TP : Implémentation et cryptanalyse de systèmes de chiffrement par flot

Exercice : Complexité linéaire d'un LFSR

a) Soit $P(X) = X^m \oplus c_{m-1}X^{m-1} \oplus \ldots \oplus c_0$ le polynôme caractéristique d'un LFSR. Démonter que :

$$S(X) = \bigoplus_{i \geq 0} k_i X^i = \frac{\bigoplus_{j=0}^{m-1} \bigoplus_{i=0}^{j} c_{m-j+i} k_i X^i}{X^m P\left(\frac{1}{X}\right)}.$$

b) Considérons le LFSR de longueur 10 de polynôme caractéristique $P(X) = X^{10} \oplus X^9 \oplus X^7 \oplus X^6 \oplus X^3 \oplus 1$ et d'état initial `1001001001`. Calculer le polynôme caractéristique du plus petit LFSR capable de produire la même suite chiffrante et son état initial.

Exercice : Implémentation d'un système de chiffrement par flot synchrone

Le système SC (*Stream Cipher*) est un système de chiffrement par flot conçu dans un but pédagogique (par E. Filiol). C'est un système à combinaison de registres de rétroaction comportant trois registres donnés par les polynômes de rétroaction suivants :

$$\begin{aligned} P_1(X) &= X^{17} \oplus X^{15} \oplus X^{14} \oplus X^{13} \oplus X^{11} \oplus X^{10} \oplus X^9 \oplus X^8 \oplus X^6 \oplus X^5 \oplus X^4 \oplus X^2 \oplus 1 \\ P_2(X) &= X^{19} \oplus X^{18} \oplus X^{16} \oplus X^{15} \oplus X^{11} \oplus X^{10} \oplus X^5 \oplus X^3 \oplus X^2 \oplus X \oplus 1 \\ P_3(X) &= X^{23} \oplus X^{22} \oplus X^{21} \oplus X^{20} \oplus X^{17} \oplus X^{16} \oplus X^{15} \oplus X^{12} \oplus X^{10} \oplus X^8 \oplus X^7 \oplus X \oplus 1 \end{aligned}$$

La fonction de combinaison de ces trois registres est la fonction majorité parmis trois définie par :

$$f(X_1, X_2, X_3) = X_1X_2 \oplus X_1X_3 \oplus X_2X_3.$$

Implémenter en C le système de chiffrement SC. Vérifier la conformité de votre implémentation à ses spécifications à l'aide de la suite étalon suivante (en base 16) :

Pour $R_1 =$ `3130`, $R_2 =$ `21999` et $R_3 =$ `66C6A6`,
les dix premiers octets générés par SC sont : `B0 11 62 F2 80 15 95 16 41 E5`.

Exercice : Cryptanalyse du système de chiffrement par flot synchrone SC

Cryptanalyser le système SC en appliquant l'attaque par corrélation de Siegenthaler.

Exercice : Recherche de polynômes irreductibles primitifs

Il y a huit relations de récurrence linéaire de degré quatre telles que $c_0 = 1$. Déterminer lesquelles engendrent une séquence de clés de période 15 (à partir d'un vecteur initial non nul).

Exercice : Chiffrement par flot asynchrone

On considère le système de chiffrement par flot asynchrone suivant : soit $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}_{26}$ et la suite chiffrante :

$$\begin{array}{rcll} k_i = f_i(K, x_1, \ldots, x_{i-1}) & = & K & \text{si} \quad i = 1 \\ & = & x_{i-1} & \text{si} \quad i \geq 2. \end{array}$$

Pour $0 \leq k \leq 25$, $\forall x, y \in \mathbb{Z}_{26}$, on définit :

$$\begin{array}{rcll} e_k(x) & = & x + k & \mod 26 \\ d_k(x) & = & y - k & \mod 26. \end{array}$$

Décrypter le message chiffré suivant obtenu par utilisation de ce système de chiffrement asynchrone :

`MALVVMAFBHBUQPTSOXALTGVWWRG`