Composition de Cryptographie - 2006

La composition est décomposée de 3 exercices.

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. Caractéristique DES et Applications (12 points)

Soit x un bit, /x est l'inverse de x càd /x= b XOR 1
Soit X une donnée de 8 octets /X est l'inverse de X çàd : /X = X XOR (FF FF FF FF FF FF FF FF).

Notons :

$$X = \sum_{i=0}^{i=n-1} x_i * 2^i \quad \text{et} \quad /X = \sum_{i=0}^{i=n-1} /x_i * 2^i$$

$$X \ XOR \ Y = \sum_{i=0}^{i=n-1} x_i \ XOR \ y_i * 2^i$$

Soit P une fonction de permutation appliquée à X :

$$P(X) = \sum_{i=0}^{i=n-1} x_{f(i)} * 2^i$$

avec f(i) est fonction de la position du bit et f(i) ≠ f(j) pour i ≠ j et 0≤ f(i) ≤ n-1

K est la clé DES de chiffrement.

a) Démontrer P(/X) = /P(X) (2 lignes)
b) Démontrer que quelque soit i, les clés intermédiaires de /K sont les inverses des clés intermédiaires de K (5 lignes).
c) Démontrer quel a fonction élémentaire du DES FRK(/R, /Ki) = FRK(R, Ki)
d) Démontrer si DES(M, K) = M' ⇔ DES(/M, /K) = /M' (il suffit de démontrer pour le premier étage, déduire pour les autres étages par récurrence)
e) Calculer L0R0 = IP(AA AA AA AA AA AA AA AA). Déduire sans calcul : IP(55 55 55 55 55 55 55 55)
f) Pour K1 (clé intermédiaire premierétage) = 55 55 55 55 55 55, calculer FRK(R0, K1). Déduire sans calcul FRK(/R0, AA AA AA AA AA AA).

2. Utilisation la signature PKCS7 dans une application de notaire électronique (12 points)

On désire utiliser les services d'un notaire électronique pour la notarisation de contrats établis entre diverses parties.

a) Quand un document est déposé chez un notaire (du monde réel) quelles sont les opérations réalisées par le notaire sur le document papier ?
b) A partir des réponses du point a, transposer dans le monde électronique les techniques que le notaire doit réaliser sur un document.
c) Les signatures (hors signature du notaire) sur le contrat doivent être des co-signatures ou des signatures hiérarchiques (sur-signatures) ?
d) La signature électronique du notaire doit être une co-signature ou une signature hiérarchique (sur-signature) ? Pour quelle raison ?
e) A partir des techniques décrites dans le point b et à partir de la définition de la signature PKCS7 avec attributs authentifiés, quels sont les attributs (noms et oid) à être utilisés pour la signature PKCS7 du notaire ? (se référer au cours partie pkcs9)
f) En supposant que la date de notarisation est le Premier Avril 2006 à 12 heures 50 min 10 s, écrire la zone DER de l'attribut date.
g) En supposant que le hash de type MD5 du contrat est 12 34 56 78 9A BC DE F0 12 34 56 78 9A BC DE F0, écrire la zone DER de l'attribut hash.
h) En supposant que le certificat a été livré par l'autorité « ESIB – MASTER SECURITE », que la référence du certificat est FA BC, que la signature RSA/PKCS1 est sur 128 octets et vaut XXXXXXX ….XX, écrire la zone DER correspondant à SignerInfo.

3. Format des exposants privés RSA pour certaines valeurs de Modulo (6 points)

Les relations suivantes seront utilisées pour RSA:

- N = p*q avec p et q premiers
- S * V = 1 mod ((p-1)(q-1)) / (pgcd(p-1)(q-1)); /* Formule générale*/
- p = 2*p'+1 et q = 2*q'+1, p' et q' premiers

où S, V et N sont respectivement l'exposant privé, l'exposant publique et le modulo.

a) calculer pgcd((p-1)(q-1))
b) Ecrire S *V sous la forme de k * a + b
c) Ecrire S * V sous forme d'approximation sur les grands nombres en utilisant N et k
d) D'après l'approximation déduire S en fonction de N, k et V
e) Pour k = 1 et N commençant par FF FF FF FF FF FF, déduire le format du début de S pour V = 3 et V = 0x10001.
f) Est-ce que on peut faire varier k pour avoir d'autres valeurs de S ? (appliquer pour v=3 différentes valeurs de k).