

# Historique et évolution du cryptographie

## Cryptographie et Sécurité Informatique

Cycle d'ingénieur : Génie Informatique option Génie Logiciel

Présenté par :

*Nour El-houda El-Messaoudi et Ayman Amokrane*

# PLAN

- 1 Introduction
- 2 Antiquité et Cryptage Ancien
- 3 Cryptographie au Moyen Âge
- 4 Les premières avancées de la cryptographie
- 5 La Cryptographie durant les Guerres Mondiales, de Cryptage Informatique
- 6 Débuts de la Cryptographie Moderne à Clé Publique et Internet
- 7 Les avancées de la Cryptographie Symétrique
- 8 La Cryptographie durant les GMs, Cryptage Informatique
- 9 Débuts de la Cryptographie Moderne à Clé Publique et Internet
- 10 Les avancées de la Cryptographie Symétrique

# Introduction

- Le cryptage et la sécurité informatique sont fondamentaux pour protéger les informations sensibles en assurant leur confidentialité, intégrité et disponibilité. Ensemble, ils garantissent la protection des données personnelles et professionnelles, renforçant ainsi la confiance des utilisateurs dans les systèmes numériques.



# Définitions

## Cryptage

Processus de transformation de l'information pour la rendre illisible aux personnes non autorisées.

## Cryptanalyse

Science et art de déchiffrer les messages chiffrés sans en connaître les clés.

## Sécurité informatique


Ensemble des techniques pour protéger les systèmes, les réseaux et les données contre les accès non autorisés et les dommages.

Le terme cryptographie vient du grec ancien:

- kruptos (ό) « caché »
- graphein (ά) « écrire »



## Égypte ancienne (vers 1900 av. J.-C.)

- Les premières formes de cryptage ont été observées dans les hiéroglyphes égyptiens, où des substitutions symboliques étaient utilisées pour sécuriser les informations.
- 
- **Méthode** : La substitution symbolique permettait de protéger des informations sacrées et administratives, assurant ainsi que seuls les initiés pouvaient comprendre le contenu.

## La Scytale spartiate (Grèce antique (vers 500 av. J.-C.))

- Chez les Spartiates, au Vème siècle avant Jésus-Christ (Sparte est une ancienne ville grecque du Péloponnèse), la scytale, également connue sous le nom de bâton de Plutarque, était un bâton de bois utilisé pour lire ou écrire une dépêche chiffrée. Considérée comme le plus ancien dispositif de cryptographie militaire connue, elle permettait l'inscription d'un message chiffré sur une fine lanière de cuir ou de parchemin que le messager pouvait porter à sa ceinture.



# Méthode d'utilisation de la Scytale Spartiate

## 1 Préparation de la Scytale :

- Un bâton cylindrique de diamètre approprié est nécessaire. La taille du bâton est essentielle, car elle déterminera la largeur de la bande de cuir et la lisibilité du message.
- Le bâton doit être d'une taille standard, connue uniquement par l'expéditeur et le destinataire.

## 2 Enroulement de la bande de cuir :

- Une bande de cuir ou de papyrus est prise. Sa longueur doit être suffisante pour écrire le message souhaité.
- L'expéditeur enroule la bande de cuir autour du bâton de manière régulière, sans superposition, en veillant à ce qu'elle soit bien serrée.

## 3 Écriture du message

- Le message est ensuite écrit sur la bande de cuir en suivant le contour du bâton. L'écriture se fait verticalement, en s'assurant que chaque lettre est alignée avec le bâton.
- L'expéditeur peut écrire un message complet sans se soucier de sa lisibilité, car il sera illisible une fois la bande déroulée.



# Méthode d'utilisation de la Scytale Spartiate (suite)

## 1 Déroulement de la bande :

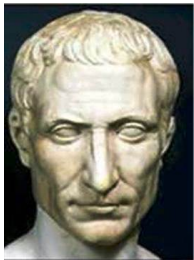
- Une fois le message écrit, l'expéditeur retire la bande de cuir du bâton. Le message apparaît alors comme un ensemble de lettres éparses, illisibles sans le bâton.
- Pour transmettre le message, l'expéditeur envoie la bande de cuir au destinataire sans le bâton.

## 2 Déchiffrement par le destinataire :

- À la réception de la bande, le destinataire doit utiliser un bâton de même diamètre.
- Il enroule la bande de cuir autour de son propre bâton. En procédant ainsi, le message devient lisible car les lettres s'alignent correctement.
- Le destinataire peut alors lire le message en suivant l'ordre vertical.



# Le chiffre de César (58 av. J.-C)

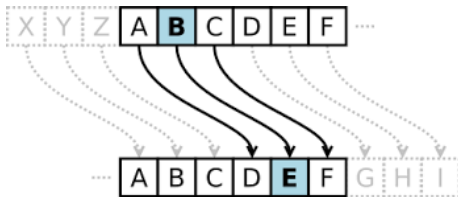


(Vers 58 av. J.-C.)  Empire romain

- **Le chiffre de César**, utilisé par l'empereur romain Jules César dans sa correspondance militaire. Ce chiffre servait à protéger les messages transmis à ses généraux pour éviter qu'ils ne soient interceptés et lus par l'ennemi.
- Le chiffre de César est aujourd'hui souvent utilisé comme une introduction à la cryptographie dans l'enseignement.

# Le chiffre de César (suite)

- Le chiffre de César repose sur une méthode de **substitution simple**, où chaque lettre du message est décalée d'un nombre fixe de positions dans l'alphabet. Par exemple, avec un décalage de 3, la lettre "A" devient "D", "B" devient "E", et ainsi de suite.



# Invention de la cryptanalyse par Al-Kindi (9 siècle)

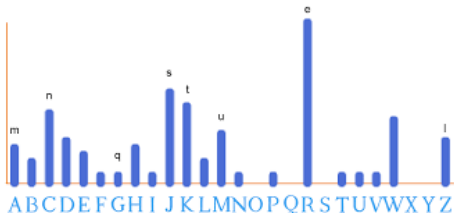
## (9 siècle) ? Islam médiéval

- Vers 850 apr. J.-C., le **savant Al-Kindi**, l'un des intellectuels majeurs de l'époque abbasside, pose les fondations de la cryptanalyse. Dans son ouvrage intitulé Manuscrit sur le déchiffrement des messages cryptographiques, il décrit une méthode permettant de déchiffrer des messages chiffrés par **substitution**.
- L'invention de la cryptanalyse par Al-Kindi a marqué une étape décisive dans l'histoire de la cryptographie.



# Analyse de fréquence (cryptanalyse)

- Al-Kindi a développé la technique **d'analyse de fréquence**, qui consiste à observer la fréquence d'apparition des lettres dans un texte chiffré.
- Al-Kindi exploitait ces différences de fréquence pour identifier les lettres et casser le code du message.
- Dans les langues écrites, certaines lettres apparaissent plus fréquemment que d'autres (par exemple, en français, la lettre "E" est la plus courante).



# Le chiffre de Vigenère (1553)



(1553) ♦ Italie

**Le chiffre de Vigenère** système de chiffrement inventé par "Blaise Vigenère" (1523-1596) qui mit en échec les cryptanalystes durant trois siècles. C'est une modification du chiffre de "Giovan Battista Bellaso".

**L'un des premiers systèmes** de chiffrement polyalphabétique, introduisant une avancée importante dans la cryptographie. Contrairement aux chiffres monoalphabétiques qui utilisent un seul alphabet pour remplacer chaque lettre par une autre, le chiffre de Vigenère applique plusieurs alphabets de substitution en fonction d'une clé répétée tout au long du texte en clair.

# Le chiffre de Vigenère (suite)

- La méthode repose sur l'utilisation d'un **tableau de substitution** , appelé tableau de Vigenère ou carré de Vigenère, qui contient toutes les lettres de l'alphabet décalées dans chaque rangée.
- Ce tableau permet d'utiliser différents alphabets pour chaque lettre du message, rendant **l'analyse de fréquence** beaucoup moins efficace et augmentant la complexité du chiffrement.
- **La lettre chiffrée** est déterminée en combinant la lettre du message en clair avec une lettre de la clé, choisie dans la colonne et la rangée correspondantes du tableau.

# Le tableau 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	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



# Les codes de Mary Stuart et son exécution

## (1586) ♦ Angleterre

- **Mary Stuart**, reine d'Écosse, a été impliquée dans un complot visant à assassiner la reine Élisabeth I d'Angleterre, pour lequel elle utilisait un chiffre de substitution complexe afin de communiquer secrètement avec ses partisans. Ce chiffre servait à masquer le contenu de ses messages en remplaçant chaque lettre par une autre, rendant le texte difficile à lire sans la clé appropriée.



Figure: : Mary Stuart

# Méthode de codage utilisée par Mary Stuart

## 1 Chiffre de substitution

- Mary Stuart utilisait un chiffre de substitution pour ses messages secrets, où chaque lettre de l'alphabet était remplacée par une autre lettre ou un symbole spécifique.
- Ce type de code permettait de masquer le contenu en utilisant des substitutions uniques pour chaque lettre, rendant les messages incompréhensibles sans la clé.

## 2 Usage de symboles pour la complexité

- Certains caractères ou symboles étaient également utilisés pour représenter des mots entiers ou des noms propres, ajoutant un niveau de complexité au code.
- Par exemple, un symbole spécifique pouvait représenter "reine" ou "assassinat", rendant les intentions moins évidentes pour quelqu'un qui n'avait pas la clé.

## 3 Transmissions secrètes

- Les lettres codées étaient cachées dans des objets ou dissimulées dans des envois apparemment inoffensifs, puis transmises à ses partisans par des messagers de confiance.

a b c d e f g h i k l m n o. p q r s t u x y z  
 o ‡ ʌ ⁂ a □ θ ∞ ∣ ð ʒ ∥ ∅ ∇ ∫ ∩ ∪ ∩ 7 8 9

Nulles ff. —. —. d. Dowbleth σ

and for with that if but where as of the from by  
 2 3 4 4 4 3 ʒ ʒ m ʒ x ∞

so not when there this in wich is what say me my wyrt  
 ʒ x ‡ ʒ ʒ x ʒ m n m m d

send lre receave bearer I pray you Mte your name myne  
 ʒ ∫ ʒ T I I I I ʒ ʒ ss

Génie Informatique : Génie Logiciel

# Étapes de décryptage par Walsingham

## 1 Interception des messages

- Walsingham, le conseiller en chef et espion de la reine Élisabeth I, avait des agents qui interceptaient systématiquement les communications suspectes de Mary Stuart.
- Les lettres interceptées étaient remises à son équipe de cryptanalystes pour analyse.

## 2 Analyse de la structure des codes

- Les analystes ont d'abord observé la structure et les motifs de la substitution dans le code, notant les symboles et leurs fréquences dans les messages.

## 3 Analyse de fréquence

- L'équipe de Walsingham a appliqué l'analyse de fréquence pour identifier les lettres les plus utilisées dans le message chiffré.
- En comparant ces fréquences avec celles de la langue anglaise, ils ont pu faire des hypothèses sur les lettres ou symboles courants, facilitant l'identification de certains caractères.

# Étapes de décryptage par Walsingham (suite)

## 1 Identification de mots courants

- Les analystes ont cherché à identifier des mots typiques qui apparaissent dans les lettres politiques et militaires de l'époque, comme "reine", "roi", et "complot".
- Ils ont testé des substitutions pour ces mots courants, ce qui a permis de découvrir davantage de substitutions précises.

## 2 Déchiffrement complet

- Une fois les mots et lettres de base identifiés, l'équipe de cryptanalystes a pu compléter le reste du message, obtenant ainsi une version lisible du texte.
- Le message décrypté de Mary Stuart contenait des preuves explicites de son implication dans le complot contre Élisabeth I.

## 3 Utilisation de la preuve au procès

messages décryptés ont été utilisés comme preuves pour accuser Mary Stuart de trahison. Ces preuves solides ont convaincu le tribunal de son implication dans le complot, conduisant à sa condamnation et à son exécution en 1587.

(1854) ♦ États-Unis

- **Le carré de Polybe** est une technique cryptographique qui utilise une grille pour coder les lettres d'un message. La méthode de Playfair, développée par Charles Wheatstone et souvent attribuée à son ami Lord Playfair, améliore la sécurité en utilisant un chiffrement par paires de lettres, rendant le message plus difficile à déchiffrer.



Figure: Charles Wheatstone

# Utilisation du carré de Polybe et du chiffre Playfair

## 1 Carré de Polybe

- Un carré de Polybe est une grille de 5x5 (ou 6x6) contenant l'alphabet, où chaque lettre est représentée par ses coordonnées dans la grille.
- Par exemple, pour un carré de 5x5 avec les lettres "I" et "J" regroupées, la lettre "A" pourrait être codée en "11", "B" en "12", etc.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

## 2 Chiffre Playfair

- Le chiffre Playfair utilise une grille similaire mais encode les lettres en paires (digrammes) au lieu de les coder individuellement.
- Chaque lettre du message est combinée par paire. Par exemple, dans le mot "HELLO", les lettres sont regroupées en "HE" et "LO."

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

# Règles de chiffrement Playfair

- **Lettres identiques dans un digramme** : Si une paire contient deux lettres identiques, une lettre "X" est insérée entre elles (par exemple, "LL" devient "LXL").
- **Lettres dans la même ligne** : Si les deux lettres d'un digramme se trouvent sur la même ligne du carré, chacune est remplacée par la lettre à sa droite (en revenant au début de la ligne si nécessaire).
- **Lettres dans la même colonne** : Si elles sont dans la même colonne, chaque lettre est remplacée par celle située juste en dessous (en remontant en haut de la colonne si nécessaire).
- **Lettres dans des lignes et colonnes différentes** : Si les lettres sont dans des positions différentes, elles forment un rectangle, et chaque lettre est remplacée par la lettre se trouvant sur la même ligne dans l'autre coin du rectangle.



## 1854 – Charles Babbage : Brise le chiffre de Vigenère

- **Charles Babbage**, mathématicien et inventeur britannique, a réussi à casser le chiffre de Vigenère en 1854, bien que ses travaux soient restés non publiés. Le chiffre de Vigenère, un des premiers chiffres polyalphabétiques, avait longtemps été réputé incassable. Babbage a identifié des failles dans ce chiffrement en exploitant les répétitions dans les textes chiffrés.

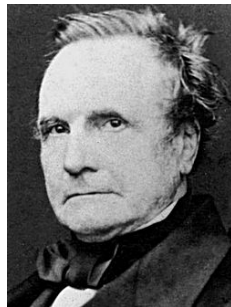


Figure: Charles Babbage

# Méthode utilisée pour casser le chiffre de Vigenère

## 1 Analyse des répétitions

- Babbage a commencé par rechercher des séquences répétées dans le texte chiffré. Ces répétitions peuvent révéler des indices sur la longueur de la clé utilisée pour le chiffrement.

## 2 identification de la longueur de la clé (période)

- En repérant les intervalles entre les répétitions de certaines séquences, Babbage a pu déterminer la longueur probable de la clé, appelée "période".
- Une fois la longueur de la clé identifiée, le texte peut être traité comme plusieurs messages codés avec des chiffres de César distincts.

## 3 Diviser le message en sous-textes

- Le texte chiffré est ensuite divisé en plusieurs sous-textes, chacun étant chiffré avec un décalage constant correspondant à une lettre de la clé.

## 1 Analyse de fréquence sur les sous-textes

- Pour chaque sous-texte, Babbage a appliqué une analyse de fréquence afin de trouver les lettres les plus courantes, qui révèlent des indices sur le décalage de César appliqué dans chaque position de la clé.

## 2 Déchiffrement du texte

- En utilisant les décalages identifiés pour chaque sous-texte, Babbage a pu reconstituer la clé complète et déchiffrer le message entier.

# La Cryptographie durant les GMs, Cryptage Informatique

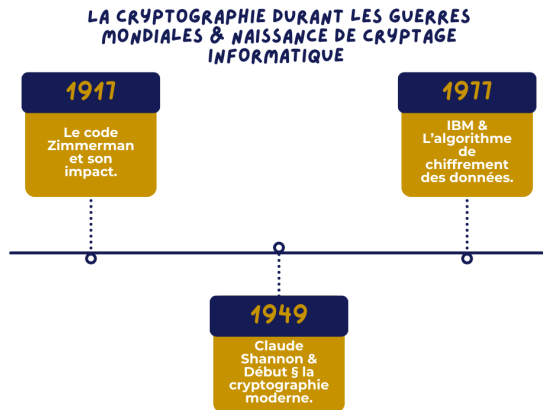


Figure : Timeline de la section

## Première Guerre mondiale (1917) : Le code Zimmermann

**Télégramme Zimmermann**, télégramme codé envoyé le 16 janvier 1917 par le ministre allemand des Affaires étrangères **Arthur Zimmermann** au ministre allemand au Mexique.

La note révèle un projet de reprise de la guerre sous-marine sans restriction et d'alliance avec le Mexique et le Japon si les États-Unis déclarent la guerre à l'Allemagne. Le message a été intercepté par les Britanniques et transmis aux États-Unis ; sa publication a suscité l'indignation et a contribué à l'entrée des États-Unis dans la Première Guerre mondiale.



Figure: : Arthur Zimmermann

- **Chiffrement par substitution de mots:**

Le message utilise un code où chaque mot ou phrase est remplacé par un nombre

- **Livre de code et clé:**

Seuls les diplomates allemands possèdent ce dictionnaire, qui est essentiel pour encoder et décoder les messages, car il convertit les mots en chiffres spécifiques.

- **Pattern-matching et fragments connus:**

En possession de fragments de codes allemands interceptés auparavant, utilisent ces éléments pour identifier des motifs dans le message Zimmermann.

- **Analyse de fréquence:**

En étudiant la fréquence des nombres dans le message, les cryptanalystes déduisent des mots-clés, ce qui aide à reconstituer le contenu.

- **Reconstruction du message:**

Grâce à ces techniques, les Britanniques parviennent à décoder le message, révélant l'offre d'alliance entre l'Allemagne et le Mexique.

# Zimmermann Code

**WESTERN UNION TELEGRAM**

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

GERMAN LEGATION  
MEXICO CITY

via Galveston

JAN 19 1917

862.20219/728

130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13805	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11249	18276	18101	0317	0228	17694	4473	
22284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21001	17388	7446	23638	18222	6719	14331	15021	23845	
3156	23552	22096	21604	4797	9497	22464	20855	4377	

Figure : Message Crypté de Telegramme Zimmermann

## Claude Shannon (1949) : Théorie de la communication et fondements de la cryptographie moderne

**Claude Shannon**, un ingénieur et mathématicien américain, est souvent considéré comme le père de la cryptographie moderne grâce à son travail fondateur en 1949. Dans son article "Communication Theory of Secrecy Systems", Shannon développe les concepts théoriques qui restent les fondements de la cryptographie. Il introduit le concept de sécurité parfaite, qui stipule qu'un système de chiffrement est inviolable si l'on utilise une clé aussi longue que le message, aléatoire et utilisée une seule fois (le one-time pad).

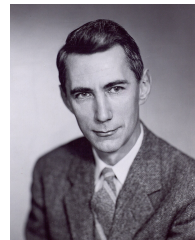


Figure: : claude shannon



## Sécurité parfaite

- **Principe de la sécurité parfaite** : Un système de chiffrement est parfaitement sécurisé si un attaquant, même avec un temps de calcul illimité, ne peut pas deviner le contenu du message sans la clé.
- **One-time pad**: Shannon démontre que la sécurité parfaite est atteinte uniquement si la clé est aléatoire, aussi longue que le message, et utilisée une seule fois.
- **Indépendance entre message et clé** : Avec la sécurité parfaite, chaque caractère chiffré est indépendant des autres, empêchant tout lien statistique exploitable entre le texte chiffré et le texte clair.

## Entropie

- **Mesure de l'incertitude** : L'entropie est utilisée pour mesurer l'incertitude ou le hasard d'un système de cryptage. Plus l'entropie est élevée, plus il est difficile de prédire le contenu du message.
- **Complexité des clés** : Shannon explique que plus une clé est complexe et aléatoire, plus l'entropie est élevée, et donc plus le message est sécurisé.
- **Lien avec le chiffrement** : En maximisant l'entropie (càd la quantité d'aléatoire), le système de chiffrement devient résistant aux attaques statistiques, car il ne présente aucun motif exploitable.

En résumé, la sécurité parfaite assure une protection absolue sous des conditions idéales, tandis que l'entropie mesure le niveau d'aléatoire requis pour que le chiffrement soit robuste et difficile à déchiffrer.

# Algorithme de Shannon

Formellement, un algorithme de Shannon est une paire de fonctions de cryptage (E) et de décryptage (D) :

$$\mathcal{E} = (E, D)$$

- **Cryptage** : La fonction de chiffrement E prend en entrée une clé k et un message m, pour produire un texte chiffré c. Autrement dit,  $c = E(k, m)$ . c.à.d le chiffrement de m sous k.
- **Décryptage** : La fonction de décryptage D prend en entrée une clé k et un texte chiffré c, pour produire un message m. Autrement dit,  $m = D(k, c)$ , c.à.d m est le décryptage de c sous k.
- **Propriété de correction** Le décryptage "annule" le cryptage, c.à.d que le système de cryptage doit satisfaire à la propriété de correction suivante : pour toutes les clés k et tous les messages m,  $D(k, E(k, m)) = m$ , c.à.d m est le décryptage de E(k, m) sous k.

# Algorithme de Shannon

En cryptographie, un tampon à usage unique (OTP) est une technique de cryptage qui ne peut pas être craquée (ne peut pas être calculée).

## Definition de OTP

Un tampon à usage unique est un chiffrement de Shannon  $\mathcal{E} = (E, D)$  où les clés ( $k$ ), les messages ( $m$ ) et les textes chiffrés ( $c$ ) sont des chaînes de bits de même longueur. En d'autres termes, le chiffrement de Shannon à tampon unique  $\mathcal{E}$  est défini sur  $(K, M, C)$ , où

$$\mathcal{K} := \mathcal{M} := \mathcal{C} := \{0, 1\}^L$$

pour un paramètre fixe  $L$ . Pour une clé  $K \in \{0, 1\}^L$  et un message  $m \in \{0, 1\}^L$ , la fonction de chiffrement  $E(k, m)$  est définie comme  $k \oplus m = c$ , où  $\oplus$  désigne l'addition modulo 2 dans le sens des composantes.

One time pads fonctionnent en associant un message  $m$  en clair à une clé secrète aléatoire (appelée pavé à usage unique). Ensuite, chaque bit ou caractère du message est chiffré en le combinant avec le bit ou caractère correspondant du bloc-notes à l'aide de l'arithmétique modulaire. Si le bloc-notes à usage unique utilisé présente les propriétés suivantes :

- 1 Il est véritablement aléatoire;
- 2 Il est au moins aussi long que le texte en clair;
- 3 Il n'est jamais réutilisé en tout ou en partie;
- 4 Il est gardé complètement secret. Il est gardé complètement secret ; on peut alors démontrer que le texte chiffré est impossible à décrypter ou à déchiffrer, c'est-à-dire qu'il est **parfaitement sûr**.

## IBM (1977) : L'algorithme de chiffrement des données

Le 15 mai 1973 le NBS (National Bureau of Standards, aujourd'hui NIST) a lancé un appel dans le Federal Register pour la création d'un algorithme de chiffrement répondant aux critères suivants :

- posséder un haut niveau de sécurité lié à une clé de petite taille servant au chiffrement et au déchiffrement
- être compréhensible
- ne pas dépendre de la confidentialité de l'algorithme
- être adaptable et économique
- être efficace et exportable

Fin 1974, IBM propose "Lucifer", qui, grâce à la NSA, est modifié le 23 novembre 1976 pour donner le DES (Data Encryption Standard). Le DES a finalement été approuvé en 1978 par le NBS.

## Description du fonctionnement du DES

Le DES est un algorithme de chiffrement par bloc de 64 bits, c'est-à-dire que le texte est d'abord découpé en bloc de 64 bits et que l'on applique l'algorithme à chaque bloc. Comme précisé plus haut, la clé de chiffrement comporte elle aussi 64 bits, même si seuls 56 bits sont utiles, les 8 bits restant étant des bits de contrôle destinés à éviter les erreurs de transmission.

Les grandes lignes de l'algorithme sont :

### Phase 1 : Préparation - Diversification de la clé:

On diversifie la clé  $K$ , c'est-à-dire qu'on fabrique à partir de  $K$  16 sous-clés  $K_1, \dots, K_{16}$  à 48 bits. Les  $K_i$  sont composés de 48 bits de  $K$ , pris dans un certain ordre.

# IBM et l'algorithme DES

## Phase 2 : Permutation initiale:

Pour chaque bloc de 64 bits  $X$  du texte, on calcule une permutation  $Y = P(X)$ .  $Y$  est représenté sous la forme  $Y = G_0 D_0$ ,  $G_0$  étant les 32 bits à gauche de  $y$ ,  $D_0$  les 32 bits à droite.

## Phase 3 : Itération - Schéma de Feistel

On applique 16 tours d'un même schéma de Feistel. A partir de  $G_{i-1} D_{i-1}$  (pour  $i$  de 1 à 16), on calcule  $G_i D_i$  en posant :

$$G_i = D_{i-1}; \text{ et } D_i = G_{i-1} \oplus f(D_{i-1}, K_i)$$

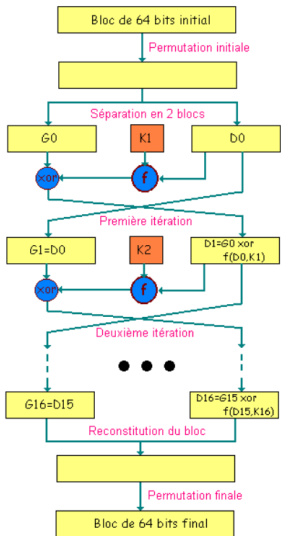
et  $f$  est une fonction de confusion, suite de substitutions et de permutations.

## Phase 4 : Permutation finale:

On applique à  $G_{16} D_{16}$  l'inverse de la permutation initiale.  $Z = P^{-1}(G_{16} D_{16})$  est le bloc de 64 bits chiffré à partir de  $x$ .



# IBM et l'algorithme DES



# Débuts de la Cryptographie Moderne à Clé Publique et Internet

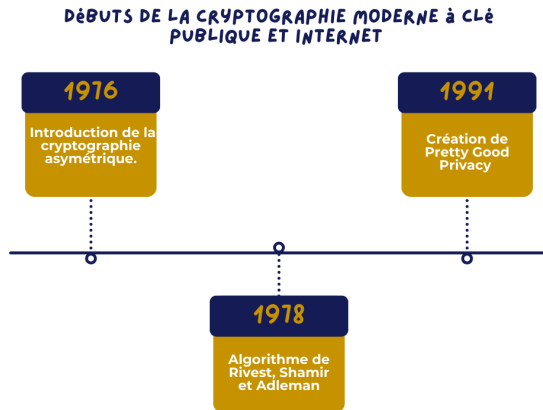


Figure : Timeline de la section

## Le Chiffrement asymétrique

Le chiffrement est la conversion de données appelées **texte en clair** en **texte chiffré**, ou le codage sécurisé de données à l'aide de **clés**, de sorte que le texte en clair ne puisse être récupéré à partir du texte chiffré qu'en utilisant une clé secrète pour garantir la sécurité des données. La cryptographie est la science du chiffrement. Le processus de chiffrement repose fondamentalement sur un certain nombre d'éléments. La **clé**, qui peut être un code ou un mot de passe, est le paramètre décisif du chiffrement. De nos jours, elle est générée automatiquement dans les processus informatiques afin d'éliminer le facteur humain et la menace d'utiliser un mot de passe qui n'est pas sûr.

## Le Déchiffrement

La "**clé**", qui peut être un code ou un mot de passe, est le paramètre décisif du chiffrement.

Le déchiffrement est nécessaire pour récupérer le texte en clair à partir du texte chiffré et nécessite une clé secrète. Dans les méthodes de chiffrement symétrique, on utilise la même que pour le chiffrement. Dans le chiffrement asymétrique, deux clés sont nécessaires.

Le terme "**déchiffrer**" n'est pas le même que "**décrypter**", car cela signifierait briser le code sans avoir accès à une ou plusieurs clés ou sans en avoir connaissance au préalable. C'est l'activité d'un cryptanalyste, souvent appelé **briseur de code**. Idéalement, il ne devrait pas être possible de déchiffrer un message grâce à un chiffrement suffisamment **fort**.

# La Cryptographie asymétrique

## CRYPTAGE ASYMÉTRIQUE

Le chiffrement symétrique

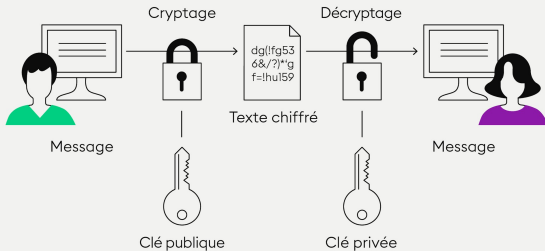


Figure : Cryptage asymétrique

## Cryptage RSA (1978) : un aperçu

Le cryptage RSA est un algorithme de cryptage à clé publique qui a été proposé pour la première fois par "Ron Rivest", "Adi Shamir" et "Leonard Adleman" en 1978. Le cryptage RSA fonctionne en utilisant une paire de clés - clés publiques et privées - pour crypter et décrypter les données. La clé publique est utilisée pour chiffrer les données, tandis que la clé privée est utilisée pour déchiffrer les données. Le chiffrement RSA est basé sur les

propriétés mathématiques **des grands nombres premiers**. L'algorithme fonctionne en générant deux grands nombres premiers,  $p$  et  $q$ , et en calculant leur produit,  $n=pq$ .

## Cryptage RSA : propriétés importantes

- **Sécurité:** Le chiffrement RSA est considéré comme une méthode de communication sécurisée, car la clé privée est nécessaire pour déchiffrer les données.
- **Évolutivité:** Le cryptage RSA peut être utilisé pour les messages petits et volumineux, ce qui en fait une méthode de communication évolutive.
- **Compatibilité:** Le cryptage RSA est largement pris en charge par les logiciels et le matériel, ce qui en fait une méthode de communication compatible.
- **La flexibilité:** Le cryptage RSA peut être utilisé dans diverses applications, notamment la messagerie sécurisée, le transfert de fichiers et les transactions en ligne.

## ① Sécurité :

- **Forte sécurité:** RSA est basé sur la difficulté mathématique de factoriser de grands entiers, ce qui le rend hautement sécurisé pour les signatures numériques.
- **Asymétrique :** Utilisation des clés améliore la sécurité car la clé privée est non partageable

## ② **Forte : Signatures numériques** RSA peut être utilisé pour créer des signatures numériques, vérifiant l'authenticité et l'intégrité d'un message ou d'un document.

## ③ **Non-répudiation : Preuve irréfutable** Une fois qu'un document est signé avec une clé privée, l'expéditeur ne peut pas nier l'authenticité de sa signature.



## ① Compatibilité :

- **Largement adopté:** RSA est une norme de chiffrement largement reconnue et utilisée, garantissant la compatibilité avec de nombreux systèmes et applications.
- **Interopérabilité:** Fonctionne bien avec d'autres protocoles et systèmes cryptographiques, ce qui le rend polyvalent pour différentes applications.

## ② Échange de clés sécurisé: Facilite l'échange sécurisé de clés dans les canaux publics, permettant de partager en toute sécurité des clés de chiffrement symétriques.

## 1 Performance:

- **Traitement lent:** Les processus de chiffrement et de déchiffrement RSA nécessitent des calculs intensifs et sont plus lents que les algorithmes de chiffrement symétriques.
- **Grandes tailles de clés:** nécessite des clés de grande taille (2 048 bits ou plus) pour maintenir la sécurité, ce qui peut ralentir davantage les performances.

## 2 Gestion des clés:

- **Gestion des clés complexes:** La gestion des clés publiques et privées peut être complexe, nécessitant un stockage et une manipulation sécurisés pour empêcher tout accès non autorisé.
- **Longueur de la clé:** À mesure que les exigences de sécurité augmentent, le besoin de clés plus longues augmente également, ce qui peut être fastidieux à gérer.

- 1 **Vulnérabilité à l'informatique quantique:** Le cryptage RSA pourrait potentiellement être brisé par les ordinateurs quantiques à l'avenir, car ils sont capables de factoriser de grands entiers beaucoup plus rapidement que les ordinateurs classiques.
- 2 **Taille du message limitée:** La taille maximale du message en clair pouvant être chiffré est limitée par la taille de la clé, ce qui nécessite souvent un traitement supplémentaire pour les grands ensembles de données.
- 3 **Configuration initiale complexe:** La configuration initiale du chiffrement RSA, y compris la génération et la distribution de clés, peut être plus complexe que celle des systèmes de chiffrement à clé symétrique.

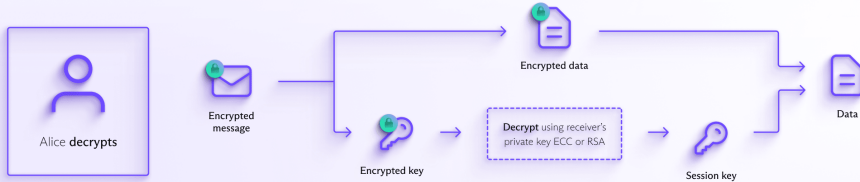
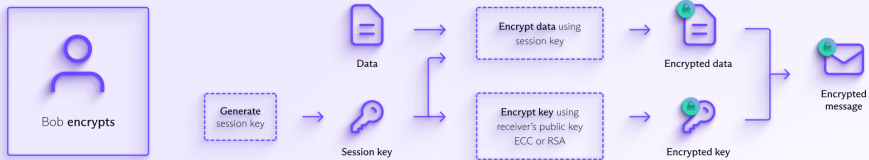
## Définition de PGP (1991)

PGP est une méthode de cryptage qui vous permet de communiquer en ligne en toute confidentialité. Il est généralement utilisé pour crypter les courriels, mais il peut également être utilisé pour crypter des fichiers et d'autres données.

Lorsque vous envoyez un courrier électronique à l'aide de PGP, le message est converti en texte chiffré illisible (nouvelle fenêtre) sur votre appareil avant d'être transmis sur l'internet. Seul le destinataire possède la clé permettant de reconvertir le texte en un message lisible sur son appareil.

PGP est également utilisé pour l'authentification. En fournissant un moyen de "**signer**" numériquement les courriels cryptés, PGP vous permet de vérifier que le message provient bien de la personne qui prétend être l'expéditeur et qu'il n'a pas été altéré en cours de route.

# Pretty Good Privacy -PGP-



# Les avancées de la Cryptographie Symétrique

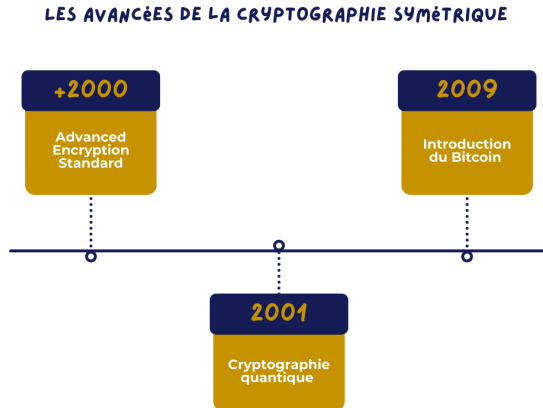


Figure : Timeline de la section

## Qu'est-ce que le cryptage AES ?

Le chiffrement AES, ou norme de chiffrement avancée, est un chiffrement par bloc symétrique utilisé pour chiffrer les données sensibles. Avec une sécurité et une vitesse égales, AES est devenu une norme de sécurité pour les utilisateurs et les applications qui ont besoin d'un chiffrement facile à utiliser.

Cette méthode a été conceptualisée pour la première fois en 1997 lorsque le National Institute of Standards and Technology (NIST) est devenu vulnérable aux attaques par force brute et avait besoin d'une méthode de cryptage plus puissante. Le NIST a engagé des développeurs pour résoudre le problème – Vincent Rijmen et Joan Daemen – qui ont développé la technologie finalement sélectionnée, AES, en 1998.

AES est la norme de chiffrement du NIST depuis son adoption à grande échelle en 2002.

## Les types d'AES

- AES-128 : Cette méthode utilise une longueur de clé de 128 bits pour le chiffrement et le déchiffrement, ce qui donne 10 cycles de chiffrement avec  $3,4 \times 10^{38}$  combinaisons potentielles différentes.
- AES-192 : Cette méthode utilise une longueur de clé de 192 bits pour le chiffrement et le déchiffrement, ce qui donne 12 cycles de chiffrement avec  $6,2 \times 10^{57}$  combinaisons potentielles différentes.
- AES-256 : Cette méthode utilise une longueur de clé de 256 bits pour le chiffrement et le déchiffrement, ce qui donne 14 cycles de chiffrement avec  $1,1 \times 10^{77}$  combinaisons potentielles différentes.

Pourquoi ces différents types d'AES ? Tout dépend du cas d'utilisation spécifique. AES-256 est la plus puissante, mais son exécution nécessite beaucoup plus de puissance de traitement, de temps et de ressources qu'AES-128.



# Advanced Encryption Standard

## LES BASES DU CRYPTAGE AES



Une méthode de cryptage qui utilise plusieurs cycles de transposition, de substitution et de mélange



Se décline en trois variétés : AES-128, AES-192 et AES-256



Considéré comme la norme de l'industrie pour la sécurité des données commerciales et personnelles

## À quoi sert AES

- **Les VPN** : le travail d'un réseau privé virtuel (VPN) consiste à fournir une navigation en ligne sécurisée et privée. Étant donné que ce processus connecte les utilisateurs à différents serveurs, le cryptage AES est utilisé pour protéger les données des utilisateurs contre les fuites et les cyberattaques.
- **Les gestionnaires de mots de passe** : pour stocker en toute sécurité les identifiants de connexion sous une seule clé principale. Étant donné qu'une seule violation pourrait compromettre l'ensemble de la collection de mots de passe d'un utilisateur, AES est souvent utilisé pour sécuriser ce logiciel.
- **Le Wi-Fi** : l'internet sans fil utilise généralement de nombreuses méthodes de cryptage telles que WPA2.
- **Les applications mobiles** : Toute application qui implique la messagerie ou le partage de photos utilise généralement AES pour contribuer à la sécurité des données.



## **AES-128 contre AES-256**

Ce sont deux variantes d'AES.  
AES-128 est bon pour les petits cas  
d'utilisation, tandis que AES-256  
est une sécurité de niveau  
gouvernemental.



## AES contre RSA

Les principales différences sont la vitesse et la complexité. AES a une clé longue, ce qui le rend plus fort – RSA a deux clés plus courtes, ce qui le rend plus rapide.



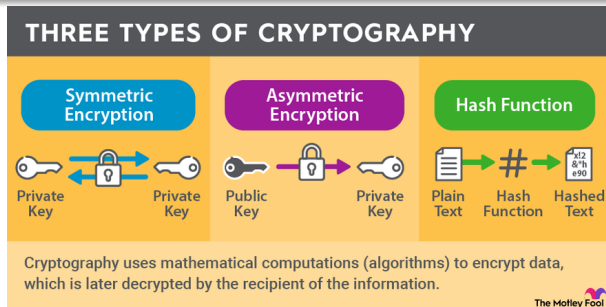
**AES contre DES**

AES est considéré comme l'évolution la plus forte du DES. DES n'a qu'une clé de 56 bits, tandis qu'AES a des clés de 128, 192 et 256 bits.

# Introduction du crypto-monnaies

## Cryptage asymétrique et crypto-monnaies (2009 - aujourd'hui)

Les crypto-monnaies restent sûres en s'appuyant sur des méthodes modernes de cryptage asymétrique et sur la nature sécurisée des transactions sur une blockchain. Les détenteurs de crypto-monnaies utilisent des clés privées pour vérifier qu'ils sont bien les propriétaires de leur crypto-monnaie. Les transactions sont sécurisées par des techniques de hachage et de cryptage de la blockchain.



## Définition de la cryptographie quantique(2001 - Future)

La cryptographie quantique (également connue sous le nom de chiffrement quantique) fait référence à diverses méthodes utilisées en cybersécurité pour chiffrer et transmettre des données sécurisées en fonction des lois de la nature immuables de la mécanique quantique. Bien qu'il n'en soit encore qu'à ses balbutiements, le chiffrement quantique a le potentiel de devenir un mécanisme bien plus sécurisé que les autres types d'algorithmes cryptographiques qui l'ont précédé. Et en théorie, il est même impossible à pirater.

# Cryptographie quantique

## Comment ça marche ?

Contrairement à la cryptographie traditionnelle, qui repose sur les mathématiques, la cryptographie quantique repose sur les lois de la physique. Elle repose plus précisément sur les principes uniques de la mécanique quantique :

- Les particules sont intrinsèquement incertaines
- Les photons peuvent être mesurés aléatoirement dans des positions binaires
- Un système quantique ne peut pas être mesuré sans être modifié
- Les particules peuvent être partiellement, mais pas totalement clonées

## Le problème ?

**Algorithme de Shor pour la factorisation :** Conçu pour briser la cryptographie RSA, cet algorithme quantique trouve efficacement les facteurs premiers d'un nombre très grand, rendant obsolètes les systèmes basés sur la difficulté de la factorisation.



## Chiffrement par réseaux (Lattice-based cryptography) :

Basé sur des problèmes mathématiques de réseaux (lattice problems), il est conçu pour être résistant aux algorithmes quantiques, en particulier contre l'algorithme de Shor. Il utilise des opérations vectorielles pour rendre la décryption difficile sans la clé.

## Code-based cryptography (McEliece) :

Cet algorithme utilise des codes correcteurs d'erreurs pour chiffrer les données. Résistant aux attaques quantiques, il utilise des matrices pour encoder le message, rendant le déchiffrement sans clé pratiquement impossible.

## Multivariate Polynomial Cryptography :

Utilise des équations polynomiales multivariées pour générer des clés et chiffrer des données. Les algorithmes quantiques ont du mal à résoudre efficacement ces équations, ce qui en fait une option prometteuse pour la cryptographie post-quantique.

## Supersingular Isogeny Diffie-Hellman (SIDH) :

Utilise des isogénies de courbes elliptiques supersingulières pour créer des clés partagées. Ce type de chiffrement post-quantique est résistant à certaines attaques par calcul quantique, car il est difficile de calculer les isogénies sans la clé privée.