Enigma

La machine Enigma

Le but de ce TD est de modéliser une machine Enigma, utilisée par les Allemands durant la seconde guerre mondiale. D'un point de vu technique, la machine Enigma est une machine électro-mécanique. Elle se présente comme une grosse machine à écrire qui en plus du clavier contient un tableau de lampes (les 26 lettres de l'alphabet dont une lettre est allumée à chaque fois qu'une touche est appuyée, voir Fig. 1) situé au-dessus du clavier et un tableau de fils situé en face avant sous le clavier qui permet de définir une substitution supplémentaire. Tout le mécanisme modifie et ferme un circuit électrique qui va allumer une lampe. Si l'opérateur est en train de taper le texte clair, les lampes indiquent le texte chiffré et inversement.

Le mécanisme de la machine se compose de 3 rotors assemblés en cascade et d'un réflecteur, qui permet d'avoir la même machine avec le même paramétrage pour le codage et le décodage. De plus sur les 2 premiers rotors, une bague est fixée à une certaine position (donnée par la clé). Cette position permet à la machine de faire tourner le rotor suivant d'un cran uniquement lorsque le décalage du rotor vaut la valeur de la position de la bague.

La clé va se composer comme suit :

- 3 chiffres indiquant l'ordre d'assemblage des rotors
- 3 lettres indiquant le décalage initial des 3 rotors
- 2 lettres indiquant la position des bagues situées entre le 1^{er} et le $2^{\text{ème}}$ rotor et entre le $2^{\text{ème}}$ et le $3^{\text{ème}}$ rotor.

Exemple 1. *Nous définissons la clé suivante :* `132ACFBZ`*. Cette clé indique que les rotors à placer dans la machine seront dans cet ordre le rotor* 1*, puis le rotor* 3 *puis le rotor* 2*. La première série de* 3 *lettre code la position des rotors, ainsi le* A *indique que le premier rotor sera placé à la position* 0*, le* C *indique que le deuxième rotor sera positionné à la position* 2 *et le troisième sera positionné à la position* 5*. Enfin, les deux dernières lettres indiquent la position des bagues. La première bague sera placée au niveau de la position* 1 *du premier rotor et la seconde bague sera positionnée au niveau de la position* 25 *du deuxième rotor.*

Nous disposons donc de 3 rotors différents numérotés de 1 à 3 dont les liens internes sont décrits dans la Fig. 2, et du réflecteur décrit dans la Fig. 3. Dans un premier temps, nous n'allons pas considérer le tableau de connexion (la permutation initiale). Ainsi, la lettre A du clavier et du tableau de lampes est liée à la position absolue 0, la lettre B à la position absolue 1, ... et la lettre Z est à la position absolue 25.

Exemple 2. *Nous allons considérer que la clé de notre message est* `132ACFBZ`*. Et que nous voulons coder le mot "été". Nous appuyons sur la lettre* E*. Cette lettre est à la position absolue* 4*. Le* 1^{er} *rotor traversé est le rotor N*ř1 *qui a un décalage de* 0*, c'est-à-dire que la position relative* 0 *du rotor*

FIG. 1 – L'opérateur appuie sur la lettre S et la lettre N s'allume.

se situe en face de la position absolue 0. *Ainsi le lien qui va de* $4 \rightarrow 11$ *est utilisé. À la sortie du rotor* 1, *le circuit allimenté se trouve à la postion absolue* 11. *Le rotor* 3 *qui se trouve après le rotor* 1 *possède un décalage de* 2 *crans. Ainsi la position relative* 13 *se trouve face à la position absolue* 11. *La position* 13 *du rotor* 3 *est liée à la position* 11 *qui correspond avec ce décalage à la position absolue* 13, *et ainsi de suite... La Fig. 4 représente le processus de cryptage complet du mot "été".*

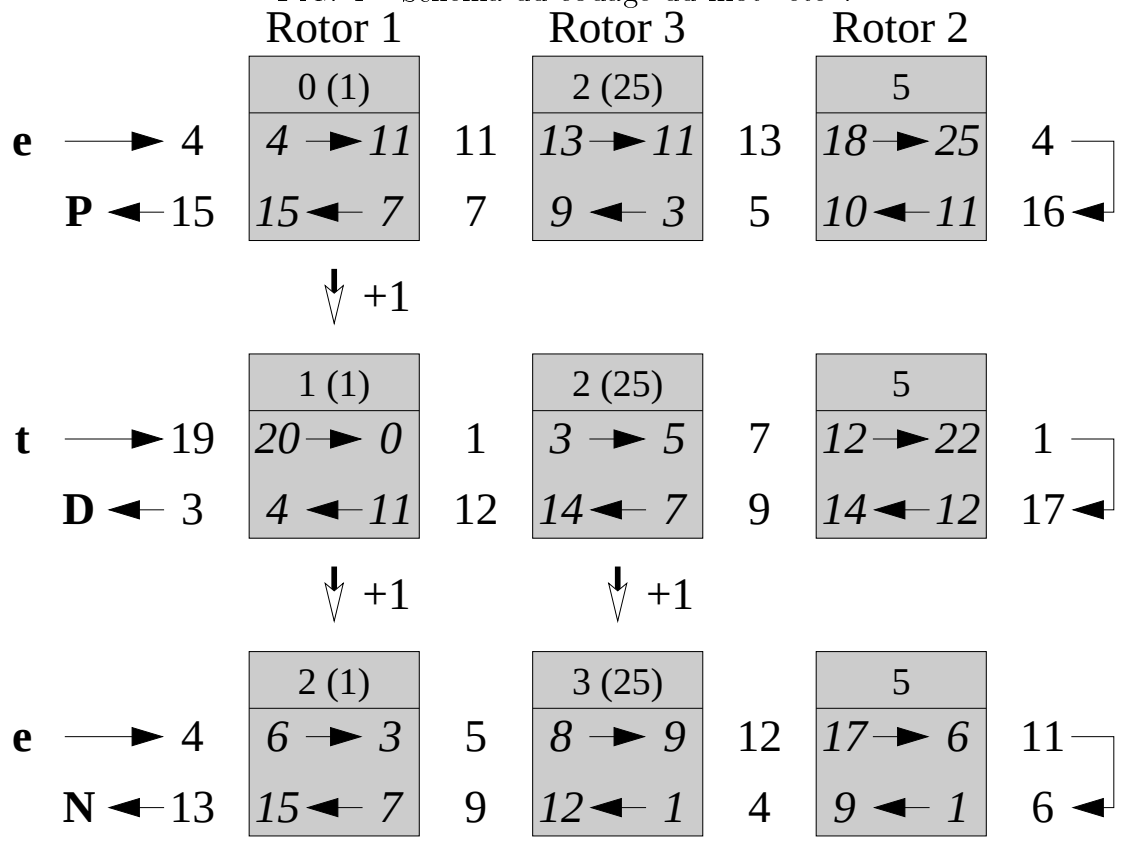
FIG. 2 – Câblage des rotors.

pos. rel. début	pos. rel. fin rotor Nř1	pos. rel. fin rotor Nř2	pos. rel. fin rotor Nř3
0	4	0	13
1	10	9	15
2	12	3	24
3	5	10	5
4	11	18	21
5	6	8	14
6	3	17	4
7	16	20	0
8	21	23	9
9	25	1	3
10	13	11	20
11	19	7	23
12	14	22	1
13	22	19	11
14	24	12	7
15	7	2	10
16	23	16	18
17	20	6	8
18	18	25	17
19	15	13	22
20	0	15	19
21	8	24	12
22	1	5	2
23	17	21	16
24	2	14	6
25	9	4	25

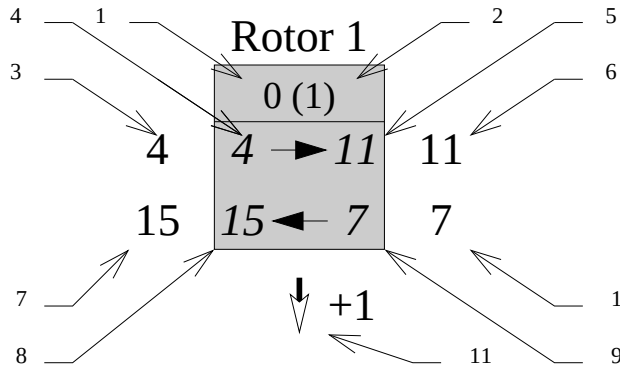
FIG. 3 – Câblage du réflecteur.

$0 \leftrightarrow 24$	$1 \leftrightarrow 17$	$2 \leftrightarrow 20$	$3 \leftrightarrow 7$	$4 \leftrightarrow 16$
$5 \leftrightarrow 18$	$6 \leftrightarrow 11$	$8 \leftrightarrow 15$	$9 \leftrightarrow 23$	$10 \leftrightarrow 13$
$12 \leftrightarrow 14$	$19 \leftrightarrow 25$	$21 \leftrightarrow 22$		

FIG. 4 – Schéma du codage du mot "été".



Légende :



1. Décalage du rotor (Δ).
2. Position de la bague.
3. Position absolue avant le rotor (Pa_{in}).
4. Position relative en entrée du rotor ($Pr_{in} \equiv (Pa_{in} + \Delta)\ mod\ 26$).
5. Position relative en sortie du rotor (Pr_{out}) donnée par la Fig 2 en fonction de Pr_{in}.
6. Position absolue en sortie du rotor ($Pa_{out} \equiv (Pr_{out} + \Delta)\ mod\ 26$).
7. Position absolue en entrée du rotor lors du retour (Pa_{in}^{inv}).
8. Position relative en entrée du rotor lors du retour ($Pr_{in}^{inv} \equiv (Pa_{in}^{inv} - \Delta)\ mod\ 26$).
9. Position relative en sortie du rotor lors du retour (Pr_{out}^{inv}) donnée par les transformations inverses de la Fig 2 en fonction de Pr_{in}^{inv}.
10. Position absolue en sortie du rotor lors du retour ($Pa_{out}^{inv} \equiv (Pr_{out}^{inv} - \Delta)\ mod\ 26$).
11. Modification du décalage du rotor après le codage de la lettre.