KALITLARNI TAQSIMLASH PROTOKOLLARINING TAHLILI.

Mamadaliyev Ahadjon Abdusalom o‘gli
Toshkent Axborot Texnalogiyalar Universiteti. Talaba.
E- mail. axadjonmamadaliyev22@gmail.com
+998938317755
Saloxiddinov Og’abek Uyg’unjon o’g’li
Toshkent Axborot Texnologiyalari Universiteti,talaba
E-mail:salohiddinovogabek15@gmail.com
+998938555568
Boboqulov Behro'z Muzaffar o'g'li
Toshkent Axborot Texnologiyalari Universiteti,talaba
E-mail. boboqulovbehruz639@gmail.com
+998976750402
Ilmiy rahbar: ***Imamaliyev Aybek Turapbayevich***
oimamaliyev1987@gmail.com

Annotatsiya: Ushbu maqolada kalitlarni taqsimlash protokollari tahlil qilinadi, jumladan, klassik, kvant va blokcheyn asosidagi yondashuvlar ko'rib chiqiladi. Har bir protokolning o'ziga xos xususiyatlari, afzalliklari va kamchiliklari muhokama qilinadi. Shuningdek, ushbu protokollarning zamonaviy axborot texnologiyalari va xavfsizlik talablariga mosligi tahlil qilinadi.

Kalit so'zlar: kalitlarni taqsimlash protokollari, Diffi-Xellman, RSA, kvant kalit taqsimoti, blokcheyn, axborot xavfsizligi.

Аннотация: В данной статье анализируются протоколы распределения ключей, включая классические, квантовые и блокчейн-ориентированные подходы. Рассматриваются специфические особенности, преимущества и недостатки каждого протокола. Также анализируется соответствие этих протоколов современным требованиям информационных технологий и безопасности.

Ключевые слова: протоколы распределения ключей, Диффи-Хеллман, RSA, квантовое распределение ключей, блокчейн, информационная безопасность.

Abstract: This article analyzes key distribution protocols, including classical, quantum, and blockchain-based approaches. The specific features, advantages, and disadvantages of each protocol are discussed. Additionally, the compliance of these protocols with modern information technology and security requirements is analyzed.

Keywords: key distribution protocols, Diffie-Hellman, RSA, quantum key distribution, blockchain, information security.

Kirish

Axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda, ma'lumotlarning xavfsizligini ta'minlash muhim ahamiyat kasb etmoqda. Shifrlash tizimlarida kalitlarni ishonchli taqsimlash va boshqarish ushbu xavfsizlikning asosiy omillaridan biridir. Kalitlarni taqsimlash protokollari orqali ikki yoki undan ortiq tomonlar o'rtasida maxfiy kalitlarni xavfsiz almashish imkoniyati yaratiladi. Ushbu maqolada turli kalit taqsimlash protokollari tahlil qilinadi va ularning afzalliklari hamda kamchiliklari ko'rib chiqiladi.

Tahlil va muhokama

1. Klassik kalit taqsimlash protokollari

Klassik kriptografiyada kalitlarni taqsimlash uchun asosan ikkita asosiy protokol qo'llaniladi: Diffi-Xellman va RSA.

Diffi-Xellman kalit almashinuvi: 1976 yilda Whitfield Diffie va Martin Hellman tomonidan taklif etilgan ushbu protokol ikki tomon o'rtasida umumiy maxfiy kalitni ochiq kanal orqali xavfsiz yaratish imkonini beradi. Bu usul katta butun sonlarning darajalarini hisoblashning bir tomonlama funksiyasiga asoslanadi. Biroq, Diffi-Xellman autentifikatsiyani ta'minlamaydi, ya'ni tomonlarning shaxsini tasdiqlamaydi.

RSA algoritmi: Rivest, Shamir va Adleman tomonidan 1977 yilda ishlab chiqilgan RSA algoritmi ochiq kalitli kriptografiyaning asosiy namunasidir. U katta butun sonlarni faktorlashning murakkabligiga asoslanadi va nafaqat kalitlarni taqsimlash, balki raqamli imzolar uchun ham qo'llaniladi. RSA autentifikatsiyani ta'minlaydi, lekin hisoblash jihatidan Diffi-Xellmandan sekinroq ishlaydi.

2. Kvant kalit taqsimoti

Kvant kompyuterlarining rivojlanishi bilan klassik kriptografik tizimlarning zaifliklari yaqqol namoyon bo'ldi. Kvant kalit taqsimoti (QKT) kvant mexanikasi prinsiplari asosida maxfiy kalitlarni xavfsiz almashish imkonini beradi. QKT protokollari, masalan, BB84, fotonlarning kvant xususiyatlaridan foydalangan holda, eshitish (eavesdropping) urinishlarini aniqlash imkoniyatiga ega. Biroq, QKT tizimlari amaliyotda hali keng qo'llanilmaydi va texnologik cheklovlarga ega.

3. Blokcheyn asosidagi kalit taqsimlash protokollari

So'nggi yillarda blokcheyn texnologiyasi turli sohalarda, jumladan, kalitlarni taqsimlashda ham qo'llanilmoqda. Blokcheynning o'zgarmasligi va markazlashmaganligi tufayli, kalitlarni taqsimlash jarayonida ishonchlilik va shaffoflikni ta'minlash imkoniyati mavjud. Biroq, blokcheyn asosidagi yondashuvlar hali rivojlanish bosqichida bo'lib, ularning samaradorligi va xavfsizligi bo'yicha qo'shimcha tadqiqotlar talab etiladi.

4. Simsiz sensor tarmoqlari uchun kalit taqsimlash

Simsiz sensor tarmoqlari (SST) cheklangan resurslarga ega bo'lgan kichik qurilmalardan tashkil topgan bo'lib, ularda kalitlarni taqsimlash alohida muammolarni

keltirib chiqaradi. An'anaviy protokollar SST uchun mos emasligi sababli, maxsus yondashuvlar, masalan, tasodifiy kalit oldindan taqsimlash va iyerarxik kalit boshqarish sxemalari taklif etilgan. Biroq, bu yondashuvlarning xavfsizligi va samaradorligi tarmoqning o'lchami va topologiyasiga bog'liq.

5. Internet narsalari (IoT) uchun kalit yaratish

Internet narsalari (IoT) qurilmalari sonining ortishi bilan, ularga mos keladigan yengil va samarali kalit yaratish mexanizmlari zarurati yuzaga keldi. IoT uchun kalit yaratish usullari, masalan, fizik jihatdan klonlab bo'lmaydigan funksiyalar (PUF) asosida, qurilmalar o'rtasida xavfsiz kalit almashish imkonini beradi. PUF-lar qurilmalarning jismoniy xususiyatlariga asoslanib, har bir qurilma uchun noyob kalit yaratadi, bu esa autentifikatsiya va kalit taqsimlash jarayonlarini soddalashtiradi. Biroq, PUF-larning amaliyotda qo'llanilishi hali ham tadqiqot bosqichida bo'lib, ularning ishonchliligi va xavfsizligi bo'yicha qo'shimcha tadqiqotlar talab etiladi.

Xulosa

Kalitlarni taqsimlash protokollari axborot xavfsizligini ta'minlashda muhim rol o'ynaydi. Klassik yondashuvlar, masalan, Diffi-Xellman va RSA, uzoq yillardan beri qo'llanilib kelinmoqda va o'zining samaradorligini isbotlagan. Biroq, texnologik rivojlanish va yangi tahdidlar paydo bo'lishi bilan kvant kalit taqsimoti va blokcheyn asosidagi yondashuvlar kabi yangi protokollar ishlab chiqilmoqda. Shuningdek, simsiz sensor tarmoqlari va IoT kabi cheklangan resurslarga ega tizimlar uchun maxsus kalit taqsimlash usullari talab etiladi. Har bir yondashuvning o'ziga xos afzalliklari va kamchiliklari mavjud bo'lib, ularni tanlashda tizimning xususiyatlari va xavfsizlik talablarini hisobga olish zarur.

Foydalanilgan adabiyotlar ro'yxati

1. Gheorghieș, A.-Ș., Lăzăroi, D.-M., & Simion, E. (2021). A Comparative Study of Cryptographic Key Distribution Protocols. Cryptology ePrint Archive.
2. Alshammari, M. R., & Elleithy, K. M. (2018). Efficient and Secure Key Distribution Protocol for Wireless Sensor Networks. Sensors, 18(10), 3569.
3. Zhang, Z., Liu, Y., Zuo, Q., Harn, L., Qiu, S., & Cheng, Y. (2020). PUF-Based Key Distribution in Wireless Sensor Networks. Computers, Materials & Continua, 64(2), 1261-1280.
4. Szymoniak, S., Piątkowski, J., & Kurkowski, M. (2024). Key Distribution and Authentication Protocols in Wireless Sensor Networks: A Survey. ACM Computing Surveys, 56(6).
5. Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.
6. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.

7. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum Cryptography. Reviews of Modern Physics, 74(1), 145-195.
8. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
9. Zhou, J., & Leung, V. C. M. (2008). A Survey of Key Management in Wireless Sensor Networks. Journal of Network and Computer Applications, 31(2), 1-15.
10. Liu, A., & Ning, P. (2003). TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks.