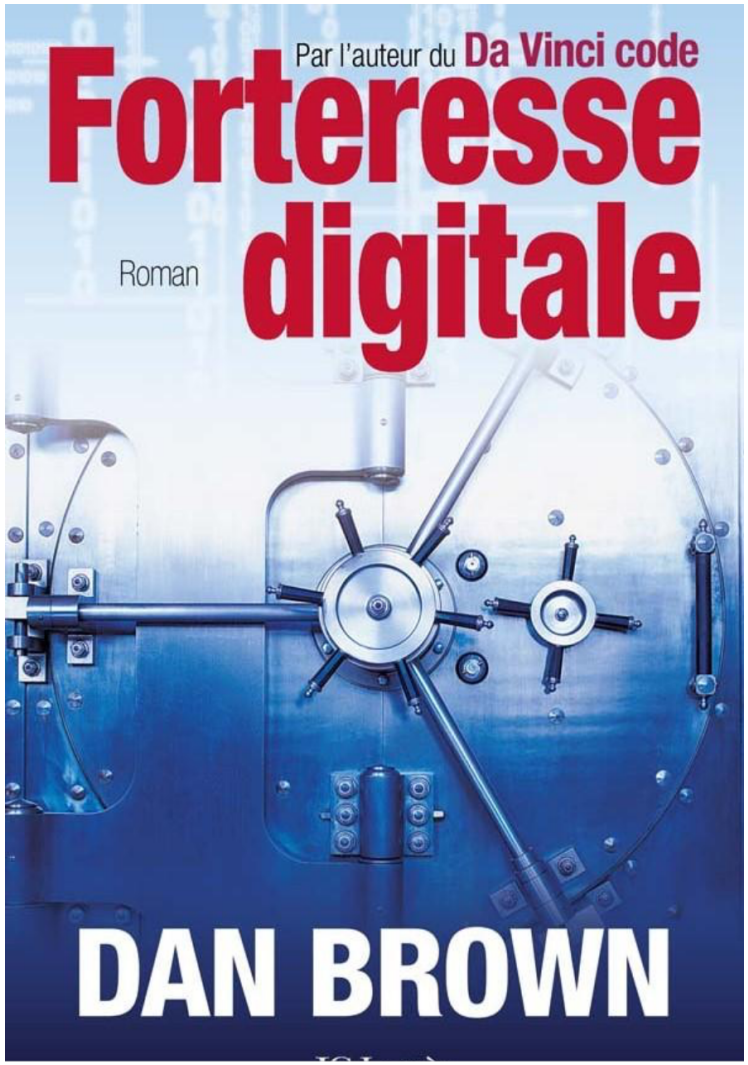
Cryptologie I

Dario Salvadore

28 mars 2023

Forteresse digitale – Dan Brown



Forteresse digitale – Dan Brown

Ce code apparaît à la dernière page.

113-19-5-28-5-53-66-113-76-19-128-10-92-15-19-128

Forteresse digitale – Dan Brown

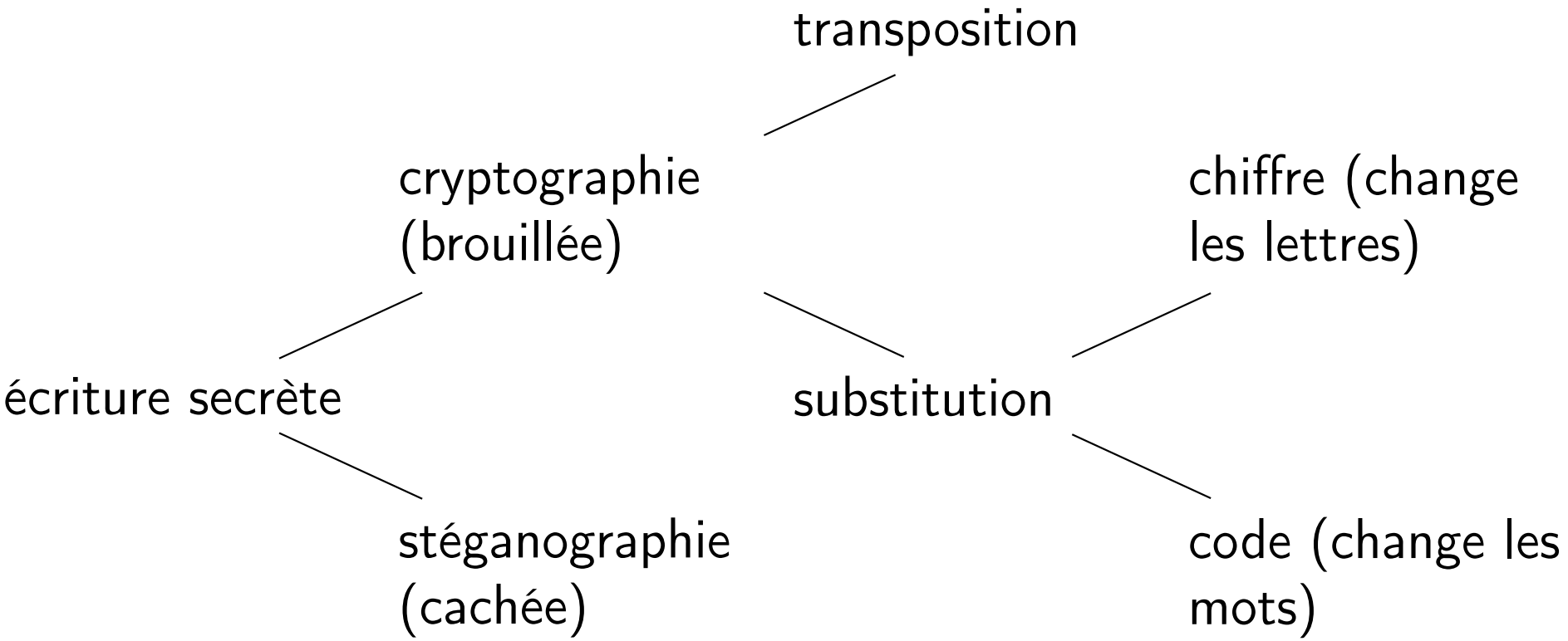
Pour déchiffrer ce code, il faut avoir le roman à portée de main et prendre la première lettre de chacun des chapitres dont les numéros sont indiqués dans cette série. Il y a bien 128 chapitres, et le nombre 128 est là pour aider à trouver la relation.
On obtient alors :

VEOROTBVUESESSES

Préserver le secret d'un message

- La stéganographie
- Le chiffrement

Différentes formes d'écriture secrète



Procédé stéganographique

La stéganographie est l'art de la dissimulation. Elle consiste à cacher un message au sein d'un autre message anodin, de sorte à ignorer l'existence même du secret.

Histiée incite son gendre Aristagoras, gouverneur de Milet, à se révolter contre son roi, Darius, et pour ce faire, « il fit raser la tête de son esclave le plus fidèle, lui tatoua son message sur le crâne et attendit que les cheveux eussent repoussé ; quand la chevelure fut redevenue normale, il fit partir l'esclave pour Milet. »

Qu'est-ce que la cryptologie ?

C'est la science des messages secrets.

Elle se décompose en deux disciplines :

1. la cryptographie
2. la cryptanalyse

Qu'est-ce que la cryptographie ?

Le mot *cryptographie* est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique.

Le verbe **crypter** est parfois utilisé mais on lui préfèrera le verbe **chiffrer**.

Qu'est-ce que la cryptanalyse ?

C'est l'ensemble des techniques et méthodes utilisées pour retrouver le texte en clair à partir du texte crypté.

C'est déchiffrer les messages sans connaître la clé.

Principes de la cryptographie

1. Principe de **Kerckhoffs** : la sécurité repose sur le secret de la clé, et non sur le secret de l'algorithme (19ème siècle).
2. Le déchiffrement sans la clé est impossible (à l'échelle humaine).
3. Trouver la clé à partir du clair et du chiffré est impossible (à l'échelle humaine)

Chiffrement et déchiffrement

Le **chiffrement** est le procédé avec lequel on rend la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement.

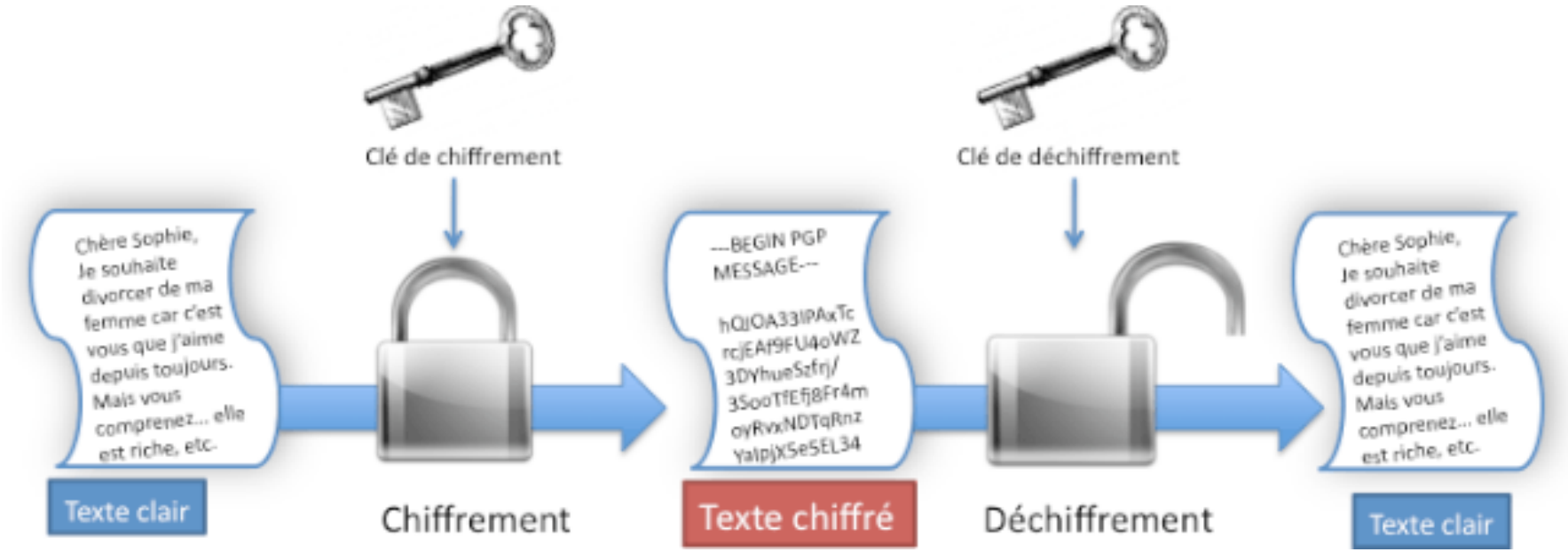
Concrètement, lorsqu'on chiffre un document, on transforme à l'aide de la clé de chiffrement un message en clair en un message incompréhensible (dit texte chiffré) pour celui qui ne dispose pas de la clé de déchiffrement (en anglais encryption).

Chiffrement et déchiffrement

Le **déchiffrement** est logiquement l'opération inverse du **chiffrement**.

C'est donc le processus transformant le texte chiffré en texte clair. Concrètement, cela consiste à retrouver le message original d'un texte chiffré dont on possède la clé de déchiffrement (en anglais decryption).

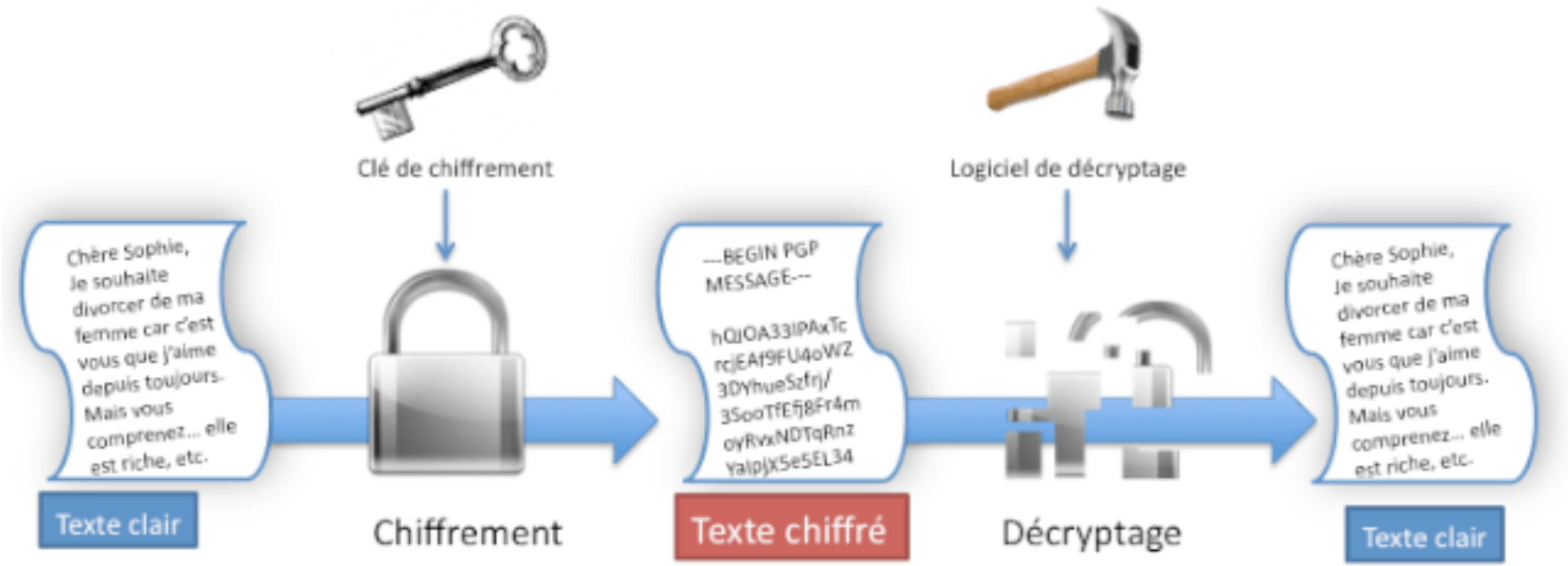
Chiffrement et déchiffrement



Chiffrement et décryptage

Le **décryptage** consiste à retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement !

Chiffrement et décryptage



La scytale

Chiffrement monoalphabétique

Le chiffrement mono-alphabétique consiste à remplacer systématiquement dans le message clair une lettre donnée de l'alphabet par une autre lettre. Deux lettres distinctes doivent être chiffrées en deux signes distincts, sinon il y aurait ambiguïté lors du déchiffrement.

Une même lettre est toujours chiffrée par le même signe.

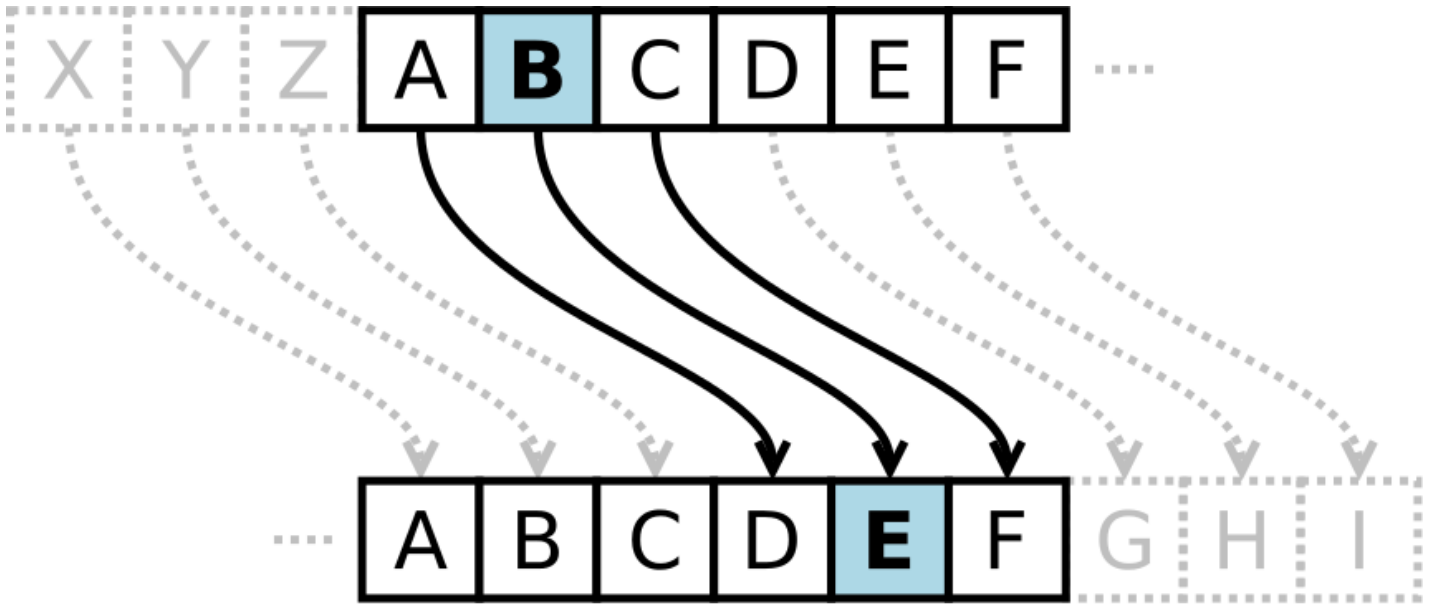
Chiffre de Polybe

	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

Par exemple, le mot bonjour est ainsi chiffré par le carré de Polybe :

$$\textit{bonjour} \rightsquigarrow 12\ 34\ 33\ 24\ 34\ 45\ 42$$

Chiffrement par décalage



Le chiffre de César fonctionne par décalage des lettres de l'alphabet. Par exemple dans l'image ci-dessus, il y a une distance de 3 caractères, donc B devient E dans le texte codé.

Chiffrement polyalphabétique

La substitution polyalphabétique ne fait pas correspondre à une lettre une seule et autre unique lettre, comme la substitution monoalphabétique, mais bien à plusieurs lettres.

Par exemple, un `A` du texte clair peut être aussi bien associé à un `Q` qu'à un `Z` ou un `V`.

$\rightsquigarrow$ La sécurité est ainsi renforcée.

Le chiffre 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

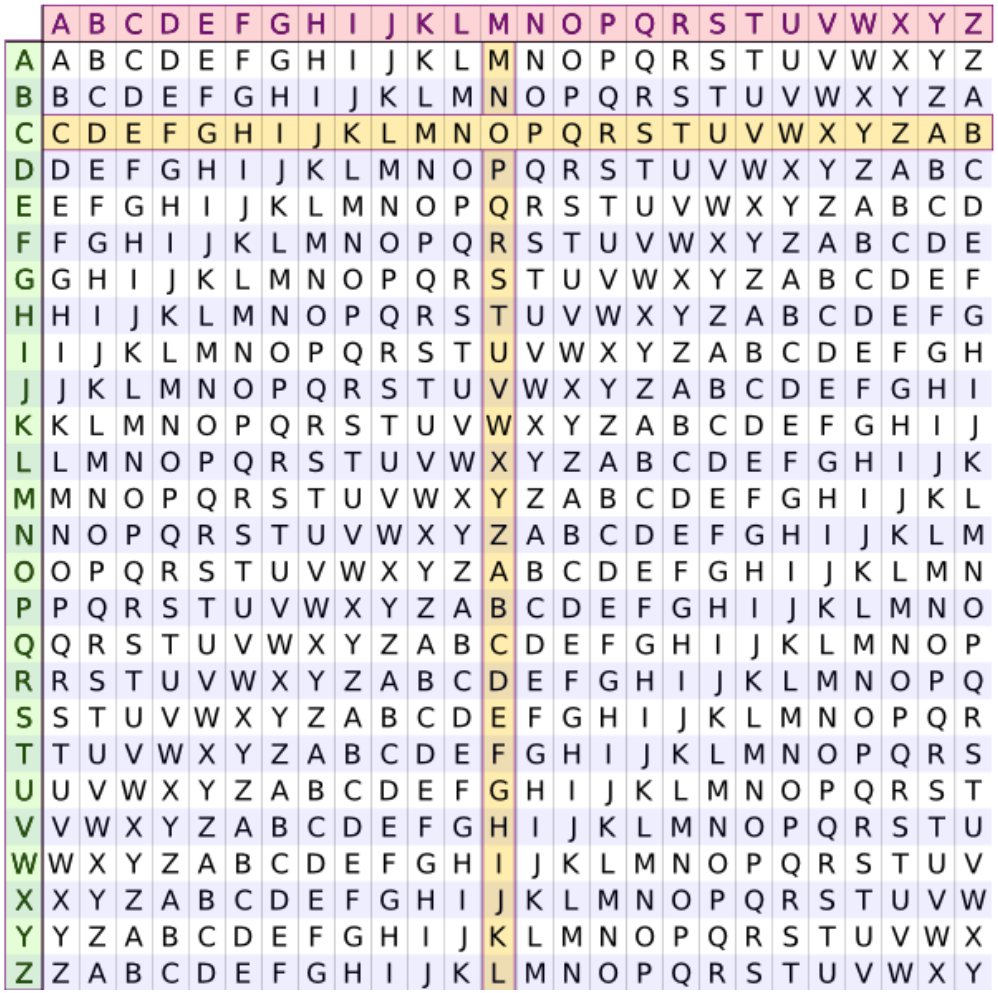
Le chiffre de Vigenère

Coder le texte `CRYPTOGRAPHIE DE VIGENERE` avec la clé `MATHWEB`.
On commence par écrire la clef sous le texte à coder :

C	R	Y	P	T	O	G	R	A	P	H	I	E	D	E	V	I	G	E	N	E	R	E
M	A	T	H	W	E	B	M	A	T	H	W	E	B	M	A	T	H	W	E	B	M	A

Codons la lettre `C`, la clé est donnée par la lettre `M`. On regarde dans le tableau l'intersection de la ligne donnée par le `C` de la première colonne (en vert), et de la colonne donnée par le `M` de la première ligne (en violet).

Le chiffre de Vigenère



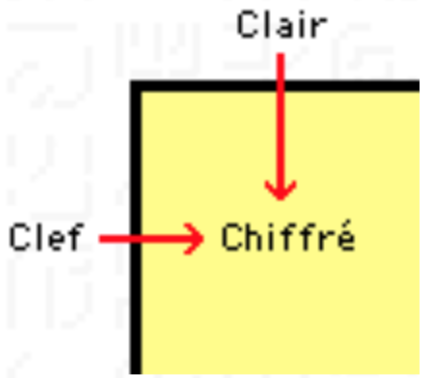
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

On trouve `O`. Puis on continue.

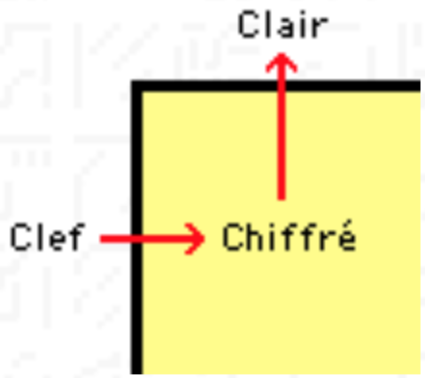
On trouve : `ORRWPSHDAIOEI EQ VBNARFDE`

Le chiffre de Vigenère

La lettre de la clé est dans la colonne la plus à gauche, la lettre du message clair est dans la ligne tout en haut.
La lettre chiffrée est à l'intersection de la ligne de la lettre clef et de la colonne de la lettre claire.



Pour chiffrer

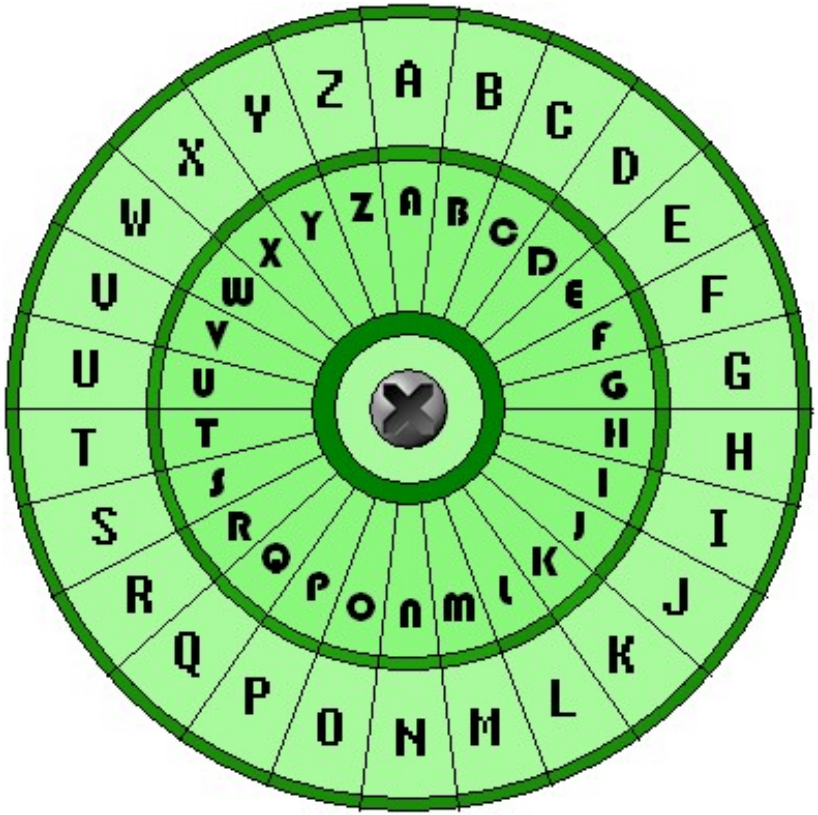


Pour déchiffrer

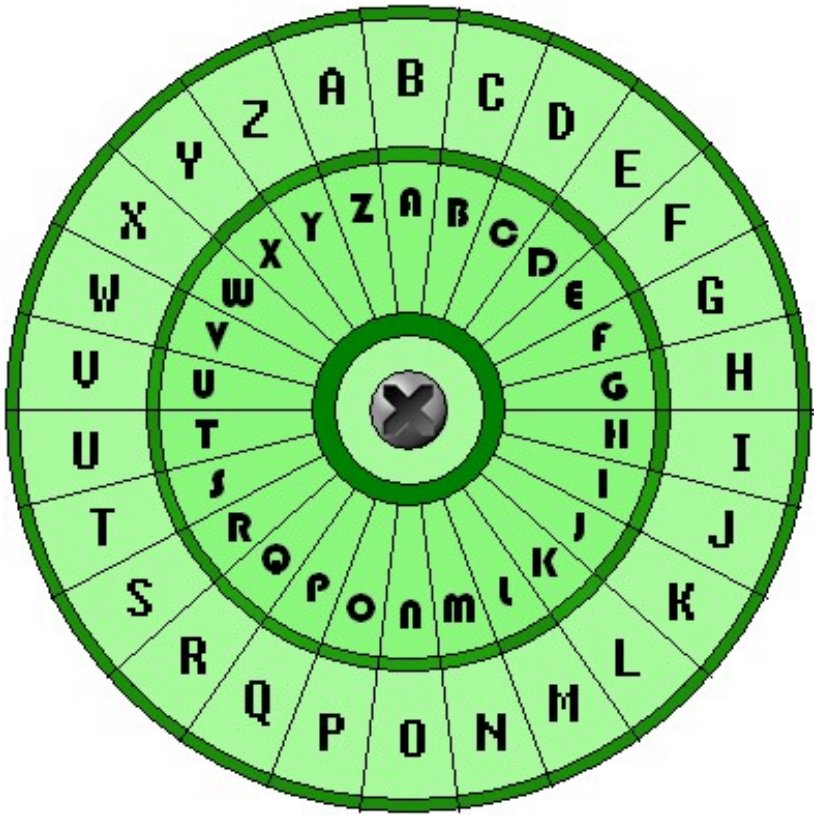
```
clair     MONMESSAGE
clef      MACLEFMACL
chiffré   YOPXIXEAIP
```

Exemple

Chiffrement polyalphabétique

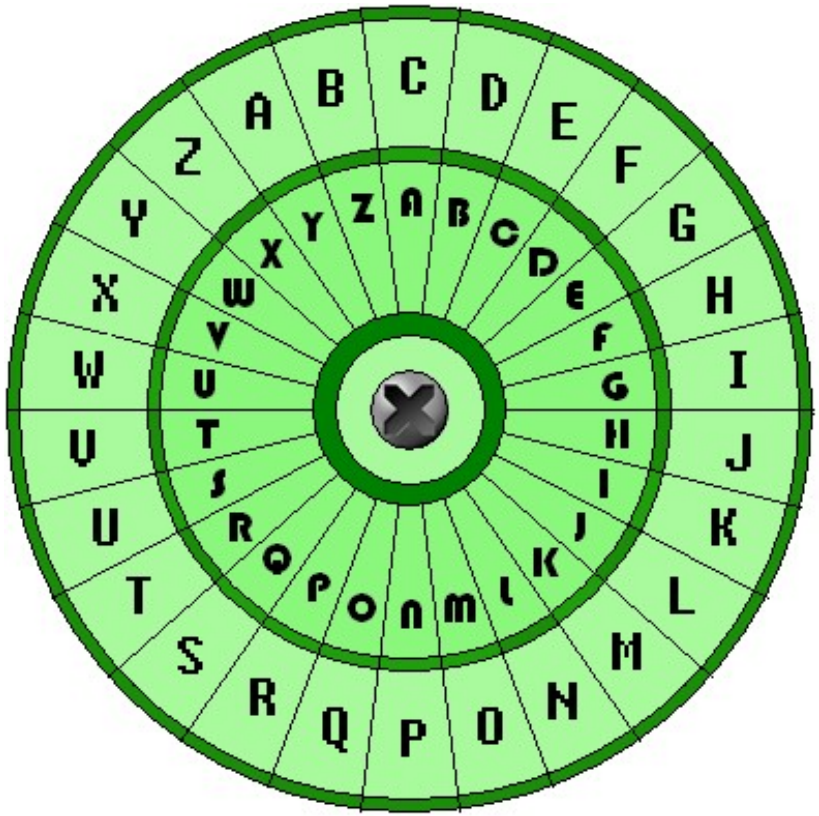


Chiffrement polyalphabétique



$\mathtt{C} \rightarrow \mathtt{D}$

Chiffrement polyalphabétique



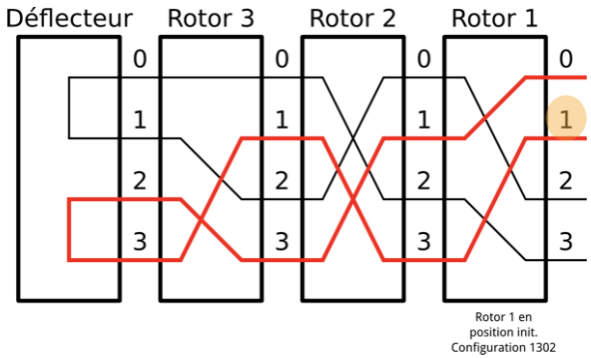
$\mathtt{C} \rightarrow \mathtt{D}$

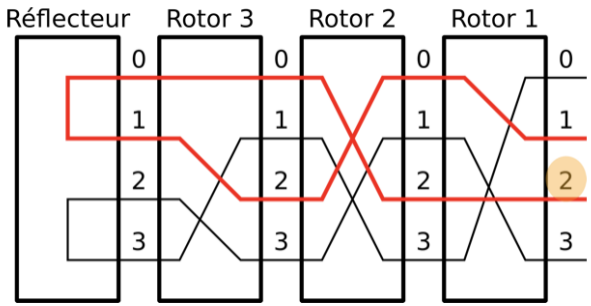
$\mathtt{R} \rightarrow \mathtt{T}$

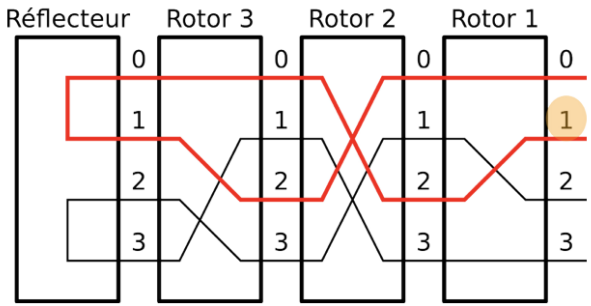
La machine Enigma

La machine Enigma – Fonctionnement 1

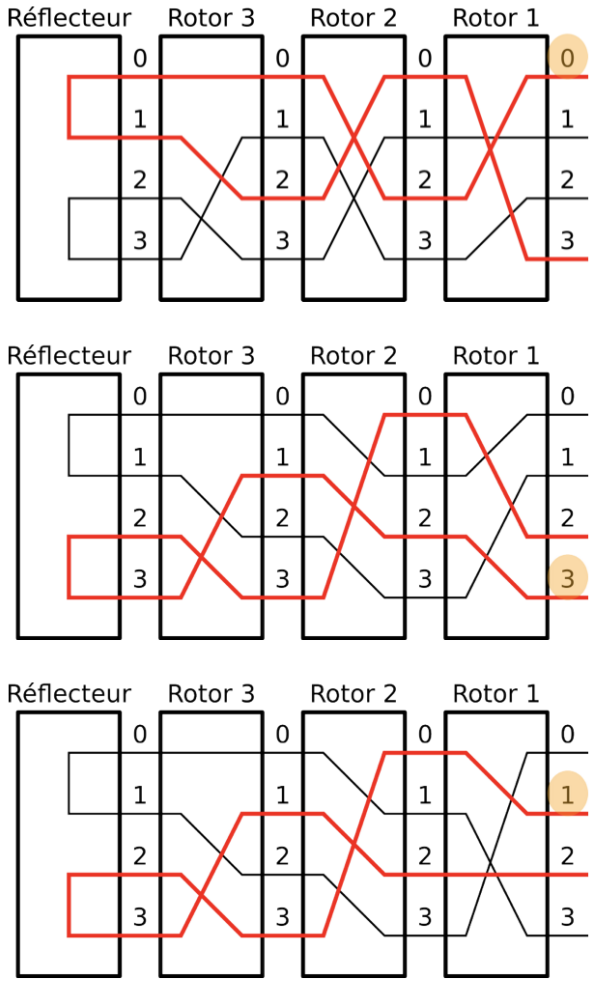
Codage du message 010322







La machine Enigma – Fonctionnement 2



Le codage du message 010322 est donc 121031

La machine Enigma – Fonctionnement 3

Pour déchiffrer le message obtenu, il suffit de remettre les 3 rotors dans la même configuration qu'au début du chiffrement et de présenter le message chiffré.

On obtient alors le message en clair (c'est la présence du réflecteur qui le permet).

Lien internet

pydefis.callicode.fr/defis/Enigma/txt

Forteresse digitale – Dan Brown

VEOROTBVUESESSES

Forteresse digitale – Dan Brown

VEOROTBVUESESSES

V	O	U	S
E	T	E	S
O	B	S	E
R	V	E	S