

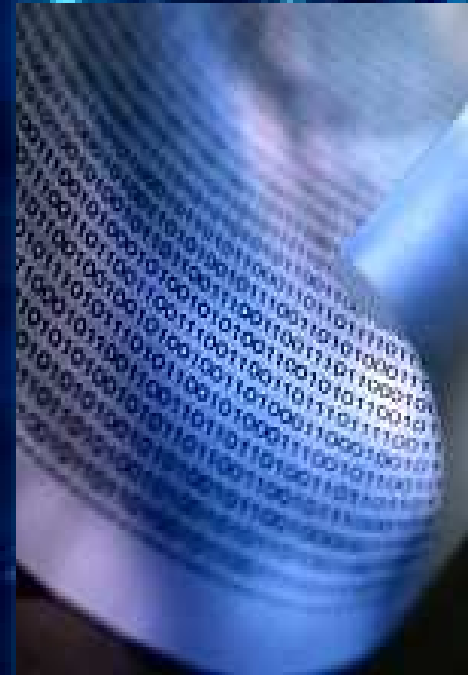
# Cryptographie :

## Problématique :

*Comment transmettre des informations d'une manière sécurisée ?*

## Présentation :

- 1) Introduction
- 2) Évolution de la cryptographie
- 3) Le système RSA



# 1) Introduction :

- La cryptographie est la science du chiffrement. Elle est utilisée depuis l'antiquité dans le but d'échanger des informations de façon sécurisée. C'est une branche de la cryptologie.

- La cryptologie est à la fois un art ancien et une science nouvelle.

Elle regroupe divers domaines :

- La **cryptographie**
- La **cryptanalyse**
- La **stéganographie** .



# ● ● ● Cryptologie :



❖ La cryptologie est la science qui étudie les aspects scientifiques des méthodes de chiffrement et de déchiffrement d'informations.

Elle englobe donc la cryptographie et la cryptanalyse.



❖ La cryptographie est l'art de chiffrer un message dans le but de le rendre indéchiffrable.

❖ La cryptanalyse est l'art de déchiffrer un message dans le but de le rendre compréhensible.



❖ La stéganographie est l'art de dissimuler un message par l'intermédiaire d'un autre.





# Stéganographie :

❖ Voici quelques exemples de procédés sténographiques utilisés dans notre passé :

❖ **Le crâne rasé :**

A l'antiquité, les Grecs utilisaient parfois la tête des esclaves pour tatouer des messages. Ils étaient ensuite envoyés chez le destinataire et après un long voyage, il fallait raser leur tête dont les cheveux avaient repoussés, pour lire le message.

❖ **L'encre invisible :**

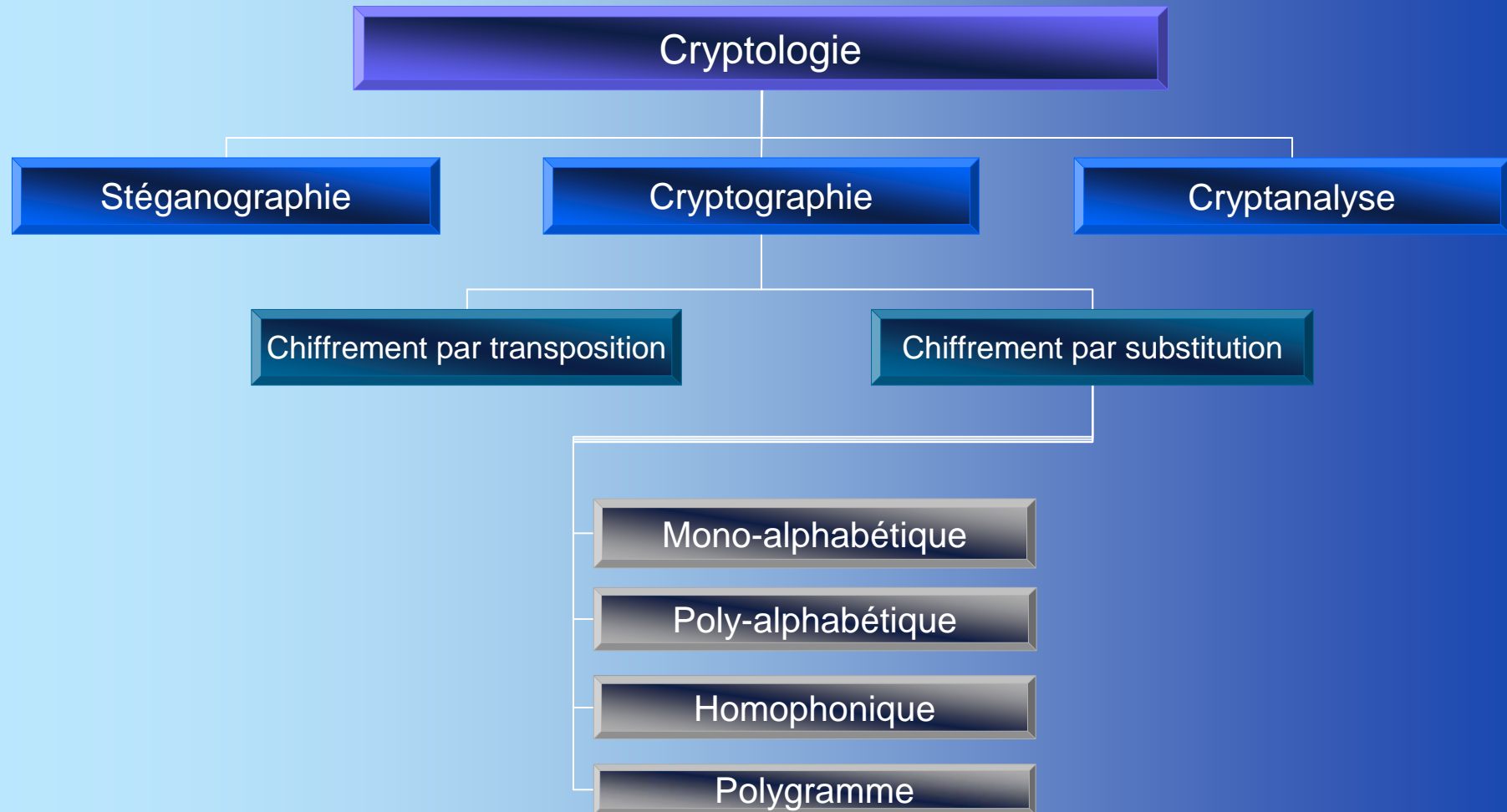
Au 1er siècle av. J.C, apparut une méthode de dissimulation de message consistant à écrire avec du lait ou du jus de citron. Il suffisait de chauffer le support pour faire réapparaître le message.

❖ **Le micro point :**

Pendant la seconde guerre mondiale, les Allemands utilisaient la technique du micro-point, consistant à dissimuler des photos ou des textes dans un point de ponctuation d'une lettre. Il suffisait alors d'agrandir le point pour voir apparaître le message.

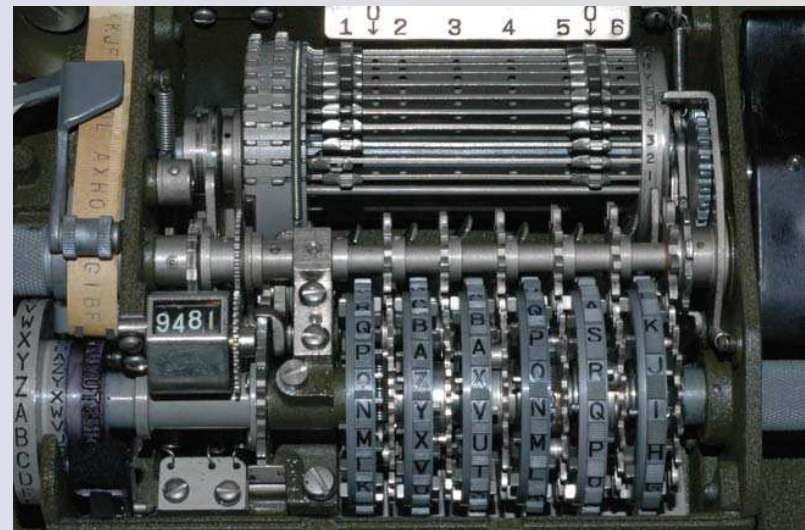


# Organigramme :



## 2) Evolution de la cryptographie :

- Depuis l'antiquité, la cryptographie n'a cessé d'évoluer, laissant place à des méthodes de cryptages toujours de plus en plus complexes et fiables.
- Cette évolution a donné lieu à de nombreux systèmes de chiffrements :
  - Chiffrement par **transposition**,
  - Chiffrement par **substitution** :
    - mono-alphabétique
    - poly-alphabétique
    - homophonique
    - polygramme



# Méthode assyrienne :



## Scytale :

- La scytale est un support cylindrique souvent en bois et utilisé pour crypter des messages.
- La clé de cryptage est dans ce cas le diamètre de la scytale.

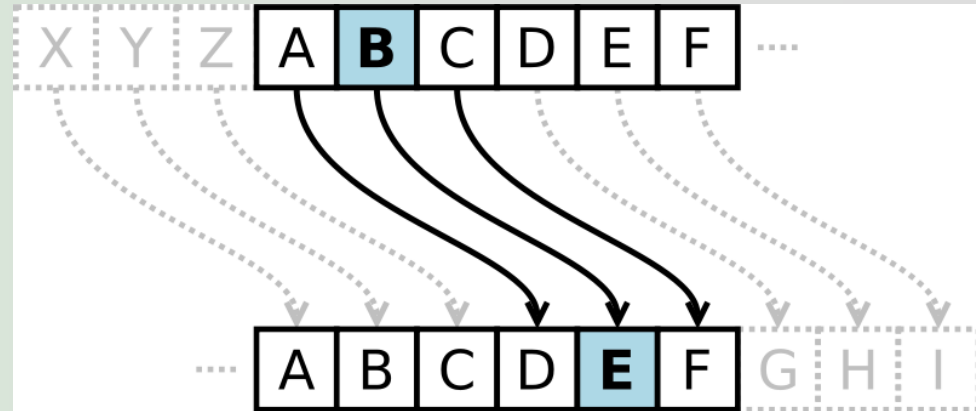
❖ La méthode assyrienne est un système de **chiffrement par transposition** utilisant une scytale.

❖ Ce procédé était utilisé dans les environs de 600 avant J.C et son fonctionnement consistait à enrouler une bande de papyrus autour de la scytale, et d'écrire un message à sa surface de façon à rendre le message illisible une fois déroulé.

# Méthode de César :

❖ La méthode de César est un système de **chiffrement par substitution mono-alphabétique**.

❖ Ce procédé était utilisé dans les environs de 200 avant J.C et son fonctionnement consistait à décaler chaque lettre de l'alphabet par une autre de façon à rendre le message illisible.



## Exemple :

- Si l'on choisit un décalage de 3 rangs dans l'alphabet, le message « **Bonjour** » devient « **Erqmrxu** » .
- Ici, la clé de cryptage est le nombre de décalage dans l'alphabet.

# Méthode 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
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 méthode de Vigenère est un système de **chiffrement par substitution poly-alphabétique** utilisé au 16ème siècle.

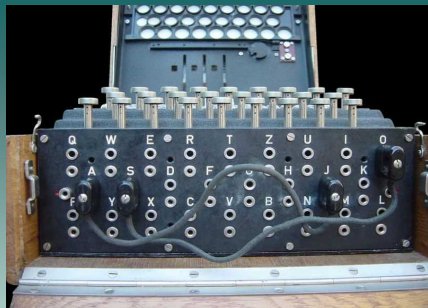
❖ Ce système plus complexe que le chiffre de César, a résisté sur presque deux siècles aux décrypteurs. Afin de trouver le tableau de Vigenère, il faut décaler l'alphabet d'une case à chaque ligne vers la droite.

❖ La première ligne correspond aux lettres du texte en clair à crypter et la 1ere colonne correspond à la clé utilisée.

# Machines de cryptage :

Pendant le début du 20ème siècle, notamment pendant les guerres, des machines électromécaniques portables étaient utilisées dans le but de protéger des informations d'importance capitales. Leur fonctionnement était dû à des rotors montés sur cylindres, servant à chiffrer des informations. L'utilisation de la même machine (et des mêmes réglages) permettait de déchiffrer le message.

Voici quelques unes de ces machines :



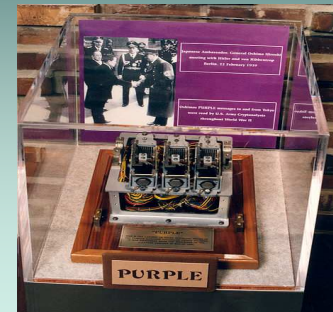
**Enigma**

**Sigaba**



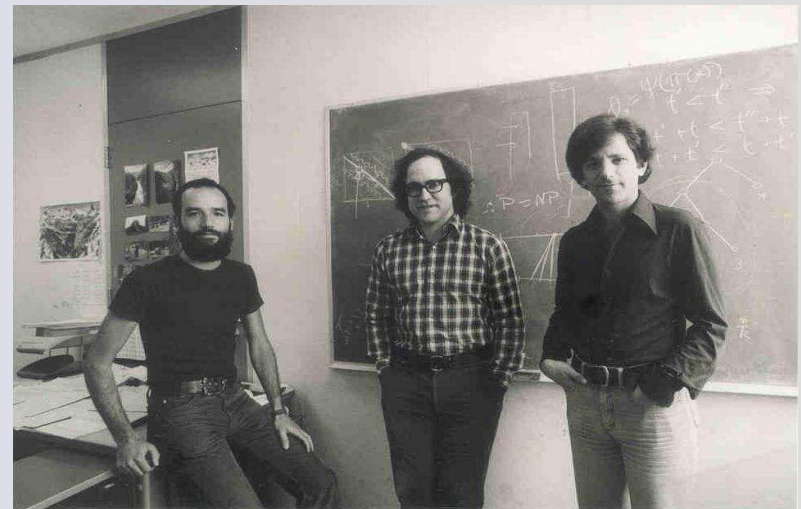
**Typex**

**Purple**



### 3) Le système RSA :

- La méthode **RSA** est un algorithme de chiffrement à clé publique inventé en 1977 par les 3 informaticiens ci-contre.
- Ce système est aujourd'hui utilisé dans de nombreuses situations de la vie courante :
  - Transactions bancaires
  - Achats sur internet
  - Echanges d'informations confidentielles (services secrets).
- Sa grande fiabilité réside dans la difficulté de décomposer de grands nombres en produit de facteurs premiers



**Rivest**   **Shamir**   **Adleman**

# 1. Confection des clés :

- Choix de 2 nombres premiers **p** et **q**
- $n = p \times q$
- Choix de **e** premier avec  $(p - 1)(q - 1)$
- Détermination d'un entier **d** tel que :  
$$ed \equiv 1 \pmod{(p - 1)(q - 1)}$$
$$ed = k (p - 1)(q - 1) + 1$$
avec k entier et  $1 \leq d < (p - 1)(q - 1)$

## ❖ Clé :

Série de symboles utilisée pour le chiffrement et le déchiffrement de messages.

## ❖ Clé publique :

$(n ; e)$

## ❖ Clé privée :

$(p ; q ; d)$

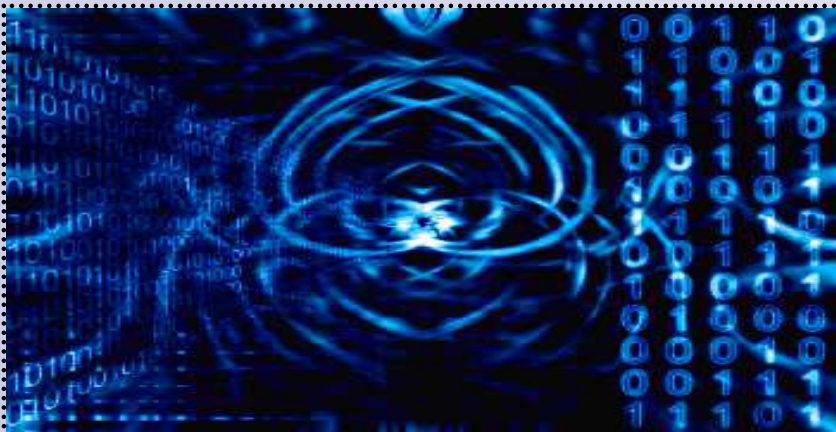
## 2. Préparation du message :

### ❖ A) Numérisation :

- **M** message original (alpha numérique)
- **M'** message numérisé (utilisation du code ASCII)

### ❖ B) Découpage :

- Découpage du message **M'** en tranches **t**
- La longueur des tranches **t** est déterminée par le nombre de chiffres de **n**



### Code ASCII :

Ce code est une norme anglaise de transcription de données informatiques permettant le passage d'une écriture littérale en écriture numérique.

# 3. Échange du message

## ❖ A) Cryptage

- L'émetteur crypte le message pour l'envoyer au destinataire.
- $t^e \equiv t' \pmod{n}$
- $t$  tranche du message original.
- $t'$  tranche du message crypté.

## ❖ B) Décryptage

- Le destinataire reçoit le message crypté et le déchiffre.
- $t'^d \equiv t \pmod{n}$
- $t'$  tranche du message crypté.
- $t$  tranche du message décrypté.

# Cryptographie :

## Conclusion :

*Il existe donc de nombreux procédés et méthodes permettant de transmettre des informations de manière sécurisée.*

*À partir du moment où aucun moyen de factorisation rapide ne verra le jour, alors le système RSA restera probablement le système de cryptage-décryptage le plus fiable et le plus sécurisé au monde.*

*Enfin, comme tout domaine scientifique, la cryptographie aura grandement évolué au cours du temps, et continuera encore de le faire dans notre avenir. Ce sujet est donc essentiel pour le développement de l'informatique et de la communication à l'échelle planétaire.*

*Pour plus d'informations à ce sujet, il est possible de consulter le site de référence de ce TPE : <http://www.cryptotpe.fr>*

