Université de Bordeaux
Collège Sciences et Technologies
Année 2017-2018

Master CSI
Cryptologie

Devoir Surveillé, 28 février 2018
Durée 1h30, documents interdits

La qualité de la rédaction sera un facteur d'appréciation.

Exercice 1 – On rappelle le principe du chiffrement de Hill. Soit un entier $n \geq 1$. On pose $\mathcal{M} = \mathcal{C} = (\mathbb{Z}/26\mathbb{Z})^n$ (les clairs et chiffrés sont vus comme vecteurs colonnes) et $\mathcal{K} = \mathrm{GL_n}(\mathbb{Z}/26\mathbb{Z})$. Si la clé secrète est K, le clair m est chiffré en $c = K \cdot m$. On suppose que les messages clairs sont équiprobables. Montrer que le chiffrement de Hill n'est pas à confidentialité parfaite.

Exercice 2 – On considère un système de chiffrement où l'espace des messages clairs est $\mathcal{M} = \{a, b, c\}$, l'espace des messages chiffrés est $\mathcal{C} = \{1, 2, 3, 4, 5, 6\}$ et celui des clés est $\mathcal{K} = \{\mathrm{i}, \mathrm{ii}, \mathrm{iii}, \mathrm{iv}, \mathrm{v}, \mathrm{vi}\}$. Le système est décrit par le tableau suivant :

$\mathcal{M}$ \ $\mathcal{K}$	i	ii	iii	iv	v	vi
a	1	2	3	4	5	6
b	2	3	4	5	6	1
c	3	4	5	6	1	2

On suppose que les messages clairs et les clés sont équiprobables. On suppose aussi que la clé est indépendante du message clair.
1. Ce système est-il à confidentialité parfaite ? Justifier proprement.
2. Quelles sont les probabilités d'imposture et de subsitution de ce système ?

Exercice 3 – On veut distinguer un schéma de Feistel à trois tours (sans permutation finale) d'une fonction aléatoire. Le schéma correspond donc à la composée $F_3 \circ F_2 \circ F_1$ de trois transformations $F_i : A\|B \mapsto B\|A \oplus f_i(B)$ $(1 \leq i \leq 3)$. On suppose que l'on a accès aux fonctions de chiffrement et de déchiffrement. On demande à déchiffrer $0 \,\|\, 0$ et on obtient $X^L\|X^R$. On demande alors à chiffrer $0\,\|X^R$ et on obtient $Y^L\|Y^R$. Enfin on demande à déchiffrer $Y^L\|X^L \oplus Y^R$ et on obtient $Z^L\|Z^R$. Montrer que $Z^R = X^R \oplus Y^L$.

Exercice 4 – On utilise un chiffrement par bloc et le mode opératoire dit BC (pour "Block Chaining"). Les blocs sont des éléments de $\mathbb{F}_2^k$. Notons E_K et D_K les fonctions de chiffrement et de déchiffrement utilisées qui dépendent de la clé K. On désire chiffrer $n > 1$ blocs consécutifs $m_1, m_2, \ldots, m_n$. On choisit un bloc d'initialisation IV et on applique l'algorithme suivant :

(1) $c_1 = E_K(m_1 \oplus IV)$;
(2) $I_1 = (0, 0, \ldots 0) \in \mathbb{F}_2^k$;
(3) Pour $2 \leq i \leq n$, $I_i = I_{i-1} \oplus c_{i-1}$ et $c_i = E_K(m_i \oplus I_i)$.

On transmet alors les blocs $c_0, c_1, c_2, \ldots, c_n$ où $c_0 = IV$.
1. Décrire l'algorithme de déchiffrement.
2. On admet que lors de la transmission un bloc chiffré c_i a été altéré $(0 \leq i \leq n)$. Combien de blocs obtenus à l'issue du déchiffrement seront probablement erronés ?

Exercice 5 – On considère les suites $u = (u_i)_{i \geq 0}$ et $v = (v_i)_{i \geq 0}$ de $\mathbb{F}_2^{\mathbb{N}}$ engendrées par la relation de récurrence

$$(E): \; s_{i+5} = s_{i+4} + s_i, \quad \text{pour tout } i \geq 0$$

et par la donnée des vecteurs initiaux respectifs

$$(u_0, u_1, u_2, u_3, u_4) = (1, 0, 1, 1, 0) \; \text{ et } \; (v_0, v_1, v_2, v_3, v_4) = (1, 0, 0, 1, 0).$$

1. Quelle est la période de u ?
2. En déduire que le polynôme $X^5 + X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_2[X]$.
3. Quelle est la période de v ?
4. Déterminer les séries génératrices de u et v :

$$U(X) = \sum_{i=0}^{\infty} u_i X^i \; \text{ et } \; V(X) = \sum_{i=0}^{\infty} v_i X^i.$$

5. Quelles sont les complexités linéaires de u et v ?
6. Trouver les relations de récurrence linéaire les plus courtes vérifiées par u et v.
7. Déterminer la complexité linéaire et la période de la suite $u + v$.