SECURITE INFORMATIQUE - Fiche TD N°2 Stream Cipher

Exercice 01 - Cryptographie moderne

1- Quelles sont les limites de la cryptographie classiques ?
Expose les proprites statistiques

2- A quoi consiste le principe de shannon ?
Diffusion : cacher les PS
Confusion : cacher la relation entre la clé et les messages cryptés

3- Quelles sont les differences entre crypto symmetrique et asymmetrique ?
Sym : meme clés pour e(x) & d(x)
Asym : des clés differentes

4- Quelles sont les differences entre crypto par bloc et flot ?
Bloc : clé de taille fixe
Flot : clé de taille variable (on parle plutôt d'un generateur de clé)

5- Pour chiffrement par flot, Dans quelle condition peut-on avoir une securité parfaite ?
Si le generateur est 100% purement aleatoire.

6- Quelles sont les proprietes de la fonction XOR qui la transforment à une fonction de cryptage par exellence.
Permet de trouver x a partir de son image (inverse d'elle meme) et en connaissant pas la clé, on a 50% pour deviner la valeur du bit clair (x 0 ou 1), la probabilité de trouver la bonne clé d'un message crypté de 64bits est $1/(2^{64}) \sim 0$ (presque 0).

Exercice 02 – Cryptographie par flux SC RC4

1- Decrypter le resultat trouver dans l'exemple du cours sur RC4.
Refaire l'exemple du cours avec K [6 3 2 1] et PT [2 2 2 1]

1- Initialisation de S

S = [0, 1, 2, 3, 4, 5, 6, 7] T = [6, 3, 2, 1, 6, 3, 2, 1]

I	j	S			
0	6	[6, 1, 2, 3, 4, 5, 0, 7]	1	2	[6, 2, 1, 3, 4, 5, 0, 7]
2	5	[6, 2, 5, 3, 4, 1, 0, 7]	3	1	[6, 3, 5, 2, 4, 1, 0, 7]
4	3	[6, 3, 5, 4, 2, 1, 0, 7]	5	7	[6, 3, 5, 4, 2, 7, 0, 1]
6	1	[6, 0, 5, 4, 2, 7, 3, 1]	7	3	[6, 0, 5, 1, 2, 7, 3, 4]

S = [6, 0, 5, 1, 2, 7, 3, 4]

2- Generer la clé et crypter le message

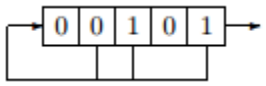
I	j	S	P	K	X	Y
0	6	[3, 0, 5, 1, 2, 7, 6, 4]	1	0-000	2-010	2-010
1	6	[3, 6, 5, 1, 2, 7, 1, 4]	7	4-100	2-010	6-110
2	3	[3, 6, 1, 5, 2, 7, 1, 4]	6	1-001	2-010	3-011
3	0	[5, 6, 1, 3, 2, 7, 1, 4]	0	5-101	1-001	4-100

Le message crypté est CT [2, 6, 3, 4]

Exercice 03 - SC LFSR

Soit l'alphabet E={A..Z} ou chaque symbol est codé sur k bits et mot est obtenu en concatenant les bits de ses caracteres. On considere un SC ou la generation de la clé est assurée par le LFSR suivant :

1- Trouver la la valeur minimale de k pour coder E
   Le k min doit verifier $2^{k-1} <|E|<= 2^k$ donc k <= log2(|E|) pour |E|=26 on a k = 5
2- Coder la chaine C_0 = 'ST'
   On a le code(S)=18, code(T)=19, code(C0) =1001010011



3- Generer la clé de cryptage correspondante à C_0

C	$s_4 s_3 s_2 s_1 s_0$	Out ($s_{i+5} = s_{i+3} + s_{i+2}+1$)					
1	0 0 1 0 1	1	s0	2	0 0 0 1 0	0	s1
3	0 0 0 0 1	1	s2	4	1 0 0 0 0	0	s3
5	0 1 0 0 0	0	s4	6	1 0 1 0 0	0	s5
7	1 1 0 1 0	0	s6	8	1 1 1 0 1	1	s7
9	1 1 1 1 0	0	s8	10	0 1 1 1 1	1	s9
11	1 0 1 1 1	1	s10	12	0 1 0 1 1	1	s11
13	0 0 1 0 1	1	s12*				

   K = 10100001011111010000101111101000010111 1….

4- Crypter la chaine C_0
   C0 + K = 1001010011 + 1010000101 = 0011010010 = 6 18 = 'GS'
5- Quelle est la periode de LFSR
   On remarque que la sequence initiale reapparait au 13ieme iteration donc p=13
6- Donner son polynome caracteristique
   $P(x) = x^5 + x^3 + x^2 + 1$
7- Trouver un autre LFSR equivalent au LFSR de l'exercice ?
   LFSR de p case initialiser avec la sequence periode 1010000101111 sans retroaction sauf pour la derniere case.

Exercice 04 - SC LFSR

Donnez les suites binaires produites par LFSR de longueur 4, en fonction des états initiaux du registre et quelles sont leurs periodes pour chaque polynome de rétroaction P(x) suivant :

1- $1 + x + x^2 + x^4$. $1 + x + x^2 + x^3 + x^4$. $1 + x^3 + x^4$.

Exercice 05 - SC LFSR

Expliquer pourquoi les suites binaires produites par les LFSR sont periodiques à apartir de certain rang.

Quelle est la plus grande periode d'une suite produite par un LFSR de longueur L ?

Parceque LFSR est deterministe et sa taille est finie alors l'ensemble de ses etats est fini à certain moments (apres k transition) il va revenir (repeter) à un etat déjà produit (E0) et à ce moment la il va produire la meme sequence comme celle generée apres E0 apres p transition.

Le p qui la valeur max pour un LFSR de longueur h est $p=2^h-1$ (sauf config tous nul)

Exercice 06 - SC LFSR Composition

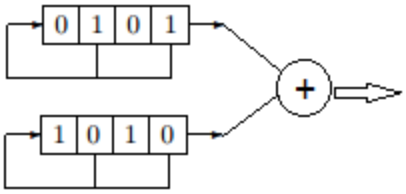
On veut etudier la compostion de deux LFSRs (CR). De meme taille et structure.

1- Est-ce que la composition CR est un LFSR pourquoi?
   Non pas decalage global.
2- Quelle condition sur les sequences d'initialisation pour CR valide

Doivent etre differentes sinon on va generer une suite de 0s.

3- Trouver LFSR equivalent au CR (qui donne la meme sequence de sortie) pour la figure donnée.
LFSR est de meme periode p=7 et meme structure et sequence init 1111 xor des deux sequences initiales

4- En general, comment peut on determiner LSFR-equivalent au CR?
On chercher la periode commune entre les deux LFSR et puis on construit notre LFSR equivalent.



C	s_3 s_2 s_1 s_0	Out ($s_{i+4}=s_{i+2}+1$)		r_3 r_2 r_1 r_0	Out ($r_{i+4}=r_{i+2}+1$)		ci si+ri
1	0 1 0 1	1	s0	1 0 1 0	0	r0	1
2	0 0 1 0	0	s1	0 1 0 1	1	r1	1
3	0 0 0 1	1	s2	0 0 1 0	0	r2	1
4	1 0 0 0	0	s3	0 0 0 1	1	r3	1
5	0 1 0 0	0	s4	1 0 0 0	0	r4	0
6	1 0 1 0	0	s5	0 1 0 0	0	r5	0
7	0 1 0 1	1	s6*	1 0 1 0*	0	r6	1

C	c_3 c_2 c_1 c_0	Out ($c_{i+4}=c_{i+2}+1$)					
1	1 1 1 1	1	c0	2	0 1 1 1	1	c1
3	0 0 1 1	1	c2	4	1 0 0 1	1	c3
5	1 1 0 0	0	c4	6	1 1 1 0	0	c5
7	1 1 1 1	1	c6*				

Exercice 07 - SC RC4

On considere une variante simplifiée de RC4 ou l'operation d'echange S[i] <->S[j] est omise.

a- Montrer que la suite chiffrante est periodique et de periode 512

b- En deduire un moyen pour reconstruire le permutation S à partir de z_k

Algorithm 1: RC4

Data: Permutation S de $\{0,\dots,255\}$ et entier $n > 0$
Result: $(z_1,\dots,z_n) \in \{0,\dots,255\}^n$

$i, j \leftarrow 0$;
for *k from 1 to n* **do**
  $i \leftarrow (i+1) \bmod 256$;
  $j \leftarrow (j+S[i]) \bmod 256$;
  $S[i] \leftrightarrow S[j]$;
  $z_k \leftarrow S[(S[i]+S[j]) \bmod 256]$;
end
return $z_1,\dots,z_n$