NOSSIMMETRIK KRIPTOTIZIMLARNING TADQIQI

Xolbekov Umarali Zokir o‘g‘li

Jizzax politexnika instituti “ICHJA va B” kafedrasi, assistenti

umaralixolbekov@gmail.com

Annotatsiya: *Har bir aloqa tomoni bajaradigan amallarni bu kungi davrimizning Kumush va Otabeklari orasidagi elektron maktublar almashish va ularga nisbatan tajovuzkor shaxs Hamid timsolida namoyish qilamiz. Nosimmetrik Kriptotizimda axborot almashish jarayoni ishlab chiqildi.*

Kalit so‘zlar: *Simmetrik kriptotizim, Otabek va Kumush, butun son, shaxsiy maxfiy kalit, M moduli, Bryus Shnayer tizimi, amaliy kriptografiya, protokollar, algoritmlar, dastlabki matn, ekvivalent uzunliklar.*

Аннотация: *Мы покажем действия, совершаемые каждой стороной общения в образе агрессивного человека Хамида, обменивающегося электронными письмами между Кумушем и Отабеками нашего времени. Процесс обмена информацией был разработан в Симметричной Криптосистеме.*

Ключевые слова: *Симметричная криптосистема, Отабек и Сильвер, целое число, закрытый секретный ключ, М-модуль, система Брюса Шнайера, прикладная криптография, протоколы, алгоритмы, открытый текст, эквивалентные длины.*

Annotation: *We will show the actions performed by each side of communication in the form of Hamid, an aggressive person, exchanging e-mails between Kumush and Otabeks of our time. Information exchange process was developed in Symmetric Cryptosystem.*

Key words: *Symmetric cryptosystem, Otabek and Silver, integer, private secret key, M-module, Bruce Schneier system, applied cryptography, protocols, algorithms, plain text, equivalent lengths.*

Kirish.

Faraz qilaylikki, Otabek va Kumush simmetrik kriptotizimdan foydalanish uchun o‘zaro maxfiy kalit belgilab olamiz. Buning uchun ulardan biri biror katta tub son M

ni va 1 bilan M-1 orasidan butun son g ni tanlab himoyalangan aloqa kanali (masalan, telefon) orqali ikkinchilariga bildirib kelishib oladilar. So‘ngra ikkovlari ham 1 bilan M-1 orasidan alohida ixtiyoriy butun sonlarni tanlab uni o‘zlarininng shaxsiy maxfiy kalitlari deb belgilaydilar va uni hech kimsaga (bir birlariga ham) bildirmaydilar. Faraz qilaylikki, Otabekning shaxsiy maxfiy kaliti o, Kumushning shaxsiy maxfiy kaliti esa k bo‘lsin.

Bu shaxsiy maxfiy kalitlar o‘zaro maxfiy (ikkovlaridan boshqa hech kim bilmaydigan)kalitni hosil qilishda qatnashadigan kalitlardir. Otabek o‘z shaxsiy oshkora kaliti E_{ota} ni, Kumush o‘z shaxsiy oshkora kaliti E_{kum} ni hosil qilish uchun g sonini M modul bo‘yicha o‘z shaxsiy maxfiy kalitlariga teng bo‘lgan darajaga ohirishlari kifoya. Ular o‘z shaxsiy oshkora kalitlarini bir-birlariga va boshqalarga ham ochiq aloqa kanali orqali ma’lum qilganlaridan so‘ng o‘zaro maxfiy kalitni hisoblab topishlari mumkin bo‘ladi.

Shaxsiy oshkora kalitlar, M moduli va g asos Xomidga ham ma’lum. Lekin, u haxsiy maxfiy kalitlardan bexabar bulgani uchun Otabek va Kumushlarning o‘zaro maxfiy kalitlarini bilaolmaydi. Chunki, buning uchun yo Otabekning yo Kumushning shaxsiy maxfiy kalitini bilish zarur. Uni bilish uchun g asosda m moduli bo‘yicha oshkora kalitning diskret logarifmini hisoblab topish zarur.

M soni 2^{512} chi darajasiga teng songa yaqin son bo‘lsa va u “puxta tub son” (ya’ni, undan bitta kam sonni yarmisi ham tub son) bo‘lsa diskret logarifmni hisoblashda ishlatiladigan ko‘paytuv amallarining (M moduli buyicha) soni 2^{256} darjasiga yakin bo‘ladi.

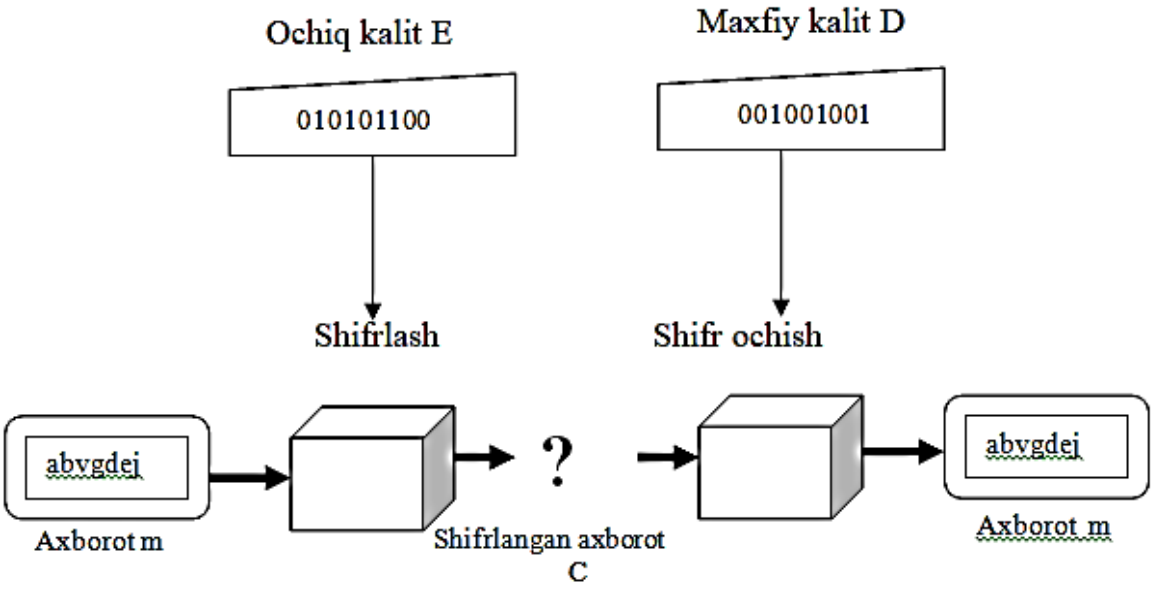
Ko‘rib o‘tilgan bir tomonlama hisoblanadigan funktsiya asosiga qurilgan shaxsiy oshkora va maxfiy kalitlar, xabarlarni bevosita shifrlash va shifrni yechish muammosinigina emas, balki xabar (umuman, har qanday axborot)larni simmetrik kriptotizimlarda shifrlashda va shifr ochishda foydalaniladigan o‘zaro maxfiy kalitlarni ochiq aloqa kanalidan foydalanib ta’minlash muammosini echib beradi.

Faraz qilaylikki, Otabek Kumushga nosimmetrik kriptotizimdan foydalanib pinhona maktub yo‘llamoqchi. Ular orasida aloqa boshlanguncha Kumush o‘z oshkora kaliti nusxasini Otabekka va boshqalarga ma’lum qilgan.

Otabek Kumushga m maktubini yozib, uni Kumushning oshkora kaliti E bilan shifrlaydi(1-rasm). Natijada m maktubi shifrlangan matn S ga aylanadi. So‘ngra Otabek shifrlangan maktubni elektron pochta orqali Kumushga jo‘natadi.

Xat Kumushning oshkora kaliti bilan shifrlangan bo‘lgani uchun uni Kumush o‘z maxfiy kaliti D bilan bemalol o‘qiy oladi.

Ya’ni shifrlangan matn s Kumushning maxfiy kaliti D bilan dastlabki matn m ga aylantiriladi.



1-rasm. Nosimmetrik Kriptotizimda axborot almashish jarayoni

Aloqa kanali himoyalanmagan bo‘lgani uchun bu maktub Homidning qo‘liga ham tushishi mumkin. Lekin Homidda Kumushning maxfiy kaliti bo‘lmagani uchun u xatning mazmunini bala olmaydiva xatni o‘zgartirib qo‘ya olmaydi. Iomidning qo‘lidan maktubni yo‘q qilib yuborish va yoki Kumushga uning oshkora kalitidan foydalanib Otabek nomidan shifrlangan yangi qalbaki maktub yo‘llash keladi. Hamid maktub mazmunini bilmay turib Otabek nomidan shifrlangan maktub jo‘natsa, buning qalbaki ekanligi Kumushga darhol oshkora bo‘lmasligi mumkin.

Chunki, xat Kumushning oshkora kaliti bilan shifrlangan bo‘lgani uchun uni Kumush o‘z maxfiy kaliti bilan ochib o‘qiydi. Bu xatning chindan ham otabekdan ekaniga ishonch hosil kilish uchun bu erda autentifikatsiya muammosini (Otabekning raqamli imzosini tekshirish orqali) hal qilish lozim bo‘ladi. Bu muammoni yechishda raqamli imzo qo‘yish uchun shaxsiy mahfiy kalitdan, imzoni tekshirish uchun shaxsning oshkora kalitidan foydalaniladi.

Barcha nosimmetrik kriptotizimlarni kriptotaxlil qilish asosan kalitlarni bir boshdan ko‘rib chiqish asosida amalga oshiriladi. Shuning uchun ularning simmetrik kriptotizimlarga teng bardoshliligini ta’minlash maqsadida ancha uzun (bitlar soni bo‘yicha) kalitlardan foydalaniladi. Bryus Shnayer o‘zining “Amaliy kriptografiya:Si da protokollar, algoritmlar va dastlabki matn” kitobida kalitlarning ekvivalent uzunliklari uchun quyidagi raqamlarni keltiradi.

Bunda kalitni qanday hosil qilish, aloqa qatnashchilariga bu kalitni maxfiyligi saqlangan holda etkazish, va umuman, ishtirokchilar orasida kalit uzatilgunga qadar

xavfsiz aloqa kanalini xosil qilish asosiy muammo bo‘lib turadi. Bunda yana boshqa bir muammo-autentifikatsiya muammosi ham ko‘ndalang bo‘ladi. Chunki:

-dastlabki matn xabar shifrlash kalitiga ega bo‘lgan kimsa tomonidan shifrlanadi. Bu kimsa kalitning haqiqiy egasi bo‘lishi ham, begona (mabodo kriptotizimning siri ochilgan bo‘lsa)bo‘lishi ham mumkin.

Bu muammolarni turli kriptotizimlar turlicha hal qilib beradi.

Foydalanuvchilar soni kam bo‘lganda simmetrik kriptotizimdan foydalanish qulay. Lekin foydalanuvchilar ko‘p bo‘lib ular butun dunyo bo‘ylab tarqalgan bo‘lishsa kalit taqsimlash katta muammoga aylanadi. Har bir kishi bunday tarmoqda har bir boshqa kishi bilan axborot almashishi uchun alohida maxfiy kalitga ega bo‘lishi kerak.

Masalan, 1000 foydalanuvchiga ega bo‘lgan tizim taxminan 500,000 kalit bo‘lishini va shuncha almashuv jarayonini amalga oshirishni va shuncha kalitni maxfiy saqlashni talab etadi.

Nosimmetrik-kalitli kriptotizimlarda tarmoqdan foydalanuvchining har biri o‘zining yagona maxfiy kalitiga ega. ¡zining va boshkalarning oshkora kalitlarini sir saqlashga hojat yuq. Masalan, 1000 foydalanuvchisi bo‘lgan tarmoqda har bir foydalanuvchi bittadan oshkora va bittadan maxfiy kalitga ega bo‘lishi kifoya. Ya’ni bunda, simmetrik kalitli tizimdagi 500,000 kalit o‘rniga hammasi bo‘lib 2000 kalit bo‘lishi etarli.

Simmetrik kalitli tizimlar nosimmetrik tizimlarga nisbatan tez ishlashlashi tufayli, katta hajmdagi axborotlarni shifrlashda nosimmetrik tizimli kriptotizimlar ular bilan raqobotlasha olmaydilar.

Ochiq kalitli kriptotizimlarni kichik qurilmalarda amalga oshirish mumkin emas, deyiladi, ammo bu noto‘ri. Assimetrik shifrlash ajoyib texnologiya, undan ko‘p va turli maqsadlarda foydalanish mumkin.

Uzatilayotgan ochiq ma’lumot ko‘rinishini almashtirish muammosi aloqa tarmog‘ida foydalanuvchilari o‘rtasida echilishi kerak bo‘lgan masalaning bir tomoni bo‘lsa, ikkinchi tomoni - malumotlar almashuvi amalga oshirilganda uzatilayotgan va qabul qilib olinayotgan malumotlarning hamda foydalanuvchilarning haqiqiyligiga ishonch hosil qilish.

Bu keltirilgan muammoni yechish uchun quyidagilarni:

-o‘zaro muomalaga kirishib malumot almashinuvchi tomonlarning bir-birlariga zarar keltirish yoki aldash maqsadida qasddan qiladigan har-qanday hatti harakatlarini qayd qilishni va oldini olishni;

Nosimmetrik algoritmlarning simmetrik algoritmlardan afzalligi ularda kalitni almashish uchun ximoyalangan kanal zarur emasligida namoyon bo‘ladi.

Simmetrik kriptografiyada kalit 2 tomon uchun ham sir saqlanadi, nosimmetrik kriptotizimda esa faqat bitta kalit maxfiy saqlanadi.

Simmetrik shifrlashda ma’lumotni xar bitta jo‘natgandan keyin almashtirib turilishi shart, nosimmetrik shifrlashda esa (*E*,*D*) juftliklarni biroz vaqtgacha o‘zgartirmay ishlatsa bo‘ladi.

Katta tarmoqli tizimlarda nosimmetrik kriptotizim kalitlari simmetrikka qaraganda kam.

Shu bilan birga quyidagi kamchiliklarga ega:

Simmetrik algoritmlarda nosimmetrikka qaraganda ma’lumotga o‘zgartirish kiritish oson.

Ma’lumot ishonchli shifrlansada, jo‘natuvchi va qabul qiluvchi orasida xabar almashinadi.

Nosimmetrik algoritmlarda simmetrikka nisbatan uzun kalitlar ishlatiladi. Quyida algoritmlarni bir biriga teng keluvchi o‘xshash kalitlar jadvali keltirilgan:

1-jadval.

Simmetrik kalit uzunligi, bit	**Nosimmetrik kalit uzunligi, bit**
56	**384**
64	**512**
80	**768**
112	**1792**
128	**2304**

Nosimmetrik algoritmda shifrlash va dastlabki matnga o‘girish simmetrikka qaraganda 2-3 baravar sekin kechadi.

Xulosa: Umuman olganda nosimmetrik kriptotizim xisoblash uchun ko‘proq xisoblash resurslari talab qiladi shuning uchun amalda bu tizim bilan birgalikda boshqa, simmetrik tizimni ham qo‘shgan holda ishlatiladi va tizim simmetrik kalit uzunligi, bitlarda xisoblash amalga oshirildi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Akbarov D.E. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. “O‘zbekiston markasi “, 2009. - 432 b.

2. O‘z DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari».

5. Брюс Шнаер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ - Москва: ТРИУМФ, 2002.

6. Xasanov X.P. Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari. - Toshkent, 2008. 208 b.