Composition de Cryptographie - 2007

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 des exposants privés RSA pour formats prédéfinis de valeurs de Modulo

Les relations suivantes seront utilisées pour RSA:

- N = p*q avec p et q premiers

Lors d'un audit d'une autorité de certification il s'est avéré que le modulo de 1024 bits est de la forme 0xFF,'T','o','t','o','D','U','P','O','N','T',0xBA,……..0x55

a) Quelle est la probabilité d'avoir la chaîne 'T','o','t','o','D','U','P','O','N','T' apparaissant d'une façon aléatoire ?
b) Quelle autre raison syntaxique laisse à penser que cette chaîne n'a pas été le résultat d'un tirage aléatoire ?
c) Rappeler le en quelques lignes le procédé de tirer p, q et d'aboutir à N.
d) Modifier brièvement le procédé précédent pour générer des clés RSA avec modulos de formats prédéfinis de style 0xFF,'T','o','t','o','D','U','P','O','N','T', …….

2. Accès à un octet dans le cas d'un fichier accès aléatoire chiffré CBC

Une fichier de taille N est chiffré par AES-128 en mode CBC par une clé K et un vecteur d'initialisation IV.

a) Ecrire l'équation du bloc chiffré B'_n (n étant le nième bloc) en fonction de B_n, K, IV, B'_{n-1} ?
b) On désire accéder à un octet de position j du fichier d'une façon aléatoire. Quelle est la relation qui lie la position de l'octet (à savoir j) au numéro du bloc auquel il appartient (par exemple m).
c) Est-ce qu'on a besoin de lire le fichier en entier pour pouvoir déchiffrer l'octet de position j ? Justifier. (deux lignes)
d) On veut changer la valeur de l'octet en clair de position j . Ecrire les opérations nécessaires pour re-chiffrer l'octet et le bloc auquel il appartient et en prenant en compte la conséquence de la modification de l'octet.
e) Est-ce que le mode CBC est adapté à des fichiers en accès aléatoire ?

3. PKCS7 et ASN1

Une application a besoin d'utiliser des enveloppes pkcs7 et implémentant les services de sécurité suivants : Confidentialité et Non Répudiation.

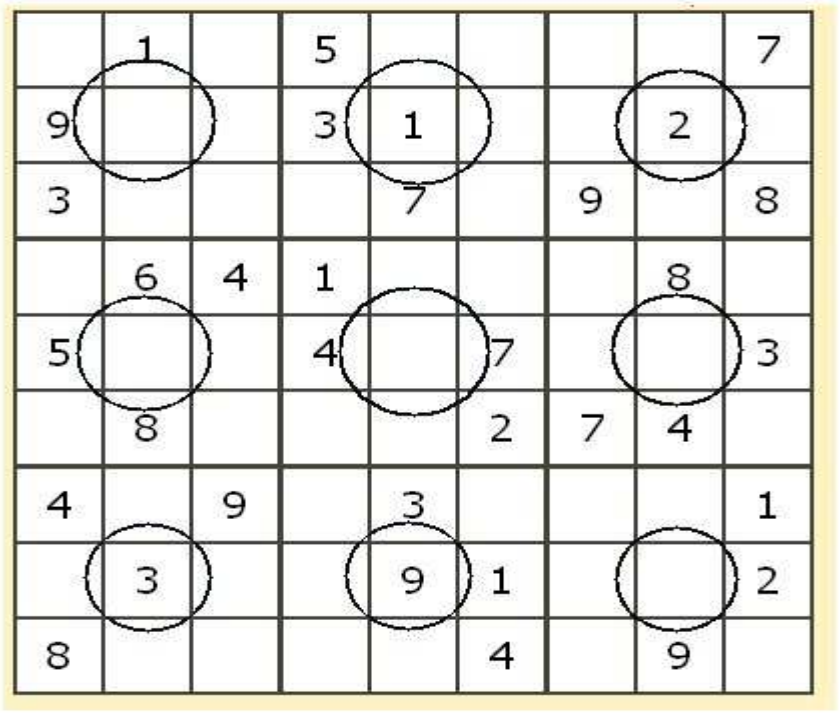
a) Quelles sont les deux possibilités d'enveloppes et combinaisons d'enveloppes possibles pour aboutir à ces services ? (2 lignes)
b) Décrire les avantages et inconvénients de chaque méthode. (5 lignes)
c) La non-répudiation est basée sur l'utilisation de l'algorithme RSA en mode PKCS V1.5, fonction de hash MD5, type de bloc 1. Sachant que la valeur hash (en hexa) est 01 23 45 67 89 AB CD EF 01 23 45 67 89 AB CD EF, écrire la valeur de la zone sur laquelle est appliquée la clé privée. L'oid du MD5 est 1.2.840.113549.2.5

4. Comment choisir parmi plusieurs certificats sur un même dispositif

Un dispositif de sécurité doit contenir trois certificats délivrés par la même autorité. Chaque certificat est à usage différent : signature, authentification et chiffrement de clés. Décrire deux méthodes différentes basées sur les divers paramètres X509 pour qu'une application puisse choisir directement un certificat pour un usage défini. (10 lignes maximum)

5. Sudoku et Stéganographie

Des espions s'échangent entre eux des messages chiffrés d'une façon ponctuelle en utilisant les grilles de Sudoku apparaissant dans des revues de sudoku comme clés de chiffrement d'une fonction XOR. On va supposer que seule la case du milieu de chaque carré de 3*3 est un chiffre de la clé (case entourée) et ceci après solution de la grille. Nous supposant que le message chiffré est transmis par un tuyau quelconque et non sujet de cet exercice.



dr

Chaque espion qui veut envoyer un message met dans un journal de publicité le numéro de la revue de sudoku RRRR, la page PP et le numéro de grille GG dans la page et ceci sous la forme d'un message innocent de type :
« Vos chiffres de chance sont : RR RR PP GG »
Le destinataire achète le journal et lit la publicité puis soit achète soit cherche dans son stock de revues.

a) Imaginer une méthode pour que l'espion destinataire puisse s'assurer que la publicité provient de son collègue.
b) Imaginer une méthode pour que les chiffres de la publicité soient moins clairs.
c) Quel est le nombre de clés possibles ?
d) En supposant que chaque chiffre de la clé chiffre un seul caractère du message, quelle est la taille maximale d'un message ?
e) Comment on peut chiffrer un message plus long ? Dans ce cas quelles sont les nombres de clés pour le message de taille maximal ?
f) Pour utiliser le Sudoku comme support stéganographique pour une clé AES hexadécimale, quelles sont les modifications à apporter au système précédent.