CYB1003 – Introduction à a cybersécurité

Travail de session : sujet au choix

Travail de session : sujet I.

Objectif :

Le but de ce travail est de mieux maîtriser le fonctionnement d'un système cryptographique classique. En particulier, vous allez programmer une variante de la machine de codage Enigma que l'armée allemande a utilisé du début des années trente jusqu'à la fin de seconde guerre mondiale.

Fonctionnement de la machine :
La machine que nous voulons programmer est composée de trois rotors et d'un réflecteur (voir figure 1). Chaque rotor est modélisé par un tableau de deux lignes (1ère ligne= ligne en bas ; 2ème ligne =ligne en haut) et de 26 colonnes.

Lorsque nous tapons une lettre, les trois rotors sont parcourus de bas vers le haut jusqu'au réflecteur, puis de haut vers le bas jusqu'à trouver la lettre cryptée correspondante.

- Durant la phase d'allée (de la lettre tapée en direction du réflecteur), le chemin est calculé à partir de la première ligne de chaque rotor. Ainsi lorsque nous tapons une lettre qui a le code *i* selon l'ordre alphabétique (A=0, B=1,. . .,Z=25), elle rentre dans la colonne *i* du rotor 1. Dans ce cas, la case [1, i] (1ère ligne, *i*- ème colonne) du rotor 1, nous donne la valeur du décalage (à droite si la valeur est positive, à gauche si la valeur est négative) à faire pour trouver la colonne d'entrée du rotor 2. Par exemple, si nous avons une valeur *v* dans la case [1, *i*], cela veut dire que nous devrons entrer au rotor 2 par la colonne ($i + v$) mod 26.

  De la même manière, la colonne d'entrée du rotor 2 nous donne la colonne d'entrée du rotor 3 qui elle même va nous donner la colonne d'entrée du réflecteur. Finalement, la colonne d'entrée du réflecteur va nous donner la colonne d'entrée du rotor 3 pour la phase de retour.

- Pendant la phase de retour, nous appliquons le même principe sauf que nous nous servions de la 2ième ligne de chaque rotor pour calculer le chemin de retour.

- Par exemple, si l'utilisateur tape la lettre A (A = 0), alors elle va rentrer par la colonne 0 du premier rotor, puis par la colonne 10 du rotor 2, puis par la colonne 7 ($7 = 10 - 3 \bmod 26$) du rotor 3 ; puis la colonne 9 ($9 = 7 + 2 \bmod 26$) du réflecteur. Nous sortons du réflecteur pour rentrer par la colonne 16 ($16 = 9 + 7 \bmod 26$) dans le rotor 3, puis par la colonne 22 ($22 = 16 + 6 \bmod 26$) du rotor 2,
  puis par la colonne 13 ($13 = 22 - 9 \bmod 26$) du rotor 1 et finalement nous sortons par la colonne 19 ($19 = 13 + 6 \bmod 26$) du rotor 1 pour trouver la lettre T qui est le résultat de l'encryption de notre lettre de départ A. Ce qui est noté en rouge dans la Figure 1 indique le chemin d'allée et ce qui noté en bleu indique le chemin de retour.

Le rôle principal du réflecteur est qu'il permette d'utiliser la même machine pour encrypter et décrypter facilement. En effet, grâce à ce réflecteur, déchiffrer un message $E_k(M)$ qui a été encrytpté par une clé k revient à l'encrypter de nouveau avec la même clé. Autrement dit : $E_k(E_k(M)) = M$.

Une fois une lettre est encryptée, un des trois rotors va tourner d'un cran (décalage d'une position des deux lignes du rotor en même temps) avant de commencer l'encryption de la lettre suivante. C'est la valeur de la clé qui détermine le rotor qui doit commencer à tourner en premier et dans quelle direction c'est fait, quels seraient le deuxième et le troisième rotor à tourner et dans quelles directions. Par exemple, si la clé contient (R3,G)(R1,D) (R2,D), cela veut dire que c'est le rotor R3 qui devrait commencer à tourner le premier, et ce toujours à gauche, jusqu'à ce qu'il fasse un tour complet. Au moment où le rotor R3 revient à sa position de départ et durant cette dernière rotation, le rotor R1 tourne d'un cran à droite et il poursuit sa rotation (un cran à droite par lettre à encrypter) jusqu'à ce qu'il ai fait un tour complet. De manière similaire, au moment où le rotor R1 revient à sa position de départ, le rotor R2 tourne d'un cran à droite et il poursuit par après sa rotation (un cran à droite par lettre à encrypter) jusqu'à ce qu'il ai fait un tour complet. Une fois, le cycle terminé nous reprenons avec un nouveau cycle. Quant au réflecteur, il garde toujours sa position initiale (il ne tourne pas).

La clé nous donne également la position de départ de chaque rotor, et ce par rapport à une position de base (celle de la figure 1). Donc la clé est représentée par trois triplets qui donnent l'ordre et les sens des rotations des rotors ainsi que leurs positions initiales. Par exemple, si la valeur de la clé est (R3, G, +7) (R1, D, -6) (R2, D, +5) alors la position initiale du rotor R3 est obtenue en faisant un décalage de 7 (à droite) par rapport à la position de base donnée dans la Figure 1. La position initiale du rotor R2 est obtenue en faisant un décalage de 6 (à gauche) de celle donnée dans la Figure 1. Finalement, la position initiale du rotor R1 est obtenue en faisant un décalage de 5 (à droite) de celle donnée dans la Figure 1.

+25	+23	+21	+19	+17	+15	+13	+11	+9	+7	+5	+3	+1	-1	-3	-5	-7	-9	-11	-13	-15	-17	-19	-21	-23	-25	Réflecteur
+12	-1	+23	+10	+2	+14	+5	-5	+9	-2	-13	+10	-2	-8	+10	-6	+6	-16	+2	-1	-17	-5	-14	-9	-20	-10	
+1	+16	+5	+17	+20	+8	-2	+2	+14	+6	+2	-5	-12	-10	+9	+10	+5	-9	+1	-14	-2	-10	-6	+13	-10	-23	Rotor 3
+25	+7	+17	-3	+13	+19	+12	+3	-1	+11	+5	-5	-7	+10	-2	+1	-2	+4	-17	-8	-16	-18	-9	-1	-22	-16	
+3	+17	+22	+18	+16	+7	+5	+1	-7	+16	-3	+8	+2	+9	+2	-5	-1	-13	-12	-17	-11	-4	+1	-10	-19	-25	Rotor 2
+17	+4	+19	+21	+7	+11	+3	-5	+7	+9	-10	+9	+17	+6	-6	-2	-4	-7	-12	-5	+3	+4	-21	-16	-2	-21	
+10	+21	+5	-17	+21	-4	+12	+16	+6	-3	+7	-7	+4	+2	+5	-7	-11	-17	-9	-6	-9	-19	+2	-3	-21	-4	Rotor 1
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	

Figure 1

Description du mandat :

Implantez la machine Enigma décrite plus haut. Votre interface devrait être inspirée de celle donnée par la Figure 2. Dans la partie supérieure de cette interface, l'utilisateur voit

la configuration des trois rotors ainsi que celle de réflecteur. Dans la partie inférieure, nous trouvons les champs nécessaires pour configurer la machine et l'utiliser.

La configuration initiale de la machine est celle donnée par la Figure 1. L'utilisateur commence par choisir sa clé sous forme de trois triplets comme expliqué précédemment. Par la suite, il appuie sur le bouton « Configurer » pour que la nouvelle configuration de la machine s'affiche à l'écran.

Lors de l'encryption, l'utilisateur tape une ou plusieurs lettres dans le champ de saisie du texte à encrypter. Ensuite, il appuie sur le bouton « Encrypter » pour que le résultat de l'encryption du la première lettre s'affiche dans la zone d'affichage du texte encrypté. Après cette étape, la première partie de l'interface devrait montrer en rouge le chemin de l'allée et en bleu le chemin de retour (voir l'interface).

L'utilisateur appuie par la suite sur le bouton « Étape suivante ». Dans ce cas, la nouvelle configuration (avec un rotor qui a tourné d'un cran) de la machine s'affiche à l'écran. Puis, il faut appuyer sur le bouton "Encrypter" pour que la deuxième lettre de son texte s'encrypte et ainsi de suite.

Pour décrypter, l'utilisateur procède de la même manière que l'encryption sauf que le texte à décrypter est saisi dans la zone du texte à décrypter et le résultat du décryptage s'affiche dans la zone du texte à encrypter.

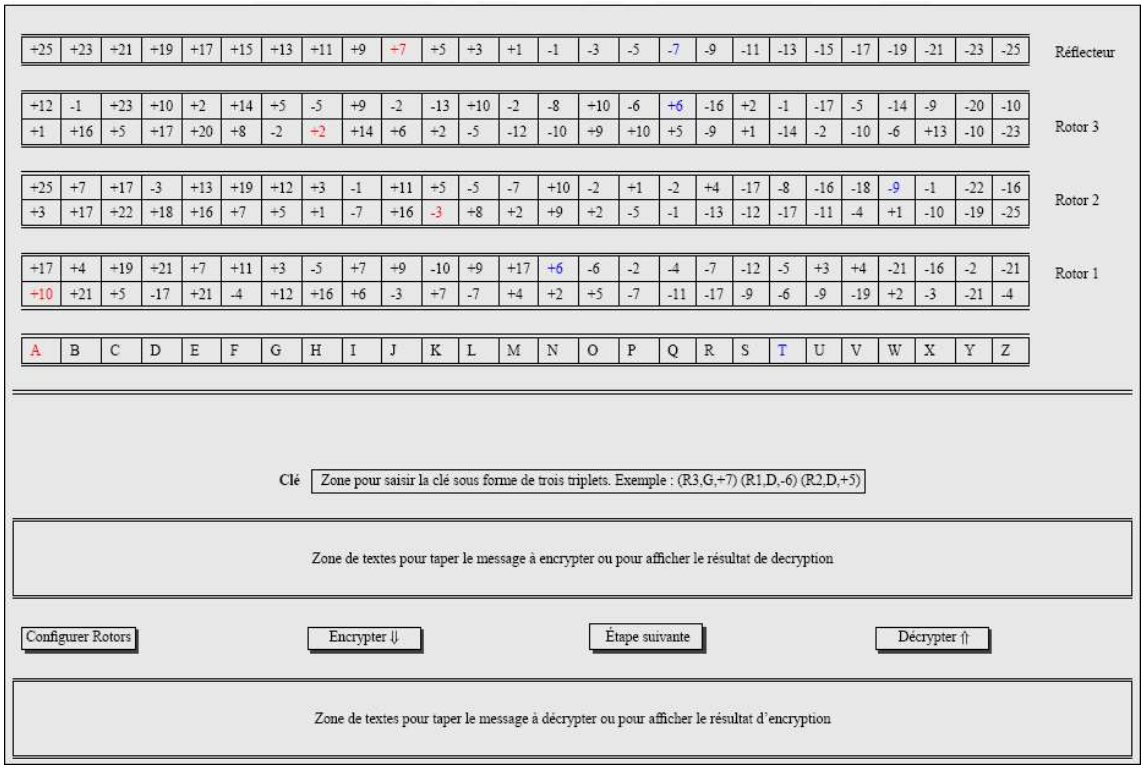

Figure 2