Cryptographic Information Protection: Securing Our Digital World

Why do I need cryptography?

Cryptography is essential for protecting your data during everyday digital interactions, such as online payments, email communication, and cloud services. The 'HTTPS' lock in your browser's address bar signifies cryptographic protection, without which the internet would be vulnerable to data interception.

Privacy

Ensuring only the authorised recipient can read a message.

Integrity

Detecting any alteration to data, no matter how small.

Authenticity

Verifying the message originates from the legitimate sender.

Symmetric Encryption: Speed and Shared Secrets

Symmetric encryption, the fastest method, uses a single shared secret key for both encryption and decryption. Imagine two identical safes with the same combination: you lock a message inside, send it, and the recipient opens it with their matching combination.

The main challenge is securely sharing this key. If an unauthorised party intercepts the key, the entire system is compromised.

Key Characteristics

- Uses a single key for encryption and decryption.
- Highly efficient for large volumes of data.
- Requires secure key exchange.

Real-world Applications

- Encrypting hard drives.
- Securing network transfers.

In practice, standards like GOST 28147-89 (Russia) and AES (Advanced Encryption Standard) in the West are widely used and considered robust. Their primary advantage is speed, allowing gigabytes of data to be encrypted in seconds.

Asymmetric Encryption: The Public–Private Key Revolution

The late 1970s brought a revolution: asymmetric encryption, utilising a pair of mathematically linked keys – one public and one private. The public key can be widely distributed, while the private key remains a closely guarded secret.

How It Works

Messages encrypted with the public key can only be decrypted by the corresponding private key holder, and vice versa.

Practical Scenario

To send a secret email, encrypt it with the recipient's public key. Only they, with their private key, can read it, even if intercepted.

Key Standards

GOST R 34.10-94 and GOST R 34.10-2001 (Russia).

RSA (named after Rivest, Shamir, Adleman) in the West.

While groundbreaking, asymmetric encryption is significantly slower (100 to 1,000 times) than symmetric methods. Therefore, it's typically not used for encrypting large files but is crucial for protecting keys and signing documents.

Hybrid Encryption: The Best of Both Worlds

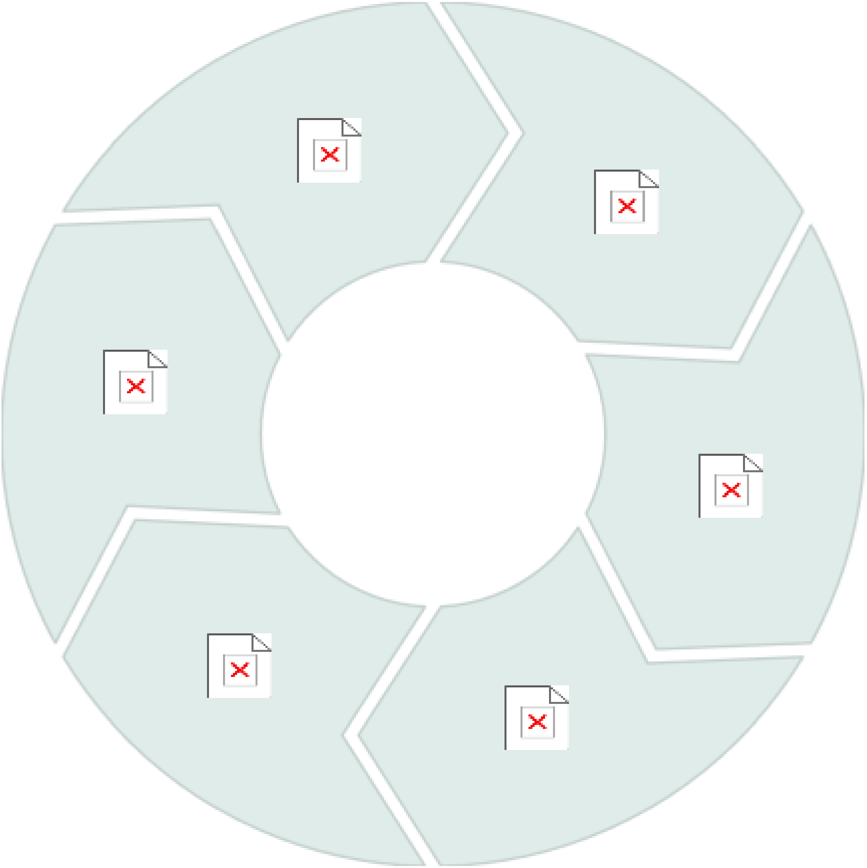
Hybrid encryption combines the speed of symmetric encryption with the convenience of asymmetric encryption, offering robust security for modern digital communications.

Generate Session Key

A random, one-time symmetric session key (128-256 bits) is created.

Encrypt Message

The entire message is encrypted quickly using the session key via a symmetric algorithm.



Encrypt Session Key

The session key itself is encrypted using the recipient's public asymmetric key.

Transmit Data

Both the encrypted message and the encrypted session key are sent.

Decrypt Session Key

The recipient decrypts the session key using their private key.

Decrypt Message

The recipient then uses the session key to decrypt the main message.

This approach is efficient even with multiple recipients: the message is encrypted once, and only the small session key is encrypted individually for each person. This is the foundation of HTTPS, PGP for emails, and VPN connections.

Electronic Digital Signature (EDS): Guaranteeing Integrity and Authenticity

An Electronic Digital Signature is a cryptographic calculation linked to a document, ensuring its integrity and authenticity. Unlike a scanned image, any change to the document, even a single character, will invalidate the signature, giving it the same legal force as a traditional signature.

Signing Process: Step 1

A unique "fingerprint" (hash) of the document is computed (e.g., using SHA-256).

Signing Process: Step 2

This fingerprint is encrypted with the author's private key, creating the EDS.

Signing Process: Step 3

Both the original document and the EDS are sent to the recipient.

Verification: Step 1

Recipient decrypts the EDS with the author's public key to retrieve the original fingerprint.

Verification: Step 2

Recipient independently calculates the fingerprint of the received document.

Verification: Step 3

If fingerprints match, the signature is authentic and the document is unaltered; otherwise, it's forged or changed.

The EDS does not encrypt the document, meaning its content remains open. For confidentiality, the document must be encrypted separately. EDS is widely used for legal and financial documents, such as contracts and tax reports.

Cryptographic Keys: The Foundation of Security

A cryptographic key is a sequence of random numbers or characters, with its strength measured by its length in bits (e.g., 128, 256, 2048). Longer keys offer greater resistance to brute-force attacks but come with slower encryption. Currently, 256 bits for symmetric and 2048 bits for asymmetric keys are considered secure.

Hardware Sensors

Generate keys based on physical processes like radioactive decay or thermal noise, offering the highest reliability.

Software Sensors

Collect entropy from system activities (keystrokes, mouse movements), providing faster but less reliable key generation.

Hybrid Approach

Combines both hardware and software methods for enhanced security and efficiency.

Private keys are always stored in encrypted form, protected by a password. Practical solutions often involve USB tokens, which are physical devices that securely store the private key and perform encryption operations internally. This prevents the key from ever leaving the token, even if stolen, as it remains password-protected.

Certificates and Public Key Infrastructure (PKI)

While public keys can be freely published, verifying their authenticity is crucial to prevent impersonation. This is where certificates come into play, providing a verifiable link between a public key and its owner.

A Certificate Contains:

- The owner's public key.
- Detailed owner information (name, organisation, email).
- Issue and validity dates.
- A unique serial number.

The electronic signature of a trusted Certification Authority (CA).

A CA is a trusted organisation that verifies the key owner's identity and then signs their certificate with its own EDS. Trusting the CA means trusting the certificate. This system forms a Chain of Trust (PKI), where certificates are signed by various authorities, leading up to a root certificate pre-installed in operating systems and browsers. Verification proceeds upwards through this chain, and any mismatch invalidates the entire certificate, ensuring robust security.

Key Compromise: Detection and Revocation

Key compromise occurs when a private key is exposed or suspected of being leaked. This can happen through malware, theft of physical tokens, employee misconduct, software vulnerabilities, or server breaches.

> ### The danger of a compromised key:
> Attackers can impersonate the key owner, decrypt sensitive information, or forge digital signatures, undermining the entire security framework.

Solution: Revocation and Renewal

Upon detection or suspicion, the certificate linked to the compromised key must be immediately revoked. The CA adds it to the Certificate Revocation List (CRL) or its modern alternative, OCSP (Online Certificate Status Protocol). Systems validating digital signatures and secure connections regularly check these lists. If a certificate is listed, all signatures made with its private key become invalid, and secure connections are blocked, preventing attackers from exploiting the leaked key.

Subsequently, the legitimate owner generates a new cryptographic key pair and obtains a new certificate, restoring secure operations.

Security Questions & References

Fundamental Differences

Symmetric vs. asymmetric encryption: speed, key usage, and why one is faster.

Usage Examples

Applications of symmetric (e.g., hard drives) and asymmetric (e.g., key protection).

Hybrid Encryption Explained

How it works, and why it's favoured over pure asymmetric methods.

EDS Guarantees

What an electronic digital signature ensures, and if it offers confidentiality.

Public Key Certificates

Their purpose, issuers, and contents.

Chain of Trust (PKI)

Its function in certificate verification.

Key Compromise

What happens when a private key is compromised and how it's revoked.

List of References

- GOST 28147-89. Information processing systems. The protection is cryptographic. Algorithm Cryptographic conversion algorithm.
- GOST R 34.10-2001. Information technology. Cryptographic protection of information. Processes of forming and verifying EDS.
- GOST R 34.11-94. Information technology. Cryptographic protection of information. Function Hashing function.
- Moldovyan A. A., Moldovyan N. A., Sovetov B. Ya. Cryptography: a textbook for universities. St. Petersburg: LanPubl., 2000.
- Partyka T. L., Popov I. I. Informatsionnaya bezopasnost': uchebnoe posobie [Information Security: a textbook]. Moscow: FORUM-INFRA-M, 2002.
- Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd Edition. Wiley, 1996.
- Galatenko V. A. Fundamentals of information security. Course of lectures, Moscow: INTUIT Publ., 2008.