TD 1 : Cryptographie classique

• Exercice 1: Ordre de grandeur

Le facteur de travail d'un algorithme est le nombre d'instructions élémentaires nécessaire à son execution. La puissance d'une machine est le nombre d'instructions qu'elle exécute par unite de temps. Nous allons approximer la puissance d'un PC actuel à environ 2000 Mips (millions d'instructions par seconde). Le facteur de travail d'un algorithme optimise pour tester une clé de 128 bits de l'algorithme AES est d'environ 1200 instructions élémentaires. On dispose d'un couple clair/chiffre connu et on désire retrouver la clé utilisée par force brute, c'est-a-dire en testant toutes les clés les unes après les autres. Une clé est constituée d'un mot de 128 bits. On suppose que toutes les clés sont équiprobables.

- En combien de temps une machine de 2000 Mips teste-t-elle une clé ?
- Combien y a-t-il de clés possibles ? Quel est le nombre moyen de clés à tester avant de trouver la bonne ?
- A quel temps moyen de calcul cela correspond-il si on suppose qu'un seul PC effectue la recherche ? Si les 1 milliard de PC de l'Internet sont mobilisées à cette tache ?

• Exercice 2 : chiffrement par substitution

- Coder le message "textenclair" à l'aide du chiffrement par décalage et de la clé K = 5.
- Décoder le message "RGNEIDVGPEWXTRAPHHXFJT" sachant qu'il a été créé par un chiffrement par décalage.
- Chiffrer avec le chiffre de vigenère "textenclair" avec la clé "crypto"

• Exercice 2 : Analyse de frequence

L'analyse des fréquences d'apparition des lettres dans un message codé montre que ceux sont les lettres K et O les plus fréquentes dans ce message. Dans un texte en français les lettres les plus fréquentes sont le A (8.4 %) et le E (17.26 %). Sachant que le message est en français, codé en utilisant le chiffrement par décalage sur les 26 lettres de l'alphabet, déterminer la clef et déchiffrer le début du message :
SVOXFYIKNKXCVKVSQEBSOKMRODOBNOCCYVNKDC