TD 3 : Cryptanalyse

Exercice 1

La reine d'Écosse, Mary Stuart, a utilisé un code secret par homophonie, alors qu'elle essayait d'organiser l'assassinat de la reine d'Angleterre Elisabeth Ière.

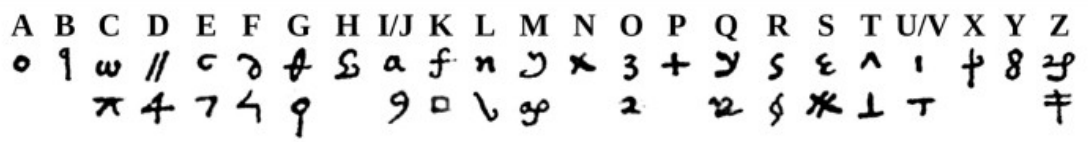

FIGURE 1 – Code homophonique de Mary Stuart reine d'Écosse au 16e siècle.

Le principe est de remplacer les lettres avec un alphabet secret, mais pour éviter les attaques par fréquence de lettres, on choisit un alphabet plus grand tel qu'une lettre peut être associée à plusieurs symboles. Par exemple, supposons que pour chaque lettre de l'alphabet on ait deux symboles. On tirera alors au sort l'un ou l'autre des symboles à chaque étape au moment du chiffrement.

1. Quelle est l'entropie de la clé de chiffrement pour ce code avec un message de longueur n ?
2. Quelle doit être la longueur minimale d'un message intercepté pour pouvoir espérer le déchiffrer sans la clé ? On rappelle que pour le chiffrement avec un alphabet simple de 26 lettres on avait estimé ce nombre à 17.
3. Pouvez-vous imaginer une meilleure stratégie de substitution avec un alphabet à 52 lettres ?

Exercice 2 (Machine Enigma)

Enigma était la machine de chiffrement de la Wehrmacht durant la deuxième guerre mondiale. Pour simplifier on peut dire que c'était une machine à écrire qui fonctionnait avec trois rotors appliquant une permutation différente l'alphabet appliquée à la suite. Après qu'une lettre soit tapée, le rotor le plus à droite tourne d'un cran, conjuguant la permutation par le cycle $(1 \dots 26)$. Si le rotor le plus a droite revient à sa position initiale il entraine le second rotor qui se décale lui aussi d'un cran. De même pour le second avec le troisième. Ainsi pour être sur de faire tourner le troisième rotor le plus à gauche, il faut taper au moins 26×26 lettres.

La clef de chiffrement est donnée par le choix des trois rotors parmi les cinq, de leur ordre de disposition, ainsi que leur position initial de rotation.

1. Quelle est l'entropie de la clé de chiffrement pour ce code avec un message de longueur n ?
2. Quelle doit être la longueur minimale d'un message intercepté pour pouvoir espérer casser le code ?

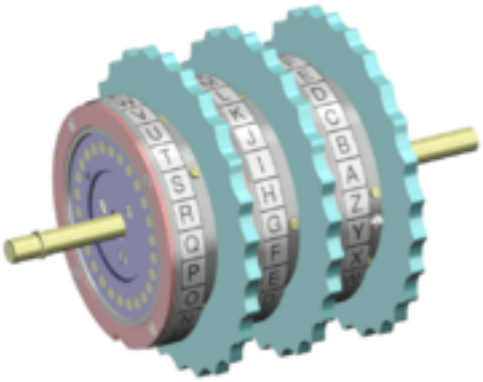

FIGURE 2 – Les trois rotors d'une machine Enigma.

Après quelques années, une sécurité a été ajoutée, rajoutant une systèmes de câblage qui permet de permuter 10 paires de lettres entre elles.

3. Répondre aux questions précédentes avec cette nouvelle information.

Pour des raisons pratiques, les ingénieurs allemands ont décidé de faire une machine symétrique, telle que si on rentre le message codé dans la machine, c'est le message initial qui s'affichera en sortie. L'inconvénient est que pour des raisons de conceptions, une lettre ne pourra alors pas être codé par elle même.

4. Calculer la quantité d'information obtenue sur le message grace à cette propriété de la machine.

Un crib est une supposition sur ce que pourrait être le texte en clair. Imaginez que les Britanniques savent qu'un Allemand très important voyage de Berlin à Aix-la-Chapelle, et ils interceptent des messages codés par Enigma envoyés à Aix-la-Chapelle. Il est fort probable qu'un ou plusieurs des messages en clair originaux contiennent la chaîne

OBERSTURMBANNFUEHRERXGRAFXHEINRICHXVONXWEIZSAECKER

avec le nom du personnage important. Un crib pourrait être utilisé dans une approche de force brute pour trouver la clé Enigma correcte (en faisant passer les messages reçus à travers toutes les machines Enigma possibles et vérifier si l'un des textes décodés correspond au texte en clair mentionné ci-dessus). Cette question se concentre sur l'idée que le crib peut également être utilisé de manière beaucoup moins coûteuse : faire glisser le crib de texte en clair le long de tous les messages codés jusqu'à ce qu'une discordance parfaite entre le crib et le message codé soit trouvée ; si c'est le cas, cela pourrait indiquer que le crib est correctement aligné.

5. Pour être certain que le crib est correctement aligné avec le texte chiffré, quelle longueur de crib serait nécessaire ?
6. De même, quelle longueur de crib serait nécessaire pour identifier avec certitude la clé correcte ?