Master CSI 2 2011-2012

Cryptanalyse — M1MA9W06
Responsable : G. Castagnos

Examen — mercredi 14 décembre 2011, 8h30

Durée 3h
Notes de cours autorisées
Nombre de pages : 3
Les 4 exercices sont indépendants

$\boxed{1}$ On considère un système de chiffrement à flot utilisant une suite chiffrante produite par un LFSR de longueur 3. Le LFSR est initialisé par une clef secrète K de 3 bits notés z_0, z_1, z_2. Après l'initialisation, on effectue 11 itérations du LFSR sans utiliser les bits de sortie $(z_0, z_1, \ldots, z_{10})$. Les bits de sortie suivants $z_{11}, z_{12}, \ldots$ sont utilisés de manière habituelle pour faire un chiffrement à flot.

On suppose qu'Alice et Bob connaissent tous les deux la clef secrète K et P un polynôme de rétroaction pour ce LFSR. On suppose que ce polynôme P utilisé par Alice et Bob est secret.

(a) Expliquer comment Alice et Bob peuvent utiliser ce système de chiffrement afin qu'Alice transmette un message m de ℓ bits $m = m_0, m_1, \ldots, m_{\ell-1}$ à Bob de manière confidentielle.

On intercepte la totalité d'un message chiffré c de 10 bits : $c = 0,0,0,1,1,1,0,0,1,1,0$ envoyé par Alice pour Bob avec ce système. On sait d'autre part que les 6 premiers bits du message clair m sont $0,1,0,0,0,1$.

(b) Quel est le polynôme P ? Est-il primitif ? x^3+x^2+1 , oui

(c) Déchiffrer le message tout entier. 01000 11110

(d) Quelle est la clef secrète ? 111

$\boxed{2}$ On rappelle qu'on associe à une boîte $S : \mathbf{F}_2^s \to \mathbf{F}_2^s$ d'un algorithme de chiffrement symétrique la matrices D_S, à 2^s lignes et 2^s colonnes, indexée sur $\mathbf{F}_2^s$ (identifié aux entiers de 0 à 2^s-1), définie par :

$$D_S[\alpha,\beta] := \mathrm{Card}\{(x,x^*) \in (\mathbf{F}_2^s \times \mathbf{F}_2^s) \text{ tel que } x + x^* = \alpha \text{ et } S(x)+S(x^*) = \beta\},$$

(a) Rappelez brièvement quelle propriété de la matrice D_S est recherchée pour éviter les attaques par cryptanalyse différentielle.

(b) Montrer que les coefficients de D_S sont tous pairs.

(c) Quelle est la forme de la matrice D_S si S est une application linéaire inversible de $\mathbf{F}_2^s \to \mathbf{F}_2^s$?

Dans toute la suite de l'exercice, on se place dans le cas de l'AES. On rappelle que la boîte S de l'AES est de la forme $S : \mathbf{F}_2^8 \to \mathbf{F}_2^8$ avec $S(x) = A.I(x) + b$ où A est une certaine matrice carrée inversible 8×8 sur $\mathbf{F}_2$, b est un certain vecteur 8×1 sur $\mathbf{F}_2$ et I désigne l'application de $\mathbf{F}_{2^8}$ dans $\mathbf{F}_{2^8}$:

$$x \mapsto I(x) = \begin{cases} 0 \text{ si } x = 0 \\ x^{-1} \text{ si } x \neq 0 \end{cases}$$

où l'inversion est effectuée dans le corps $\mathbf{F}_{2^8}$ après identification avec $\mathbf{F}_2^8$ par le choix d'un certain polynôme irréductible.

(d) Montrer que les coefficients de la matrice D_S peuvent se déduire des coefficients de la matrice D_I, définie par :

$$D_I[\alpha, \beta] := \mathrm{Card}\{(x, x^*) \in (\mathbf{F}_2^8 \times \mathbf{F}_2^8) \text{ tel que } x + x^* = \alpha \text{ et } I(x) + I(x^*) = \beta\}.$$

(e) Dans la suite on souhaite expliciter les coefficients de la matrice D_I. Que vaut $D_I[\alpha, \beta]$ si α ou β est nul ? On suppose maintenant dans toute la suite que α et β sont non nuls.

(f) Soit $x, x^* \in \mathbf{F}_2^8$ tels que $x + x^* = \alpha$. Dans cette question uniquement, on suppose que x et x^* sont non nuls. Montrer que $I(x) + I(x^*) = \beta$ si et seulement si x et x^* sont solutions d'une équation de degré 2 à une inconnue dans le corps $\mathbf{F}_{2^8}$. Montrer que si cette équation a une solution alors elle en a deux.

(g) Montrer que l'équation $x^2 + x + 1$ admet deux solutions dans $\mathbf{F}_{2^8}$.

(h) On suppose que $\beta^{-1} = \alpha$ dans $\mathbf{F}_{2^8}$. Montrer que $D_I[\alpha, \beta] = 4$.

(i) Conclure : que peuvent valoir les coefficients $D_S[\alpha, \beta]$, pour tout $\alpha, \beta \in \mathbf{F}_2^8$? Que peut on en déduire sur l'AES ?

$\boxed{3}$ On considère le réseau $\mathscr{L}$ de $\mathbf{Z}^2$ de base $M = \begin{pmatrix} 6 & 1 \\ 10 & 3 \end{pmatrix}$.

(a) Quel est le déterminant de ce réseau ?

(b) Quel est le minimum de $\mathscr{L}$? Donner un vecteur atteignant ce minimum.

(c) Le vecteur $(2, -5)$ est il dans le réseau ? Sinon quel est le vecteur non nul du réseau le plus proche ?

(d) Même question avec le vecteur $(1, 0)$.

(e) De manière générale, donner un algorithme qui prend en entrée M une matrice donnant une base d'un réseau $\mathscr{L}$ de dimension n inclus dans $\mathbf{Z}^n$ et un vecteur v, et qui renvoie vrai si et seulement si $v \in \mathscr{L}$.

$\boxed{4}$ Dans cet exercice, on s'intéresse à la sécurité du système de chiffrement à clef publique défini de la façon suivante :

- **Génération des clefs :** Soit k un entier, le paramètre de sécurité. On choisit un nombre premier p de k bits et k polynômes de degrés 1, $f_1(x), f_2(x), \ldots, f_k(x)$ à coefficients dans $\mathrm{Z}/p^2\mathrm{Z}$.
  On notera $f_i = f_{i,0} + f_{i,1}x$ les coefficients du polynôme f_i pour $i = 1, \ldots, k$.
  On suppose de plus qu'il existe un entier s tel que pour tout $i = 1, \ldots, k$, $f_i(s) \mod p^2 < p/k$.
  La clef publique est constituée de p et des polynômes $f_1, \ldots, f_k$.
  La clef privée est l'entier s.

- **Chiffrement** d'un message clair $m \in \mathrm{Z}/p\mathrm{Z}$:
  on génère aléatoirement k bits, $r_1, r_2, \ldots, r_k \in \{0, 1\}$. Le chiffré de m est le polynôme de degré 1 défini par :
  $$c(x) := m \times p + \sum_{i=1}^{k} r_i f_i(x) \mod p^2.$$

- **Déchiffrement** d'un chiffré $c(x)$:
  on calcule dans $\mathbf{Z}$,
  $$\frac{c(s) - (c(s) \mod p)}{p}.$$

(a) Soit $c(x) = c_0 + c_1 x$ un message chiffré d'un message clair m en utilisant les bits aléatoires $r_1, r_2, \ldots r_k$. Soit $z_0, z_1 \in \mathbf{N}$, deux entiers strictement inférieurs à p tels que
$$z_0 + z_1 p = \sum_{i=1}^{k} r_i f_i(s) \mod p^2.$$
Montrer que l'on a $z_1 = 0$.
En déduire que le système est correct, c'est à dire que le déchiffrement de $c(x)$ redonne bien m modulo p.

(b) Soit $c(x) = c_0 + c_1 x$ un message chiffré d'un message clair m en utilisant les bits aléatoires $r_1, r_2, \ldots r_k$. Donner l'expression du coefficient de degré 1, c_1 de $c(x)$ en fonction des coefficients des polynômes publics $f_1, \ldots, f_k$.

(c) Comment s'appelle le problème de retrouver $r_1, r_2, \ldots r_k$ dans l'expression de c_1 donnée précédemment ? Indiquer comment et pourquoi on peut résoudre ce problème dans ce cas précis en utilisant l'algorithme LLL.

(d) En déduire une attaque permettant de déchiffrer un chiffré c à l'aide de la clef publique, sans connaître la clef secrète.