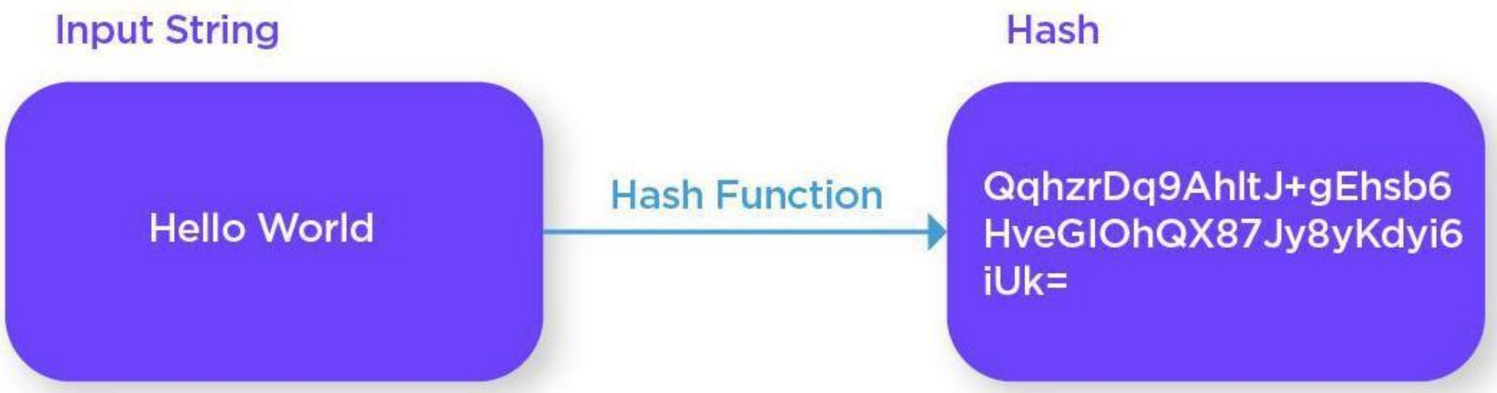
Hash function

Definition

- Mathematical compression function that converts a string of any length into a fixed-size string (often smaller, called a fingerprint).



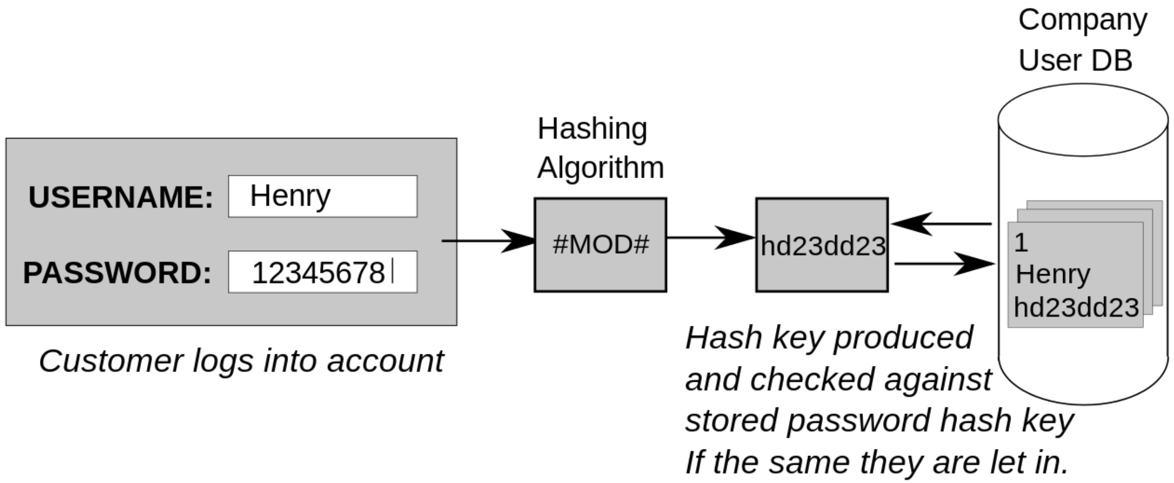
- It is easy to calculate the fingerprint from an input string, but it is difficult to generate strings that have a specific fingerprint

Hash function

Utilization

The hash function is public and is primarily used in digital signatures, data integrity verification, and identification.

For example, to access an account on Unix, the system calculates the fingerprint from the password and compares it to the known fingerprint, which is located in the etc/passwrd file. The same process applies for a web login



Customer logs into account

Hash key produced and checked against stored password hash key If the same they are let in.

Hash function

Hashing algorithms

- **MD2, MD4 et MD5.** Message Digest 2, 4 et 5 :
  - Developed by Ron Rivest for RSA Security.
  - They are hash functions that produce all a fingerprint of 128 bits.

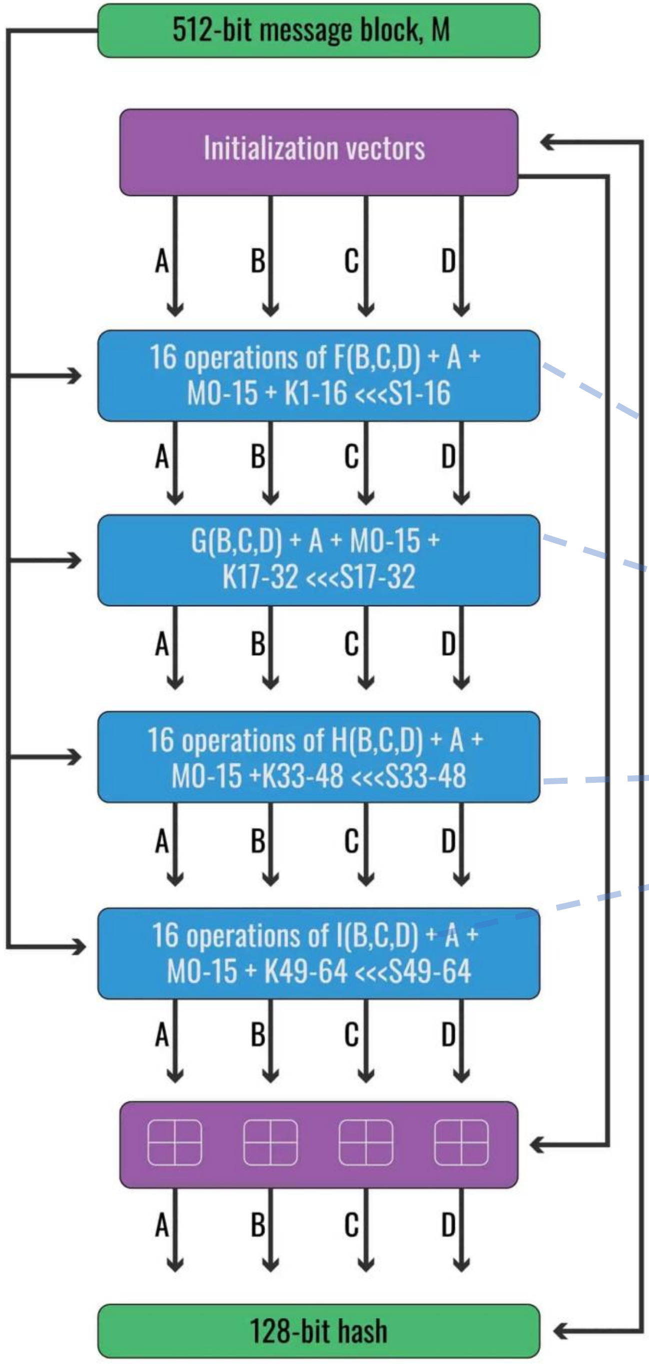
- **SHA, SHA1 et SHA2.** (Secure Hash Algorithm) :
  - Developed by NSA.
  - The two algorithms (SHA and SHA1) produce fingerprints of 160 bits for a message deux millions Terabytes long.
  - La taille de son empreinte le rend très difficile à percer, mais il est plus lent que MD5.

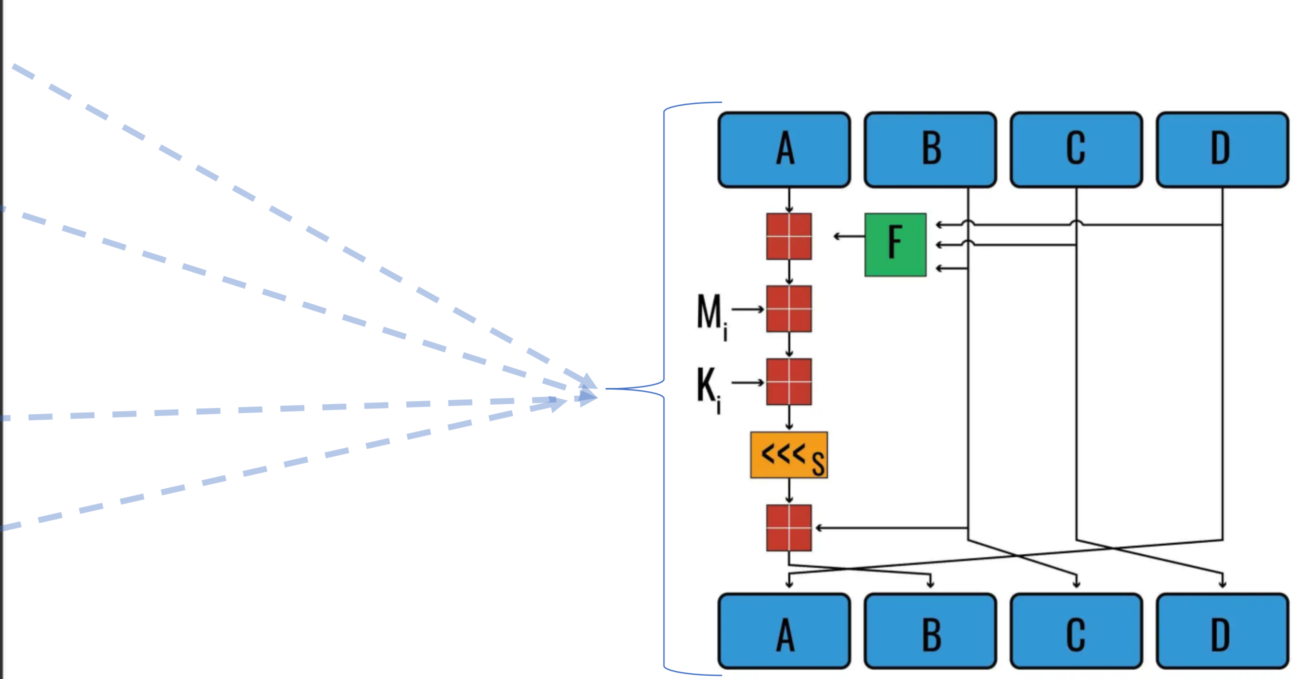
- **Snefru** (128 and 256 bits), **N-Hash** (128 bits), …

MD5

IV

A – 01234567
B – 89abcdef
C – fedcba98
D – 76543210

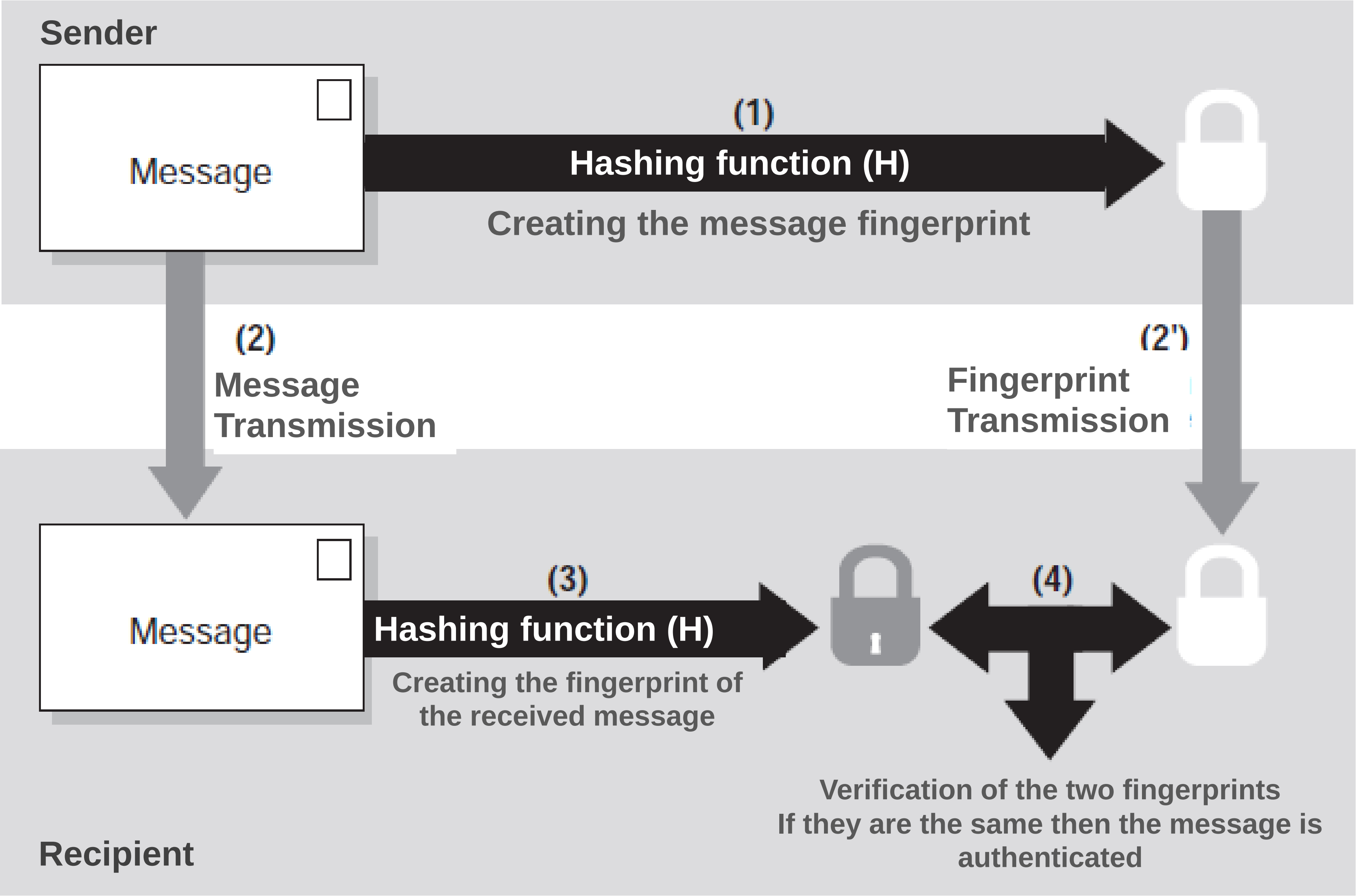

512-bit message block, M
Initialization vectors
A
B
C
D
16 operations of F(B,C,D) + A + M0-15 + K1-16 <<<S1-16
A
B
C
D
G(B,C,D) + A + M0-15 + K17-32 <<<S17-32
A
B
C
D
16 operations of H(B,C,D) + A + M0-15 +K33-48 <<<S33-48
A
B
C
D
16 operations of I(B,C,D) + A + M0-15 + K49-64 <<<S49-64
A
B
C
D
A
B
C
D
128-bit hash



J. Lake. The MD5 algorithm (with examples). 2021
https://www.comparitech.com/blog/information-security/md5-algorithm-with-examples/

Hash function

Integrity check



Sender
Message
(1)
Hashing function (H)
Creating the message fingerprint
(2)
Message Transmission
(2')
Fingerprint Transmission
Message
(3)
Hashing function (H)
Creating the fingerprint of the received message
(4)
Verification of the two fingerprints
If they are the same then the message is authenticated
Recipient

Digital Signature

Definition

- A **digital signature** is any authentication process for documents, **generated** and **managed** purely electronically by **computers**. A digital signature serves the same purpose as a handwritten signature.

- A handwritten signature is easy to forge. On the other hand, a **digital signature** is practically **unfalsifiable**; moreover, it attests to both the content of the information and the identity of the signer. It is unique, easy for the recipient to authenticate, easy to generate, and economically viable.

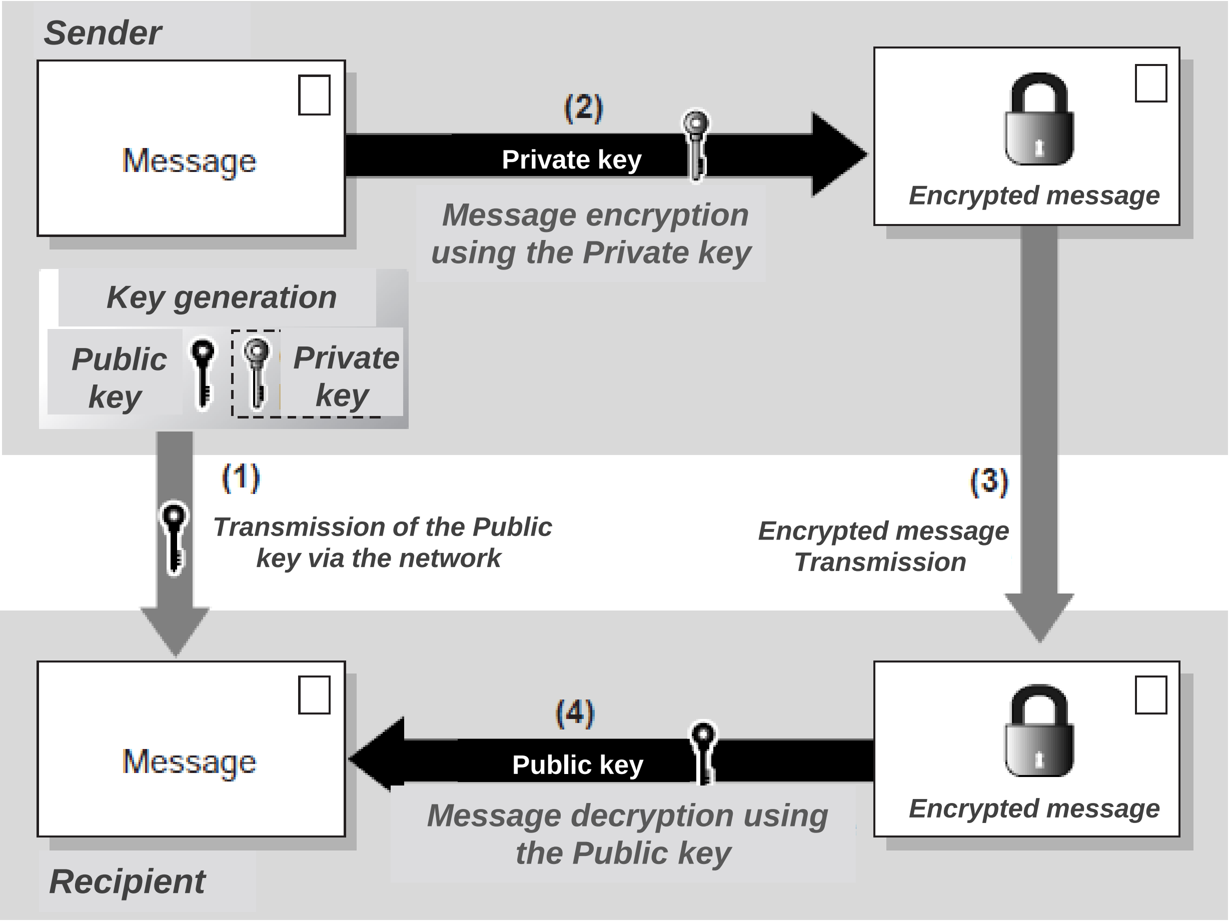
Digital Signature

Creation et utilization

- The basic method used to create a digital signature involves **encrypting** the information with the **sender's private key**. The recipient has the ability to verify and authenticate the information using only the **sender's public key**. Indeed, if the recipient is able to decrypt the signature with the sender's public key, then the information is **authentic:**
  - **Signature:** $X = M^d \pmod{n}$
  - **Authenticity check:** $M = M^e \pmod{n}$

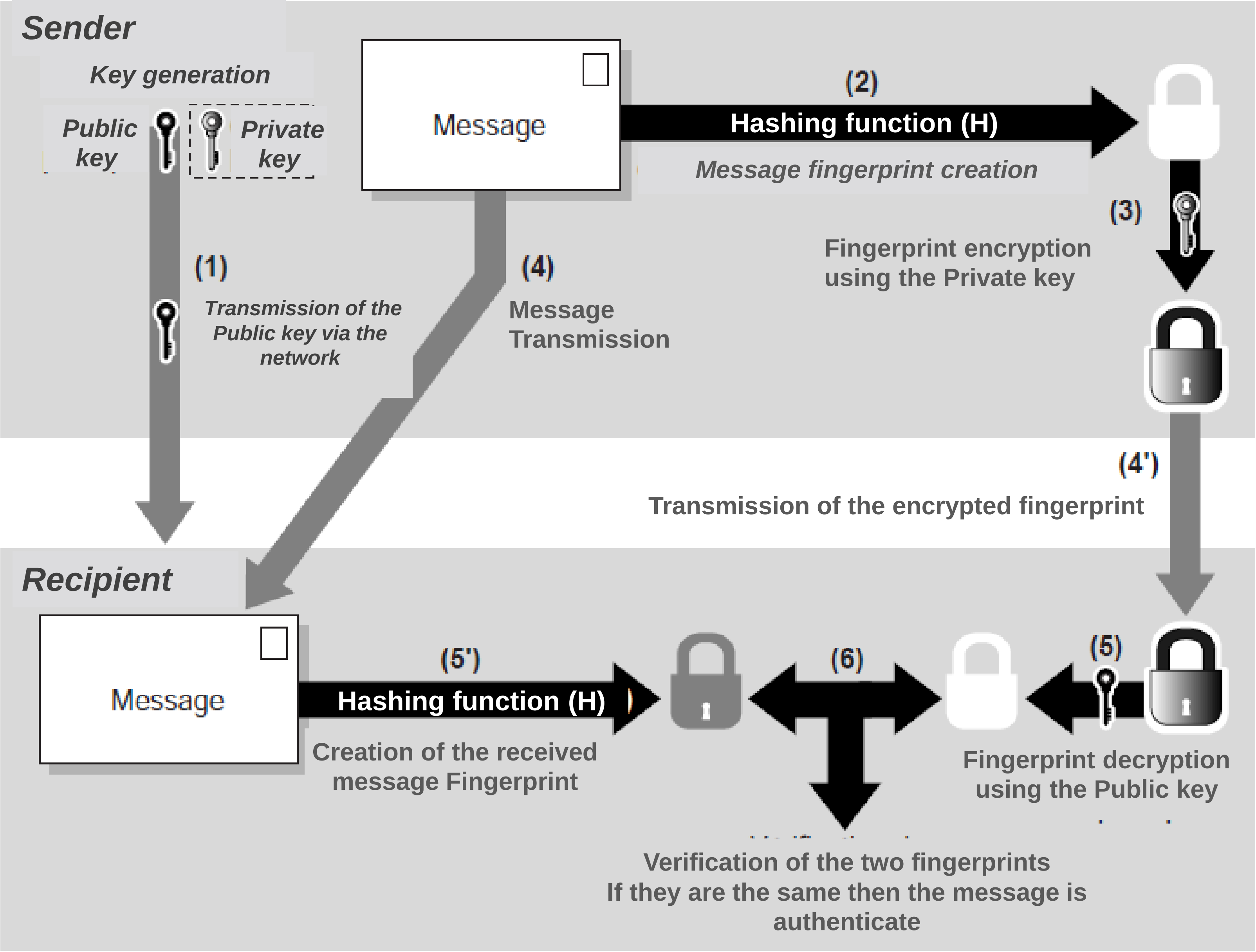
Digital Signature

- To authenticate themselves, the sender uses their private key to sign a message. On the other hand, the receiver uses the sender's public key to verify if the message is signed.
- In this way, the receiver can verify **both** that the <u>data has not been altered</u> and that it has indeed been <u>sent by the sender</u>.


Sender
Message
(2)
Private key
Message encryption using the Private key
Encrypted message
Key generation
Public key
Private key
(1)
Transmission of the Public key via the network
(3)
Encrypted message Transmission
Message
(4)
Public key
Message decryption using the Public key
Encrypted message
Recipient

Authentication using Public key

Combination of a hash function and encryption with public key


Sender
Key generation
Public key
Private key
Message
(2)
Hashing function (H)
Message fingerprint creation
(3)
Fingerprint encryption using the Private key
(1)
Transmission of the Public key via the network
(4)
Message Transmission
(4')
Transmission of the encrypted fingerprint
Recipient
Message
(5')
Hashing function (H)
Creation of the received message Fingerprint
(6)
(5)
Fingerprint decryption using the Public key
Verification of the two fingerprints
If they are the same then the message is authenticate

Cryptanalysis

Definition

- The cryptanalysis is the art of analyzing an encrypted message (its weaknesses) in order to decode it (and break the code).
- The aim of cryptanalysis is to find plaintext messages corresponding to encrypted messages

Attacker

- The individual attempting to decrypt (without knowledge of the key) is called the attacker.
- The attacker employs a combination of analytical reasoning, application of mathematical tools, and discovery of redundancies

Kerckhoffs principle

- The security of encryption should rely solely on protecting the key. This means that the algorithm (method or procedure) is public (not secret)

Cryptanalysis

Types of cryptanalysis

- Partial cryptanalysis: the attacker decrypts one or more messages (but not all of them).
- Total cryptanalysis: the attacker discovers a way to decipher all messages (for example, if they discover the key)

Cryptanalysis Techniques:

1) Exhaustive search

- Try all possible combinations of a key.
- Programs that use this method are called brute-force programs (crackers). They require as input the name of the file to crack and a regular expression.
- The cracker tries all possible combinations of keys that satisfy the regular expression.

Example: For the Caesar cipher, this search is feasible because there are few possibilities (25)

Cryptanalysis

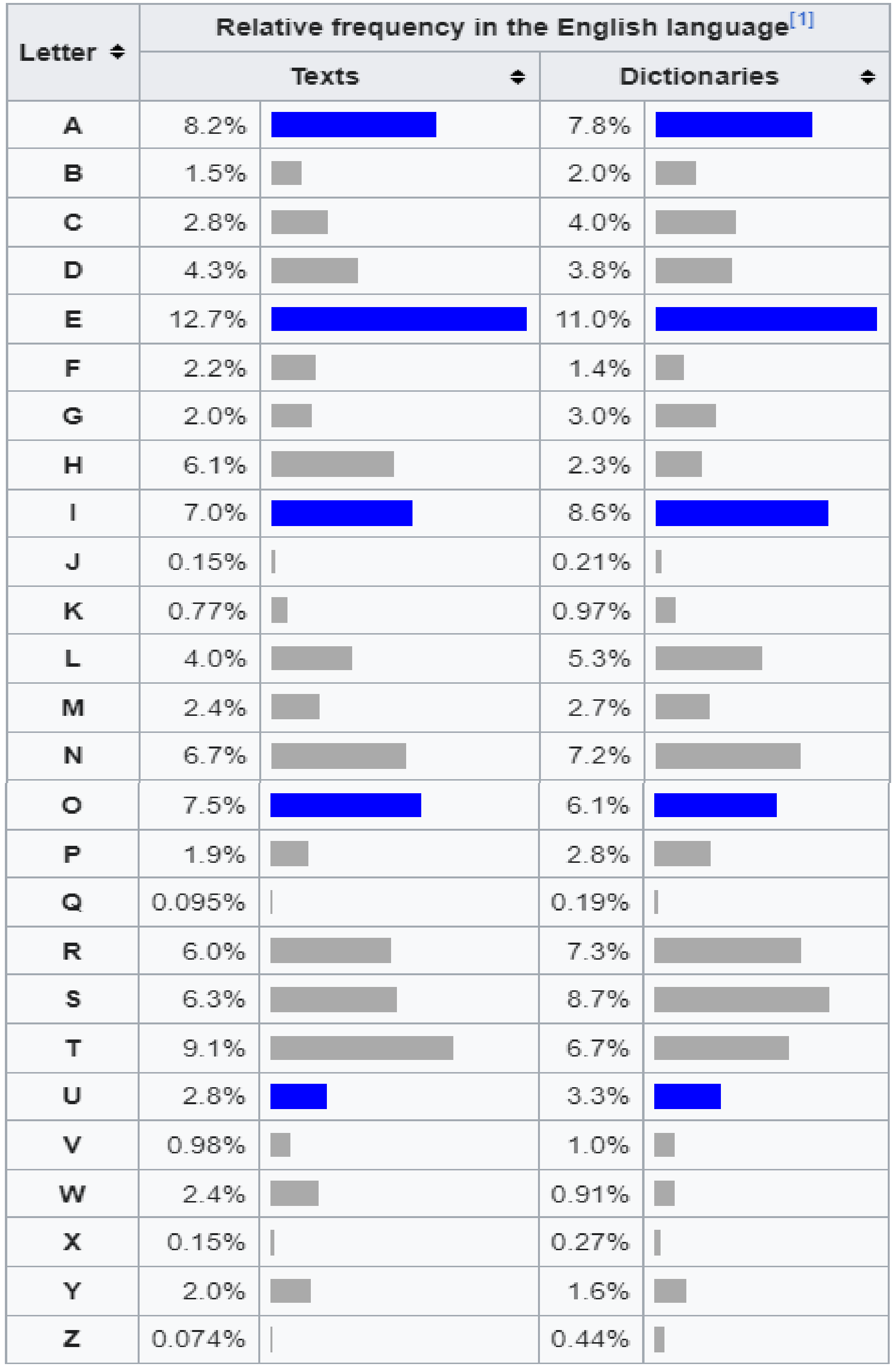
2) Dictionary attack

- Find the key using common words from the language using a database (dictionary). This dictionary includes words from the language, names of actors, film or cartoon characters, philosophical phrases, etc.
- The cracker attempts to decipher the text by trying these words (reversed, in lowercase, or uppercase...).

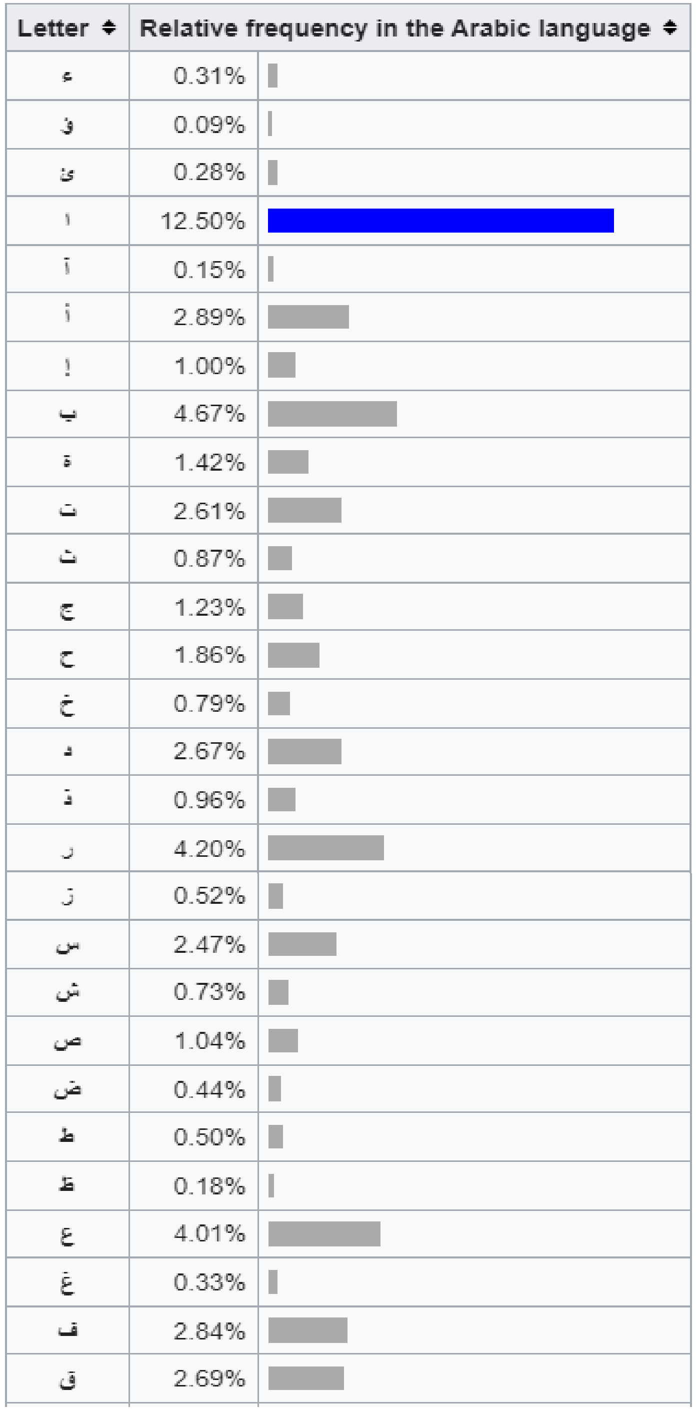
3) Statistical attack (frequency-based)

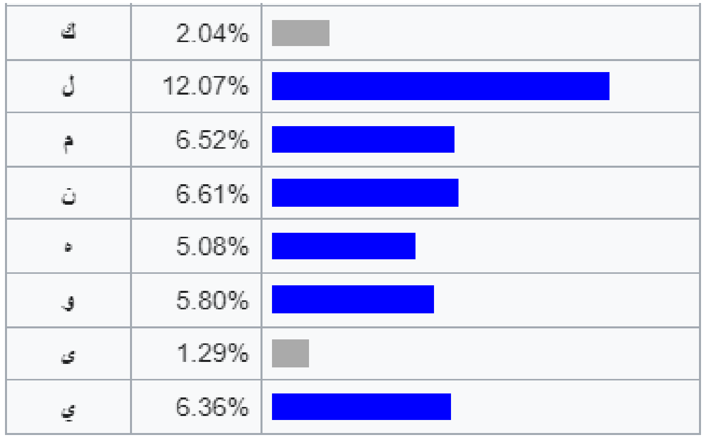
A statistical attack involves statistically analyzing encrypted texts, which means:

- Determining the frequencies of occurrence of symbols;
- Comparing them with the typical frequency characteristics of languages.



Letter	Relative frequency in the English language[1]	
	Texts	Dictionaries
A	8.2%	7.8%
B	1.5%	2.0%
C	2.8%	4.0%
D	4.3%	3.8%
E	12.7%	11.0%
F	2.2%	1.4%
G	2.0%	3.0%
H	6.1%	2.3%
I	7.0%	8.6%
J	0.15%	0.21%
K	0.77%	0.97%
L	4.0%	5.3%
M	2.4%	2.7%
N	6.7%	7.2%
O	7.5%	6.1%
P	1.9%	2.8%
Q	0.095%	0.19%
R	6.0%	7.3%
S	6.3%	8.7%
T	9.1%	6.7%
U	2.8%	3.3%
V	0.98%	1.0%
W	2.4%	0.91%
X	0.15%	0.27%
Y	2.0%	1.6%
Z	0.074%	0.44%





Letter	Relative frequency in the Arabic language
ء	0.31%
ؤ	0.09%
ئ	0.28%
ا	12.50%
آ	0.15%
أ	2.89%
إ	1.00%
ب	4.67%
ة	1.42%
ت	2.61%
ث	0.87%
ج	1.23%
ح	1.86%
خ	0.79%
د	2.67%
ذ	0.96%
ر	4.20%
ز	0.52%
س	2.47%
ش	0.73%
ص	1.04%
ض	0.44%
ط	0.50%
ظ	0.18%
ع	4.01%
غ	0.33%
ف	2.84%
ق	2.69%
ك	2.04%
ل	12.07%
م	6.52%
ن	6.61%
ه	5.08%
و	5.80%
ى	1.29%
ي	6.36%

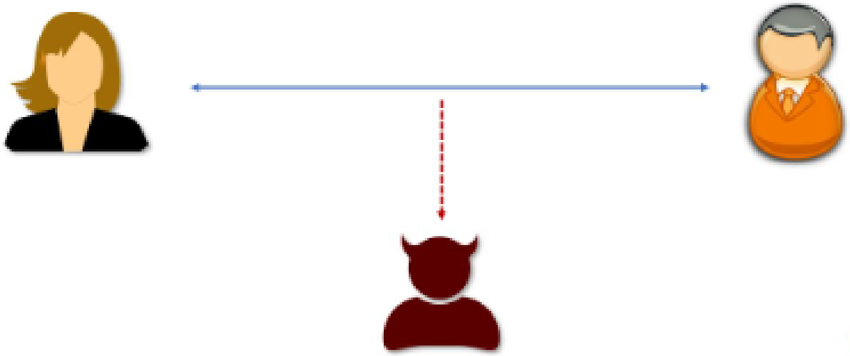
[1] Mička, Pavel. "Letter frequency (English)". *Algoritmy.net*. Archived from the original on 4 March 2021. Retrieved 14 June 2022.

Cryptanalysis

4) Protocol attack

- **Passive attack (listening to the channel):** involves collecting information, recovering a secret key, or observing the sender writing plaintext. This type of attack is very difficult to detect.

- **Active attack:** involves inserting messages, deleting messages, or destroying communication channels. The manner in which the attack is conducted depends on the network.



Encryption tools

There are two types of tools: Hardware and Software

PGP (Pretty Good Privacy)

Software encryption for documents, invented by Philippe Zimmerman

Features of PGP:

- PGP offered encryption keys of more than 1024 bits.
- PGP combines the best features of both conventional cryptography and public-key cryptography.

Algorithms used by PGP:

- The RSA public-key encryption algorithm (for signing and encryption),
- The IDEA secret-key encryption algorithm (for encryption),
- The MD5 one-way hash algorithm (for signing and authentication).

Encryption tools

Other tools

- GNU Privacy Guard (Windows/Mac/Linux)

Open-source implementation of PGP

- Disk Utility(Mac)

Encryption using AES 128 bits or 256 bits

- TrueCrypt(Windows/Mac/Linux)

Create and secure virtual disks

- AxCrypt(Windows)

Use AES 256 bits

- 7-zip(Windows)

Use AES 256 bits

PKI (Public Key Infrastructure)

Definition

- PKI is based on a **public key** encryption architecture
- It consists of a set of outsourced services that ensure better management of key criteria for network security, such as **authentication** and **integrity**. It ensures **confidentiality** as well as **non-repudiation** of information. These services are based on the concept of the **electronic certificate**

PKI (Public Key Infrastructure)

Key Management in PKI

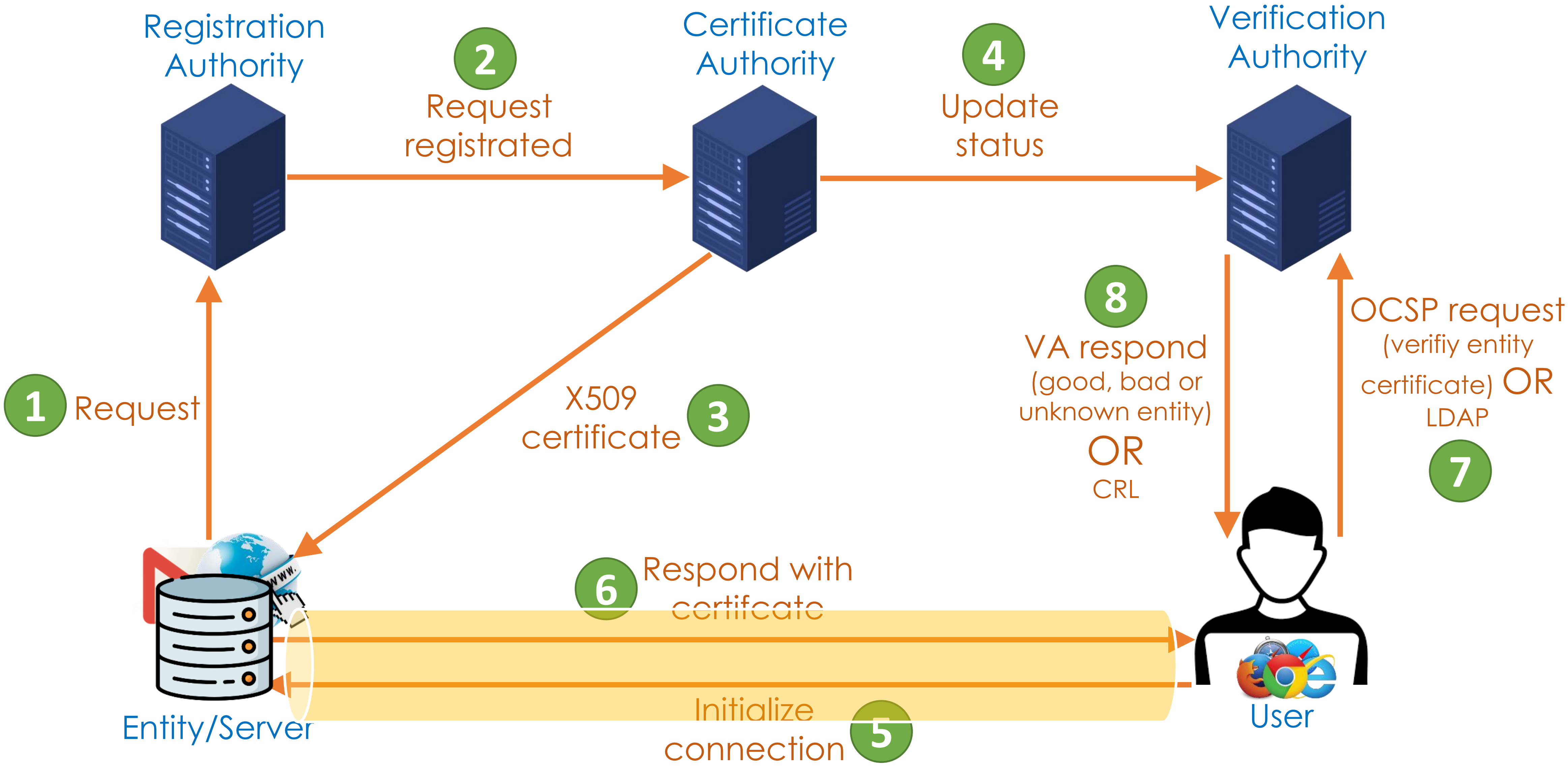
- Generation
- Distribution
- Storage
- Deleting
- Archiving
- Recovery

PKI (Public Key Infrastructure)

PKI Components

- **Registration Authority**
  - Verify the registration request of a new entity in the infrastructure
- **Certification Authority**
  - Generate the certificate for an entity, containing the public identity and the certificate validity period
- **Verification Authority**
  - Store valid or revoked certificates

PKI (Public Key Infrastructure)



Registration Authority
2
Request registrated
Certificate Authority
4
Update status
Verification Authority
8
VA respond (good, bad or unknown entity) OR CRL
OCSP request (verifiy entity certificate) OR LDAP
7
1
Request
X509 certificate
3
6
Respond with certifcate
Entity/Server
Initialize connection
5
User