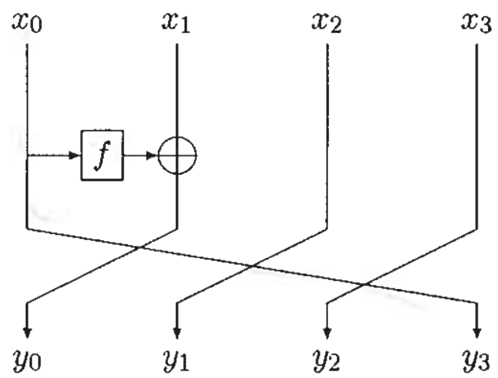
Université de Limoges
Faculté des Sciences et Techniques

Année universitaire 2018-2019

Master 2 Math - CRYPTIS
Examen Écrit - Cryptographie à clée secrète

Problème 1 : Schéma de Feistel généralisés

On cónidère un schémas de Feistel à 4 branches suivante, où l'entrée d'un tour est constituée de 4 blocs de k bits $(x_0; x_1; x_2; x_3)$ et la sortie du tour de 4 blocs de k bits $(y_0; y_1; y_2; y_3)$:



1. Montrer que le tour est inversible et préciser son inverse.
2. Expliciter les sorties en fonction des entrées sur 4 tours.
3. Montrer que la sortie y_1 (après 4 tours) ne dépend que des entrées x_0 et x_1. En supposant la fonction f inconnue, en déduire un distingueur sur 4 tours de cette construction avec une permutation aléatoire.

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 : 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 $M = m_1||m_2$

Répondre aux questions suivantes :

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