Examen M2 SeCReTS 2016-2017 : "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) écrite de votre main et avec le contenu de votre choix 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 la méthode de Dixon qui permet la factorisation de nombre naturel. Détaillez la méthode sur un exemple de votre choix.

à faire

Question 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.

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 19 pour le(s) exposant(s) retenu(s) au point précédent. Utilisez la méthode la plus efficace que vous connaissez.

on choisit une clé K choisie de façon aléatoire dans $\{00, 01, 10\}$. L'opération de chiffrement consiste à faire le "XOR" de M et de K, i.e. $C = M \oplus K$.

1. Donnez le mécanisme de déchiffrement.
2. Calculez l'information mutuelle entre le message et le chiffré. (piste : $I(X,Y) = I(Y,X)$ où $I(\cdot,\cdot)$ est l'information mutuelle). Exprimez votre réponse en terme de rationnels et valeurs $log_2(k)$ où les k's sont des naturels non-nuls. Simplifiez votre formule au maximum.
3. Est-ce que ce système est parfait ? Si ce n'est pas le cas, comment le modifier pour qu'il le soit en gardant la taille des espaces des messages et des clés.

Question 6

a. Considérez l'algorithme de chiffrement à trois tours basé sur la construction de de Lai-Massey. 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 $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$. 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.

b. Considérons le polynôme primitif $P(X) = X^4 + X + 1$ appartenant à l'ensemble $\mathbb{Z}_2[X]$. Calculez le représentant minimal de l'inverse de chacune des classes inversibles (par rapport à la multiplication) de l'anneau $(\mathbb{Z}_2[X]/(P(X)), +, *)$.

Question 4
Le but de cet exercice est de construire un protocole de Diffie-Hellman particulier.

Soit un nombre premier p impair. Considérons l'anneau $(\mathbb{Z}/p^2\mathbb{Z}, +, *)$. Considérons le sous-ensemble G de $\mathbb{Z}/p^2\mathbb{Z}$ avec

$$G = \{[x + p^2\mathbb{Z}] \mid x \equiv 1 \bmod p\}.$$

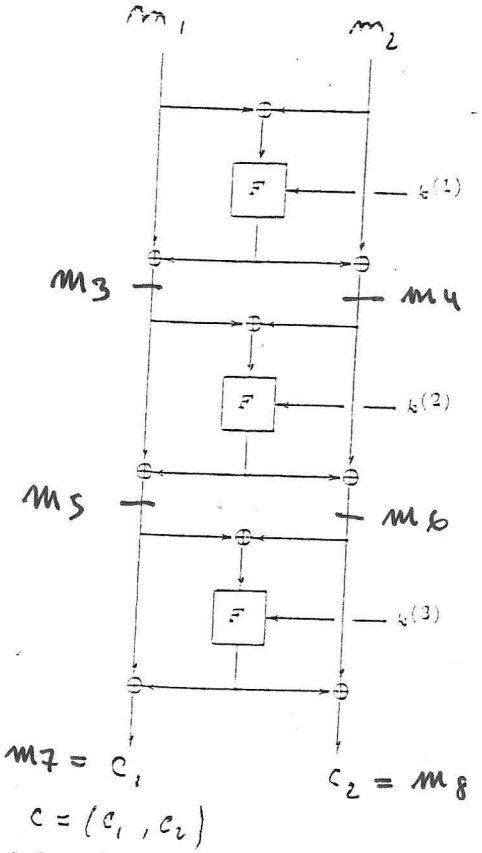
1. Décrire l'ensemble des représentants minimaux des classes de cet ensemble et déduisez que la cardinalité de G est p.
2. Montrez que $(G, *)$ est un groupe (d'ordre p).
3. En utilisant une algorithme efficace montrez que $[p+1+p^2\mathbb{Z}]$ est un générateur de G.
4. Supposons que Alice et Bob souhaitent déterminer en commun une clé $K \in G$. Pour cela :
   - Alice tire au hasard $x \in \{0, \cdots, p-1\}$ (et le garde secret), calcule $\alpha = [p + 1 + p^2\mathbb{Z}]^x$ et envoie α à Bob via un canal non sécurisé.
   - Bob tire au hasard $y \in \{0, \cdots, p-1\}$ (et le garde secret), calcule $\beta = [p+1+p^2\mathbb{Z}]^y$ et l'envoie β à Alice via un canal non sécurisé.

   On demande :
   (a) Comment Alice et Bob déterminent une clé commune à partir de ces échanges (piste : binôme de Newton : $(x+y)^n = \sum_{i=0}^{n} C_n^i x^i y^{n-i}$ et $C_n^i = \frac{n!}{i!(n-i)!}$) ?
   (b) Montrez qu'une attaquant passif (qui n'intervient pas dans les échanges) est capable de déterminer facilement (en temps polynomial) la clé commune.
   (c) Qu'en déduisez-vous ?

Question 5
Considérons le système de chiffrement symétrique suivant. Pour chaque message M choisi de façon aléatoire dans l'espace $\{00, 01, 10\}$,

Question 6 :

$m = (m_1, m_2)$



$c = (c_1, c_2)$

Figure 4.2 A three-round Lai-Massey scheme