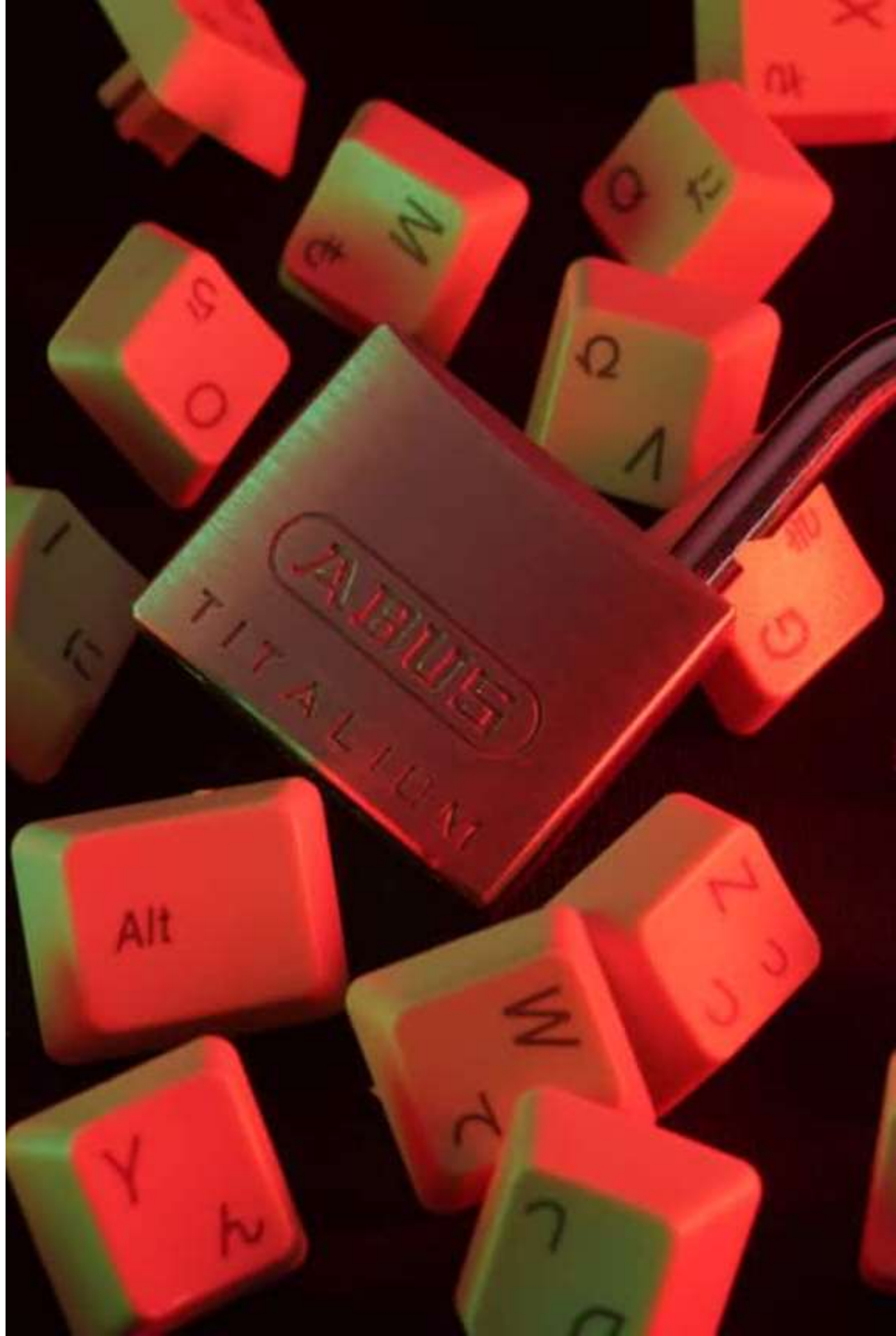
Encryption Standards

Understanding the science of protecting information through cryptographic methods



What is Cryptography?

Cryptography is the science of information protection through encryption. It transforms open information into encrypted data and back through encryption and decryption processes.
For successful decryption, two conditions must be met: the decryption function must correspond to the encryption function, and the decryption key must match the encryption key.

Core Functions

- Confidentiality of transmitted data
- Integrity and authenticity verification
- Subscriber authentication

The Evolution of Encryption

1st Century BC

Julius Caesar develops the Caesar cipher, the first documented symmetric encryption system

1

1977

DES standard introduced in the United States with 56-bit key length

2

1989

Russian GOST 28147-89 encryption standard established

3

Modern Era

Advanced Encryption Standard (AES) becomes the new US cryptographic standard

4

Symmetric vs. Asymmetric Encryption

Symmetric Encryption

Same key for encryption and decryption

- Fast and computationally simple
- Requires secure key exchange
- Examples: DES, GOST 28147-89, AES

Asymmetric Encryption

Key pairs: public and private keys

- Slower but more secure distribution
- No direct key exchange needed
- Examples: RSA, DSA, GOST R 34.10

Cryptographic Keys Explained

A cryptographic key is a sequence of characters generated by specific rules, used for cryptographic transformations. According to GOST 28147-89, a key is "the specific secret state of parameters that ensures selection of one transformation from all possible transformations."

01

Key Generation

Created using algorithms based on unique random number sequences

02

Key Application

Same source information encrypted differently with different keys

03

Cryptographic Strength

Measures difficulty of obtaining source text without the corresponding key

Challenges in Cryptography

Symmetric Encryption Issues

Keys must be transferred "from hand to hand," making it unsuitable for systems with many participants.

Asymmetric Encryption Limitations

- Significantly slower due to computationally expensive operations
- Cryptographic strength not formally proven
- Risk of public key spoofing by attackers

Hybrid Cryptography Solution

Session Key Creation

Generate one-time symmetric encryption key for the message

Message Encryption

Encrypt message quickly using symmetric algorithm with session key

Key Encryption

Encrypt session key with recipient's public key using asymmetric algorithm

Transmission

Send encrypted message with encrypted session key to recipient

This approach combines the speed of symmetric encryption with the security of asymmetric key distribution, significantly reducing message size and encryption time.

Digital Signatures & Certificates

Electronic Digital Signature

Digital analogue of manual signature that verifies document authenticity and integrity. If a document is altered during transmission, the signature is recognized as incorrect.

Certificates

Data sets containing public keys and owner information, issued by certification centers. Certificates are verified through chains of trust ending in root documents.

Key Management & Security

Random Number Generation

Keys created using hardware sensors or keyboard generators based on unique random sequences

Private Key Storage

Stored encrypted in files or USB tokens like Blizzard, protected by passwords

Key Compromise

Unauthorized access requires immediate key revocation and addition to CRL stop lists

Critical Security Practice: Never store private keys on a computer's hard drive. Always use separate encrypted media with password protection.

Key Takeaways

Cryptography ensures confidentiality, integrity, and authenticity

The foundation of modern information security systems protecting data transmission and storage

Multiple encryption methods serve different purposes

Symmetric for speed, asymmetric for secure distribution, hybrid for optimal balance

Keys are the critical element in all cryptographic systems

Proper key generation, management, and protection determine the security of encrypted data

Standards evolve to meet emerging security challenges

From Caesar cipher to AES, cryptographic algorithms continuously advance to protect against new threats

Questions for Students

1. What is cryptography, and why is it crucial for data protection in modern systems?
2. What are the main differences between symmetric and asymmetric encryption?
3. How does the encryption and decryption process work, and what is the role of cryptographic keys?
4. How does the RSA algorithm function, and what are its strengths and limitations?
5. What are the challenges associated with symmetric encryption and the sharing of encryption keys?

Recommended Literature

1. Stallings, W. Cryptography and Network Security: Principles and Practice. – Pearson, 2017.
2. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – Wiley, 2015.
3. Katz, J., Lindell, Y. Introduction to Modern Cryptography. – CRC Press, 2021.
4. Ferguson, N., Schneier, B., Kohno, T. Cryptography Engineering. – Wiley, 2010.
5. Menezes, A., van Oorschot, P., Vanstone, S. Handbook of Applied Cryptography. – CRC Press, 1996.