

MP2 - Cryptographie et applications

12 novembre 2008 - une feuille manuscrite autorisée

Questions de cours:

- Quels sont les avantages du chiffrement à clé secrète par rapport au chiffrement à clé publique, donner des exemples d'algorithmes.
- Expliquer pourquoi si on utilise du chiffrement à flot, réutiliser le même flot quasi-aléatoire sur différents message est une mauvaue idée.
- 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.
- Comment doit-on procéder pour échanger de façon optimale en temps avec qq'un une grande taille de données chiffrées, sans avoir de clé secrete partagé au préalable ?
- Quelles sont les grandes propriétés qu'on attend d'une fonction de hachage ?

Exercice 1 (Cryptographie à clé publique):

Soit $N = pq$ un module RSA. Soit $g \in [0, N^2]$ un entier vérifiant $g = aN + 1 \pmod{N^2}$ pour $a \in Z_N^*$. On considère le schéma de chiffrement suivant. La clé publique est (N, g) . Pour chiffrer un message $m \in Z_N$ on procède de la façon suivante: (1) on prend un h aléatoire dans $Z_{N^2}^*$ et calculer $C = g^m \cdot h^N \pmod{N^2}$. On veut trouver un algorithme de déchiffrement.

- Montrer que le problème de log discret en base g est facile dans ce cas. C'est a dire montrer que pour un g donné et $B = g^x \pmod{N^2}$ il existe un algorithme efficace pour retrouver $x \pmod{N}$. Utiliser le fait que $g = aN + 1$ pour un $a \in Z_{N^2}^*$.
- Montrer que pour g donné ainsi que la factorisation de N , déchiffrer $C = g^m \cdot h^N \pmod{N^2}$ peut être fait efficacement. (Indice: considérer $C^{\phi(N^2)} \pmod{N^2}$, utiliser le fait que que d'après le thm d'Euler $x^{\phi(N^2)} = 1 \pmod{N^2}$ pour tout $x \in Z_{N^2}^*$).
- Montrer qu'on peut reconstruire certains messages. Plus précisément: soient a, b , des entiers de $[1, N]$, montrer qu'étant donné N, c ainsi que le chiffré de a et b , il est possible de construire le chiffré de $a + b$ et le chiffré de $c \cdot a$.

Exercice 2 (Clé secrète) :

On considère le schéma utilisant 3 DES mais 2 clés k_1 et k_2 : $E_{k_1}(E_{k_2}(E_{k_2}(m)))$. (L'ordre des clés a été modifié par rapport au TDES classique). Montrer comment on peut attaquer ce schéma avec une attque de type meet-in-the-middle.

Exercice 3 (Cryptographie à clé publique):

a. On suppose que A et B utilise le même module RSA n avec deux clés publiques e_A et e_B premières entre elles. On suppose que C envoie le même message chiffré m^{e_A} et m^{e_B} à A et B. Montrer que E qui écoute les communications peut retrouver facilement alors le message m .

b. Afin d'améliorer la sécurité des messages Bob choisit deux exposants e_1 et e_2 et demande à Alice de chiffrer d'abord son message par e_1 , pour obtenir $c_1 = m^{e_1}$ puis de rechiffrer par e_2 pour obtenir $c_2 = c_1^{e_2}$. Et d'envoyer c_2 . Est-ce que ce double chiffrement améliore la sécurité. Si oui pourquoi, si non pourquoi.

Exercice 4 (LFSR):

On intercepte un message chiffré avec un système de chiffrement à flot produit par une suite chiffrante récurrente de type LFSR.

Le message binaire intercepté est: 0000011011110010

On sait d'autre part que les six premiers bits du message clair sont 110101. On admet que la complexité linéaire de la suite chiffrante du LFSR est au plus 3.

Déchiffrer le message en entier.