UNIVERSITÉ DE RENNES 1

M1 2015 - 2016

Introduction à la Sécurité **TD4**

Exercice 1 - RSA

Dans cet exercice on se propose d'énumérer tous les couples clé publique / clé privé pour RSA avec $p = 3$ et $q = 11$.

1. Déterminer $\varphi(33)$.
1. Déterminer tous les entiers x tels que $\text{pgcd}(x, \varphi(33)) = 1$.
2. Déterminer tous les couples (e, d) tels que $ed = 1 \mod \varphi(33)$.

Exercice 2 - Étude du jeu de pile ou face en réseau

Alice et Bob communiquent à distance au moyen d'un réseau (par messages asynchrones ou tout autre mode de communications par messagerie textuelle, par téléphone etc ...). Ayant un différent relativement à une décision, ils veulent s'en remettre au hasard pour la décision finale. Pour cela ils doivent construire un protocole par échange de messages asynchrones qui réalise une décision aléatoire de même nature que celle de pile ou face lorsque deux personnes sont en présence.

Pour remplacer le lancement de la pièce de monnaie Alice et Bob décident de tirer un entier au hasard (noté n). Selon que l'entier n est pair ou impair, on considère que la pièce est retombée coté pile ou coté face. Pour remplacer le choix au hasard entre pair et impair, Alice et Bob décident d'utiliser le tirage aléatoire d'une variable entière binaire (notée p).

1. Une version de base du protocole pourrait être la suivante. Dans une première phase, Alice est la participante qui tire l'entier n au hasard et Bob le participant qui choisit pair ou impair. Dans la seconde phase, Alice et Bob échangent en clair leur valeur. Dans la troisième phase les deux partenaires décident qui est gagnant.
   a) Quelles sont les fraudes possibles ?
2. Pour sécuriser le protocole, Alice propose d'utiliser une fonction de chiffrement symétrique E. Elle propose de générer une clé k en plus de l'entier n et d'envoyer $E_k(n)$ à Bob. Ensuite, une fois p reçu, elle révèle k et n à Bob.
   a) Quelles sont les fraudes possibles ?
   b) Comment remplacer E par un chiffrement à clé publique ? Cela rend-il le protocole sûr ?
3. Après avoir cherché à utiliser un système de chiffrement, on cherche maintenant à utiliser une fonction de hachage cryptographique H.

a) Décrire un protocole simple.

b) Étudier la sécurité de ce protocole si H n'est pas résistante aux collisions.

c) Même question dans le cas où H n'est pas résistante aux préimages.

d) Alice et Bob souhaitent définir un protocole, qui puisse être en cas de litige, soumis à un juge. Pour cela, Alice et Bob se proposent de modifier le protocole qui vient d'être décrit (avec fonction de hachage) ou d'ajouter l'utilisation d'autres fonctions cryptographiques dans les messages. Proposez des modifications pour une version du protocole qui puisse être soumise à l'arbitrage en non répudiation d'un juge (justifiez les mécanismes introduits permettant de défendre le point de vue que seuls Alice ou Bob peuvent être l'auteur de leurs messages et que les messages émis ont effectivement été reçus).

4. La méthode de Diffie-Hellman est réputée permettre un échange de clé secrète aléatoire entre deux entités qui ne peuvent communiquer que sur un réseau non sécurisé. L'objectif est donc que la clé ne circule jamais en clair sur le réseau et qu'elle soit aléatoire. On peut donc essayer de résoudre le problème posé par la sécurisation du jeu de pile ou face en réseau, en utilisant la solution de Diffie-Hellmann pour partager les deux variables aléatoires nécessaires au jeu de pile ou face. Peut-on construire une solution au jeu de pile ou face empêchant Alice ou Bob de tricher et qui serait basé sur l'utilisation du protocole de Diffie-Hellmann ?