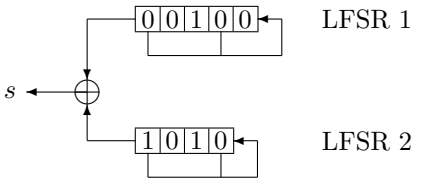
Principes et Algorithmes de Cryptographie

DS du 25 mars 2005

Durée 1 heure - documents autorisés
Toute réponse devra être justifiée

Exercice 1 : *LFSRs*

On considère une suite $s = (s_n)_{n\geq 0}$ produite par la combinaison de deux LFSRs comme indiqué ci-dessous:



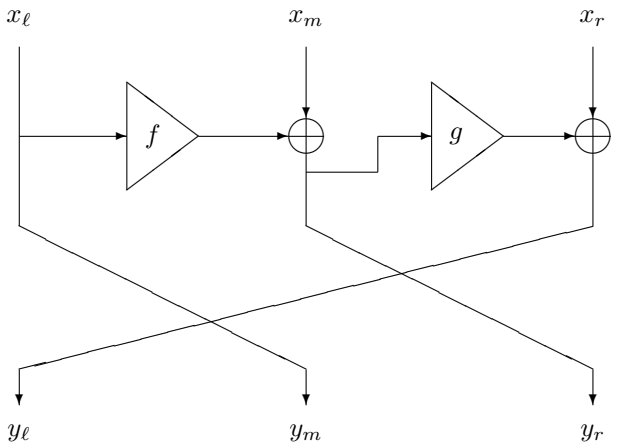
Q 1 . Quels sont les 10 premier termes de la suite s ?
Q 2 . Donnez la liste des polynômes de $\mathbb{F}_2[X]$ de degré $1, 2, 3$ et qui sont irréductibles.
Q 3 . Pour chacun des deux LFSRs :

- donnez son polynôme caractéristique ;
- dîtes s'il est irréductible, primitif ?
- donnez la longueur de la période de la suite qu'il produit.

Q 4 . Donner la longueur de la période de la suite s.
Q 5 . Donnez un algorithme pour calculer le plus petit LFSR permettant de générer s.
Q 6 . Voyez-vous un avantage à combiner ainsi deux (ou plus) LFSRs ?

Exercice 2 : *chiffrement par blocs*

On considère un système de chiffrement itératif par blocs. Un tour de chiffrement prend un bloc de 48 bits en entrée ; il est réalisé en partageant le bloc en 3 sous-blocs (x_ℓ, x_m, x_r) de 16 bits chacun selon le schéma ci-dessous:



que l'on peut également écrire

$$\begin{cases} y_\ell &= x_r + g(x_m + f(x_\ell)) \\ y_m &= x_\ell \\ y_r &= x_m + f(x_\ell) \end{cases}$$

Q 1 . Montrer que quelles que soient les fonctions f et g, ce schéma (correspondant à un tour) réalise une bijection. Faire un schéma et écrire l'équation de la fonction réciproque d'un tour.
Q 2 . Expliquer comment on peut distinguer une fonction réalisée par deux tours de ce schéma d'une fonction aléatoire.