UDC 004.056.5

CRYPTOGRAPHIC PRINCIPLES IN THE AGE OF ARTIFICIAL INTELLIGENCE

A. R. Taylyyeva

Oguz han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan

Abstract. Cryptographic information protection is paramount in today's digital age, safeguarding sensitive data from unauthorized access. This discipline employs algorithms to encrypt information, rendering it unintelligible without the correct decryption keys. Encryption ensures confidentiality, while cryptographic hash functions guarantee data integrity by detecting alterations. Secure authentication protocols, like Public Key Infrastructure (PKI), verify identities and prevent repudiation. Effective key management is crucial, encompassing secure key

generation, distribution, and storage. The strength of cryptographic systems relies on robust algorithms and diligent key handling. Ongoing research and development are essential to counter evolving cyber threats. As data breaches become more frequent, the application of strong cryptographic measures is vital for maintaining trust and security in digital interactions. This field is constantly adapting to new challenges, ensuring that sensitive information remains protected.
Keywords: Encryption; decryption; algorithms; keys; integrity; authentication; confidentiality; Public Key Infrastructure; hash functions; cybersecurity.

Introduction

In our modern world, computers and the internet are used for almost everything. We send emails, shop online, and store important documents digitally. All this information needs to be protected from people who might want to steal it or change it. That's where cryptographic information protection comes in. Imagine you have a secret message you want to send to a friend. You wouldn't want anyone else to read it, right? Cryptography is the process of converting between readable text, called plaintext, and an unreadable form, called ciphertext. This occurs as follows:

1. The sender converts the plaintext message to ciphertext. This part of the process is called encryption (sometimes encipherment).

2. The ciphertext is transmitted to the receiver.

3. The receiver converts the ciphertext message back to its plaintext form. This part of the process is called decryption (sometimes decipherment).

Main Part

Encryption: Turning Plain Text into Secret Code: The process of turning your message into a secret code is called encryption. You use an algorithm, which is like a set of rules, to scramble the letters of your message. Think of it as a special recipe that changes your message into something only you and your friend understand. To make the algorithm work, you need a key. A key is like a secret password. Without the key, the algorithm can't scramble or unscramble the message. There are different kinds of keys. Some keys are used for both encryption and decryption, while others come in pairs, a public key and a private key.

Decryption: Unscrambling the Secret Code: When your friend receives the encrypted message, they use the same algorithm and the correct key to turn it back into the original message. This is called decryption. It's like using the recipe in reverse to get back to the original message.

Algorithms: The Secret Recipes: Algorithms are the heart of cryptography. They are mathematical formulas that make encryption and decryption possible. Some common algorithms include AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman). These algorithms are very complex, and it's nearly impossible to break the code without the key.

Keys: The Secret Passwords: Keys are essential for keeping information secure. Without the right key, even the strongest algorithm is useless. There are two main types of keys:

– Symmetric keys: These keys are used for both encryption and decryption. Both the sender and receiver need to have the same key.

– Asymmetric keys: These keys come in pairs: a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret. The public key encrypts the message, and the private key decrypts it.

Integrity: Making Sure the Message Stays the Same: Integrity means making sure that the message hasn't been changed or tampered with during transmission. To check integrity,

we use hash functions. A hash function takes the message and creates a unique "fingerprint" called a hash. If the message is changed, even slightly, the hash will be different.

Hash Functions: Digital Fingerprints: Hash functions are one-way functions, meaning you can't get the original message back from the hash. They are used to verify that a file or message hasn't been altered.

Authentication: Proving You Are Who You Say You Are: Authentication is the process of verifying that someone is who they claim to be. This is important for preventing unauthorized access to systems and information. For example, when you log in to your email account, you need to provide your username and password, which are used to authenticate you.

Public Key Infrastructure (PKI): Public Key Infrastructure (PKI) is a system that helps manage and distribute public keys. It uses digital certificates to verify the identity of individuals and organizations. PKI helps to ensure that public keys are authentic and haven't been tampered with.

Confidentiality: Keeping Information Secret: Confidentiality is one of the main goals of cryptography. It means keeping information secret from unauthorized people. Encryption is the primary way to achieve confidentiality.

Cybersecurity: Protecting the Digital World: All these cryptographic techniques are part of a larger field called cybersecurity. Cybersecurity is about protecting computers, networks, and data from unauthorized access, damage, or theft. It includes everything from using strong passwords to implementing complex encryption systems.

Why Cryptographic Information Protection Matters

Cryptographic information protection is essential for many reasons:

– Protecting sensitive information: It keeps personal information, financial data, and business secrets safe.

– Ensuring secure communication: It allows people to communicate securely over the Internet.

– Maintaining trust: It helps to build trust in online transactions and services.

– Combating cybercrime: It makes it harder for criminals to steal or manipulate data.

Conclusion

Cryptographic information protection is a fundamental pillar of cybersecurity. By understanding the core concepts and applying appropriate techniques, organizations and individuals can safeguard their sensitive data from unauthorized access and ensure the integrity of their digital communications. As technology continues to advance, cryptography will remain a critical tool for protecting information in an increasingly interconnected world.

References

1. Applied Cryptography: Protocols. Algorithms. and Source Code in C" by Bruce Schneier
2. Cryptography and Network Security: Principles and Practice" by William Stallings
3. Handbook of Applied Cryptography" by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone.
4. NIST (National Institute of Standards and Technology) Publications
5. "Guidelines on cryptographic algorithms usage and key management" (2023) Published by the European Payments Council (EPC).

Information about the author

Taylyyeva A.R., Student. Oguz han Engineering and Technology University of Turkmenistan. taylyyewaaynur@gmail.com