ZAMONAVIY KRIPTOGRAFIYA USULLARI VA AXBOROT XAVFSIZLIGINI TA'MINLASHDAGI ROLI

Norinov Muhammad Yunus Usibjonovich
Toshkent Axborot Texnologiyalari Universiteti Farg'ona filiali
mnorinov@umail.com
Telefon:+998 93 735 00 40
Tug'unboyev Ismoiljon Oybek o'g'li
Toshkent Axborot Texnologiyalari Universiteti Farg'ona filiali Dasturiy injiniring va kiberxavfsizlik fakulteti Axborot xavfsizligi yo'nalishi 2-bosqich talabasi
E-mail: ismoiljonturgunboyev66@gmail.com
Telefon:+998 99 930 08 28

Annotatsiya: *Maqolada axborot xavfsizligi va kriptografiyaning zamonaviy yo'nalishlari tahlil qilingan. Kriptografiya axborotni himoya qilish va yaxlitligini ta'minlashda muhim vosita sifatida ko'rsatilgan. Shuningdek, kriptografiyaning asosiy usullari, elektron imzo va kiberxavfsizlikdagi roli haqida ma'lumot berilgan. Ilmiy va amaliy takliflar orqali tizimlarni mustahkamlash tavsiya qilingan.*

Kalit so'zlar: *Kriptografiya, Axborot xavfsizligi, Shifrlash, Kriptotahlil, Ochiq kalitli tizim, Maxfiylik, Yaxlitlik, Kriptografik algoritmlar, Sun'iy intellekt, Kiberxavfsizlik, Elektron imzo, Kriptotizimlar, Kvant kompyuterlar, Standartlashtirish, Ma'lumotlarni himoya qilish.*

Annotation. *The article analyzes modern trends in information security and cryptography. Cryptography is presented as an essential tool for protecting information and ensuring its integrity. Key methods of cryptography, the role of electronic signatures, and their significance in cybersecurity are discussed. Scientific and practical recommendations for strengthening systems are proposed.*

Keywords: *cryptography, information security, encryption, cryptanalysis, public key systems, confidentiality, integrity, cryptographic algorithms, artificial intelligence, cybersecurity, electronic signature, cryptosystems, quantum computers, standardization, data protection.*

Аннотатsiя. *В статье анализируются современные направления информатsионной безопасности и криптографии. Криптография представлена как важный инструмент для защиты информатsии и обеспечения её целостности. Рассмотрены основные методы криптографии, роль электронной подписи и её значение в кибербезопасности. Рекомендовано укреплять системы с помощью научных и практических предложений.*

Ключевые слова: *криптография, информатsионная безопасность, шифрование, криптоанализ, системы с открытым ключом, конфиденциальность, целостность, криптографические алгоритмы, искусственный интеллект, кибербезопасность, электронная подпись, криптосистемы, квантовые компьютеры, стандартизатsия,*

защита данных.

Bugungi kunda axborot texnologiyalari sohasi yildan-yilga rivojlanib, uning turli yo‘nalishlari shakllanmoqda. Jumladan, axborot xavfsizligi bu yo‘nalishlarning eng muhimlaridan biri hisoblanadi. Axborot xavfsizligi zamonaviy hayotimizda katta ahamiyatga ega bo‘lib, bizning shaxsiy ma’lumotlarimizni himoya qilishda, ma’lumotlarning to‘g‘ri saqlanishini ta’minlashda, shuningdek, ularni ruxsatsiz kirish va o‘zgartirishdan himoya qilishda muhim rol o‘ynaydi. Axborot xavfsizligi bo‘limlari orasida kriptografiya alohida o‘rin egallaydi, chunki u maxfiylik va yaxlitlikni ta’minlashga qaratilgan ilg‘or usullarni o‘z ichiga oladi.

Kriptografiya: Ta’rif va Tarix

Kriptografiya so‘zi qadimdan "maxfiy yozuv" yoki "shifrlash" ma’nosini anglatgan. Ushbu soha insoniyat tarixida yozuvning ilk paydo bo‘lish davrlaridayoq shakllangan. Dastlabki bosqichlarda kriptografiya ma’lumotlarni oddiy usullar bilan yashirishni o‘z ichiga olgan bo‘lsa, zamonaviy texnologiyalar bilan u ancha takomillashdi. Bugungi kunda kriptografiya ma’lumotlarni diskda, tarmoqda yoki boshqa raqamli formatlarda saqlash va uzatishda himoya qilish maqsadida qo‘llaniladi. Shifrlash jarayonida turli matematik algoritmlar qo‘llanilib, ma’lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasi ta’minlanadi.

Kriptografiya har qanday raqamli ma’lumotga nisbatan qo‘llanilishi mumkin. Ushbu texnologiya yordamida ma’lumotlarning o‘zgartirilishini, o‘g‘rilanishini yoki soxtalashtirilishini oldini olish mumkin. Ayniqsa, to‘lov hujjatlarini elektron pochta orqali yuborish yoki onlayn tranzaksiyalarni amalga oshirishda kriptografiya muhim ahamiyatga ega. Bu jarayonda ma’lumotlarning haqiqiyligi va butligi maxsus algoritmlar orqali ta’minlanadi.

Kriptografiyaning Asosiy Yo‘nalishlari

Kriptologiya – bu ikki asosiy bo‘limdan iborat kompleks soha:

1. **Kriptografiya** – ma’lumotlarning maxfiyligi va haqiqiyligini ta’minlashga qaratilgan.
2. **Kriptotahlil** – shifrlangan ma’lumotlarni tahlil qilish va himoya tizimlarining zaif tomonlarini aniqlashni o‘z ichiga oladi.

Kriptografiyaning vazifasi nafaqat ma’lumotlarni ruxsatsiz kirishdan himoya qilish, balki ularni autentifikatsiyalash, ya’ni haqiqiyligini tasdiqlashdir. Bu jarayon ma’lumotlarning kelib chiqishini aniqlash va ularning manba tomonidan yuborilganligiga ishonch hosil qilishni ham o‘z ichiga oladi.

Asimmetrik va Simmetrik Tizimlar

Kriptografiya ikki asosiy tizimga bo‘linadi:

1. **Simmetrik kalitli tizimlar** – bitta kalit yordamida ma’lumotlar shifrlanadi va dekodlanadi. Ushbu usul oson va samarali bo‘lsa-da, kalitni xavfsiz saqlash katta ahamiyatga ega.
2. **Asimmetrik kalitli tizimlar** – ikki xil kalitdan foydalaniladi: biri ochiq, ikkinchisi maxfiy. Ochiq kalit orqali ma’lumot shifrlansa, maxfiy kalit uni tiklash uchun

ishlatiladi. Bu usul yuqori darajadagi xavfsizlikni ta’minlaydi va elektron imzo, autentifikatsiya kabi texnologiyalarni qo‘llash imkonini beradi.

Kriptografiyada Maxfiylik va Yaxlitlik

Kriptografiyaning asosiy maqsadlaridan biri – ma’lumotlarning maxfiyligi va yaxlitligini ta’minlashdir:

- ***Maxfiylik*** – ma’lumotlarni ruxsatsiz kirishdan himoya qilishni bildiradi.
- ***Yaxlitlik*** – ma’lumotlarni o‘zgartirishdan himoya qilishni anglatadi.

Bu jarayonlarda kalitlarni xavfsiz saqlash muhimdir. Simmetrik tizimda kalitlarni xavfsiz uzatish uchun himoyalangan kanallar qo‘llaniladi. Asimmetrik tizimlarda esa faqat ochiq kalit uzatiladi, maxfiy kalit sir saqlanadi.

Kriptografiyada Almashtirish Usullari

Kriptografiyada ma’lumotlarni shifrlash uchun turli usullar qo‘llaniladi. Shulardan biri – **Sezar usuli**. Ushbu usulda harflar belgilangan k darajadagi siljish orqali shifrlanadi. Masalan, "SAMARQAND" so‘zi Sezar usuli yordamida "VDPDUTDQG" ko‘rinishiga keladi.

Sezar usulidan tashqari quyidagi usullar ham mavjud:

- **Sehrli kvadrat** – bu usulda raqamlar va belgilardan foydalangan holda maxsus jadval tuziladi.
- **Affin usullari** – ma’lumotlarni matematik formulalar yordamida o‘zgartirish.
- **Tayanch so‘zli usullar** – belgilangan kalit so‘z asosida shifrlash.

Sehrli Kvadrat Usuli

Sehrli kvadrat – bu shifrlash usullaridan biri bo‘lib, unda raqamlar va belgilar maxsus kvadrat shaklidagi jadvalga joylashtiriladi. Misol sifatida 4x4 o‘lchovli sehrli kvadratni olaylik. Ushbu kvadratdagi har bir ustun, diagonal va satrdagi raqamlar yig‘indisi bir xil bo‘ladi. Shifrlash jarayonida kvadratning ichiga matn belgilar tartib bo‘yicha kiritiladi va olingan matn satrlar bo‘yicha o‘qiladi. Masalan, "DASTURLASH TILLARI" matni sehrli kvadrat yordamida shifrlanganda quyidagicha ko‘rinishga ega bo‘ladi: **ISAL UTIA SHRLL TRAD**.

Sehrli kvadrat, Sezar usuli va boshqa kriptografik yondashuvlar yordamida ma’lumotlarni himoya qilish texnologiyalari axborot xavfsizligini ta’minlashda muhim rol o‘ynaydi. Shu bilan birga, zamonaviy kriptografiya yangi algoritmlar va texnologiyalar bilan boyitilib, axborot xavfsizligini ta’minlashni yangi bosqichga olib chiqmoqda.

Xulosa. Kriptografiya va axborot xavfsizligi zamonaviy texnologiyalar davrida juda muhim ahamiyatga ega. Kriptografiya ma’lumotlarning maxfiyligini saqlash va yaxlitligini ta’minlashda muhim rol o‘ynaydi. Ochiq kalitli tizimlar va shifrlash usullari yordamida axborotlarni himoya qilish mumkin. Kriptotahlil tizimlarning zaifliklarini aniqlashga yordam beradi, bu esa tizimlarning mustahkamligini oshiradi.

Ilmiy va amaliy takliflar, masalan, yangi shifrlash algoritmlarini yaratish, matematik tahlilni chuqurlashtirish va sun’iy intellektni qo‘llash orqali axborot xavfsizligini kuchaytirish mumkin. Kriptografiya va axborot xavfsizligi sohalarining rivojlanishi kiberxavfsizlikni ta’minlashda muhim rol o‘ynaydi, shuningdek, doimiy yangilanishlar va texnologik takomillashtirishlar zarur.

FOYDALANILGAN ADABIYOTLAR

1. Schneier, B. **Applied Cryptography: Protocols, Algorithms, and Source Code in C.** Wiley, 2015.
2. Stallings, W. **Cryptography and Network Security: Principles and Practice.** Pearson, 2020.
3. Katz, J., & Lindell, Y. **Introduction to Modern Cryptography.** CRC Press, 2020.
4. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. **Handbook of Applied Cryptography.** CRC Press, 1996.
5. Diffie, W., & Hellman, M. E. **New Directions in Cryptography.** IEEE Transactions on Information Theory, 1976.
6. Rivest, R. L., Shamir, A., & Adleman, L. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.** Communications of the ACM, 1978.
7. Koblitz, N. **A Course in Number Theory and Cryptography.** Springer, 2006.
8. Nielsen, M. A., & Chuang, I. L. **Quantum Computation and Quantum Information.** Cambridge University Press, 2010.
9. Boneh, D., & Shoup, V. **A Graduate Course in Applied Cryptography.** Stanford University, 2020.
10. ENISA. **Algorithms, Key Sizes and Parameters Report 2022.** European Union Agency for Cybersecurity, 2022.
11. Shor, P. W. **Algorithms for Quantum Computation: Discrete Logarithms and Factoring.** Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.
12. Rouse, M. **The Role of Artificial Intelligence in Cybersecurity.** TechTarget, 2023.
13. National Institute of Standards and Technology (NIST). **Post-Quantum Cryptography Standardization.** U.S. Department of Commerce, 2023.
14. Kaspersky Lab. **The State of Cybersecurity 2025.** Kaspersky Security Report, 2023.