Université de Nice-Sophia Antipolis
M2 IFI, parcours CSSR
Cryptographie & Sécurité 2010–2011

Examen de octobre 2010

Durée : 1h

Note :

Nom :
Prénom :

L'examen comporte plusieurs parties indépendantes. Répondez sur la copie avec clarté et concision.

1 Chiffre de Feistel

On considère un chiffre de Feistel à deux tours comme décrit dans la figure 1.

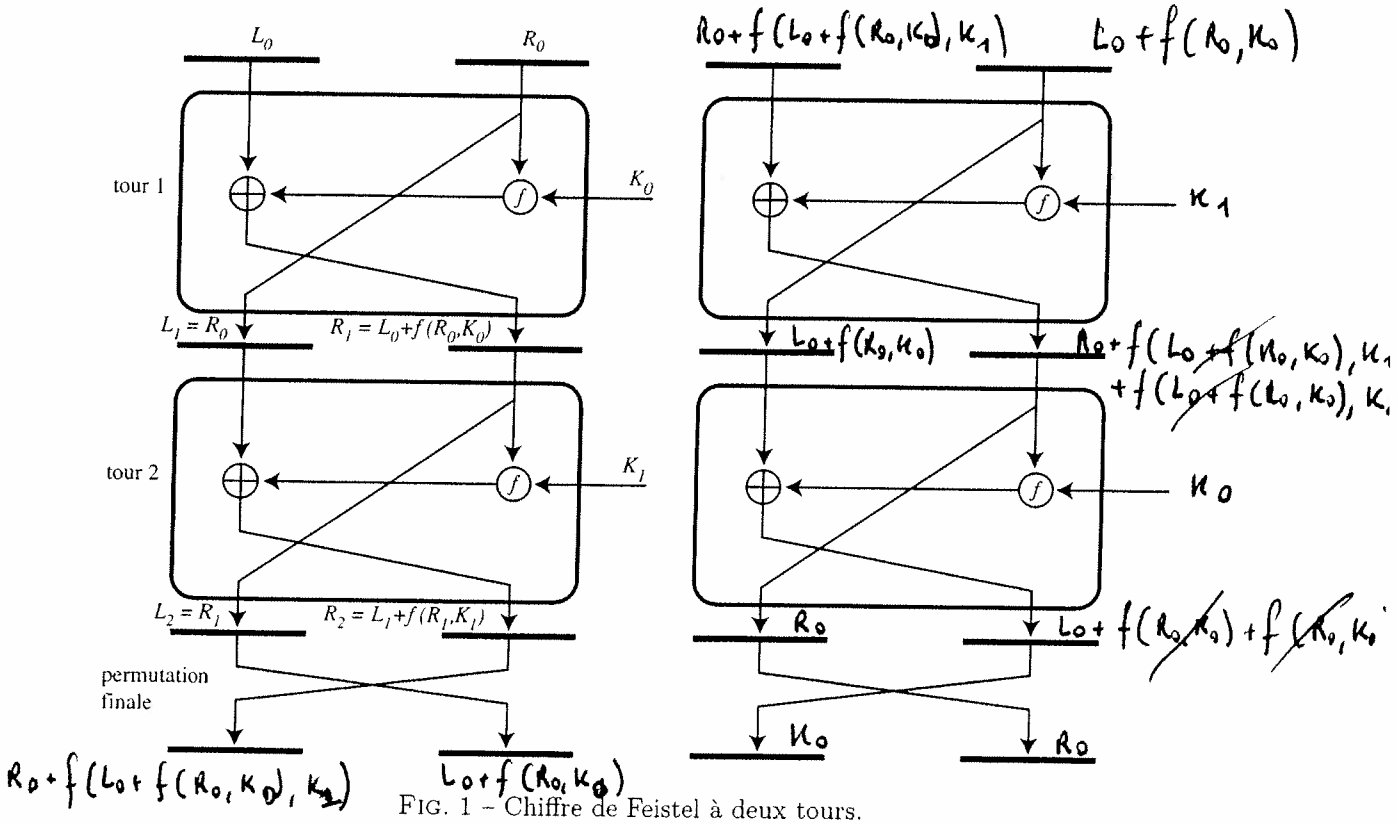

FIG. 1 – Chiffre de Feistel à deux tours.

1. Montrez que le même algorithme permet bien de déchiffrer en inversant l'ordre d'utilisation des clés de tour dans un chiffre de Feistel. (Répondez directement sur la partie droite de la figure et détaillez le cas échéant vos calculs ci-dessous).

$L_2 = L_0 + f(R_0, K_0)$

$R_2 = R_0 + f(L_0 + f(R_0, K_0), K_1)$

2 Cryptanalyse différentielle

On définit une boîte S sur des mots binaires de longueur 3 au moyen de la substitution sur des entiers modulo 8 : $x \mapsto x + 2 \mod 8$.

1. Décrivez la boîte S en base 8 et en binaire (avec le bit de poids fort à gauche MSB à gauche) :

bin	oct	bin	oct
000	0	010	2
001	1	011	3
010	2	100	4
011	3	101	5
100	4	110	6
101	5	111	7
110	6	000	0
111	7	001	1

2. Cherchez les valeurs de ΔY pour un ΔX fixé à la valeur octale de 3 (011 en binaire) :

X	Y	X'	Y'	ΔY
000	010	011	101	111
001	011	010	100	111
010	100	001	011	111
011	101	000	010	111
100	110	111	001	111
101	111	110	000	111
110	000	101	111	111
111	001	100	110	111

Listez celles qui apparaîssent le plus fréquemment en donnant les probabilités associées :

$Pr[\Delta Y = 111 / \Delta X = 011] = 1$

3. Quelle serait la probabilité d'apparition de chaque ΔY si la boîte S était parfaite ?

1/8

4. On utilise cette boîte S directement pour chiffrer en mode OFB. Calculez la suite des z_i en choisissant 000 comme IV pour $i = 1, 2, 3$.

$000 \xrightarrow{S} 010 \xrightarrow{S} 100 \rightarrow 110 = 000\,010\,100\,110$

$z_0 \qquad z_1 \qquad z_2 \qquad z_3$

5. Utilisez la suite des z_i précédente pour le chiffrement OFB du clair : 10011 01110 01

P = 100 110 111 001

K = 000 010 100 110

C = 100 100 001 000

011 111

3 Boîte S définie algébriquement

1. Terminez la constructionde la table de multiplication du corps à 8 éléments obtenu par la relation $\mathbb{F}_2[x]/(x^3+x+1)\mathbb{F}_2[x]$:

$x^3 = x+1$

$x^4 = x^2+x$

	0	1	x	x^2	$x+1$	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	x^2	$x+1$	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	$x+1$	x^2+x	1	x^2+x+1	x^2+1
x^2	0	x^2	$x+1$	x^2+x	x^2+x+1	x	x^2+1	1
$x+1$	0	$x+1$	x^2+x	x^2+x+1	x^2+1	x^2	1	x
x^2+1	0	x^2+1	1	x	x^2	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	x^2+1	1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	1	x	x^2+x	x^2	$x+1$

Détaillez vos calculs ci-dessous :

$(x^2+x+1)(x+1) = x^3+x^2+x+x^2+x+1 = x+1+1 = x$

$(x^2+x)(x^2+1) = x^4+x^3+x^2+x+x+1 = x+1$

$(x^2+x+1)(x^2+1) = x^4+x^3+x^2+x^2+x+1+x^2+1 = x^2+x$

$(x^2+x)(x^2+x) = x^4+x^2 = x$

$(x^2+x+1)(x^2+x) = x^4+x^3+x^2+x^3+x^2+x = x^2$

$(x^2+x+1)(x^2+x+1) = x^4+x^2+1 = x^2+x+x^2+1 = x+1$

2. Déduisez-en la table des inverses dans $\mathbb{F}_8$:

0	
1	1
x	x^2+1
x^2	x^2+x+1
$x+1$	x^2+x
x^2+1	x
x^2+x	$x+1$
x^2+x+1	x^2

en précisant comment vous avez obtenu ce résultat :

On cherche le polynôme qui a un produit égal à 1 dans la table de multiplication.

3. Sauriez-vous terminer la construction d'une boîte S *à la* AES avec ces paramètres ?

- On convertit chaque mot de 3 bits en polynôme
- on inverse dans $\mathbb{F}_8$ et on reconvertit en binaire
- associer au binaire son poly dans $\mathbb{F}_2[Y]/Y^3+1 = N(Y)$
- Calculer $a(Y)N(Y)+b(Y) \mod Y^3+1$

avec, par exemple

$a = Y^2+Y+1$

$b = Y^2+1$

4 Secret parfait

Soit M un mot de ℓ lettres sur l'alphabet $\{a, \ldots, z\}$. Chaque lettre m_i du message est codée par un entier modulo 26. la clé k définit un décalage comme dans le chiffre de César. L'opération de chiffrement est :

$$\mathrm{Enc}(k, (m_1, \ldots, m_\ell)) = (m_1 + k \mod 26, \ldots, m_\ell + k \mod 26)$$

1. Montrez que le chiffre par substitution défini ci-dessus vérifie la condition du secret parfait lorsque $\ell = 1$.

Le chiffre défini ci-dessus vérifie la condition du secret parfait pour $\ell = 1$. En effet, pour tous $m, c \in \{a, \ldots, z\}$ seule une des 26 permutations définissant la clé k associe la lettre c à la lettre m d'où

$$\mathrm{Prob}[\mathrm{Enc}(k, m) = c] = 1/26$$

Il s'ensuit que $\forall m_1, m_2 \in \{a, \ldots, z\}$ on a :

$$\mathrm{Prob}[\mathrm{Enc}(k, m_1) = c] = \mathrm{Prob}[\mathrm{Enc}(k, m_2)] = c] = 1/26$$

$$\mathrm{Prob}[C = c \mid M = m_1] = \mathrm{Prob}[C = c \mid M = m_2] = \Pr(C) = 1/26$$

c'est le lemme du transparent 19