Chiffrement

- Auteur : P. Petit (pascal.petit@shayol.org)
- La bibliographie cite des sources/ressources utiles de deux catégories:
  - Des sources dont je me suis inspiré pour certains points (notamment support de cours de C. Laforest qui a assuré cet enseignement jusqu'en 2007-2008)
  - Des sources pour des approfondissements
- Les schémas/photos qui ne sont pas de moi ont en général étaient récupérés sur wikipedia

Définitions

- *Texte en clair* : un texte sous sa forme originale, compréhensible tel quel
- *Chiffrement* : transformer un texte en clair en un texte incompréhensible
- La transformation inverse quand on possède tous les éléments pour le faire s'appelle le *déchiffrement* (ne pas confondre avec décryptage)
- *Décrypter* un texte: faire de même sans avoir les éléments (clef, ...). Le correspondant légitime déchiffre le texte, l'attaquant le décrypte.

Définitions

- *cryptographie :* domaine scientifique et technique dont le but est de garder les messages secrets. Pratiquée par les cryptographes
- *cryptanalyse* : domaine scientifique et technique dont le but est de retrouver les messages en clair sans avoir tous les éléments pour le faire. Pratiquée par les cryptanalystes
- *cryptologie:* : regroupe cryptographie et cryptanalyse. Pratiquée par les cryptologues.
- *Stéganographie*: domaine scientifique et technique dont le but est de faire passer inaperçu un message dans un autre objet

Stéganographie : exemple (G. Sand à A. De Musset)

Je suis très émue de vous dire que j'ai bien compris l'autre soir que vous aviez **toujours une envie folle de me faire** danser. Je garde le souvenir de votre **baiser et je voudrais bien que ce soit** la une preuve que je puisse etre aimee **par vous. Je suis prete a montrer mon** affection toute desinteressee et sans cal- **cul, et si vous voulez me voir aussi** vous devoiler sans artifice mon ame **toute nue, venez me faire une visite.** Nous causerons en amis, franchement. **Je vous prouverai que je suis la femme** sincère, capable de vous offrir l'affection **la plus profonde comme la plus étroite** en amitié, en un mot la meilleure preuve **que vous puissiez rêver, puisque votre** âme est libre. Pensez que la solitude ou j'ha- **bite est bien longue, bien dure et souvent** difficile. Ainsi, en y songeant j'ai l'âme **grosse. Accourez donc vite et venez me la** faire oublier par l'amour ou je veux me **mettre.**

Définitions

- Soit M un message en clair à faire transiter de façon sûre entre Alfred et Bachir
- Soit E le processus de chiffrement
- Soit D le processus de déchiffrement
- Alfred calcule et transmet C=E(M)
- Bachir reçoit C et doit connaître D pour retrouver M=D(C)
- On doit avoir M=D(E(M))

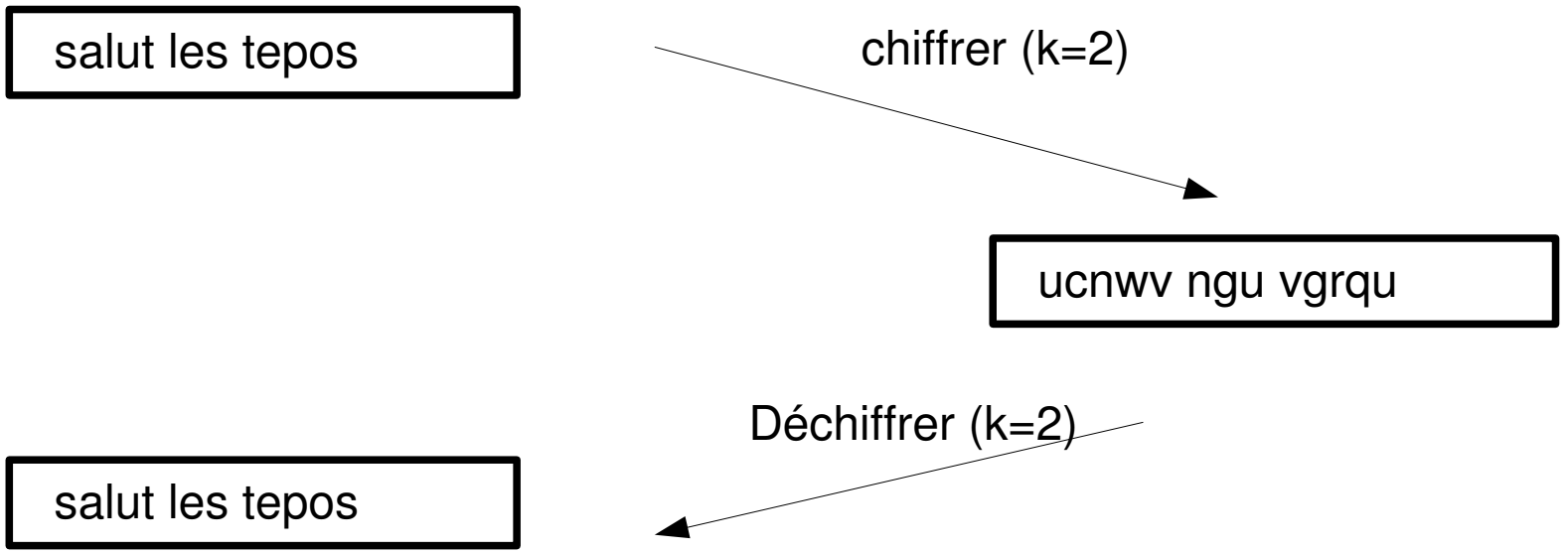
Historique

- L'artisanat
  - Chiffrement de césar
  - Permutation et attaque statistique
- La technique
  - ENIGMA
- Masque jetable
- L'ère scientifique (actuelle)
- Principes actuels

Chiffrement de césar

k=2 (décalage de l'alphabet pour chiffrer)

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
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



Chiffrement de césar

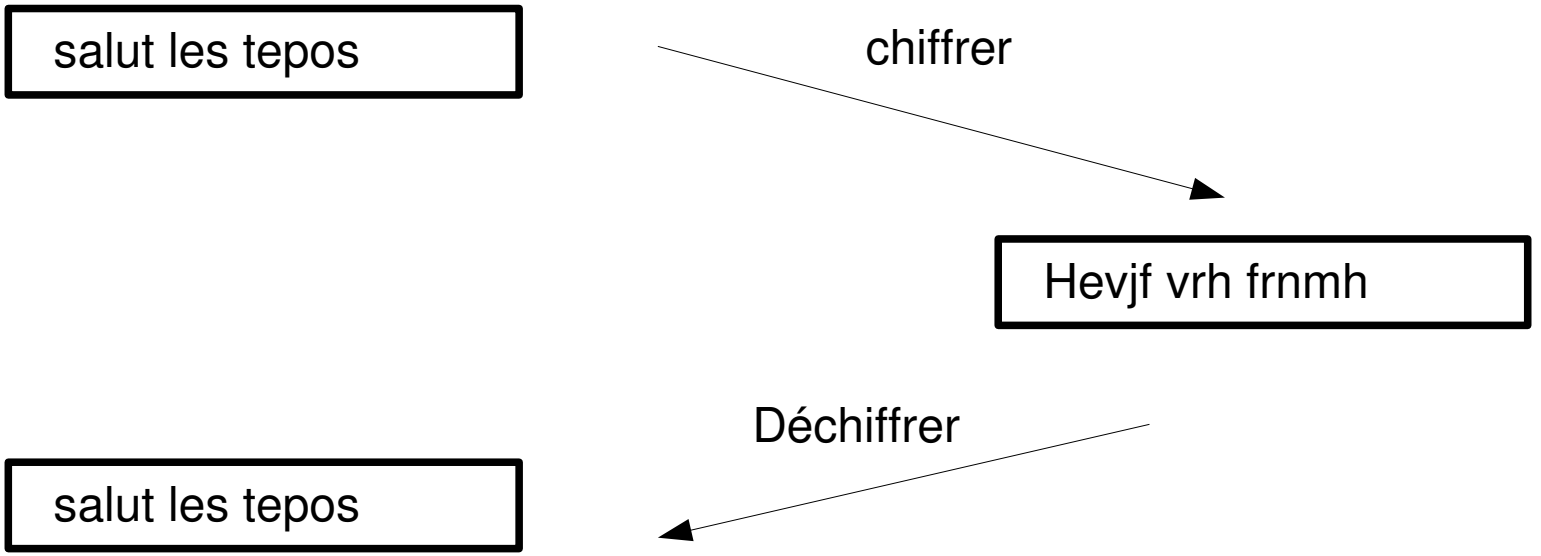
- Décaler chaque lettre de K caractères dans l'alphabet
- Exemple1: k=2 « salut les tepos » devient « ucnwv ngu vgrqu »
- Le déchiffrement se fait en décalant les lettres dans l'autre sens
- Exemple2: rot13: l'opération de codage et de décodage sont les mêmes (but: qu'un texte ne soit lu que par les gens qui souhaitent le lire. Utilisé couramment sur les forums USENET)

Chiffrement de césar

- Une fois le mécanisme est connu, la sécurité repose sur la connaissance de k
- 25 valeurs possibles pour k. Il suffit de les essayer toutes jusqu'à trouver un texte qui a un sens
- Attaque en force brute: on essaie tout ou partie des clefs
- Ici :
  - l'espace des clefs est trop petit (25 valeurs possibles)
  - Les textes résultats sont reconnaissables

Permutation alphabétique

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
e	t	c	g	r	u	i	o	q	a	x	v	w	s	m	n	b	d	h	f	j	k	l	y	z	p



Permutation alphabétique

- On utilise une permutation quelconque de l'alphabet
- Avec un alphabet de n caractères, n ! permutations possibles
- L'espace des clefs devient très grand (26! ~ 2^88). L'attaque par force brute devient trop longue

Permutation alphabétique

- Problème: chaque lettre est toujours remplacée par la même lettre. Si on a réussit à la décoder une fois, on saura la décoder partout
- 3 attaques complémentaires possibles :
  - Parfois, de notre connaissance de la structure du message, on peut en déchiffrer certaines parties
    - On peut déchiffrer les lettres correspondantes partout dans le message
  - Attaque statistique: connaissant la langue dans laquelle le message a été écrit, on peut s'appuyer sur des statistiques d'occurrences des caractères dans cette langue

Permutation alphabétique: exemple

- Sur la page WeB de ressources du cours, on vous propose un fichier chiffré à l'aide d'une permutation alphabétique
- Cf https://www.ibisc.univ-evry.fr/~petit/Enseignement/Chiffrement-compression/crypto-2009-2010/exemple-noPonctuation-code-MAJ.txt
- Déchiffrez le

Chiffrement de vigenère: substitution polyalphabétique

- Au XVe siècle, Alberti eu l'idée de combiner plusieurs alphabets chiffrés mais sans aboutir à un système complet viable
- Son idée avait l'avantage de casser les attaques statistique puisqu'une même lettre peut être codée de plusieurs façon différente
- Jean Tritheme, un abbé allemand, Giovanni Porta, un savant italien continuèrent son travail
- Blaise de Vigénère, un diplomate français, s'appuya sur leur travail pour proposer un système de chiffrement révolutionnaire qui portera son nom.

Chiffrement de vigenère: substitution polyalphabétique

- Principe: chaque lettre du message est chiffré à l'aide d'un chiffrement de César avec un décalage différent;
- Pour simplifier la transmission des tables, on indique la version chiffrée de A (et on en déduit le décalage et donc les versions chiffrées des autres lettres);
- La clef est un texte indiquant la suite des versions chiffrées de la lettre A
- Un fois arrivé au bout de la clef, on repart au début

Vigénère: exemple

- Clef: tepos ; Texte à chiffrer: « ilfai tfaim »
- La lettre « i » est chiffrée avec la transformation de César transformant « a » en « t », « l » avec celle transformant « a » en « e »

```
i l f a i t f a i m   (texte à chiffrer)

t e p o s t e p o s  (clef répétée autant que nécessaire)

----------------------

B P U O A M J P W E  (version chiffrée du texte)
```

La table de la page suivante simplifie le travail de chiffrement.

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Vigénère: solidité

- Espace des clefs : n^p (avec n: nombre de caractères possibles et p: taille de la clef)
- 26^8 (avec un alphabet non accentué en minuscules et une clef de 8 lettres) = $\#2*10^{11} = \#2^{31}$
- Des lettres identiques sont chiffrées différemment: attaque statistique impossible

Attaques sur Vigénère

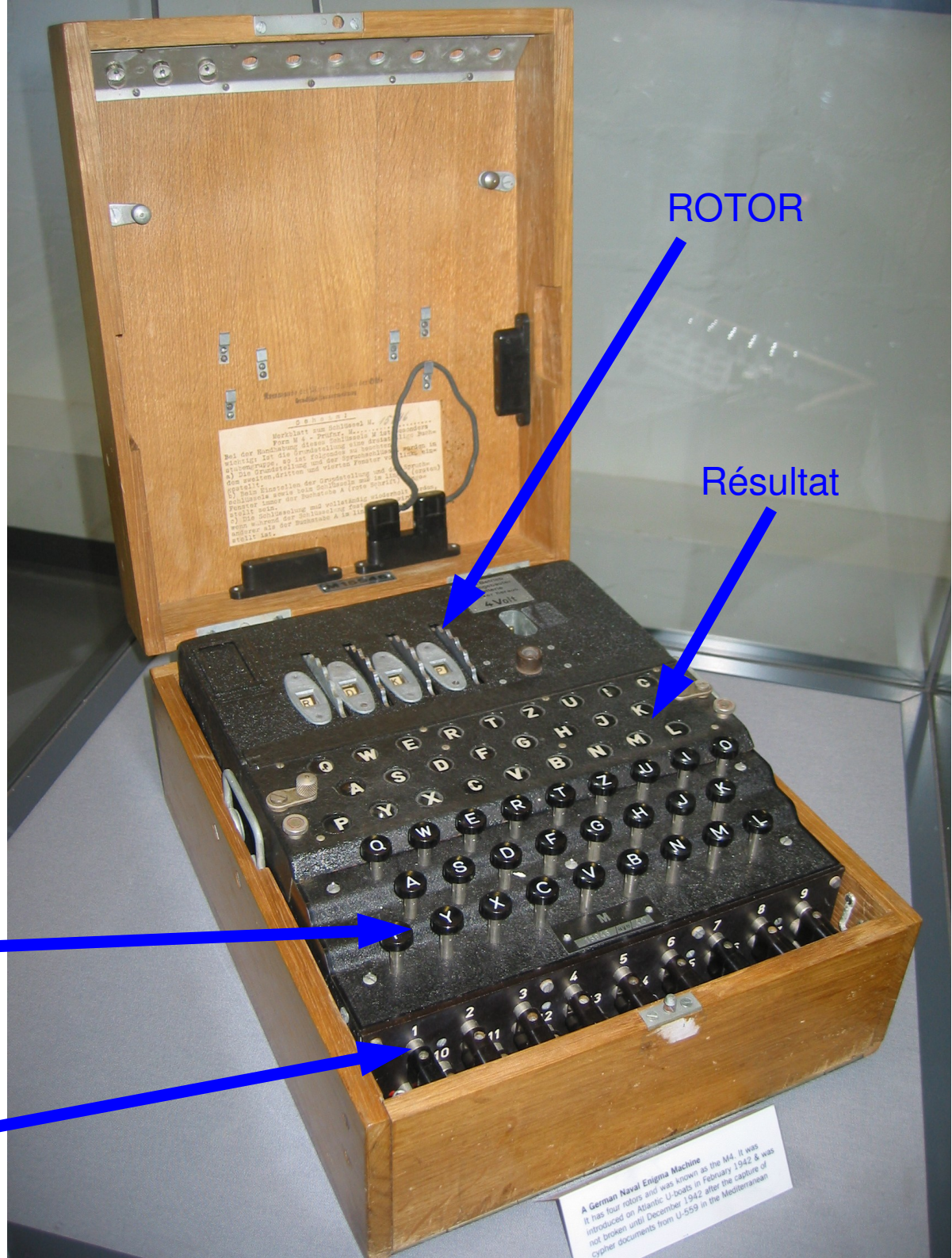
- Pb: comment trouver la taille de la clef ?
- Exemple tiré de [SINGH-1999] :
  - Voir en TD

Transposition

- Transposition: changer l'ordre des lettres du texte
- Très à la mode au XVIIIe et XIXe siècle
- Exemple:
  - on range le texte du message dans un tableau rectangulaire ligne par ligne
  - Le message chiffré s'obtient en lisant le tableau colonne par colonne
- Cryptanalyse:
    - Pas très solide
    - Voir Bauer: « decrypted secrets »

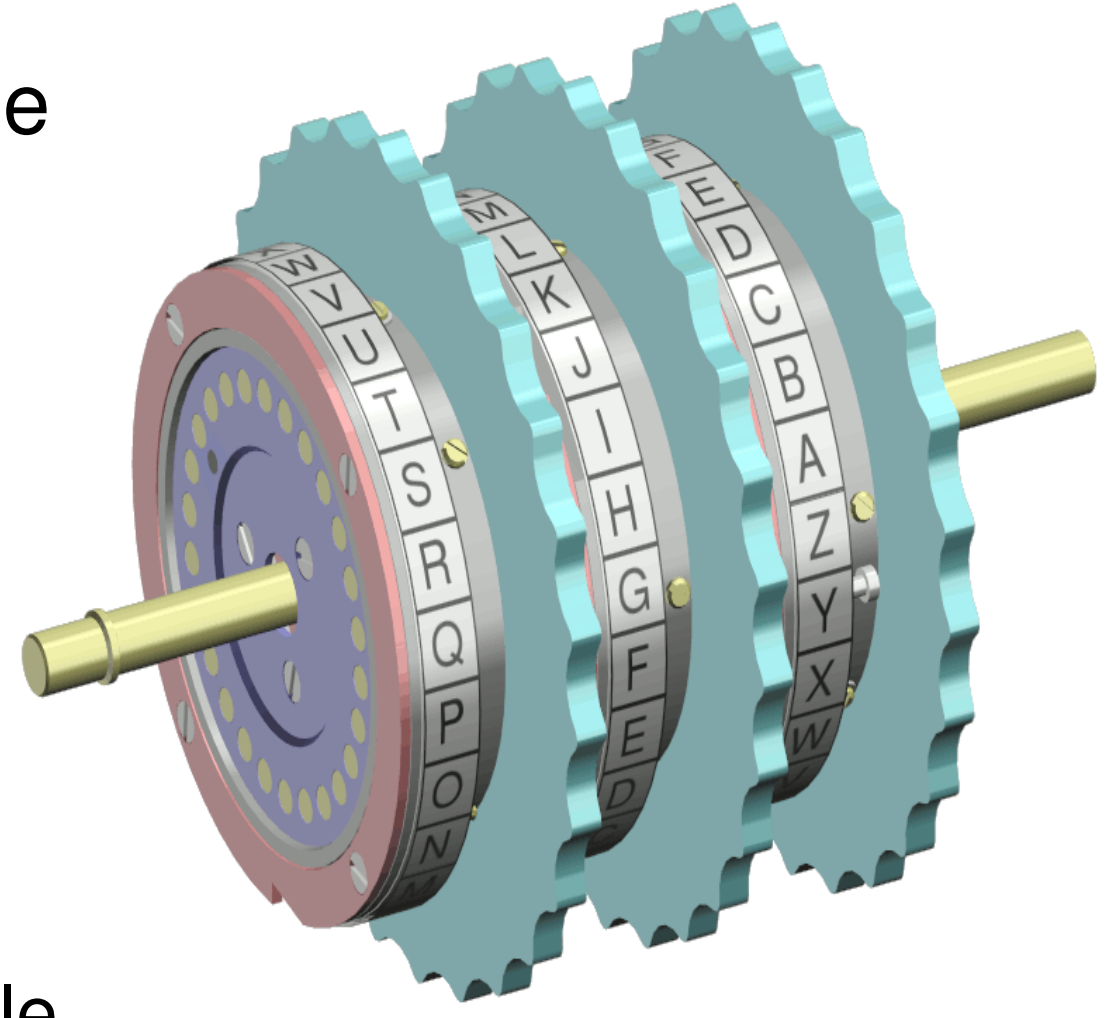
ENIGMA

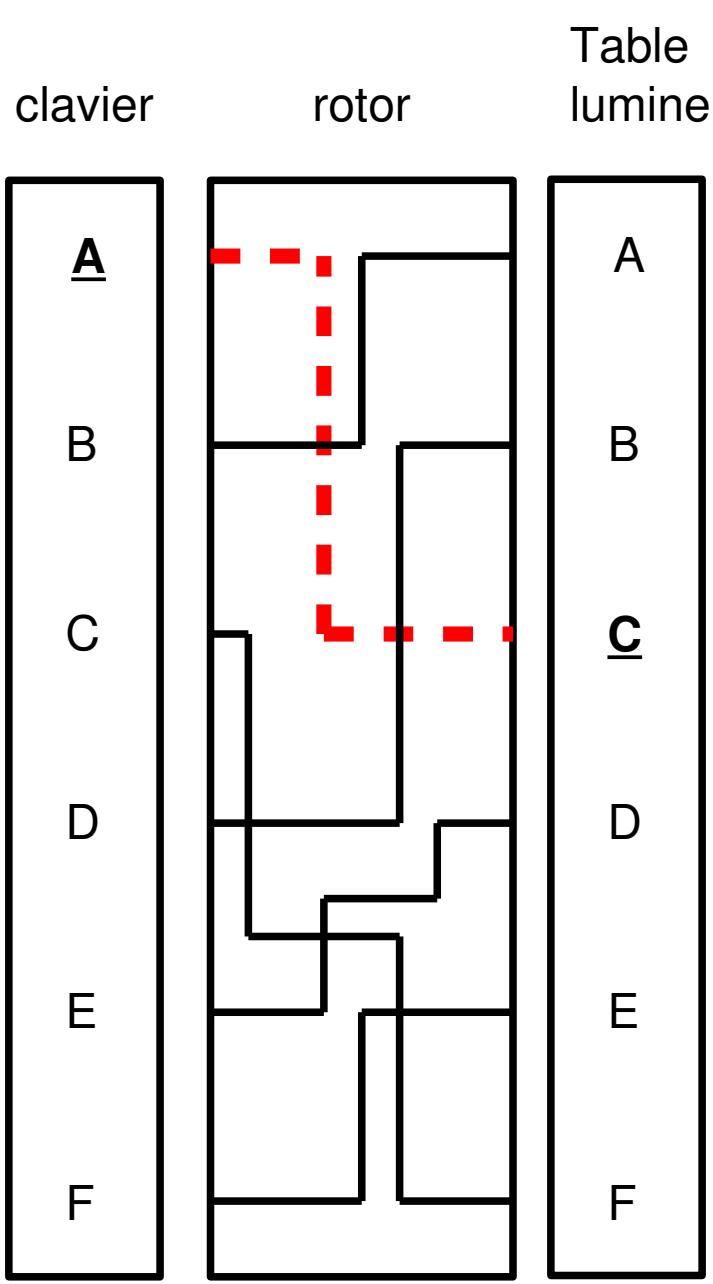
- Utilisé par les allemands durant la seconde guerre mondiale
- déchiffré par les anglais sur de longue périodes



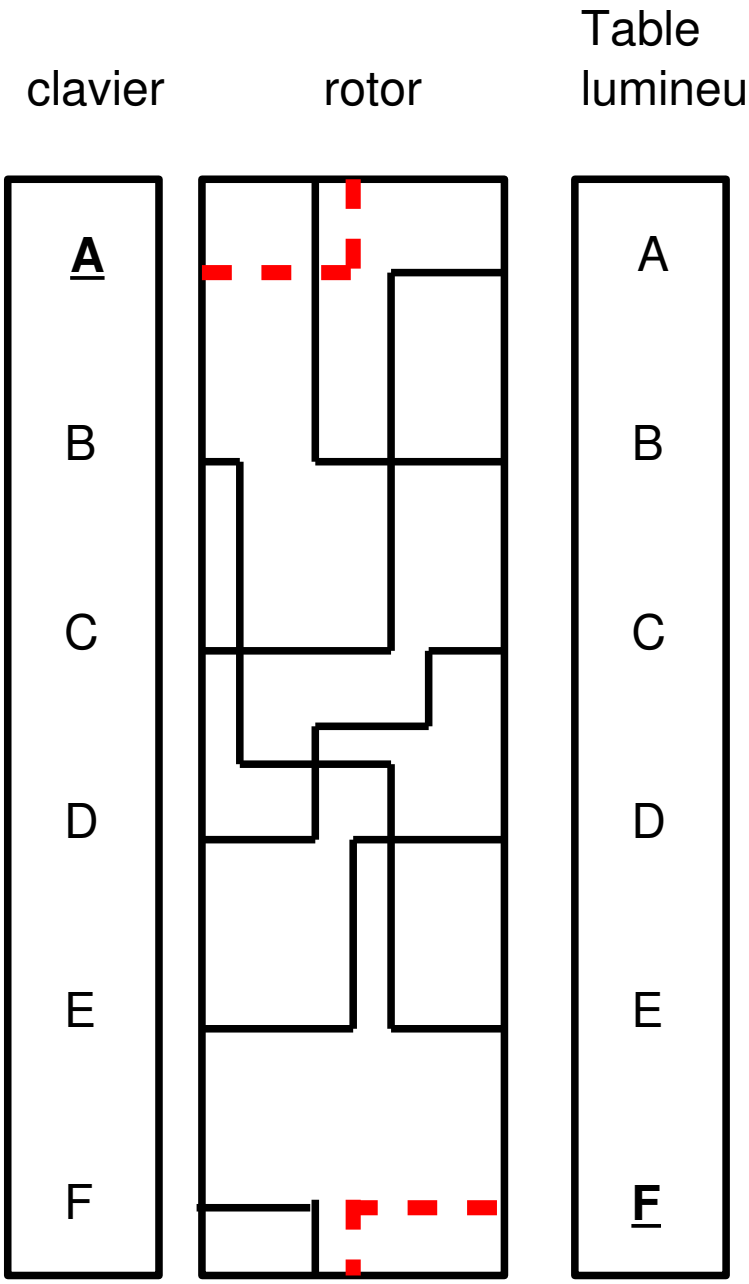
ENIGMA

- Chaque rotor réalise une substitution alphabétique
- À chaque codage d'un caractère,
  - le premier rotor tourne
  - Quand le premier rotor a fait un tour, le second rotor tourne
  - ...





Enigma



Enigma après avancement du rotor d'un cran

Enigma

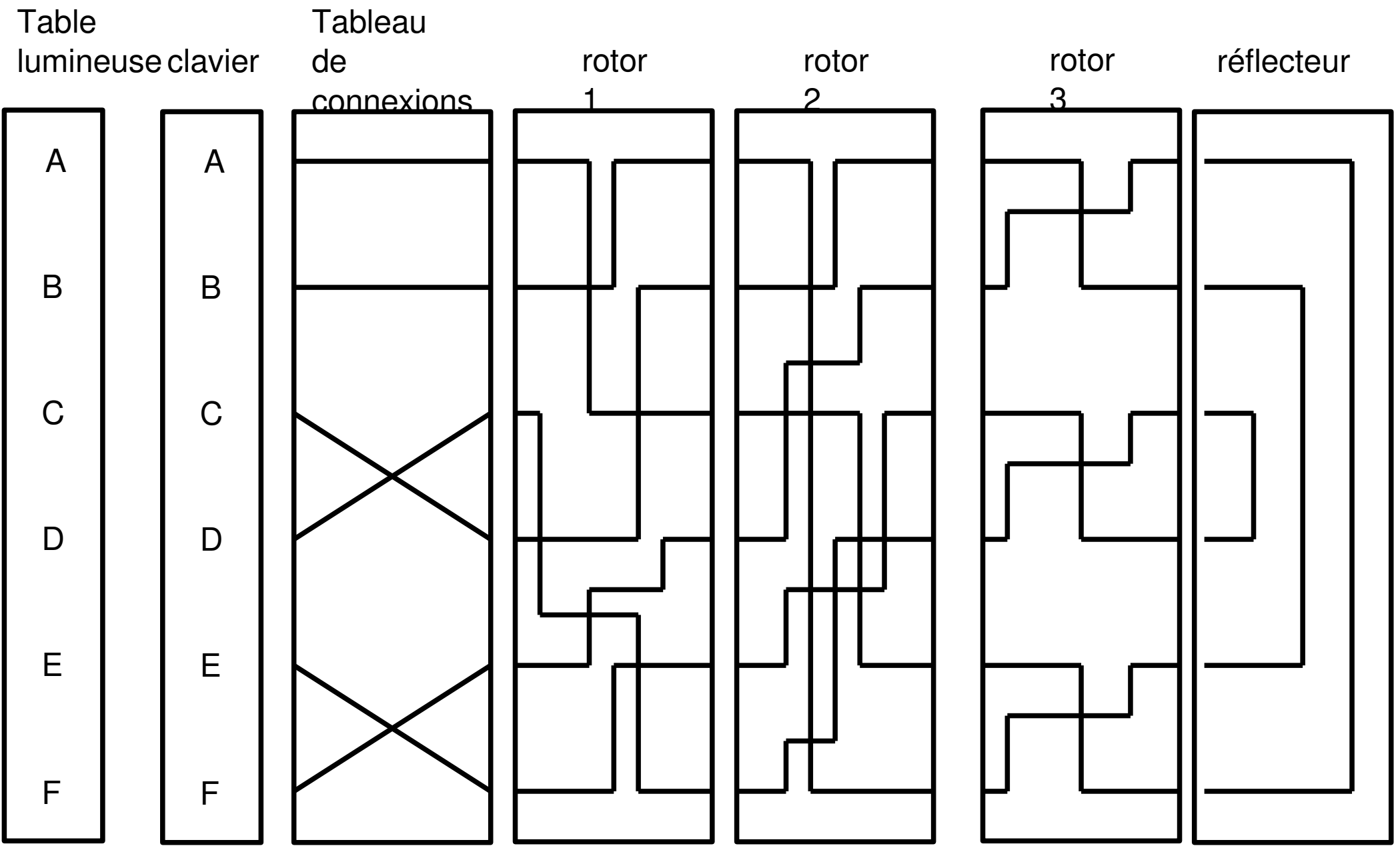
- Conséquence :
  - Les substitutions changent donc à chaque caractère codé
  - Il faut que **tous** les rotors aient fait un tour complet pour qu'on retrouve la même transformation
    - Avec un rotor alphabétique, il faudrait 26 mouvements pour revenir à la transformations initiale
    - Avec deux rotors, 26*26
    - Avec n rotor 26^n
  - Les attaques sur vigenere ont montré la faiblesse que constituait de la répétition des transformations
  - Là, on les limite à défaut de les supprimer

ENIGMA: transpositions

- Pour compliquer :
  - ajout d'un étage de transposition permettant d'échanger deux lettres: ENIGMA avait 6 mécanismes permettant l'échange de 2 lettres au choix
  - Ajoute 100 391 791 500 possibilités = C(26,12)*11*9*7*5*3*1
    - C(26,12): choisir 12 lettres parmi 26 sans tenir compte de l'ordre
    - Ensuite, on choisir la lettre qu'on associe à la première: 11 possibilités.
    - Il reste 10 lettres disponible.On fait de même pour la première de ces 10 lettres: reste 9 possiblités
    - ...

ENIGMA: nature et nombre des clefs

- Clef:
  - Le choix de la position des rotors. 3 rotors différents que l'on peut placer à la place de son choix :6 possibilités
  - La position initiale des rotors => 26^3=17576 clefs
- des attaques manuelles sont encore possible
- Plus tard: jusqu'à 8 rotors + choix des rotors
- Un mécanisme de permutations de 6 fois 2 lettres multiplie le nombre de possibilités par 100 391 791 500
- => espace de clef très grand = #10^{16} = #2^{53}



Permutations: 2 permutations de 2 lettres dans notre exemple

Réflecteur: codage et décodage sont une seule et même opération

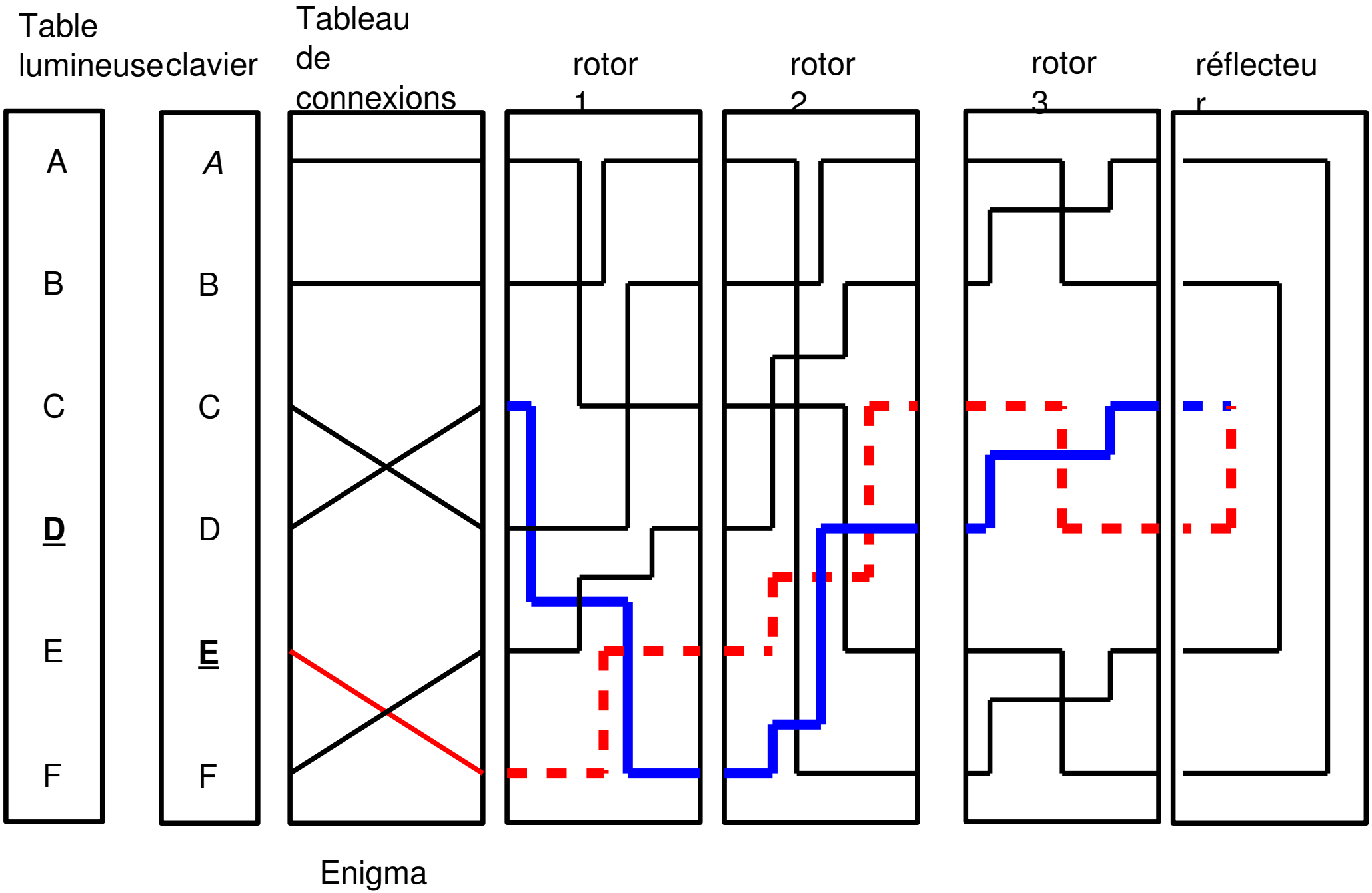


Table lumineuse
clavier
Tableau de connexions
rotor 1
rotor 2
rotor 3
réflecteur
A
B
C
D
E
F
A
B
C
D
E
F
Enigma

Mise en oeuvre d'Enigma

- Une clef différente par jour (unique pour toutes les Enigma) :
  - Réglage des connexions: A/L,B/T,E/U,P/F,O/Y
  - Emplacement des brouilleurs : 2, 1, 3
  - Orientation des brouilleurs: Q-C-W (lettre visible)
  - Cette clef sert à chiffrer et transmettre la clef qui servira à chiffrer réellement le message :
    - Pour chaque message, l'émetteur choisit une orientation des brouilleurs et la transmet chiffrée avec la clef du jour. Les autres réglages restent identiques

Bibliographie

- [SINGH-1999]: « Histoire des codes secrets » de Simon Sigh, Livre de poche, 1999 : un ouvrage de vulgarisation qui lit facilement et qui contient aussi pas mal d'informations techniques sur les chiffrements historiques et notamment Enigma