Cryptographie : Exercices

MOHAMED MEJRI

Groupe LSFM

Département d'Informatique et de Génie Logiciel

Université LAVAL

Québec, Canada

Exercice 1

Trouver le message m tel que :

- $e(m)$=RO VU XT QX DS YX HU DP JQ XH SQ XR HO FW VH TW HX XO GQ VH HG AX VH PW OD GD AH,
- $e = e_2 \circ e_1$,
- $e_1(x) = x + 3 \; mod \; 26$, et
- e_2= permutation 2 1.

Exercice 2

1. En utilisant un système de chiffrement affine ($mod\ 26$), l'encryption du message $HAHAHA$ a donné $NONONO$.
   – Trouver la fonction de cryptage et celle de décryptage.
2. Supposons que vous avez intercepté N messages (N assez grand) $M_1, \ldots, M_n$ encryptés avec un chiffrement de Vigenère en utilisant la même clé. Sachant que le langage d'origine des messages est l'anglais, décrire comment peut-on retrouver la clé.

3. Le message GEZXDS est le résultat de l'encryption du mot $SOLVED$ en utilisant un chiffrement de Hill avec une matrice 2×2 (clé).
   – Trouver la valeur de la clé.

Exercice 3

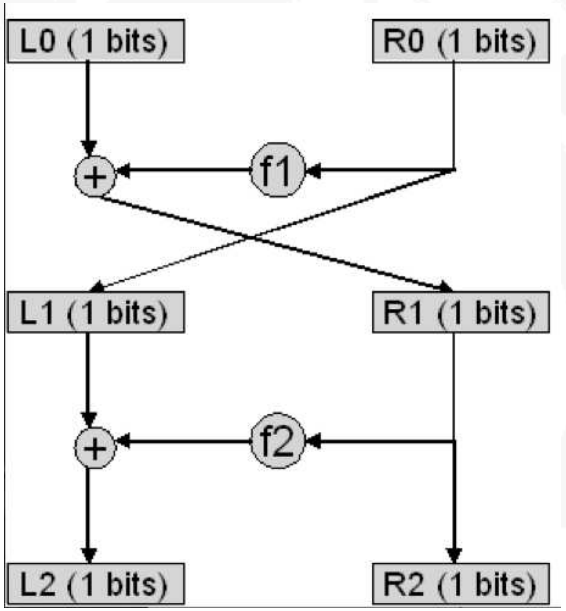
Supposons que l'encryption du message "LIFEI SNOTA DRESS REHEA RSAL" en utilisant un chiffrement de Vigenere a donné le message "EZZXP LEIMH WIYLZ KVBXH KJUE".

1. Trouver la taille de la clé (sans calculer la clé). Justifier.
2. Trouver la valeur de la clé.
3. Décrypter le message "UVUNA RZMHU EPNAL IIIFP LVIYO TGJBU XJM" en utilisant le système de Vigenere précédent.

Exercice 4

Soit E la fonction d'encryption définie par le réseau de Feistel suivant :

f_1			f_2		
0	$\rightarrow$	0	0	$\rightarrow$	1
1	$\rightarrow$	0	1	$\rightarrow$	1



– Encrypter le message $M = 1011$ en utilisant E et le mode CBC avec $c_0 = 10$.

Exercice 5

Nous considérons un réseau de Feistel à n itérations où la taille de la clé est égale à la taille de la moitié d'un bloc et la fonction f est définie de la manière suivante $f(K;R) = K \oplus R$. Analyser la sécurité de ce réseau contre les attaques à textes chiffrés et les attaques à textes claires pour chacun des cas suivants :

- $n = 2$
- $n = 3$
- n est quelconque.

Exercice 6

Encrypter le message suivant m=101 100 010 100 1010 en utilisant les modes CBC avec $c_0 = 1010$, CTR avec IV = 0010, CFB avec $r = 3$ et $IV = 1010$ et OFB avec $r = 3$ et $IV = 1010$. Nous supposons par ailleurs que le système cryptographique utilisé est une permutation E_π avec $\pi = 2341$.

Exercice 7

Compléter les tableaux suivants en utilisant AES :

round number	start of round	after subbytes	after shiftrows	after mixcolumns		round key value									
3	aa 61 82 68	ac ef 13 45	ac ef 13 45	75 20 53 bb	⊕	3d 47 1e 6d	=	48 67 4d d6							
	8f dd d2 32	73 c1 b5 23	c1 b5 23 73	ec 0b c0 25		80 16 23 7a		6c 1d e3 5f							
	5f e3 4a 46														
	03 ef d2 9a	7b df b5 b8	b8 7b df b5	93 33 7c dc		7d 3e 44 3b		ee 0d 38 e7							

sachant que la clé de l'itération 2 est :

f2	7a	59	73
c2	96	35	59
95	b9	80	f6
f2	43	7a	7f

Exercice 8

1. Supposons que nous utilisons l'algorithme de Shamir de partage de secrets. Étant donnés un seuil $(3, 4)$ et un secret s dans $\mathbf{Z}_p$ avec $p = 127$. Les trois utilisateurs suivants se sont réunis pour retrouver le secret s :

   A : (1, 64),

   B : (2, 10),

   C : (7, 97).

   Trouver l'interprétation polynomiale de Lagrange ainsi que le secret s.

2. Un village de 9 familles (de 2 à 6 personnes chaque) et un maire veut que chaque décision importante soit approuvée par au moins un membre adulte de chaque famille ainsi que le maire. Décrire, sans faire de calculs, comment se servir d'un algorithme de partage de secrets pour atteindre cet objectif.

3. Reprendre la question précédente en exigeant qu'au moins 4 représentants de familles différentes et le maire soient présents.