2e année

DAPM

Examen D34: 2ème session

Juillet 2015

Aucun document n'est autorisé. Toutes les réponses doivent être justifiées.

Exercice 1. Attaques par canaux cachés (4pts)

1. Définir les caractéristiques et les motivations d'une attaque passive puis d'une attaque active.
2. Une attaque passive peut-elle être exécutée sur une de signature RSA? Quel serait le but? Une telle attaque a-t-elle un intérêt dans le cas de la vérification de la signature?

Exercice 2. Comparaison multiplication/carré (2pts)

Le but de l'exercice est de comparer le coût de la multiplication et de l'élévation au carré de polynômes à coefficients réels. On représentera le coût d'une multiplication (resp. d'une élévation au carré) de coefficients par `m` (resp. `s`).

1. On considère l'algorithme de multiplication standard. Quel est le coût d'une multiplication et d'une élévation au carré de polynômes de degré 1? Même question pour des polynômes de degré 2.
2. Quelle est le coût de ces opérations pour des polynômes de degré n? En déduire qu'un carré est asymptotiquement deux fois moins coûteux qu'une multiplication.

Exercice 3. Algorithme de Karatsuba (4pts)

1. On considère deux entiers de n bits $A = A_1 2^{\frac{n}{2}} + A_0$ et $B = B_1 2^{\frac{n}{2}} + B_0$ (on admettra que n est pair). Rappeler l'astuce de Karatsuba pour effectuer la multiplication de A part B en seulement 3 multiplications d'entiers de $\frac{n}{2}$ bits. Quelle est la complexité de l'algorithme complet?
2. Appliquer de façon détaillée l'algorithme de Karatsuba aux polynômes $X^3 + X^2 + X + 2$ et $X^3 - X^2 - 1$.

Exercice 4. Réduction modulaire (3pts)

1. Décrire la procédure permettant de réduire un entier A de $2n$ bits modulo $p = 2^n - 1$ en au plus 2 additions d'entiers de n bits.
2. Montrer que 999999999 divise 12345678987654321.

Exercice 5. Représentation de Zeckendorf (4pts)

On rappelle la définition de la suite de Fibonacci (F_n): $F_0 = 0, F_1 = 1, \forall n \geq 2, F_n = F_{n-1} + F_{n-2}$. On admettra que tout entier k peut se représenter comme somme d'éléments de la suite de Fibonacci. Ex: $19 = 13 + 5 + 1 = F_7 + F_5 + F_2$. On adoptera une représentation binaire pour décrire un entier donné sous cette forme (on pourra omettre F_0 et F_1). Ex $19 = (101001)_{\mathcal{F}}$. Dans la suite de l'exercice, x est un élément de groupe G quelconque.

1. Soit $n \geq 2$. Décrire un algorithme simple permettant de calculer x^{F_n} en effectuant une élévation au carré et $n - 4$ multiplications.
2. En déduire un algorithme type `double-and-add` (droite à gauche) pour calculer x^k, où $k = (k_{l-1} \dots k_0)_{\mathcal{F}}$.

Exercice 6. Algorithme de Montgomery (1pt)

1. Décrire les étapes de l'algorithme de Montgomery pour le calcul de $[71]P$, où P est un point sur une courbe elliptique quelconque.

Exercice 7. Bases Doubles (2pts)

1. Convertir l'entier 247 en base double chaînées.
2. Décrire les étapes de l'algorithme de multiplication de point `cBDNS` pour le calcul de $[247]P$.