Développement Logiciel Cryptographique

Examen de session 1

Février 2016

Préambule

Les supports de cours de l'UE Développement Logiciel Cryptographique **sont les seuls documents autorisés** pour cet examen.

L'usage d'une calculatrice est autorisé.

1 Quizz [7 points]

1. Pour calculer un logarithme discret, quel est le principal avantage de la méthode *rho* de POLLARD sur la méthode *baby step - giant step* ?
2. Quelle peut être la taille du produit d'un entier de n_1 bits par un entier de n_2 bits ? Justifiez votre réponse.
3. Il est parfois laissé à l'utilisateur la possibilité de choisir la valeur de l'exposant public de sa clé RSA. A-t-il totale liberté dans le choix de cet élément de clé ? Si vous pensez que non, quelles sont selon vous les restrictions, et pourquoi ?
4. Il est souvent considéré que l'exposant privé d'une clé RSA est *full size*. Que signifie ce terme, et pourquoi s'applique-t-il à cet élément de clé ?
5. Dans l'attaque SQUARE à 4 tours, expliquez pourquoi il peut être intéressant d'utiliser deux λ-sets plutôt qu'un seul.
6. Pour quelle raison est-il dangereux d'utiliser un module RSA égal au produit d'un premier p de 800 bits par un premier q de 224 bits ?
7. Laquelle des deux méthodes, celle de GAUSS ou celle de GARNER, est-elle la plus adaptée au déchiffrement en mode CRT en environnement contraint ? Expliquez pourquoi.

2 Bibliothèque GMP [6 points]

1. La fonction `mpz_probab_prime_p(const mpz_t n, int reps)` permet de tester la primalité de l'entier `n`.

   a) Expliquez pourquoi il est déconseillé de générer un nombre premier avec l'implémentation suivante :

```
do
    mpz_urandomb(z_n, prng, bit_size);
while (mpz_probab_prime_p(z_n, 5) != 2);
```

   b) Dans quelle situation adopter cette implémentation ne présente aucun problème ?

2. Écrivez en langage C une fonction qui calcule la valeur de $a^k \bmod n$ (où a et n sont deux grands entiers) par la méthode *square and multiply* de droite à gauche.

3 Génération de premiers [7 points]

1. Quel "degré de confiance" atteint-on lorsqu'on teste la primalité d'un entier par la méthode de Miller-Rabin avec 5 itérations ?

2. Expliquez de manière claire et précise comment il faut comprendre la notion de "degré de confiance" de la question précédente.

3. On suppose une génération de premiers consistant à répétitivement tirer au hasard un entier n de r bits et à en tester la primalité par un test de Miller-Rabin à 5 itérations. On considère que le temps mis pour générer un premier de cette manière est essentiellement dominé par les exponentiations modulaires. Sachant que la densité des premiers autour de x est bien approximée par $1/\ln x$, évaluez :

   a) le nombre total moyen d'itérations effectuées pour générer un premier de $r = 512$ bits,

b) le rapport entre le temps moyen nécessaire pour générer des premiers de $r = 1024$ bits, et celui nécessaire pour générer des premiers de $r = 512$ bits.

4. Est-il possible qu'un nombre de CARMICHAEL soit identifié comme étant composé lorsqu'on utilise le test de FERMAT ? Justifiez votre réponse.

5. Même question pour le test de MILLER-RABIN.

6. Étant donnée une base choisie aléatoirement, une itération du test de FERMAT est-elle plus rapide ou plus lente qu'une itération du test de MILLER-RABIN ? Justifiez votre réponse.