Composition de Cryptographie - 2010

Il est recommandé aux élèves de bien choisir l'ordre des questions selon leurs compétences et rapidités.

Si l'élève n'arrive pas à faire une démonstration, il peut considérer que le résultat de la démonstration est admis sur le reste l'exercice.

Le support de cours et les calculatrices sont permis.

1. Génération clé RSA

Soit à générer une clé RSA de 2048 bits.

a) Rappeler la définition de la taille d'une clé RSA (2 lignes)
b) Rappeler le schéma général d'une génération d'une clé (5 lignes)
c) Lors de la génération par OpenSsl de clés de 2048 bits, on remarque la génération de clés de 2047 bits. (problèmes aux limites).
    i. Comment améliorer le schéma en b pour détecter ce genre de génération (2 lignes) (amélioration à postériori)
    ii. Comment améliorer le schéma en b pour éviter ce genre de génération (2 lignes) (amélioration à priori)

2. Implémentation DES électroniquement

Implémenter la fonction FRK du DES en utilisant des composants électroniques.

3. Générateur Aléatoire

On implémente un générateur pseudo aléatoire en utilisant

Xn = SHA256(Xn-1)

a) Quelle est la taille L en octets en sortie de ce générateur ?
b) On désire générer un nombre dont la taille est égale à la taille en sortie de ce générateur. Pour quelle raison principale il ne faut pas prendre tous les octets obtenus en sortie de ce générateur, mais un bit ou un octet ?

4. Accélération particulière de la réduction RSA

Nous allons étudier le cas où le modulo sous le format $N = 2^m - k$ avec taille de k = ¾ de la taille de N. Soit à calculer M mod (N). M s'écrit sous la forme $M= A*2^m + B$ et A est de la taille de ¼ de N. (M a la taille de 1,25 de N)

a) Quelle est la valeur particulière du début de N ?
b) Sur quelle taille maximale est cette valeur particulière du début de N ?
c) Calculer M' = M – A*k en faisant apparaître N
d) A partir de la valeur M' + A*k déduire que M mod (N) = B + A*k
e) Comparer le temps d'exécution de cette réduction par rapport à une réduction directe M mod N?

5. Accélération du RSA par sauvegarde de réponses intermédiaires

Soit à calculer une signature M' = M pow(S) mod (N). Cette méthode consiste à utiliser une table de recherche.
pow dénote la fonction à la puissance ; M pow (i) est équivalent à M^i .

S sera présenté par une succession de bits de taille constante et est noté

$S = \Sigma (d_i * m^i)$ $0 \leq i < t$

Où $0 \leq d_i \leq m$ et m est un multiple de 2

La table de recherche est constituée des puissances de M : M, M pow(2), M pow(3),… M pow(m)

a) Quelle est la relation entre la taille n de S, t et m ?
b) On note y_0 = M pow(d_t). Calculer y_1 = (y_0 pow(m)) * M pow(d_{t-1}) .
c) Calculer y_2 = (y_1 pow (m)) * M pow(d_{t-2}) .
d) Par récurrence calculer y_t en fonction de M, S et N.
e) En fixant m = 16, modifier la routine fastexp pour implémenter cette méthode appelée fastexp16.
f) Comparer les performances de fastexp16 par rapport à fastexp.

Nous rappelons que l'implémentation de fastexp est la suivante :
si S = $S_n S_{n-1} .. S_0$ avec S_n, S_{n-1}. . S_0 représentent les bits de S.
Sn est le bit le plus significatif et S0 est le bit le moins significatif.

```
Début
    X :=  M.
    Si   S0  =1   alors Y :=X
    Sinon          Y := 0
     Pour (i = 1;  i  < n; i++)
    {
          X= X*X mod (N)
          Si Si=1 alors   Y = Y*X  mod(N)
    }

    M' := Y.
Fin.
```

6. Questions à choix unique

Mettre le numéro de question ainsi que sa réponse (a, b ou c). Dans le cas d'une réponse « Faux » ou « Parfois », la justifier ou la corriger.
La réponse « Parfois » peut indiquer que les cas évoluent de rarement à souvent.

Question	**a**	**b**	**c**
1. Un certificat autosigné est un certificat d'autorité.	Vrai	Faux	Parfois
2. Un certificat d'autorité est un certificat autosigné	Vrai	Faux	Parfois
3. Une PKI nécessite l'utilisation de certificats	Vrai	Faux	Parfois
4. Sur un serveur l'état en temps réel d'un certificat se fait en testant s'il est en CRL	Vrai	Faux	Parfois
5. Une PKI est une autorité de certification	Vrai	Faux	Parfois
6. Les bits de poids fort de chaque octet d'une clé DES doivent être testés	Vrai	Faux	Parfois
7. Les bits de poids faible de chaque octet d'une clé AES ne doivent pas être testés	Vrai	Faux	Parfois
8. RSA est le seul algorithme asymétrique	Vrai	Faux	Parfois
9. Diffie Helman est uniquement utilisé pour l'échange des clés	Vrai	Faux	Parfois
10. Un nombre aléatoire ne doit pas être prévisible	Vrai	Faux	Parfois
11. Le mode PKCS1 est utilisé pour la signature	Vrai	Faux	Parfois
12. Le mode PKCS1 est utilisé pour le chiffrement	Vrai	Faux	Parfois
13. L'algorithme de hash le plus sûr	SHA1	MD5	SHA512
14. En doublant la taille d'une clé RSA, le temps d'exécution de la signature augmente de	2	4	8
15. Le certificat du destinataire est utilisé pour signer un document qui lui est envoyé	Vrai	Faux	Parfois
16. L'émetteur utilise la clé publique du destinataire pour lui transmettre une clé de session	Vrai	Faux	Parfois
17. Le mode CBC est utilisé en RC4	Vrai	Faux	Parfois
18. SHA256 n'a aucun mode d'utilisation	Vrai	Faux	Parfois
19. SHA256 peut être utilisé pour l'authentification	Vrai	Faux	Parfois
20. AES peut être utilisé pour l'authentification	Vrai	Faux	Parfois