Partie I : Théorie

Question 1

1. Détailler 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 à clé publique. Explicitez votre raisonnement au cas d'El Gamal. Un esprit de synthèse est demandé.

Question 2

Donner les enjeux de la cryptographie moderne. Décrivez le principe des algorithmes de chiffrement par substitution (mono-alphabétique et polyalphabétique) et par transposition. Expliquez en quoi ces deux principes de chiffrement sont à la base de la conception des algorithmes de chiffrement modernes. Explicitez votre réponse sur l'algorithme DES. Expliquez l'intérêt des réseaux de Feistel.

Partie II : Exercices

Question 3

Cette question concerne le RSA de Takagi. Il s'agit d'un RSA classique dans lequel le module RSA est le produit d'une puissance d'un nombre premier et d'un autre nombre premier. Considérons les nombres premiers $p = 5$, $q = 7$ et dénotons par $n = p^2 \cdot q$ le module RSA de notre système. Dénotons par Φ la fonction totient d'Euler.

1. Calculer le module RSA n et $\Phi(n)$.
2. Parmi les nombres 12 et 31, déterminer ceux qui satisfont les hypothèses d'exposant de signature et pour ceux-la calculer l'exposant de vérification correspondant.

3. Signer le message 19 pour le(s) exposant(s) retenu(s) au point précédent. Utiliser la méthode la plus efficace que vous connaissez.

Question 4

On souhaite factoriser $n = 77$ par la méthode de Dixon en utilisant la base $\{2, 3, 5, 7\}$. On supposera dans l'exercice que le générateur aléatoire fournit les nombres $\{10, 35, 12, 14, 19, 26\}$. 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

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. Montrer que $(G, *)$ est un groupe (d'ordre p).
3. Montrer que $[p + 1 + p^2\mathbb{Z}]$ est un générateur de G.
4. Pout tout $n = 0...p-1$, donner le représentant minimal de la classe obtenue via le calcul de $[p+1+p^2\mathbb{Z}]^n$. (piste : binôme de Newton : $(x+y)^n = \sum_{i=0}^{n} C_n^i x^i y^{n-i}$ et $C_n^i = \frac{n!}{i!(n-i)!}$). Déduire de votre formule que l'application

$$\Gamma : \{0, \cdots, p-1\} \to G : n \mapsto [p + 1 + p^2\mathbb{Z}]^n$$

est une bijection.

5. 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 ?

(b) Montrer qu'une attaquant passif (qui n'intervient pas dans les échanges) est capable de déterminer facilement (en temps polynomial) la clé commune (piste : déterminer Γ^{-1}). Comment s'appelle l'application Γ^{-1} ?

(c) Qu'en déduisez-vous ?

Question 6

Considérons le système de chiffrement symétrique suivant. Pour chaque message M choisi de façon aléatoire dans l'espace $\{00, 01, 10\}$, 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. Donner le mécanisme de déchiffrement.
2. Calculer l'information mutuelle entre le message et le chiffré. (piste : $I(X,Y) = I(Y,X)$ où $I(\cdot,\cdot)$ est l'information mutuelle). Exprimer votre réponse en terme de rationnels et valeurs $log_2(k)$ où les k's sont des naturels non-nuls. Simplifier 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.

Examen M2 SeCReTS 2014-2015 : "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.