TD 3 : One-Time-Pad et LFSR

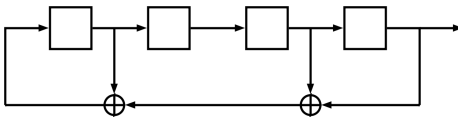
christina.boura@uvsq.fr

13 février 2018

Exercice 1 *Peut-on casser OTP avec une recherche exhaustive de la clé ?*
À première vue il semble qu'une recherche exhaustive de la clé est possible contre OTP. Supposons qu'un message court, composé par exemple de 5 caractères du code ASCII (40 bits) à été chiffré avec OTP. Expliquer pourquoi une recherche exhaustive de la clé ne réussira pas malgré le fait que nous avons les ressources de calcul nécessaires.

Exercice 2 *Calculer la suite chiffrante produite par un LFSR*
Calculer les deux premiers octets de la suite générée par le LFSR de degré $m = 8$, ayant comme coefficients de retroaction $(c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7) = (1, 1, 0, 1, 1, 0, 0, 0)$ et initialisé par `0xff`.

Exercice 3 *Calculer la période d'un LFSR*
On considère le LFSR suivant



1. Calculer les premiers bits de la suite chiffrante produite avec ce LFSR ayant comme vecteur d'initialisation $(s_0, s_1, s_2, s_3) = (0, 1, 1, 0)$.
2. Quelle est la période de cette suite ? S'agit t'il de la période maximale pour un LFSR de degré $m = 4$?
3. Dessiner un LFSR de degré $m = 3$ qui produit la même suite chiffrante.

Exercice 4 *Attaque à clair connu contre un LFSR*
On mène une attaque à clair connu contre un chiffrement à flot dont la suite chiffrante a été produite par un seul LFSR de période maximale. On suppose connaître le message clair

```
1001 0010 0110 1101 1001 0010 0110
```

ainsi que le message chiffré

```
1011 1100 0011 0001 0010 1011 0001
```

1. Quel est le degré (taille du registre) m du LFSR ?
2. Quel est le vecteur d'initialisation ?
3. Déterminer les coefficients de retroaction du LFSR.
4. Dessiner ce LFSR.

Exercice 5 *Déchiffrer un message généré avec par un chiffrement à flot basé sur un LFSR*
Un LFSR a engendré la suite périodique de période 15

$$s = (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, \dots)$$

1. Montrer que le degré d'un tel LFSR est supérieur ou égal à 4.
2. Montrer qu'il existe un unique LFSR de longueur 4 engendrant s et le déterminer.

3. On a utilisé ce LFSR pour générer une suite chiffrante pour être utilisée dans un chiffrement à flot. L'initialisation n'est pas la même que celle utilisée pour engendrer s. Les vingt-six lettres a,..., z, sont codées de 0 à 25 dans l'ordre alphabétique ; de plus, chaque entier de 0 à 25 est représenté par son écriture binaire sur cinq bits. Par exemple, a = 0 = `00000`, d= 3 = `00011`. Un message de quatorze lettres a été chiffré. Le message chiffré est

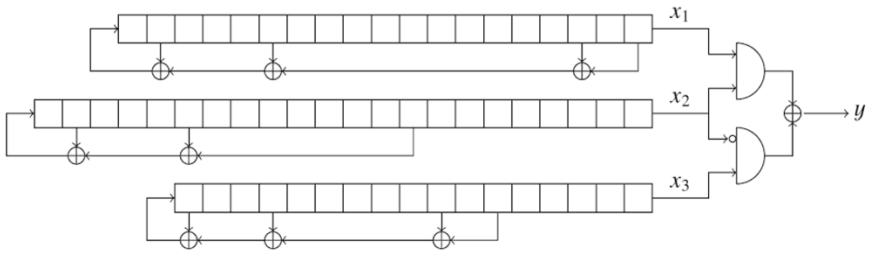
   `11011011001011111101000001000111010100111111001111001101001011100000000.`

   Le déchiffrer.

Exercice 6 *Attaque par correlation contre le générateur de Geffe*
Le générateur de Geffe est un générateur des nombres pseudo-aléatoires, conçu par P. Geffe en 1973 pour le chiffrement à flot. Il emploie trois LFSR de tailles différentes. La clé secrète est constituée par l'ensemble des initialisations des trois registres et sa taille est égale à la somme des tailles (degrés) des ceux-ci. À chaque coup d'horloge, les bits de sortie des trois registres sont combinés de façon non-linéaire afin de produire un bit de la suite chiffrante. Plus précisément, un bit y de la suite chiffrante est calculé de la manière suivante :

$$y = x_1x_2 \oplus (1 + x_2)x_3,$$

où x_1 est le bit de sortie du premier registre, x_2 est le bit de sortie du deuxième registre et x_3 est le bit de sortie du troisième registre.



Le but de cet exercice est de montrer que le générateur de Geffe n'est pas cryptographiquement sûr. En effet, nous allons montrer que la clé secrète peut être retrouvée plus rapidement qu'avec une recherche exhaustive. Pour cela, nous allons considérer le générateur de Geffe composé des trois registres de taille respectives 19, 22 et 17, comme on peut le voir sur l'image.

1. Si un attaquant souhaite retrouver la clé secrète du générateur, combien de clés doit-il examiner dans le pire des cas ?
2. Calculer pour chacune des valeurs (x_1, x_2, x_3) des trois bits de sortie, le bit de sortie y du générateur. La sortie du générateur, est-elle équilibrée ?
3. Y-a-t-il une correlation entre la sortie du générateur y et la sortie x_1 du premier registre ? Même question pour le deuxième et le troisième registre.
4. Expliquer comment un attaquant peut exploiter l'information ci-dessus pour deviner le contenu du premier et du troisième registre. Quelle est la complexité en temps de cette attaque ?

Exercice 7 *Attaque* deviner et déterminer *sur le générateur de Geffe*

Considérons trois registres à décalage à retroaction linéaire (LFSR) R_1, R_2, R_3 de longueur ℓ_1, ℓ_2 et ℓ_3 (respectivement) et le générateur de Geffe associé.

1. Donner l'expression formelle de la sortie du générateur y en fonction de la valeur de sortie x_2 du générateur R_2.
2. On suppose que l'attaquant connaît le contenu du registre R_2. Montrer comment l'attaquant peut exploiter cette information afin de retrouver le contenu des deux autres registres R_1 et R_3.
3. En déduire une attaque contre le générateur de Geffe de complexité de l'ordre de $2^{\ell_2}(\ell_1^3 + \ell_3^3)$.
4. Donner la complexité de cette attaque contre le générateur de Geffe de l'exercice précédent et la comparer avec la complexité de la recherche exhaustive de la clé pour le même générateur.