TELECOM

Contrôle des connaissances 2007/2008

CRYPTOGRAPHIE

6 novembre 2007

durée 2 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 $a_0 a_1 \dots a_7$ avec le polynôme $a_0 + a_1 X + \cdots + a_7 X^7$

On demande de calculer dans AES

1. la somme des octets 10010100 et 01101101
2. le produit des octets 10101101 et 11110001
3. l'inverse multiplicatif de l'octet 10110000

Exercice 3

On rappelle et on admet les faits et théorèmes suivant:

Théorème 0.1. *Si $\mathbb{K}$ est un corps et si $P(X) \in \mathbb{K}[X]$ il existe un corps $\mathbb{L} \supset \mathbb{K}$ tel que le polynôme $P(X)$ y ait toutes ses racines, autrement dit*

$$P(X) = a_0(X - \alpha_1)....(X - \alpha_d), \text{ avec } \alpha_1, \alpha_2, \dots, \alpha_d \in \mathbb{L}, \quad a_0 \in \mathbb{K}$$

Théorème 0.2. *Si $\mathbb{K}$ est un corps il existe un corps $\bar{\mathbb{K}} \supset \mathbb{K}$ tel que tout polynôme $P(X) \in \mathbb{K}[X]$ y ait toutes ses racines, ce corps qui n'est pas unique est appelé une clôture algébrique de $\mathbb{K}$*

Théorème 0.3. *Soit $\mathbb{K}$ est un corps et soit $\bar{\mathbb{K}} \supset \mathbb{K}$ une clôture algébrique de $\mathbb{H}$ fixée. Si $(u_n)_{n\in\mathbb{N}}$ est une suite récurrente linéaire de degré d définie sur $\mathbb{K}$, c'est à dire qu'il existe $a_0, a_1, \ldots, a_{d-1}$ tels que*

$$\text{Pour tout } n \in \mathbb{N},\ u_{n+d} = a_0 u_{n+d-1} + a_1 u_{n+d-2} + \cdots + a_{d-1} u_n\ ,$$

telle que le polynôme compagnon $X^d - aX^{d-1} - a_1 X^{d-2} - \cdots - ad - 1$ ait toute ses racines simples (en particulier s'il est irréductible), alors il existe $\alpha_1, \ldots, \alpha_d \in \bar{\mathbb{K}}$ et $\lambda_1, \ldots, \lambda_d \in \bar{\mathbb{K}}$ tels que

$$u_n = \lambda_1 \alpha_1^n + \lambda_2 \alpha_2^n + \cdots + \lambda_d \alpha_d^n$$

Les α_i sont les racines du polynôme $X^d - a_0 X^{d-1} - a_1 X^{d-2} - \cdots - a_{d-2} X - a_{d-1}$

Théorème 0.4. *Soit p un nombre premier et soit $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments. On fixe une fois pour toute une clôture algébrique $\bar{\mathbb{F}}_p$ de $\mathbb{F}_p$. Il existe pour chaque entier n un unique corps fini $\mathbb{F}_{p^n} \subset \bar{\mathbb{F}}_p$ ayant p^n éléments et réciproquement tout sous-corps fini de $\bar{\mathbb{F}}_p$ est de la forme $\mathbb{F}_{p^n}$.*

Si $P(X) \in \mathbb{F}_p[X]$ est de degré d alors le plus petit sous corps de $\bar{\mathbb{F}}_p$ contenant toute ses racines est contenu dans le corps $\mathbb{F}_{p^d}$.

Si $q = p^n$ alors le sous-groupe multiplicatif des éléments inversibles de $\mathbb{F}_q$ noté $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ est un groupe cyclique d'ordre $q-1$, c'est à dire que

Pour tout $y \in \mathbb{F}_q^*$, $\quad y^{q-1} = 1$

Il existe $g \in \mathbb{F}_q^*$ tel que pour tout $y \in \mathbb{F}_q^*$ il existe $\ell(y) \in \mathbb{N}$, $0 \leq \ell(y) \leq q-2$, tel que $y = g^{\ell(y)}$

Théorème 0.5. *Si $y \in \mathbb{F}_q^*$ ($q = p^n$, $n \in \mathbb{N}$, $n \geq 1$, p premier) alors le plus petit entier non nul e tel que $y^e = 1$ est un diviseur de $q-1$*

Question 1 Montrer que tout élément $y \in \mathbb{F}_q^*$ est racine du polynôme $X^{q-1} - 1$, autrement dit que

$$X^{q-1} - 1 = \prod_{y \in \mathbb{F}_q^*} (X - y)$$

Question 2 Montrer que tout polynôme $P(X) \in \mathbb{F}_p[X]$ de degré d divise le polynôme $X^{p^d-1} - 1$.

Question 3 On considère le LSFR sur $\mathbb{F}_2$, défini par la relation de récurrence

$$u_{n+4} = u_{n+1} + u_n$$

et les conditions initiales $(k_0, k_1, k_2, k_3) \in \mathbb{F}_2^4$.
Montrer que pour tout choix de conditions initiales la période de la suite récurrente linéaire $(u_n)_{n\in\mathbb{N}}$ est majorée par 15, (étudier la période de la suite $n \to \alpha^n$ où α est n'importe quelle racine du polynôme $X^4 - X - 1$.

Question 3 On code par XORisation à l'aide du LFSR précédent avec les conditions initiales $(k_0, k_1, k_2, k_3) = (1, 0, 0, 0)$. Chaque lettre de l'alphabet est codée par le quintuplet $(a_0, a_1, a_2, a_3, a_4)$ tel que $a_0 + 2a_1 + 4a_2 + 8a_3 + 16a_4)$ soit le rang de la lettre dans l'alphabet ordinaire compté entre 1 et 26, le quintuplet $(0, 0, 0, 0, 0)$ correspond à l'espace entre deux mots (exemples: A la première lettre de l'alphabet est codée $(1, 0, 0, 0, 0)$, M la treizième de l'alphabet lettre est codée $(1, 0, 1, 1, 0)$). Décoder le message page 4.

Exercice 4

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?

Exercice 5

Alice et Bob veulent correspondre en utilisant un système El Gamal. Bob a le choix des paramètres suivants pour son système El Gamal

- $(p = 32,\ g = 4,\ \alpha = 2)$
- $(p = 17,\ g = 3,\ \alpha = 7)$
- $(p = 17,\ g = 3,\ \alpha = 5)$
- $(p = 17,\ g = 2,\ \alpha = 7)$

Quels sont ses choix possible? Quelles peuvent être ses clés privées et publiques?

Message à déchiffrer

1	1	0	0	0	1	0	0	1	0	1	1	0	0	1
1	0	1	0	1	1	0	0	1	0	1	1	1	0	0
1	0	0	0	1	0	0	0	1	0	0	0	0	1	1
0	0	1	1	1	1	0	1	1	0	0	0	1	0	1
1	1	1	1	1	0	0	1	1	0	0	0	0	0	1
0	0	0	1	1	0	0	0	1	0	0	0	1	0	1
1	0	0	0	1	0	1	0	1	1	0	0	1	0	1

1	0	1	1	1	0	0	0	0	0	0	0	0	1	1
1	0	1	0	0	1	0	1	1	0	1	1	0	0	1
0	0	1	0	1	1	0	0	1	1	0	1	1	1	0
0	0	1	0	1	0	0	1	1	0	1	0	1	1	1