

# La Cryptographie

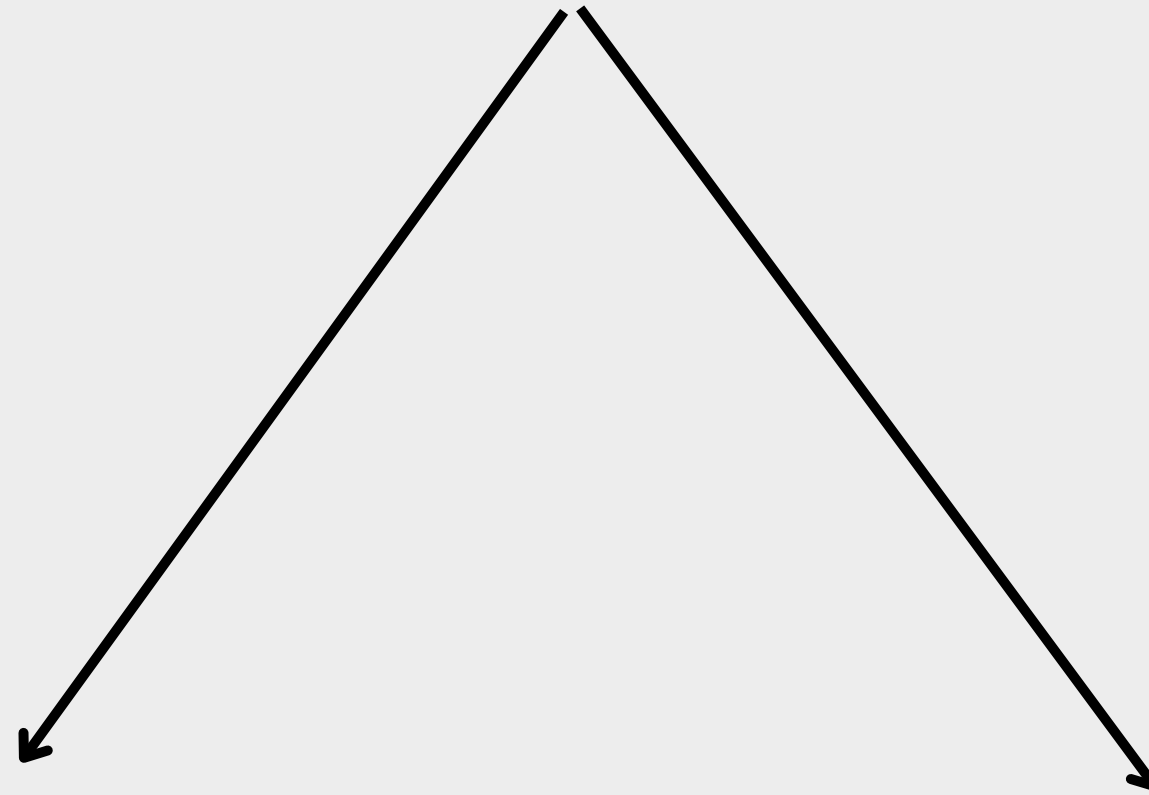
Alan Arens<sup>TM</sup>



Dépôt légal  
2022

Tous droits réservés<sup>©</sup>

# Cryppologieie ( Science du secret )



Cryptographie

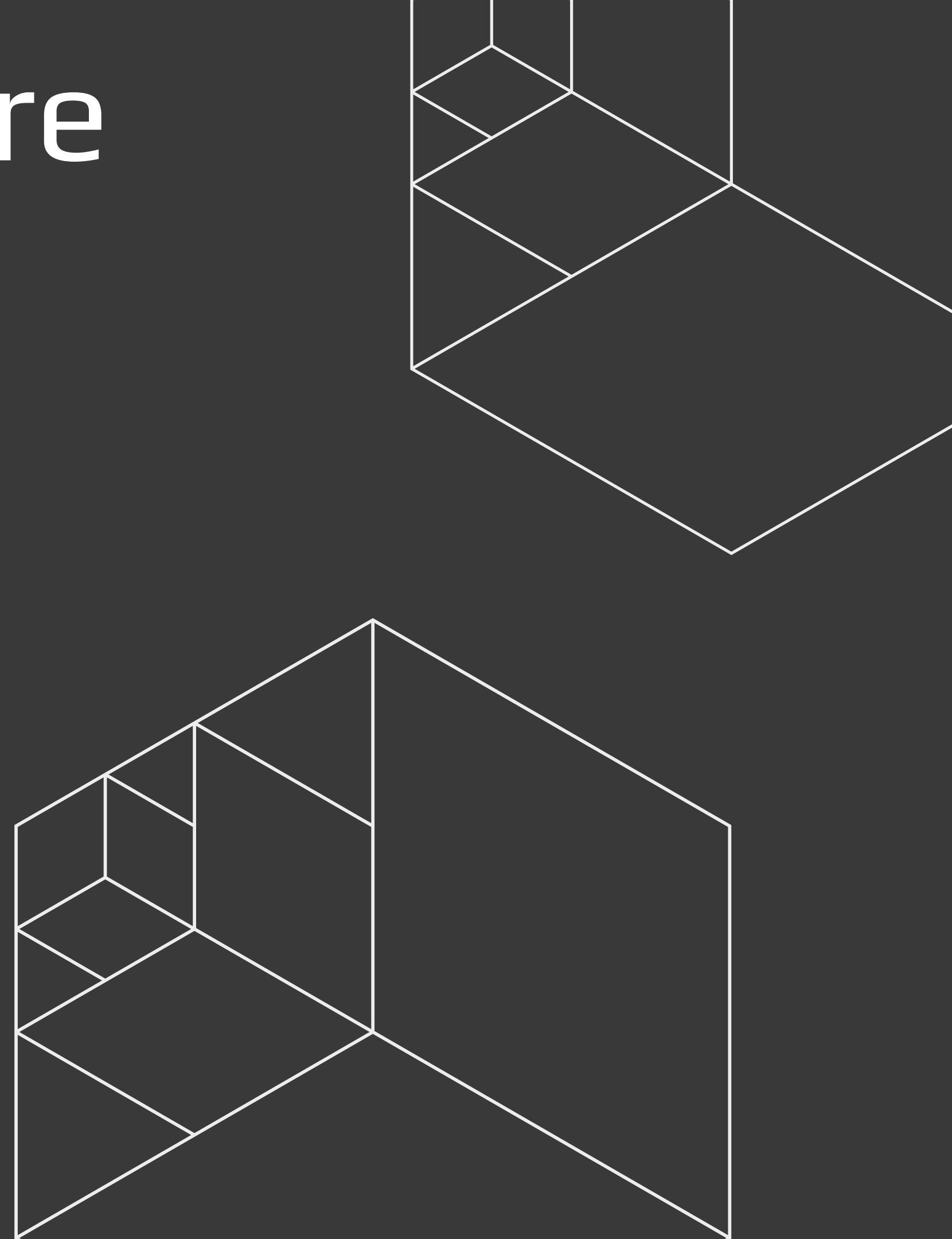
- Pratique de l'écriture secrète

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



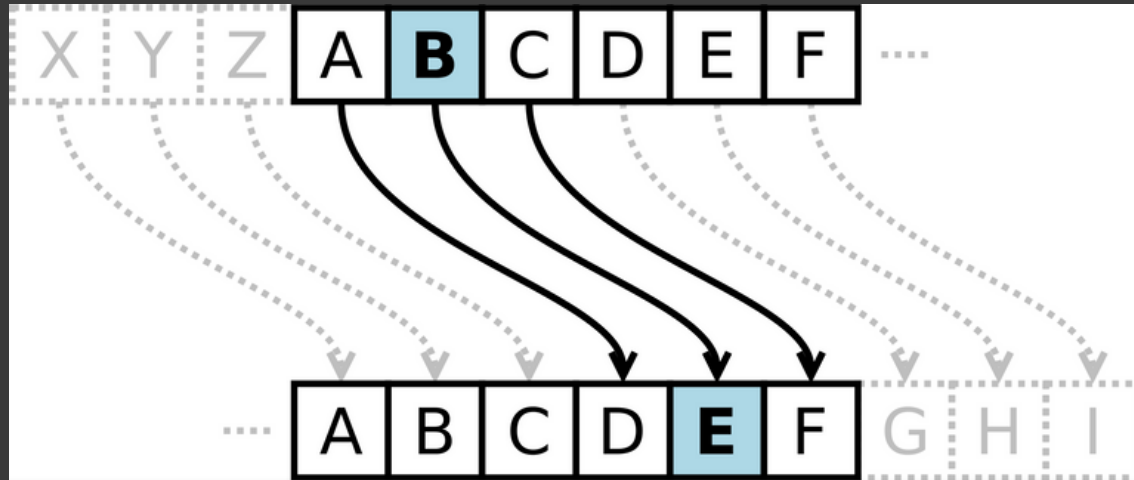
Message chiffré :  
MSETSEUEARR\_SISG\_EMQN



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 :  
"MESSENGER\_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 appelé 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	
	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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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

0 8 3 1 4 6 8 7 6 7	0 8 7 6 2	6 3 1 8 3	7 6 4 8 7	0 6 2 6 7	6 9 0 6 8
2 1 2 6 4 6 8 4 3 2	4 6 0 5 1	8 7 9 3 1	7 8 2 9 2	0 3 0 2 3	4 6 9 9 3
6 9 1 4 0	1 0 3 9 9	4 4 7 1 3	4 0 0 1 4	4 4 6 7 9	0 9 2 8 0
2 3 7 9 7	6 8 2 7 9	6 5 8 6 7	0 8 7 0 9	5 8 3 9 5	7 6 5 8 8
6 2 7 7 3	4 1 1 6 9	4 2 3 5 7	4 7 4 5 1	6 2 1 3 3	7 1 3 9 0
8 5 6 8 0	0 9 3 3 8	0 7 1 1 4	4 5 1 5 4	1 0 4 2 8	5 7 8 7 8
4 3 0 9 5	8 7 0 8 9	5 8 6 7 2	7 1 5 7 8	7 2 8 4 3	9 3 7 0 7
4 8 7 9 4	0 7 8 8 8	4 8 1 2 8	8 0 0 9 8	6 2 9 8 5	4 8 6 9 6
0 1 9 8 9	8 4 8 6 9	9 6 9 9 7	5 1 5 1 6	3 4 7 2 2	7 1 3 9 5
3 2 7 2 6	5 0 8 3 3	8 2 0 8 8	2 8 7 2 7	6 8 6 2 6	3 1 8 3 3
8 4 7 5 0	1 9 4 7 1	7 8 2 1 3	7 6 6 9 9	5 8 8 3 0	4 2 5 4 0
1 6 2 7 6	6 9 2 0 4	5 0 2 9 1	9 4 3 1 1	5 6 4 5 6	7 3 3 7 3
7 7 7 7 7	2 8 3 6 6	5 8 9 7 6	4 6 7 6 0	9 7 6 1 3	0 5 8 6 7
1 2 8 6 4	3 5 6 0 1	9 4 5 0 8	5 2 0 6 8	5 7 8 7 1	5 2 5 0 4
8 9 7 8 1	5 3 9 6 7	4 2 4 7 4	9 8 7 2 0	4 4 4 8 4	5 7 3 6 1
2 7 7 3	7 8 2 0 8	7 6 9 2 6	3 8 3 9 6	3 2 6 7 6	0 3 9 4 6
6 7 6 1 8	0 0 6 2 1	0 7 4 0 8	7 5 5 9 3	6 7 2 3 0	6 7 8 0 8
8 0 0 0 1	7 8 8 2 9	7 3 3 2 4	0 3 8 8 1	9 9 8 0 6	6 0 7 4 4
1 5 4 3 9	7 6 8 5 8	9 8 7 6 7	2 6 7 9 6	5 9 3 7 7	9 3 9 8 7
2 3 8 9 2	3 0 5 6 2	3 8 0 9 1	4 8 1 6 9	4 8 4 2 3	4 6 8 2 5
3 1 2 2 1	0 6 9 1 0	2 6 7 5 8	6 1 8 9 5	9 7 7 4 0	3 9 7 0 2
5 8 7 2 8	7 3 3 3 3	0 0 0 7 7	1 5 8 8 2	8 5 8 5 0	6 5 8 7 2
0 6 3 8 4	2 5 0 6 7	3 2 2 4 7	8 8 0 1 1	8 2 8 8 3	3 2 3 8 1
4 5 4 0 8	9 8 3 3 2	3 2 2 1 4	9 3 2 9 3	6 7 9 3 3	9 7 1 5 3

← CLAIR

← CLÉ

← CHIFFRÉ

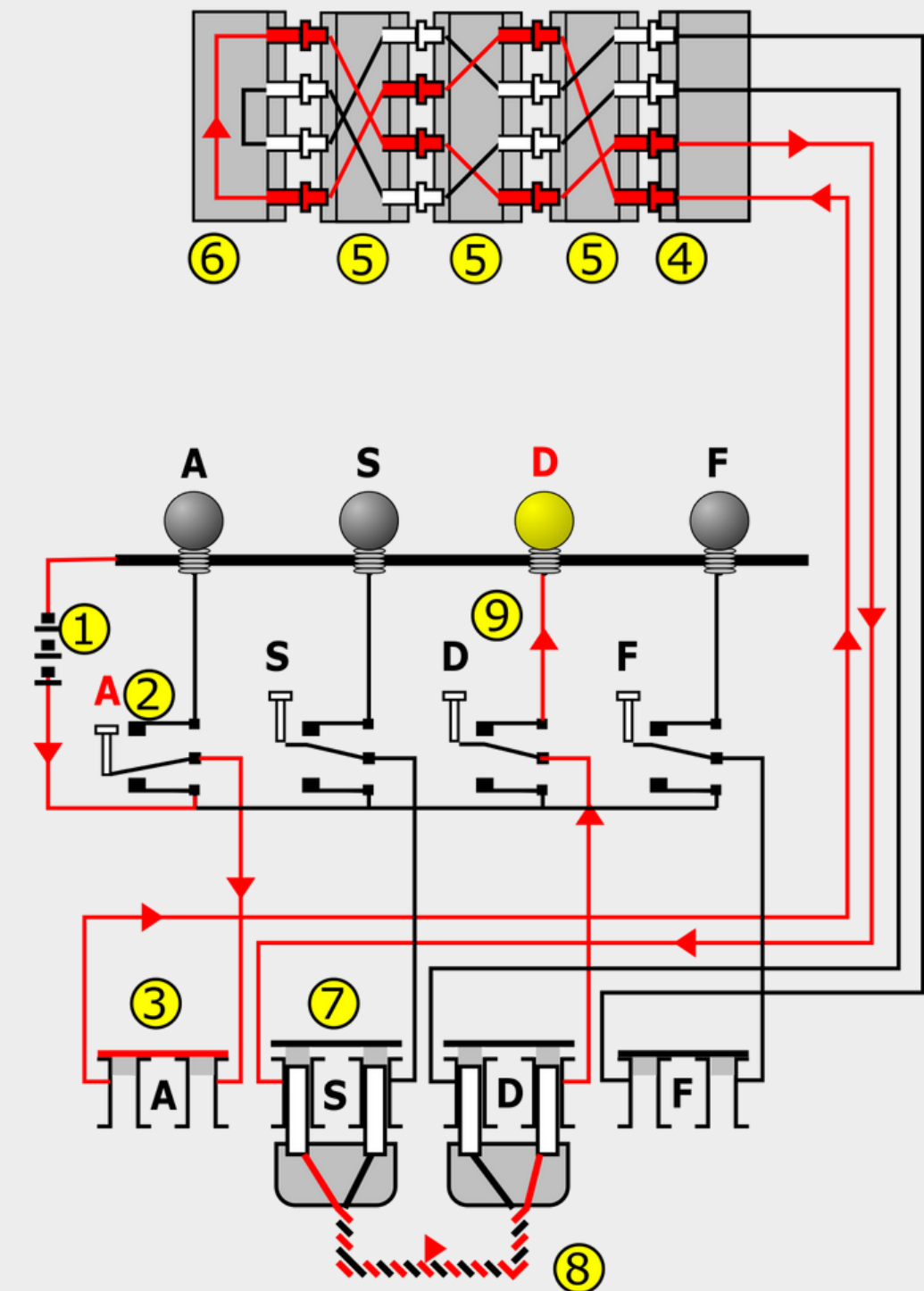
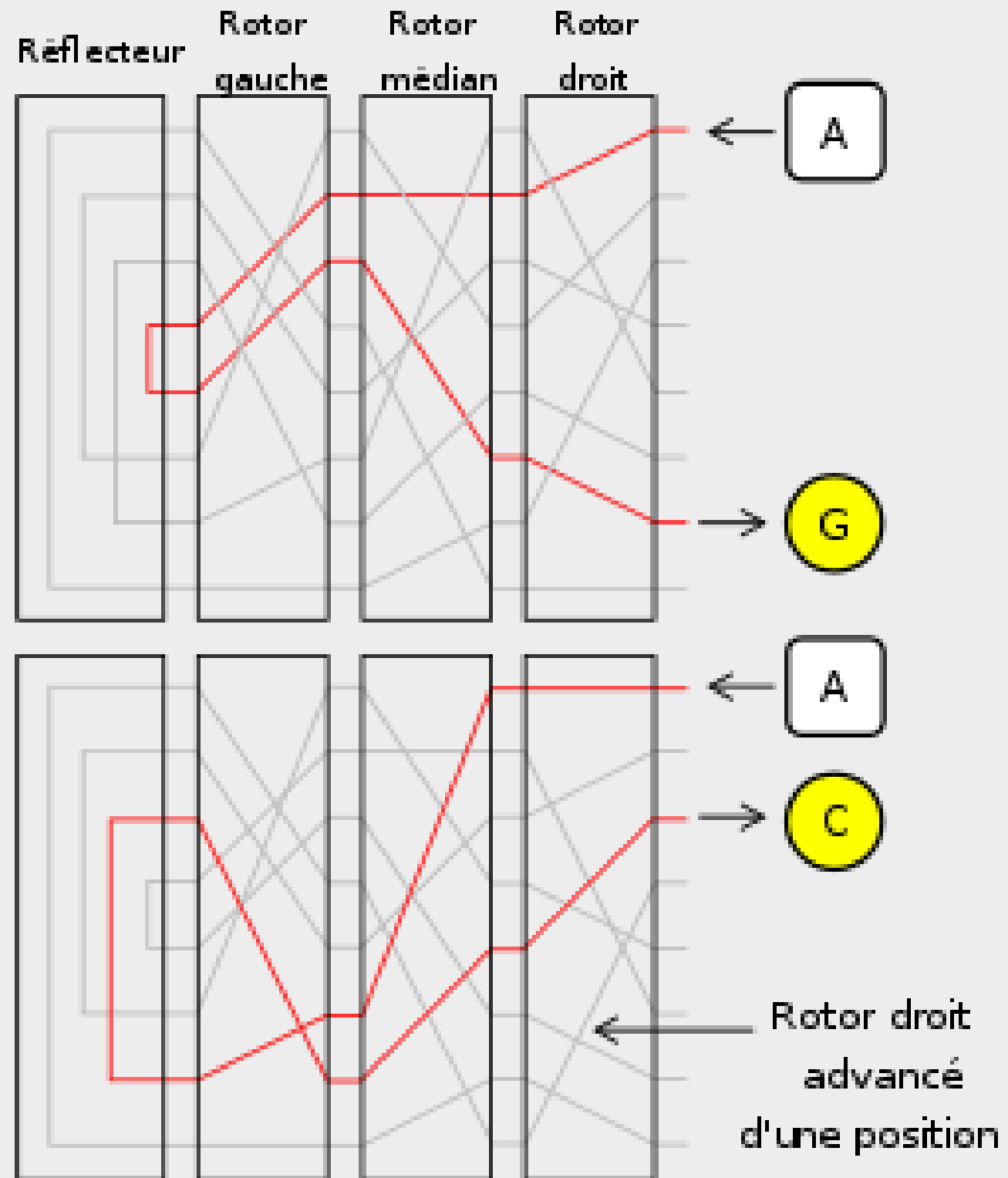
# Enigma

- 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

```
graph TD; A[Algorithmes de chiffrement] --> B[Symétrique]; A --> C[Hybride]; A --> D[Asymétrique];
```

## Symétrique

La clé de chiffrement est la même pour chiffrer 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'algorithme de chiffrement

stéganographie  $\neq$  cryptographie  
= faire passer un message inaperçu dans un autre message



# Mercè

