Cours 8 :

La cryptographie

JACQUEMIN Mathieu

Disclaimer

- Ce cours a été créé dans le but d'informer et d'éduquer les participants sur les sujets liés à la cybersécurité. L'ensemble des techniques présentées le sont à titre pédagogique et préventif afin de pouvoir se prémunir d'attaque potentiel.
- Certaines des techniques présentées sont illégales et dangereuses si elles sont utilisées à mauvais escient, sans maitrise, et sans consentement.
- Il est interdit d'utiliser ces techniques contre toute entité dont vous ne disposez pas le consentement. Dans le cadre d'un accord pour audit, il est obligatoire d'agir dans le cadre d'un contrat parfaitement défini, écrit, et signé par les deux parties.
- Vous devez respecter la loi en vigueur ainsi qu'utilisez les techniques avec éthique et responsabilité.
- Je me dédouane de toute responsabilité en cas de problème ou d'incidents à la suite de ce cours.
- Vous êtes seul responsable de l'usage fait des connaissances enseignées.

Définition

Cryptographie :
Qui comprend l'ensemble des méthodes de protection d'une information

Elle sert à garantir la confidentialité, l'authenticité et l'intégrité d'une information lors de communications ou lors de son stockage, en utilisant le chiffrement

Du grec kruptos qui signifie « caché »

Le chiffrement

La Confidentialité : On veut que personne ne puisse voir le message sur le trajet.

L'authenticité : Être sûr de l'expéditeur.

L'intégrité : Être sûr que le message n'a pas été modifié en cours de route.

Ne pas confondre

Cryptologie : Science du secret
Qui se compose de 2 disciplines

Cryptographie, que nous venons de définir

Cryptanalyse :

Méthodes utilisées pour analyser les messages chiffrés et « casser » la protection cryptographique de ces messages


Pause
00:00

Vocabulaire

Le chiffrement : C'est la transformation d'une information claire en une information chiffrée, incompréhensible, mais que l'on peut déchiffrer avec une clé pour obtenir l'information en clair originale

Le système de chiffrement est composé d'algorithmes de chiffrement et déchiffrement, et d'une clé de chiffrement

Un texte en clair est une information non protégée et compréhensible par tout le monde

Un texte chiffré est une information incompréhensible pour qui ne possède pas la clé de déchiffrement mais que l'on peut déchiffrer, retransformer en texte clair, si on possède la clé

Vocabulaire

Un algorithme de chiffrement est une fonction qui prend en entrée le texte clair et la clé de chiffrement, transforme le texte par des opérations, et fournit en sortie un texte chiffré

L'algorithme de déchiffrement est la fonction inverse, qui prend en entrée le texte chiffré et la clé de déchiffrement, transforme ce texte par des opérations, et fournit en sortie le texte clair d'origine

La clé de chiffrement est l'information qui permet de transformer un texte clair en texte chiffré en utilisant un algorithme de chiffrement. De même, la clé de déchiffrement est l'information qui permet de transformer un texte chiffré en son texte clair d'origine

Disclaimer

Les termes "crypter", "encrypter" et "messages cryptés", que vous entendrez parfois, n'existent pas dans la langue française et sont des anglicismes.

En anglais, chiffrer se dit encrypt et déchiffrer se dit decrypt.

Decrypt est un faux-ami du verbe français décrypter car il signifie précisément "retrouver le texte clair sans connaître la clé de déchiffrement", alors que déchiffrer signifie "retrouver le texte clair en utilisant la clé de déchiffrement".

Un système de chiffrement se dit cipher en anglais et un texte chiffré est appelé ciphertext.

Les origines

La cryptologie est utilisée depuis l'antiquité, principalement dans le domaine militaire

Scytale spartiate

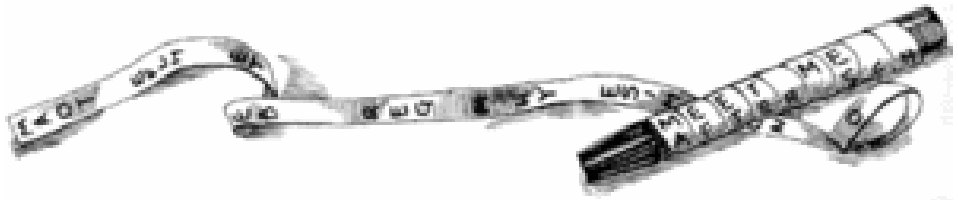
Le chiffre de césar (chiffrement par décalage)

Le chiffre de Vigenère

Machine Enigma

La scytale spartiate

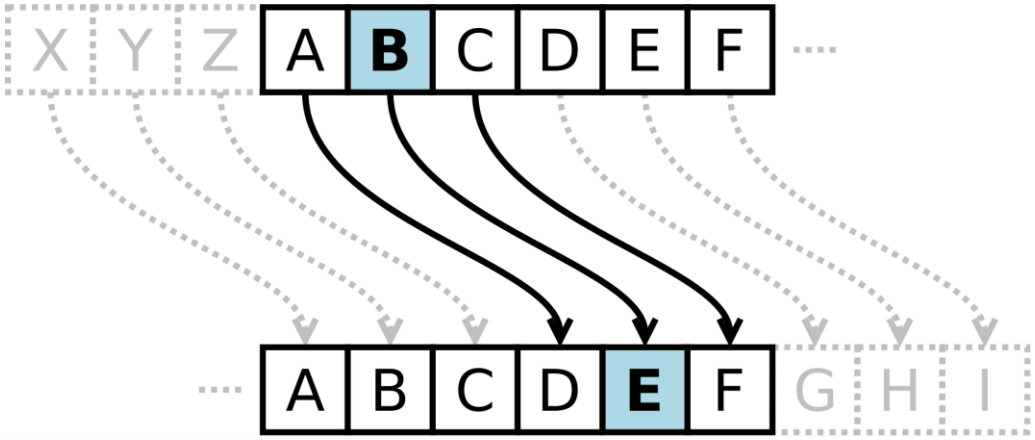
Utilisation d'un bâton de bois pour lire ou écrire un texte chiffré



Considéré comme le plus ancien dispositif de cryptographie militaire

Le chiffre de césar

Consiste à décaler chaque lettre d'un message clair par la lettre de l'alphabet située à une distance fixée



Par exemple, le message clair:

ATTAQUEZ A L AUBE

Est transformé avec une distance de 3 en message chiffré :

DWWDTXHC D O DXEH

Utilisé par Jules César pendant la guerre des Gaules. Il est aussi appelé chiffrement par décalage

Le chiffre de Vigenère

	Lettre en clair																								
	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
Lettre de la clé	Lettres chiffrées (au croisement de la colonne *Lettre en clair* et de la ligne *Lettre de la clé*)																								
A	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	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	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	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	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	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	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	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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	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
U	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
V	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
W	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
X	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
Y	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
Z	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

La clé est une séquence de lettres et elle définit le décalage pour chaque lettre

Utilisation de 26 alphabets

Par exemple, le message clair avec la clé « RABELAIS » :

SCIENCE SANS CONCIENCE N EST QUE RUINE DE L AME
+ RABELAIS RABELAIS RABELAIS RABELAIS RABELAIS RABE

= JCJIYCM KRNT GZNAUZEOGP N MKK QVI CUQFV DF P LMM

Enigma

Utilisé durant la 2nd Guerre Mondiale par les Allemands, même si les alliés ont réussi à déchiffrer certains messages

Machine électromécanique portable utilisant des rotors pour le chiffrement et le déchiffrement

Chiffrement symétrique

Utilisation de la même clé, appelée « privée » pour chiffrer et déchiffrer

Algorithmes existants : AES, DES, RC5…

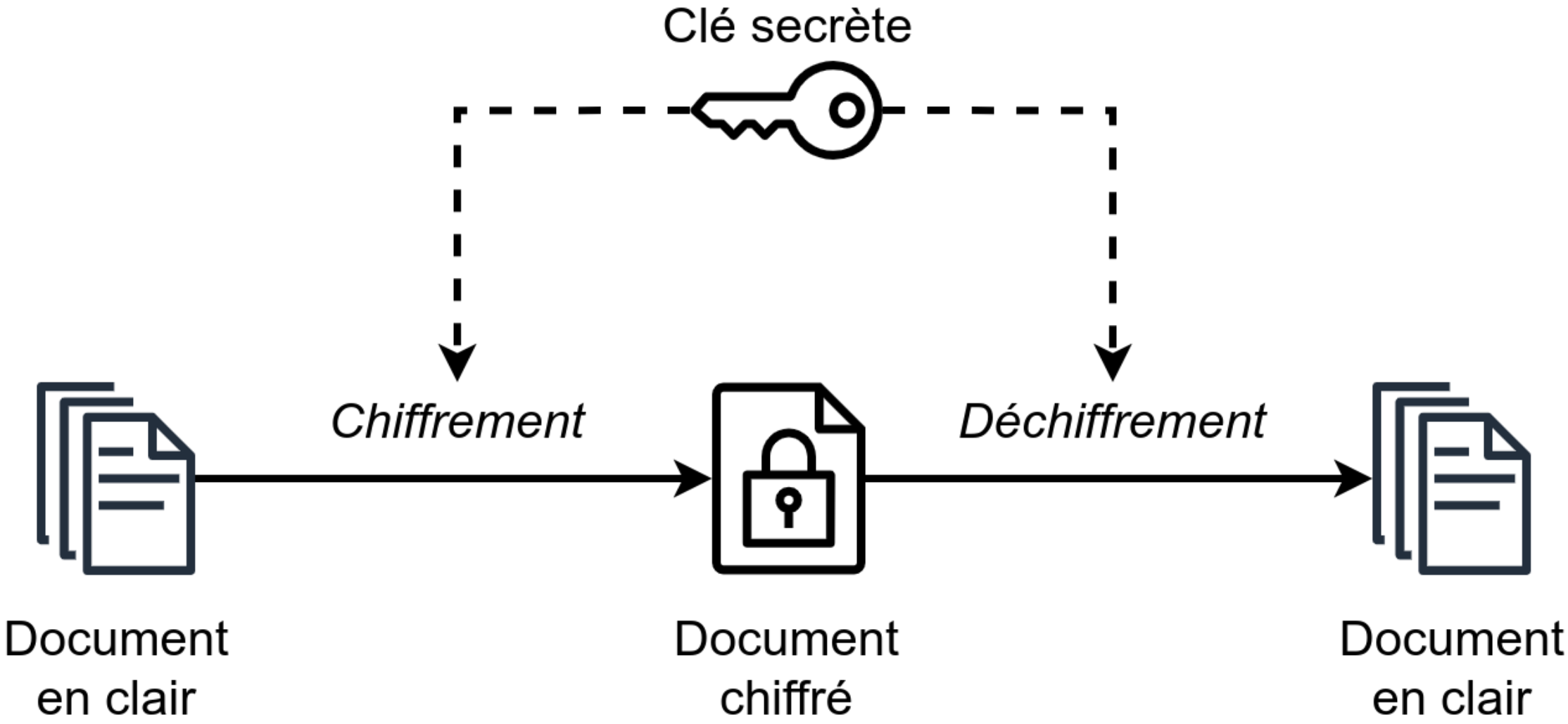
Avantages:

- Facile à mettre en œuvre
- Plus rapide
- Moins gourmand en ressources

Inconvénients:

- La perte d'une clé signifie que les données sont compromises
- La clé doit être partagée en toute sécurité

Chiffrement symétrique



Chiffrement asymétrique

Utilisation d'une clé publique pour chiffrer et une clé privée pour déchiffrer

Algorithmes existants : RSA, ECC, DSA...

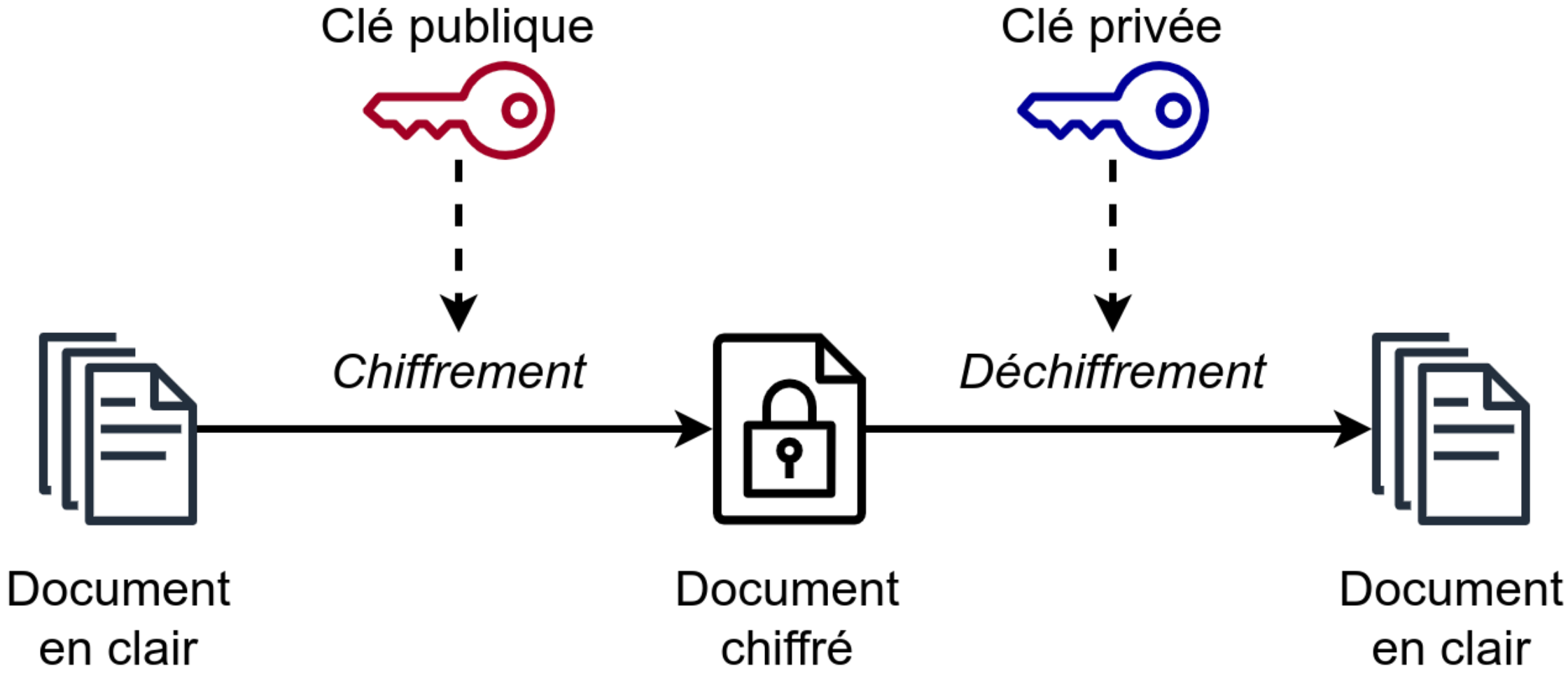
Avantages:

- Les données ne peuvent être déchiffrées qu'à l'aide de la clé privée
- En cas de perte ou vol de la clé publique, les données ne sont pas compromises

Inconvénients:

- Plus lent que le chiffrement symétrique
- Utilise plus de ressources
- En cas de perte de la clé privée, aucun moyen de la récupérer

Chiffrement asymétrique



Les certificats

Il permet d'associer une clé publique à une entité afin d'en assurer sa validité

Il s'agit d'un fichier contenant :

- **La clé publique**
- **Informations sur la personne**
- **Informations sur le certificat**
- **Signature électronique d'une autorité de certification**

Le Hachage

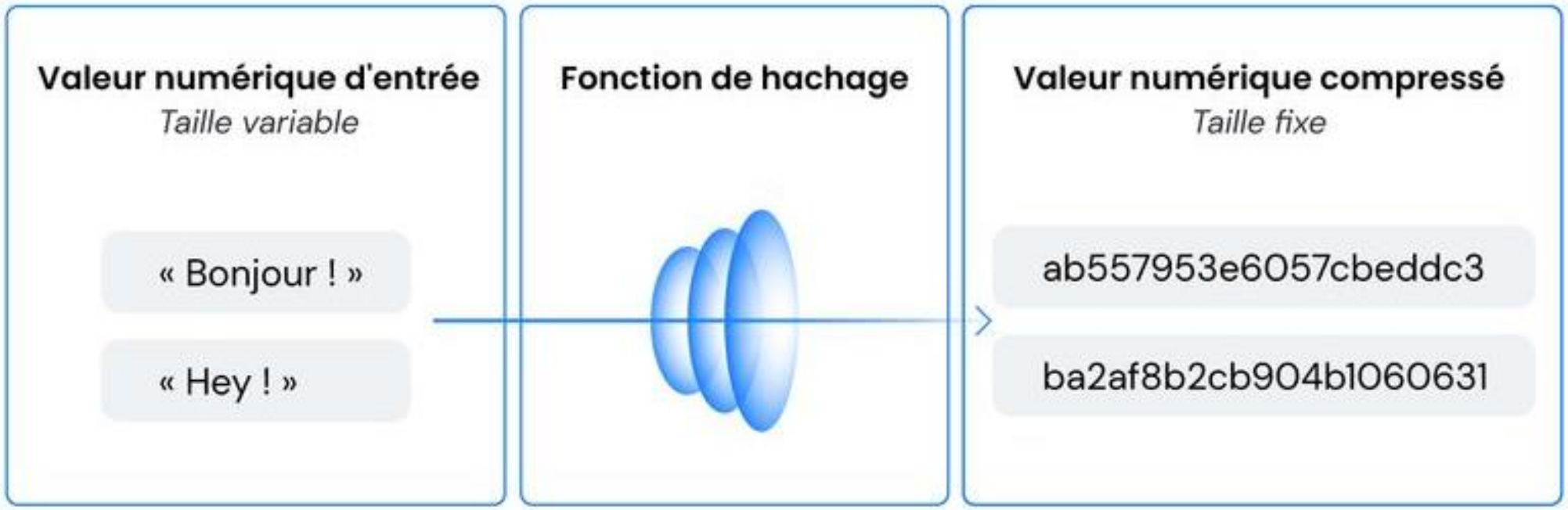
Vérifier l'intégrité d'un fichier ou une signature numérique

Transforme un message clair en une donnée unique appelée empreinte. Il n'est pas possible de retrouver le message clair en partant de l'empreinte.
Le hachage est irréversible !

Permet de ne pas stocker des mots de passe en clair mais uniquement de stocker une empreinte de ces derniers

Algorithmes existants : MD5, SHA1, SHA256, SHA-512...

Le Hachage


Valeur numérique d'entrée
Taille variable
« Bonjour ! »
« Hey ! »
Fonction de hachage
Valeur numérique compressé
Taille fixe
ab557953e6057cbeddc3
ba2af8b2cb904b1060631


SHA-256
9578C1ea7cd3b312
9efea270c64e0d16
37f6184f325b58e1
d02e95829d03ba6c

Exercices