Université de Limoges
Faculté des Sciences et Techniques

Année universitaire 2015-2016

Master 2 Math - CRYPTIS

Examen Écrit - Cryptographie à clée secrète

Problème 1 : Fonctions à sens unique

Problème 1.1

Suppose qu'il existe des fonctions à sens unique. Montrer que : pour toute fonction $h : \{0,1\}^* \to \{0,1\}$, il existe d'une fonction à sens unique $f : \{0,1\}^* \to \{0,1\}^*$ telle que h n'est pas un prédicat "hard-core" de f.

Problème 1.2

Soient $f_1, f_2 : \{0,1\}^* \to \{0,1\}^*$ deux fonctions à sens-unique. Déterminer si les fonctions F définies comme suit sont à sens-unique :

1. $$F(x) = (f_1(x), f_1(x) \oplus f_2(x))$$
2. $$F(x||y) = (f_1(f_2(x)) \oplus y, f_2(f_1(y)) \oplus x),$$

(où $|y| \leq |x| \leq |y| + 1$)

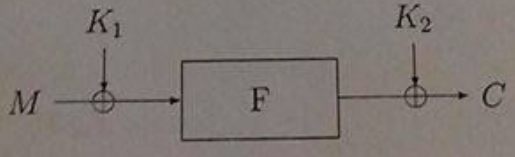
Problème 2 : Générateur pseudo-aléatoire

Soit G un générateur pseudo-aléatoire avec un facteur d'expansion $l(n) = 2n$. Reécrire $G(s) = G_0(s)||G_1(s)$ où $|G_0(s)| = |G_1(s)|$. Déterminer si les fonctions G' définies comme suit sont des générateurs pseudo-aléatoires :

1. $G'(s) = G_0(G_0(s \oplus 1))||G_0(G_1(s \oplus 10))||G_1(G_0(s \oplus 11))||G_1(G_1(s \oplus 100))$
2. $G'(s_1||s_2) = G_0(G_1(s_1))||G_1(G_0(s_1 \oplus s_2))||s_1$ (où $|s_1| \leq |s_2| \leq |s_1| + 1$)

Problème 3 : Chiffrement par bloc de type Even Mansour

Un chiffrement par bloc de type Even Mansour est défini par la figure suivante :



où $K = (K1||K2)$ est la clé de chiffrement de taille $2n$, M est le message à chiffrer, C est le chiffré, tous les deux de taille n, et F est une bijection publique de F_2^n dans lui-même. On peut remarquer que la taille de la clé est le double de celle du chiffrée. Puisque F est connu, l'attaquant peut calculer la valeur $F(X)$ pour tout X de son choix.

1. Montrer que la connaissance de deux couples clair/chiffré permet de réduire l'espace des clés valides à seulement deux clés en 2^n évaluations de la fonction F.
2. Montrer que si un attaquant peut demander le chiffrement de k couples de messages clairs (M_i, M_i') pour $i = 1, \ldots, k$ avec $M_i \oplus M_i' = \Delta$, où $\Delta \in \{0,1\}^n$ est constant, alors l'attaque précédente peut être accélérée d'un facteur k. Donner la valeur optimale de k lorsque la mémoire de l'attaquant n'est pas limitée.

Problème 4 : Fonction pseudo-aléatoire - chiffrement symétrique

Supposons qu'il existe une famille de fonctions pseudo-aléatoires $\mathcal{F} = \{F_K : \{0,1\}^n \to \{0,1\}^n, K \in \{0,1\}^n\}$. On définit un schéma de chiffrement symétrique $\pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ de la façon suivante :

Générateur des clés : $\mathcal{G}(1^n)$ retourne une clé aléatoire $K \in \{0,1\}^n$

Chiffrement : Il s'agit d'un chiffrement de $\{0,1\}^{2n}$ à $\{0,1\}^{2n}$. Pour chiffrer $M \in \{0,1\}^{2n}$, écrire d'abord $M = m_1||m_2$ avec $|m_1| = |m_2| = n$, puis tirer aléatoirement $r \in \{0,1\}^n$, et finalement retourner $(r, F_K(r) \oplus m_1, F_K(r) \oplus m_2)$:

$$E_K(m_1||m_2) := (r, F_K(r) \oplus m_1, F_K(r) \oplus m_2)$$

Déchiffrement : Pour déchiffrer (r, c_1, c_2), calculer

$$m_1 = c_1 \oplus F_K(r), m_2 = c_2 \oplus F_K(r),$$

puis retourner $M = m_1||m_2$

On considère les quelques notions suivantes :

— Notion de sécurité IND (indistinguabilité) : Un schéma de chiffrement est dit IND-sûr si l'attaquant ne peut pas distinguer les chiffrés de deux messages son choix. Plus formellement, le jeu IND est décrit comme suit : l'attaquant choisit deux messages M_0 et M_1 dans l'espace des clairs, puis reçoit un challenge $C = E_K(r, M_b)$ où $b \in \{0,1\}$ est choisi aléatoirement et l'aléa r est aléatoirement tiré ; l'attaquant gagne s'il peut deviner le bit b avec un avantage non-négligeable par rapport à $\frac{1}{2}$ et perd sinon. Le schéma est IND-sûr si tout attaquant en temps polynomial perd le jeu IND.

— Modèle d'attaque : un attaquant à clair choisi, dénoté CPA, a le droit de demander à l'oracle de chiffrement de chiffrer tout message de son choix ; un attaquant à chiffré choisi, dénoté CCA, a le droit de demander à l'oracle de déchiffrement de déchiffrer tout chiffré de son choix. L'attaquant à chiffré choisi dans le jeu IND est interdit à demander le challenge à l'oracle de déchiffrement.

Répondre aux questions suivantes :

1. Le schéma de chiffrement π est-il IND-sûr face aux attaquants CPA ?
2. Le schéma de chiffrement π est-il IND-sûr face aux attaquants CCA ?