Lezione 1

Security definition and properties

Protecting information, either on a standalone system or on a network.
To consider a system secure it must have the following properties:

- **Authenticity**
  A general entity should be correctly identified. (e.g., User login guarantees authenticity as long as its credentials are not leaked somewhere.)
- **Confidentiality**
  Any information should only be accessible to whoever has authorization, not anyone. (e.g., Data confidentiality means that confidential information, such as personal information, should not be disclosed to unauthorized entities.)
  A way of protecting confidentiality is **Access control**.
- **Integrity**
  Information should only be modified by whoever has authorization.
  Integrity is not a binary measurement (you either have it or not), but depends on the context. As an example, let's assume a quote from a politician.
  Data integrity means that the quote will not be modified in any way but does not necessarily guarantee that the person who made the quote will be the same. This is ensured with **origin integrity**.
- **Availability**
  Information should only be available (or usable) to authorized users.
  When ensuring availability, those properties should be ensured:
  - Timely request response (reasonable time to respond to a request).
  - Fair allocation of resources.
  - Fault tolerance.
  - Easy to use in the intended way.
  - Controlled concurrency (thread management, deadlock control, starvation control, etc.)
- **Non-repudiation**
  An entity should not be able to deny an event. (e.g., PEC email messages are non-repudiable.)

Type of attacks

Note: Add images from slides
When information is sent, it's usually expected to go from a source to a destination.
However, an attacker can try to manipulate the flow in different ways, such as:

- **Interruption**
  The attacker will stop the flow of information.
  Properties gone: Availability and possibly integrity (you only receive part of the message).
- **Eavesdropping**
  The attacker sees the flow of information.
  Properties gone: Confidentiality.
  It's not easy to notice an eavesdropping attack.
- **Modification**
  The attacker intercepts the flow of information and modifies it however they please.
  Properties gone: Integrity (and possibly confidentiality).
- **Forging**
  The attacker introduces new information not coming from the source.
  Properties gone: Authenticity, Accountability, Integrity.

Passive vs Active attacks

- **Passive attacks**
  Eavesdropping, ...
- **Active attacks**
  Interruption, forgery, modification.

Cryptography

A way of protecting information when the environment is insecure. How can we do that?

- **Encryption**
  Transforming a plain text message using some rules (encryption algorithm) into a cipher text.
  You usually either hide the algorithm, and only the sender and receiver understand the algorithm. This works as long as nobody else knows the algorithm (security by obscurity).
  A common way of encrypting messages nowadays is the following:
  The encryption algorithm is public, and the sender and receiver share privately some information, mainly the encryption key that is not accessible to anybody else. If an attacker knows the key, the sender and receiver only have to change the key, not the whole algorithm.
- **Decryption**
  Starting from the cipher text, the original plain text is reconstructed. This passage

has to be easy (fast and efficient) for the receiver but computationally impossible (unfeasible) for a generic attacker.

Examples of encryption algorithms

Caesar Cipher

Every letter is permuted with a certain rule.
To encrypt a message with the Caesar Cipher you must first decide a key K, for example $K = 3$ this means that each letter will be mappeed to the corresponding K successive letter (in modulo): eg. $A \to D$ $Z \to C$.
To decipher, you do the same thing but in reverse (subtraction in modulo).