TD 2 : Cryptographie symétrique

Exercice 1) Chiffre de Vernam A quelle condition ce chiffre est-il un chiffre *parfait* ?

Exercice 2) LFSR (*Linear Feedback Shift Register*) Les LFSR sont des générateurs pseudo-aléatoires dont la sortie peut être utilisée comme clef secrète. En français ce sont les *registres à décalage linéaire*. Ils généralisent les *générateurs congruentiels* de sorte que :

$$x_n = (a_1 x_{n-1} + ... + a_k x_{n-k}) \mod 2$$

avec $x_0, ..., x_{k-1}$ donnés. On les représente sous forme polynomiale :

$$\Pi(X) = X^k - a_1 X^{k-1} - ... - a_k$$

Calculez les 10 premiers *bits aléatoires* produits par le LFSR : $\Pi = X^4 + X^3 + X^2 + 1$ sur les valeurs initiales $(0, 1, 1, 0)$.

Exercice 3) Déchiffrement de DES Montrez qu'il n'est pas nécessaire d'inverser f pour inverser un *tour* de DES. En déduire l'algorithme de déchiffrement du DES.

Exercice 4) Mots de passe UNIX

1. Quelle est la raison profonde à l'ajout de *sel* dans le calcul de l'empreinte d'un mot de passe ?
2. A quoi riment les 25 itérations de DES pour chiffrer un mot de passe ?

Exercice 5) Chiffre de Vernam Un utilisateur a chiffré 2 mots (sans accent ni cédille *etc*) de la langue française de 7 lettres avec le chiffrement de Vernam mais il a été imprudent et a utilisé 2 fois la même clef pour chiffrer ces 2 messages. Sachant que les chiffrés obtenus sont les mots `hqdtmap` et `onooiup`, faire une recherche informatique dans un *corpus* de la langue française et trouver tous les couples de textes clairs susceptibles de produire ces chiffrés.