Examen M2 SeCReTS 2015-2016 : "Bases de la cryptographie".

Remarques :

- Pour chacune des questions, on demande de justifier les étapes en mentionnant notamment les algorithmes utilisés.
- Aucun document, calculatrice, téléphone, Ipad etc ne sont admis.
- Les sacs doivent rester à terre et aucune feuille de brouillon n'est admise.
- Un feuille quadrillée recto (A4) avec vos notes est autorisée (écriture sur les lignes).
- La durée de l'examen est de 3 heures.

Partie I : Théorie

Question 1

1. Détaillez le RSA en chiffrement et montrez que l'algorithme de chiffrement et de déchiffrement forment une paire de permutation inverse l'une de l'autre.
2. Expliquez en quoi la notion de réduction calculatoire est importante pour donner des éléments de sécurité concernant les schémas cryptographiques. Définissez la notion "polynomialement réductible" et "calculatoirement équivalent". Enoncez deux problèmes mathématiques de votre choix et montrez qu'ils sont calculatoirement équivalents. Un esprit de synthèse est demandé.

Question 2

Expliquez les différentes façons de concevoir un algorithme de chiffrement par bloc. Comparez ces différents designs en expliquant les choix qui sont généralement faits et en donnant les contraintes imposées sur les composantes de ces algorithmes. Détaillez un standard pratique pour chacun des designs. Expliquez en quoi les attaques donnent des critères de conception. Donnez un exemple. Un esprit de synthèse est demandé ($\approx 1/1.5$ pages)

Partie II : Exercices

Question 3

Cette question concerne le RSA à trois facteurs. Il s'agit d'un RSA classique dans lequel le module RSA est le produit de trois facteurs, au lieu de deux classiquement. Considérons les nombres premiers $p = 3$, $q = 5$ et $r = 7$. Dénotons par Φ la fonction totient d'Euler.

1. Calculez le module RSA à trois facteurs (que l'on dénotera n) et $\Phi(n)$.
2. Parmi les nombres 12 et 19, déterminez ceux qui satisfont les hypothèses d'exposant de chiffrement et pour ceux-la calculer l'exposant de déchiffrement correspondant.

3. Déchiffrez le message 17 pour le(s) exposant(s) retenu(s) au point précédent. Utilisez la méthode la plus efficace que vous connaissez.

Question 4

On souhaite factoriser $n = 165$ par la méthode de Dixon en utilisant la base $\{2, 3, 5\}$. On supposera dans l'exercice que le générateur aléatoire fournit les nombres $\{14, 15, 16, 30, 45, 75\}$. Dans les calculs modulaires intervenant dans l'algorithme, vous pouvez utiliser toutes les techniques que vous connaissez pour limiter le calcul mental au maximum.

Question 5

1. Testez la primalité de 17 au moyen d'un algorithme efficace en utilisant un paramètre de sécurité t = 2.
2. Considérons le polynôme irréductible $P(X) = X^4 + X + 1$ appartenant à l'ensemble $\mathbb{Z}_2[X]$. Testez au moyen d'un algorithme systématique efficace si la classe $[X + (P(X))]$ est un générateur du groupe $(\mathbb{Z}_2[X]/(P(X)))^*$. Même question pour la classe $[X^3 + (P(X))]$.

Question 6

1. Considérons le système de chiffrement symétrique suivant. Pour chaque message M choisi de façon aléatoire dans l'espace $(\mathbb{Z}/4\mathbb{Z}, +)$, on choisit une clé K choisie de façon aléatoire dans $(\mathbb{Z}/4\mathbb{Z}, +)$. L'opération de chiffrement consiste à faire une addition dans $\mathbb{Z}/4\mathbb{Z}$ de M et de K, i.e. $C = M + K$.
   (a) Donnez le mécanisme de déchiffrement.
   (b) Rappelez la définition de système de chiffrement parfait. En vous basant sur la définition, déterminez si le système précédent est parfait ou non.
2. Considérez l'algorithme de chiffrement à trois tours basé sur la construction de Lai-Massey (voir ci-dessous). Si la taille du

bloc est $2n$, le message est d'abord découpé en deux morceaux de taille n. Ces deux morceaux sont ensuite appliqués à l'algorithme tel que décrit à la page suivante. $\oplus$ est l'opération XOR sur n bits et F_K est une application de $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$. Les sous-clé $k^{(i)}$ sont choisies de façon indépendante (pas d'algorithme de cadencement des clés).

On demande de déterminer l'algorithme de déchiffrement ; donnez le diagramme et justifiez mathématiquement la construction de celui-ci.

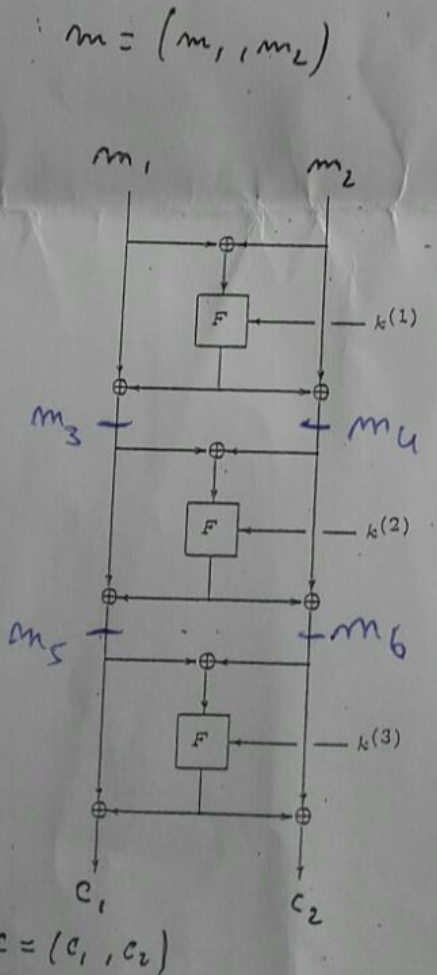

Figure 4.2. A three-round Lai-Massey scheme