0. Introduction

Security is freedom from, or resilience against, potential harm caused by others; (different from **Safety**: prevents from unintentional accidents.)

- **Physical security**: guy that check entrance
- **Logical security**: sw safeguards (subset of pc security)

Computer security (cybersecurity) refers to security of devices and networks.

Cryptography provides building blocks for Cybersecurity.

Cryptology: it can be divided into:

1. **Cryptography:** techniques for secure communications
2. **Cryptoanalysis:** study of cryptosystems

building blocks: milestones for other topics, in this case to offer Security Services:

- Confidentiality: info kept secret (ciphers are designed to offer this)
- Data Integrity: info not tampered while in transit (not altered, hash functions ensure this)
- Availability: info reliably available to the end users (prevent attack that can affect availability, firewalls help)
- Message authentication: sender is authentic (also includes integrity of the message, use of: message authentication code, digital signature, AE)
- Entity Authentication: verify identity of an entity (passwords are one common way; single vs multi-factor auth (e.g. 2FA))
- Non Repudiation: sender cannot deny the creation of the message.

Adversary model

- Passive (pack sniffing): reads all messages
- Active (ip spoofing): forge messages, create requests —> DoS, DDoS (e.g. syn packets)

Assume adversary knows algorithms, protocols, message and key space

Adversary doesn't know secret keys

Kerckhoffs' principle:

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.

very hard to prove a scheme is secure; just try to hack it.

Attack models

- **Eavesdropping**: secretly listening to private conversation of others without their consent

- **Known plaintext:** has szamples of both plaintey and its encrypted version and can use them
- **Chosen plaintext:** attacker has the capability to choose arbitray plaintexts; goal: gain info o reduce security of the scheme; could reveal sectey key
- **Adaptive chosen plaintext:** makes a series of interactive queries
- **Chosen cybertext:** cryptoanalyst gathers info by choosing a cyphertext
- **Physical access**

Common attacks

- **Replay:** valid data transmission maliciously replayed
- **Reflection:** some protocols are based on challenge-response auth; attempts to trick an entity into proving the right answer to its own challenge
- **Man in the middle: attacker** relays and alters communication between two parties

Security goals

if secret keys are unknown to the adversary, it should be hard (unfeasible to compute, 2^64 is feasible, 2^80 unfeasible) to retrieve information on the message m and retrieve keys.