Sécurité des SI

TD4 (cryptographie)

Questions de cours :
quels sont les avantages et inconvénients du chiffrement asymétrique par rapport au chiffrement symétrique?
Vous utilisez un chiffrement symétrique avec des clés de 128 bits, quelle longueur de clé devez-vous choisir pour le chiffrement asymétrique (non elliptique)? Quelle fonction de hachage correspond à cette même sécurité?
Pourquoi le chiffrement doit-il être probabiliste? Donnez un exemple.
A quoi sert un certificat?
Quel est le principal intérêt de la cryptographie elliptique?

Exercices :

1) Ecrire un protocole qui utilise l'enveloppe digitale pour chiffrer mais qui en plus signe le message
2) Adaptative chosen-ciphertext attack on RSA encryption.
    1. Montrez que le chiffrement du produit de deux clairs est le produit des chiffrés.
    2. Soit m et c resp le clair et le chiffré. Soit A un adversaire. On suppose que A a accès à un oracle de déchiffrement et peut donc déchiffrer tout chiffré différent de c. Comment l'adversaire va-t-il faire pour retrouver le message?

3) RSA : Small encryption exponent. Supposons que la clé de chiffrement soit e=3 pour tout le monde mais chacun utilise un module différent. Une personne du groupe souhaite chiffrer un même message m pour l'envoyer aux autres (on suppose que les autres sont trois). Iwan, l'adversaire qui snif le réseau, obtient les trois chiffrés. Comment va-t-il retrouver m? Voyez-vous une solution pour éviter cette attaque tout en gardant la même clé?
4) Alice veut construire un protocole, à base de RSA, qui permette à Bob de signer un message sans que Bob ne puisse connaître le message ni la signature associée à m. L'idée est la suivante : Alice envoie le message camouflé à Bob. Bob le signe et le renvoie à Alice. A partir de cette signature, Alice peut calculer la signature de Bob sur le message m choisi par Alice dès le début. Les paramètres de RSA sont n=pq, la clef publique est (n, e) et la clef privée est d. Alice choisi un entier k premier avec n et considère une fonction qui permet de « camoufler » le message m : $f(m) = m.k^e \bmod n$ et une fonction de « décamouflage » : $g(m) = k^{-1}.m \bmod n$. Essayez d'aider Alice à la mise au point du protocole.
5) Attaque sur RSA. Soit m un message, n le module RSA, e la clé publique et c le chiffré (on a donc c=m^e mod n).

Le chiffrement RSA étant une permutation sur l'espace des messages {0, 1,2, ... , n-1}, il existe un entier positif k tel que c^{e^k}=c. Cette observation amène à une attaque "cyclique" du chiffrement RSA. Un adversaire calcule successivement c^e mod n, c^{e^2}mod n, c^{e^3}mod n,... jusqu'à obtenir c pour la première fois. Comment l'adversaire obtient-il le message m?