Cybersecurity

Alessio Marini, 2122855

Appunti presi durante il corso di **Cybersecurity** nell'anno **2025/2026** del professore Angelo Spognardi.
Gli appunti li scrivo principalmente per rendere il corso più comprensibile **a me** e anche per imparare il linguaggio Typst. Se li usate per studiare verificate sempre le informazioni 🙏🏻.

Contatti:

alem1105

marini.2122855@studenti.uniroma1.it

September 27, 2025

Indice

1. Definition of Cybersecurity

Definition by NIST (National Institute of Standards and Technology)

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

1.1. A definition of Computer Security

Computer Security: Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system **assets** including hardware, software, firm-ware, and information being processed, stored, and communicated.

An asset is something important for the system.

1.2. Assets

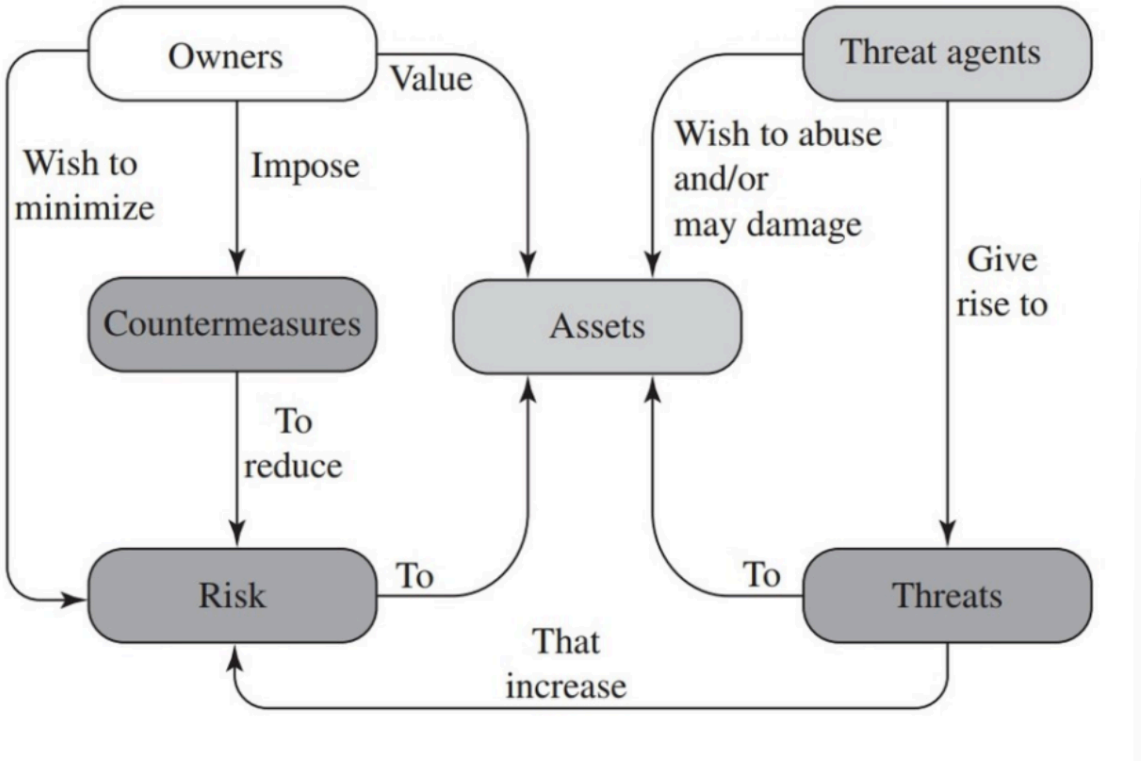
The asset is a key concept, the assets are important for a person or a company and need to be protected.

Some examples:
- Patient records
- Equipment
- Keys for net-banking

What should be protected?

- **Personal Data** of users like name, surname, email ecc...
- **Company Data** like financial data, internal information about products or personal data of the customers, partners ecc...

1.3. Security Concepts and Relationships



1.4. Threat Agent (Adversary)

Who conducts or has the intent ro conduct detrimental activities.

1.5. Countermeasure

A device or technique that ha as its objective the impairment adversarial activity.

1.6. Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event.

1.7. Threat

Any circumstance or event with the potential to adversely impact organizational operations.

1.8. Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Observation about Security

The security of a system, application or protocol is relative to:

- A set of desidere properties
- An adversary with specific capabilities

For example the file access permissions in Linux or Windows are not effective against someone who can boot from a CD or USB drive.

1.9. Threats

There are different type of threats.

- **Active Attack**: An attempt to alter system resources or affect their operation. Some example:
  - Replay
  - Masquerade
  - Modification on Messages
  - Denial of Service
- **Passive Attack**: An attempt to learn or make use of information from the system that does not affect

system resources. For example an adversary could steal some information for use them in the future in a new attack.

- **Inside Attack**: Initiated by an entity inside the security perimeter (an "insider"). The insider is

authorized to access system resources but uses them in a way not approved by those who granted the authorization.

- **Outside Attack**: Initiated from outside the perimeter, by an unauthorized or ille-gitimate user of the

system (an "outsider"). On the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

2. Security Goals

There are 3 foundamental concepts in security, **C.I.A.**:

- **Confidentiality**
- **Integrity**
- **Availability**

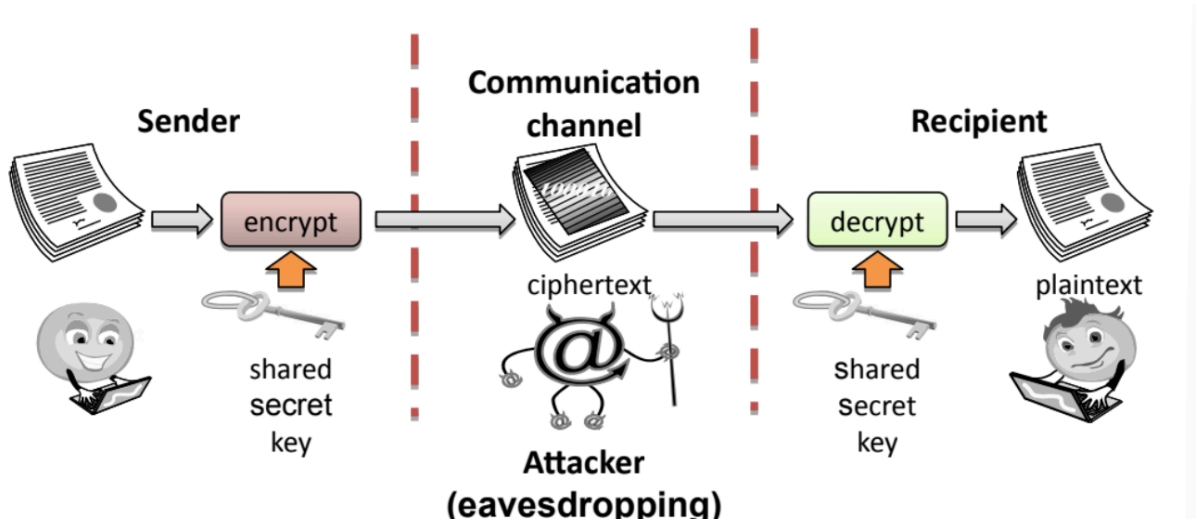
2.1. Confidentiality

The avoidance of the unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it while disallowing others.

Let's look some **tools for confidentiality**

2.1.1. Encryption

The transformation of information using a secret, called an **encryption key**, so that the transformed information can only be read using another secret, called the **decryption key** (which may, in some cases, be the same as the encryption key).



2.1.2. Access Control

Rules and policies that limit access to confidential information to those people and/or systems with a "need to know."

For example we can grant this «need to know» with a device, a password, a role ecc...

2.1.3. Authentication

The determination of the identity or role that someone has. This determination can be done in a number of different ways:

- An object
- A password
- Fingerprint

2.1.4. Authorization

The determination if a person or system is allowed access to resources, based on an **access control policy**.

2.1.5. Physical Security

The establishment of physical barriers to limit access to protected computational resources.

2.2. Integrity

The property that something has not be altered in an unauthorized way. Some tools for integrity:

- **Backups**: Periodic archiving of data.
- **Checksums**: The computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
- **Data correcting codes**: Methods for storing data in such a way that small changes can be easily detected and automatically corrected.

2.3. Availability

The property that something is accessible and modifiable in a timely fashion by those authorized to do so.

Some tools for the availability:
- **Physical Protections**: Infrastructure meant to keep information available

even in the event of physical challenges.
- **Computational redundancies**: Computers and storage devices that serve as

fallbacks in the case of failures.

2.4. Other Security Concepts

Some other important concepts are **Authenticity, Accountability e Anonymity**.

2.4.1. Authenticity

Is the ability to determine that statements, policies, and permissions issued by persons or systems are genuine.

An example of tool for authenticity could be **digital signature**

2.4.2. Accountability

Is the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

The system must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

This goal supports non-repudiation, intrusion detection, recovery, legal action and other security concepts.

2.4.3. Anonymity

The property that certain records or transactions not to be attributable to any individual. Some useful tools:

- Aggregation: The combining of data from many individuals.
- Mixing: The interwining of transactions, information or communications in a way that cannot be traced to any individual.
- Proxies: Trusted agents that are willing to engage in actions for an individual in a way that cannot be traced back to that person.
- Pseudonyms: Fictional identities that can fill in for real identities in communications and transactions but are known only by trusted identity.

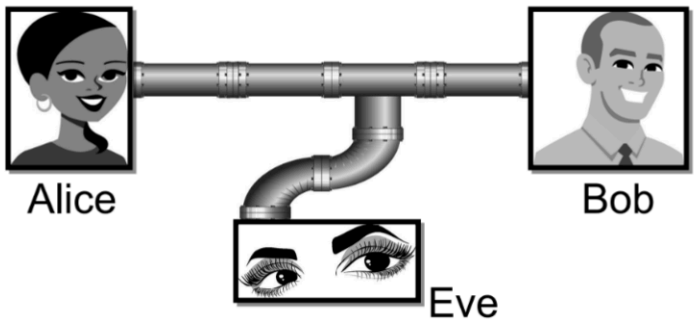
2.5. Threat Consequences

2.5.1. Unauthorized Disclosure

This is a threat to confidentialy. Is a circumstance or event where an entity gains access to data for which the entity is not authorized.

In this event can occurs:

- Exposure: Sensitive data are directly released to an unauthorized entity.
- Interception: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.



- Inference: A threat action where an unauthorized entity indirectly accesses sensitive data by reasoning from characteristics or by-products of communications.

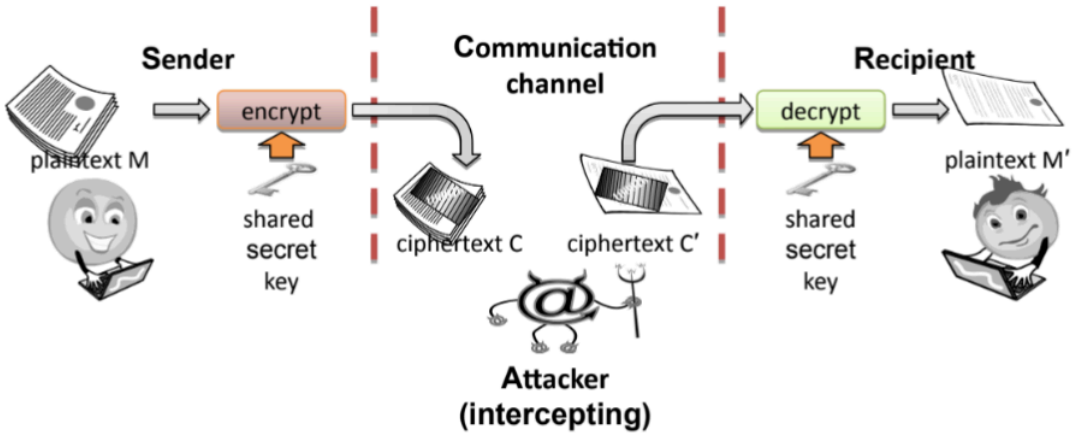
Inference is also called **correlation or traceback**, is the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information.

- Intrusion: An unauthorized entity gains access to sensitive data by circumventing a system's security protection.

2.5.2. Deception

Is a threat to system integrity and data integrity. An authorized entity receive false data and believe it to be true.

Some type of attack:
- Masquerade: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.
- Falsification: False data deceive an authorized entity. For example the **man-in-the-middle attack** where a network stream is intercepted, modified and retransmitted.



- Repudiation: An entity deceives another by falsely denying responsability for an act.

2.5.3. Disruption

Is a threat to availability or system integrity. An event that interrupts or prevents the correct operation of system services.

Some example:

- Incapacitation: Prevents or interrupts system operation by disabling a system component.
- Corruption: Undesirably alters system operation by adversely modifying system functions or data.
- Obstruction: A threat action that interrupts delivery of system services by hindering system operation.
- **Denial-of-service**: The obstruction or degradation of a data service or information access. For example email spam.

2.5.4. Usurpation

Is a threat to system integrity. An event that results in control of system services by an uauthorized entity.

- Misappropriation: An entity assumes unauthorized logical or physical control of a system resource.
- Misuse: Causes a system component to perform a function or service that is detrimental to system security.

Example

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted USB drive is stolen.	
Software	Programs are deleted, denying access to users.		
Data		An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks			Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

3. Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system.

Examples:

- Open ports on outward facing Web and others servers, nad code listening on those ports
- Services available on the inside of a firewall.
- Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats.
- Interfaces, SQL, Web Forms.
- An employee with access to sensitive information vulnerable to a social engineering attack.

3.1. Attack Surface Categories

Network Attack Surface

Vulnerabilities over an enterprise network, wide-area network or the Internet. This also include network protocol vulnerabilities.

Software Attack Surface

Vulnerabilities in application, utility, or operating system code, with particular focus on Web Server Software.

Human Attack Surface

Vulnerabilities created by personnel or outsiders with social engineering, human error or trusted insiders.

4. Computer Security Strategy

- **Security Policy**: Formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
- **Security Implementation**: Involves four complementary courses of action:
  - Prevention
  - Detection
  - Response
  - Recovery
- **Assurance**: Encompassing both system design and system implementation, assurance is an attribute of an information system that provides grounds for having confidence that the system operates such taht the system's security policy is enforced.
- **Evaluation**: Process of examining a computer product or system with respect to certain criteria. It also involves testing and may also involve formal analytic or mathematical techniques.

5. Standards

Standards have been developed to cover management practices and the overall architecture of security mechanisms and services. The most important are:

- **National Institute of Standards and Technology (NIST)**: A U.S. Federal Agency that deals with measurement science, standards, and technology.
- **Internet Society (ISOC)**: A professional membership society that provides leadership in addressing issues that confront the future of the internet.
- **International Telecommunication Union (ITU-T)**: ITU is a United Nations agency in which governments and the private sector coordinate global telecom networkds and services.
- **Internetional Organization for Standardization (ISO)**: ISO is a nongovernmental organizaton whose work results in international agreements that are published as International Standards.

6. Economy of Mechanism

This principle stresses simplicity in the design and implementation of security measures.

The notion of simplicity is especially important in the security domain, since a simple security framework facilitates its understanding by developers and users and enables the efficient development and verification of enforcement methods for it.

6.1. Fail-Safe defaults

This principle states that the defualt configuratoin of a system should have a **conservative protection scheme**. For example when adding a new user to an operating system the default group of the user should have minimal access rights. Unfortunately, operating systems and applications often have default options that favor usability over security.

6.2. Complete Mediation

The idea behind this principle is that every access to a resource must be checked for compliance with a protection scheme.

6.3. Open Design

The security architecture and design of a system should be made publicly available.

- Keeping cryptographic keys secret
- Open design allows for a system to be scrutinized by multiple parties.
- The open design principle is the opposite of the approach knows as security by obscurity, which tries to achieve security by keeping cryptographic algorithms secret and which has been historically used without success by several organizations.

6.4. Separation of Privilige

This principle dictates that multiple conditions should be required to achieve access to restricted resources or have a program perfrom some action.

6.5. Least Privilege

Each program and user of a computer system should operate with the bare minimum privileges necessary to function properly.

6.6. Least common mechanism

In systems with multiple users, mechanism allowing resources to be shared by more than one user should be minimized.

6.7. Psychological Acceptability

This principle states that user interfaces should be well designed and intuitive, and all security-related settings should adhere to what an ordinary user might expect.

6.8. Work Factor

According to this principle, the cost of circumventing a security mechanism should be compared with the resources of an attacker when designing a security scheme. For example a system developed to protect student grades which may be attacked by snoopers or students

trying to change theri grades, probably needs less sophisticated security measures than a system built to protect military secrets.

6.9. Compromise Recording

This principle states that sometimes it is more desirable to record the details of an intrusion than to adopt more sophisticated measures to prevent it.

7. Crypto Concepts

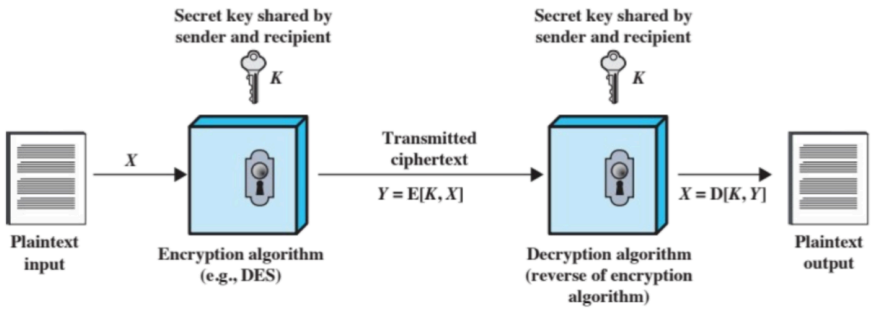
7.1. Symmetric encryption

The universal technique for providing confidentiality for transmitted or stored data, it uses a single-key encryption.

Two requirements for secure use:

- Need a strong encryption algorithm
- Sender and receiver must have obtained copies of the secret key in a secure way and must keep the key secure.

Simplified model of symmetric encryption



7.1.1. Attacking Symmetric Encryption

There two main type of attacks:

- **Cryptanalytic Attack**: They rely on the **nature of the algorithm**, some knowledge of the general characteristics of the plaintext, some sample plaintext-ciphertext pairs. Ususally the exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used.
- **Brute-Force Attacks**: Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained.

Bruteforcing Modern Block Ciphers

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$2! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

7.1.2. Symmetric Encryption Algorithms

- **AES**: Advanced Encryption Standard (Rijndael)
  - 128 bit lock cipher

    - 128, 192 or 256 bit secret keys
- **DES**: Data Encryption Standard (now insecure)
    - 64 bit locker cipher
    - 56 bit secret key
    - 3DES (Triple-DES), variant with secret of 112 or 168 bits. (It repeat the basic DES three times)

  It was the most studied encryption algorithm in existence but the speed of commercial processors makes the 56bit key woefully inadequate
- **RC4** (now insecure, also known as ARC4 or ARCFOUR)
    - Stream cipher
    - 40-2048 bits secret keys

7.2. Practical Security Issues

Typically symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block. **ECB (Electronic codebook)** is the simplest approach to multiple-block encryption:
- Each block of plaintext is encrypted using the same key
- Cryptanalysts may be able to exploit regularities in the plaintext

Alternatives techniques developed to increse the security of symmetric block encryption for large sequences.

7.2.1. Block vs Stream Ciphers

- **Block Cipher**: Processes the input one block of elements at a time and produces an output block for each input block.
- **Stream Cipher**: Processes the input continuously and produces output one element at a time. They are almost always faster and use far less code. Pseudorandom stream is one that is unpredictable without knowledge of the input key.

7.3. Message Authentication

Protects against active attacks by verifing that received messages are authentic:
- Contents have not been altered
- From authentic source
- Timely and in correct sequence

It can use concentional encryption where only sender and receiver share a key.

Message Authentication Without Confidentiality

Message encryption by itself does not provide a secure form of authentication but we can combine authentication and confidentiality in a single algorithm:
- Encryption + Authentication Tag

7.3.1. Message Authentication Code (MAC)

A number of algorithms could be used to generate the code, however, authentication algorithm need not be reversible.

When we send a message we generate and send a MAC tag, the receiver need to calculate the MAC tag from the message and if the two tags are the same means that the message is arrived with integrity.

The MAC function takes in input a shared secret key within the message.

7.3.2. Cryptographic hash function

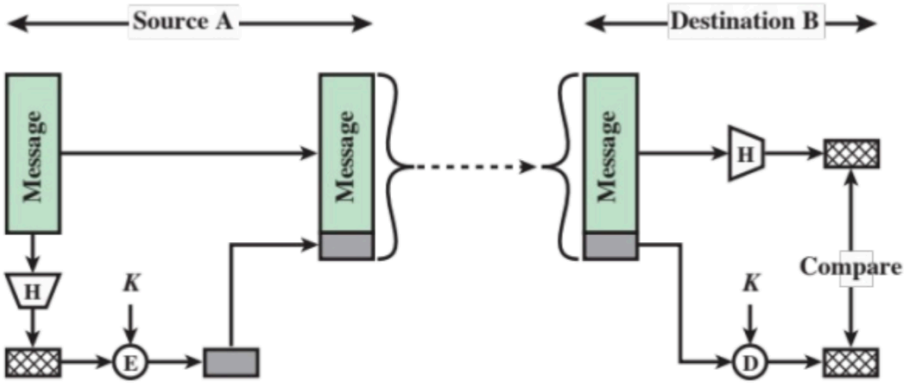
The purpose of a hash function is to produce a «fingerprint» of a file, message or other block of data. It generates a set of k bits from a set of $L(\geq k)$ bits.

The result of applying a hash function is called **hash value**, or message digest, or checksum.

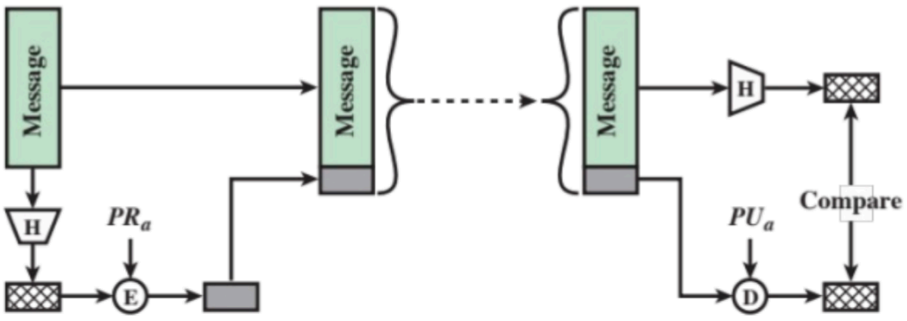
7.3.3. MAC with one-way hash functions

As we said, unline the MAC an hash function does not take a secret key as input but just the plain text (or file). However it is possibile to get MACs using hash functions.

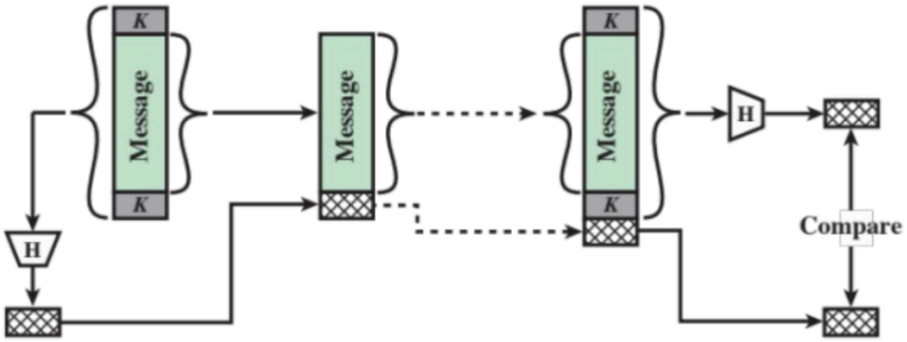
Some methods:



(a) Using symmetric encryption



(b) Using public-key encryption



(c) Using secret value

The public-key approach advantages:

- It provides a digital signature as well as message authentication
- It does not require the distribution of keys to communicating parties.ù

Properties for a good hash function

- Can be applied to a block of data of any size
- Produces a fixed-length output
- H(x) is relatively easy to compute for any given x
- One-way or pre-image resistant, computationally infeasible to find x such that H(x)=h
- Computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$
- Collision resistant or strong collision resistance, computationally infeasible to find any pair (x, y) such that $H(X) = H(y)$

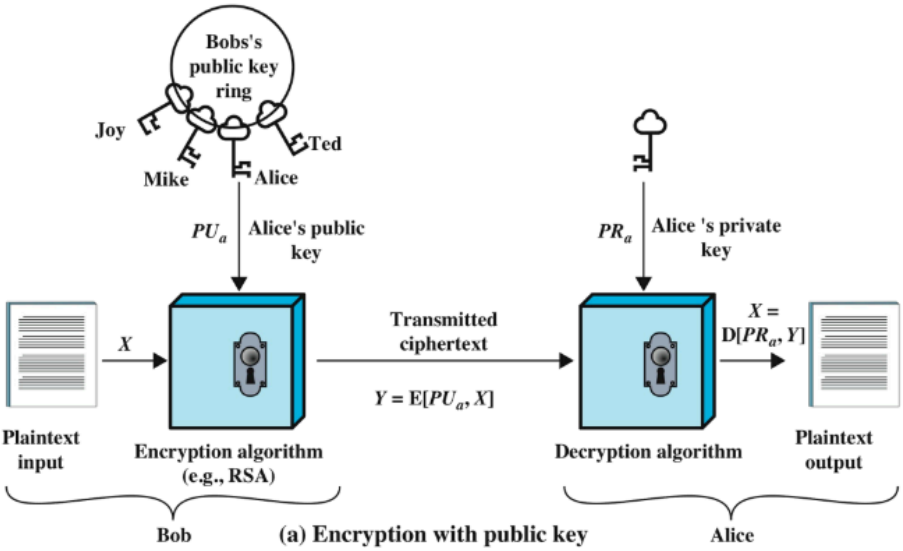
There are two approaches to attacking a secure hash function:

- Exploit logical weaknesses in the algorithm
- Strength of hash function depends solely on the length of the hash code produced by the algorithm

The SHA is the most widely used hash algorithm.

8. Public-Key Encryption Structure

This is based on mathematical functions, it's asymmetric so it uses two separate keys, the public keys and the private keys.



It works with pair of public and private key, you need to encrypt a message with a public key and only the people with the matching private key can decrypt the message. Everyone can see us encrypting a message with a public key but the important thing is that the private key remains secret.

We can classify the use of public-key cryptosystems into three categories:

- Digital signature
- Symmetric key distribution
- Encryption of secret keys

Requirements for Public-Key Cryptosystems

- Computationally easy to create key pairs
- Computationally easy for sender knonwing public key to encrypt messages
- Computationally easy for receiver knowing private key to decrypt ciphertext
- Computationally infeasible for opponent to determine private key from public key
- Computationally infeasible for opponent to otherwise recover original message
- Useful if either key can be used for each role

There different asymmetric encryption algorithms:

- **RSA (Rivest, Shamir, Adleman):** Most widely accepted and implemented approach to public-key encryption. Block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.
- **Diffie-Hellman key exchange algorithm**: Enables two parties to securely reach agreement about a shared secret for subsequent symmetric encryption of messages. Limited to exchange of the keys.

- **Digital Signature Standard (DSS)**: Provides only a digital signature function with SHA-1, cannot be used for encryption or key exchange.
- **Elliptic curve cryptography (ECC)**: Security like RSA, but with much smaller keys.

The NIST FIPS PUB 186-4 defines a digital signature as:

"The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation."