Sécurité informatique

***TD 1***



**Exercice 1.** (Chiffrement de Vigenère)

On désire chiffrer le texte suivant par la méthode de Vigenère.

« Les problèmes de sécurité qu’on peut rencontrer sur un réseau d'entreprise ou sur l'Internet relèvent d'abord de la responsabilité des victimes avant d'être imputables aux hackers »

Dont la clé est la suivante : « **Faille de sécurité sur internet** »

1. Donner le chiffré de ce message.
2. Proposer une méthode de chiffrement rapide
3. Un algorithme implémentable en software.
4. Dans le cas où l’information est codée sur 8 bits, Imaginer un chiffrement de Vigenère pour ce système.

**Exercice 2.** Calcul dans GF(28)

* Calculer la multiplication de 8F par 05.
* Proposer un circuit (à base de porte Xor) permettant de faire cette opération.
* Donner le nombre de portes et la latence de ce circuit.

**Exercice 3.**

On désire avoir un passwd dont la force équivaut celle d’une clé de chiffrement de 105 bits.

1. Quelle est la taille de ce passwd si on utilise 82 caractères.
2. Quelle est le temps de son craquage (si on utilise une machine qui peut craquer 1 milliard de passwds par second).