MP2 - Cryptographie et applications

13 février 2018 - une feuille manuscrite autorisée - durée - 2h

Questions de cours:

a. Quels sont les avantages du chiffrement à clé secrète par rapport au chiffrement à clé publique, donner des exemples d'algorithmes.

b. Expliquer pourquoi si on utilise du chiffrement à flot, réutiliser le même flot quasi-aléatoire sur différents message est une mauvause idée.

c. Est-ce que la factorisation est un problème difficile à résoudre ? Comparer ce problème à la résolution du problème du log discret sur un anneau de type Z/nZ ou sur des courbes elliptiques.

d. Quelle est la compexité de la meilleure attaque connue sur le problème du logarithme discret sur les courbes elliptiques sur un corps avec de l'ordre de 2^n élément en fonction de n, et ce pour le cas d'un ordinateur classique et aussi dans le cas d'un oridnateur quantique suffisamment puissant.

e. Quelle est la difference entre signer et hacher ?

f. On utilise souvent la compression de données pour le stockage d'informations. Supposons qu'on veuille compresser des données avec du chiffrement. Est-ce qu'il vaut mieux chiffrer et puis compresser ou le contraire ?

Exercice 1 (Cryptographie à clé publique):

a) on souhaite faire signer un document par n personnes. Comment peut-on s'y prendre ? Donnez une solution et analysez ses points forts/faibles en vous aidant des points suivants:longueur de la cle, longueur de la signature , importance de l'ordre des signataires , et si l'un des signataires triche ?

b) on suppose maintenant que lors de ses vacances (d'une durée fixe) un responsable souhaite déléguer sa signature électronique á son adjoint. Comment peut-il s'y prendre ? Proposer un cadre réaliste et proposer une solution. Bien sur l'adjoint doit pouvoir signer à la place du responsable mais sans que le responsable donne sa clé secrete.

Exercice 2 (Cryptographie à clé secrete):

On suppose qu'Alice et Bob partagent une clé aléatoire K dans $\{0,1,2\}$ et que Alice veut envoyer un message M de $\{0,1,2\}$.

a. On suppose tout d'abord qu'elle procède en convertissant K et M en ensembles de deux bits (00,01,10) et qu'elle fait un XOR entre les deux representations binaires. Montrer qu'un tel schéma n'est pas bon, en ce sens qu'il y a de l'information qui fuit et que ce schéma n'est pas parfaitement sur. On pourra montrer que tous les chiffrés c_1, c_2 (où c_i est un bit) n'ont pas la même probabilités d'exister.

b. Proposer un autre schéma à base de modulo qui serait parfaitement sur.

Exercice 3 (Calcul de la signature RSA par les restes chinois):

On considère un module RSA, $n = pq$ et d l'exposant privé. Soit un m un message à signer, on cherche à calculer $S = m^d \pmod n$. On note $d_p = d \pmod{p-1}$, $d_q = d \pmod{q-1}$ et $i_q = q^{-1} \pmod p$. Soient $S_p = m^{d_p} \pmod p$ et $S_q = m^{d_q} \pmod q$.

a. Rappeler le thèoreme des restes chinois, montrer que $S \pmod p = S_p$ et $S \pmod q = S_q$, expliquer alors pourquoi on peut retrouver S à partir de S_p et S_q.

b. Montrer que $S = S_q + q(i_q * (S_p - S_q) \pmod p))$.

c. Expliquer l'intérêt (en terme de cout calculatoire) de calculer S par cette méthode plutôt que directement par en calculant $m^d \pmod n$?

Exercice 4 (Chiffrement):

Etant donnés deux protocoles pour lesquels l'envoyeur procède de la manière suivante:

Protocole A:

$$y = e_{k_1}(x||H(k_2||x)),$$

où x est le message, H est une fonction de hachage comme SHA-1, e est un algorithme de chiffrement à clé symétrique, "||" est la concaténation, et k_1 et k_2 des clés secrètes connues seulement de l'emetteur et du receveur.

Protocole B:

$$y = e_{k_1}(x||sig_{k_{pr}}(H(x))),$$

où k est une clé partagée et k_{pr} est la clé privé de l'emetteur.

a) Donner une description étape par étape, de ce que le receveur doit faire en recevant y pour retrouver le message.

b) Préciser en les justifiant si les propriétés suivantes sont vérifiées pour chacun des protocoles:
confidentialité, intégrité , non répudiation.

Exercice 5 (Schéma de signature de Lamport à usage unique)

On considère le schéma de signature suivant. On suppose qu'on a une fonction de hachage f qui renvoie des hachés de longueur n. On va maintenant expliquer comment on peut signer un message m de longueur k: $m =$

$(m_1, m_2, \cdots, m_k)$ avec $m_i \in \{0,1\}$ à partir de f. Pour $1 \leq i \leq k$ et $j \in \{0,1\}$ on prend $2k$ valeurs aléatoires y_{ij} de longueur k. Et on calcule $z_{ij} = f(y_{ij})$. Les $2k$ z_{ij} forment la clé publique et les $2k$ y_{ij} sont la clé secrète. Pour signer un message $m = (m_1, m_2, \cdots, m_k)$ de k bits, on a:

$$Signature(m) = (y_{1m_1}, y_{2m_2}, \cdots, y_{km_k}) = (s_1, \cdots, s_k)$$

a. Calculer pour $n = 256$ et $k = 80$ les tailles des clés publiques et privées. Comparer aux tailles de clés pour RSA ou DSA.

b. Expliquer comment de manière plus générale on pourrait signer des messages de taille quelconque en utilisant le protocole précédent.

c. Justifier que pour 1 seule signature la sécurité du schéma repose sur la sécurité de la fonction de hachage f.

d. Peut-on prendre k petit pour le protocole, par exemple $k = 1$ ou 2 ?

e. Montrer qu'en prenant une attaque à message choisis en deux signatures pour 2 messages choisis on peut recupérer toute la clé publique. Justifier du coup la notion d'usage unique pour ce protocole.

f. En fait ce protocole peut être couplé avec un algorithme (de Merkle) uniquement à base de fonction de hachage qui permet de signer un nombre quelconque de fois mais fixé à l'avance. Quel est l'intérêt de ce type protocole par rapport aux protocoles classiques de théorie des nombres cités plus haut ?

Exercice 6 (Cryptographie basée sur l'identité)

a) Rappeller les grandes propriétés des couplages (pairings) utilisées pour la cryptographie. Donner 3 applications des couplages en cryptologie.

b) Rappeler la définition d'un schéma de chiffrement basé sur l'identité.

c) Définir en généralisant la définition du b), la notion de signature basée sur l'identité et d'authentification basée sur l'identité.

d) Alors que trouver des schémas de chiffrement basés sur l'identité est un problème difficile, montrer qu'il est très facile de construire de manière gènèrique (ie: à partir d'un schéma quelconque de signature) des protocoles de signature et d'authenfication basés sur l'identité.