

University Mohamed Khider of Biskra
Computer Science Department



CYBERSECURITY COURSES

LEVEL: 3RD YEAR LICENSE

Teacher : Dr. Somia Sahraoui



Outline

1. Introduction and generalities
2. Introduction to cryptography
3. Public key infrastructure

Introduction and generalities about Cyber-security

Introduction & generalities

➔ Terminology related to cybersecurity (1)

❖ Vulnerability:

Any weakness or flaw in information systems/communication networks is a vulnerability in cyber security. Cybercriminals and Hackers may target these vulnerabilities and exploit them to attack the system/network.

■ Examples of vulnerabilities :

- Missing data encryption.
- Unrestricted upload of dangerous files.
- Using broken algorithms.
- Weak and unchanged passwords.
- URL Redirection to untrustworthy websites.
- Website without SSL.

Introduction & generalities

➔ Terminology related to cybersecurity (2)

- ❖ **Risk** : the probability of exposure or loss resulting from a cyber attack or data breach in a system/network. A better, more encompassing definition is the potential loss or harm related to the exploitation of existing vulnerabilities.
 - *The more vulnerabilities a system or network has, the greater potential for threats and the higher risk we will have and vice versa.*
- ❖ **Threat/Attack**: refers to any possible malicious action that seeks to unlawfully damage, access data or disrupt digital operations. Cyber threats can originate from various actors, including terrorist groups, hostile persons, criminal organizations, hackers and even dishonest employees.
 - *Examples of attacks: Malware, Denial of Service (DoS), Man in the middle, spying, etc.*

Introduction & generalities

➔ Terminology related to cyber-security (3)

- ❖ **Attacker** = Adversary = Intruder = Hacker = Cybercriminal
- ❖ **Target** = Victim
- ❖ **Legitimate entity** ≠ (Attacker & Target)
- ❖ **Countermeasure** : any security solution or defense strategy that aims to protect the system against cyber-attacks. Counter measures can be preventive or detective.

Introduction & generalities

→ Objectives of cybersecurity

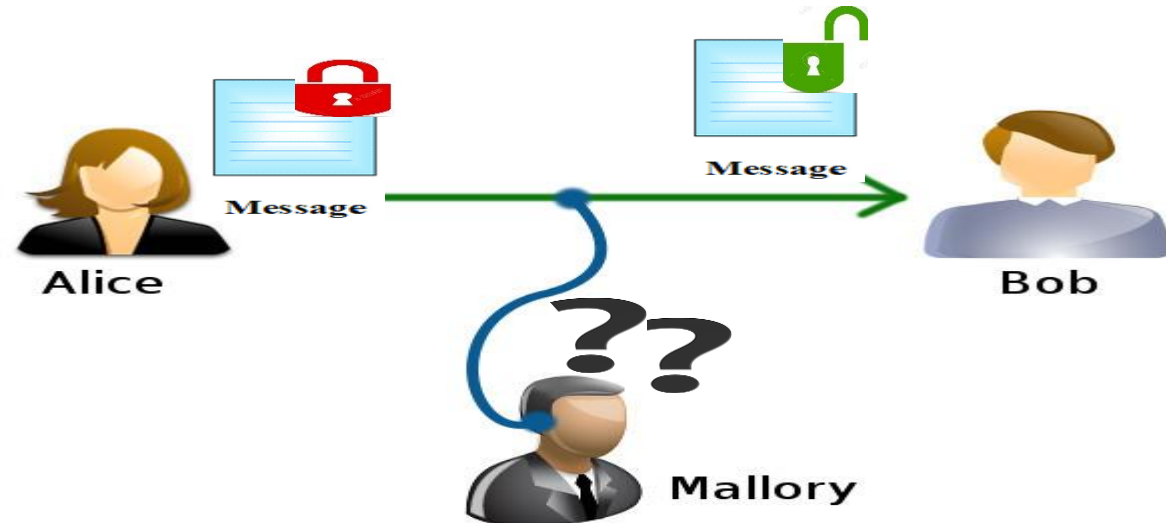
1. Confidentiality
2. Authentication
3. Non repudiation
4. Integrity
5. Access control
6. Availability

Introduction & generalities

→ Objectives of cyber-security (1)

■ Confidentiality

Confidentiality ensures that only authorized entities can access the information, while preventing others from discovering anything about its contents. It ensures that vital information does not reach the wrong people while also ensuring that the appropriate ones receive it. Data encryption is a wonderful example of how to keep information private.



Introduction & generalities

→ Objectives of cyber-security (2)

■ Authentication

- An authentication procedure is one that ensures and confirms a user's identity or role. Authentication is a must for all companies because it allows them to safeguard their networks by allowing only authenticated users to access protected information.
- In the context of communications, authentication refers to any mechanism that checks the validity of the pretended source of information / data messages.
- It can be ensured by means of digital signatures, Message authentication codes (MACs), digital fingerprint

Introduction & generalities

→ Objectives of cyber-security (3)

■ Non-repudiation:

It refers to a situation where someone cannot deny the validity of something. In the context of communications, a sender of an authenticated message cannot thereafter deny the act of having sent that message.

- It is usually guaranteed by strong authentication tools like digital signatures

■ Integrity

The means for guaranteeing that data is real, correct, and protected against unauthorized modification/alteration is referred to as integrity. It is a property that information has not been tampered with in any manner and that the information's source is legitimate.

- It can be ensured by tools like: Hash functions and checksums.

Introduction & generalities

→ Objectives of cyber-security (4)

■ Access control

Access control refers to the set of rules and procedures that govern who has access to a system or to physical or virtual resources. It is the process of granting users access to systems, resources, or information, as well as particular privileges.

Users of access control systems must present credentials such as a person's name, passwords, digital fingerprint, or a computer's serial number before granting access.

These credentials can take numerous forms in physical systems, but credentials that cannot be transferred provide the best security.

Introduction & generalities

→ Objectives of cyber-security (5)

■ Availability

Availability is the property of being able to access and modify information in a timely manner by those who are allowed to do so. It ensures that only authorized personnel have access to the sensitive data on a consistent and dependable basis. The availability principle is operated by employing the following tools:

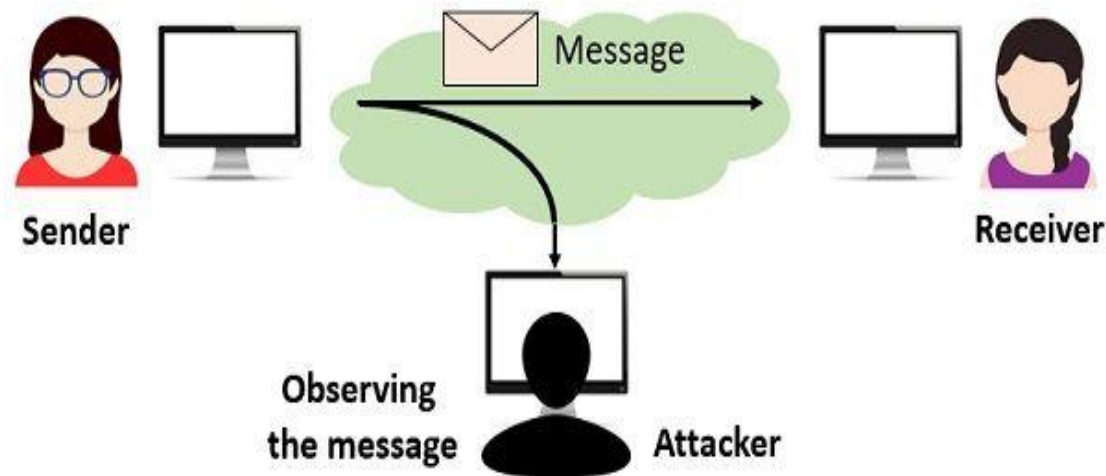
- **Physical Protection:** the ability to keep information accessible even when faced with physical difficulties. It ensures that sensitive data and important information technologies are kept in safe places.
- **Computational Redundancy:** used as a fault-tolerant system against intentional and unintentional failures.

Introduction & generalities

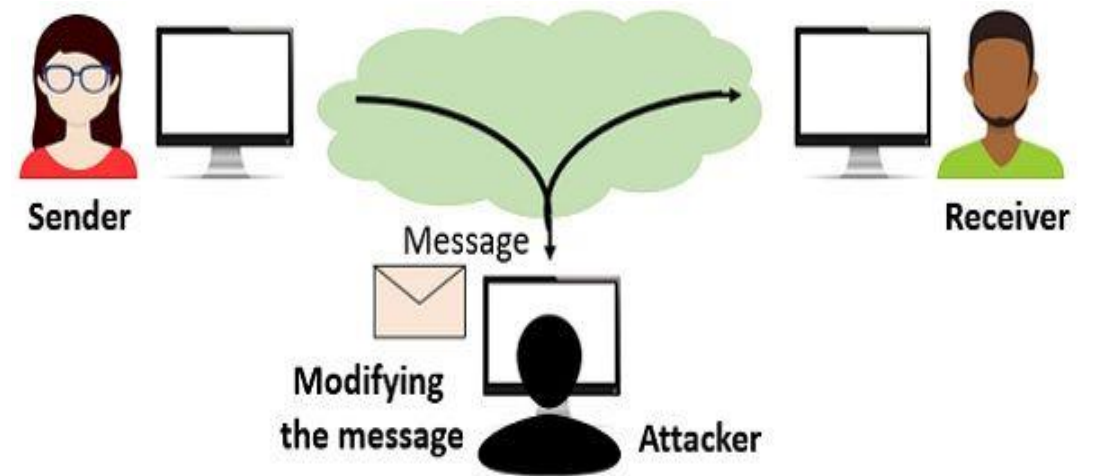
→ **Classes of attacks** : There are several classes of cyber-attacks

■ Passive vs Active attacks

In passive attacks, adversaries just attempt to analyze, capture network traffic (exchanged messages), spy on communications without changing or subverting anything. Whereas, in an active attacks, the adversary performs malicious actions that cause damage, negative changing in communications, system resources or databases.



Passive Attack



Active Attack

Introduction & generalities

→ Classes of attacks

■ Random vs deterministic attacks

In random attacks the behavior of attackers is random; malicious actions can be of any type and they are launched at anytime. However, in deterministic attacks every action is performed at specific and well determined timing /phase.

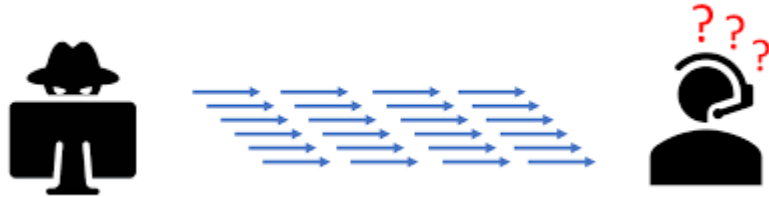
■ Centralized vs distributed attacks

In centralized attacks, attacks are originated from one centralized source. Distributed attacks are launched by a group of adversaries that are generally supervised by one hidden attacker.

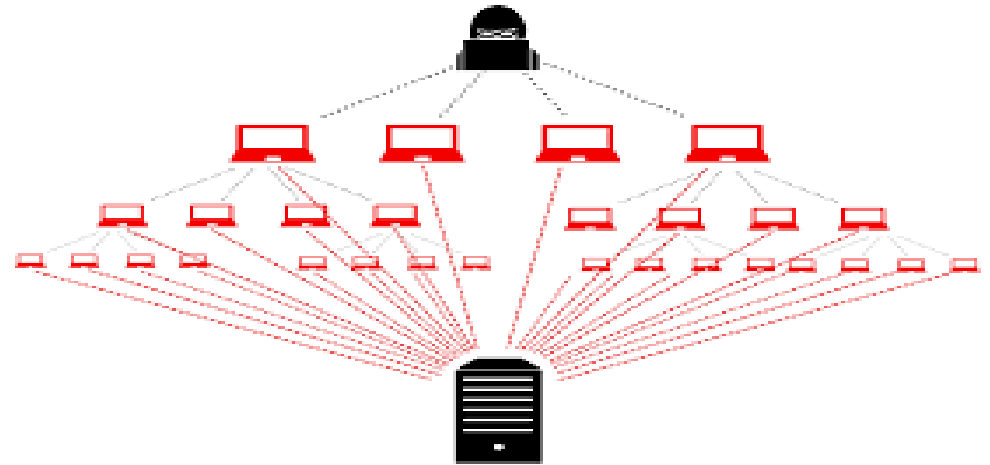
Introduction & generalities

→ Classes of attacks

■ Centralized vs distributed attacks



Centralized attacks



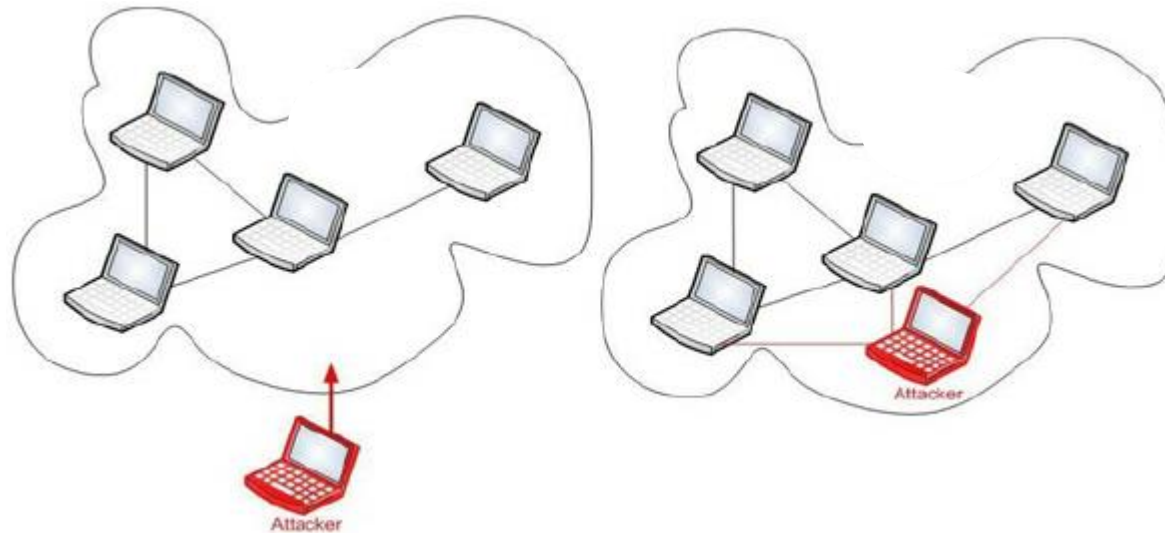
Distributed attacks

Introduction & generalities

→ Classes of attacks

■ Internal vs external attacks

Internal attacks are exercised by attackers that belong to the network or company's system. External attackers attack the network or the company's information system from the outside.



Introduction to cryptography

Introduction to cryptography

➔ Definitions

- **Steganography:** Hiding the existence of the message.
- **Cryptography:** Making messages understandable only by their legitimate destination entities.
- Cryptography is composed of the Greek words:
 - **CRYPTO** = *hidden*
 - **GRAPHY** = *to write*
- It is therefore the art of secret writing.
- **Cryptanalysis:** Cryptanalysis is the art of decrypting encrypted messages.
- Cryptanalysts are also called "hackers" !

Introduction to cryptography

→ Objectives

- Guarantee confidentiality
- Verify data integrity
- Ensuring authentication
- Ensuring non-repudiation

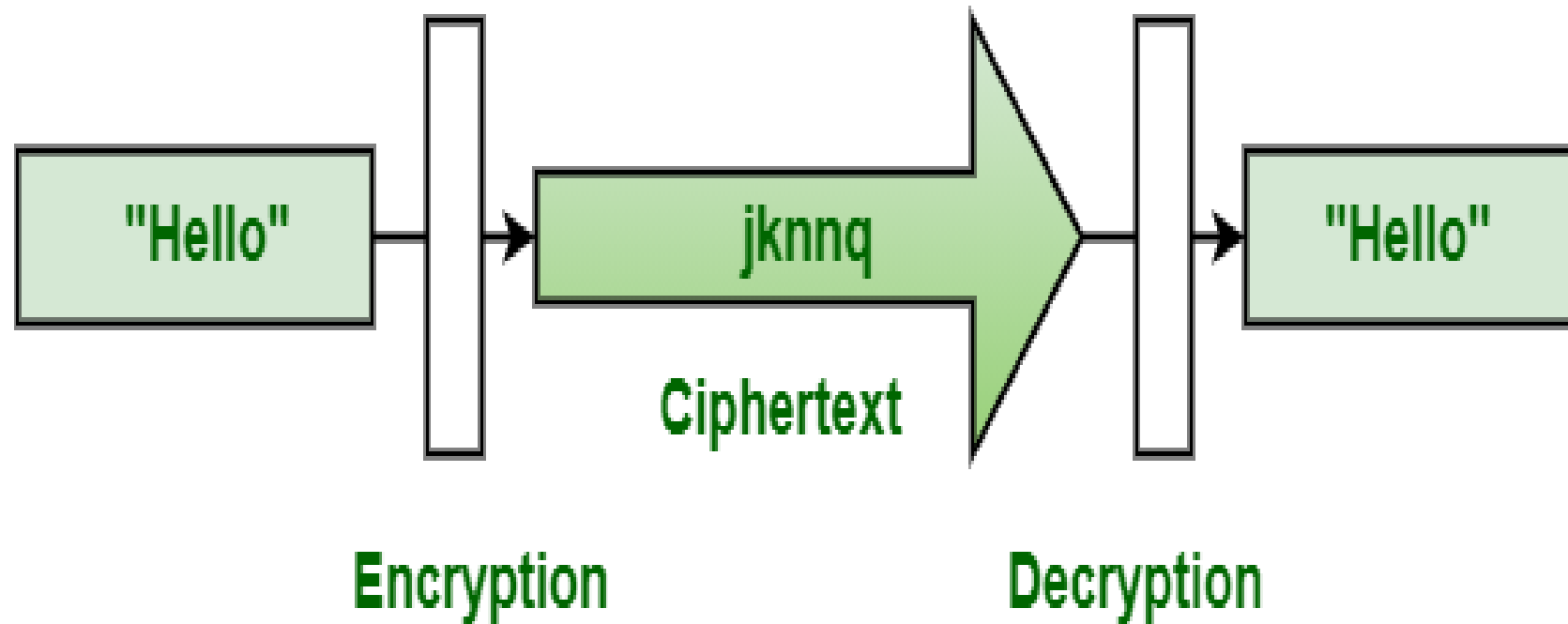
Introduction to cryptography

→ Cryptography-related Terminology

- **Plain text:** readable and understandable data without specific intervention.
- **Encryption (cipher):** A method of concealing plain text by hiding its content.
This operation ensures that only the people for whom the information is intended will be able to access it.
- **Cipher text:** unintelligible text resulting from encryption
- **Decryption:** reverse process of transforming cipher text into plaintext

Introduction to cryptography

→ Cryptography-related Terminology



Introduction to cryptography

→ Caesar cipher (Casear code, Shift cipher or Casear shift)

- The most known classical cryptographic algorithm
- Its operation is quite simple and consists of replacing each letter in the plaintext by another letter, where the position is a fixed number of shifts in the alphabet.
 - *Encryption Phase with shift n* $E_n(x) = (x + n) \bmod 26$
 - *Decryption Phase with shift n* $D_n(x) = (x - n) \bmod 26$

Introduction to cryptography

➔ Caesar cipher (Casear code, Shift cipher or Casear shift)

■ Example of Caesar cipher using a right rotation of three places

$$C = (P + 3) \bmod 26$$

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

■ Plaintext = **Hello** Ciphertext = **KHOOR**

Introduction to cryptography

→ Cryptographic Algorithms

- A mathematical function used for encryption and decryption. We are talking about encryption and decryption algorithms
- For good security, all modern algorithms use a **key**. This key can take one of the values among a large number of possible values (key space).
- The size and the value of the key "K" affects the encryption and decryption algorithms, and therefore the corresponding functions:
 - *Enc (message, K)*
 - *Dec (message, K)*

Introduction to cryptography

→ A cryptosystem

■ Cryptosystem: quintuplet (P, C, K, E, D), such as:

-P: set of plaintexts

-C: finite set of cipher texts

-K: key space

- E: encryption rules

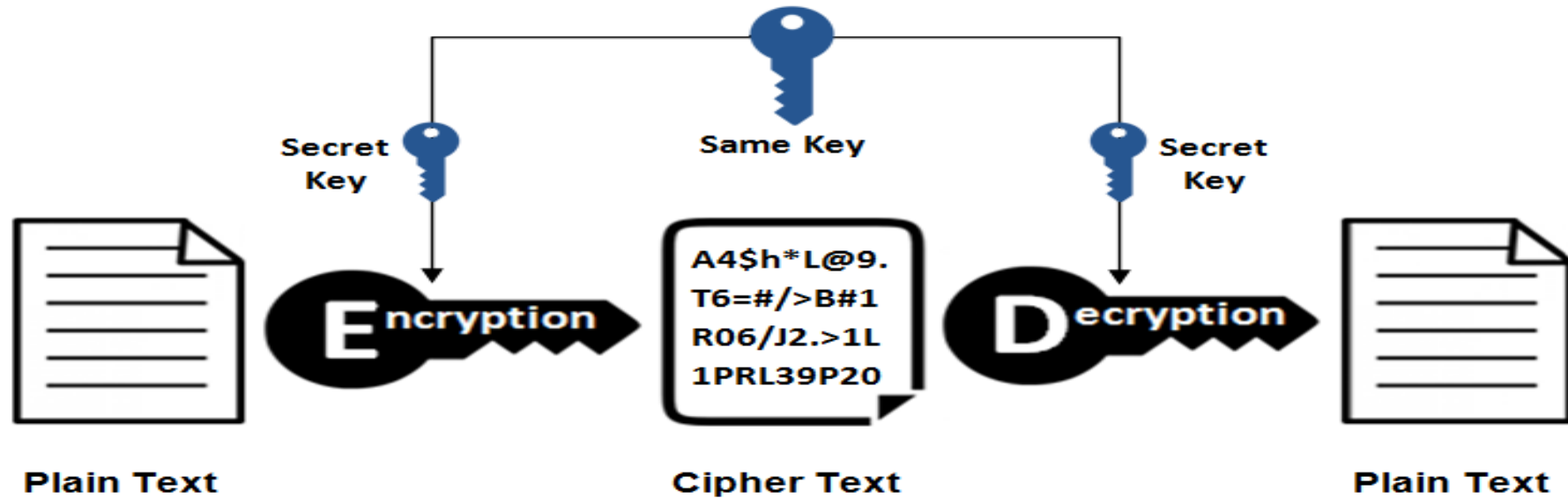
-D: decryption rules

■ For each K in K , there is an encryption rule E_K in E , and a corresponding decryption rule D_K in D , such that:

$$\{\{X\}_{E_K}\}_{D_K} = x, \text{ for all } x \text{ in } P$$

Introduction to cryptography

Symmetric Encryption



- We denote the symmetric key by : **K_{ab}** (the secret key shared between two entities : Alice and Bob).
- To send an encrypted message M from A to B: $A \Rightarrow B: \{ M \}_{K_{ab}}$
- To decrypt the received encrypted message, Bob uses the same secret key like:
 $\{ \{ M \}_{K_{ab}} \}_{K_{ab}}$

Introduction to cryptography

→ Symmetric cryptography

- Shared key cryptography, also called symmetric or secret key cryptography.
- In most symmetric systems, the encryption key and the decryption key are one and the same key.
- The length of the key has a great influence on the security of a system
- The main types of shared key cryptosystems in use today fall into two broad categories:
 - *Stream cipher*
 - *Block cipher.*

Introduction to cryptography

→ Symmetric cryptography : Stream Cipher

- Messages are encrypted character by character or bit by bit.
- The length of the key is therefore equal to that of the message.
- Example:
- Message: "Hello" 01010011 01000001 01001100 01001100 01110100
- Key (randomly generated) = 01110111 01110111 00100100 00011111 00011010
- ((Hello)binary XOR key) = 00100100 00110110 01101000 01001010 01001110
- The encrypted message is **\$6JSF**
- Example of symmetric stream cipher cryptosystems:
 - **A5, RC4**

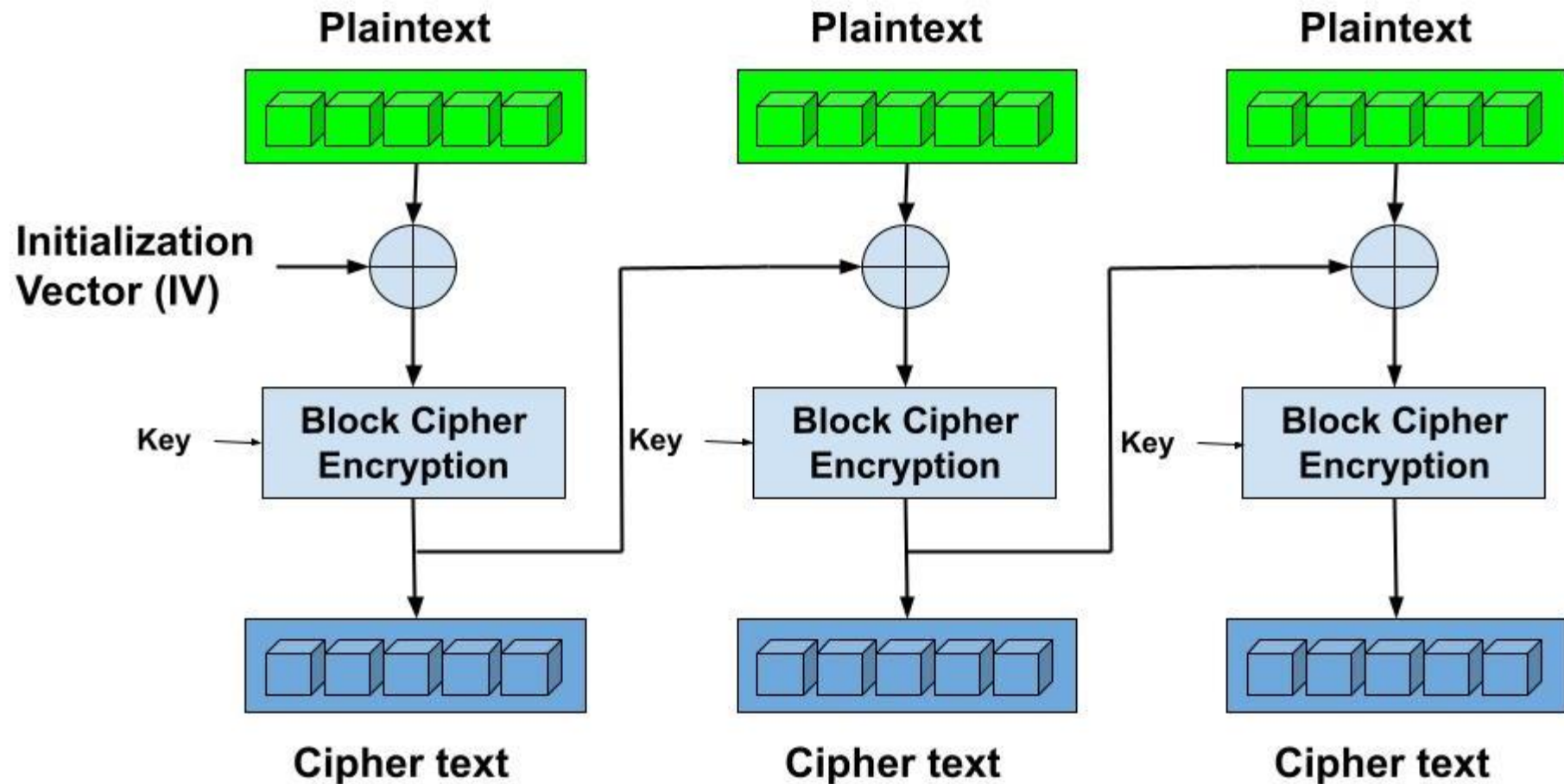
Introduction to cryptography

→ Symmetric cryptography : Block Cipher

- The plain text is split into blocks of equal length
- Block cipher algorithms are generally built on an iterative model.
- This model uses a function $F()$ that takes as parameters a key k and a message of n bits.
- F is repeated a certain number of times, called a round.
- At each round, the message that is encrypted is the result of the previous iteration
- Example of block cipher cryptosystems
 - *RC5, DES, AES*

Introduction to cryptography

→ Symmetric cryptography : Block Cipher



Introduction to cryptography

→ Symmetric cryptography : comparison between Stream & Block ciphers

	Stream cipher	Block cipher
Advantages	<ul style="list-style-type: none">+ Faster encryption+ Used when the size of input data is unknown (e.g. chat)	<ul style="list-style-type: none">+ More secure+ Most used+ Good for data where the size is well-known.
Drawbacks	<ul style="list-style-type: none">– Difficult to be implemented correctly	<ul style="list-style-type: none">– It is more memory requiring– If an encryption error occurs on one block, the entire message encryption is affected.

Introduction to cryptography

→ Symmetric cryptography

■ Advantages/Pros

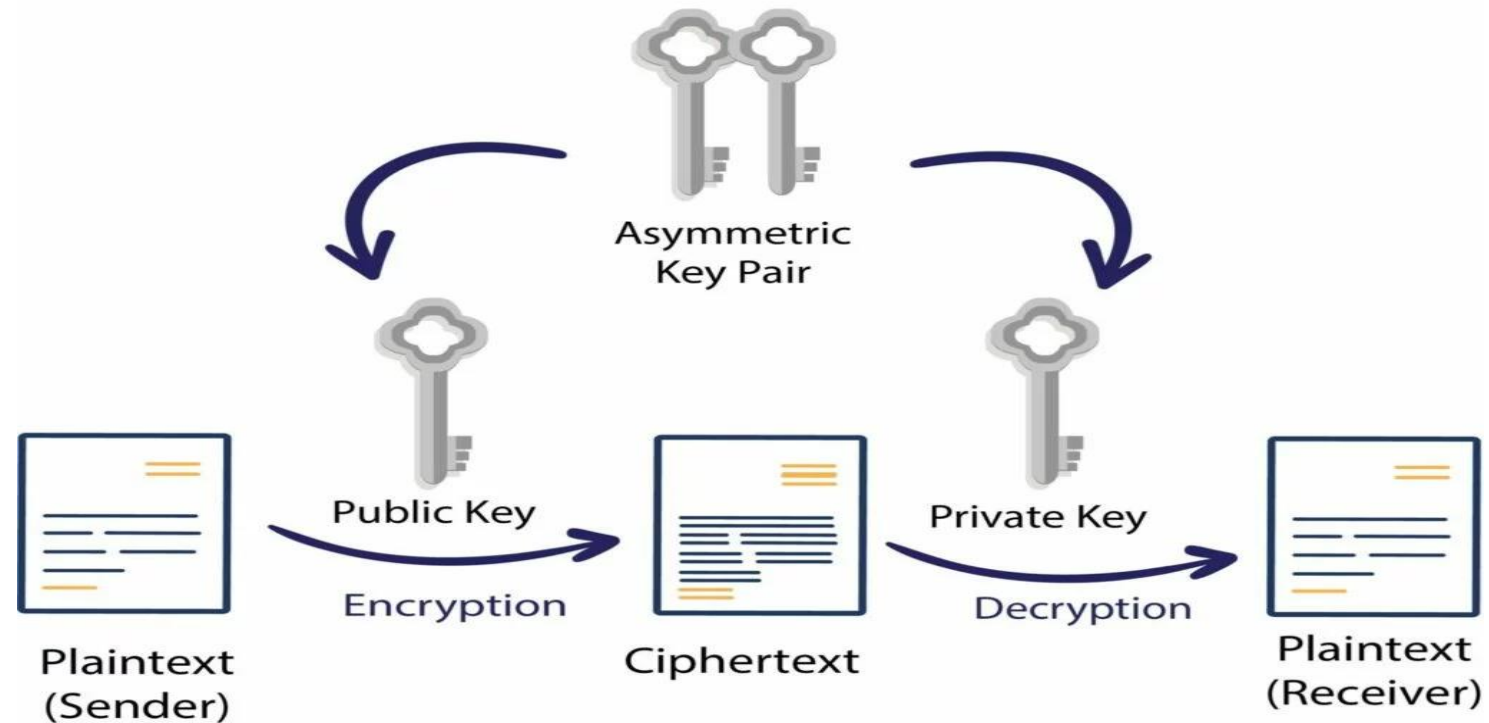
- *Fast encryption compared to asymmetric algorithms*
- *Key sizes are typically small (128 bis, 256 bits ..)*
- *Have lower complexity and costs*

■ Drawbacks /Cons

- *Number of handled keys is important (memory consuming)*
- *Key management (generation and security of secret keys) is difficult*
- *Few security services to ensure*

Introduction to cryptography

Asymmetric Encryption



Introduction to cryptography

→ Asymmetric cryptography

- The public keys of two entities Alice and Bob are denoted respectively as: **PKa** and **PKb**
- The private keys of Alice and Bob are denoted respectively as : **SKa** and **SKb**
- To send an encrypted message M from A to B, Alice uses the public key of Bob:
$$A \Rightarrow B : \{ M \} PKb$$
- *To decrypt the received message Bob uses its private key SKb :*
$$\{ \{ M \} PKb \} SKb$$
- To send an encrypted message M' from B to A, Bob uses the public key of Alice:
$$B \Rightarrow A : \{ M' \} Pka$$
- *To decrypt the received message Alice uses its private key SKa :*
$$\{ \{ M' \} PKa \} SKa$$

Introduction to cryptography

→ Asymmetric cryptography

■ *Examples of asymmetric cryptosystems:*

- RSA
- ElGamal
- DSA
- Diffie-Hellman
- ...

Introduction to cryptography

→ Asymmetric cryptography

■ *Example of RSA encryption and decryption*

- Choose $p = 3$ and $q = 11$
- Compute $n = p * q = 3 * 11 = 33$
- Compute $\phi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$
- Choose e such that $1 < e < \phi(n)$ and e and $\phi(n)$ are coprime. Let $e = 7$
- Compute a value for d such that $(d * e) \% \phi(n) = 1$. One solution is $d = 3$
[(3 * 7) % 20 = 1]
- Public key is $(e, n) \Rightarrow (7, 33)$
- Private key is $(d, n) \Rightarrow (3, 33)$
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

Introduction to cryptography

→ Hybrid cryptography

- Uses symmetric encryption for messages.
- Asymmetric encryption for the protection of symmetric/secret keys and generate digital signatures.

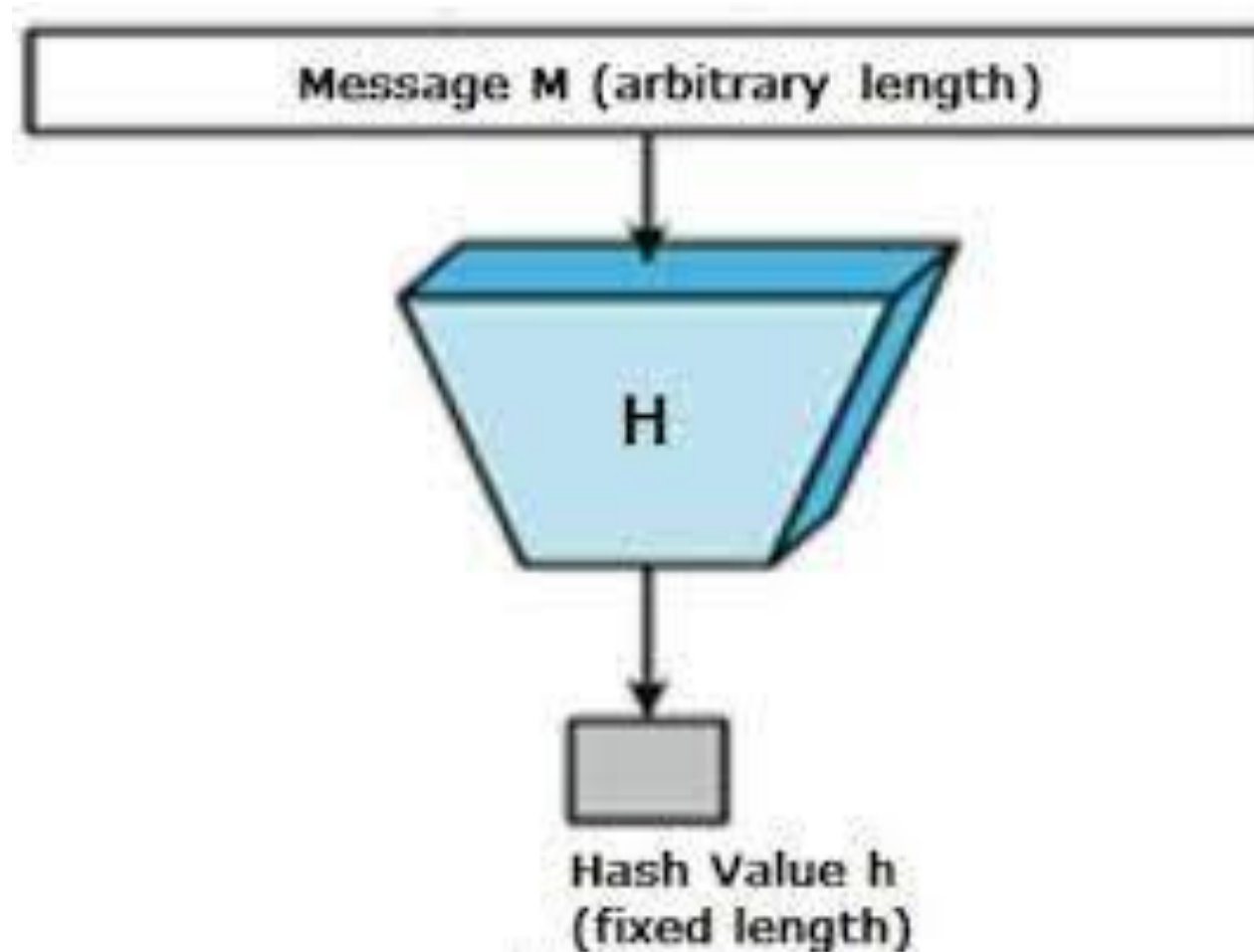
Introduction to cryptography

→ Hash functions

- Mathematical functions that can be used to map data of arbitrary (variable) size to fixed-size code,
- They have two main features:
 - *No collisions: for two different input data M and M' , it is impossible to have the same resulting hash code: $H(m) = C1$ $H(m') = C2$, $C1 \neq C2$.*
 - *It is impossible to discover the initial data from the generated hash code*
- Hash functions have many use cases in cryptography, namely:
 - *Digital signatures*
 - *Symmetric key generation*
 - *Symmetric authentication (MAC code generation).*
 - *Password protection*
 - *Etc,.*

Introduction to cryptography

→ Hash functions



Introduction to cryptography

→ Digital Signatures using hash functions

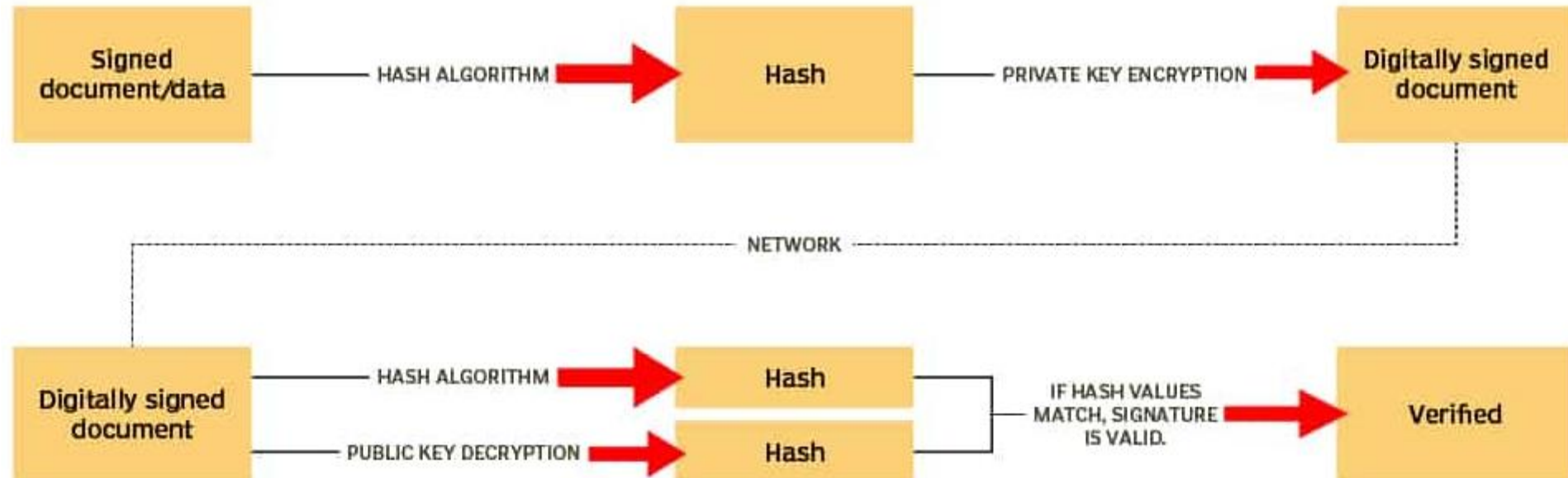
- As defined before, digital signature is an asymmetric encryption using the sender's private key.
 - $A \Rightarrow B: M. \{ M \} SK_a$
- For better performances, it is highly recommended to sign the hash value/code of the message rather than applying the asymmetric encryption on the entire message.
 - $A \Rightarrow B: M. \{ h(M) \} SK_a$
- The verification process is one as follows:
 - *First, the receiver (Bob) decrypts the signature using the public key of the sender. $\{ \{ h(M) \} SK_a \} PK_a$*
 - *Compare the obtained hash value from the signature with the one get from the message (computed by the receiver). If there is a match, the signature is verified. Otherwise, the signature is considered bad and the message is discarded.*

Introduction to cryptography

→ Digital Signatures using hash functions

- Digital signatures based on hash functions ensure *integrity service* in addition to the authentication and non-repudiation services.

The digital signature process



Introduction to cryptography

→ HMAC (Hash Message Authentication Code)

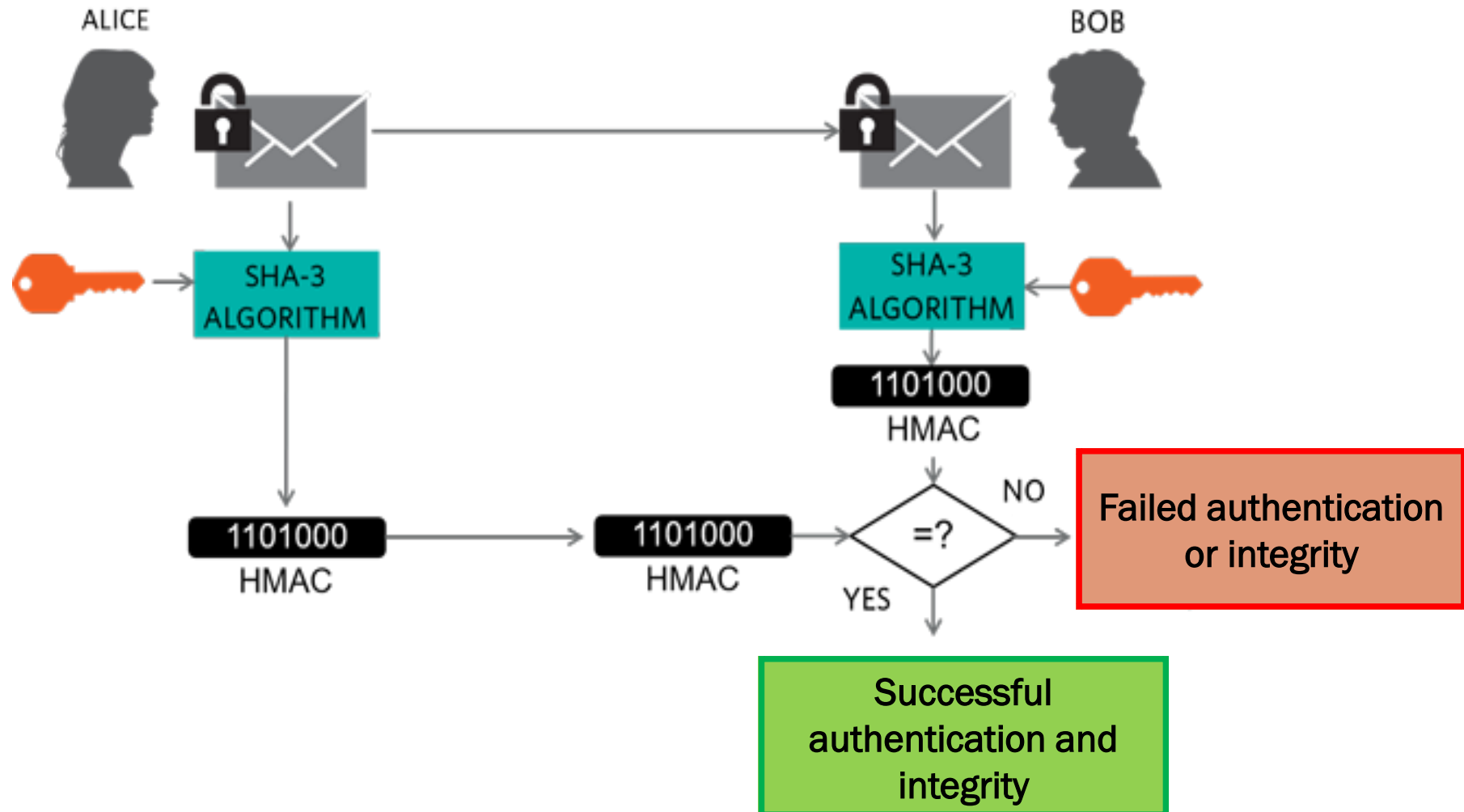
- HMAC is a symmetric cryptographic algorithm that generates a MAC code from a message and a secret key
- We denote it by : $H_k(m)$
- It ensures **authentication** and **integrity**.
- HMAC combines the hash code of a message obtained with SHA-based hash function with the secret key and other padding data.

$$H_k(m) = h [(K_{ab} \oplus opad) . h ((K_{ab} \oplus ipad) . m)]$$

- *Where: $ipad$ and $opad$ are defined by: $ipad = 0x363636...3636$ and $opad = 0x5c5c5c...5c5c$. So if the block size of the hash function is 256 bits, $ipad$ and $opad$ are 64 repetitions of the bytes 0x36 and 0x5c, respectively.*

Introduction to cryptography

→ HMAC (Hash Message Authentication Code)



Public Key Infrastructure

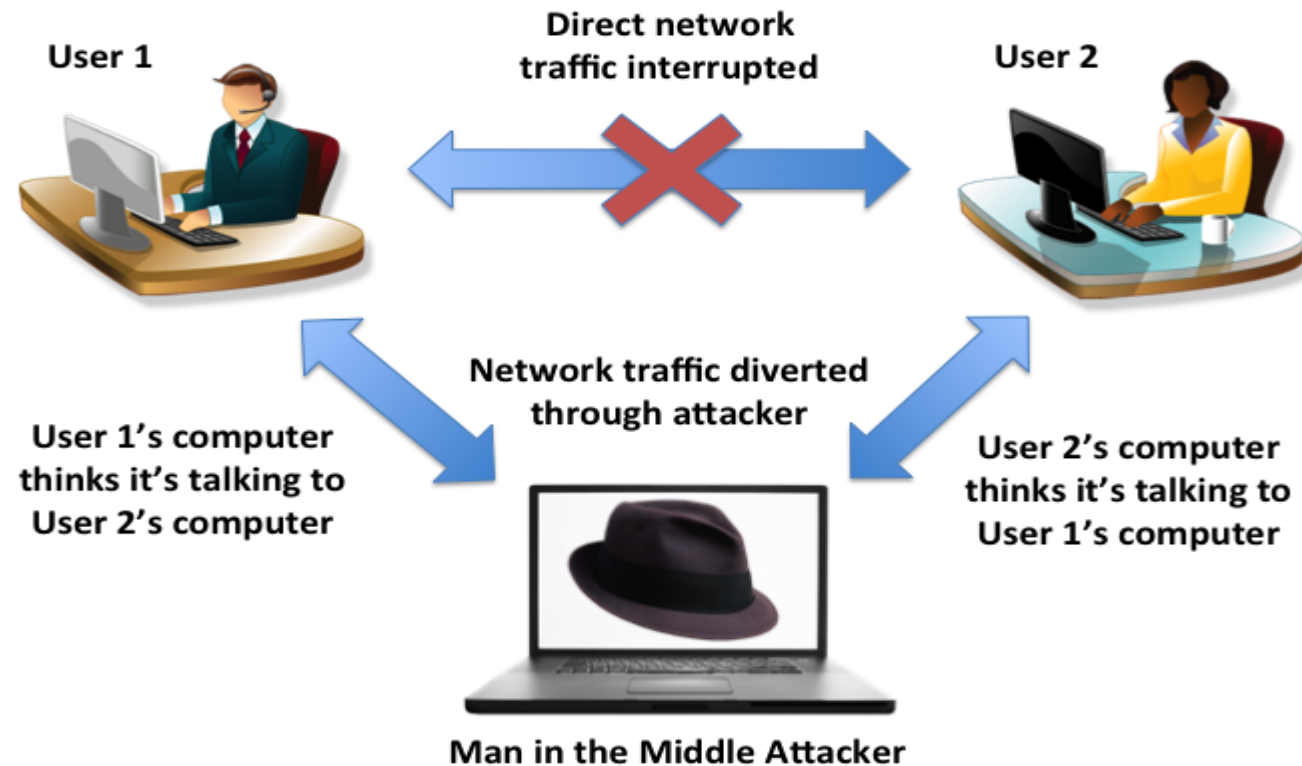
Public Key Infrastructure

→ Main issue with the asymmetric cryptography

- In asymmetric cryptography, it is required that the communicating entities know the public keys of each other.
 - $A \Rightarrow B: A. Pka$
 - $B \Rightarrow A: B. PKb$
- *Warning : Risk of Man In The Middle (MITM) attack !*
 - *Intruder $\Rightarrow B: A. Pki$*
 - *Intruder $\Rightarrow A: B. PKi$*
- So, how to guarantee that the public key of an entity really corresponds to the pretended owner?

Public Key Infrastructure

→ Main issue with the asymmetric cryptography



Public Key Infrastructure

→ Solution

- It is required that an authority guarantees (certifies) the correspondence between the identities (a, b, ...) and the corresponding public keys (PKa, PKb, ...).
- This authority is called: Certification Authority (CA)
 - *The CA should be trustworthy.*
 - *Its public key is well known to our operating systems/web browsers*
- There are many certification authorities deployed around the world.
 - *See the following two figures*

Settings - Google Chrome

Settings

Chrome | chrome://settings/privacy

Settings

You and Google

Auto-fill

Privacy and security

Appearance

Search engine

Default browser

On start-up

Advanced

Languages

Downloads

Printing

Accessibility

System

Reset settings

Help improve Chrome security

To detect dangerous apps and sites, Chrome sends URLs of some pages that you visit, limited system information and some page content to Google

Send a 'Do Not Track' request with your browsing traffic

Allow sites to check if you have payment methods saved

Preload pages for faster browsing and searching

Uses cookies to remember your preferences, even if you don't visit those pages

Manage certificates

Manage HTTPS/SSL certificates and settings

Manage security keys

Reset security keys and create PINs

Appearance

Themes














GTK+

Show Home button

Disabled

Settings

🔍 Search settings

-  You and Google
-  Auto-fill
-  Privacy and security
-  Appearance
-  Search engine
-  Default browser
-  On start-up
- Advanced
 -  Languages
 -  Downloads
 -  Printing
 -  Accessibility
 -  System
 -  Reset settings

← Manage certificates

Your certificates

Servers

Authorities

Others

You have certificates on file that identify these certificate authorities

[Import](#)

org-AC Camerfirma S.A.



org-AC Camerfirma SA CIF A82743287



org-ACCV



org-Actalis S.p.A./03358520967



org-AddTrust AB



org-AffirmTrust



org-Agencia Catalana de Certificacio (NIF Q-0801176-I)



org-Amazon



Public Key Infrastructure

- How do the CAs do to certify the public keys?
- Solution: the CA signs a message that includes the public key and the identity of its owner → **the certificate**

$A \implies CA : A . PKa$

$B \implies CA : B . PKb$

Alice and Bob send request
messages to issue a certificate

$CA \implies A : A . PKa . \{ h (A . PKa) \} SKca$

$CA \implies B : B . PKb . \{ h (B . PKb) \} SKca$

The certification authority sends
the certificates to Alice and Bob

$A \implies B : A . PKa . \{ h (A . PKa) \} SKca$

$B \implies A : B . PKb . \{ h (B . PKb) \} SKca$

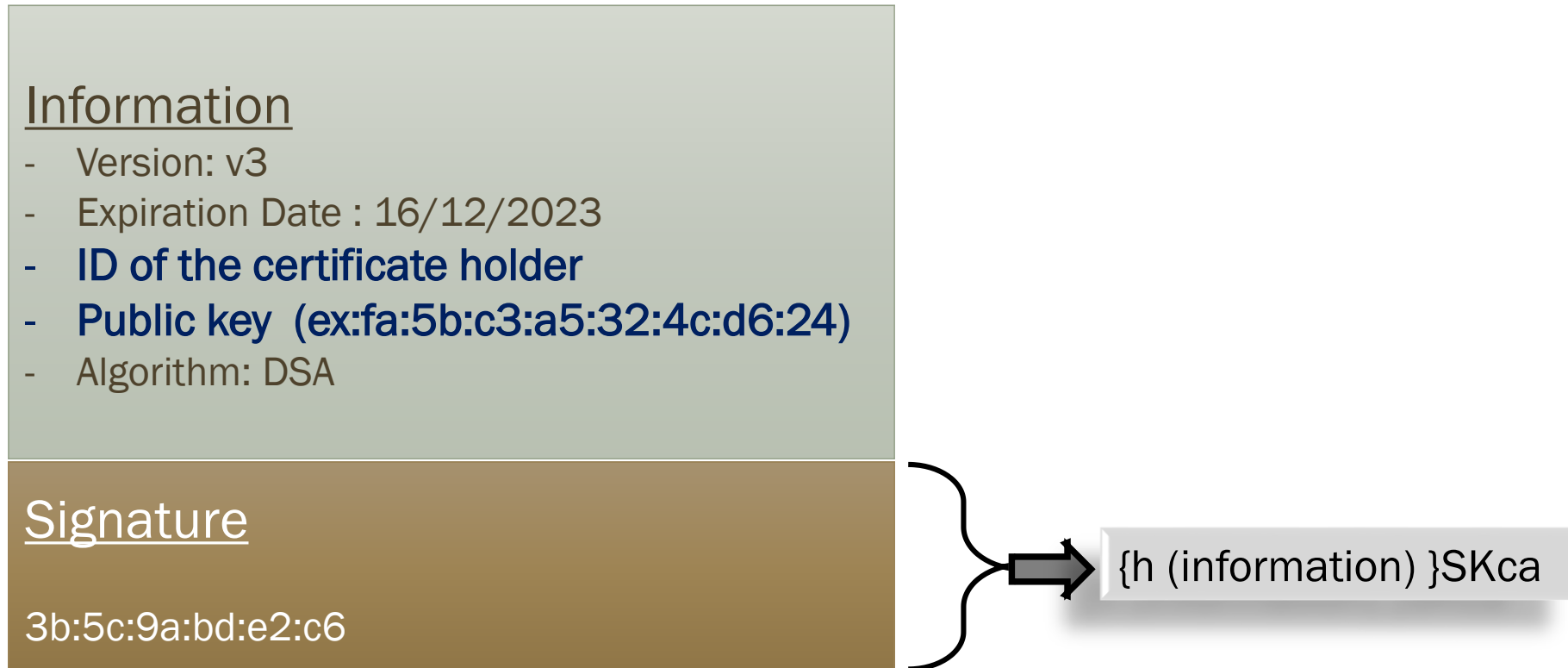
Alice and Bob send their
certificates to each other

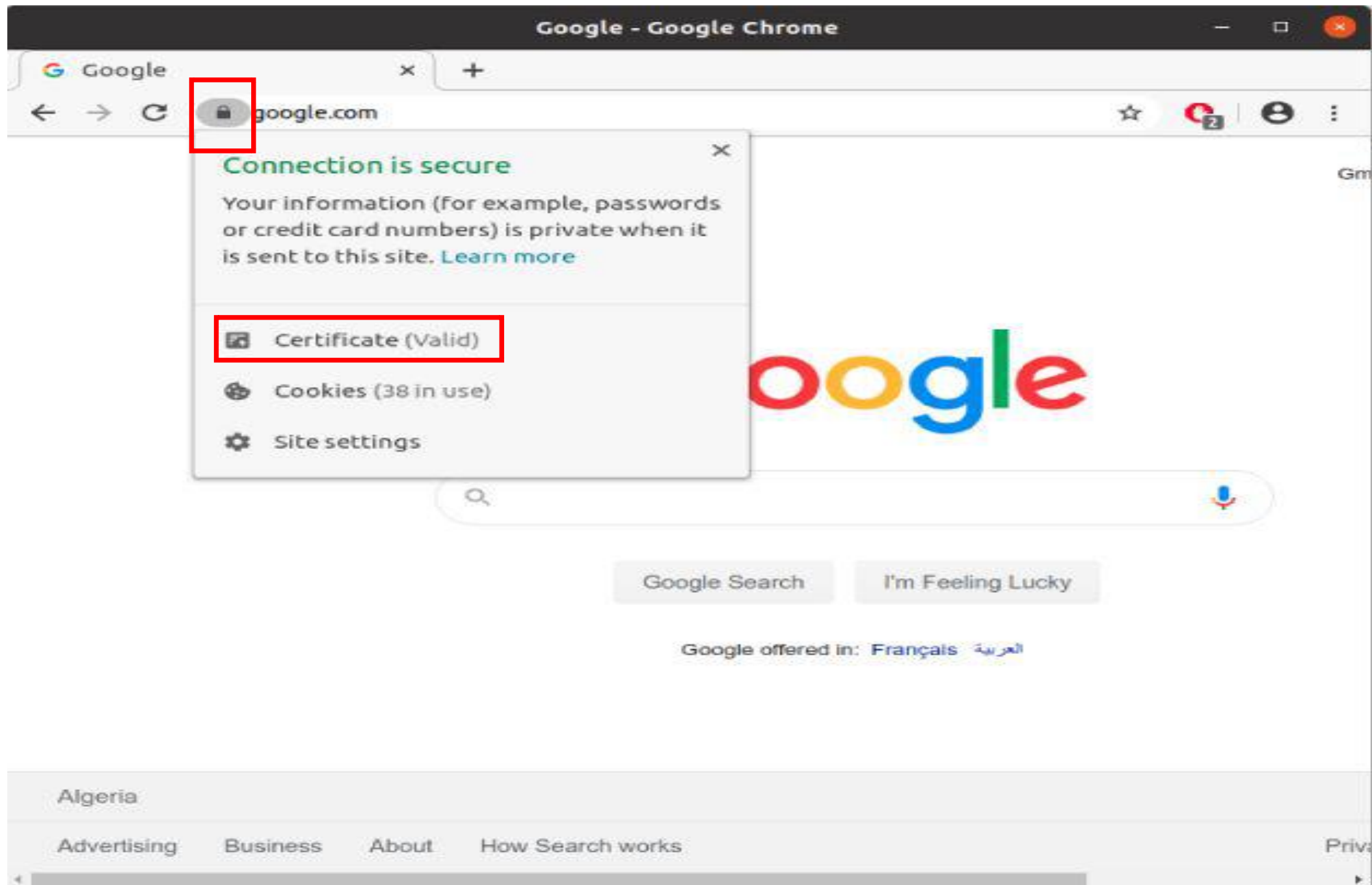
Public Key Infrastructure

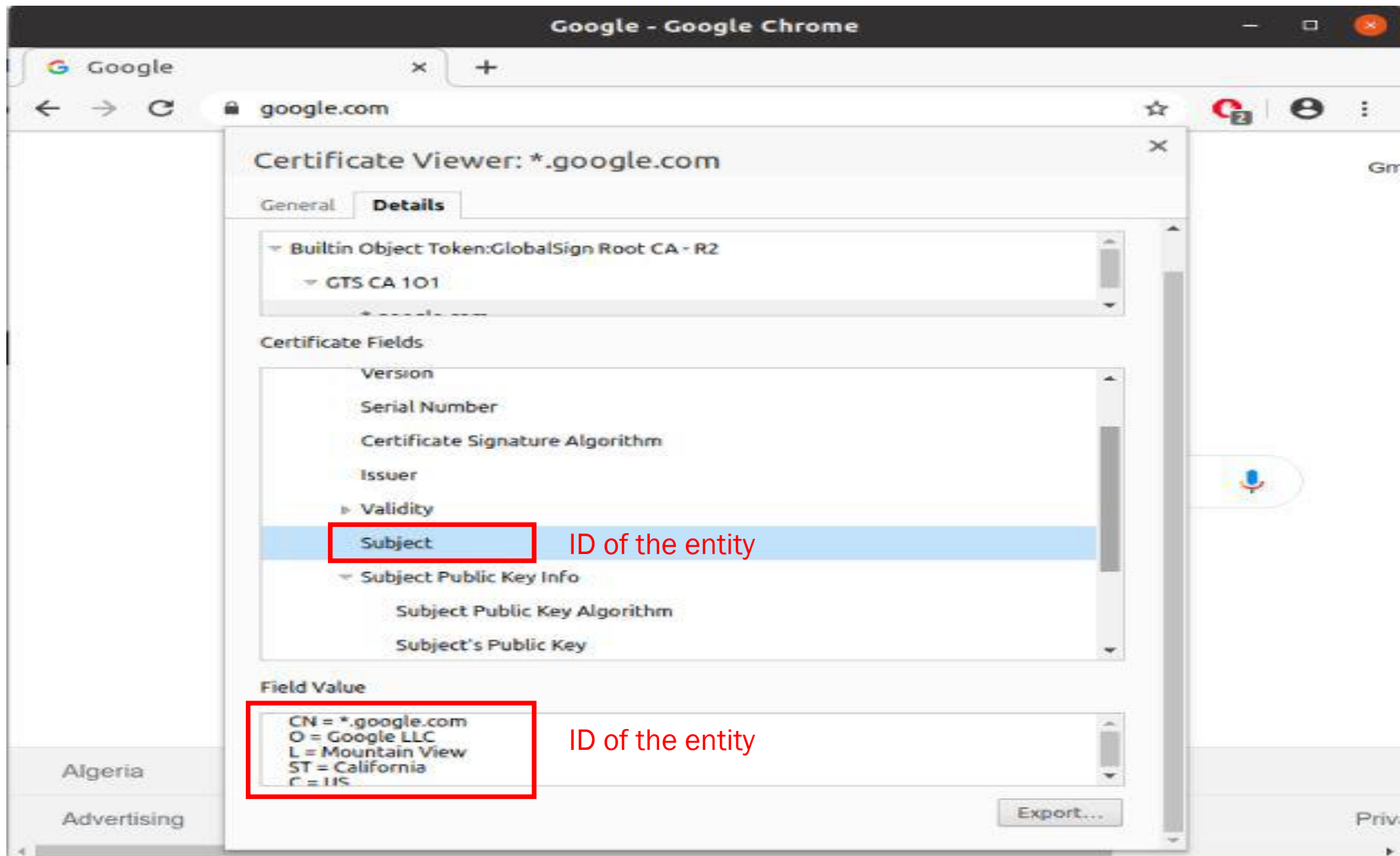
- The public keys of the certification authorities are self-signed by the authorities themselves.
 - *Ex : CA . PKca.{H(CA.PKca)}SKca: certificate self-signed by CA*
- The certificates of CA are saved in the browsers and with the operating systems.
- When you buy a new computer, or smartphone, ... these certificates come pre-installed in browsers/systems.
- New certificates may be installed during browser/system updates or manually by the user

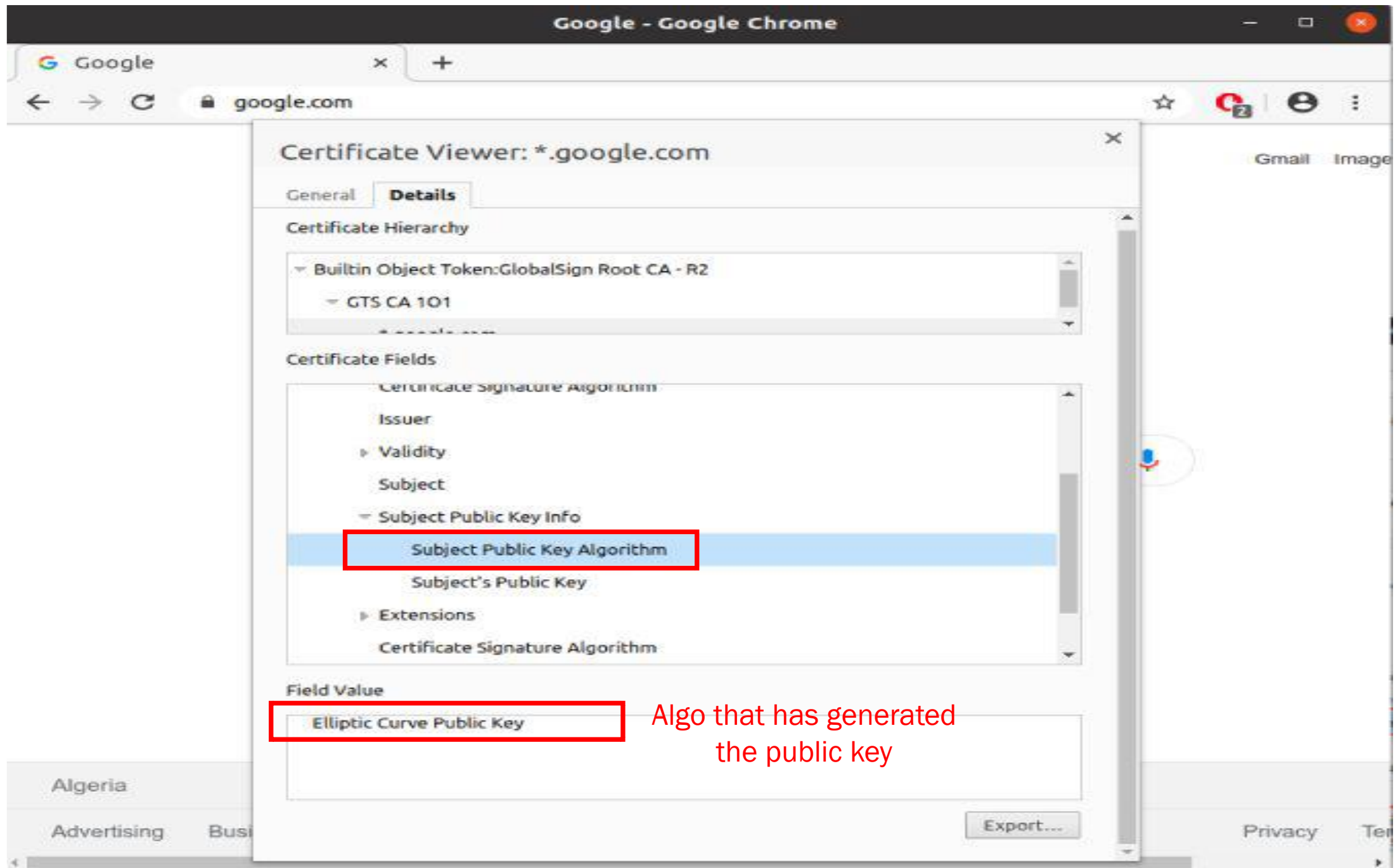
Public Key Infrastructure

■ Standard structure of a certificate









Google - Google Chrome

Google google.com

Certificate Viewer: *.google.com

General Details

Certificate Hierarchy

- Built-in Object Token: GlobalSign Root CA - R2
 - GTS CA 101

Certificate Fields

- Certificate Signature Algorithm
- Issuer
- Validity
- Subject
- Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key**
 - Extensions
- Certificate Signature Algorithm

Field Value

```
04 84 92 27 F7 E3 DB A8 16 86 B5 38 74 64 20 98
CE C3 DC 4E 17 51 18 F5 55 BF C9 D5 46 10 42 FC
7E 6A F6 04 D6 8A 67 02 54 B5 0B 51 80 2F 8F 52
25 FB 4E C5 67 DE 2D D2 F1 72 FC E7 D3 6F 18 3C
4B
```

Export...

Algeria Advertising Business Privacy Terms

Public key of the entity

