

Introduction à la Cryptographie



Mathieu Quittard - mathieu.qtrd@gmail.com

01

**Qu'est ce que
la
Cryptographie
?**

Qu'est ce que la Cryptographie ?

Définition : La cryptographie est l'art de protéger les informations en les transformant pour qu'elles soient illisibles pour des tiers non autorisés

- **Confidentialité** : Seuls les destinataires autorisés peuvent lire les données
- **Authentification** : Garantir l'identité de l'émetteur et du destinataire
- **Intégrité** : Vérifier que les données n'ont pas été modifiées pendant la transmission
- **Non-répudiation** : Empêcher un acteur de nier une action qu'il a réalisée

Historique de la Cryptographie

Les notions de cryptographie existent depuis l'antiquité !

Grèce antique

La scytale



Empire Romain

Le code de César



Renaissance Française

Le chiffre de Vigenère

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

Le Principe de Kerckhoffs

Les points fondamentaux de la cryptographie

1. Le système doit être matériellement, sinon mathématiquement indéchiffrable
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi
3. La clef doit pouvoir être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants
4. Il faut qu'il soit applicable à la correspondance télégraphique
5. Il faut qu'il soit portatif et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes
6. Il faut que le système soit d'un usage facile

02

Les protocoles de chiffrement

Les protocoles SSL et TLS

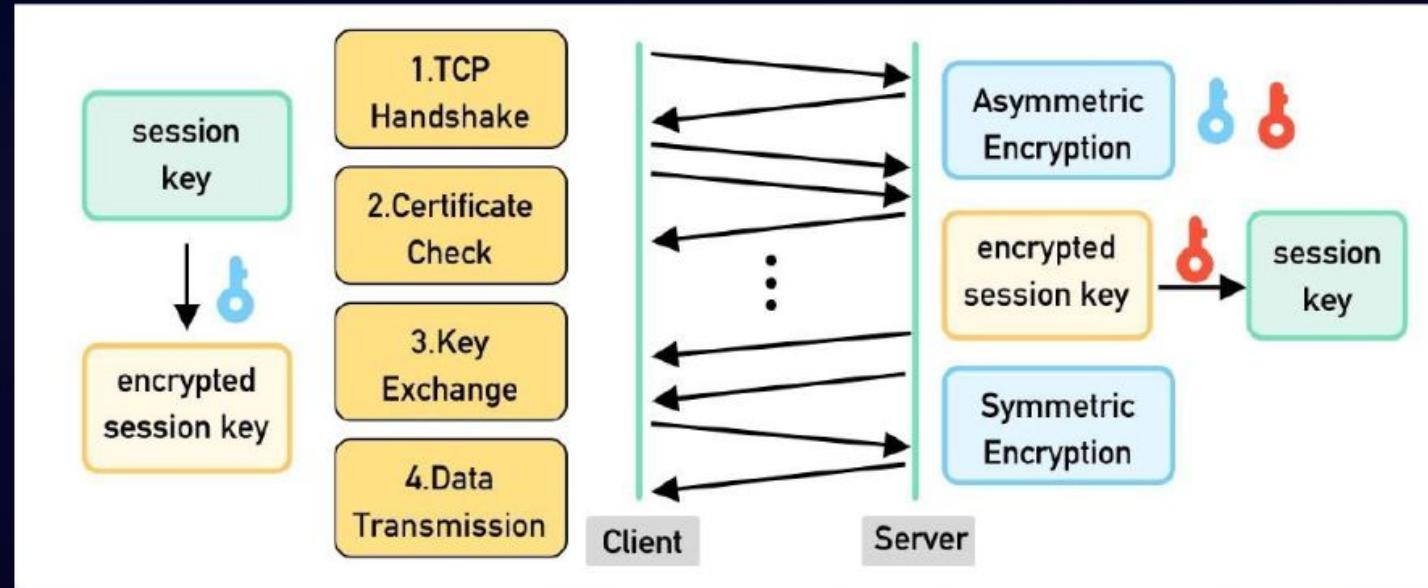
SSL

: Secure Sockets Layer

TLS : Transport Layer Security

- **SSL** : Développé par Netscape en 1995
 - Sécurité des connexions internet entre deux systèmes, protège les données par chiffrement
- **TLS** : Développé par l'IETF (Internet Engineering Task Force) en 1999
 - Version améliorée du SSL, règle les problèmes de faille de sécurité telles que le middle-man
 - Le TLS implémente la notion d'identification des deux parties par des certificats numériques
- Lorsque l'on parle basiquement des protocoles SSL, on parle en réalité d'un mix de ces deux protocoles

Le concept du Handshake



Le protocole HTTP/HTTPS

HTTPS

: HyperText Transfer Protocol Secure

- C'est une extension sécurisée de HTTP
- HTTPS indique que notre site utilise des chiffrements sécurisés SSL/TLS
- C'est à activer simplement sur l'hébergement

03

La manipulation avec OpenSSL

Qu'est ce que OpenSSL ?

OpenSSL : Bibliothèque open source et outil de ligne de commande pour mettre en place des protocoles de cryptographie

Principaux rôles :

- Chiffrement et déchiffrement
- Génération de clés
- Certificats
- Hachage

Les suites cryptographique

Suites Cryptographique

:

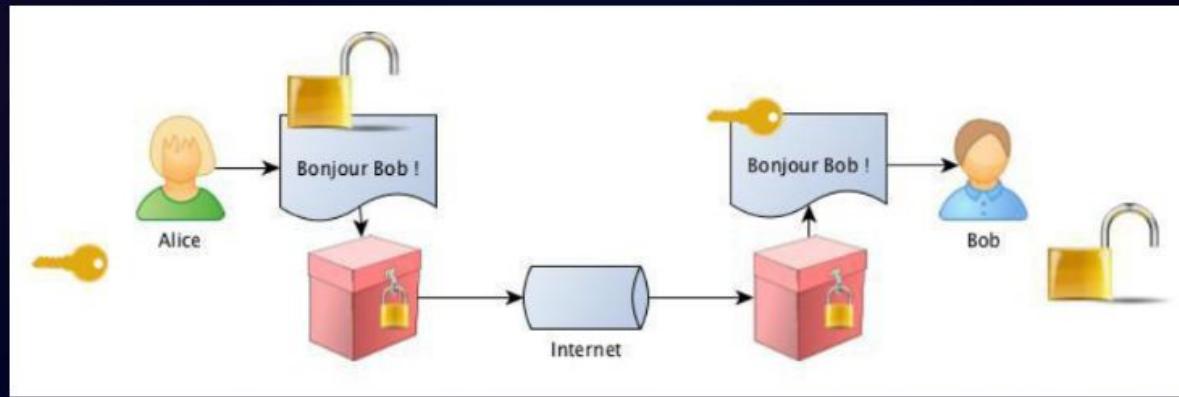
Ensemble de méthodes ou algorithmes utilisés conjointement pour assurer la sécurité des communications

Composants d'une suite cryptographique :

- Algorithme d'échange de clés (RSA, DH, ECDH)
- Algorithme de chiffrement (AES, ECIES)
- Fonction de hachage (SHA-256, MD5)
- MAC (Message Authentication Code)

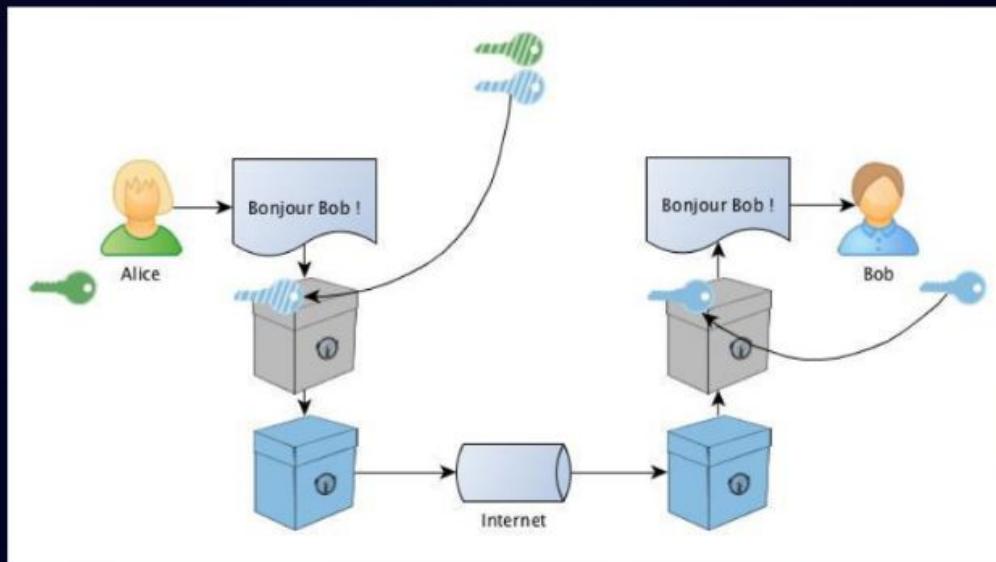
Le chiffrement symétrique

Une seule clé utilisée pour le chiffrement et le déchiffrement



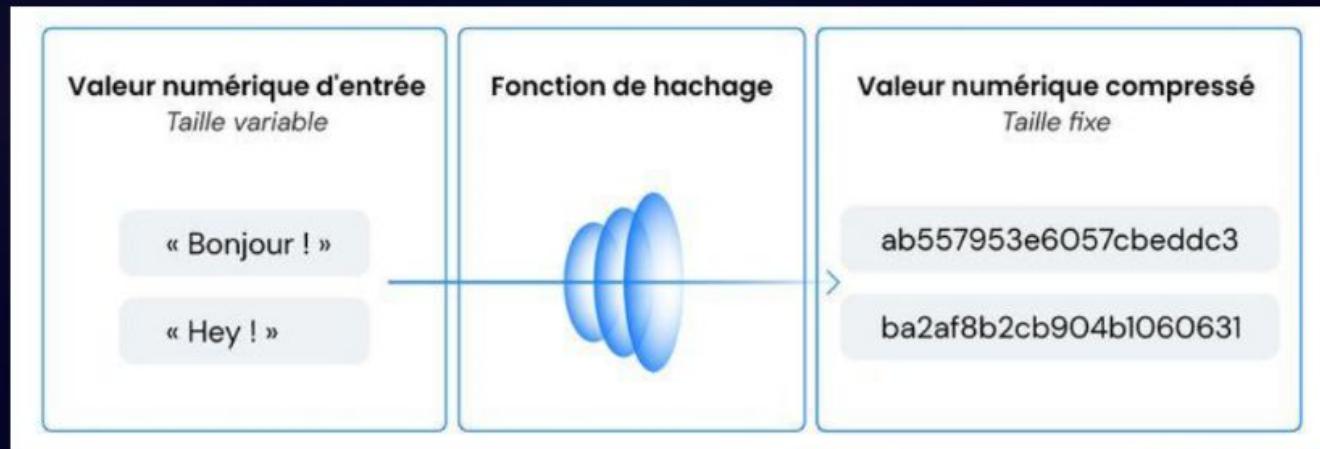
Le chiffrement asymétrique

Utilise une paire de clé, une publique pour chiffrer, une privée pour déchiffrer



Le hachage

Transformation unidirectionnelle des données



Exemples de manipulation

- En lignes de commande :

- Affichage de version OpenSSL : `openssl version`
- Liste des algorithmes utilisables : `openssl list -cipher-algorithms`
- Encoder un fichier : `openssl enc -e -algorithme -in fichieracrypter -out fichierensortie`
- Décoder un fichier : `openssl enc -d -algorithme -in fichiercrypt -out fichierclairensortie`
- Création d'une clé symétrique : `openssl enc -aes-256-cbc -k "ma_clé_secrète" -nosalt -out ma_clé.bin`

Exemples de manipulation

- En PHP via les fonctions openssl intégrées :

```
// Génération d'une paire de clés RSA de 2048 bits
$result = openssl_pkey_new(
    [
        "private_key_bits" => 2048,
        "private_key_type" => OPENSSL_KEYTYPE_RSA
    ]
);

// Exportation de la clé privée au format PEM
openssl_pkey_export($result, $private_key);
file_put_contents('ma_cle_privee.pem', $private_key);

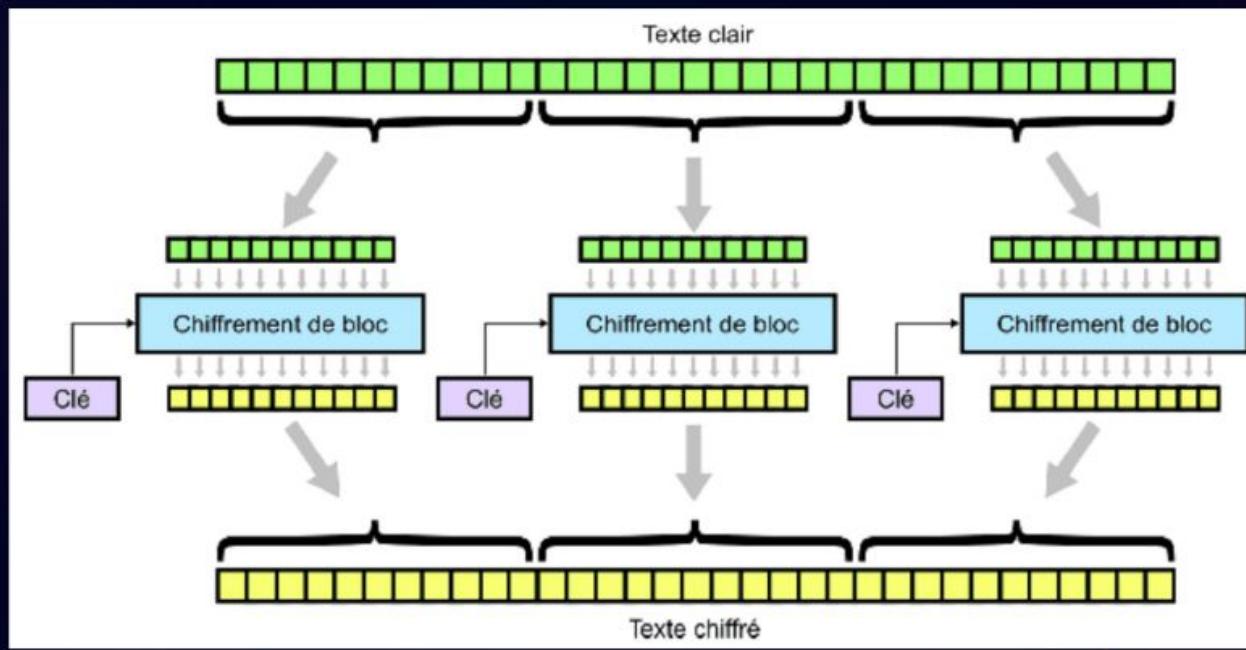
// Exportation de la clé publique au format PEM
$public_key = openssl_pkey_get_public($result);
openssl_pkey_export($public_key, $public_key_pem);
file_put_contents('ma_cle_publique.pem', $public_key_pem);

// Chiffrement et déchiffrement
$data = "Message à chiffrer";
openssl_public_encrypt($data, $encrypted, file_get_contents("ma_cle_publique.pem"));
echo base64_encode($encrypted);

$encrypted = base64_decode("le_message_chiffre_en_base64");
openssl_private_decrypt($encrypted, $decrypted, file_get_contents("ma_cle_privee.pem"));
echo $decrypted;
```

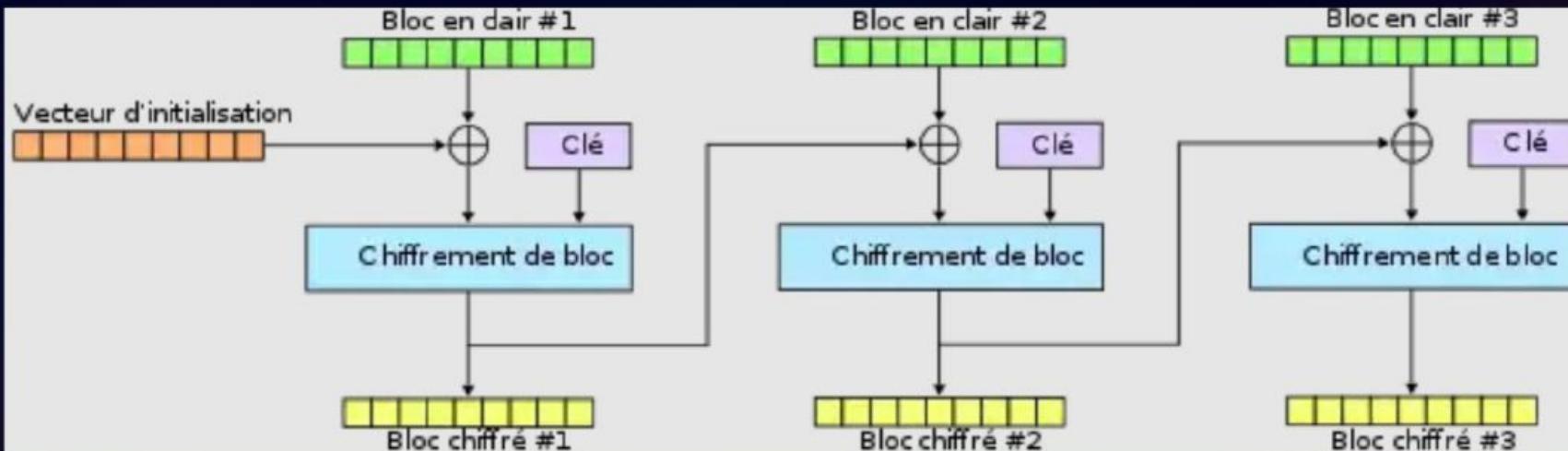
Les modes de chiffrement

ECB - Electronic CodeBook



Les modes de chiffrement

CBC - Cipher Block Chaining

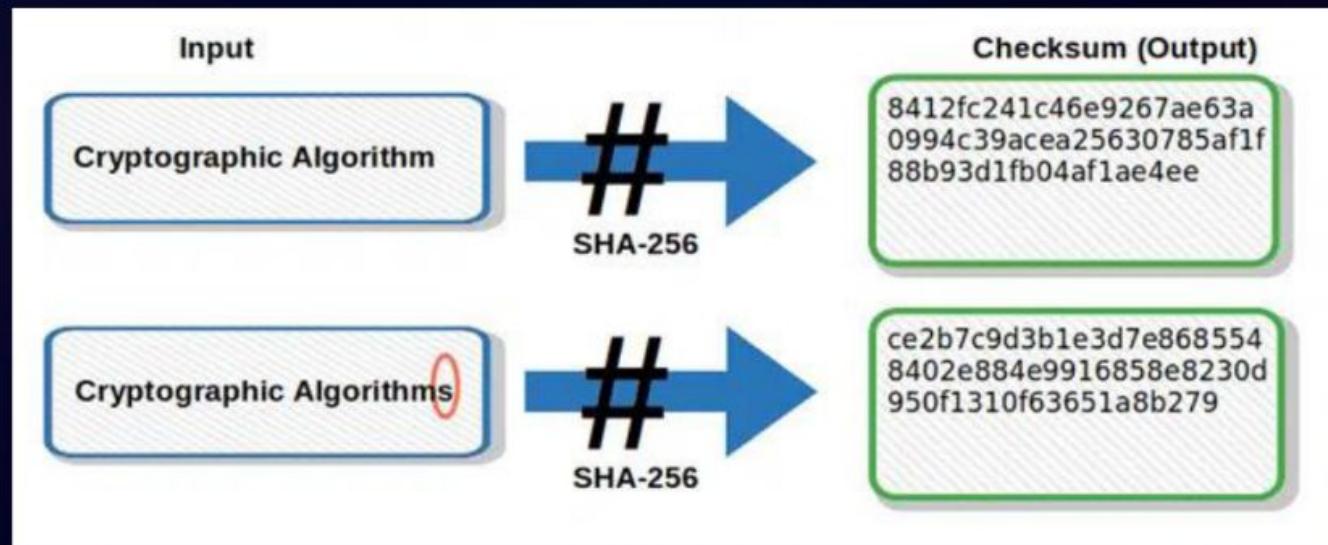


04

Vérification de l'intégrité et fiabilité des données

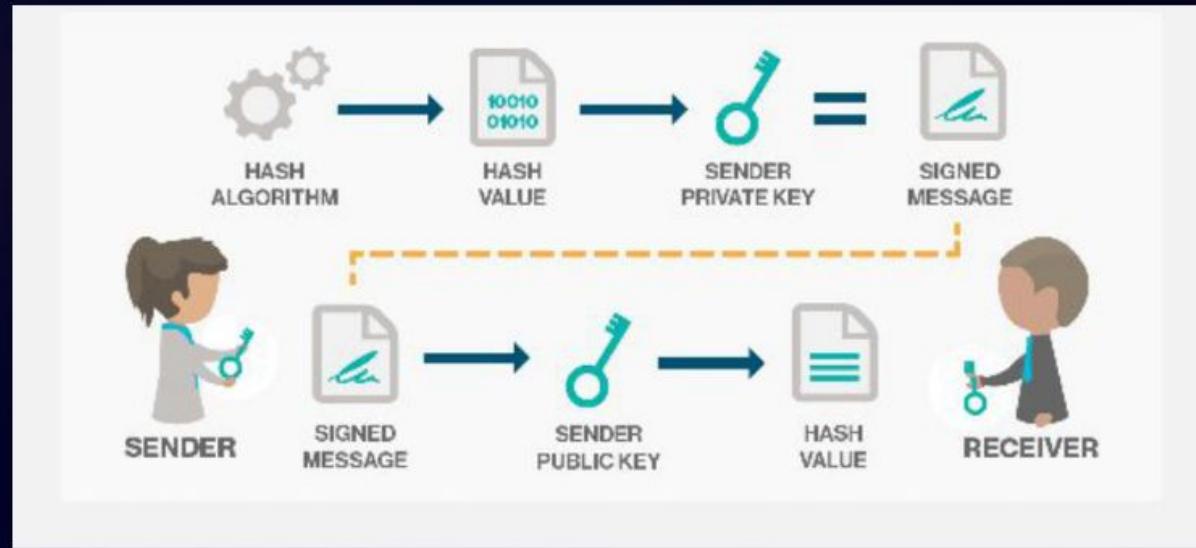
La somme de contrôle - checksum

Permet de vérifier si un fichier n'a pas été altéré entre le client et le serveur



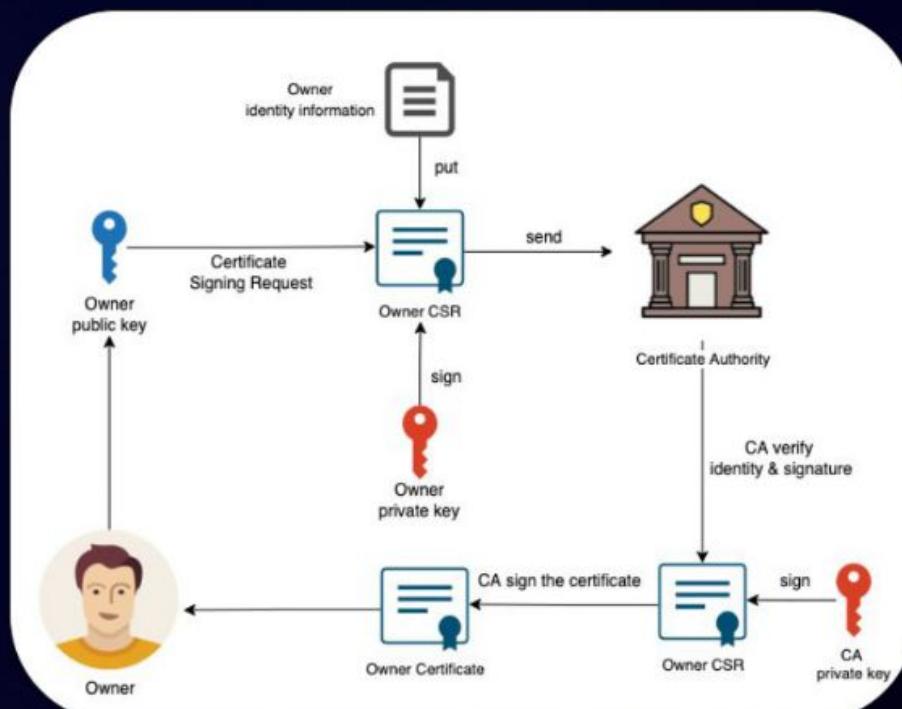
Les signatures numériques

Permet de vérifier l'authenticité et l'intégrité d'un document numérique



Les certificats

Permet de vérifier l'identité d'un système et prouver son "innocence"



05

Séparation des responsabilités

Responsabilité de l'hébergeur / Ops Team

- Gestion des certificats SSL/TLS
- Mise en place du HTTPS
- Chiffrement des connexions
- Stockage des données chiffrés au niveau matériel
- Sécurisation des clés privés

Responsabilité du développeur

- Chiffrement des données sensibles
- Hachage des passwords
- Stockage sécurisé des clés
- Choix des algorithmes

Ce que l'on retient

Les principes

- Confidentialité
- Intégrité
- Authentification

Les outils courants

- Chiffrement symétrique
- Chiffrement asymétrique
- Hachage

La responsabilité partagée

- Le serveur configure correctement les certificats
- Le développeur implémente correctement les outils de sécurité

Merci !

Introduction à la Cryptographie

Mathieu Quittard -
mathieu.qtrd@gmail.com

CREDITS: This presentation template was created by [Slidesgo](#), and includes icons by [Flaticon](#), and infographics & images by [Freepik](#)

