ASSIMETRIK SHIFRLASH ALGORITMLARI

Eshonqulova Feruza Abdirazoq qizi

TDShU "Tashqi iqtisodiy faoliyat" kafedrasi o'qituvchisi.

O'zbekiston Respublikasi, Toshkent shahri

Annotatsiya: Kriptografiya zamonaviy axborot xavfsizligida muhim rol o'ynaydi va texnologiyalar rivoji bilan birga takomillashib boradi. Ushbu ilmiy maqolada assimetrik shifrlash algoritmlari ya'ni Assimetrik shifrlash (RSA, ECC) – ochiq va yopiq kalitdan foydalanish haqida fikr va mulohazalar keltirilgan.

Kalit so'zlar: Kriptografiya, shifrlash, elektron tizim, axborot, assimetrik shifrlash, xavfsizlik.

АСИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Эшонкулова Феруза Абдиразок кызы

Преподаватель кафедры «Внешнеэкономическая деятельность» Ташкентского государственного университета информационных технологий.

Республика Узбекистан, город Ташкент

Аннотация: Криптография играет важную роль в современной информационной безопасности и совершенствуется вместе с развитием технологий. В данной научной статье представлены идеи и соображения об алгоритмах асимметричного шифрования, а именно об асимметричном шифровании (RSA, ECC) – использовании открытых и закрытых ключей.

Ключевые слова: Криптография, шифрование, электронная система, информация, асимметричное шифрование, безопасность.

ASYMMETRIC ENCRYPTION ALGORITHMS

Eshonkulova Feruza Abdirazoq qizi

Teacher of the Department of "Foreign Economic Activity" of the Tashkent State University of Information Technology.

Republic of Uzbekistan, Tashkent City

Abstract: Cryptography plays an important role in modern information security and is improving along with the development of technologies. This scientific article presents ideas and considerations about asymmetric encryption algorithms, i.e. Asymmetric encryption (RSA, ECC) - the use of public and private keys.

Keywords: Cryptography, encryption, electronic system, information, asymmetric encryption, security.

Shifrlash mashhur so'zga aylandi. Biz har doim shifrlash oraqali bizni tinglash va kuzatuvdan qanday himoya qilishini eshitamiz. Ko'pgina Internet foydalanuvchilari ulanishni himoya qilish uchun shifrlangan ilovalar, elektron pochta, tezkor xabarlar yoki VPN-lardan foydalanadilar. Shu bilan birga, hukumatlarning shifrlangan xizmatlar haqida o’z g’oyalari bor – ular favqulodda vaziyatlarda turli akkauntlarga to’liq kirishni va shuning uchun ular qonun orqali shifrlangan xizmatlarga orqa eshiklarni taqdim qilishni talab qilmoqdalar. Tabiiyki, ushbu yangi qonunlar ommaviy axborot vositalarining katta e'tiborini tortmoqda va shifrlashni diqqat markaziga qo'ymoqda.

Kriptografiya – bu ma’lumotlarni shifrlash va himoya qilish usullarini o‘rganadigan fan sohasi bo‘lib, uning asosiy maqsadi axborot xavfsizligini ta’minlashdir. U tarixan maxfiy yozishmalarni shifrlash usullaridan boshlab, bugungi kunda zamonaviy kompyuter tarmoqlari va elektron tizimlarda axborotni himoya qilish uchun ishlatiladigan murakkab algoritmlargacha rivojlangan. Kriptografiya simmetrik va assimetrik shifrlash usullariga bo‘linadi. Simmetrik shifrlashda bir xil kalitdan foydalangan holda ma’lumotlar shifrlanadi va qayta ochiladi. Assimetrik shifrlashda esa ochiq va yopiq kalit juftligi ishlatiladi, bu esa xavfsizlikni oshirishga imkon beradi.

Hozirgi kunda RSA, AES, ECC kabi kriptografik algoritmlar keng qo‘llaniladi. Shuningdek, kriptografiya elektron imzo, blokcheyn, tarmoq xavfsizligi va maxfiy aloqa sohalarida muhim ahamiyatga ega. Uning amaliy qo‘llanilishi bank tizimlarida, internet xavfsizligida va davlat axborot tizimlarida

keng tarqalgan. Kriptografiyaning rivojlanishi kiberxavfsizlikni mustahkamlashga xizmat qiladi va axborotning maxfiyligi, yaxlitligi hamda autentifikatsiyasini ta’minlashda asosiy vositalardan biri hisoblanadi.

Asimmetrik shifrlash tizimlarida ma'lumotlarni shifrlash va de-shifrlash uchun ikki kalitdan foydalaniladi: ochiq kalit (public key) va yopiq kalit (private key). Ochiq kalit ma’lumotni shifrlash uchun ishlatiladi va uni himoyalanmagan kanallar orqali bemalol uzatish mumkin. Yopiq kalit esa faqat shifrlangan ma’lumotni ochish (deshifrovka qilish) uchun ishlatiladi.

Ochiq va yopiq kalitlar juda katta sonlar bo‘lib, ular o‘zaro maxsus matematik bog‘liqlikka ega, biroq shunday tarzda tuzilganki, birini bilgan holda ikkinchisini aniqlash juda mushkul (amaliy jihatdan deyarli imkonsiz). Ochiq kalit ommaviy tarqatiladi, yopiq kalit esa foydalanuvchiga xavfiy tarzda saqlanadi. Bu tizimlarda ochiq kalit ma'lumotlarni shifrlash uchun ishlatiladi, va shifrlangan ma'lumotni de-shifrlash uchun foydalanuvchining yopiq kaliti kerak bo'ladi. Asimmetrik shifrlash tizimlari ma'lumotlarni xavfsiz tarzda almashish imkonini beradi va autentifikatsiya, kalit almashish, va tizimlararo aloqalar jarayonlarini osonlashtirish imkonini beradi. Bu tizimlarning kamchiliklari murakkablik, bajarish tezligi, kalitlar boshqarish, kalitlarning o'tkazilishi, va matn uzunligi bo'lishi mumkin. Standartlarni tanlashda standartning afzalliklarini va kamchiliklarini qarshilashish kerak, va foydalanuvchilar o'zlariga mos standartni tanlashadi. Assimetrik shifrlash algoritmlari ikkita kalitdan foydalanadi: — shifrlash kaliti yoki umumiy, va — shifrni ochish kaliti yoki sir. Ochiq kalit sirdan hisoblanadi:. Asimmetrik shifrlash algoritmlari bir tomonlama funksiyalardan foydalanishga asoslangan. Ta'rifga ko'ra, funktsiya bir yo'nalishli, agar: barcha mumkin bo'lgan variantlar uchun hisoblash oson va eng mumkin bo'lgan qiymatlar uchun bunday qiymatni hisoblash juda qiyin.

Asimmetrik shifrlashning ishlash prinsipi

Ochiq kalitdan foydalangan holda ikki subyekt (A va B) o‘rtasida ma’lumot uzatish sxemasi quyidagicha ishlaydi:

Subyekt A ochiq (publik) va yopiq (shaxsiy) kalitlardan iborat juftlikni yaratadi.

Subyekt A ochiq kalitni subyekt B ga uzatadi. Bu uzatish himoyalanmagan kanallar orqali amalga oshirilishi mumkin.

Subyekt B A dan olgan ochiq kalit yordamida ma’lumotlar paketini shifrlaydi va uni subyekt A ga yuboradi. Bu uzatish ham himoyalanmagan kanallar orqali bo‘lishi mumkin.

Subyekt A B yuborgan shifrlangan ma’lumotni faqat o‘zida mavjud bo‘lgan yopiq (sirli) kalit yordamida ochadi (deshifrlaydi).

Bunday sxemada himoyalanmagan kanallar orqali uzatilayotgan ma’lumotlarni ushlab qolish (perexvat) foydasiz, chunki asl ma’lumotni faqatgina yopiq kalit yordamida tiklash mumkin. Bu yopiq kalit esa faqat qabul qiluvchiga ma’lum bo‘ladi va uzatilmaydi.

Asimmetrik algoritmlarning qo‘llanilishi

Asimmetrik shifrlash — bu simmetrik usuldagi asosiy muammoni hal qiluvchi texnologiya. Simmetrik shifrlashda ma’lumotni kodlash va uni ochishda bir xil kalit ishlatiladi. Agar bu kalit himoyalanmagan kanallar orqali uzatilsa, uni ushlab qolish mumkin bo‘ladi, bu esa shifrlangan ma’lumotlarga ruxsatsiz kirish xavfini tug‘diradi.

Boshqa tomondan, asimmetrik algoritmlar sezilarli darajada sekinroq ishlaydi. Shuning uchun ko‘plab zamonaviy kriptotizimlarda simmetrik va asimmetrik shifrlash birgalikda qo‘llaniladi.

Misol:

SSL va TLS kabi protokollar asimmetrik algoritmlardan aloqa o‘rnatish (handshake) bosqichida foydalanadi. Bu bosqichda simmetrik shifrlovchi kalitni xavfsiz tarzda uzatish uchun asimmetrik algoritm ishlatiladi. Shundan so‘ng, ma’lumotlar almashinuvi simmetrik kalit yordamida amalga oshiriladi.

Bundan tashqari, elektron raqamli imzolar yaratishda ham asimmetrik algoritmlar qo‘llaniladi. Imzo yopiq kalit yordamida yaratiladi, ochiq kalit

yordamida esa tekshiriladi. Bu — ma’lumot muallifligini va yaxlitligini tasdiqlashga xizmat qiladi.

Mashhur asimmetrik shifrlash algoritmlari:

1. **RSA** (Rivest, Shamir va Adleman familiyalari nomidan): Katta sonlarni faktorizatsiya qilishdagi hisoblash murakkabligiga asoslangan. SSL/TLS protokollarida, PGP, S/MIME standartlarida qo‘llaniladi. mMa’lumotlarni shifrlash va raqamli imzo yaratishda ishlatiladi.
2. **DSA** (Digital Signature Algorithm — "raqamli imzo algoritmi"): Diskret logarifm masalasining murakkabligiga asoslangan. Raqamli imzolar yaratish uchun qo‘llaniladi. DSS (Digital Signature Standard) tarkibiga kiradi.
3. **El-Gamal algoritmi**: Diskret logarifm muammosiga asoslangan. DSA asosida yaratilgan, shuningdek, eski GOST 34.10–94 standartida ham qo‘llanilgan. Shifrlash va raqamli imzo yaratishda ishlatiladi.
4. **ECDSA** (Elliptic Curve Digital Signature Algorithm): Elliptik egri chiziqlar nuqtalari ustida diskret logarifm muammosiga asoslangan. Raqamli imzolar yaratishda, xususan Ripple kriptovalyutasidagi tranzaksiyalarni tasdiqlashda ishlatiladi.

Asimmetrik shifrlashning ishonchliligi

Nazariy jihatdan, asimmetrik shifrlashning yopiq (privat) kalitini ochiq (publik) kalit asosida topish mumkin, chunki algoritmning ishlash prinsipi hamma uchun ochiq. Biroq, amaliyotda bu juda katta vaqt va resurs talab qiladi, shuning uchun bunday shifrlash usullari ishonchli deb hisoblanadi. Masalan, RSA algoritmi asosida 768 bitli kalit bilan shifrlangan ma’lumotni oddiy 2.2 GHz chastotali AMD Opteron protsessorli kompyuterda ochish uchun 2000 yil vaqt ketgan bo‘lardi.

Shifrlash ishonchliligi quyidagilarga bog‘liq:

- Kalit uzunligiga;
- Algoritm asosida yotgan matematik muammoning murakkabligiga;
- Mavjud texnologiyalar darajasiga.

Xulosa qilib aytganda kriptografik shifrlash usullari ma’lumot xavfsizligini ta’minlash uchun muhim. Assimetrik shifrlash esa xavfsizroq, lekin resurs talab qiladi. Zamonaviy xavfsizlik tizimlarida AES, RSA va ECC kabi algoritmlar keng qo‘llaniladi. Shu bilan birga, kvant shifrlash kelajakda yanada ishonchli texnologiya bo‘lishi mumkin.

Foydalanilgan adabiyotlar.

1. Балакирев П. А. АНАЛИЗ АЛГОРИТМОВ АСИММЕТРИЧНОГО ШИФРОВАНИЯ // Вестник науки. 2020. №4 (25). URL: https://cyberleninka.ru/article/n/analiz-algoritmov-asimmetrichnogo-shifrovaniya (дата обращения: 10.09.2025).

2. Sh.Z.Yo‘ldoshev tarmoq xavfsizligi dasturlari va vositalari turlari//Hayot davomidata’limparadigmasi diskursida andragogikaning kompetensiyaviy imkoniyatlari xalqaro ilmiy-amaliykonferensiya, 2024. 544-548 b.

3.Goldwasser S., Bellare M. Lecture Notes on Cryptography // IEEE Trans. Inform. Theory. 2008. C. 289.

4. Stinson D.R. Cryptography: theory and practice. Boca Raton: CRC Press, 1995. 434 с. 40 Шифр Эль-Гамаля [Электронный ресурс].
URL: https://studme.org/239583/informatika/shifr_gamalya (дата обращения: 14.03.2020)

5. Петрушенко А.А. Криптосистема Эль-Гамаля [Электронный ресурс]. URL: https://moluch.ru/conf/tech/archive/164/9306/ (дата обращения: 12.04.2020).