

Security in Computer Networks (1/7)

1

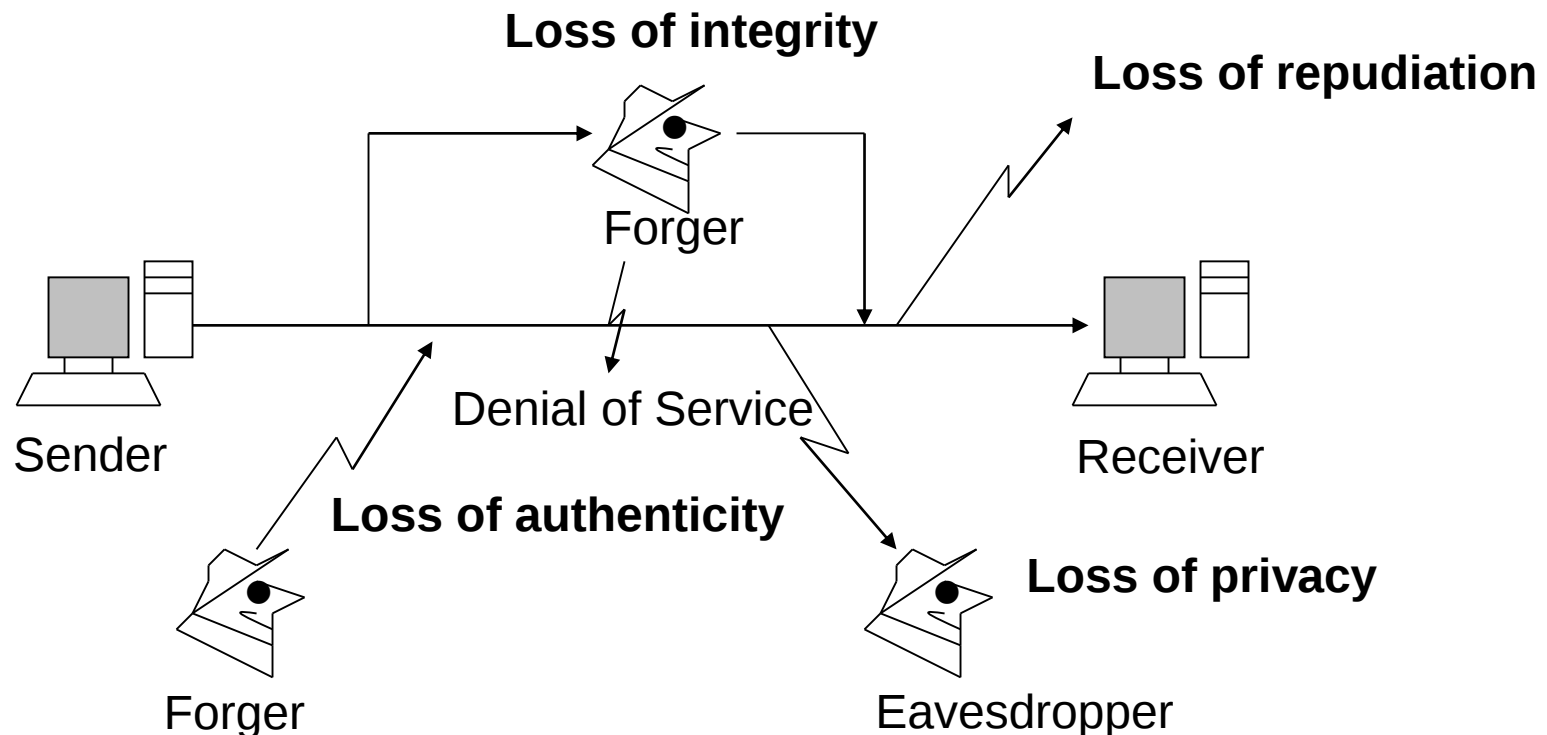
Various aspects of security play an essential or decisive role in the use of computer networks

- **Closed networks** are autonomous island networks. They cannot be accessed from the outside without gaining physical entrance
- **Open networks** have access to the worldwide Internet, thus access can be gained from the outside
 - Open networks are exposed to a large number of threats

Security in Computer Networks (2/7)

2

Different threats to communication networks:



Security in Computer Networks (3/7)

3

An analysis of the types of threats has resulted in the formulation of security goals:

- **Privacy**

- Threats e.g. from eavesdropping

- **Authenticity**

- Threats e.g. from the pretense of a false sender ("spoofing")

- **Integrity**

- Threats e.g. from data falsification during transmission

- **Non-Repudiation**

- Non-legally binding data transmission

- **Availability**

- Threats e.g. from a targeted overload ("denial of service")

Security in Computer Networks (4/7)

4

A distinction is made between

- **Active attacks**

- Attacker falsifies contents, manipulates authenticity, overloads network services, etc.

- **Passive attacks**

- Attacker eavesdrops on communication, spies on the network, records communication, ...

Active attackers are easier to detect than passive ones...

Security in Computer Networks (5/7)

5

Cryptography provides tools for secure communication in open networks and the Internet

Cryptography is a mathematical science for the

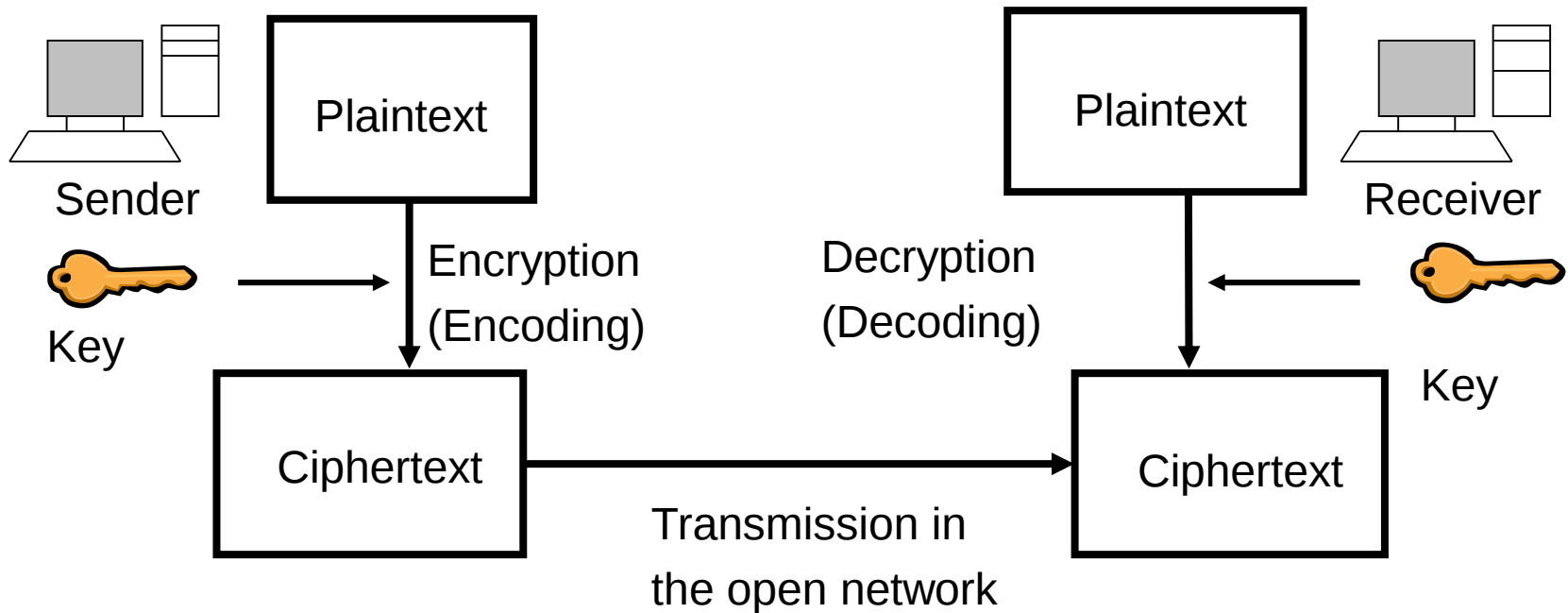
- Encryption of clear text ("plaintext")
 - Conversion ("enciphering") into "cipher text"
- Decryption of cipher text into plaintext

Encryption method/cipher is mapping used together with secret information - the "key" - selected from an astronomical amount of similar information

Security in Computer Networks (6/7)

6

Secure communication with cryptography:



Security in Computer Networks (7/7)

7

- The system for encryption and decryption - “**cryptosystem**” - is made up of
 - a cipher (encryption method)
 - a secret key
 - a decryption method
- **Cryptocomplexity** – the effort necessary for encryption and decryption
- In traditional **symmetric** or **secret key cryptosystems** the sender and receiver both use the same secret key
- In modern **asymmetric** or **public key cryptosystems** different keys are used for decryption and encryption