HARGAS ALI 22104524
EL MOUSSAFER SOUFIANE 21915493

DM Attaque contre le chiffrement à flot CSS

Question 4 :

Soit LFSR17 le LFSR de 17 bits et LFSR25 le second de 25 bits avec x1, x2 et x3 les 3 premiers octets du LFRS17, y1, y2, y3 les 3 premiers octets du LFSR25 et z1, z2, z3 les 3 premiers octets du flux généré par la fonction CSS.

On sait que z1 = (x1 +y1 + c) %256 avec c = 0 au premier tour de boucle, on obtient donc
y1 = (z1 - x1 – c) %256.

Concernant x2, y2 et z2, nous devons d'abord vérifier si c = 0 ou c = 1.
Pour cela, on vérifie x1 + y1 > 255, si c'est le cas c = 1 sinon c = 0 et donc
y2 = (z2 – x2 – c) %256

On réitère l'opération pour obtenir y3 :
Si x2 + y2 > 255, c = 1 sinon c = 0 donc y3 = (z3 – x3 – c) %256.

On sait que l'état initial s2 est composé de 24 bits, y1 représente les 8 premiers bits de s2, y2 les 8 prochains bits et y3 les 8 prochains bits et donc pour former s2, nous concaténons les 3 octets y3, y2 et y1.

Question 5 :

Nous devons démontrer une attaque qui permet de retrouver l'initialisation des générateurs de nombres pseudo-aléatoires utilisés dans le système de chiffrement CSS. Ces générateurs sont basés sur un LFSR de 17 bits ainsi qu'un autre de 25 bits.

Attaque par Force Brute :
On génère tous les états initiaux possibles de s1, il y a 2^{16} possibilités.
On simule ensuite le LFSR17 avec l'état [1]+s1 pour produire les trois premiers octets de sortie x1,x2 et x3 puis on utilise les octets de sortie connus z1,z2,...,z6 du générateur et les valeurs calculées x1, x2 et x3 pour estimer les sorties du LFSR25 y1, y2, y3 avec la formule :
y1 = z1 - x1 - c avec c = 0, ensuite yi = zi - xi - c %256 avec c = 1 si xi + yi > 255 sinon c = 0.

On génère 6 nouveaux octets avec le LFSR25 d'entrée s2 = [1] + concaténation de y1, y2, y3, et le LFSR17 d'entrée [1] + s1 puis on compare un par un les 6 nouveaux octets générés avec z1, z2,…, z6. On réitère le processus pour les 2^{16} possibilités de s1.