X

Examen M2 SeCReTS 2010-2011 : "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-verso (A4) avec vos notes est autorisée (écriture sur les lignes).
- La durée de l'examen est de trois heures.

Partie I : Théorie

Question 1

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)

Question 2

Expliquez les principes de conception des fonctions de hachage. Donnez les critères de sécurité et une attaque essayant de mettre en défaut un de ces critères. Montrez le résultat mathématique sur lequel vous vous basez et expliquez les conséquences sur les paramètres d'une fonction de hachage. Finalement, expliquez une application des fonctions de hachage en cryptographie.

Partie II : Exercices

Question 3

Alice et Bob souhaitent partager une clé commune. Pour ce faire, ils utiliseront le protocole de Diffie-Hellman. Nous travaillerons dans le groupe multiplicatif $\mathbb{Z}_{17}^*$. On utilisera comme générateur α, la classe de représentant 5.

- Si Alice choisit le secret 4 et Bob 11 calculez les différentes valeurs intervenant dans le protocole. Décrivez précisément les étapes du protocole.
- Placez-vous du coté de l'attaquant. Spécifiez les valeurs publiques intervenant dans le protocole ci-dessus. En utilisant ces valeurs, calculer la clé commune via l'algorithme du calcul d'indice avec la base {2,3,5}.

Pour chaque étape, il est demandé d'utiliser un algorithme efficace et de le mentionner. Si vous ne vous rappelez plus d'un algorithme, vous pouvez faire le calcul de façon intuitive pour pouvoir continuer mais les points associés seront nettement moindres.

Question 4

Supposons qu'Alice souhaite générer des signatures au moyen de l'algorithme de signature DSS (DSA). Pour cela, Alice génère une clé publique (ensemble de valeurs) et une clé privée que l'on dénote x (valeur unique). L'algorithme DSS est un algorithme probabiliste (plusieurs signatures sont possibles pour un même message). En particulier, Alice doit générer une nouvelle valeur k aléatoire à chaque signature de message.

L'algorithme est le suivant :

Générations des clés

- Choisir un nombre grand premier p,
- Choisir un nombre grand premier q de telle façon que $q \mid p-1$,
- Soit α un générateur du sous-groupe cyclique de $\mathbb{Z}_p^*$ d'ordre q (il suffit de choisir un générateur g de $\mathbb{Z}_p^*$ et de poser $\alpha = g^{\frac{p-1}{q}} \bmod p$),
- Choisir $x \in_R \{2, \cdots, q-1\}$

- Calculer $y = \alpha^x \bmod p$.
- La clé publique est (p, q, g, y). La clé privée est x

Signature

Pour signer un message $m \in \{0,1\}^*$.

- Choisir un nombre aléatoire $k \in_R \{1, \cdots, q-1\}$ (gardé secret),
- Calculer $r = (\alpha^k \bmod p) \bmod q$. Si cette valeur est nulle , il faut choisir un autre k,
- Calculer $s = k^{-1}(H(m)+x \cdot r) \bmod q$, où $H(m)$ est le résultat d'un hachage cryptographique sur le message m et $H(m) \in \mathbb{Z}_q$. Si cette valeur est nulle , il faut choisir un autre k.
- La signature est (m, r, s).

On demande :

- Montrer que si Alice souhaite gagner du temps et utilise la même valeur k pour la signature de deux messages différents alors un pirate est capable, uniquement sur base de données publiques, de retrouver avec une grande probabilité la clé secrète "x" d'Alice en temps polynomial.

Question 5

Considérez les nombres premiers $p = 5$ et $q = 11$. Dénotons par Φ la fonction totient d'Euler.

1. Calculez le module RSA (que l'on dénotera n) et $\Phi(n)$.
2. Parmi les nombres 4 et 17, determinez ceux qui satisfont les hypothèses d'exposant de chiffrement et pour ceux-la calculez l'exposant de déchiffrement correspondant.
3. Chiffrez le message 19 pour le(s) exposant(s) retenu(s) au point précédent.
4. Déchiffrez le message 23. Utiliser la méthode la plus efficace que vous connaissez.

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.