THE IMPORTANCE OF CRYPTOGRAPHY IN INFORMATION SYSTEMS

Ziyakulov Mirziyo
Student at Secondary School №20 of Angren City
ziyakulovmirziyo@gmail.com

Introduction: The 21st century is a period of technological innovation and information development, and an era of digitalisation. At this point, we have adopted IT across all sectors, with its latest modern tech products. The network systems previously operated only through in-person networking, while currently, we have over two-thirds of our communications online. Though these communications are being made through tech, the information flows through the overall gigantic network systems. We can assume that these networks make our communication more comfortable, but what about the safety of the information flow? What will happen if we want to tell our secrets online? If the flow goes through the whole network, will it stay secret? The answer is clear because the network uses cryptography to keep information secret between the sender and receiver.

Cryptography and Cybersecurity

Cryptography is the science of hiding information by encoding it into an unreadable form. Only people with the correct key can turn it back into its original form. The importance of cryptography in modern information systems is huge. Nearly everything that involves private information—such as passwords, banking details, or private messages—depends on cryptographic methods.

Modern cybersecurity relies heavily on encryption to protect data “in transit” and “at rest.” Without strong cryptography, common activities like online shopping or logging into social media would be unsafe. Academic research shows that encryption is one of the most effective defences against cyber attacks. According to a study on encryption and privacy protection, secure cryptographic systems form the foundation of data security, especially as digital communication continues to increase (Kumar & Singh, 2021).

Cryptographic methods like public-key encryption, hashing, and symmetric encryption are used in everything from HTTPS in web browsers to secure messaging apps. This means every time we send a message on WhatsApp or pay for something online, cryptography is working in the background.

Cyber Attacks and Information Leakage

Even with strong encryption, cyberattacks are on the rise. Hackers look for weak points—especially places where encryption is missing, outdated, or applied incorrectly. Data breaches often occur not because cryptography fails, but because organisations fail to use it properly.

Cyberattacks such as phishing, ransomware, and man-in-the-middle attacks demonstrate the extent of damage that can occur when systems are not protected. Research also shows that weak encryption or poorly managed encryption keys can lead to serious information leakage (Alshamrani et al., 2022). This means organisations must update their cryptographic tools and train employees to recognise threats. Without these steps, even the strongest cryptographic algorithms can be bypassed.

Cybersecurity and Cloud Databases

Cloud storage is now used by schools, businesses, hospitals, and governments. Even though cloud systems are convenient, they create questions about privacy and security. Who can see the stored information? What happens if the cloud provider is hacked? Most cloud services now use strong encryption to protect stored files, and many also use “zero-knowledge” encryption, meaning even the provider cannot read the data.

However, users still play an important role. Weak passwords, careless sharing of login details, or ignoring security updates can break the entire security system. Cryptography can protect data, but it cannot fix human mistakes. This is why cybersecurity education is becoming more important in schools, workplaces, and governments.

Conclusion

Cryptography is a crucial tool in modern information systems. It protects personal messages, online transactions, cloud data, and nearly every digital service we rely on. As cyber attacks grow more advanced, cryptography becomes even more essential. However, technology alone is not enough—people must use it correctly and stay aware of cyber risks. When individuals and organisations combine strong cryptographic tools with responsible cybersecurity practices, information can remain safe in our increasingly digital world.

REFERENCES

1. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2022). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 24(2), 1239–1279. https://doi.org/10.1109/COMST.2022.3143454

2. Kumar, P., & Singh, M. (2021). A survey on data encryption techniques for privacy protection in cloud computing. Materials Today: Proceedings, 47, 449–456. https://doi.org/10.1016/j.matpr.2021.02.613