Projet Cryptographie
RAMASSAMY Luc

Question 4 :

Soient y_1 y_2 y_3 les 3 premiers octets sortis du second LFSR, on a $s_2 = \{1 \,||\, y_3 \,||\, y_2 \,||\, y_1\}$
On peut donc obtenir l'état intial s_2 du second LFSR de la manière suivante
$y_i = z_i - x_i - c_i \,\%\, 256$
avec c1 = 0 et $c_{i+1} = 1$ si $y_i + x_i > 255$

Question 5 :

Si l'on connaît les 6 premiers octets z_1 à z_6 on peut alors pour chaque état initial possible du LFSR de longueur 17, reécupérer dans un premier x_1 à x_3 puis calculer les y_1 à y_3 correspondant nous ce correspond à l'état initial du LFSR de longueur 25, nous permettant x_4 à X_6 et y_4 à y_6, on peut alors calculer les z_4 à z_6 correspondant et les comparer aux z originaux et si il y a correspondance, on a alors trouvé les initialisations de chaque LFSR composant le CSS et donc la clé secrète de ce dernier.