Université de Limoges **Année universitaire 2017-2018**
Faculté des Sciences et Techniques

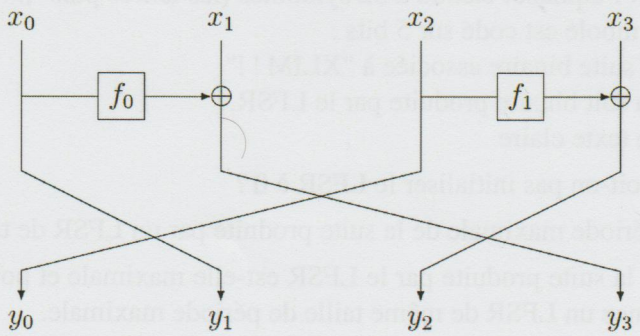
Master 2 Math - CRYPTIS

Examen Écrit - Cryptographie à clée secrète

Instructions

1. Durée 3h.
2. Manuscrits et documents autorisés. Les documents du voisin ne sont pas des documents autorisés.
3. Les solutions doivent être détaillées et les preuves présentées de la manière la plus formelle possible. La clarté de présentation des idées principales dans les preuves et/ou constructions sera prise en compte dans la notation.

Problème 1 : Schéma de Feistel généralisé



Structure Feistel généralisé. On considère le schéma de Feistel généralisé à 4 branches donné par la figure ci-dessus : les x_i et y_i représentent des blocs de m bits. La taille de l'entrée et de la sortie est donc $4m$.

Schéma de chiffrement par bloc fondé sur la structure Feistel généralisé. Ce schéma est utilisé sur r tours, à chaque tour i on note :

— f_0^s, f_1^s les fonctions f_0, f_1 au tour s, sachant que ces fonctions sont dépendantes des clés de tour et changent donc chaque itération.

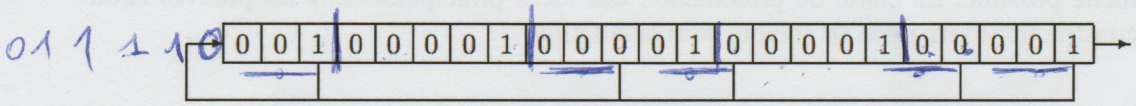
— y_i^s les valeurs des 4 blocs après s tours. Par convention $y_i^0 = x_i$, la sortie au bout de r tours est donnée par les z_i^r.

Questions :

1. Montrer que ce schémas est inversible quelque soient les fonctions f_i. Préciser son inverse.
2. Montrer qu'une diférence en entrée limitée au bloc x_1 ne peut pas induire une différence en sortie du 3ème tour sur les blocs y_1^3 et y_3^3.
3. Distinguer un schémas de Feistel généralisé en 3 tours d'une bijection aléatoire.
4. Montrer que la propriété décrite à la question 2 n'est plus vraie à partir du 4ème tour.
5. Étudier la sécurité du schéma à 4 tours, en supposant que les fonctions f_0^s, f_1^s sont sûrs (c'est-à-dire des fonctions pseudo-aléatoires avec les sous clés choisis aléatoirement) : Est ce que l'on peut le distinguer avec une permutation aléatoire avec l'attaque à clair choisi.

Problème 2 : Registres à décalage à rétroaction linéaire

Soit un système de chiffrement à flot dans lequel la suite ajoutée au texte clair est générée par le LFSR suivant :



1. En considérant l'alphabet étendu à 32 symboles (les lettres puis -,. : ! ?), et en supposant que chaque symbole est codé sur 5 bits :
   — Donnez la suite binaire associée à "XLIM ! !"
   — Générez la suit binaire produite par le LFSR.
   — Chiffrez le texte claire
2. Pourquoi ne doit-on pas initialiser le LFSR à 0 ?
3. Rappelez la période maximale de la suite produite par un LFSR de taille n
4. La période de la suite produite par le LFSR est-elle maximale et pourquoi ? Dans le cas contraire, donnez un LFSR de même taille de période maximale.

Problème 3 : Approche théorique

Cryptographie et P vs. NP problème. Construire une fonction f tel que :
— Si f est inversible en temps polynomial (sur toutes les entrées), alors $P = NP$
— f n'est pas une fonction à sens unique

Générateur pseudo-aléatoire. Supposons qu'il existe une permutation à sens unique $f : \{0,1\}^n \to \{0,1\}^n$, dénotons h un prédicat "hard-core" de f. On définit une fonction G de la façon suivante : sur une entrée $x \in \{0,1\}^n$, retourner $(f(f(x))||h(x))$.

$$G(x) := f(f(x))||h(x)$$

Déterminer si G est un générateur pseudo-aléatoire.