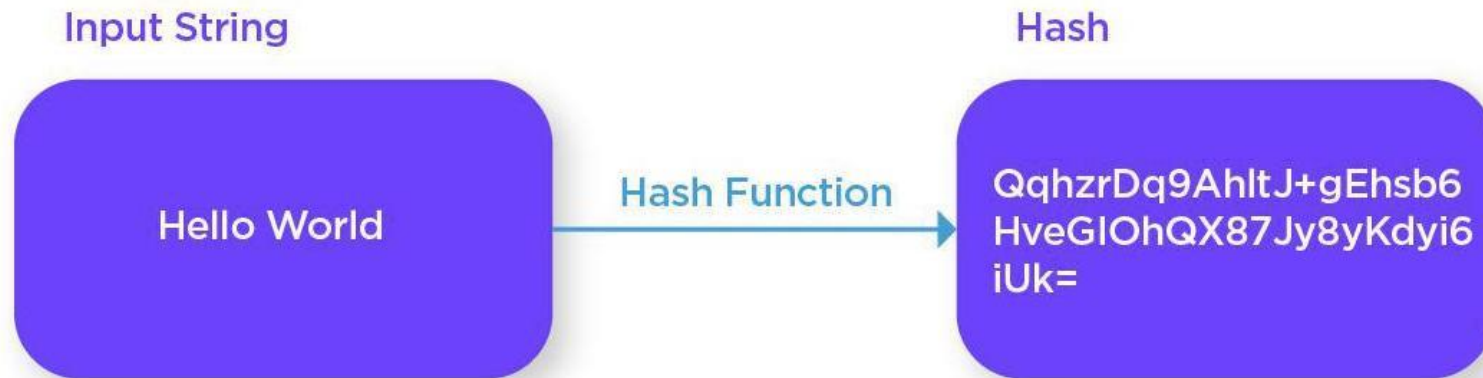


Hash function

Definition

- Mathematical compression function that converts a string of arbitrary length into a fixed-size string (often smaller, called a hash or digest).



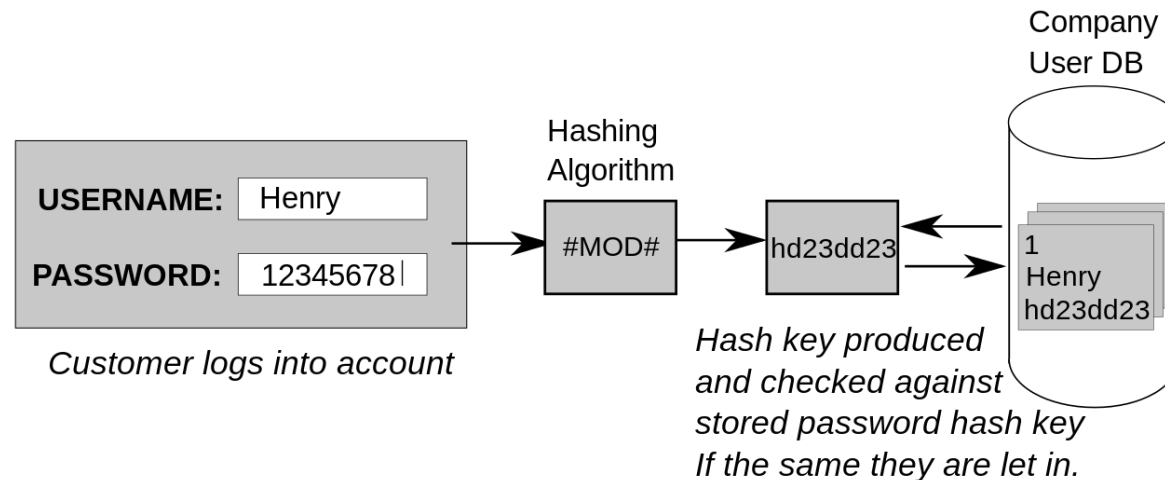
- It is easy to calculate the hash from an input string, but it is difficult to generate strings that have a specific hash

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/passwd** file. The same process applies for a web login



Hash function

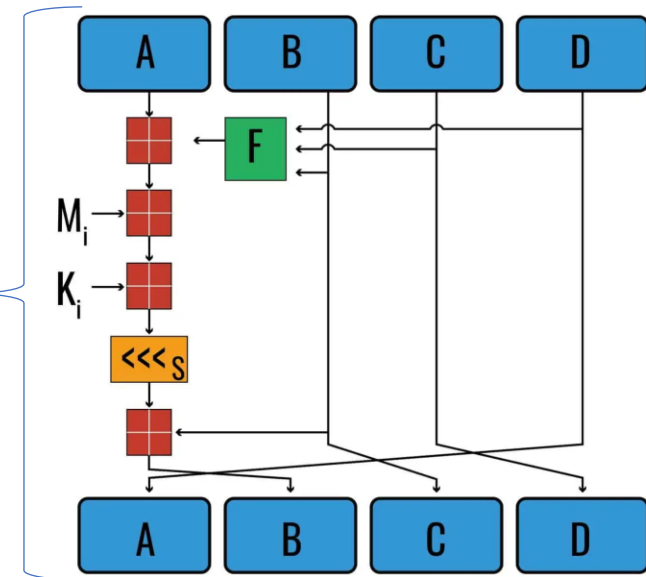
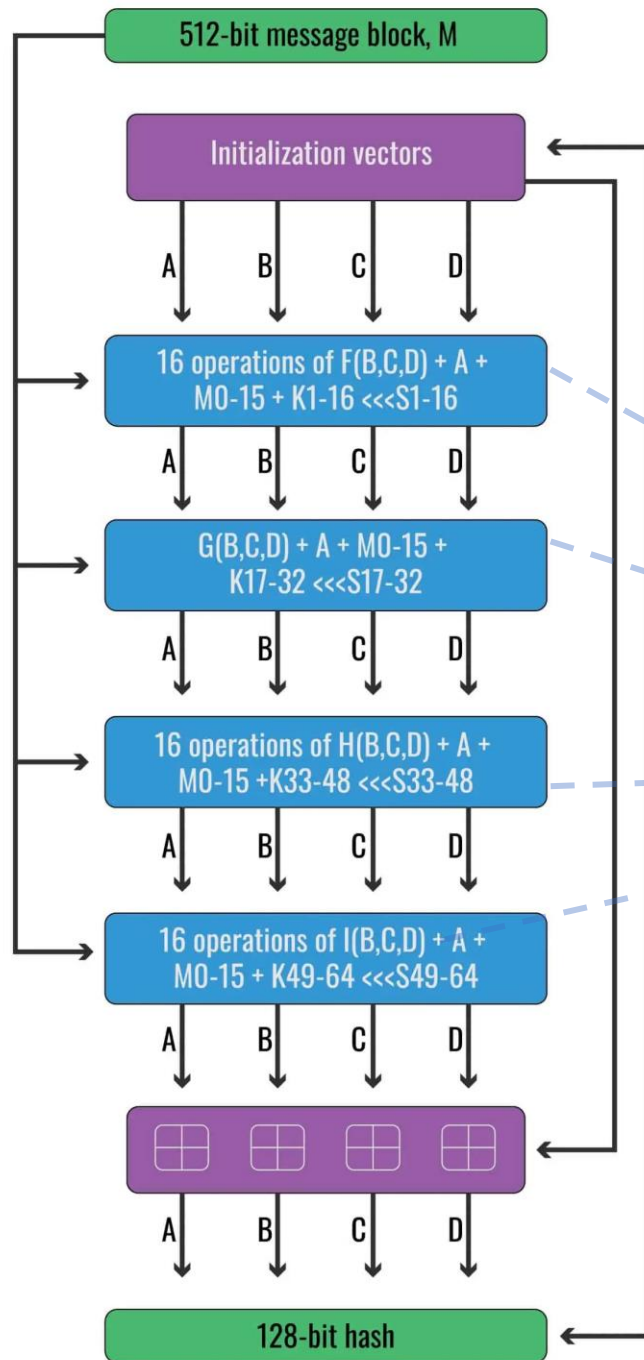
Hashing algorithms

- **MD2, MD4 and 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 and SHA2.** (Secure Hash Algorithm) :
 - Developed by NSA.
 - The two algorithms (SHA and SHA1) produce fingerprints of 160 bits for a message of two millions Terabytes long.
 - The size of its fingerprint makes it difficult to break, but it is slower than MD5.
- **Snefru** (128 and 256 bits), **N-Hash** (128 bits), ...

MD5

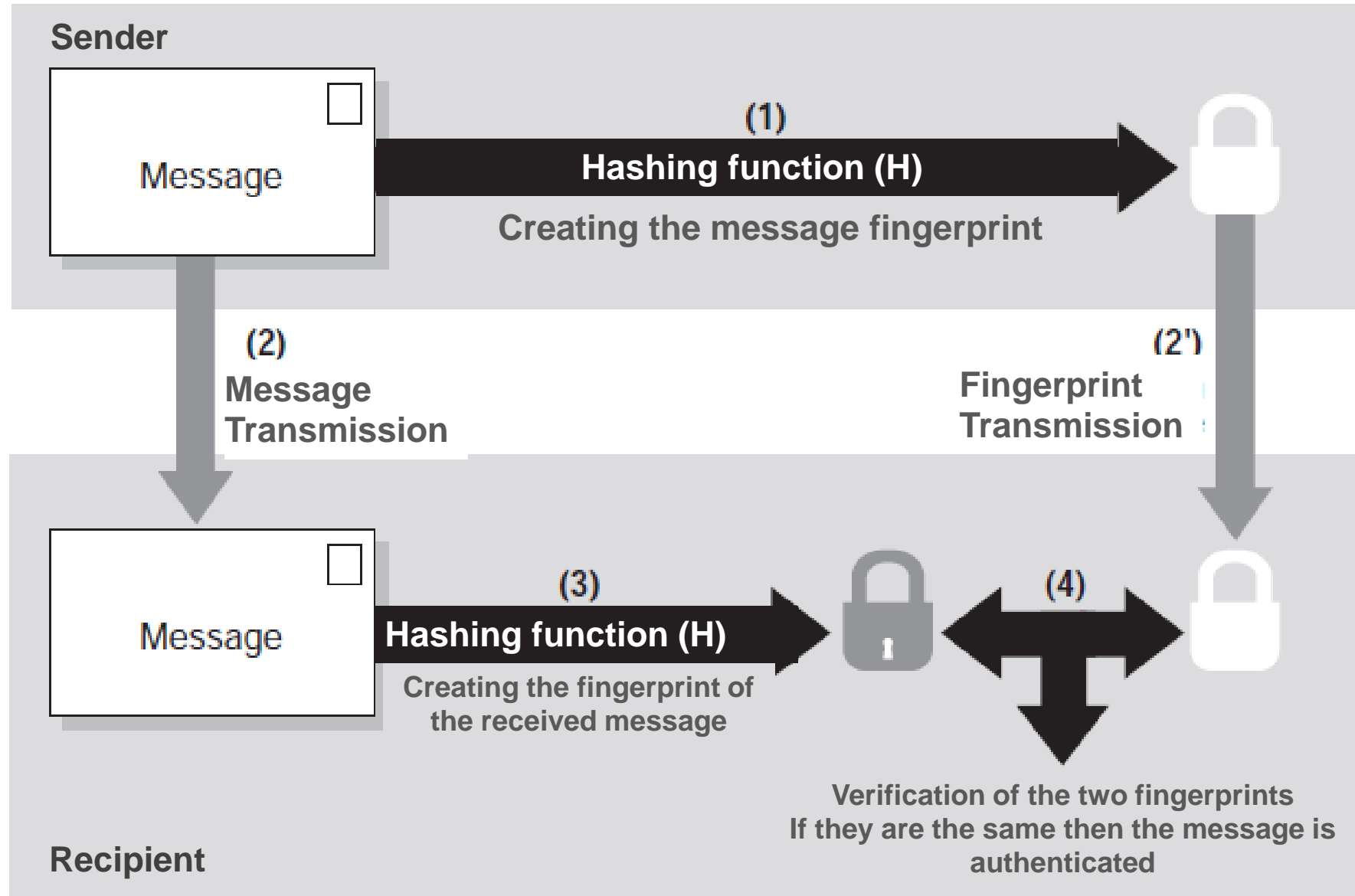
IV

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



Hash function

Integrity check



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

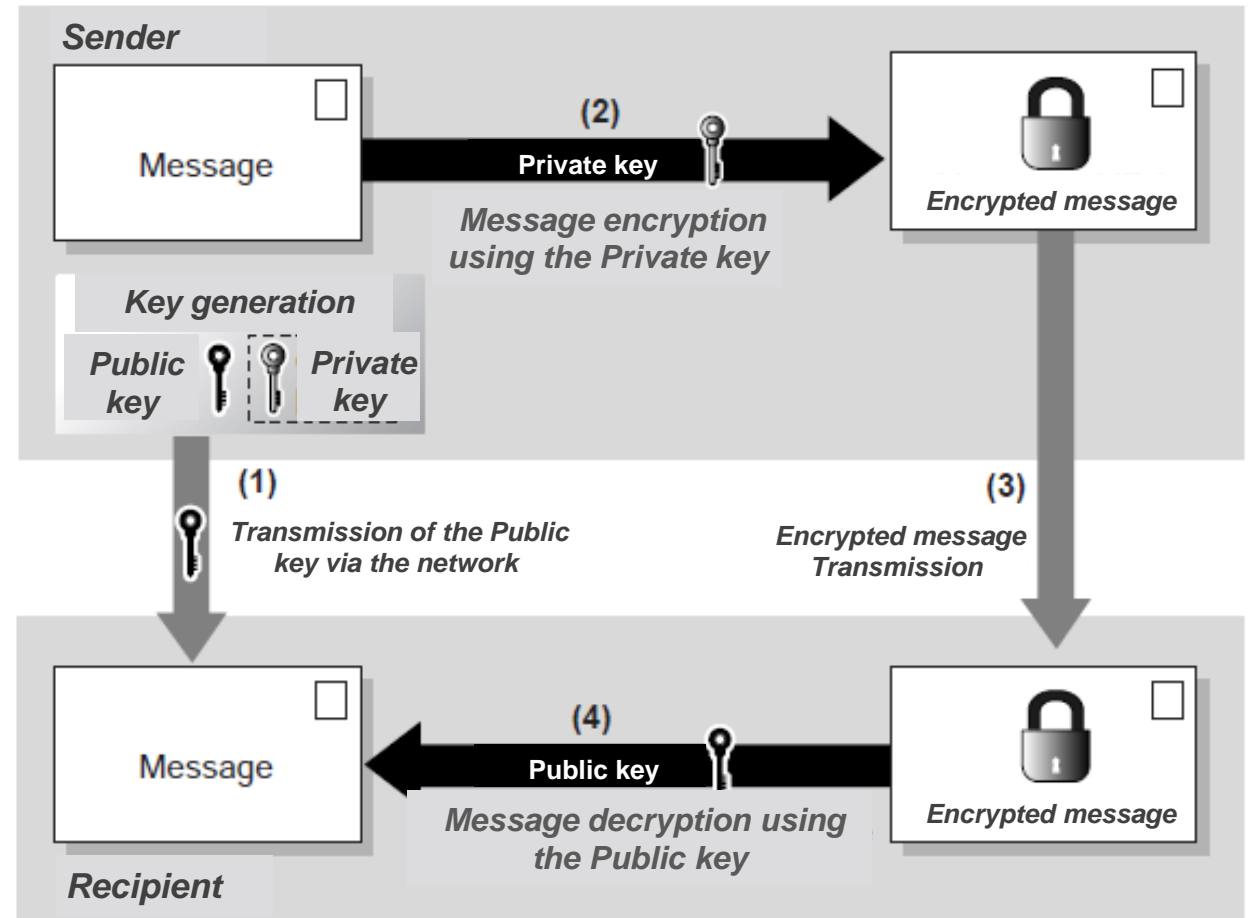
Creation et utilization

- 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:** $M = M^e \pmod n$

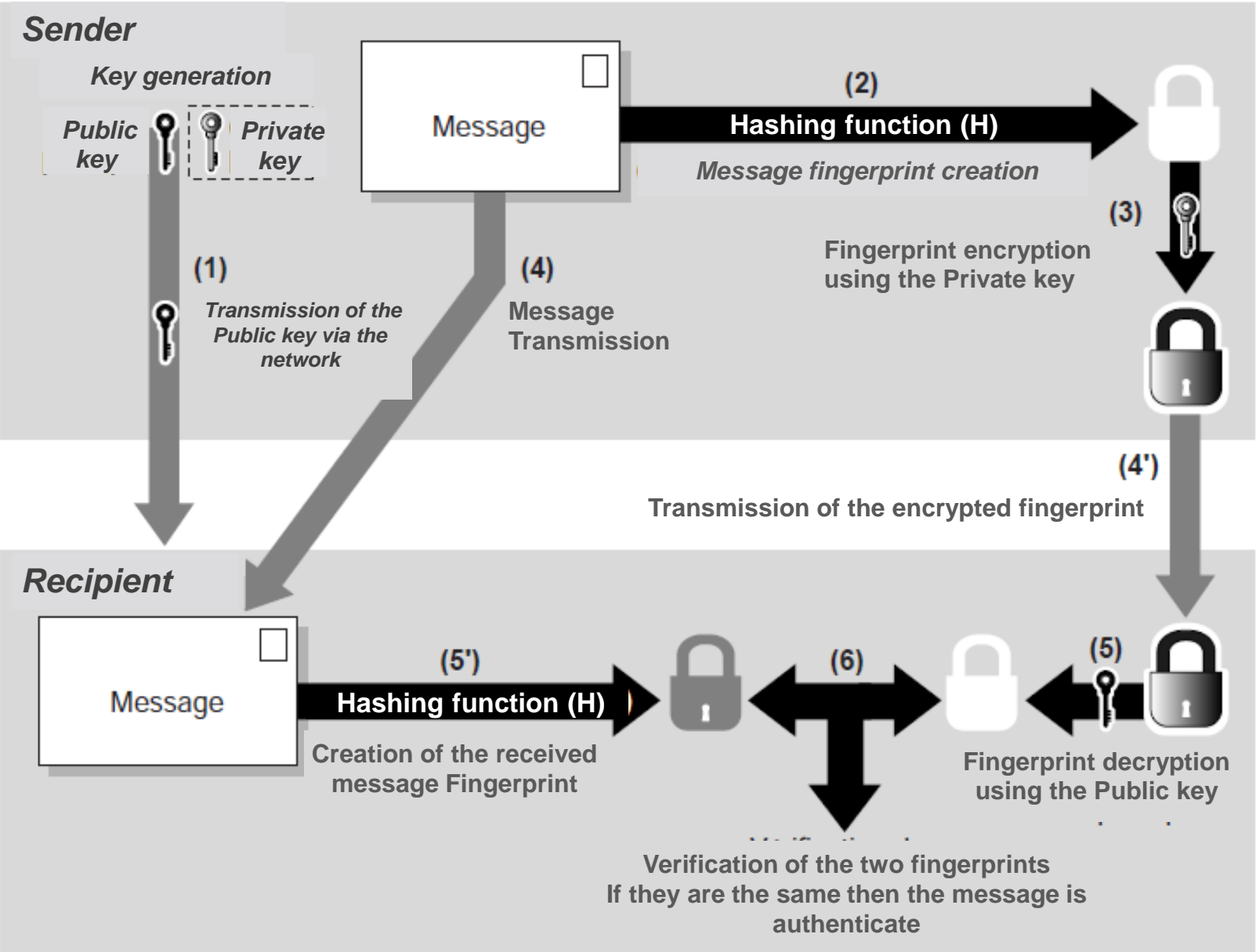
Digital Signature

- 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 data has not been altered and that it has indeed been sent by the sender.

Authentication using Public key



Combination of a hash function with public key encryption



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%	<div></div>	7.8%	<div></div>
B	1.5%	<div></div>	2.0%	<div></div>
C	2.8%	<div></div>	4.0%	<div></div>
D	4.3%	<div></div>	3.8%	<div></div>
E	12.7%	<div></div>	11.0%	<div></div>
F	2.2%	<div></div>	1.4%	<div></div>
G	2.0%	<div></div>	3.0%	<div></div>
H	6.1%	<div></div>	2.3%	<div></div>
I	7.0%	<div></div>	8.6%	<div></div>
J	0.15%	<div></div>	0.21%	<div></div>
K	0.77%	<div></div>	0.97%	<div></div>
L	4.0%	<div></div>	5.3%	<div></div>
M	2.4%	<div></div>	2.7%	<div></div>
N	6.7%	<div></div>	7.2%	<div></div>
O	7.5%	<div></div>	6.1%	<div></div>
P	1.9%	<div></div>	2.8%	<div></div>
Q	0.095%	<div></div>	0.19%	<div></div>
R	6.0%	<div></div>	7.3%	<div></div>
S	6.3%	<div></div>	8.7%	<div></div>
T	9.1%	<div></div>	6.7%	<div></div>
U	2.8%	<div></div>	3.3%	<div></div>
V	0.98%	<div></div>	1.0%	<div></div>
W	2.4%	<div></div>	0.91%	<div></div>
X	0.15%	<div></div>	0.27%	<div></div>
Y	2.0%	<div></div>	1.6%	<div></div>
Z	0.074%	<div></div>	0.44%	<div></div>

Letter ↕	Relative frequency in the Arabic language ↕	
ء	0.31%	<div></div>
أ	0.09%	<div></div>
إ	0.28%	<div></div>
آ	12.50%	<div></div>
أ	0.15%	<div></div>
إ	2.89%	<div></div>
!	1.00%	<div></div>
ع	4.67%	<div></div>
ة	1.42%	<div></div>
ن	2.61%	<div></div>
نا	0.87%	<div></div>
ج	1.23%	<div></div>
ح	1.86%	<div></div>
خ	0.79%	<div></div>
د	2.67%	<div></div>
ذ	0.96%	<div></div>
ر	4.20%	<div></div>
ز	0.52%	<div></div>
س	2.47%	<div></div>
ش	0.73%	<div></div>
ص	1.04%	<div></div>
ض	0.44%	<div></div>
ط	0.50%	<div></div>
ظ	0.18%	<div></div>
ع	4.01%	<div></div>
غ	0.33%	<div></div>
ف	2.84%	<div></div>
ق	2.69%	<div></div>

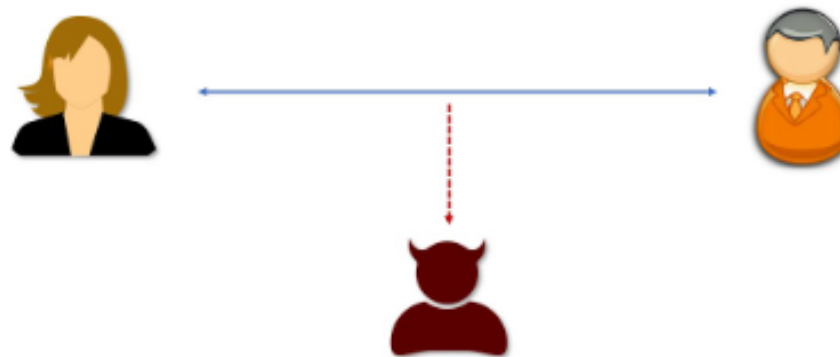
ك	2.04%	<div></div>
ل	12.07%	<div></div>
م	6.52%	<div></div>
ن	6.61%	<div></div>
ه	5.08%	<div></div>
و	5.80%	<div></div>
ى	1.29%	<div></div>
ي	6.36%	<div></div>

[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 Zimmermann

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)

