Histoire de la cryptographie

Qu'est ce que le cryptage ?

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés.

La plupart des méthodes de chiffrement reposent sur deux principes essentiels : la substitution et la transposition. Substituer signifie qu'on remplace certaines lettres par d'autres, ou par des symboles. Transposition signifie qu'on permute les lettres du message afin de le rendre inintelligible. Au cours des siècles, de nombreux systèmes cryptographiques ont été mis au point, de plus en plus perfectionnés, de plus en plus astucieux!

Qu'est ce que le cryptage ?

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés.

La plupart des méthodes de chiffrement reposent sur deux principes essentiels : la substitution et la transposition. Substituer signifie qu'on remplace certaines lettres par d'autres, ou par des symboles. Transposition signifie qu'on permute les lettres du message afin de le rendre inintelligible. Au cours des siècles, de nombreux systèmes cryptographiques ont été mis au point, de plus en plus perfectionnés, de plus en plus astucieux!

Un exemple de cryptage du XVI ème siècle : le modèle de Vigenère

Le chiffre de Vigenère est un système élaboré par Blaise Vigenère au XVI e siècle. Le chiffre de Vigenère est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message

Modèle de Vigenère avec pour clé de cryptage MATH

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

Histoire de la cryptographie

Pendant la guerre 1914-1918 la cryptographie prend un essor considérable. La maitrise de la cryptographie aident considérablement à déchiffrer les messages ennemis ce qui donne un avantage considérable lors d'un conflit.

Lors de la 2eme GM, les exploits des Alliés dans le domaine de la cryptographie auraient permit d'écourter la guerre de 1à 2 ans.

Une révolution dans la cryptographie : ENIGMA

La machine Énigma a été inventé par le hollandais Hugo Alexander en 1919.

ENIGMA

Un tableau de connexion de 3 rotors mobiles à 26 positions

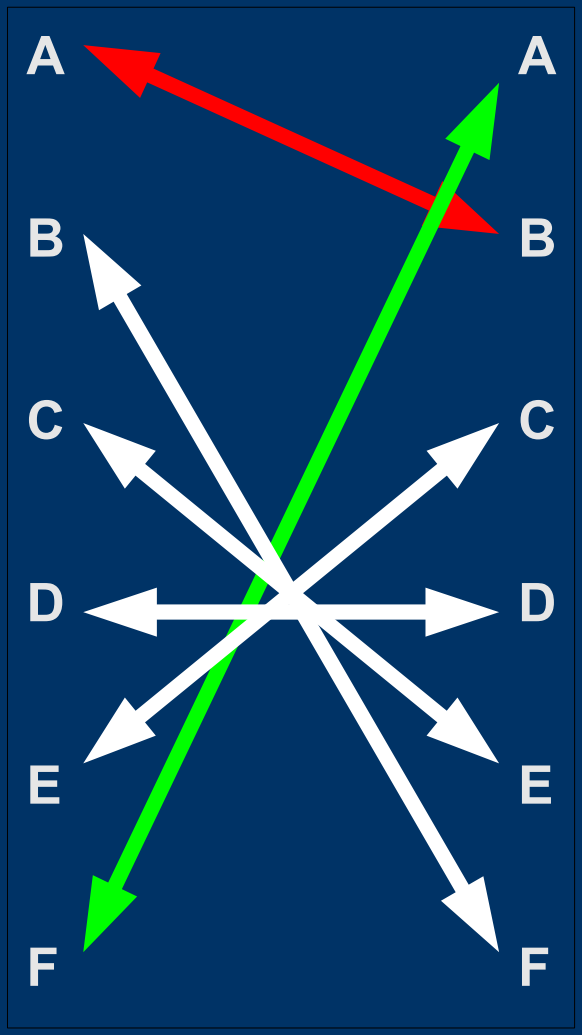
Le réflecteur

Tableau d'ampoules

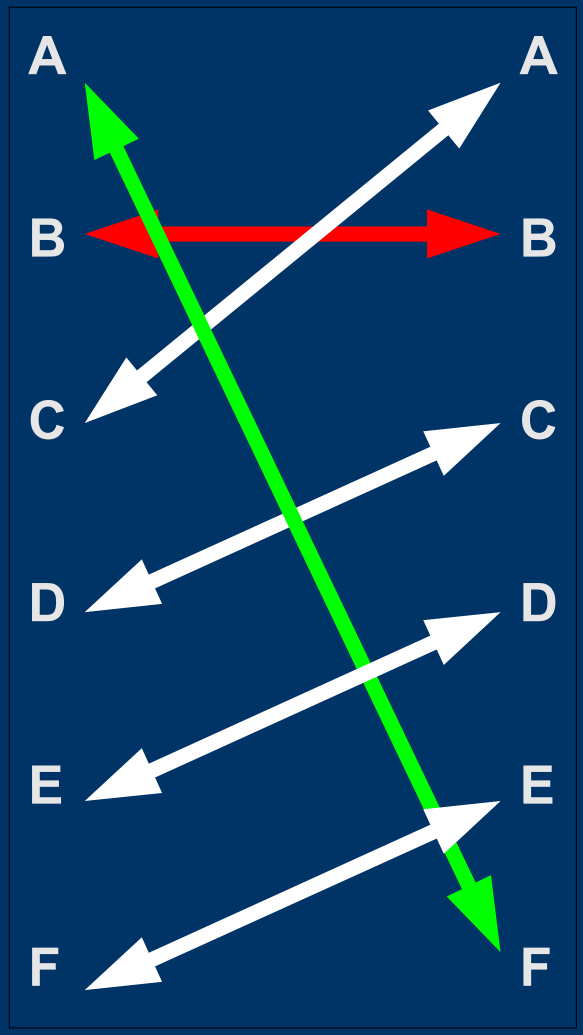
clavier alphabétique

L'Enigma se présente sous la forme d'une caisse en bois de 34×28×15 cm, et pèse une douzaine de kilos.

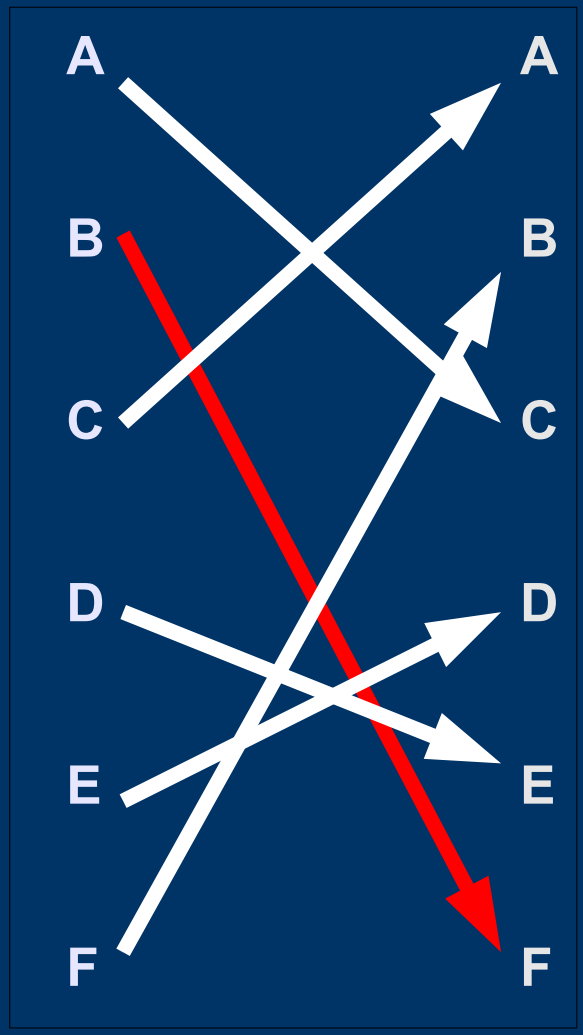
1er Rotor



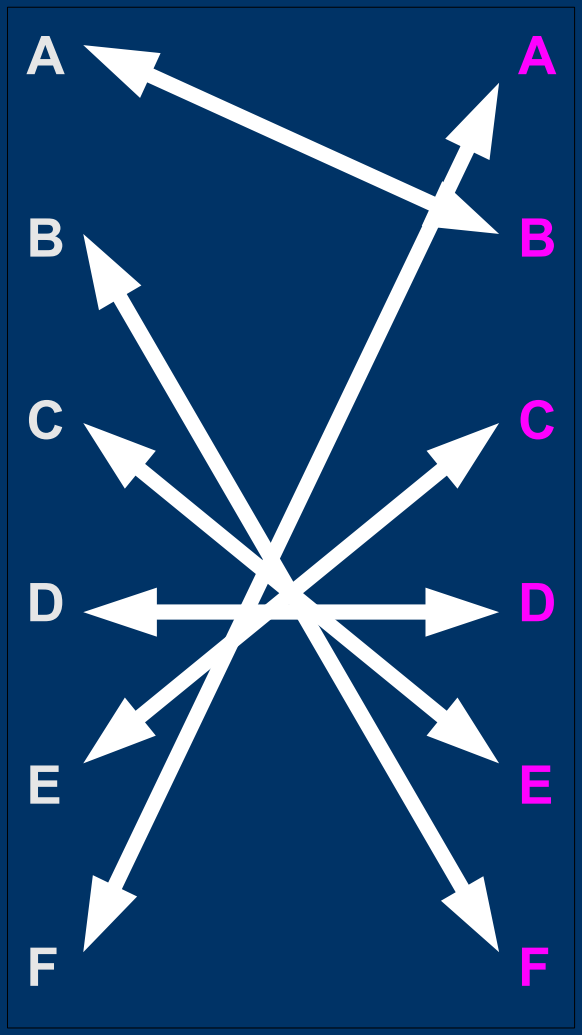
2ème Rotor



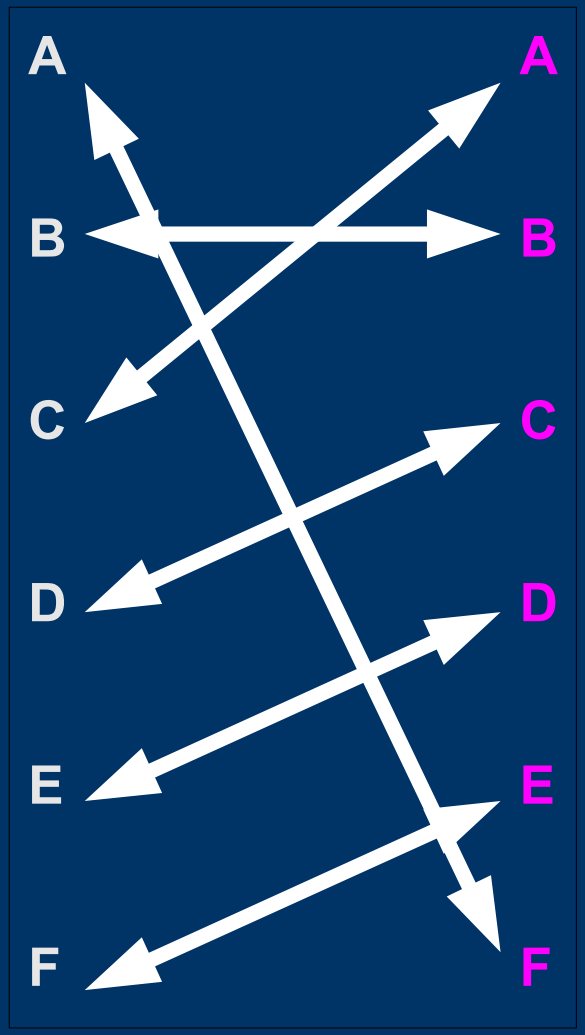
Réflecteur



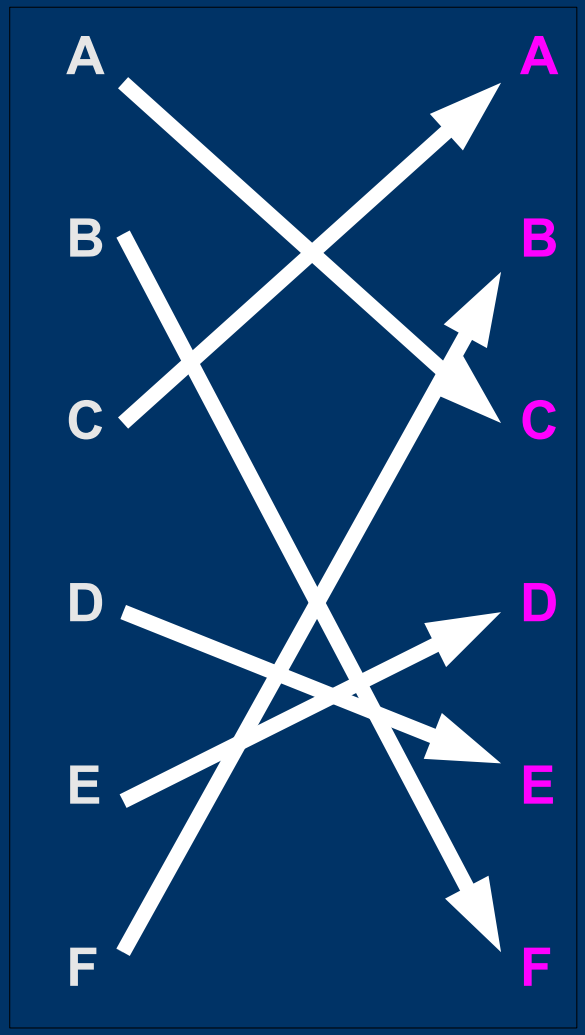
1er Rotor 0



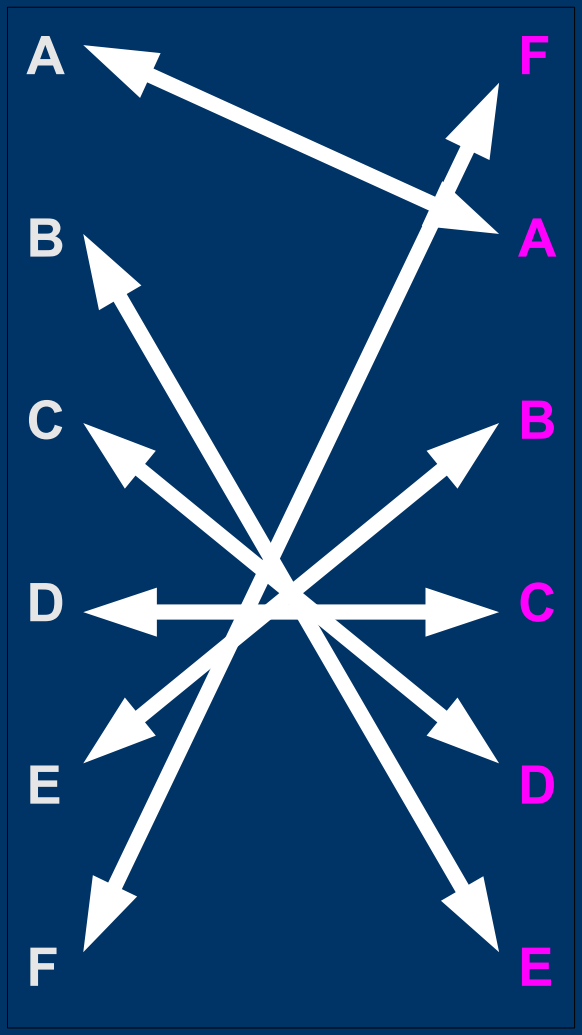
2ème Rotor 0



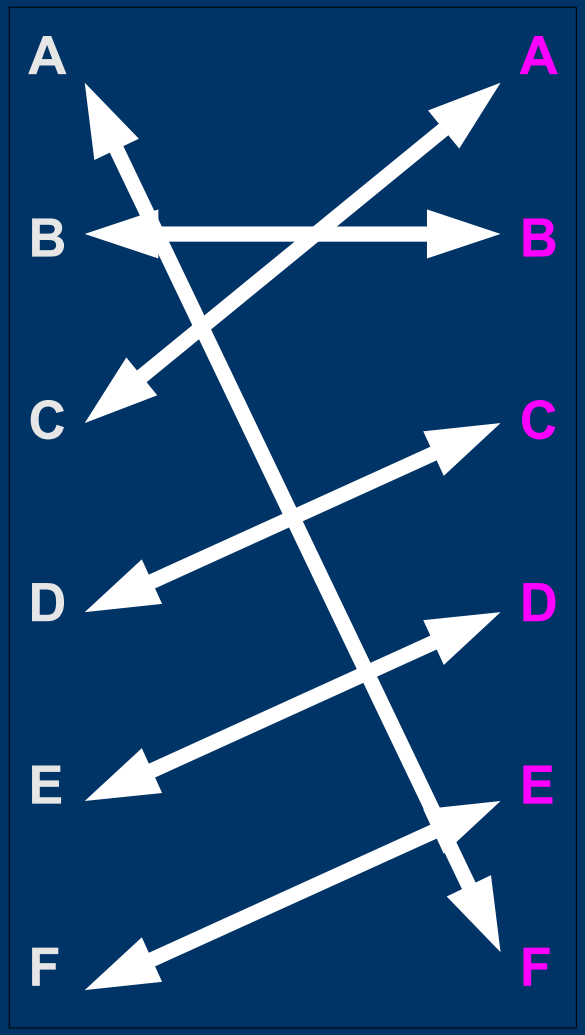
Réflecteur



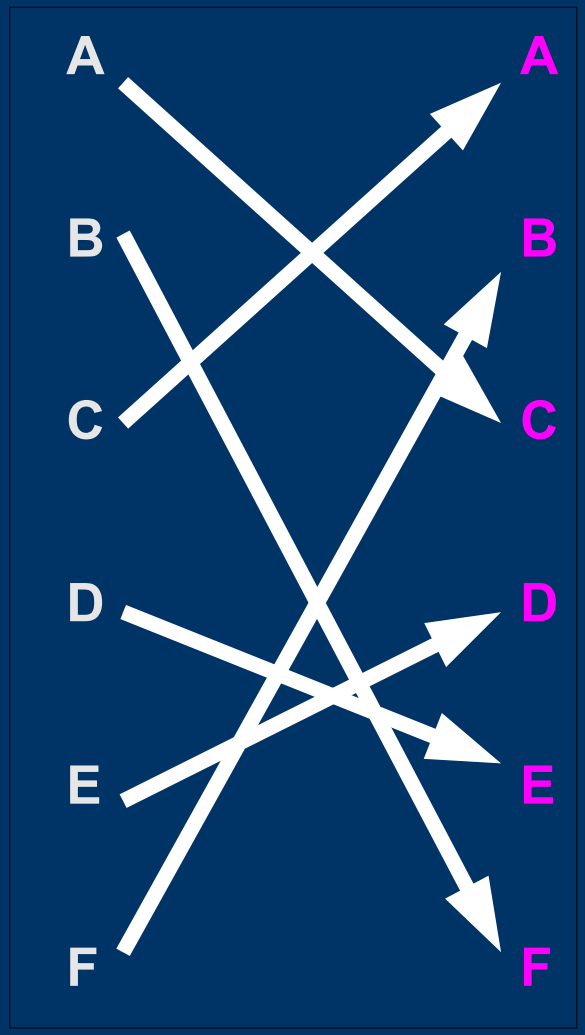
1er Rotor 1



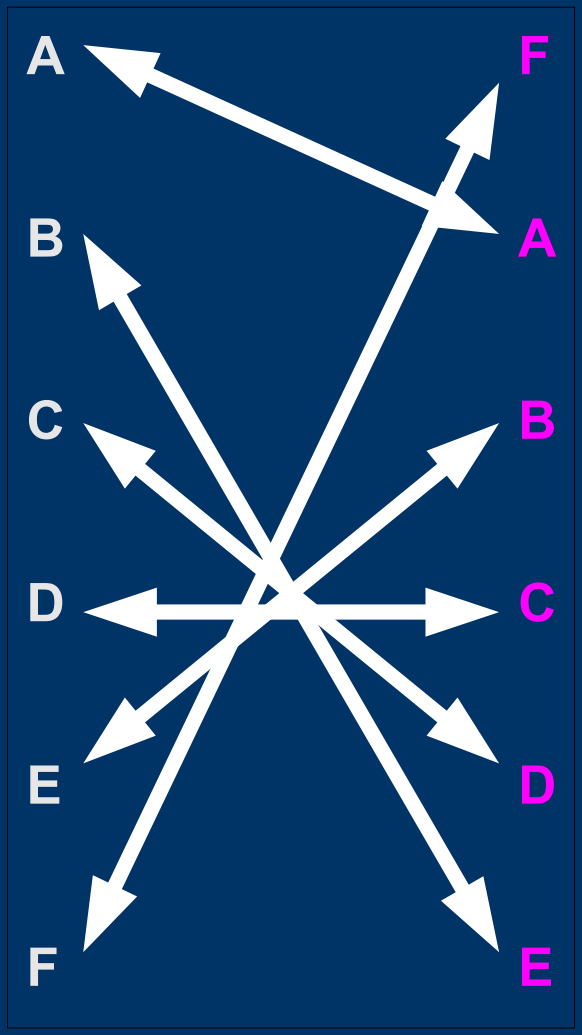
2ème Rotor 0



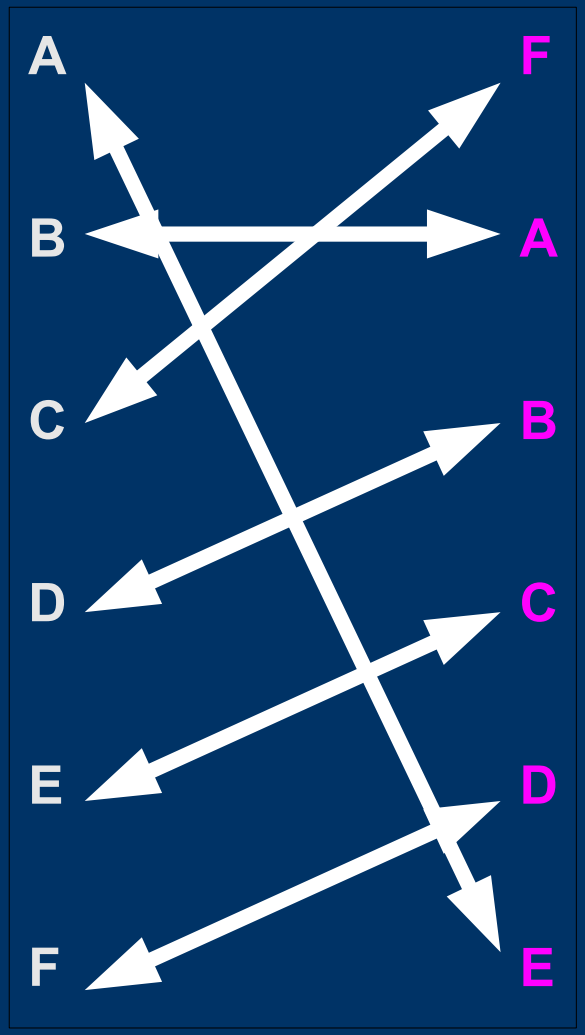
Réflecteur



1er Rotor 1



2ème Rotor 1



Réflecteur