

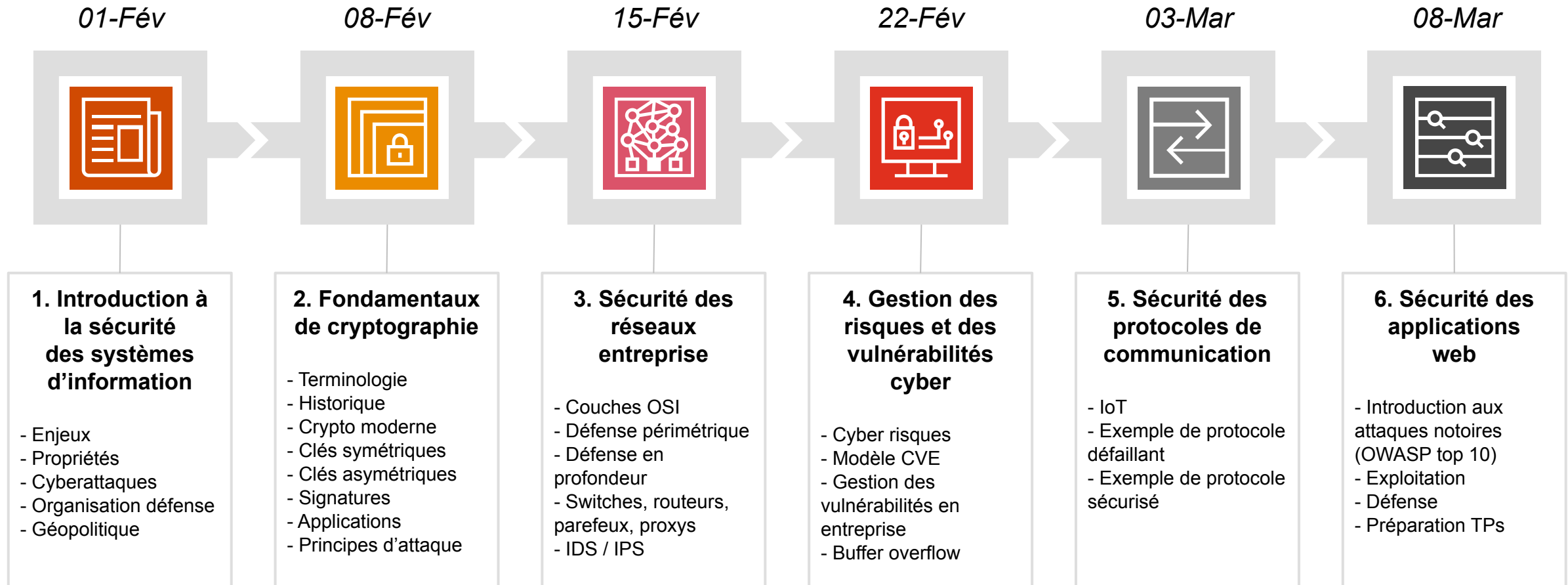
Cursus ENSEEIHT/2SN

2. Fondamentaux de cryptographie

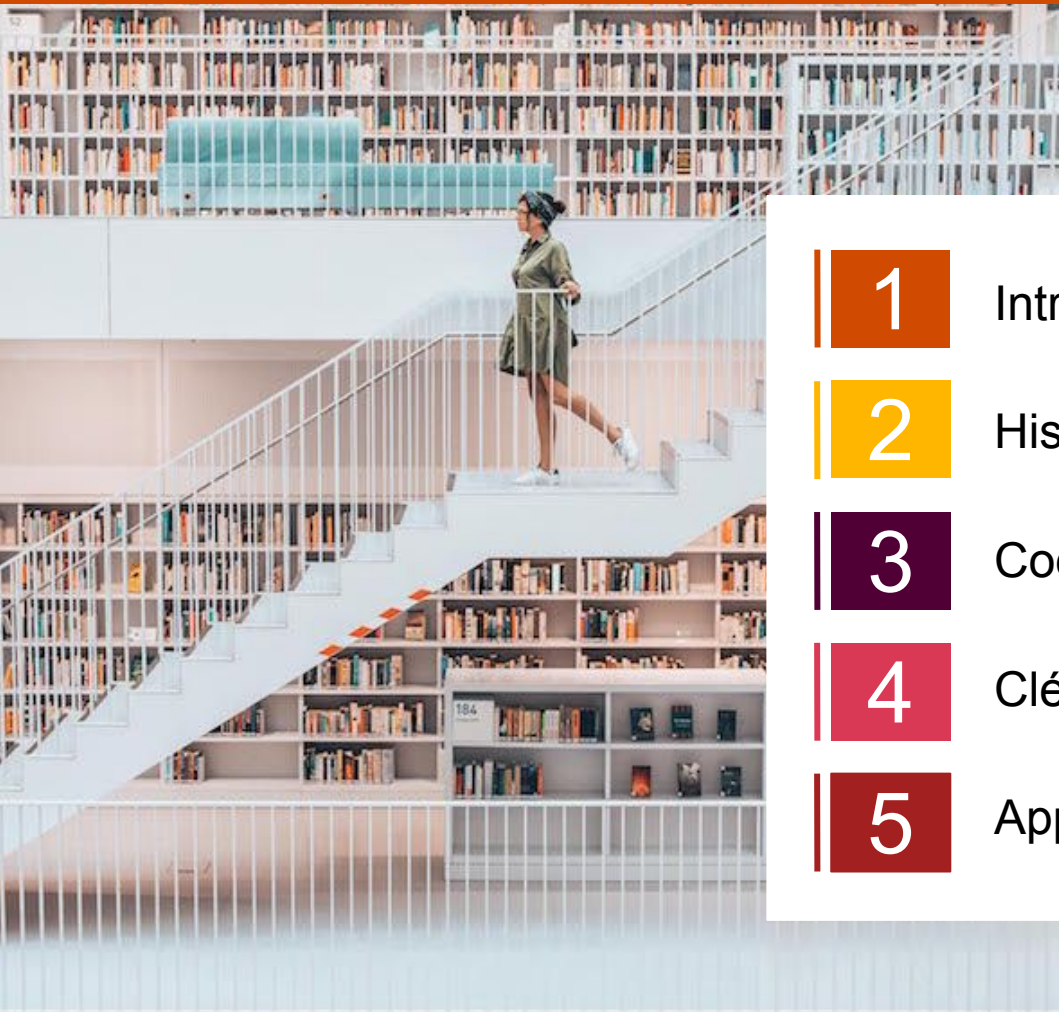
Février 2022



Déroulement du module



Agenda



- 1 Introduction et terminologie
- 2 Historique
- 3 Codes modernes: chiffrement par flux / blocs
- 4 Clés symétriques & Clés asymétriques
- 5 Applications de la cryptographie

The background features a large orange number '1' on the left. A dark grey horizontal rectangle is positioned in the upper-middle section, containing the text 'Introduction et terminologie'. To the right of this rectangle is an orange square with a white border. Below the rectangle is a white circle. Further right is a white square. In the bottom right corner, there is a white quarter-circle arc. The overall design is minimalist and geometric.

Introduction et terminologie

Qu'est ce que la cryptographie ?

Cryptographie et Stéganographie

Stéganographie

- Etymologie grecque “**steganos**” = “couvert”
- **Idée**: placer un message secret au sein d'un message ordinaire, puis le récupérer à destination
- **Le secret est laissé “en clair” au milieu du bruit**
- Personne d'autre que le destinataire ne saura *à priori* où regarder afin de découvrir le message caché

Le message peut aujourd'hui être caché:

- dans du texte,
- dans du son,
- dans une image,
- dans une vidéo...

Qu'est ce que la cryptographie ?

Cryptographie et Stéganographie

Stéganographie

- Etymologie grecque “**steganos**” = “couvert”
- **Idée**: placer un message secret au sein d'un message ordinaire, puis le récupérer à destination
- **Le secret est laissé “en clair” au milieu du bruit**
- Personne d'autre que le destinataire ne saura *à priori* où regarder afin de découvrir le message caché

Le message peut aujourd'hui être caché:

- dans du texte,
- dans du son,
- dans une image,
- dans une vidéo...

Cryptographie

- Etymologie grecque “**kryptos**” = “caché”
- **Idée**: encoder un message secret pour qu'il ne soit lu que par son destinataire légitime
- **Le message est encodé, et désormais illisible**
- Pour lire le message, il est nécessaire d'avoir une “clé” afin de le “déchiffrer”.

La cryptographie est utilisée aussi bien:

- pour du contenu statique (e.g. chiffrer un document),
- que pour de l'information en transit (i.e. chiffrement d'un canal d'information)

Principes de stéganographie

Exemples textuels

*Since **E**veryone **C**an **R**ead, **E**ncoding **T**ext
In **N**eutral **S**entences **I**s **D**oubtfully **E**ffective*

'Secret inside'

As you know I'll get married next	1
week and will be moving to London	1
with my husband, I wanna thank	0
all of you for your good wishes	0
and blessings. You've been source	1
of large joy and support in that	0
most difficult times and it deeply	1
Hidden message: 1100101	

Almouie Pediatrics

FIND THE LOST WORDS.

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

Allergies

Cough

Dust

Exam

Flu

Germs

Itch

Juice

Medicine

Nose

Oxygen

Pollen

Rash

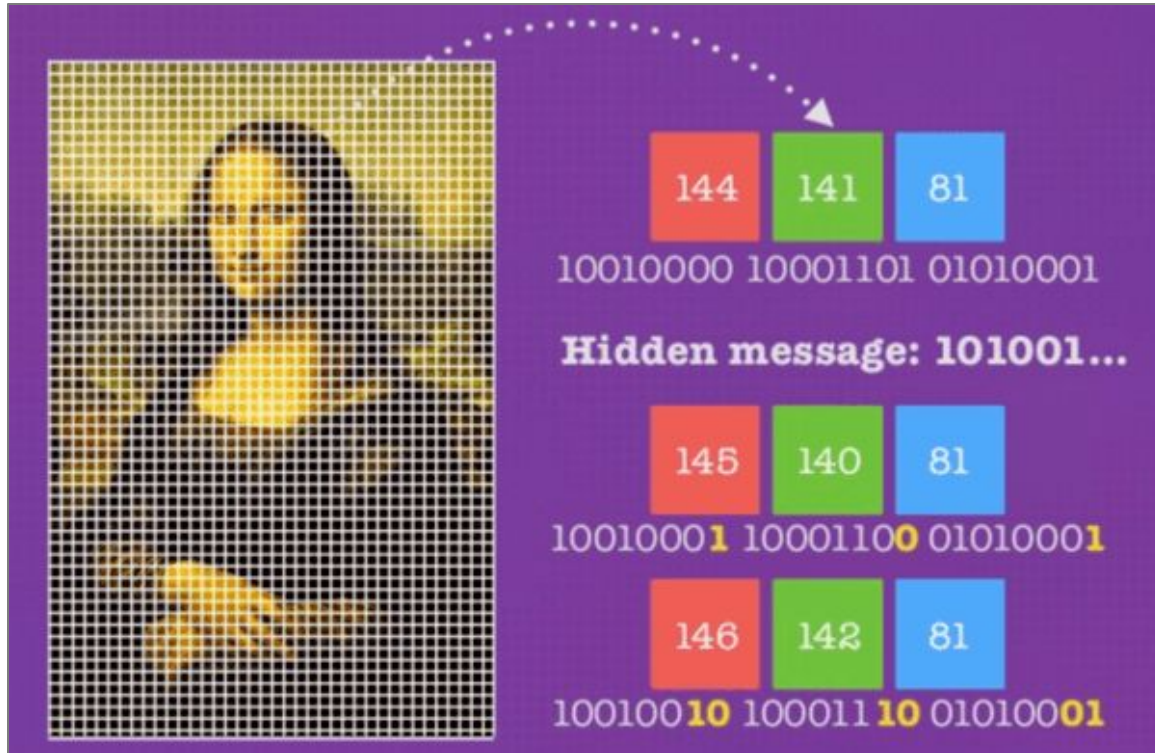
Sneeze

Throat

Vaccine

Principes de stéganographie

Exemples sur des images



Sources: <https://www.bbc.com/news/10480477>

<https://www.commonlounge.com/discussion/4bc16dbc2c7145ff87ad0f0d5401a242>

Original image

Altered image

□ Areas where binary code of pixel has been altered

Binary code from original image pixel 1

10000000 10100100 10110101 10110101 11110011 10110111 11100111 10110011 00110000

Changes made on altered image pixel 1

1000000**1** 10100100 1011010**0** 1011010**0** 1111001**0** 1011011**0** 1110011**0** 10110011 0011001**1**

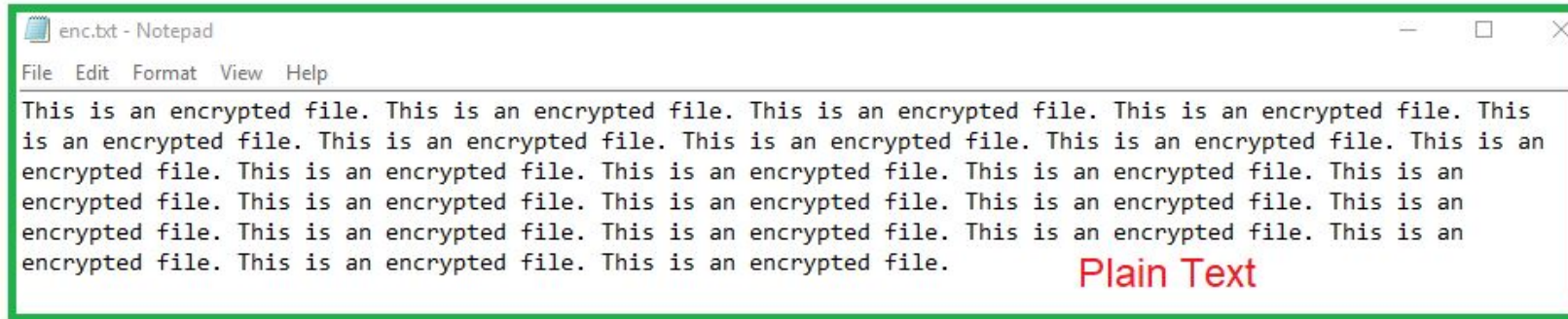
Read last digit:

100000**1** which is ASCII binary code for A

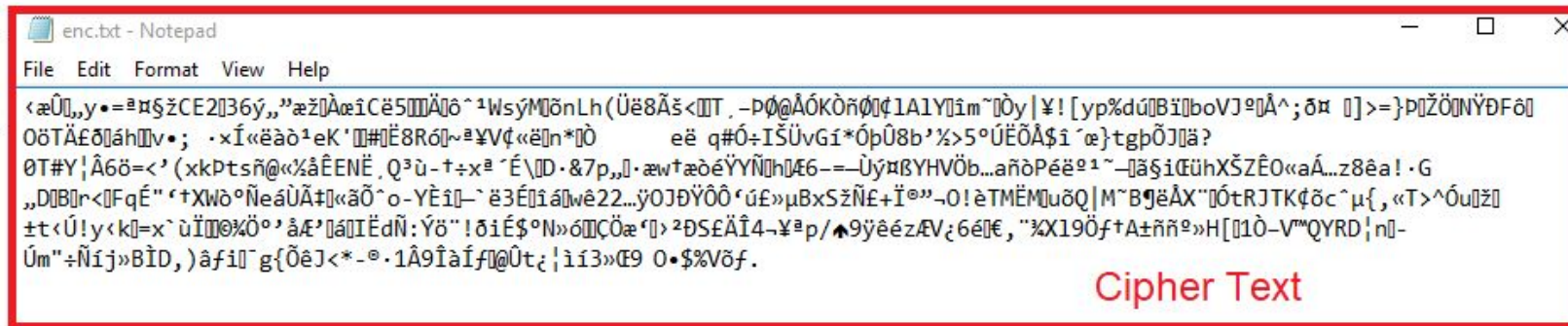
1 2 3 4

Différence avec la cryptographie

Une fois chiffré, le message est illisible



File Encryption Key
(AES-256)



Source image: <https://diyinfosec.medium.com/scanning-memory-for-fek-e17ca3db09c9>

Principes de Kerckhoffs



Auguste Kerckhoffs

(19/01/1835 - 09/08/1903)

Néerlandais

Considéré comme le père fondateur de la cryptographie moderne

Auteur de *La Cryptographie militaire* (1883) = référence de la cryptographie du XIXe siècle. À l'époque, l'une des préoccupations des cryptographes était de mettre en place un réseau de télégraphie sécurisé.

Son œuvre présente ce qu'on appelle aujourd'hui le principe de Kerckhoffs en cryptographie stratégique, qui était considérée comme une science militaire. Kerckhoffs énonce ainsi les règles que doit respecter un système cryptographique pour assurer une communication confidentielle :

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 en 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 portable, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Traduction contemporaine: la sécurité d'un cryptosystème ne doit pas reposer sur le secret de l'algorithme de codage mais qu'elle doit uniquement reposer sur la clé secrète du cryptosystème.

Qualités d'un cryptosystème

Confidentialité: seules les personnes habilitées ont accès au contenu du message.

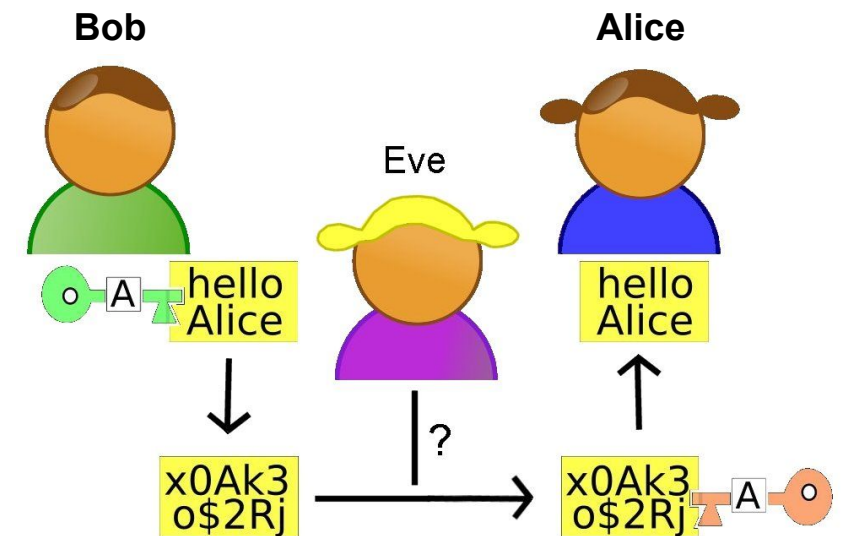
Intégrité: le message ne peut pas être falsifié.

Authentification:

- L'émetteur est sûr de l'identité du destinataire : seul le destinataire pourra prendre connaissance du message car il est le seul à disposer de la clef de déchiffrement.
- Le destinataire est sûr de l'identité de l'émetteur.

Non-répudiation:

- **A l'origine:** l'émetteur ne peut nier avoir écrit le message. L'émetteur peut également prouver qu'il ne l'a pas écrit si c'est effectivement le cas.
- **A la réception:** le destinataire ne peut nier avoir reçu le message. Il peut prouver qu'il ne l'a pas reçu si c'est effectivement le cas.
- **Pendant la transmission:** l'émetteur du message ne peut nier avoir envoyé le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas.



Cryptanalyse

Cryptanalyse = Ensemble des méthodes d'attaque d'un cryptosystème

- Indispensable pour étudier les propriétés de sécurité
- **Objectif**: pouvoir accéder à n'importe quel message secret
- Kerckhoffs → on suppose souvent l'algorithme connu. Il reste à trouver la clé.

Méthodes d'attaque

1. Chiffré connu

L'attaquant connaît seulement (y). Scénario d'écoute passive.

2. Clair connu

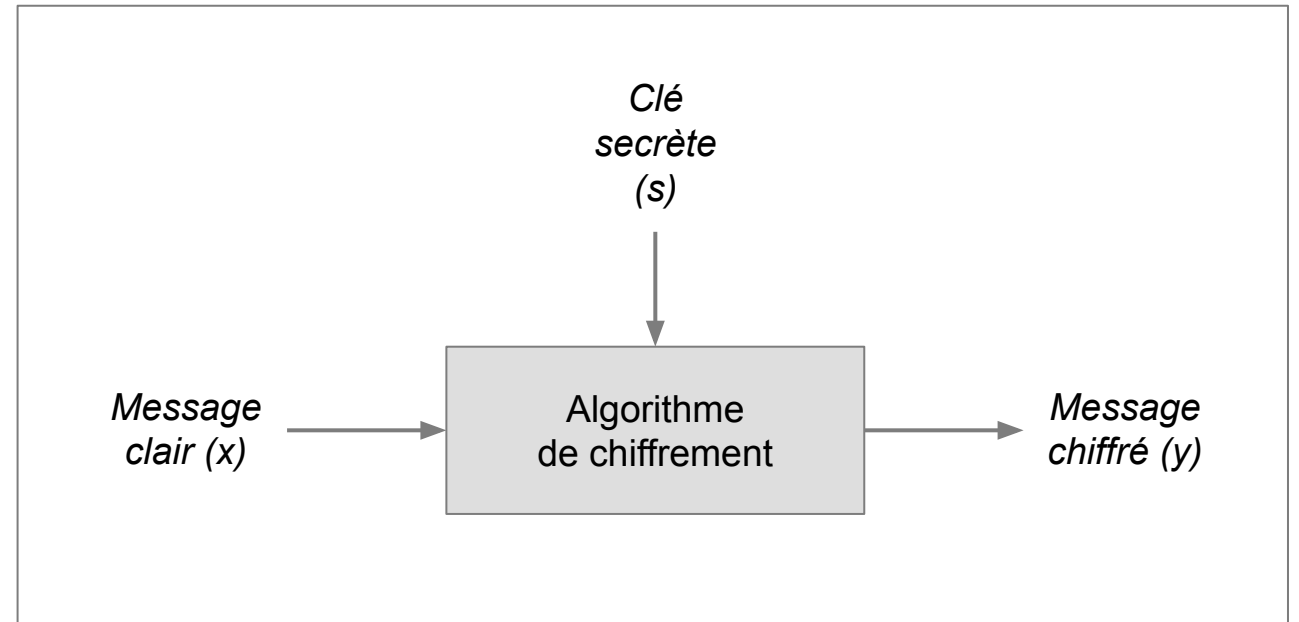
L'attaquant connaît un couple (x,y). Scénario d'interception.

3. Clair choisi

L'attaquant a accès à un poste de chiffrement contenant l'algorithme, et on peut générer une infinité de couples (x,y), avec x choisi.

4. Chiffré choisi

L'attaquant a accès à un poste de chiffrement contenant l'algorithme, et peut déchiffrer tous les messages : il peut générer une infinité de couples (x,y), avec y choisi.





Historique

Codes à répertoire

Message chiffré

24-22

23-92

24-44

24-00

Avantage:

- Difficile à déchiffrer sans le dictionnaire

Difficultés:

- Nécessité de transmettre l'intégralité du dictionnaire au destinataire
- Forts risques d'interception sur un champ de bataille ou via des tactiques de contre espionnage
- Méthode de chiffrement qui passe difficilement à l'échelle si plusieurs destinataires...

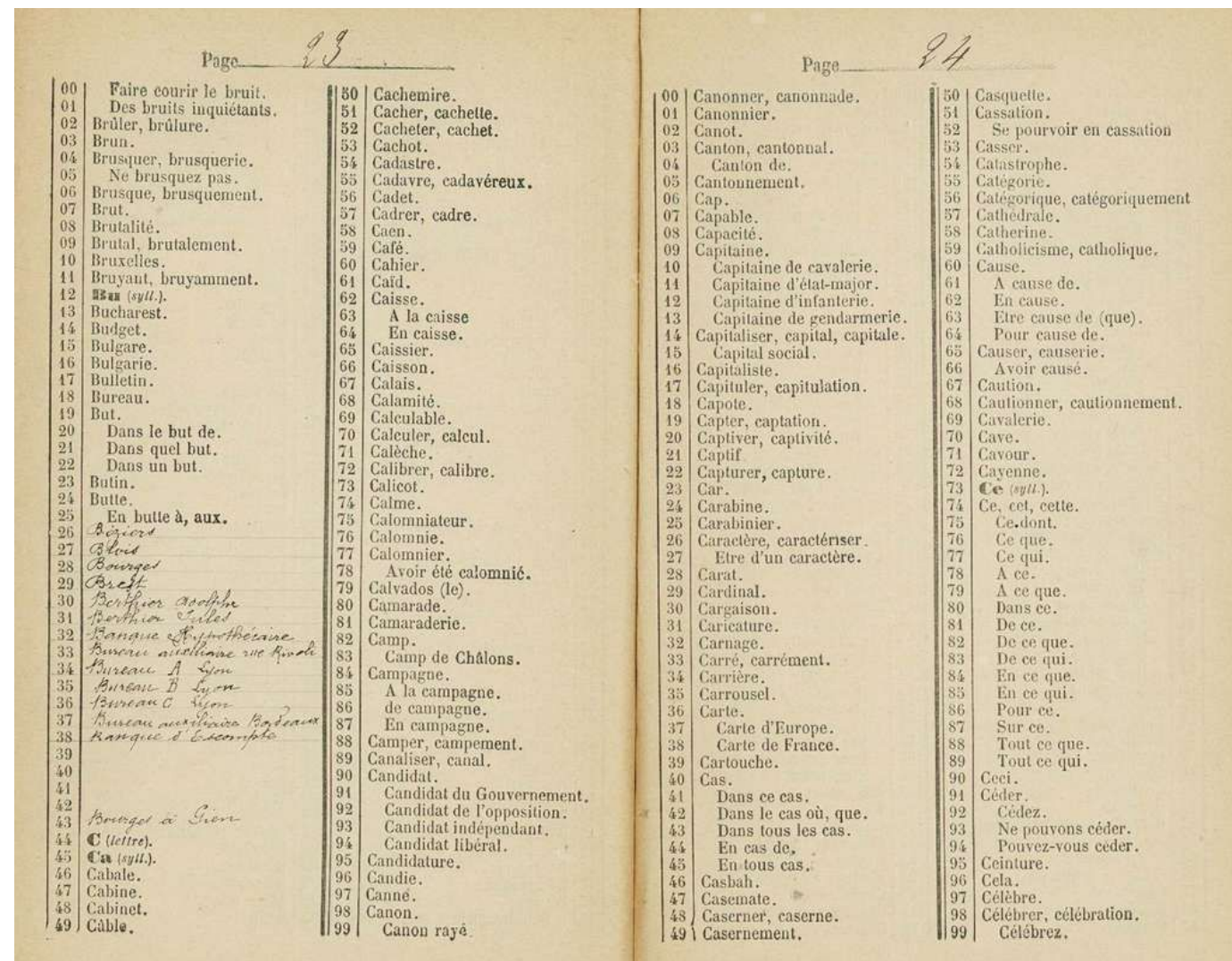
Message clair

Capturer

Candidat de l'opposition

En cas de

Canonnade



Source: <https://www.dicopathe.com/dictionnaire-codes-et-cryptographie-1ere-partie/>

Codes de permutation ou de transposition (1/2)

Idée: Partager le message en blocs, en gardant le même alphabet mais en échangeant la place des lettres au sein d'un bloc (permutation).
Principe de la scytale (grille) utilisée par les spartiates vers 450 av JC.

Message clair que l'on souhaite envoyer: CECI EST UN MESSAGE TRES TRES SECRET

Remplissage dans une matrice 6x6:

C	E	C	I	□	E
S	T	□	U	N	□
M	E	S	S	A	G
E	□	T	R	E	S
□	T	R	E	S	□
S	E	C	R	E	T

Message encodé en prenant les colonnes sans permutation:

CSME□SETE□TEC□STRCIUSRER□NAESEE□GS□T

Codes de permutation ou de transposition (2/2)

Idée: Partager le message en blocs, en gardant le même alphabet mais en échangeant la place des lettres au sein d'un bloc (permutation).
Principe de la scytale (grille) utilisée par les spartiates vers 450 av JC.

Message clair que l'on souhaite envoyer: CECI EST UN MESSAGE TRES TRES SECRET

Remplissage dans une matrice 6x6:

C	E	C	I	□	E
S	T	□	U	N	□
M	E	S	S	A	G
E	□	T	R	E	S
□	T	R	E	S	□
S	E	C	R	E	T

Utilisation d'une clé:

C A P T E R
↓ ↓ ↓ ↓ ↓ ↓
2 1 4 6 3 5

Permutation des colonnes:

E	C	I	E	C	□
T	S	U	□	□	N
E	M	S	G	S	A
□	E	R	S	T	E
T	□	E	□	R	S
E	S	R	T	C	E

Message encodé après permutation des colonnes:

ETE□TECSME□SIUSRERE□GS□TC□STRC□NAESE

Cryptanalyse:

Attaque brute force? **n!** possibilités
→ Attaques à clair connu / choisi

Codes de substitution - Code de Jules César (1/2)

Idée: Décaler les lettres du message secret dans l'alphabet. Utilisé par Jules César pendant la guerre des Gaules vers 50 av JC.

Message clair que l'on souhaite envoyer:

CECI EST UN MESSAGE TRES TRES SECRET

Décalage de chaque caractère d'un nombre fixe: clé = 3

A devient D

B devient E

C devient F

...

Z devient C

Message chiffré en sortie:

FHFL HVW XQ PHVVDJH WUHV WUHV VHFUHW

Lettre	% français	Lettre	% français
A	9,4	N	7,2
B	1,0	O	5,1
C	2,6	P	2,9
D	3,4	Q	1,1
E	15,9	R	6,5
F	1	S	7,9
G	1	T	7,3
H	0,8	U	6,2
I	8,4	V	2,1
J	0,9	W	0
K	0	X	0,3
L	5,3	Y	0,2
M	3,2	Z	0,3

Cryptanalyse:

Brute force ou analyse fréquentielle

Codes de substitution - Code de Vigenère (2/2)

Idée: Renforcer la sécurité du code de César en utilisant une substitution par blocs.

Le code de Vigenère a été mis au point par Leon Batista Alberti au XVème et développé par Blaise de Vigenère.

Message clair que l'on souhaite envoyer:

CECI EST UN MESSAGE SECRET

Choix d'un mot clé: CADEAU + adaptation des lettres en incréments de substitution (C équivaut à +3, A équivaut à +1, etc.)

Message chiffré en sortie:

C	E	C	I		E	S	T		U	N		M	E	S	S	A	G	E		S	E	C	R	E	T
C	A	D	E		A	U	C		A	D		E	A	U	C	A	D	E		A	U	C	A	D	E
+3	+1	+4	+5		+1	+21	+3		+1	+4		+5	+1	+21	+3	+1	+4	+5		+1	+21	+3	+1	+4	+5
F	F	G	N		F	N	W		V	R		R	F	N	V	B	K	J		T	Z	F	S	I	Y

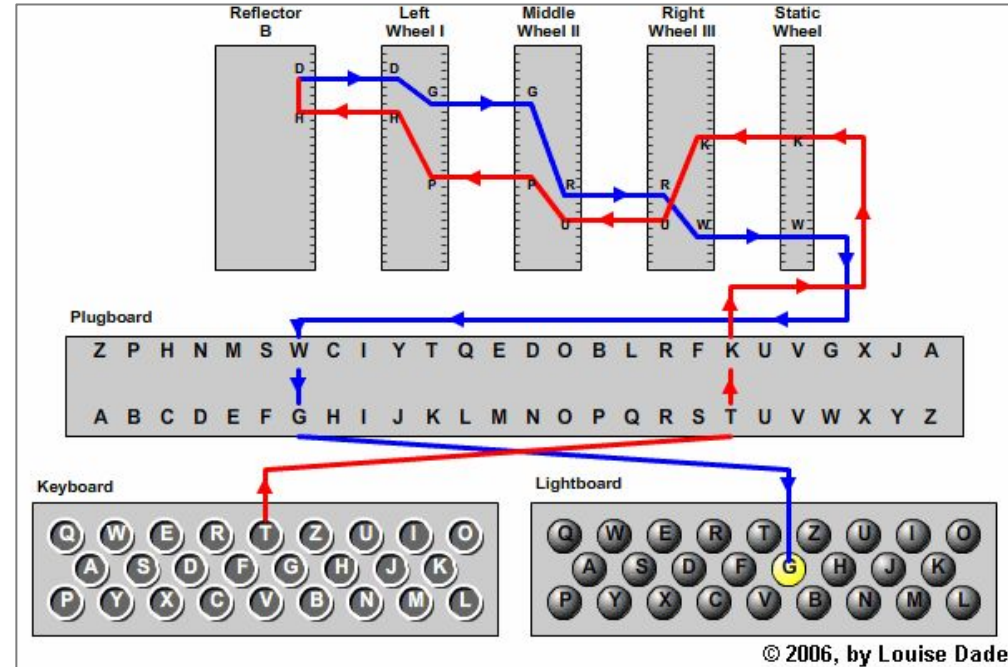
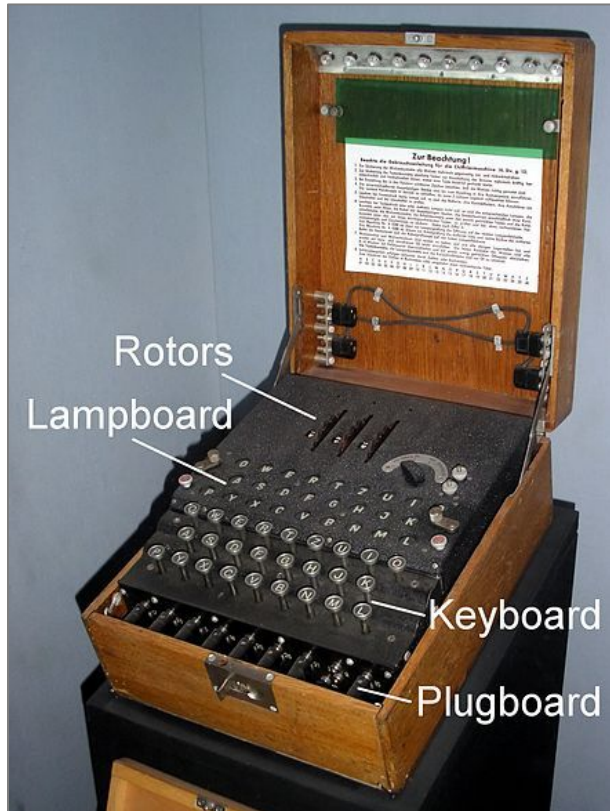
Cryptanalyse:

Considéré comme très sûr pendant plusieurs siècles, le code de Vigenère a été cryptanalysé officiellement par Charles Babbage et Friedrich Wilhelm Kasiski au XIXème siècle.

Astuce: sur un texte long, essayer de repérer des motifs répétés pour déduire la taille de la clé.

Codes de substitution - Enigma (1/2)

Enigma : nom de la machine de chiffrement utilisée par l'Armée Allemande lors de la 2ème Guerre Mondiale

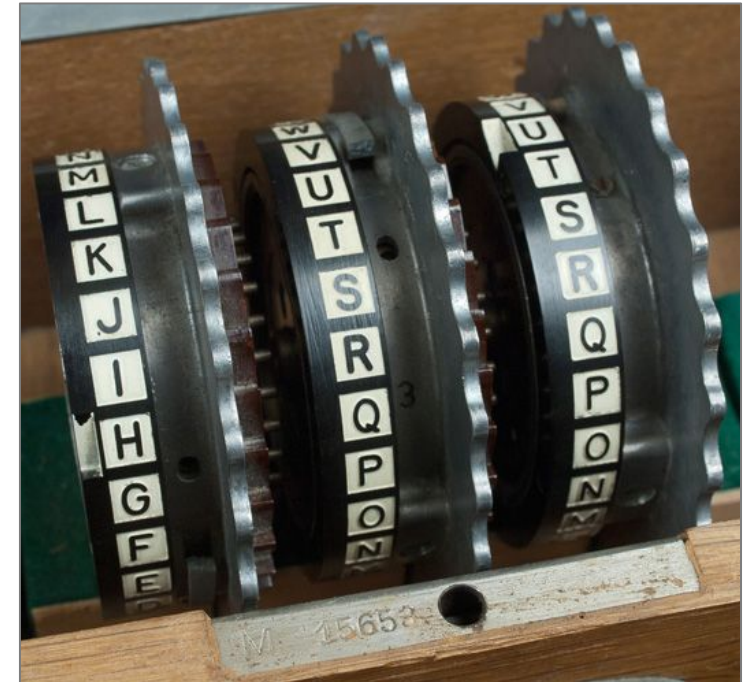


Sources images:

https://en.wikipedia.org/wiki/Enigma_machine

<https://navynews.co.uk/archive/news/item/4671>

<http://enigma.louisedade.co.uk/wiringdiagram.png>



Codes de substitution - Enigma (2/2)

Complexité d'Enigma:

- Choisir 3 rotors sur les 5 disponibles → 60 possibilités
- Choisir la configuration de départ des rotors → $26 \times 26 \times 26$ possibilités
- Choisir 10 configurations dans le tableau de permutation → $150 \cdot 10^{12}$ possibilités
- **Total: $158 \cdot 10^{18}$ possibilités**

Temps de résolution avec un ordinateur moderne: 252 ans

Difficulté additionnelle: Changement de la configuration toutes les nuits à minuit

Transmission des configurations: Sur des feuilles imprimées, avec la liste des configurations valables pour un mois (encre soluble)

Codes de substitution - Enigma (2/2)

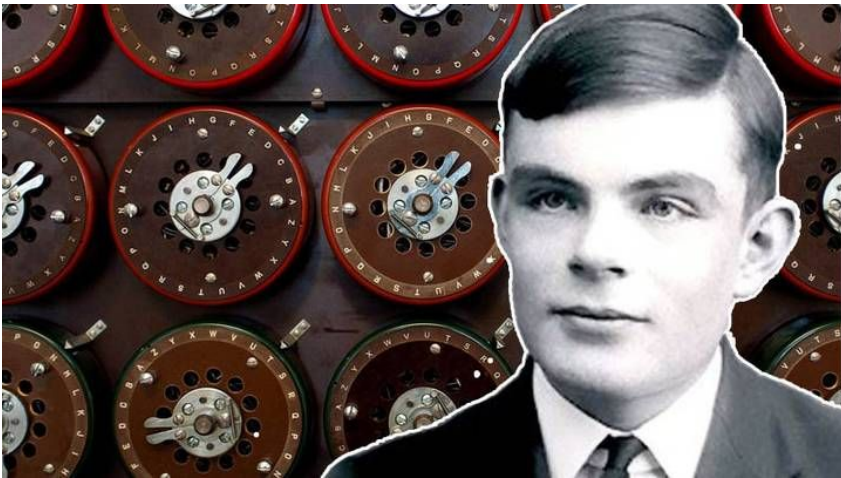
Complexité d'Enigma:

- Choisir 3 rotors sur les 5 disponibles → 60 possibilités
- Choisir la configuration de départ des rotors → $26 \times 26 \times 26$ possibilités
- Choisir 10 configurations dans le tableau de permutation → $150 \cdot 10^{12}$ possibilités
- **Total: $158 \cdot 10^{18}$ possibilités**

Temps de résolution avec un ordinateur moderne: 252 ans

Difficulté additionnelle: Changement de la configuration toutes les nuits à minuit

Transmission des configurations: Sur des feuilles imprimées, avec la liste des configurations valables pour un mois (encre soluble)



Crédit image: <https://www.ladbible.com/technology/latest-how-alan-turing-cracked-the-enigma-code-in-ww2-20190715>

Cryptanalyse: Découverte d'une négligence dans les protocoles de l'Armée Allemande

- Tous les matins à 6h, un bulletin météo était annoncé. Il avait systématiquement comme début de message "WETTERBERICHT" et les mots "HEIL HITLER" à la fin.
- Utiliser le rapport météo permet de réduire le nombre de possibilités. Le décoder permettrait d'obtenir la configuration journalière de la machine Enigma.
- Alan Turing invente "la Bombe" : la machine qui permet de tester les configurations restantes chaque jour afin d'en trouver la bonne (la configuration électrique des rotors était connue des Alliés). Brute force jusqu'à tomber sur une contradiction.
- Au final il ne faudra à la machine que **20 minutes** par jour pour casser le code Enigma.



Codes modernes:
chiffrement par flux / blocs

Chiffrement par flux - Opération XOR

La cryptographie moderne se base largement sur l'opération élémentaire XOR (OU exclusif):

$$0 \text{ XOR } 0 = 0$$

$$1 \text{ XOR } 0 = 1$$

$$0 \text{ XOR } 1 = 1$$

$$1 \text{ XOR } 1 = 0$$

Intérêt: extrêmement rapide à calculer pour un ordinateur qui procède bit-à-bit

Fonctionnement: après avoir créé une clé de chiffrement (c), on utilise l'opération XOR sur le message clair (m) pour obtenir le message chiffré (y):

$$m \text{ XOR } c = y$$

On parle alors de **clé symétrique** car on a aussi:

$$y \text{ XOR } c = m$$

Exemple:

Message = "SOS". S = ASCII 83 et O = ASCII 79. Clé = "PIN" (même longueur).

m	0	1	0	1	0	0	1	1	0	1	0	0	1	1	1	1	0	1	0	0	1	1
c	0	1	0	1	0	0	0	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
y	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0	0	0	1	1	0

Message chiffré = [END OF TEXT] [ACKNOWLEDGE] [GROUP SEPARATOR]

Attention: il est possible de rompre la confidentialité des messages si deux messages sont chiffrés avec la même clé !

Avec: "x1 XOR c = y1" et "x2 XOR c = y2"

$$y1 \text{ XOR } y2 = (x1 \text{ XOR } c) \text{ XOR } (x2 \text{ XOR } c)$$

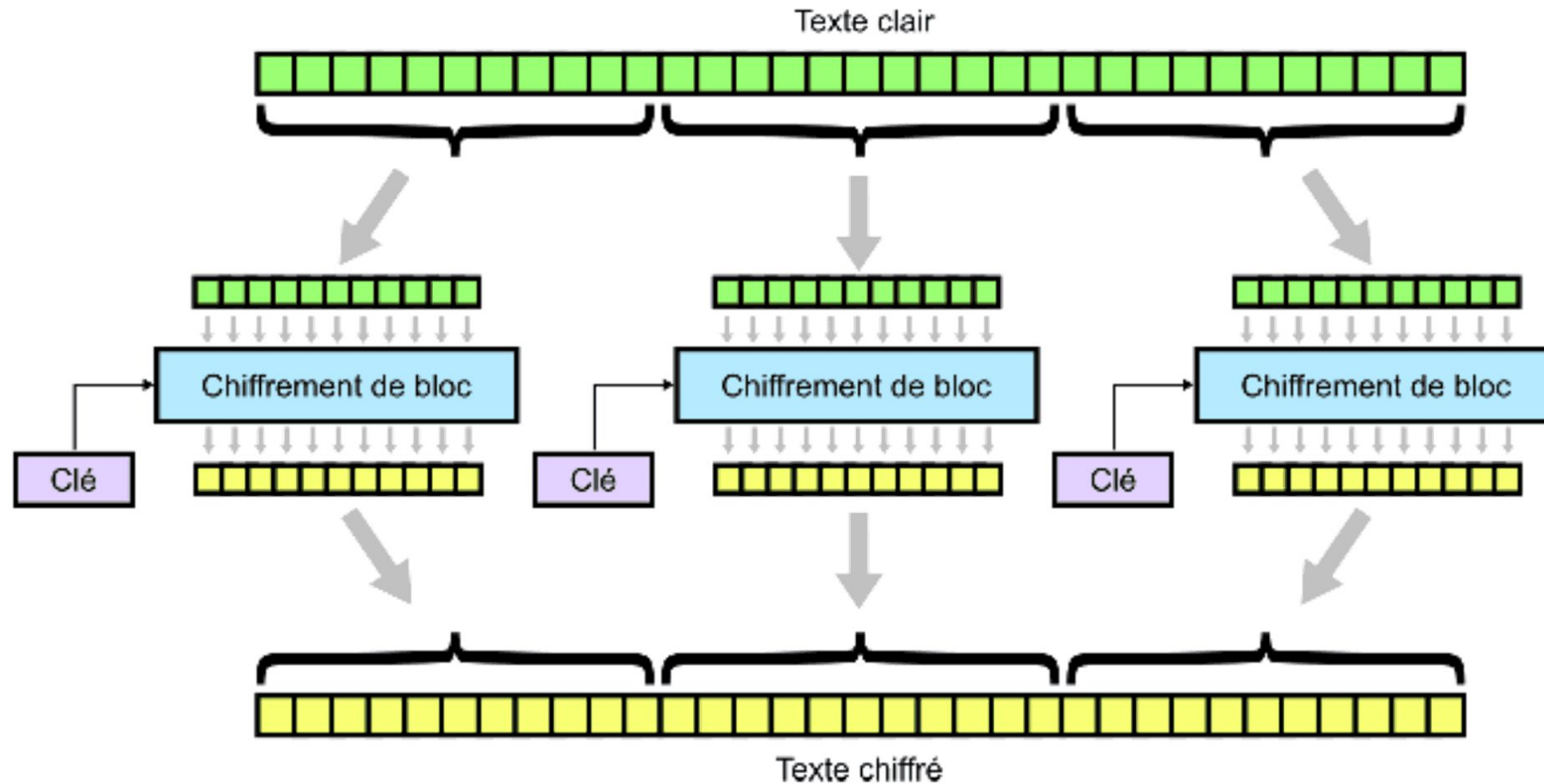
$$= x1 \text{ XOR } x2, \text{ vulnérable à une attaque fréquentielle}$$

Il faut donc incrémenter la clé à chaque message "PIN-01", "PIN-02", etc.

Exemple de protocole vulnérable : protocole Wifi **WEP**, utilisant le chiffrement de flux RC4. Le compteur utilisé dans la clé de chiffrement était régulièrement remis à 0, ce qui permettait à l'attaquant de décrypter (c'est-à-dire déchiffrer sans la clé) les textes chiffrés.

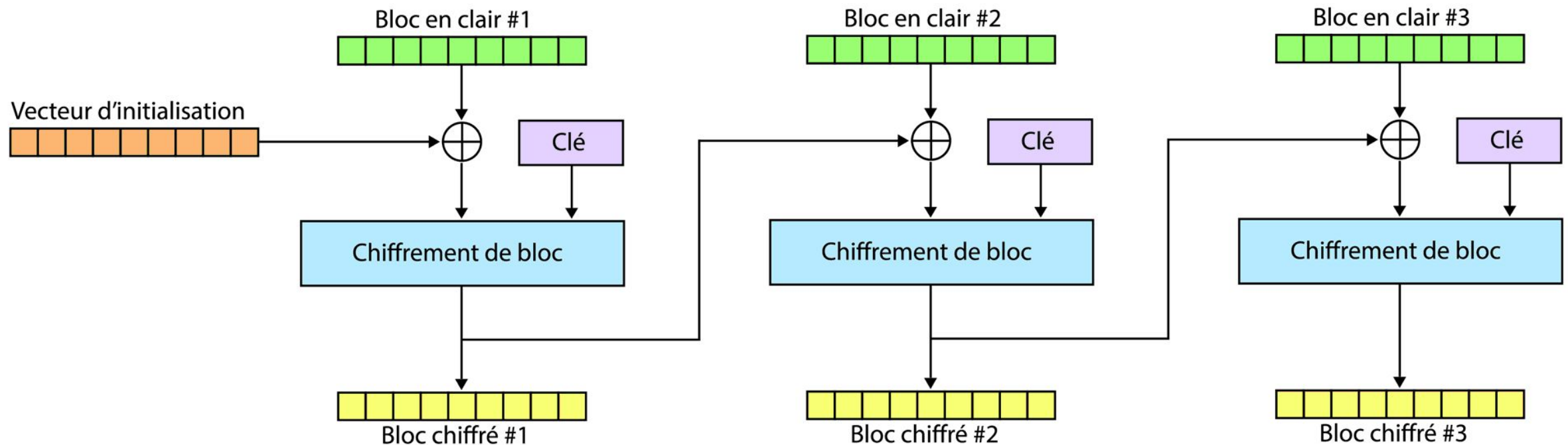
Chiffrement par blocs - Exemple de ECB

ECB : Electronic Code Book



Chiffrement par blocs - Exemple de CBC

Mode Cipher Block Chaining



Chiffrement par blocs - Différence ECB / CBC



Image non chiffrée



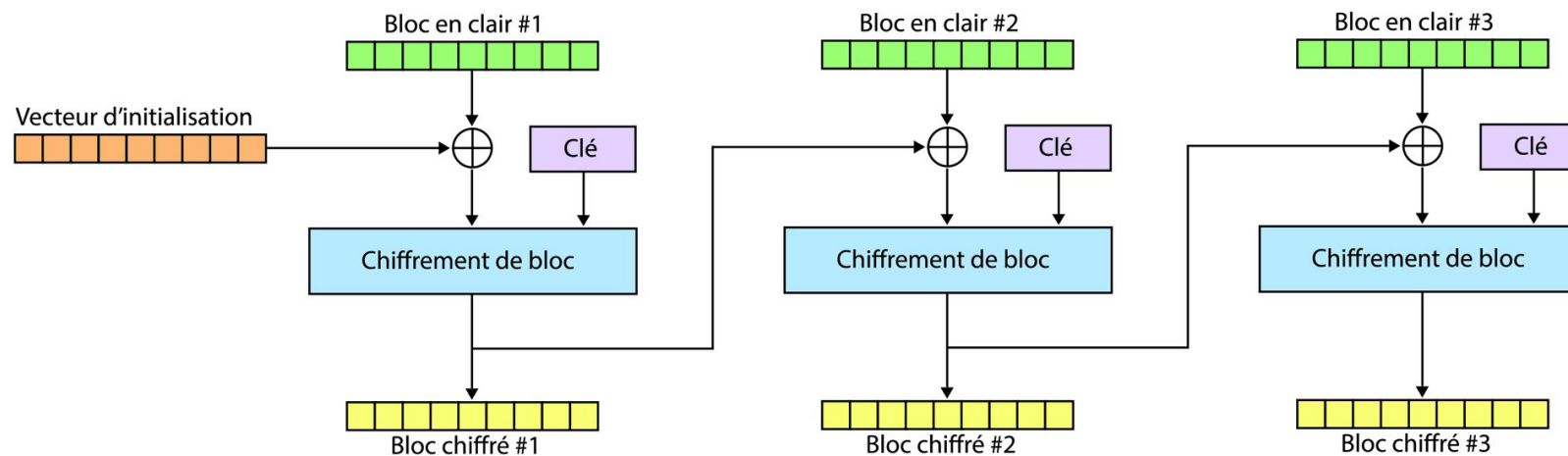
Image chiffrée en mode ECB



Image chiffrée en mode CBC

Chiffrement par blocs - CBC est il infailible pour autant ?

Mode Cipher Block Chaining

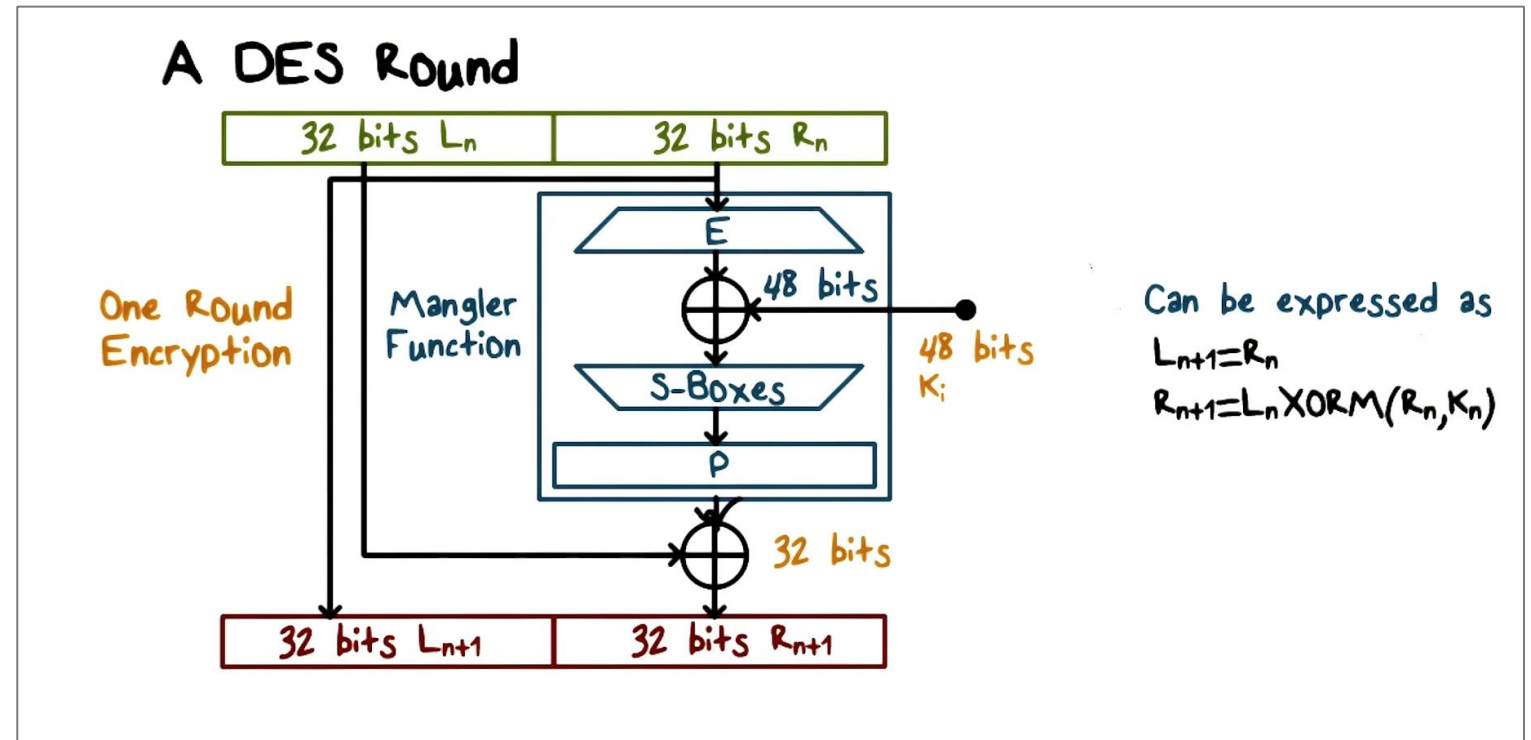
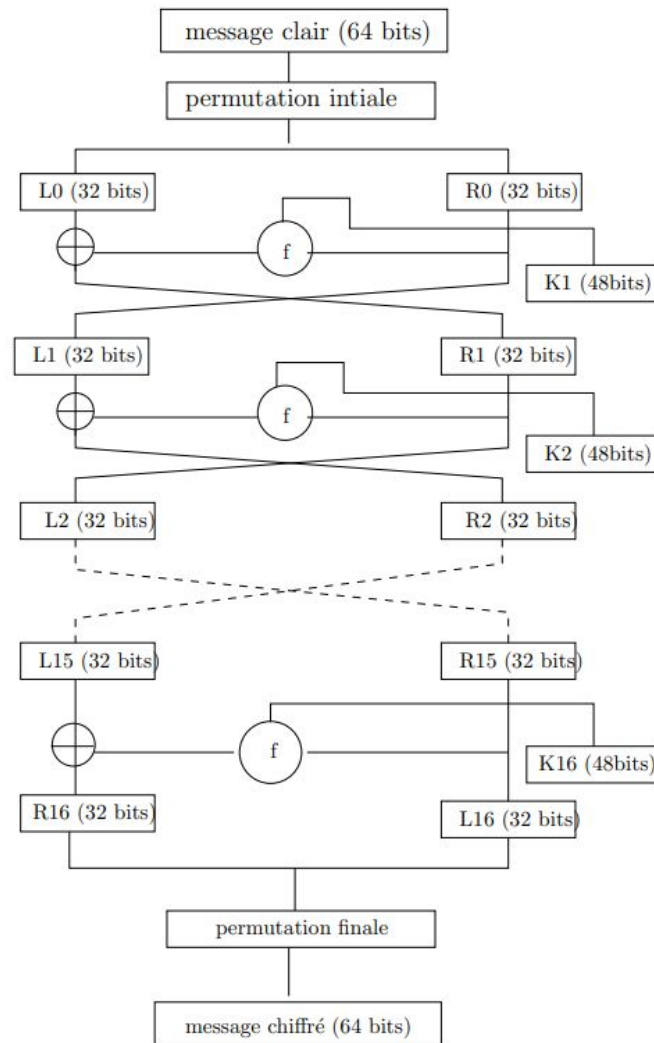


Il peut s'agir ici d'une vulnérabilité d'implémentation !

L'attaque se base sur la connaissance préalable du vecteur d'initialisation. Il est possible de déchiffrer progressivement des messages (blocs par blocs) en menant des attaques à clair choisi (bruteforce jusqu'à trouver les blocs en clair correspondant à chaque bloc chiffré).

La vulnérabilité BEAST dans le protocole TLS 1.0 exploitait par exemple le fait que TLS chiffrait les messages en mode CBC avec des IV prédictibles

Chiffrement par blocs - Data Encryption Standard (DES)



Source: <https://www.hypr.com/data-encryption-standard-des/>

Anciennement utilisé pour les **mots de passe UNIX**, ce chiffrement a été **cassé en 1997**. La clé de 56 bits est beaucoup trop courte pour les puissances de calcul actuelles et devient vulnérable aux **attaques par brute force**. En 1997, il a fallu 3 semaines pour casser le chiffrement, puis seulement 56 heures en 1998, puis moins de 22 heures en 1999 grâce à un réseau de milliers de machines.

Chiffrement par blocs - Advanced Encryption Standard (AES)

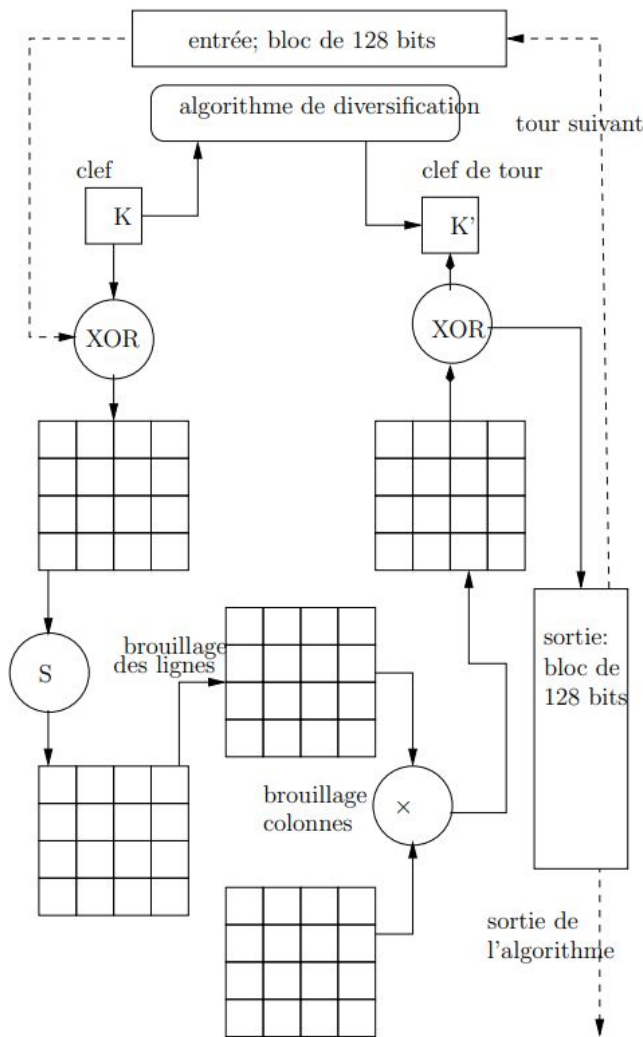


Schéma de AES pour ... 1 seule itération.

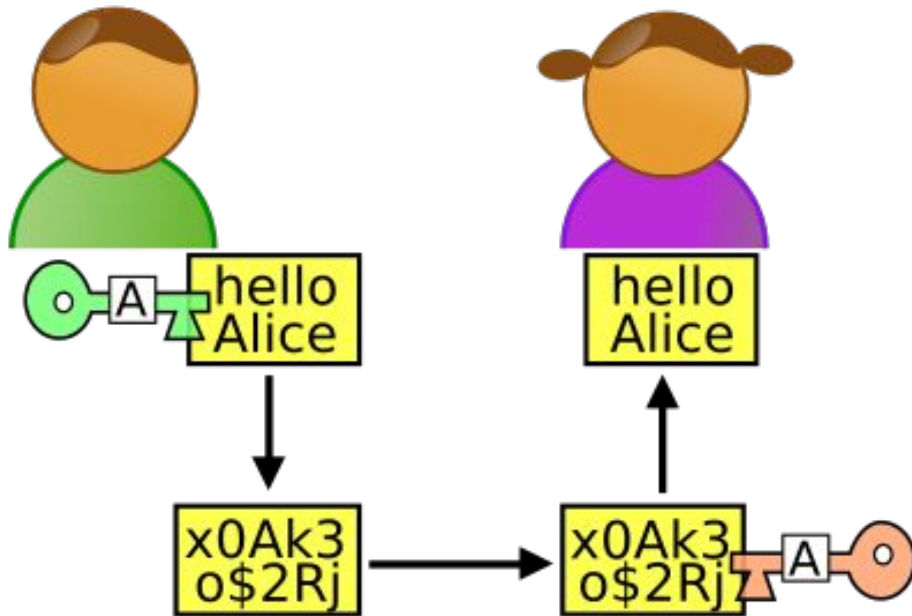
A retenir:

- Successeur de DES, triple-DES et autres algorithmes
- A remporté un appel d'offre international, conforme aux standards NIST
- **Largement utilisé aujourd'hui**
- Considéré comme **la référence en chiffrement symétrique**
- **Robuste avec les moyens de calculs actuels** (quid des calculateurs quantiques?)
 - **À condition d'utiliser une clé suffisamment longue (256 bits) !**



Clés symétriques & Clés asymétriques

Principe des codes à clés symétriques

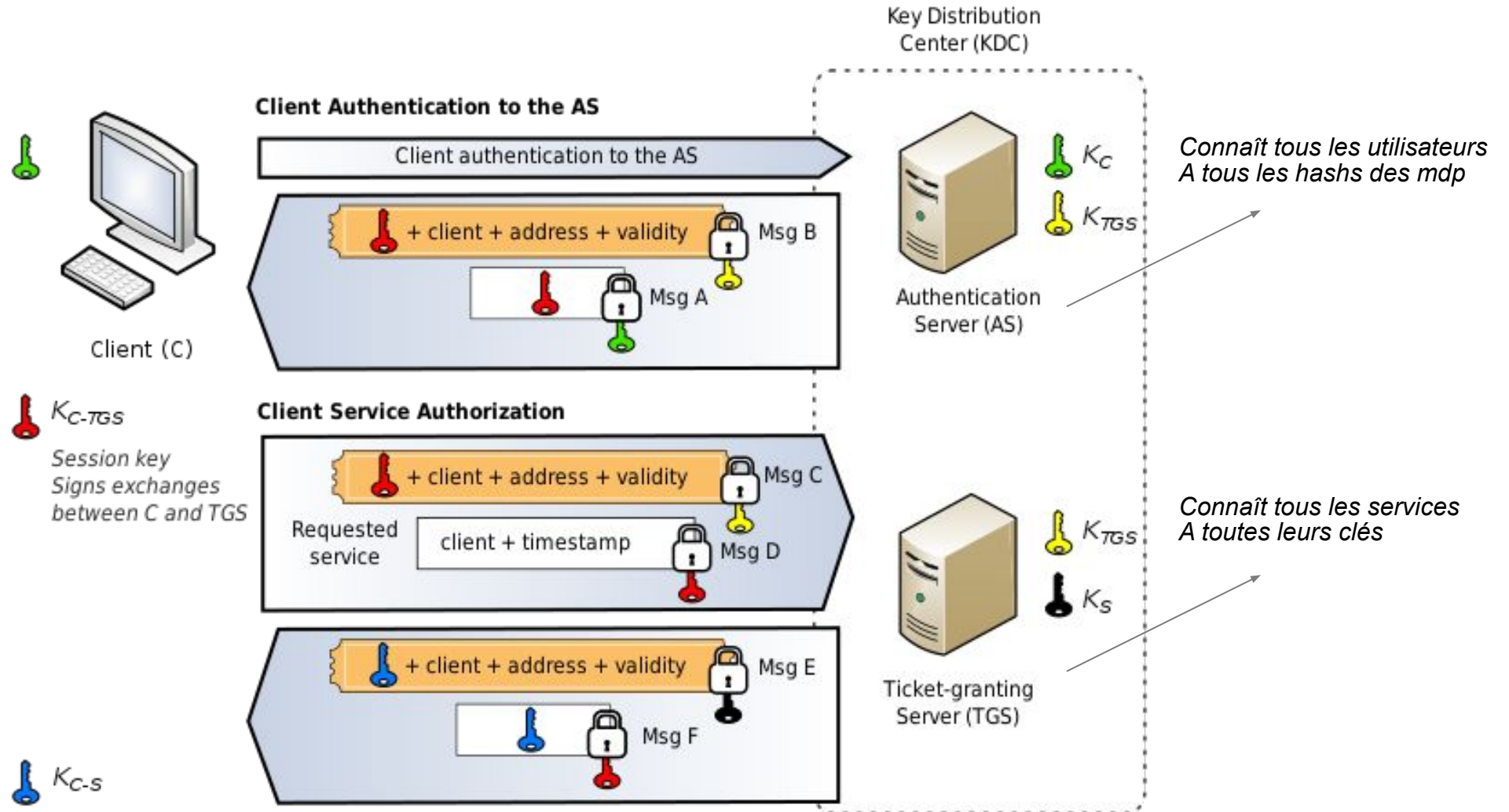


Codes à clés symétriques

- Alice et Bob disposent tous deux d'**une clé identique** : on parle donc de **clé symétrique**
- **La même clé sert à la fois pour le chiffrement et pour le déchiffrement.**
- Les clés garantissent la confidentialité du message envoyé : chaque participant doit garder sa clé secrète !
- **Une difficulté subsiste dans ce modèle : comment transmettre la clé symétrique à l'autre parti ?**

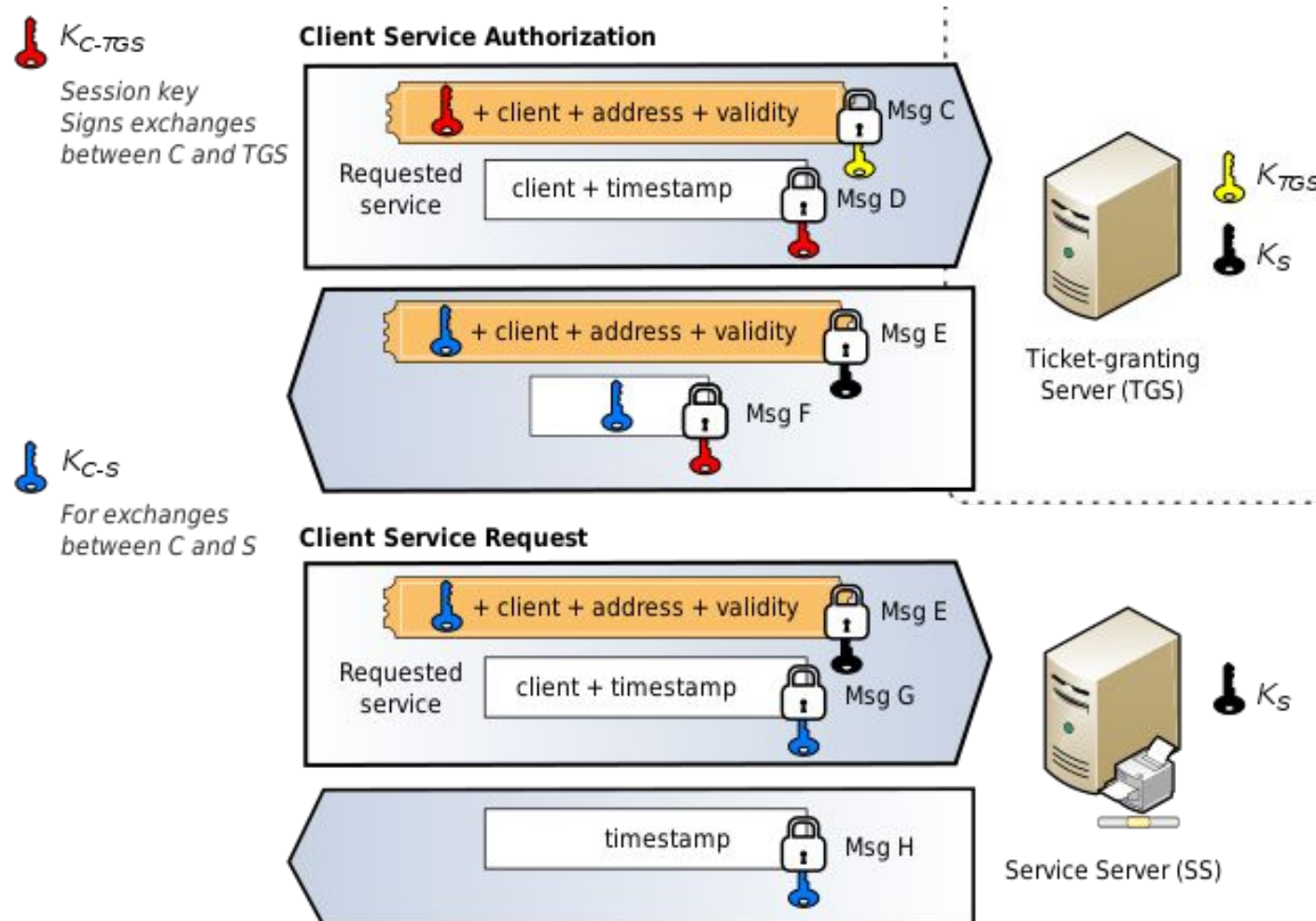
Structure à clés symétriques

Exemple de Kerberos (1/2)

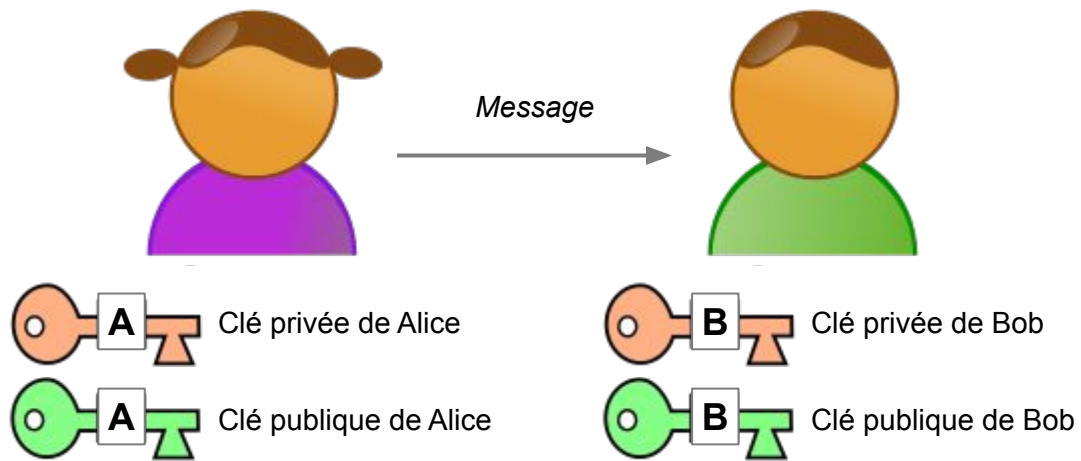


Structure à clés symétriques

Exemple de Kerberos (2/2)



Principe des codes à clés asymétriques



Codes à clés asymétriques

- L'émetteur et le destinataire ont tous les deux une paire de clés : Alice dispose d'une clé privée et d'une clé publique ; Bob dispose aussi d'une clé privée et d'une clé publique (différentes de celles de Alice) : on parle alors de **clés asymétriques**.
- Les clés fonctionnent par **paires** :
 - la **clé publique** sert pour **chiffrer**
 - la **clé privée** sert pour **déchiffrer**
- La clé publique doit être accessible au monde entier
- La clé privée doit être gardée secrète par son propriétaire

Pour envoyer un message à Bob, Alice chiffre son message avec la clé publique de Bob. Les clés fonctionnant par paires, seul Bob sera en mesure de déchiffrer le message. A la réception du message, Bob utilise sa clé privée pour déchiffrer.

Algorithme RSA - Rivest, Shamir, Adleman

RSA Algorithm

Key Generation

Select p, q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption

Plaintext:	M
Ciphertext:	$M = C^d \bmod n$

Exemple

Prenons deux nombres premiers (ici choisis petits):

$$p = 17$$

$$q = 11$$

$$n = p \times q = 187$$

$$\Phi(n) = (p - 1) \times (q - 1) = 160$$

Soit e tel que $\text{pgcd}(e, 160) = 1$

Par exemple, $e = 7$

Cherchons l'inverse de 7 modulo 160:

$$d = 23, \text{ car } ed = 7 \times 23 = 161 = 1 \bmod 160$$

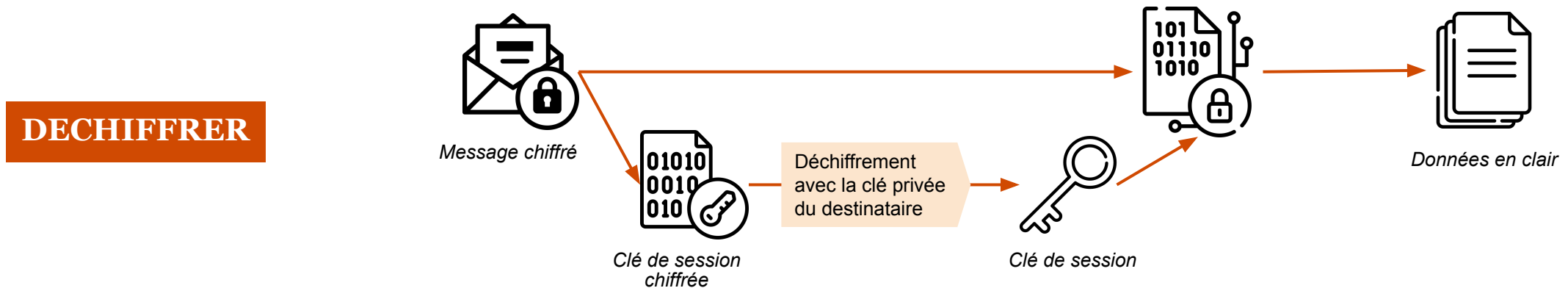
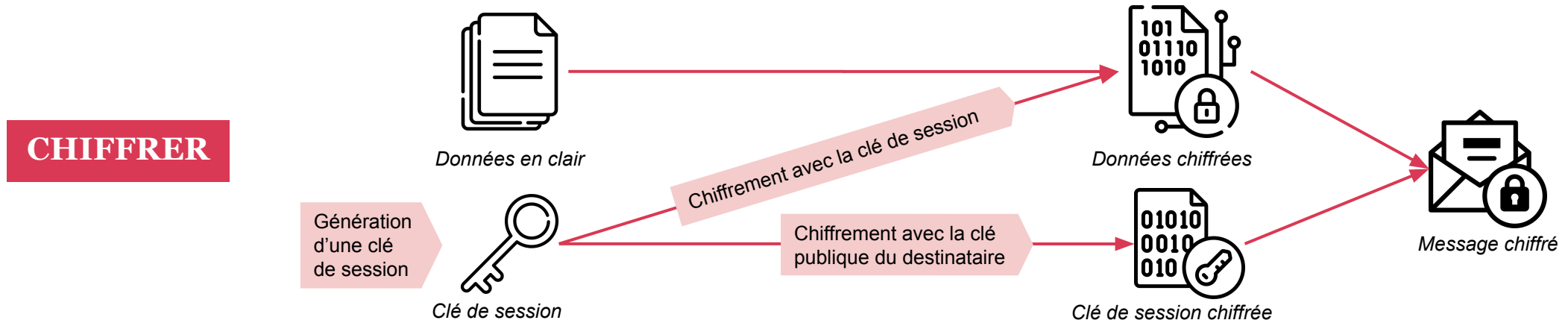
Clé publique = { 7 , 187 }

Clé privée = { 23 , 187 }

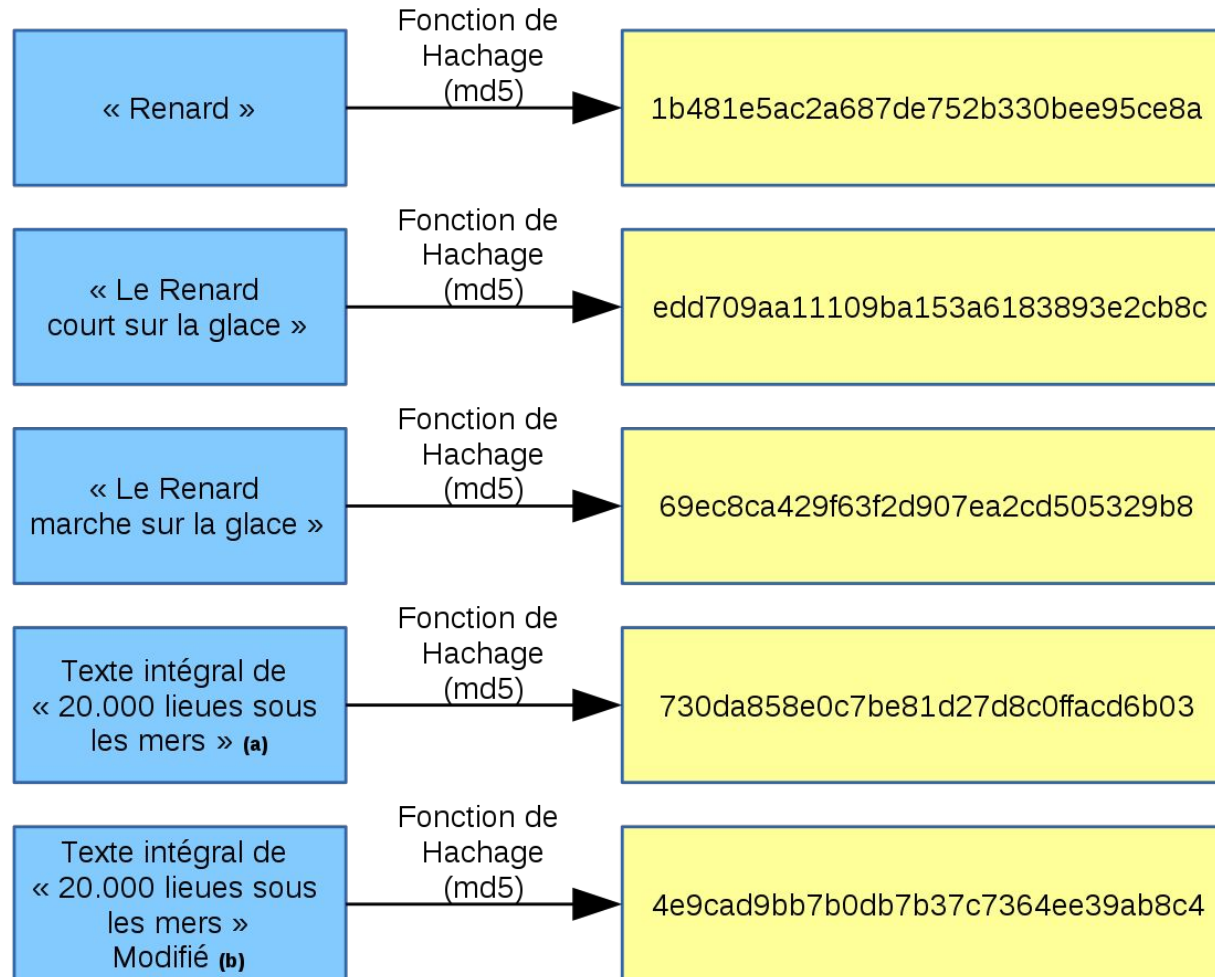
Source: <https://minarchiste.wordpress.com/2018/12/04/le-chiffage-rsa-un-miracle-economique/>

Exemple de système à clés symétriques & asymétriques

Programme de chiffrement PGP - Pretty Good Privacy



Rappel sur les fonctions de hachage - Exemple MD5



Source: https://fr.wikipedia.org/wiki/Fonction_de_hachage

Principes fondamentaux

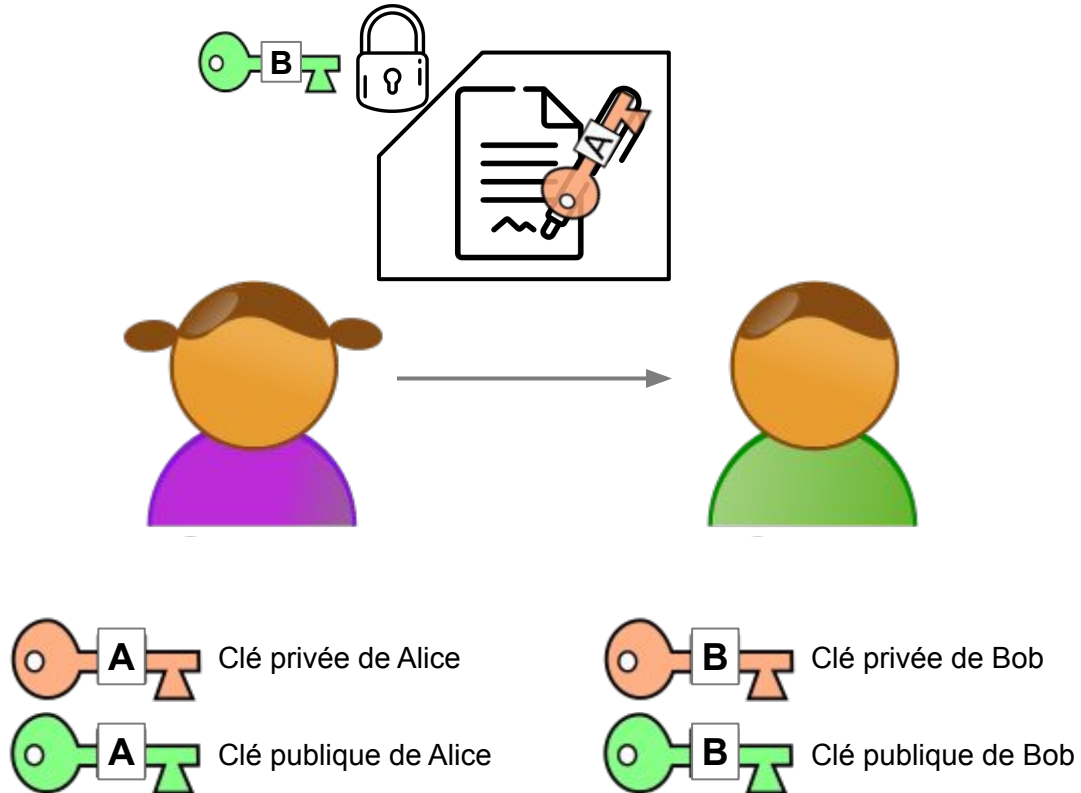
Intérêt: les fonctions de hachage permettent de créer une “signature” d’un document.

Propriétés:

- L’espace d’arrivée est de taille fixe, quel que soit le document en entrée (e.g. 32 caractères hexadécimaux pour l’algorithme MD5)
- Les collisions sont donc mathématiquement possibles, mais doivent être statistiquement difficiles à provoquer : deux hash identiques présument de documents en entrée identiques
- Changer le moindre bit du document en entrée doit changer intégralement la valeur du hash
- Le hash ne doit rien laisser transparaître du document en entrée : pas de fonction inverse

Exemples d’algorithmes de hachage:
MD5 (déprécié), SHA1, SHA256, ...

Non répudiation à l'envoi - Utilisation des signatures



Codes à clés asymétriques


- Les clés fonctionnent par **paires** :
 - la **clé publique** sert pour **chiffrer**
 - la **clé privée** sert pour **déchiffrer** et signer !

Pour envoyer un message à Bob:

- Alice signe son message avec sa clé privée (orange key with 'A')
- Alice chiffre le message signé avec la clé publique de Bob (green key with 'B')

Pour lire le message d'Alice, Bob doit:

- Déchiffrer le message avec sa clé privée (orange key with 'B')
- Vérifier la signature avec la clé publique d'Alice (green key with 'A')



Applications de la cryptographie

Applications de la cryptographie

Jusqu'au 20-ème siècle la cryptographie était essentiellement réservée aux militaires et aux diplomates et accessoirement aux industriels et banquiers... aujourd'hui la cryptographie se retrouve dans de nombreux domaines de la télécommunication.



Authentification



Transactions bancaires / boursières



Protection des télécommunications



Chiffrement des données



Télévision payante



Que retenir ?

Que retenir ?



1

Cryptographie \neq Stéganographie

2

Principes de Kerckhoffs : le secret doit reposer sur la clé !

3

Qualités d'un cryptosystème: confidentialité / intégrité /
authentification / non-répudiation

4

Chiffrement par flux / Chiffrement par bloc

5

Clés symétriques / Clés asymétriques

Merci ! Des questions ?

[pwc.fr](https://www.pwc.fr)

© 2022 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.