CRYPTOLOGIE
TD3-chiffrements à clé publique

Exercice 1 : Protocole de Diffie-Hellman

Alice et Bob souhaitent générer et s'échanger une clé afin d'utiliser un cryptosystème à clé secrète. Ils utilisent pour cela le protocole de Diffie-Hellman avec les paramètres suivants : $d = 3$, $n = 5$. Alice choisi $a = 3$ et Bob $b = 6$.

1. Quelle valeur A est envoyée par Alice (donnez la formule et la valeur numérique) ?
2. Quelle valeur B est envoyée par Bob (donnez la formule et la valeur numérique) ?
3. Quelle est est la clé que Bob et Alice vont utiliser ?

Exercice 2 : Cryptosystème RSA

Alice et Bob possèdent chacun un trousseau RSA :
- Trousseau d'Alice : $p_A = 3$, $q_A = 5$, $n_A =?$, $n'_A =?$, $e_A = 3$, $e'_A = 3$.
- Trousseau de Bob : $p_B = 3$, $q_B = 11$, $n_B =?$, $n'_B =?$, $e_B = 3$, $e'_B =?$.

Dans toute la suite, M désignera le message en clair, M_S le message signé et C le message signé chiffré.

1. Complétez les valeurs manquantes des deux trousseaux en justifiant les calculs.
2. Parmi les 3 entiers n_A, e_A et e'_A, lesquels correspondent à la clé publique et à la clé privée d'Alice ?
3. Alice veut transmettre le message M en le signant puis le chiffrant. Indiquez quel est le message transmis et en précisant à chaque étape : l'opération (chiffrement ou signature), quel type de clé (publique ou privée) de quel correspondant (Alice ou Bob) est utilisée, ainsi que la formule donnant le nouveau message.
4. Bob reçoit le message $C = 23$ qui a été signé puis chiffré par Alice. Retrouvez le message en clair en précisant à chaque étape : l'opération (déchiffrement ou "désignature"), quel type de clé (publique ou privée) de quel correspondant (Alice ou Bob) est utilisée, la formule littérale et tous les calculs. (vous pouvez utiliser le fait que $23 \equiv -10[33]$).

Exercice 3 : Chiffrements à clé publique

1. **Protocole de Diffie-Hellman**
   Alice et Bob souhaitent générer et s'échanger une clé afin d'utiliser un cryptosystème à clé secrète. Ils utilisent pour cela le protocole de Diffie-Hellman avec les paramètres suivants : $d = 2$, $n = 7$. Alice choisi $a = 5$ et Bob $b = 10$.
   (a) Quelle valeur A est envoyée par Alice (donnez la formule et la valeur numérique) ?
   (b) Quelle valeur B est envoyée par Bob (donnez la formule et la valeur numérique) ?
   (c) Quelle est est la clé que Bob et Alice vont utiliser (donnez les formules et la valeur numérique) ?
2. **Cryptosystème RSA**
   Alice et Bob possèdent chacun un trousseau RSA :
   – Trousseau d'Alice : $p_A = 3$, $q_A = 11$, $n_A =?$, $n'_A =?$, $e_A = 7$, $e'_A = 3$.
   – Trousseau de Bob : $p_B = 5$, $q_B = 7$, $n_B =?$, $n'_B =?$, $e_B = 13$, $e'_B =?$.
   Dans toute la suite, M désignera le message en clair, M_S le message signé et C le message signé chiffré.
   (a) Complétez les valeurs manquantes des deux trousseaux en justifiant les calculs.
   (b) Parmi les 3 entiers n_A, e_A et e'_A, lesquels correspondent à la clé publique et à la clé privée d'Alice ?
   (c) Alice veut transmettre le message M en le signant puis le chiffrant. Indiquez quel est le message transmis et en précisant à chaque étape : l'opération (chiffrement ou signature), quel type de clé (publique ou privée) de quel correspondant (Alice ou Bob) est utilisée, ainsi que la formule donnant le nouveau message. Sachant que $30^2 = 27 * 33 + 9$ et que $270 = 8 * 33 + 6$, appliquez ce protocole pour $M = 30$ en justifiant tous vos calculs.
   (d) Bob reçoit le message C qui a été signé puis chiffré par Alice. Indiquez comment Bob retrouve le message en clair en précisant à chaque étape : l'opération (déchiffrement ou "désignature"), quel type de clé (publique ou privée) de quel correspondant (Alice ou Bob) est utilisée, ainsi que la formule donnant le nouveau message.

Exercice 4 : Chiffrements à clé publique

1. **Cours**
   (a) Sur quel problème mathématique est basé la sécurité du protocole de Diffie-Hellman (précisez la fonction à sens unique) ?
   (b) Sur quels problèmes mathématiques est basé la sécurité du cryptosystème RSA (précisez les fonctions à sens unique) ?
   (c) Lors d'une communication signée et chiffrée avec RSA, vaut-il mieux signer puis chiffrer ou chiffrer puis signer (justifiez votre réponse) ?

2. **Protocole de Diffie-Hellman**
Alice et Bob souhaitent générer et s'échanger une clé afin d'utiliser un cryptosystème à clé secrète. Ils utilisent pour cela le protocole de Diffie-Hellman avec les paramètres suivants : $d = 2$, $n = 5$. Alice choisi $a = 13$ et Bob $b = 2$.

   (a) Quelle valeur A est envoyée par Alice (donnez la formule et la valeur numérique) ?

   (b) Quelle valeur B est envoyée par Bob (donnez la formule et la valeur numérique) ?

   (c) Quelle est est la clé que Bob et Alice vont utiliser ?

3. **Cryptosystème RSA**
Alice et Bob possèdent chacun un trousseau RSA :
– Trousseau d'Alice : $p_A = 5$, $q_A = 7$, $n_A =?$, $n'_A =?$, $e_A = 11$, $e'_A = 11$.
– Trousseau de Bob : $p_B = 3$, $q_B = 7$, $n_B =?$, $n'_B =?$, $e_B = 5$, $e'_B =?$.
Dans toute la suite, M désignera le message en clair, M_S le message signé et C le message signé chiffré.

   (a) Parmi les 3 entiers n_A, e_A et e'_A, lesquels correspondent à la clé publique et à la clé privée d'Alice ?

   (b) Complétez les valeurs manquantes des deux trousseaux en justifiant les calculs. Ces deux trousseaux vous semblent-ils bons ?

   (c) Alice veut transmettre le message M en le signant puis le chiffrant. Indiquez quel est le message transmis et en précisant à chaque étape : l'opération (chiffrement ou signature), quel type de clé (publique ou privée) de quel correspondant (Alice ou Bob) est utilisée, ainsi que la formule donnant le nouveau message.

   (d) Bob reçoit le message $C = 2$ qui a été signé puis chiffré par Alice. Retrouvez le message en clair en précisant à chaque étape : l'opération (déchiffrement ou "désignature"), quel type de clé (publique ou privée) de quel correspondant (Alice ou Bob) est utilisée, la formule littérale et tous les calculs. (vous pouvez utiliser le fait que $11^2 = 3 * 35 + 16$ et que $11^3 = 38 * 35 + 1$).