DATA PROTECTION AND ENCRYPTION METHODS.

Khusainov Shikhnazar Madamiovich
Teacher at the Department of General Professional Sciences and Accounting, Mamun University, Khiva, Uzbekistan E-mail.: shihnazar4220gmail.com

Annotation: *In the digital age, vast amounts of data are generated, stored, and transmitted. Protecting this data from unauthorized access, modification, or destruction is crucial. Encryption stands as a cornerstone of data security, scrambling information into an unreadable format using cryptographic keys. This article explores the different data protection and encryption methods, delving into symmetric and asymmetric encryption, hashing techniques, and their applications. The effectiveness of these methods and the ongoing challenges in data security are also discussed.*

Keywords: *Data protection, Encryption, Symmetric encryption, Asymmetric encryption, Hashing, Data security, Cryptography*

Аннотация: *В цифровом веке огромные объемы данных генерируются, хранятся и передаются. Защита этих данных от несанкционированного доступа, изменения или уничтожения имеет решающее значение. Шифрование является краеугольным камнем безопасности данных, превращая информацию в нечитаемый формат с помощью криптографических ключей. Эта статья исследует различные методы защиты данных и шифрования, углубляясь в симметричное и асимметричное шифрование, методы хеширования и их применения. В ней также обсуждается эффективность этих методов и постоянные проблемы безопасности данных.*

Ключевые слова: *Защита данных, Шифрование, Симметричное шифрование, Асимметричное шифрование, Хеширование, Безопасность данных, Криптография*

The digital age has ushered in an era of unprecedented data proliferation. From the personal data we entrust to social media platforms to the financial transactions conducted online, vast amounts of information are constantly being generated, stored, and transmitted. This data deluge presents both opportunities and challenges. While it fuels innovation and drives advancements in various sectors, it also creates a critical need for robust data protection measures.

Data protection encompasses a comprehensive set of practices designed to ensure the confidentiality, integrity, and availability (CIA triad) of information. Confidentiality guarantees that only authorized individuals can access sensitive data. Integrity refers to the accuracy and completeness of data, ensuring it remains unaltered during storage or transmission. Finally, availability emphasizes that authorized users can access the data whenever needed[1].

Encryption serves as a cornerstone of data security, playing a pivotal role in achieving the CIA triad. It is a cryptographic technique that transforms data (plaintext) into an unreadable format (ciphertext) using a secret key. This ciphertext appears as a scrambled mess of characters, unintelligible without the corresponding decryption key. Only authorized parties possessing the decryption key can unlock the message and revert it back to its original form.

Types of Encryption

There are two primary categories of encryption methods, each with its strengths and applications:

• Symmetric Encryption: Often referred to as private-key or secret-key cryptography, this method utilizes a single shared key for both encryption and decryption. The sender encrypts the data with the shared key and transmits it to the receiver. Upon receiving the ciphertext, the receiver uses the same shared key to decrypt and access the original message. Symmetric encryption offers efficient processing due to its reliance on a single key. However, the challenge lies in securely distributing the shared key between the sender and receiver. Common symmetric algorithms include the Advanced Encryption Standard (AES), known for its strength and efficiency, and the Triple Data Encryption Standard (3DES), which applies the DES algorithm three times for enhanced security.

• Asymmetric Encryption: Also known as public-key cryptography, this method employs a key pair – a public key and a private key. The public key is freely distributed and can be widely shared. Anyone with the public key can encrypt data and send it to the recipient. However, only the recipient possesses the corresponding private key, which is kept confidential. This private key is used to decrypt the message sent using the public key. Asymmetric encryption is particularly advantageous for secure communication over public networks like the internet, where direct and secure key exchange might be impractical. The Rivest–Shamir–Adleman (RSA) algorithm is a widely used example of asymmetric encryption.

Beyond Encryption: Hashing for Data Integrity

Another crucial data protection technique is hashing. Hashing functions operate by generating a unique mathematical fingerprint (hash) for a specific data set. This hash value acts as a digital signature, essentially a condensed representation of the data's original form. Any alteration, however minor, to the data will result in a completely different hash value. This characteristic makes hashing invaluable for ensuring data integrity. It allows for verification that the data has not been tampered with during storage or transmission. Hashing is often used in conjunction with encryption and digital signatures for robust data protection[2].

Applications of Data Protection and Encryption Methods

Data protection and encryption methods find application in a wide range of scenarios:

• Securing Communication Channels: Encryption safeguards online communication, protecting sensitive data exchange between individuals and organizations. This includes emails containing financial information, medical records transmitted between healthcare providers, and confidential business communications.

• Data Storage Security: Encryption protects data at rest, whether stored on personal devices like laptops and mobile phones, or on organizational servers and cloud storage platforms. This is particularly crucial for safeguarding sensitive data like financial records, customer information, and intellectual property.

• Protecting Data in Transit: Encryption secures data while it's being transferred across networks. This is vital for protecting online transactions, file transfers, and remote access to sensitive information.

• Ensuring Data Compliance: Many regulations, such as HIPAA (Health Insurance Portability and Accountability Act) in the healthcare sector and GDPR (General Data Protection Regulation) in the European Union, mandate data protection measures. Encryption plays a key role in organizations complying with these regulations.

Effectiveness and Challenges

Data protection and encryption methods offer significant benefits for data security. They can:

• Prevent Unauthorized Access: Encryption renders data unreadable to anyone without the decryption key, significantly reducing the risk of unauthorized access to sensitive information.

• Guarantee Data Integrity: Hashing techniques ensure that data remains unaltered during storage or transmission, fostering trust and data accuracy.

• Maintain Data Availability: Encryption protects data from ransomware attacks that encrypt files and demand payment for decryption. This helps organizations maintain access to critical information.

However, data protection also faces challenges:

• Key Management: The security of encryption relies heavily on proper key management practices. Losing or compromising encryption keys can render data permanently inaccessible.

• Evolving Threats: As computing power increases, so does the potential for breaking encryption algorithms. Continuous development of stronger algorithms and staying updated on emerging threats is crucial.

• User Education: Raising awareness about data security practices among users is essential for effective data protection. Understanding the importance of strong passwords and avoiding suspicious links can significantly reduce the risk of data breaches.

CONCLUSIONS AND SUGGESTIONS:

Data protection and encryption methods are indispensable tools in the digital age. By understanding the different techniques and their applications, organizations and individuals can create a robust defense against unauthorized access, data breaches,

and manipulation. As the technological landscape continues to evolve, ongoing research and development of stronger encryption algorithms, coupled with best practices in key management and user education, will be paramount in safeguarding information in the digital world.

REFERENCES:

9. National Institute of Standards and Technology (NIST). (2001, December). Recommendation for block cipher modes of operation. [NIST Special Publication 800-38A]. National Institute of Standards and Technology.

10. Menozzi, A., & Pozzetti, P. (2017). An overview of secure multi-party computation. ACM Computing Surveys (CSUR), 50(3), 1-28.

11. Хусаинов, Ш. М. (2023, June). АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ОБЛАСТИ БУХГАЛТЕРСКОГО УЧЕТА. In Proceedings of Scientific Conference on Multidisciplinary Studies (Vol. 2, No. 6, pp. 104-109).

12. Madaminovich, K. S., Ibragimovich, A. I., & Qurol o‘g‘li, I. B. (2023). Automated Systems in Accounting. Eurasian Scientific Herald, 20, 38-41.

13. Saidovich, R. B. ., Bakhtiyarovna, R. F. ., Madaminovich, X. S. ., & Bakhtiyarovich, S. A. . (2022). Analysis Medical Problems with Database Systems and Create New Models. Procedia of Engineering and Medical Sciences, 31–36. Retrieved from https://procedia.online/index.php/engineering/article/view/205

14. Saidovich, R. B. ., Kabulovna, S. S. ., Madaminovich, X. S. ., & Bakhtiyarovich, S. A. . (2022). New Models and Analysis Solve Medical Problems with Database Systems. Procedia of Engineering and Medical Sciences, 26–30. Retrieved from https://procedia.online/index.php/engineering/article/view/204

15. Madaminovich, K. S., Ibragimovich, A. I., & Qurol o‘g‘li, I. B. (2023). Automated Systems in Accounting. Eurasian Scientific Herald, 20, 38-41.

16. Arturovich, X. T. (2022). IoT QURILMALARINING TURLARI, QO ‘LLASH SOHALARI VA ALOQA MUHITLARI. Komputer texnologiyalari, 1(10).

17. Gulhayo, O., & Barno, A. (2023). IOT SHLYUZINI YARATISHDA MIKROKONTROLLERLARNING AHAMIYATI. Innovations in Technology and Science Education, 2(8), 1299-1310.

18. Gulhayo, O. (2023). ESP8266 MIKROKONTROLLER ASOSIDA IOT SENSORLAR TARMOG‘I UCHUN SHLYUZ YARATISH. Innovations in Technology and Science Education, 2(9), 544-554.

19. Annazarova, B. R. (2023). SENSOR MA’LUMOTLARINI QAYTA ISHLASHDA TAQSIMLANGAN TEXNOLOGIYALAR TAHLILI. Academic research in educational sciences, 4(5), 71-75.

20. Qurol o'g'li, IB, & O'rinboyevich, MM (2024). MATEMATIKA O 'QITISH METODIKASI VA TA'LIMDA ZAMONAVIY TEXNOLOGIYALARDAN FOYDALANISH. IJODKOR O'QITUVCHI , 3 (36), 1-4.

21. Qurol o‘g‘li, I. B. (2024). TELEKOMMUNIKATSIYA TARMOG ‘I MARSHRUTLASH MASALASINI GRAFLAR ORQALI IFODALASH VA YECHISH. PEDAGOG, 7(1), 129-136.

22. Urinboyevich, MM, Qurol o‘g‘li, IB, & Umarbek G‘ayrat o‘g, U. (2024). MENELAUS TEOREMASI UCHBURCHLAR HAQIDAGI VA ULARNING YANGI ISLOTLARI. SO'NGI ILMIY TADQIQOTLAR NAZARIYASI , 7 (2), 1-5.