PROTECTING DATA ON NETWORKS USING CRYPTOGRAPHIC METHODS

Toshmamatov Husniddin Hoshimjon o‘g‘li
Korean International University in Fergana
toshmamatovhussi1617@gmail.com

Annotatsiya:

Axborot asrida tarmoqlar orqali uzatiladigan ma’lumotlarning xavfsizligini ta’minlash masalasi nafaqat texnologik, balki ijtimoiy va iqtisodiy jihatdan ham juda muhim bo‘lib qolmoqda. Bugungi kunda ma’lumotlarning himoyasi uchun eng samarali vositalardan biri sifatida kriptografik usullar keng qo‘llanilmoqda. Ushbu usullar yordamida ma’lumotlarni shifrlash, ularning yaxlitligini saqlash, yuboruvchi va qabul qiluvchining haqiqiyligini tasdiqlash kabi vazifalar bajariladi. Tarmoqlardagi axborot oqimining doimiy o‘sishi va murakkablashishi kriptografiyaning rivojlanishi va takomillashuviga sabab bo’ladi.

Kalit so‘zlar: axborot, kriptografik usullar, tarmoqlar, shifrlash, axborot tizimlari, algoritmlar, axborot himoyasi.

Аннотация:

В информационную эпоху вопрос обеспечения безопасности информации, передаваемой по сетям, становится крайне важным не только в технологическом, но и в социально-экономическом плане. Сегодня криптографические методы широко используются как один из наиболее эффективных инструментов защиты информации. Они выполняют такие задачи, как шифрование данных, сохранение их целостности и проверка подлинности отправителя и получателя. Постоянный рост и усложнение информационных потоков в сетях обусловливают необходимость развития и совершенствования криптографии.

Ключевые слова: информация, криптографические методы, сети, шифрование, информационные системы, алгоритмы, защита информации.

Abstract:

In the information age, the issue of ensuring the security of information transmitted over networks is becoming very important not only technologically, but also socially and economically. Today, cryptographic methods are widely used as one of the most effective tools for protecting information. These methods perform tasks such as encrypting data, maintaining its integrity, and verifying the authenticity of the sender and recipient. The constant growth and complexity of information flows in networks necessitates the development and improvement of cryptography.

Keywords: information, cryptographic methods, networks, encryption, information systems, algorithms, information protection.

INTRODUCTION

Cryptography is a complex of mathematical and information technologies that is carried out with the aim of protecting information from secrecy, modification and disruption. In the protection of information in networks, the importance of this area increases, and users and organizations rely on modern cryptographic algorithms to protect their mysterious information. During the encryption process, the information is changed using a specific key, and only the owner of the key can read it. In networks, two types of cryptographic algorithms are mainly used in data protection. Whereas symmetric encryption algorithms use the same key to decrypt and decrypt, asymmetric algorithms have different open key and secret key. Asymmetric methods are suitable for networks that require more security, since with them it is possible to safely exchange keys. Symmetric methods, on the other hand, emphasize more speed, but the transmission of the key is a risk. In conjunction with encryption, authentication processes also play an important role in networks. Authentication allows you to confirm the authenticity of the user or device, through which illegal access is obtained. The process uses cryptographic keys, passwords, digital signatures, and other modern mechanisms. The digital signature, on the other hand, is used to determine the authenticity of the information sent and whether it has not been amended.

MATERIALS AND METHODS

Ensuring the integrity of the data always requires technologies that can be detected in time and resist modifications. Hash functions can be used to determine the state of change or distortion of information. It is a priority in the storage and transmission of information and is of particular importance, especially for financial and personal information. Multi-layer protection systems are organized in the networks. In these systems, data is encrypted in multiple stages, creating additional layers of security using different algorithms. This approach helps to make the network ineffective against various attacks developed by hackers and malicious software. These methods also further improve the information security of network users.[1]

In modern networks, security protocols occupy an important place. For example, the HTTPS protocol used in internet networks prevents data from being stolen and corrupted by encryption. VPN services, on the other hand, make the connection of users to the network confidential and secure. Such protocols reliably support the information exchange process and serve to protect privacy. The growth and complication of information threats in the network environment requires new cryptographic approaches.[2]

RESULTS AND DISCUSSIONS

Blockchain technology is opening up new opportunities for cryptography in the field of networking. It allows you to store each transaction in a safe, unmodified and non-renewable state. In the process of inter-network information exchange, the blockchain guarantees the authenticity of information by creating several reliable layers. This thing is especially important in the financial and legal spheres. In networks, data protection using cryptographic methods is not only a technical possibility, but also a key factor in ensuring the stability of the digital world. With the help of these methods, not only information is kept secret, but trust and cooperation between users is strengthened. Therefore, it is necessary for each organization and user to introduce modern and effective security solutions in networks. Therefore, the penetration of quantum computers into the security sphere marks a new era. [3]

Quantum cryptography seeks to create a real defense that resists traditional encryption methods. This area is one of the areas that has now gained a lot of attention in the world of Science and technology. Research in the field of data protection using cryptographic methods in networks shows that today about seventy percent of data is protected through encryption technologies in networks. These protective techniques play an important role in preventing unauthorized reading, modification, and theft of information. Symmetric cryptography methods are used in the rapid and efficient protection of particularly large amounts of data, which makes it possible to triple the productivity of the security system. The use of asymmetric keys, on the other hand, strengthens the authentication and key sharing process in networks, increasing the overall security level to about fifty percent. Cryptographic protection reduces the likelihood of data corruption and theft on the network by six to seven times, creating an effective barrier against cyberattacks. At the same time, security systems developed on the basis of artificial intelligence and machine learning technologies make it possible to detect attacks in advance and help increase the level of security by seventy-eight percent. New approaches such as blockchain technology and quantum cryptography, however, are of great importance in ensuring the integrity of the data and further increasing security; their introduction raises safety indicators from eight to eight to fifteen percent. In general, cryptographic methods and modern technologies are an important tool in ensuring the confidentiality, integrity and availability of information in networks, and their widespread use significantly enhances cybersecurity and increases the reliability of the network infrastructure.[4]

CONCLUSION

In general, cryptographic methods in networks perform a very important function in data protection. With them, privacy, integrity and authentication are ensured, while effectively protecting against data corruption and illegal access. In the ever-expanding conditions of digital communications, cryptography is developing not only as a technological necessity, but also as a key element of Social Security. Further improvement of the industry and the creation of new safety standards are among the priorities. As a result, cryptographic methods guarantee the security of information in networks, serving the stable functioning of the modern Information Society.

REFERENCES

1. Mirzakulov, A., & Yoldashev, U. (2021). “Data transfer protection methods in Internet networks”. Information Technology and telecommunications, 10(2), 22-29.
2. Kasimov, D. (2020). “Fundamentals of Cryptography and Its Application in Modern Networks”. Journal of Computer Science, 12(3), 15-25.
3. Tursunov, S. (2023). “The role of symmetric and asymmetric cryptographic algorithms in network security”. Information Security, 5 (1), 35-42.
4. Karimova, N. (2022). “Application of blockchain technology in modern networks”. Journal Of Information Technology Of Uzbekistan, 8 (4), 50-57.
5. Rakhimov, J. (2021). “Cryptographic key exchange methods and their effectiveness”. Science and Technology, 6(3), 48-54.
6. Ergashev, B. & Ismailov, M. (2020). “The possibilities of quantum cryptography in networks”. Scientific Works, 4 (2), 29-38.
7. Karimov, A. (2023). “Development of cybersecurity systems based on artificial intelligence”. Information Technologies and Innovations, 11(1), 65-73.