INFO3 Polytech Marseille

TD 2 de cryptographie

Chiffrement

On considère un système de chiffrement E tel qu'il existe un algorithme efficace A défini par :
à partir de n'importe quel chiffré de longueur n>5, A retourne le 5ème bit du clair.
E a-t-il une sécurité parfaite ?
E est-il sémantiquement sûr ?

PRG

On considère un PRG appelé G.
Soit k un germe, G(k) rend une séquence de longueur n paire avec autant de 0 que de 1 (#0 = #1).
G est-il sûr ?
Un test peut-il casser G ? avec quel avantage ?

LFSR

0) Afin de vérifier que vous ne vous trompez pas de sens lorsque vous déterminez une séquence à partir d'un polynôme : un LFSR avec registre 100 et polynôme de rétroaction x^3+x+1 donne la séquence 1001110. Ici, on a S0=1, S1=0, S2=0. Calculez les Si en utilisant la formule de récurrence du cours et dans un deuxième temps, dessinez le registre et la fonction linéaire et déterminez les Si en faisant tourner le registre.

1) Donnez les séquences binaires produites par le LFSR de longueur 4 et de polynôme de rétroaction P(x)=x^4+x^3+x^2+x+1. Même question avec P(x)=x^4+x+1.

2) Expliquez pourquoi les séquences binaires produites par des LFSR sont périodiques à partir d'un certain rang. Si un LFSR est de longueur m, quel est la longueur maximum de la période ? La séquence produite par le LFSR de la question 1) avec P(x)=x^4+x+1 pourrait-elle être produite par un LFSR plus court ?

3) Combinaison de LFSR.
Considérons deux LFSRs dont les sorties sont combinées par un ou-exclusif pour produire une suite binaire. Le premier a pour polynôme de rétroaction p1=x^3+x+1 et le deuxième p2=x^4+x+1. Quelle est la longueur de la séquence (période) générée ? Existe-t-il un intérêt à composer plusieurs LFSR ?

4) Quel est le LFSR le plus petit qui produit la suite binaire périodique de période 1010011 ?

5) On considère des messages écrits avec les 32 symboles suivants, chacun étant codé par un mot de 5 bits :

A	00000	*G*	00110	*M*	01100	*S*	10010	*Y*	11000	?	11110
B	00001	*H*	00111	*N*	01101	*T*	10011	*Z*	11001	!	11111
C	00010	*I*	01000	*O*	01110	*U*	10100	.	11010		
D	00011	*J*	01001	*P*	01111	*V*	10101	–	11011		
E	00100	*K*	01010	*Q*	10000	*W*	10110	,	11100		
F	00101	*L*	01011	*R*	10001	*X*	10111	:	11101		

Considérons le registre de polynôme de rétroaction f(x)=x^5+x^2+1. La séquence produite par ce LFSR sert à chiffrer des messages. James Bond envoie à Moneypenny et Q le nom d'une personne (dont la 2ème lettre est un « a ») susceptible de l'aider à détruire Spectre. Il envoie le chiffré suivant :

z-ayrmcqvm-eid

Arriverez-vous à retrouver l'état initial du registre et en déduire le nom de la personne ?