TELECOM

Contrôle des connaissances 2006/2007

CRYPTOGRAPHIE

7 novembre 2006

durée 3 heures

On sera attentif à la précision de la rédaction. Les résultats devront toujours être justifiés que ce soit par une démonstration, un algorithme ou une vérification numérique. Les protocoles seront décrits précisément.

Documents et calculettes non autorisés

Exercice 1

Décrivez un étage du système de cryptage AES

Exercice 2

On note $\mathbb{F}_2$ le corps à 2 éléments. On rappelle que dans AES on travaille sur des octets qui sont interprétés comme des éléments du corps à 256 éléments noté, $\mathbb{F}_{256}$, qui est représenté de la manière suivante:

1. $\mathbb{F}_{256} \simeq \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1)\mathbb{F}_2[X]$, et que tout élément de $\mathbb{F}_{256}$ est identifié avec un polynôme de $\mathbb{F}_2[X]$ de degré ≤ 7.
2. on identifie l'octet $a_0a_1 \dots a_7$ avec le polynôme $a_0 + a_1X + \cdots + a_7X^7$

On demande de calculer dans AES

1. la somme des octets 10011 et 011111
2. le produit des octets 0111101 et 1110001
3. l'inverse multiplicatif de l'octet 101101

Exercice 3

On rappelle qu'un LSFR est déterminé par les données initiales contituées d'un entier m, la longueur de la récurrence, et des éléments

$$k_1, \dots, k_m \in \mathbb{Z}/2\mathbb{Z}, \quad \text{les conditions initiales}$$
$$c_0, \dots, c_{m-1} \in \mathbb{Z}/2\mathbb{Z} \quad \text{les coefficients de la récurrence}$$

On construit alors à partir des données initiales une suite d'éléments $(z_i)_{i\in\mathbb{N}}$ de $\mathbb{Z}/2\mathbb{Z}$:

$$z_1 = k_1, \ldots, \ z_m = k_m, \quad z_{m+1} = c_0 z_1 + \cdots + c_{m-1} z_m$$
$$z_{m+i} = c_0 z_i + \cdots + c_{m-1} z_{m-1+i} = \sum_{j=0}^{m-1} c_j z_{j+i}$$

on peut représenter le LFSR de la manière suivante, cf.figure 1.

On considère alors les données suivantes:

1. un entier m
2. $m-1$ éléments de $\mathbb{F}_2$ $Q_1^{(0)}$, $Q_1^{(0)}$,..., $Q_i^{(0)}$,..., $Q_m^{(0)}$, les conditons initiales
3. m nombres de $\mathbb{F}_2$, a_0, a_1,.., a_i,..., a_{m-1}, a_m avec $a_0 \neq 0$ et $a_m \neq 0$.

À partir de ces données initiales on construit pour $1 \leq i \leq m$ une suite d'éléments de $\mathbb{F}_2$, $k \mapsto Q_i^{(k)}$, de la manière suivante:

$$Q_i^{(k)} = Q_{i-1}^{(k-1)} + a_{i-1} Q_m^{(k-1)} \text{ pour } i \geq 2$$
$$Q_1^{(k)} = Q_m^{(k)}$$

Montrer que la suite $k \mapsto Q_m^{(k)}$ est un LSFR, appelé LSFR de Galois. On peut le représenter de la manière suivante, cf.figure 2.

Exercice 4

Décrire un protocole de preuve sans transfert de connaissances.

Exercice 5

Alice et Bob veulent correspondre en employant un système RSA.
Pour fabriquer sa clé Alice choisit comme nombres premiers:

$$p_a = 277 \quad q_a = 281$$

Elle veut choisir son exposant e_a dans la liste 4, 5, 6, 7, 8, 9, 10, 11. Quels peuvent être ses choix. Elle choisit le plus grand. Quelle est sa clé publique, quelle est sa clef privée?

Pour fabriquer sa clé Bob choisit comme nombres premiers

$$p_b = 223 \quad q_b = 233$$

Il choisit son exposant e_b dans la liste 2, 3, 4, 5, 6. Quels sont ses choix possibles. Il choisit le plus petit. Quelle est sa clé privée, quelle est sa clé publique?

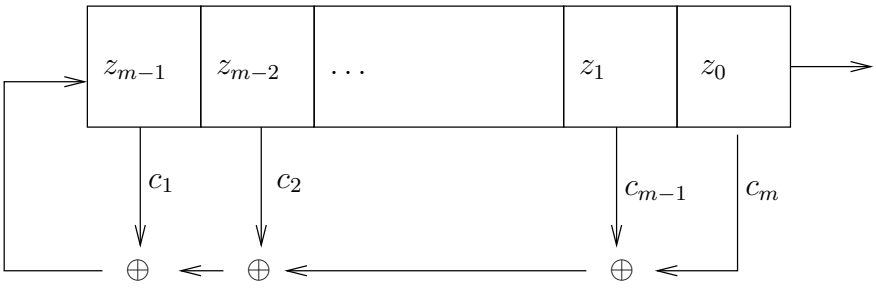

Figure 1: Diagramme d'un LSFR

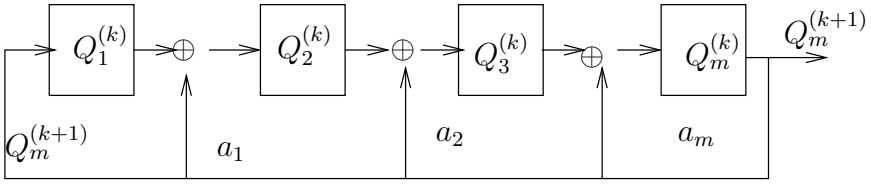

Figure 2: Diagramme d'un LSFR de Galois