Lesson 1
Cryptography and its applications

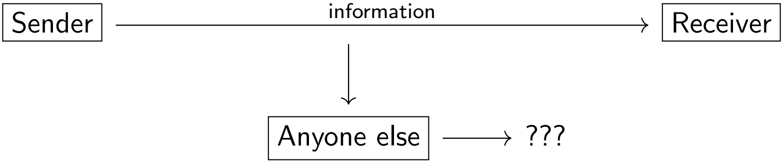
A. Sorokin (Input | Output)

Self paced course

July 29, 2025

What is cryptography?

Cryptography is a name given to encoding and transmitting information in a way that makes it difficult for someone to intercept and use.



Sender

information

Receiver

Anyone else

???

Secure transmission problem

Problem. How to transmit securely important information?

Solution. The answer breaks in two parts:

(i)) **encryption**: secure information by transforming it into an unreadable format;

(ii) **decryption**: only authorized parties can access the original information.

Secure communication

A communication is **secure** if a data transmission between parties satisfies:

(a) **confidentiality**: ensures that only the intended recipient can read the message;

(b) **integrity**: detects if data has been altered during transmission;

(c) **authentication**: verifies the identity of the sender/receiver;

(d) **non-repudiation**: prevents a sender from denying that they sent a message.

Cryptosystems

A secure communication between two parties is realized via two algorithms:

(i) **encryption** (or **encoding**): transforming a plain message into a ciphered one;

(ii) **decryption** (or **decoding**): back transforming a ciphered message into the original plain one.

These algorithms must satisfy the following property:

decryption of an encrypted message coincides with the message itself.

The above pair of algorithms is called a **cryptosystem**.

Effective operations

Not every cryptosystem is good for practical purposes due to limited resourses (such as time, memory, computation speed, etc.) An **effective operation** on data must

(i) use a reasonable amount of memory,

(ii) be performed in a reasonable time,

(iii) have a clear and easy software realization.

Effective cryptosystems

In an **effective cryptosystem**

(i) any sender encrypts a message effectively,

(ii) any receiver decrypts a received ciphered message effectively,

(iii) a communication is secure.

From now by a cryptosystem we'll always assume an effective one, as only such cryptosystems are used in practice.

Other applications of cryptography

Besides the secure communication between parties cryptosystems are used for

- storing (encrypted) data,
- signing documents,
- sharing secrets,
- proving ownership

and many other things. A brief list of cryptography purposes and real life examples is in the following slides.

Key purposes and applications of cryptography

Purpose	**Cryptographic tools**	**Use cases**
Secure communication	TLS/SSL, End-to-end encryption	Emails, VPNs, HTTPS, encrypted messaging, online banking
Data integrity	Hash functions, digital signatures	File verification, blockchain, legal documents
Identity verification	Public-key certificates, ZKPs	SSH logins, anonymous credentials

Key purposes and applications of cryptography

Purpose	**Cryptographic tools**	**Use cases**
Secure storage	Symmetric encryption, password hashing	Encrypted databases
Decentralization, digital cash	Blockchain, smart contracts, tokens	File verification, blockchain, NFTs, legal documents
Privacy-preserving computations	Homomorphic encryption, secure multi-party computations	Voting systems, medical data

Key purposes and applications of cryptography

Purpose	Cryptographic tools	Use cases
Anonymity	Onion routing, mixing networks	Whistleblowing, bypassing internet censorship
Provable fairness	Commitment schemes, verifiable random functions	Online gaming, randomized public elections
Secure hardware, supply chains	Trusted platform modules, physically unclonable fucntions	Biometric data protection, hardware authentication
Legal and compliance	Compliant anonymization	Financial regulations, healthcare