)N/2 ~= 10-125 булган да, N =1000

Масалан, Алиса куйидагиларни юборяпти: j \/ - \ - |.

Боб узининг детекторини ихтиёрий созлаб олган.

Махфий калит алгоритмининг генерацияси.

Боб кутбланишни тугри аниклаганда (Худди Алиса юборган кутблардай), у тугри натижа олади колган вазиятларда эса, натижа тасодифий булади.

Боб ва Алиса очик канал оркали бир-бирига кайси кутбланиш типидан фойдаланаётганини айтади (диоганал ёки ортогонал). Факатгина тугри натижаларни колдиради.

Бизнинг келтирилган мисолимизда Боб 2, 5 , 6, 7 - импулслар кутбланишини топди. Шундай килиб, | \ \- | колади.

Олдиндан келишилган шартларга кура, натижа битлар давомийлигига айланади (Масалан, 0 ва 45 бирини кабул килади. 90 ва -45 эса, 0).

Хабарни огирланганлигини Боб ва Алиса хатоларини текшириш оркали аниклаши мумкин, тасодифий хабарлар бетини таккослаб. Тугри келмагани, хабар угирланганини курсатади, ушанда калит узгартирилади ва кайта юборилади.

Агар фарк бўлмаа, таккослаш учун ишлатилган битлар ташланади ва калит кабул килинади.

2. Квантли протокол B92

0 ва 1ларни бу протоколда тасаввур килиш учун икки йуналишли кутбланган фотонлар ишлатилади. Узатувчи битларни кодлашда иккита кутбланган фильтрдан фойдаланилади. Бу иккита кутбли фильтрлар йуналиши орасидаги бурчак 45 градусни ташкил килади. Бу йуналишлар ортогонал эмас. Кабул килувчи фотонларни кабул килишда 90, 135 градусли фильтрдан фойдаланилади. Агар фотон кутби ва фильтри орасидаги фарки 90градусни ташкил килса, у холда фотон фильтр оркали утмайди. Агарда 45 булса, фотонни фильтрдан утиш эхтимоллиги 0.5га тенг.

Энди, B92 протоколини ишлаш кетма-кетлигини куриб чикамиз:

1-кадам: Манба икки фильтр оркали 0 ва 45 градусда 0 ва 1ли хабарни юборади.

2- кддам: Адресатнинг фильтри 90, 135 гр. йуналишда булади. Юборувчи шу йуналишдаги фотонларни жунатади.

3- кадам: Кабул килувчи кутбланишни аниклашда шу ёки бошка фильтр оркали фотонни утказади. Тасаввур килайлик, масалан битта фильтр оркали (135градус) фотон утмади. Адресат нима юборилганини билмайди. Агарда фотон фильтрдан утса, адресат ишонч билан кабул килинган фотон 0 эканлигини билдиради. Агар фотон яхши кабул килинса, навбатдаги калит бити 0 ёки 1 билан ишлатиладиган фильтрга караб'кодланади.

4- кадам: Адресат юборилган фо*онлардан тахминан 4дан

бирини олганини аниклаш осон.

5- кадам: Давомийликни кабул килиб, адресат жунатувчига 1 ООдан 25та кабул килинган фотонни айтиш мумкин. Улар навбатдаги хабарда калит булиб хизмат килиши мумкин. Шунинг билан фильтр ва кабул килинган кутбларни айтмасдан туриб бажаради. Шунинг учун бузгунчи телефон оркали сузлашувни

эшитиб турса хам, калитни туза олмайди.

6- кадам: Калитни мувофакиятли жунатишдан сунг, жунатувчи узининг хабарларини шу калит ёрдамида кодлаб юбориши мумкин. Адресатдан бошка хеч ким кодни оча олмайди. Бузгунчи томонидан хабарни калитини угирланганлиги хакидаги маълумотни, фойдаланувчилар хатоликни назорат килиш оркали топиб олиши мумкин. Бунинг учун улар худди BB84дагидек,

калитдан танланган холатларни таккослаш оркали аниклайди. Агарда бир-бирига тугри келмаган холлар аникланганда, хабар угирланганлигини курсатади ва юбориш процедураси бошкатдан кайтарилади. Агарда тугри келса, текширилаётган бит, калит эксплуатацияга кабул килинади.

3. Эккерт томонидан таклнф килинган квантли протрокол.

1991 йил Эккерт махфий калит яратишда узаро богланган квантли заррачаларни ишлатишни таклиф килди. Бундай хусусият биринчи булиб, Эйнштейн томонидан 1935 йил мантикий парадокс деб айтиб утилган, кейинрок 1969 йилда Белл томонидан тушунтирилган. Бир-бирига боглик заррачалар (ЭПР заррачалар)
харакатчан холатда булади. Бундай заррачаларнинг тулкин функциясига кура: |Y> = (1 /2)1 /2«(|0>| 1 >-| 1 >|0>)

Бу ерда заррачалар улчанаётган ЭПР парадоксига кура ёзилган. Бу икки жуфтликдан бирининг холати маълум булса (мисол учун, кандайдир базасига асосан улчашлар олиб борилаётган булса), у холда икки холатини 100% лик аниклик билан аниклаш мумкин ва бу икки зарранинг бир - бирига боглик ортоганал булади. Агар биринчи зарранинг холатини улчаши |0> ни берса, у холда иккинчи зарраники худди шу базисда |1>.

Эккерт протоколини ишлаши учун, иккита ЭПР заррани генерацияловчи курулма зарур булади. Булардан ташкари махфий калитларни шакллантиришда квантларини катнашувчиларга узатувчи канал зарур, катнашувчиларда эса кабул килинган зарраларнинг холатини улчайдиган курилма булиши керак.

1- кадам: Қурилма икки бир - бирига боглик зарраларни ишлаб чикарувчи курилма (А ва Б).

2- кадам: А заррача биринчи фойдаланувчига юборилади (одатда уни Алиса деб номлаймиз), Б' заррача эса иккинчи фойдаланувчига (уни хам Боб деб номлаймиз).

3- кадам: Алиса ва Боб уз зарраларини улчайди. улчашлар натижаси эса ЭПР парадоксига тугри келиши керак ва Беллага тенг булмаслиги керак.

4- кадам: Давомийлигидан олинган битларни бир кисмини очик канал буйича улчанади. Агарда улар квантлар кореляциясини бузилганлигини аникламаса, у холда эълон килинмай колган битлар калит деб эълон килинади.

Камчилиги: айирбошловчи катнашувчилардан бири кабул килинган кетма - кетликни инвертлаб туриши керак.

Масалан шпион квантлар узатиш каналини топиб олди ва квантларни холатини улчай бошлади. Лекин у кайси базисда улчашлар олиб боришини каердан билсин? Шу тарика бузгунчи камида 50% вазиятда ЭПР богликлигини бузади. Бузгунчининг
борлигини худди ВВ84дагидай, калитли кетма - кетликдаги куп
хатолар оркали аникланади.

4. Зичлаб кодлаш протоколи. Тасаввур килайлик, жуфт кубитларни кетма - кетлигини |00>+|11> холатда яратувчи курилма мавжуд ва хар бир жуфтликда бигга кубитни Алисада саклаш учун, бошкасини Бобда саклаш учун юбормокда. Бунгача Алиса ва Боб учун хеч качон бир - бири уртасида богланиш урнатил мае лиги талаб килинган эди. Бу холда эса, Алиса Бобга битта кубит ёрдамида, икки

классик битлар хакида хабар бериши мумкин. Бу холат шундай тушунтирилади, бир - бирига боглик булган турт ортогонал |00> + |11>, |00> -|11>, |01> + |10>, |01> -|10> холат бир холатдан бошка холатга утишдабир кубит воситасида таминланиши мумкин.

Берилган холат жуда кучли Белл - ЭПР кетма - кетлгини курсатгани учун Белла базиси деб аталади (Браунстеин эт. ал. 1992). |00> + |Ц> холатдан бошлаб, Алиса Белла базиси холатида квантларнинг бир гейт {1, X, Y, Z } ёрдамида маълум булган кубитга таъсир курсата олади. Операцияларда 4 имконият булгани учун 2 битли классик ахборот билан таъсирда аникланади.

Зичлаб кодлаш протоколини куриб чикайлик:

1- кадам: Алиса ва Боб курулмадан бир - бирига боглик булган жуфт кубитлардан (а ва б) бирини олишади.

2- кадам: Алиса узининг кубити а га гейт билан таъсир курсатади. Хар кандай гейт ишлатишга юборилаётган 2 бит ахборотга
боглик-

3- кадам: Боб Алисадан кубит кабул килгандан сунг, у кубит Белла базисини кайси холатидалигини аниклаши керак. Буни жуфт кубитга XOR гейти тасири воситасида килиш мумкин ва натижаловчи битни улчаш оркали. Шу тарика Боб |00>+-|H> холатни |01>+-|10>
холатдан фаркдай олади.

4- кадам: Боб суперпозиция белгисини аниклаши учун, у Адмара "X" узгартиришини ишлатиши керак [мисол учун 7] ва шундан сунг натижани улчаши керак. Шундай килиб Боб икки классик битлар хакида ахборот олади.

Зич кодлашни амалга ошириш кийин. Шунака фикрлар борки стандарт богланиш методидан бошка амалий маъноси йук- Лекин бунака эмас. Бу протокол алока химоя килади. Икки классик битлардаги ахборотларни олиш учун, юборувчи Алисани кубитини икки жуфтига эга булсагина ахборотни олади. Шундай килиб бузгунчи хам марказдан Бобга юборилаётган жуфт кубит олиши керак, Алиса хам' бобга юбораётган кубитни олиши керак. Кўриниб турибдики, бу кубитлар хар хил ККС билан юборилади. Бундан ташкари, агар бугунги битта кубитни олишга муваффак булса, уни ушлаб топиб олишади, чунки кубит иккинчи кубитга тулик эмас.

Бузгунчи Бобга олинган жуфт кубитдан бош бириктирилган жуфт кубитларни юбориши мумкин. У холда Алисанинг хабари хакикатдан хам угирланган булади. У холда бузгунчи бириктирилган жуфтликни ишлаб чикарадиган генераторга киришга эга булиши керак. Алиса ва Боб узларида ишлаб чикарадиган мавжуд кутбларни текшириш хакида келишиш мумкин. Бундай текшириш бузгунчини ишига 50% холатда салбий натижани курсатиши мумкин. Бундан ташкари бузгунчи Алиса юборадиган кубитни кодлаши учун канчадир вакт йукотади, бундай йукотишдан сунг, у алмаштирилган кубитни юбора олмайди. Факатгина 2 битли ахборотни олгачгина бузгунчи кубитни уз кубитига узгартириб Бобга юбориши мумкин. Каналдаги кубитларни кечикиши бузгунчи борлиги хакида шубха уйготади ва Алисага у хакида хабар килинади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Нильс Фергюсон, Брюс Шнайер «Практическая криптография»,

М.: Издательский дом «Вильяме», 2005г.-424с.

2. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.

3. Коблиц Н. Курс теории чисел в криптографии. - М., Научное издательство ТВП, 2001 й.

4. Масленников А. Практическая криптография BHV - СПб 2003Й.

5. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.

6. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002Й.

7. С.К.Ганиев, М.М. Каримов, К.А. Тошев «Ахборот хавфсизлиги. Ахборот - коммуникацион тизимлари хавфсизлиги», «Алокачи» 2008 йил, 378 бет.

6 – Лаборатория машғулотлари.

КВАНТ КРИПТОГРАФИЯСИНИНГ ИШЛАШ ПРИНЦИПИ ВА УНИНГ ЭКСПЕРИМЕНТ ТАДКИКОТИ

Оптик толали кабеллар пайдо булиши натижасида (бир неча Гбит/с), узатиш тезлиги В чизикли трактларда (ЧТ), ракамли узатиш трактларида (РУТ) бир вактда кайта тиклаш булимларининг узайиши билан бирга (100 км гача ва ундан юкори) юкори курсаткичларга эришиш мумкин булди. Оптик толали кабелларда ракамли трактнинг металл жуфтли кабеллардаги ишчанлиги 100 баравардан купрокка **ортик,** Кайсики иктисодий томондан хам фойдалидир. Купчилик кайта' тиклагичлар охирги ёки транзит станциялар билан бирлаштирилиши мумкин. Шунинг учун кайта тиклагичларни масофадан таъминлашни осонлаштиради. Шунинг учун оптик толали кабеллар транспорт тармокларида сигналларни таркатишдаги асосий
мухит хисобланади.

Транспорт тармоклари телекоммуникация тармоклари микёси

буйича куйидагича булинади.

1. Миллий микёс - бундай транспорт тармоклари минтакалар (вилоят)аро алокани таъминлайди, бу тармок тугунлари вилоят марказлари ва йирик саноатлашган шахарларда жойлашади.

2. Минтакавий микёс - бундай микёсдаги транспорт тармоклари бир минтака (вилоят)да жойлашган турли туманлар орасидаги алокани таъминлайди ва бу тармок тугунлари одатда туман марказларида жойлашади.

Миллий ва минтакавий микёсдаги транспорт тармокларида узатилиш хажмининг трафиги буйича фаркланади, маълум мивдорда миллий микёс да купрокдир Шунга биноан бундай тармокларни лойихалаштириш ва куришда оптик толали кабелларни тугри танлаш зарур Шунингдек, шу транспорт тармогида узатилиши зарур булган трафик ва бир пайтда унинг иктисодий кийматининг ошиб кетмаслигини таъминлаш зарур.

Транспорт тармокларидаги кабелларни тугри танлаш, шу тармокда ишлатиладиган тармок курилмаларининг технологияси билан узвий богликдир. Кайсики, транспорт тармоги ракамли трактни хосил килишини таъминлаши керак.

Транспорт тармогининг курилишида турли хил тармок технологиялари ишлатилади:

- синхрон ракамли иерархия SDH технологияси;
- асинхрон туридаги ахборот ташиш АТМ технологияси;
- тулкинли мултиплексор WDM технологияси.

SDH технологияси учун асосий узатиш мухити булиб G652 МЪЬ - Т тавсифномасига жавоб берадиган оптик-толали кабелларнинг стандартлари ишлатилади. АТМ технологиям хам шу оптик толали кабелларни ишлатиш мумкин, лекин одатда АТМ, SDH билан биргаликда ишлатилади. Оптик толаларда дисперсия катталикларини кичрайтириш ва SDH технологиясининг кайта тикланиш майдонини узайтириш учун сурилган дисперсияли ва G65, МЪЬ-1 тавсифномасига жавоб бера оладиган оптик толалар ишлаб чикарилган. Бундай оптик-толаларда дисперсиянинг нуктаси (0) тулкин узунлиги 1.3 мкм дан иш узунлиги 1.55 мкмтомон сурилган.

WDM (DWDM) тулкиннинг мултиплексорлари технологиясининг ва G652 тавсифномага жавоб берувчи дисперияси сурилган (G653) оптик толанинг кулланилиши натижасида оптик сигналларнинг узатилиши ёмонлашувига олиб келадиган ночизикли эффектлар хосил булади. Шунга ухшаш эффектларни бартараф этиш учун WDM ва DWDM технологияларнинг ишлатилишида G655 тавсифномасига жавоб бера оладиган дисперсия силжиши (0) га тенг булган оптик толали кабеллар ишлаб чикарилган.

Бундай толага True Wave оптик толаси мисол була олади. Хрзирги вактда Узбекистан Республикаси транспорт тармогининг хар хил микёсида тармок технологиясининг синхрон ракамли SDH иерархияси ишлатилган, шу билан бирга G652 тавсифномасига мое келувчи стандарт оптик толалар кулланилган. Бундай тармокларда ракамли ахборотнинг блок л и циклик тузилиши асосида узатиладиган STM транспорт модули деб аталади.$_{г}$ Транспорт модули узининг микёси буйича ракамли ахборотни узатиш тезлиги ва ташкил этиладиган каналлари буйича ажратилади. Улар 4 боскичдан иборат (6.1.-жадвал).

бЛ.-жадвал

SDH транспорт модули даражаси	Транспорт модули	Узатиш тезлиги (Mbit/s)	Телефон каналлар сони
SDH биринчи даража	STM- 1	155.52	1890
SDH иккинчи даража	STM-4	622.08	7560
SDH учинчи даража	STM- 16	2488.32	30240
SDH туртинчи даража	STM- 64	9953.28	120960

Маълумки, телекомуникацион транспорт тармоклари глобал, миллий, минтакавий ва махаллийларга булинади. 6.2,- жадвалда тарнспорт модуллари ва тарнспорт тармокларининг узаро богликлиги курсатилган.

6.2.-жадвал

Транспорт тармогн	Транспорт модули
Глобал	*STM-64, STM- 16*
Миллий	*STM- 16, STM- 4*
Минтакавий	*STM- 4, STM-1*
Мах^аллий	*STM- 1, STM- 4*

Лойихалаштирилаётган тармоқ боқич миқиёсига қараб керакли каналлар ташкил эта оладисган транспорт модули танланади. Шунинг учун керакли модуллар сони куйидагича аникланади:

hh.mod = (N,$_{sh}$kjm$_{r}$mod):

Бу ерда: N_{ish}k. - ишчи каналлар сони; N_{tr}mod – транспорт хосил қиладиган каналлар сони.

Транспорт модули асосида ракамли ахборотни узатиш учун 2 та оптик толали танлаш зарур. Шунда кабелдаги керакли толалар сони $N_{10}i = Ish_0mod * (2+2_{мх})$ га тенг бўлади.

Бу ерда Ish_0mod транспорт модуллар сони $2+2_{зах}$ захира тола. Кабелдаги ишчи толалар сонини аниқлаб, кабелнинг маркаси ва унинг турини биламиз. Кабелни танлашда унинг етказилиш шароити, яъни телефон канализациясини, ер ёки сувдан ўтиш жойлари бўлишини инобатга олиши зарур.

Немес кабеллари 3 синфга булинади.

Биринчи, энг ахамиятлисига чизиқли оптик толали кабеллар киради. (Fiber Optic Outdoor Cables). Бу кабеллар телефон канализациялари, ерда ва коллекторларда ишлатилиш учун мулжалланган.

Иккинчи синф ўзида станция оптик толали кабелларини акс эттирган (Fiber Optic Outdoor Cables). Бу кабеллар фақат бино иншоатлари ичида ишлатилишига мўлжалланган.

Учинчи синфга факат махсус ишлатилиши учун мулжалланган кабеллар киради. Булар осиладиган (Fiber Optic Outdoor Cables) ва сув остида ишлатиладиган (Fiber Optic Outdoor Cables) кабеллар, шунга биноан таянчларга осилади ёки даре, сув хавзалари тагидан утказилади. Келтирилган синфдаги кабеллар тузилиши, модуллар сони, тола сони, коплами сони, ишлатилган махсулоти билан фаркланади. Аник турни танлаш кабел ишлатиладиган бир неча омилга боглик, булар кайси тармокда ишлатилиши, каналлар сони, узатиш параметрлари, еткизилиш шароитлари, ташки таъсир, кабел киймати ва хоказолардир.

Оптик кабеллар маркировкасини куриб чикайлик. Кабелнинг маркаси деб шартли белгилашларга айтилади. Буларга х,арфлар гурухи ва ракамлар киради. Уларнинг маълум тартибда ёзилиши кабелнинг тузилиши ва уни ишлатилиш шароитини курсатади. Германия кабел саноатида VDE (Verband Deutscher Elecktrotechniker- Association of German Electrical Engineers) Германия электро мухандислар ташкилоти томонидан стандарт марка - белгилашлар ишлаб чикилган. Оптик-толали кабеллар учун харфли ва ракамли белгилашлар ишлатилади.

Шахарлараро модерлар оптик толали алока линияларининг уртасида етказилиш учун ишлатилади. Ахоли яшаш жойларида бу кабеллар мавжуд булган телефон канализациялари ва метро коллекторлари, ундан ташкарида ер, яъни тупрок оркали утказилади.

Шахарлараро оптик-толали алока линияларида телефон канализациялари ва ерда ёткизиш учун куйидаги кабел турлари ишлатилади. A- DF (ZN) 2Y (SR) 2Y. A- DF (ZN) 2Y (SR) 2Y 3x6E9/125 0.36F3.5+0.22N18 LG турдаги кабел тузилиши келтирилган. Кабелнинг марказий куч элемента шишапластикдан ясалган бир модли толалар тури E9/125 термобардош фторопласт найларда жойлаштирилиб, модул деб юритилади. Кабел узагида каватли мустахкамлаштирилган когоз ва саноат толаси ёткизилган. Кабелнинг ички коплами полиэтилендан, калайдан килинган коплама остида мустахкамлашган когоздан ёстикча жойлашган. Пулат коплама ташкари кобик полиэтилен шланг билан копланган кабел тулдиргичлар билан гермитизацияланган.

A- DF (ZN) 2Y (SR) 2Y 3x6E9/125 0.36F3.5+0.22N18 LG кабелнинг маркасининг укилиши куйидагича:

A- чизикли кабел;

D- куп толали модул тулатилган;

F- кабел узаги гидрофоб тулдиргичи билан;

(ZN) 2Y- полиэтилен коплама, ташки;

(SR)- катламлаштирилган пулат коплама;

2Y- ички полиэтилен коплама;

3- модуллар сони;

6- модулдаги толалар сони;

E- бир жинсли тола шиша/шиша;

9- модли майдон диаметри (1 жинсли майдон диаметри);

125- тола копламининг диаметри, мкм;
0.36- суниш коэффициента, dB/км;
F- тулкин узунлиги;
3.5- импулс кенгайиш (дисперсия х,исобига) ps/nm х км;
0.22- суниш коэффициента, dB/км;
H- тулкин узунлиги 1.55 мкм;
18- импулс кенгайиши (дисперсия хисобига) ps/nm х км;
LG- урам узаги.

ADSL (Asymetric Digitel Subscriber Line) аббревиатураси - асимметрик ракамли абонентлик линияси деб кенгайтириб изохланади. Номининг узи технологияга аввалдан жойлаштирилган абонентга ва тескари йуналишларда тезликлар алмашинуви турларини курсатади. Маълумотлар узатиш тезлиги фойдаланилаётган жихоз, телефон линияси узунлиги ва сифатига боглик- Маълумотлар узатишнинг асимметрик хусусияти махсус амалга оширилган, бунда Интернетдан типик фойдаланувчи сифатида маълумотларни у[3] компьютерига жойлаштиради, бошкарув буйруклари ва фойдаланиладиган маълумотларнинг унча катта булмаган окими (электрон почта, сах,ифаларнинг янгиланиши ва бошкалар) тескари йуналишда боради.

Ўз сифатига кура ADSL - технологияси кимматбахо толали- оптик тармокларнинг альтернатив курилмаси хисобланади. Тармокдан фойдаланувчи учун ADSL дан фойдаланиш куйидагилари билан диккат талаб этади:

- кечаю-кундуз Интернетга уланиш мумкин, бунда кунгирок килиш шарт эмас, сабаби уланиш доимийдир;
- интернет-алока тургун- ва у телефон линияси хусусиятларининг узгаришига боглик булмайди, бу эса алока узилишисиз жуда катта хджмдаги маълумотлар олиш имконинй беради.

Маълумотлар учун: ADSL - абонентлик уланишининг энг замонавий технологияларидан бири булиб, бир вактнинг узида оддий телефон линияси оркали хам овоз, хам маълумотларни узата олади. Бошкача килиб айтганда, Интернет ишлаётган вактда телефон линияси оддий кунгироклар учун эркин булиб колаверади ва алока сифати хам узгармайди. Назарий жихатдан ADSL - сервис тармовдаги абонентга маълумотлар узатиш тезлиги 8 Мбит/с дан, тескари йуналишда 1.5Мбит/с га тенг бўлади.

Оптик толали тармоклар шубхасиз алока сохасида энг кузга кўринган йуналишлардан бири. Оптик толали тармокларнинг утказувчанлик кобилияти мис кабелли линиялардан сезиларли даражада юкори. Бундан ташкари оптик тола электромагнит майдонларига таъсирчан эмас. Бу эса, мис кабелли алокалардаги баъзи бир нокулайликларни бартараф этади. Оптик толали тармоклар кам харажат билан маълумотларни узок масофага етказиб бера олади. Бу технологиянинг киммат булишига карамасдан, унинг бахоси кун сайин арзонлашиб бормовда. Мис кабелли тармоклар эса, узининг юкори ривожланиш даражасига етиб, янада ривожланиш учун куп харажат талаб килади.Хозирда квант криптографияси тижорат ва харбий ташкилот томонидан кизикиш билан каралмокда, чунки бу технология абсолют химояни кафолатлайди. Квант криптография технологиясини яратувчилари, хозирда шу технологиями лабораториядан бозорга чикдришга

якинлашиб колди. Оз вактдан сунг, банк ва махсус хизмат ходимларининг квант криптографияси яма бир кават химоя катламига айланиши мумкин.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильяме», 2005г.-424с.
2. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», ML: ДМК, 2000г. -448с.
3. Коблиц Н. Курс теории чисел в криптографии. - М., Научное издательство ТВП, 2001 й.
4. Масленников А. Практическая криптография BHV - СПб 2003 й.
5. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты ма языке Си.Триумф- 2002Й.
6. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002 й.
7. С.К.Ганиев, М.М. Каримов, К.А. Тошев «Ахборот хавфсизлиги. Ахборот - коммуникацион тизимлари хавфсизлиги», «Алокачи» 2008 йил, 378 бет.