Master CSI 2 2013-2014

Cryptanalyse — M1MA9W06
Responsable : G. Castagnos

TP 4 — Cryptanalyse du générateur de Geffe

1 Le générateur de Geffe combine les trois LFSR suivants avec la fonction booléenne $x_1x_2 + x_2x_3 + x_3$,

- LFSR1 de longueur 13 de polynôme de rétroaction $x^{13} + x^4 + x^3 + x + 1$;
- LFSR2 de longueur 11 de polynôme de rétroaction $x^{11} + x^2 + 1$;
- LFSR3 de longueur 9 de polynôme de rétroaction $x^9 + x^4 + 1$.

Écrire une fonction qui simule le générateur de Geffe. Elle doit prendre en entrée le nombre de bits à produire et les trois clefs utilisées K1, K2, K3 correspondant aux états initiaux des trois LFSR. Pour tester votre fonction, avec les clefs

$$K_1 = [1,0,1,0,1,0,1,0,1,0,1,0,1], K_2 = [1,0,1,0,1,0,1,0,1,0,1], K_3 = [1,0,1,0,1,0,1,0,1]$$

les 10 premiers bits de sortie du générateur sont

$$1,0,1,0,1,0,1,0,1,1$$

2 Vous avez intercepté la suite de bits, s :

$$0,0,1,0,1,0,0,1,0,0,0,1,1,1,1,1,0,1,0,1,0,1,0,0,0,1,$$
$$1,1,0,0,0,1,1,0,0,0,0,1,1,1,1,1,1,0,1,0,0,1,1,1,0,1,0,$$
$$0,1,1,0,1,1,1,1,1,1,1,0,1,0,0,1,0,1,1,1,0,0,0,0,0,0,0,$$
$$1,0,0,0,0,1,0,0,0,0,1,0,0,0,1,1,0,1,1,0$$

produite par le générateur de Geffe, disponible dans le fichier `http://www.math.u-bordeaux1.fr/~gcastagn/Cryptanalyse/tp4-suiteGeffe.sage`.

Retrouvez les initialisations des trois LFSR qui ont engendré cette suite à l'aide d'une **attaque par corrélation**. Pour cela faire une recherche exhaustive sur le registre du LFSR3 en comparant la sortie produite avec la suite s. Faire de même avec le LFSR1, puis finir par une recherche exhaustive sur la clef K2.

3 Calculez la complexité linéaire d'une suite pseudo aléatoire produite par ce générateur, en utilisant l'algorithme de Berlekamp Massey et vérifier qu'on trouve bien la formule du cours. Combien de bits de la suite doit on connaître pour réaliser une attaque avec Berlekamp Massey ? Laquelle des deux attaques est la plus efficace ?