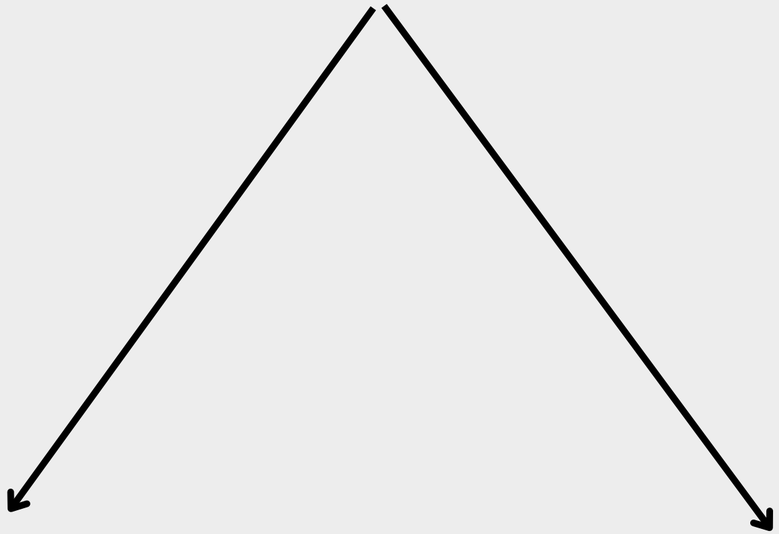
La Cryptographie

Alan Arens ™

Dépôt légal
2022

Crypologie (Science du secret)



Crypographie

- Pratique de l'écriture secrète

Cryptanalyse

- Analyse de l'écriture secrète

Histoire

- La Scytale
- Chiffre de César
- Léon Battista Alberti (XV ème siècle)
  - considéré comme le père de la cryptographie moderne
- Chiffre de Vigenère (XVI ème siècle)
  - introduit la notion de clé
- Chiffre de Vernam (XX ème siècle)

La scytale

ou bâton de Plutarque (Xème siècle avant notre ère)

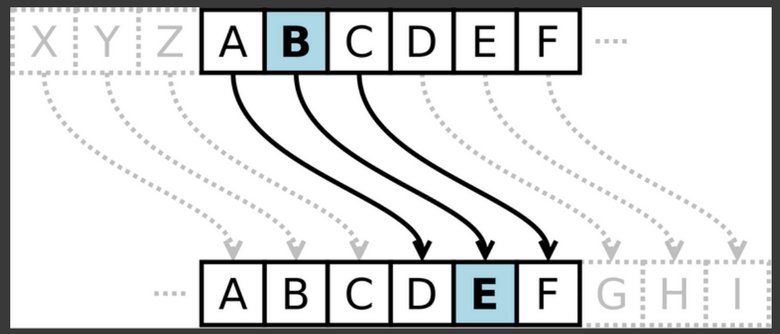
- Plus vieille méthode de chiffrement recensée
- Utilisée par les spartiates

Message chiffré :
MSETSEUEARR_SISG_EMQN

M S E T S E U
E A R R _ S I
S G _ E M Q N

On peut lire colonne par colonne :
"MESSAGER_TRES_MESQUIN".

Chiffre de César



- Utilisé par Jules César lui-même
- Le message est décalé à distance fixe

clair : ABCDEFGHIJKLMNOPQRSTUVWXYZ
chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC

original : WIKIPEDIA L'ENCYCLOPEDIE LIBRE
encodé : ZLNLSHGLD O'HQFBFORSHGLH OLEUH

Existe une variante du Code de César appellé le ROT-13 (décalage de 13)

Chiffre de Vigenère

- Résiste à l'analyse de fréquence
- Introduit la clef en cryptographie
- Déchiffrage à l'aide d'une Table de Vigenère

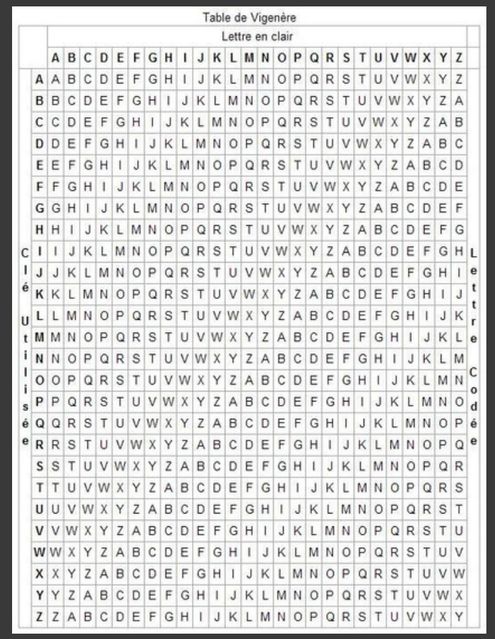


Table de Vigenère

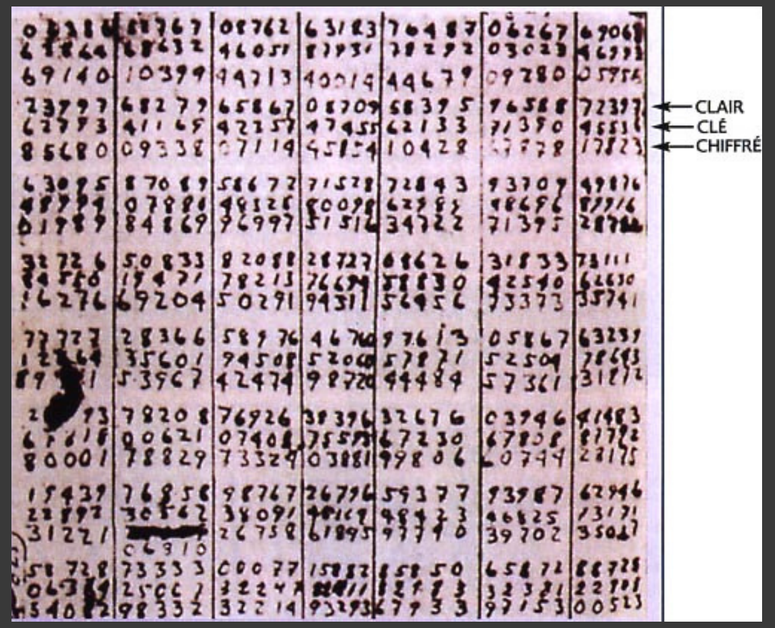
Clé Utilisée \ Lettre en clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E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

Le bon Blaise de Vigenère lui-même.

Chiffre de Vernam (ou Masque jetable)

- La clé doit être :
  - au moins aussi longue que le message
  - les caractères de la clé doivent être aléatoire
  - chaque clé ne doit être utilisée qu'une seule fois (masque jetable)

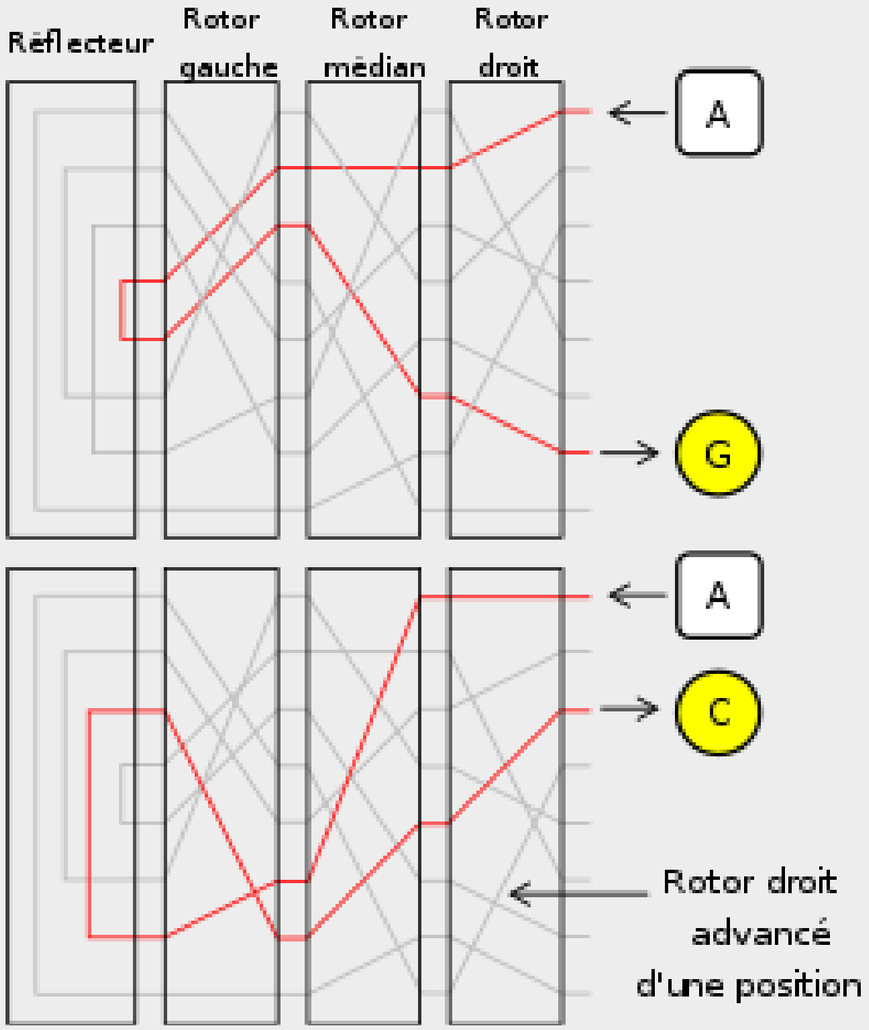
- Théoriquement impossible à casser

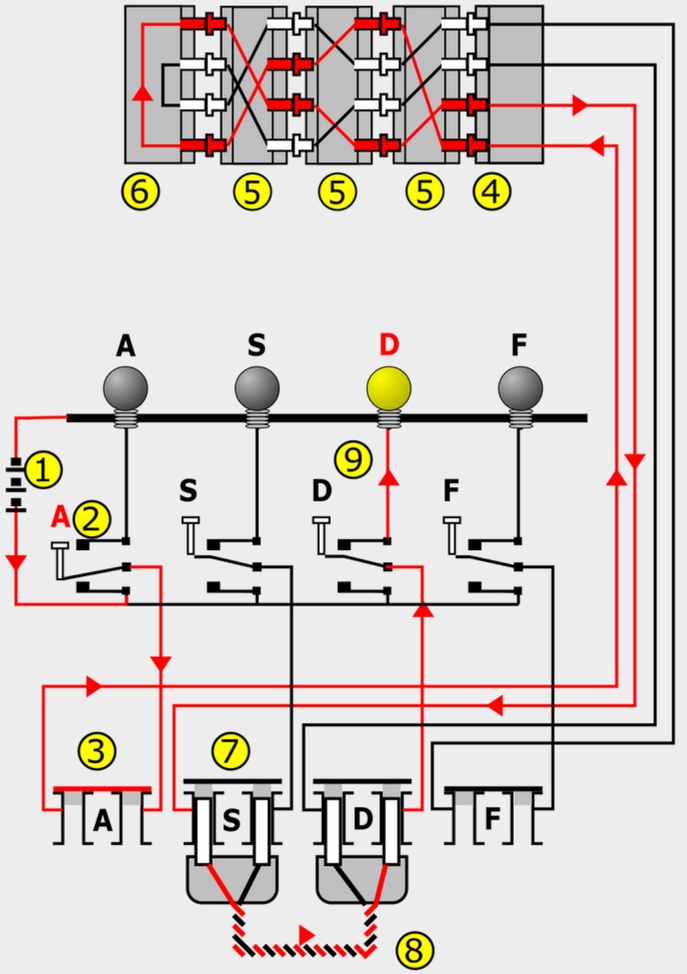


Enigma

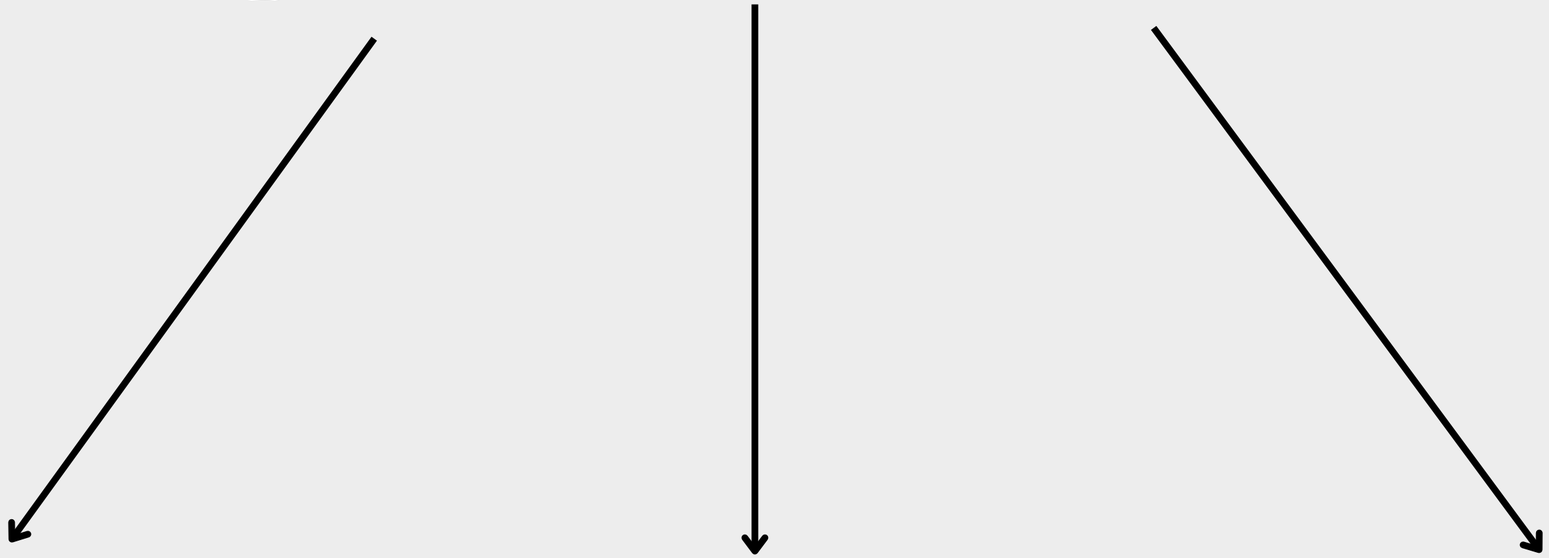
- Utilisée par les allemands durant la WW2
- Chiffre en faisant passer un courant électrique à travers ses composants
- Machine électromécanique

Enigma : Mécanisme





Algorithmes de chiffrement



Symétrique

La clé de chiffrement est la même pour chiffer et déchiffrer

ex : DES, masque jetable

Hybride

ex: PGP, GnuPG, TLS

Asymétrique

La clé est différente pour chiffrer et déchiffrer

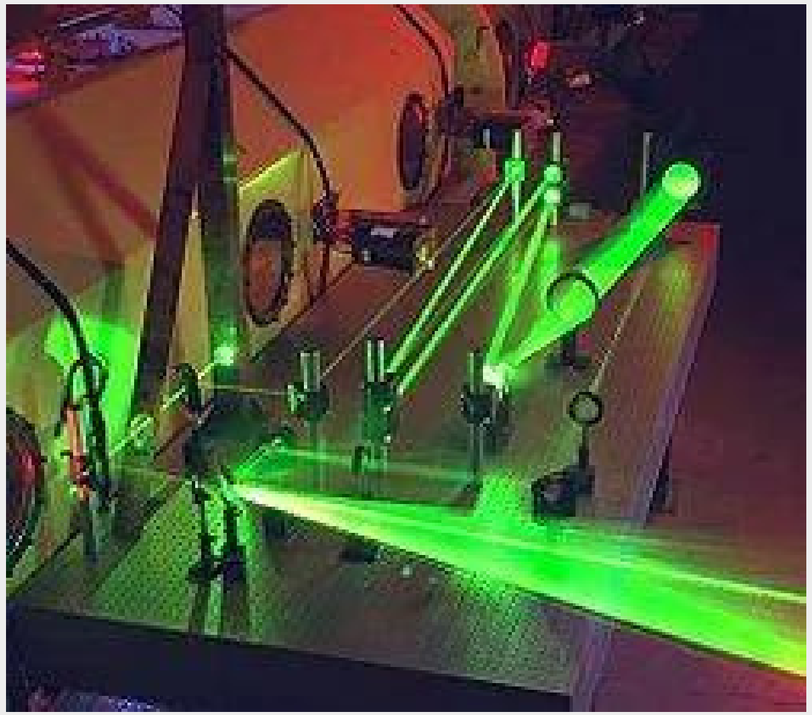
ex : RSA

Applications

- La Blockchain
- Médecine : données de patients
- Cartes bancaires
- Navigateurs

Cryptographie quantique

- Sert à transmettre la clé et non le message lui-même.
- Via la fibre optique
- La mesure des objets quantique modifie leur état, ce qui permet de détecter une interception



Définitions

Chiffrement = transformer un message clair en message incompréhensible via une clé

décrypter = retrouver le message originel sans disposer de la clé

cryptogramme = le message chiffré

cryptolecte = jargon que peuvent utiliser les personnes ayant la clé de chiffrement pour communiquer entre eux

cryptosystème = l'algorythme de chiffrement

stéganographie ≠ cryptographie
= faire passer un message inaperçu dans un autre message

Mercè