Cryptographie appliquée

Pr. Hasnae L'AMRANI

Filière : Sécurité IT
&
confiance numérique

Cryptographie Classique

Introduction à la Cryptographie

- Introduction, définition et historique
- Terminologie
- Cryptographie classique

Introduction à la Cryptographie

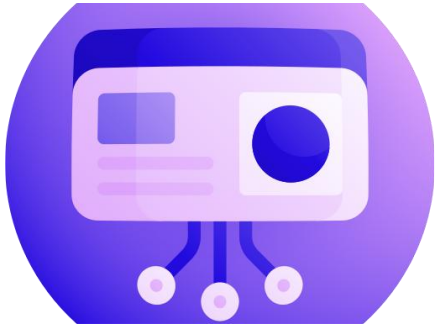
- La cryptographie dans tous les domaines.

Armée

Systèmes bancaires

Achats en ligne

TV payante

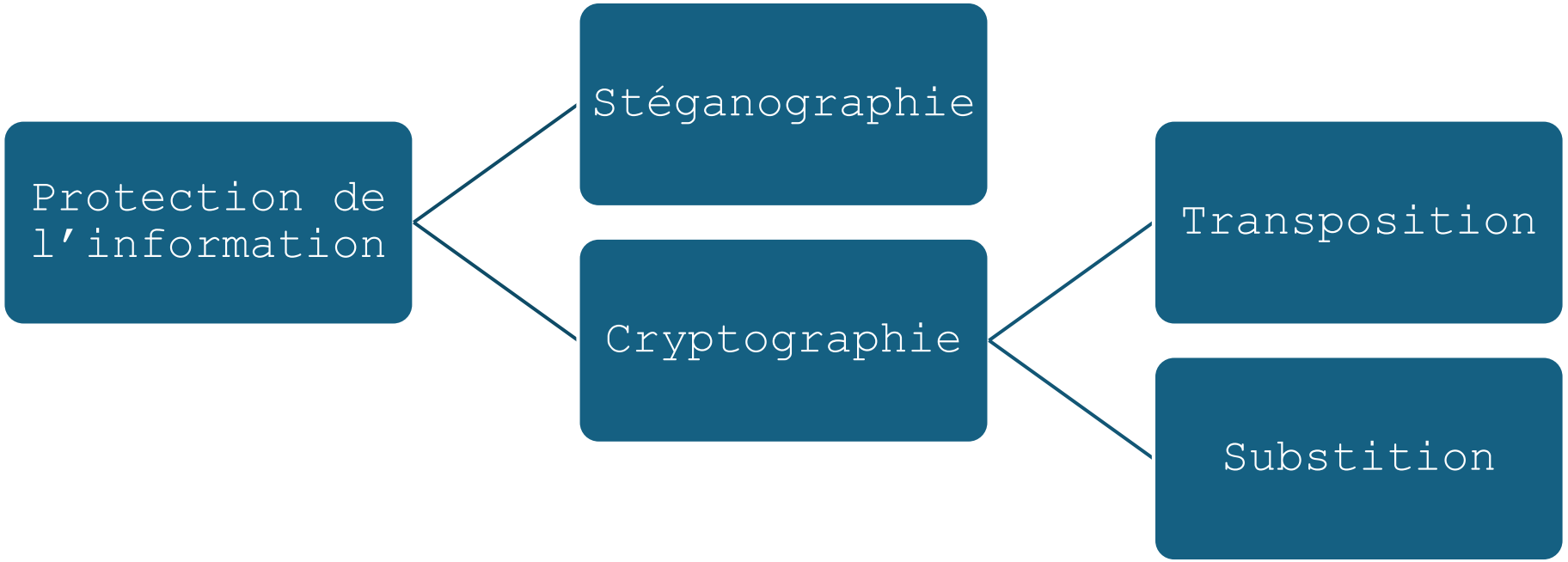


Carte d'identité électronique

Mobiles

Introduction à la Cryptographie

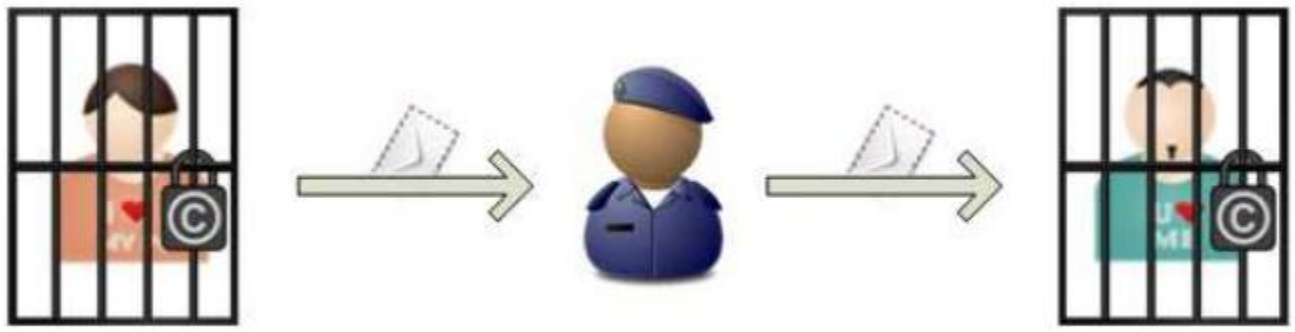
Pour protéger une information



Introduction à la Cryptographie : Stéganographie

- La stéganographie (du grec **stegano** = **dissimuler**, **stéganographie** = **écriture dissimulée**)

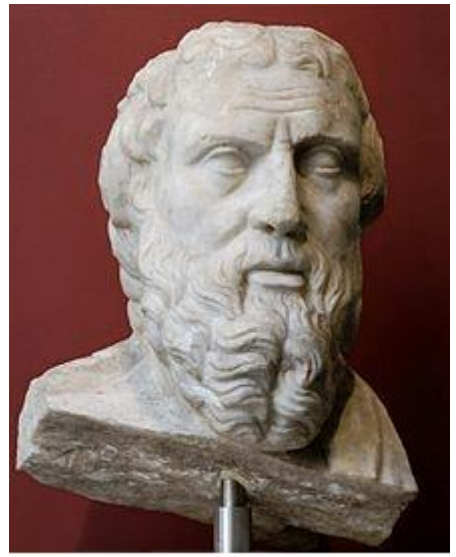
- Stéganographie : L'information n'est pas modifiée, mais elle est cachée.



Introduction à la Cryptographie : Stéganographie

- **Apparition de la stéganographie**

- La première trace écrite se trouve dans les Histoires de Hérodote parues vers 445 av J.-C.
- Une méthode ancienne consiste à raser la tête d'un esclave fidèle, à tatouer le message sur son crâne, puis à attendre que ses cheveux repoussent. Une fois la chevelure redevenue normale, l'esclave est envoyé.

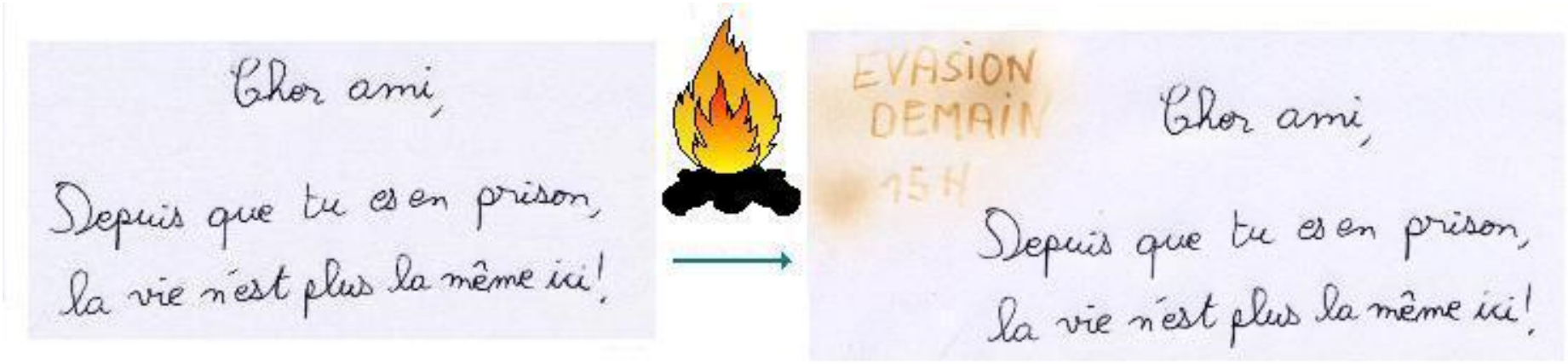


Hérodote

Introduction à la Cryptographie : Stéganographie

Écritures dissimulées

- La stéganographie ancienne utilisait des encres invisibles (jus de citron, lait…) pour cacher des messages dans un texte normal.
- Invisibles à l'œil, ils étaient révélés par la chaleur ou un réactif chimique.
- Par exemple, un message écrit au lait apparaît sous l'effet d'une flamme.



Introduction à la Cryptographie : Stéganographie

Écritures dissimulées

Une autre méthode très répandue de stéganographie est de dissimuler le message dans le texte lui-même.

A. Le ciel était d'un bleu éclatant.
B. Les nuages semblaient immobiles.
C. Un vent doux soufflait à travers les champs.
D. Les fleurs s'ouvraient lentement au soleil.
E. Les abeilles butinaient avec diligence.
F. Un ruisseau serpentait entre les arbres.
G. Le chant des oiseaux remplissait l'air.
H. Une famille de lapins traversait le chemin.
I. Les enfants couraient en riant.
J. Leur joie était contagieuse.
K. Un vieil homme observait la scène avec un sourire.
L. Il se souvenait de ses propres souvenirs d'enfance.
M. Le temps semblait s'être arrêté.
N. Les montagnes se dressaient à l'horizon.
O. Leur silhouette était majestueuse.
P. Un aigle planait haut dans le ciel.
Q. L'herbe était fraîche sous les pieds.
R. L'odeur de la terre humide flottait dans l'air.
S. La nature semblait en harmonie.
T. Le bruit des feuilles bruissait doucement.
U. Un chien aboyait au loin.
V. Le calme régnait malgré tout.
W. Une clôture en bois délimitait le pré.
X. Chaque détail avait sa place.
Y. C'était une journée parfaite.
Z. Rien ne pouvait gâcher ce moment

La nature semblait en harmonie. Les enfants couraient en riant. Le bruit des feuilles bruissait doucement. Un vent doux soufflait à travers les champs. Les montagnes se dressaient à l'horizon.

SITCN

Introduction à la Cryptographie : Stéganographie

Stéganographie moderne

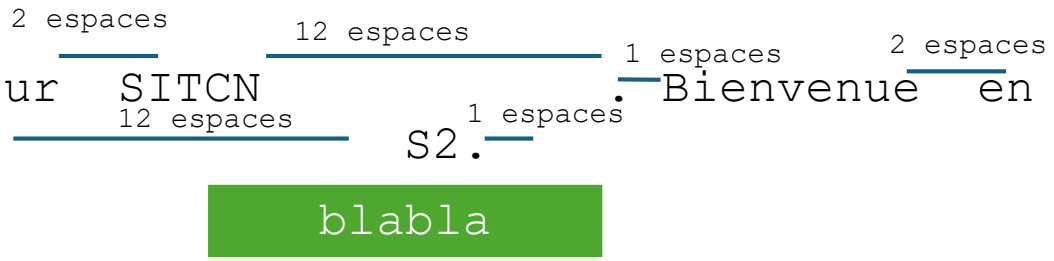
- Sur le plan numérique, il y plusieurs types principaux de stéganographie:
  - Stéganographie textuelle
  - Stéganographie d'images
  - Stéganographie vidéo
  - Stéganographie audio
  - Stéganographie réseau

Introduction à la Cryptographie : Stéganographie

Stéganographie moderne

Stéganographie textuelle

On peut cacher des messages dans des pages web en utilisant les espaces HTML : insérer un nombre d'espaces correspondant à une lettre (1 pour A, 2 pour B, etc.) entre les mots. Cette technique exploite le fait le navigateur n'affichera qu'un seul espace.

Affichage dans le navigateur	Code source
Bonjour SITCN. Bienvenue en S2.	

Introduction à la Cryptographie : Stéganographie

Stéganographie moderne

Stéganographie d'images /tatouage (watermarking)

- Cacher un texte dans une image
- Il existe plusieurs techniques de stéganographie.
- **Technique LSB : Least Significant Bit**
  - Dans le cas d'une image, elle consiste à modifier le bit de poids faible des pixels codant l'image.
  - Une image numérique est une suite de pixel, et dont on code la couleur, le plus souvent, à l'aide d'un triplet d'octets(ex : RGB sur 24 bits).
  - Chaque octet du triplet ∈ [0, 255] peut être modifié de +/ - 1 sans que la teinte du pixel ne soit visuellement altérée.
  - C'est ce que l'on fait en modifiant le bit de poids faible de l'octet.

Introduction à la Cryptographie : Stéganographie

Stéganographie moderne

Stéganographie d'images /tatouage (watermarking)

Exemple : Imaginons que
les trois pixels suivantes :

$$\{10110101, 11101010, 10010101\},$$
$$\{11101010, 10110101, 00100100\},$$
$$\{10110101, 11010101, 10101010\}$$

On va cacher le caractère 'x ' : Code ASCII: 88
Représentation binaire : **01011000**

Les trois pixels seront modifiés par substitution du LSB

$$\{10110101, 11101010, 10010101\},$$
$$\{11101010, 10110101, 00100100\},$$
$$\{10110101, 11010101, 10101010\}$$

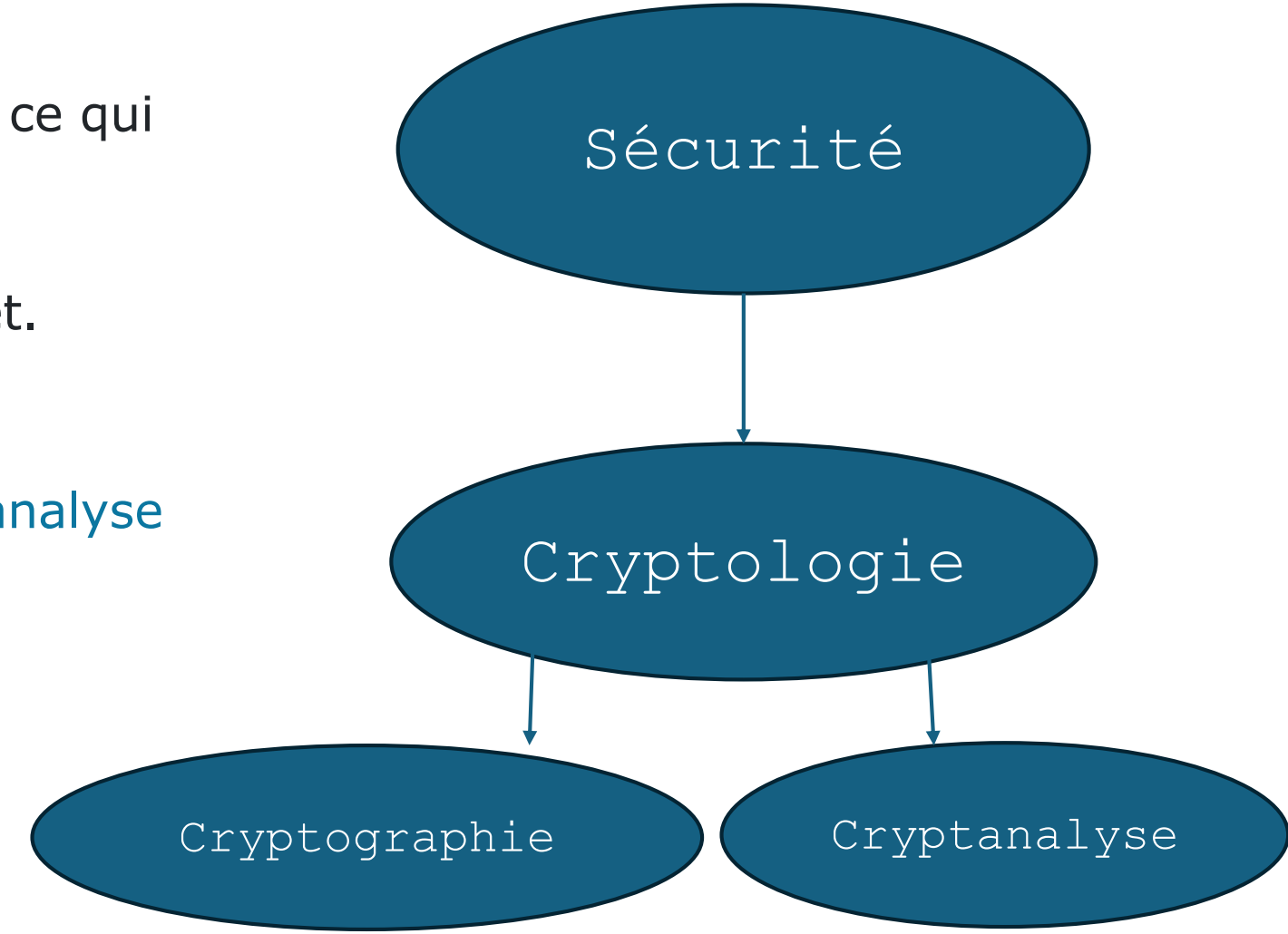
$$\{10110100, 11101011, 10010100\},$$
$$\{11101011, 10110101, 00100100\},$$
$$\{10110100, 11010100, 10101010\}$$

≈

Introduction à la Cryptographie : Cryptographie

- Le terme « crypto » fait référence à ce qui est secret ou cache.
- Cryptologie c'est la science du secret.

Cryptologie = Cryptographie + Cryptanalyse



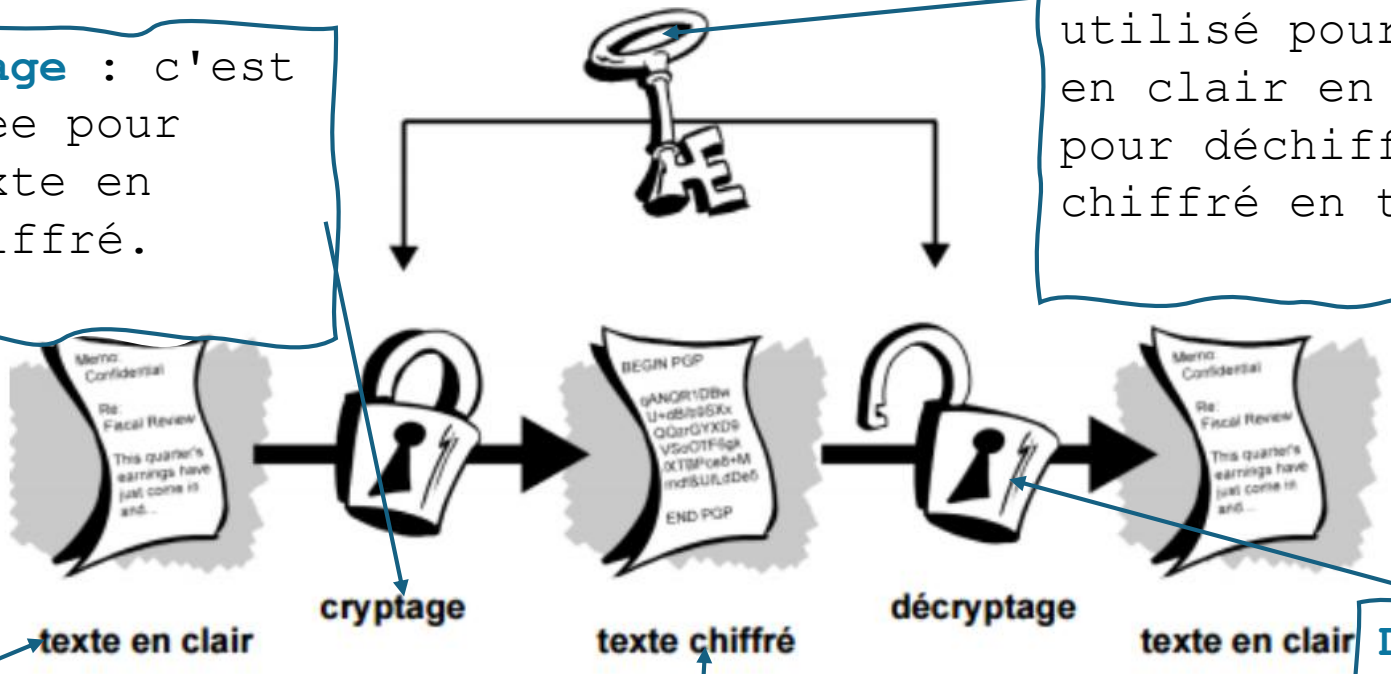
La Cryptographie

- La **cryptographie** est l'art de rendre un **message incompréhensible** pour ceux qui ne sont pas habilités à en prendre connaissance.
- Le terme «**Cryptanalyse** » est dérivé des mots grecs kryptós (« caché ») et analýein (« analyser »). Il s'agit du processus consistant à analyser des messages dissimulés en **déchiffrant** des données, même sans disposer de la **clé** de chiffrement.

La Cryptographie : Terminologies

Chiffrement/Cryptage : c'est la méthode utilisée pour transformer un texte en clair en texte chiffré.

Clé : c'est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair.



Texte en clair : c'est le message à protéger.

Texte chiffré : c'est le résultat du chiffrement du texte en clair.

Déchiffrement/Décryptage : c'est la méthode utilisée pour transformer un texte chiffré en texte en clair.

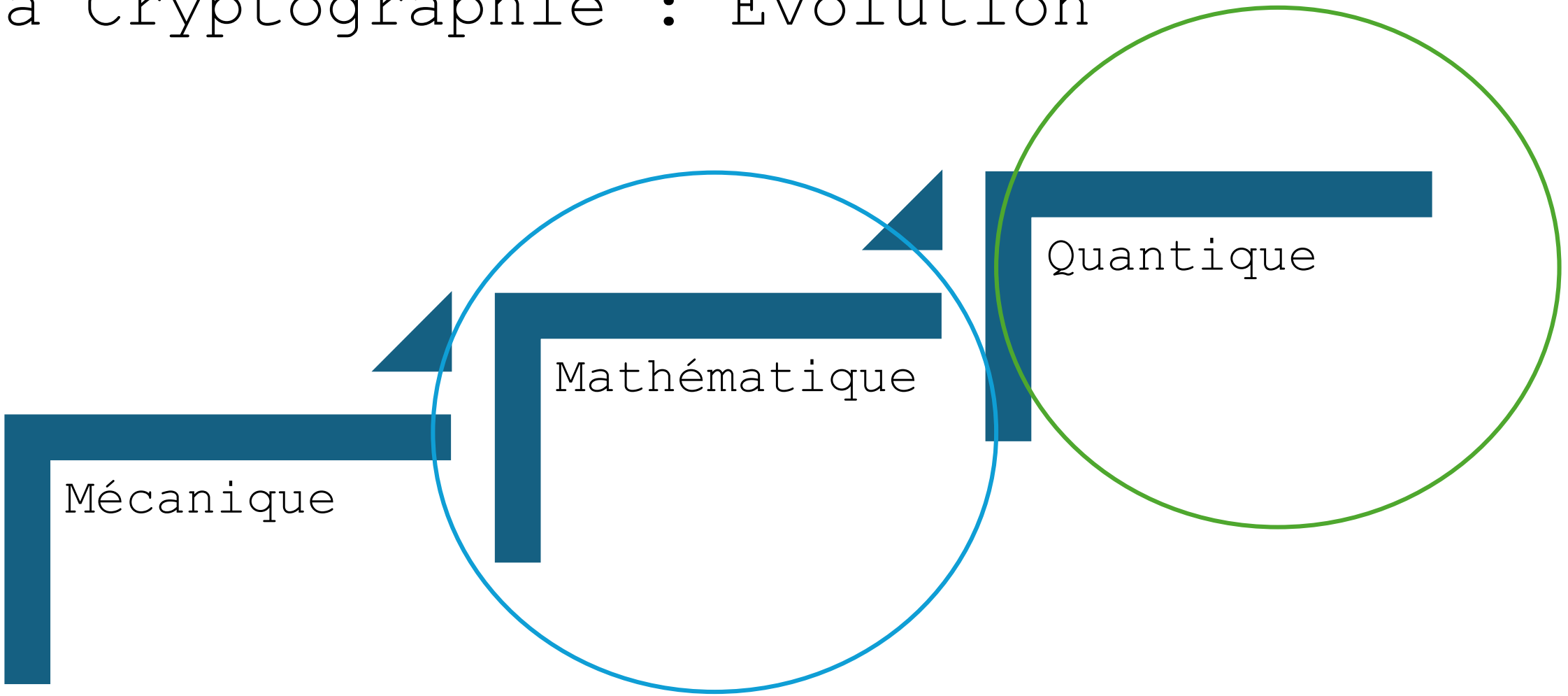
La Cryptographie : Terminologies

- **Texte en clair** : c'est le message à protéger : **M**
- **Clé** : **K** Information permettant de chiffrer/déchiffrer un message **M**
- **Chiffrement** : Fonction de transformation d'un message **M** en message incompréhensible : **C = E (M)**
- **Déchiffrement** : Fonction de reconstruire le message clair du message chiffré : **D (C) = D (E (M)) = M**
- **Texte chiffré** : c'est le résultat du chiffrement du texte en clair : **C**

$$E_{Ke}(M) = C \rightarrow \text{Chiffrement}$$

$$D_{Kd}(C) = M \rightarrow \text{Déchiffrement}$$

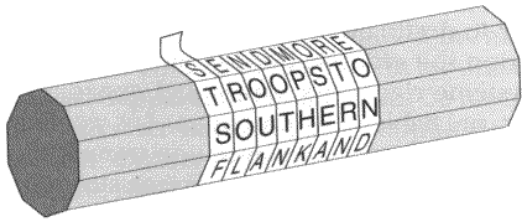
La Cryptographie : Evolution



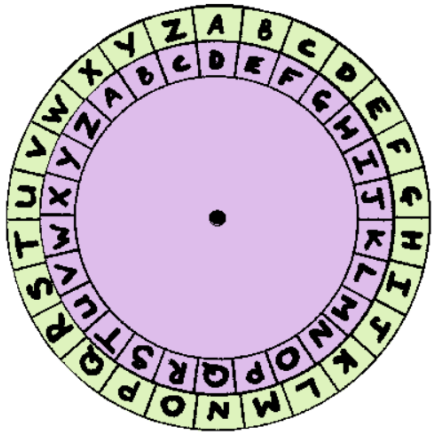
La Cryptographie : Catégories

- **Cryptographie** : L'information est modifiée selon une méthode préétablie afin de la rendre incompréhensible.
- Il existe deux grandes catégories de la **cryptographie** :
  - **Transposition** : L'information est gardée mais sa position qui est décalée (l'ordre des éléments d'une information est modifié).
  - **Substitution** : Les éléments d'une information sont remplacés par d'autres (exemple : replacer tous les A par B et tous les B par C).

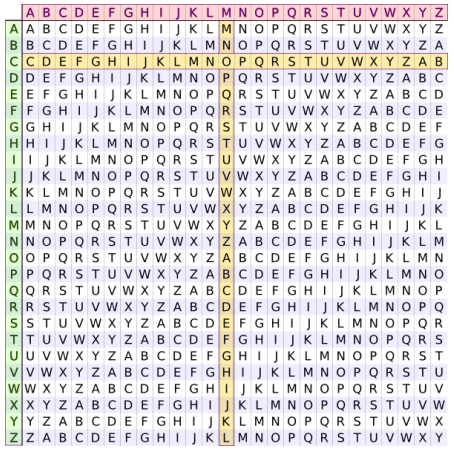
Cryptographie classique



Le Scytale



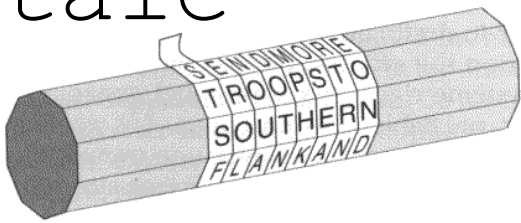
Le code de César



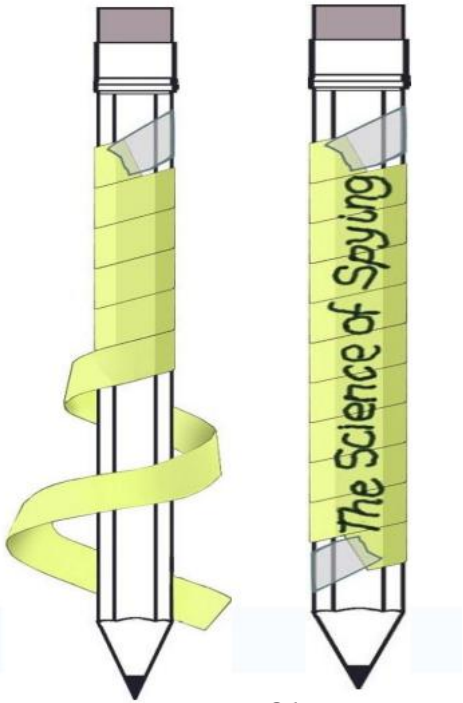
Le code de Vigenère

La machine Enigma

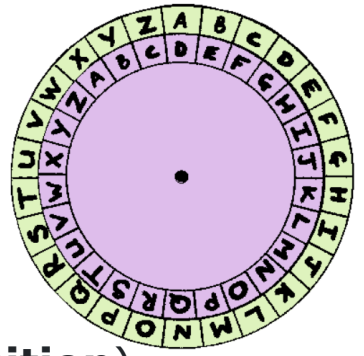
Cryptographie Classique : Le Scytale



- Les anciens Grecs, utilisaient ce chiffre pour communiquer, avec un cylindre appelé scytale pour l'expéditeur et le destinataire du même rayon.
- L'expéditeur enroulait une bande autour de son cylindre et écrivait le long de celle-ci. Une fois la bande déroulée, le message n'était lisible que par quelqu'un possédant un cylindre de même circonférence.



Cryptographie Classique : Le code de César



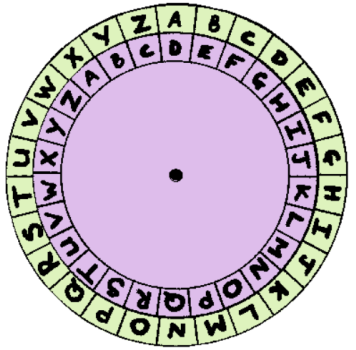
- Le chiffre de César est un exemple de ce qu'on appelle un chiffre de décalage (**Transposition**)
- Pour encoder un message, les lettres sont remplacées par une lettre située à un certain nombre de positions au-delà de la lettre actuelle
- L'alphabet chiffré est l'alphabet ordinaire, mais tourné vers la gauche ou la droite d'un certain nombre de positions.
- Un chiffre de César utilisant une rotation vers la gauche de trois positions
  (le paramètre de décalage, ici 3, est utilisé comme clé)

Num	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Texte 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

CRYPTOGRAPHIE

FUBSWRJUDSKLH

Cryptographie Classique : Le code de César



- Les fonctions de cryptage et de décryptage du chiffre de César sont les suivantes :
- **C=(M+K)mod26**
- **M=(C−K)mod26**
- où C = texte chiffré, M = texte en clair et K = clé.
- Exemple: Chiffrez «CRYPTOGRAPHIE » en utilisant le chiffre de César avec un décalage de 4.

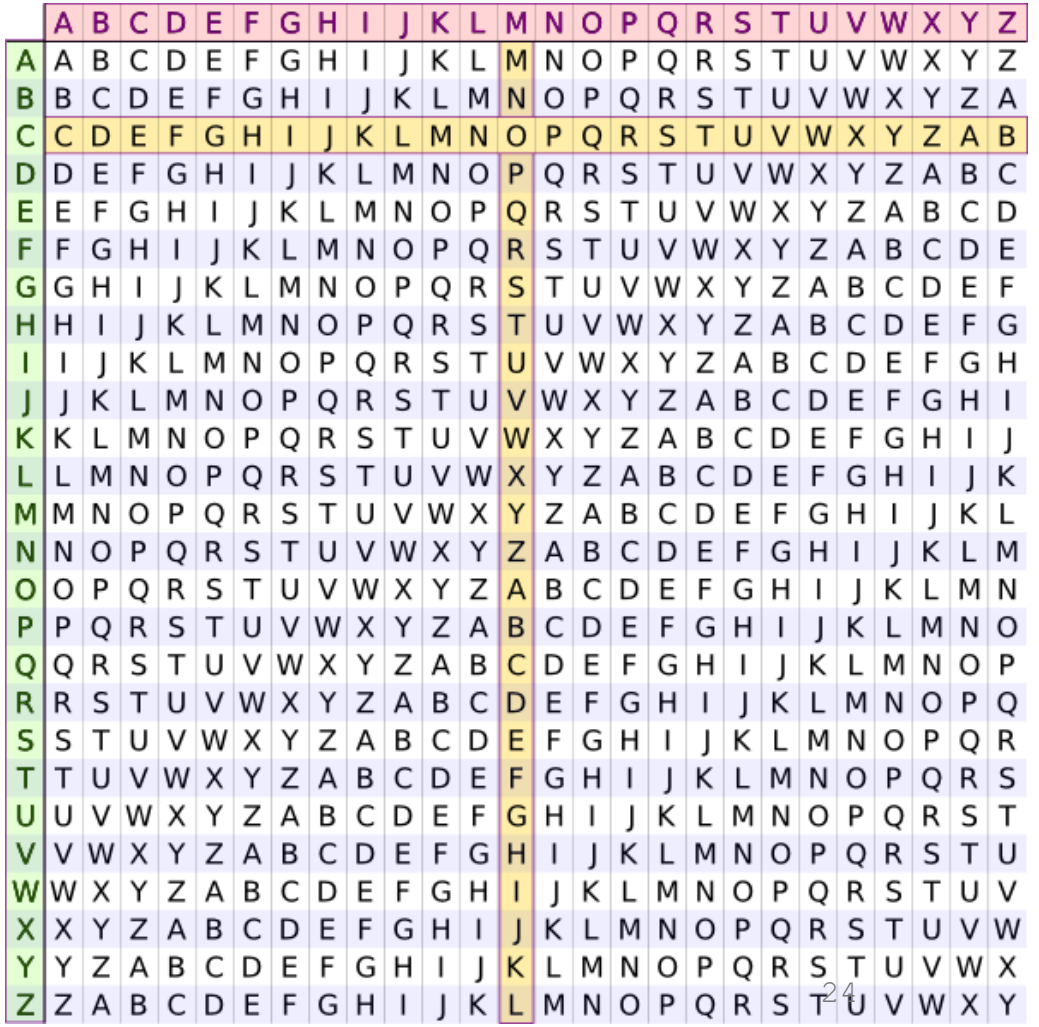
Num	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Texte clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

CRYPTOGRAPHIE

?

Cryptographie Classique : Le code de Vigenère

- Le chiffre de Vigenère utilise une table de 26×26 avec A à Z comme en-têtes de ligne et de colonne. Cette table est généralement appelée le tableau de Vigenère.
- La première ligne de cette table contient les 26 lettres de l'alphabet anglais. À partir de la deuxième ligne, chaque ligne contient les lettres décalées d'une position vers la gauche de manière cyclique.
- Le chiffrement de Vigenère nécessite également un mot-clé, qui est répété afin que la longueur totale soit égale à celle du texte 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
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

Cryptographie Classique : Le code de Vigenère

Exemple : Nous souhaitons chiffrer le texte CRYPTOGRAPHIE en utilisant la clé: SITCN.

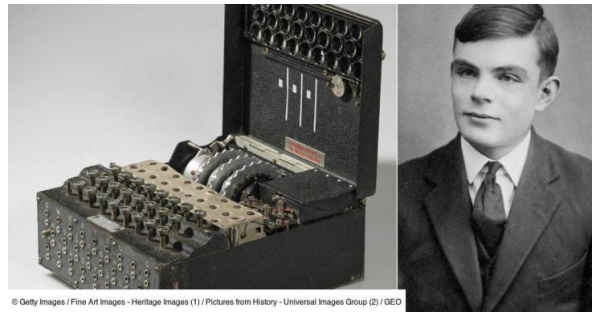
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Texte clair	C	R	Y	P	T	O	G	R	A	P	H	I	E
Texte codé	S	I	T	C	N	S	I	T	C	N	S	I	T

CRYPTOGRAPHIE

UZRRGGOKCCZQX

Cryptographie Classique : La machine Enigma



- La machine Enigma a été créée en 1918 par l'inventeur allemand Arthur Scherbius.
- Utilisée par l'armée allemande pendant la Seconde Guerre mondiale, elle est une machine mécanique capable de chiffrer et de déchiffrer des messages en combinant des méthodes de substitution et de transposition.
- Le code employé par la machine Enigma a été déchiffré pendant la Seconde Guerre mondiale.

Cryptographie Classique : Autres systèmes classiques

- Les homophones
- Chiffre Affine (polynômes)
- Chiffre de Playfair (chiffrement polygraphique)
- Chiffre de Hill (Matrices)
- Chiffre de Veranm (Masque jetable)
- …