Exercice 3 : chiffrement à clé publique

Remarques :

- Les exercices sont attribués en fonction de l'ordre alphabétique de votre nom de famille
- Les détails de résolution doivent apparaître lors de la remise de la solution
- Réponse soit sous la forme d'un fichier électronique, soit sous un format papier à déposer dans mon bureau pour le 06/11/03 au plus tard

Attribution des exercices :

- Question 1- a : [A-C], b : [D-E], c : [G-K], d : [L-P], e : [R-S]
- Questions 2, 3, 9 : [G-N]
- Questions 4, 5, 10 : [O-S]
- Questions 6, 7, 8 : [A-E]

1) Effectuer le chiffrement et le déchiffrement en utilisant l'algorithme RSA pour les valeurs suivantes :
   a. p = 3 ; q = 11 ; e = 7 ; M = 5
   b. p = 5 ; q = 11 ; e = 3 ; M = 9
   c. p = 7 ; q = 11 ; e = 17 ; M = 8
   d. p = 11 ; q = 13 ; e = 11 ; M = 7
   e. p = 17 ; q = 31 ; e = 7 ; M = 2

2) Soit un système à clé publique utilisant le RSA, vous interceptez le texte chiffré C=10 envoyé par un utilisateur dont la clé publique est e = 5 et n = 35. Que vaut M ?

3) Dans un système RSA, la clé publique d'un utilisateur donné est e = 31, n = 3599. Quelle est la clé privée de cet utilisateur ?

4) Dans un système RSA, chaque utilisateur possède une clé publique, e, et une clé privée, d. Supposons que B perd sa clé privée. Plutôt que de générer un nouveau module, il décide de générer une nouvelle paire de clé. Est-ce sur ? oui ? non ? pourquoi ?

5) Considérez le schéma suivant :
   a. Sélectionnez un nombre impair E
   b. Sélectionnez deux nombres premiers P et Q où (P-1)(Q-1)-1 est également divisible par E
   c. Multipliez P et Q pour obtenir N
   d. Calculer D = [(P-1)(Q-1)(E-1)+1]/E

   Ce schéma est-il équivalent au RSA ? Oui ? Non ? Pourquoi ?

6) Considérez le schéma suivant dans lequel B chiffre un message pour A
   a. A choisit 2 grands nombres premiers P et Q qui sont également relativement premier à (P-1) et (Q-1)
   b. A publie N = PQ comme clé publique
   c. A calcule P' et Q' tels que $PP' \equiv 1 \pmod{Q-1}$ et $QQ' \equiv 1 \pmod{P-1}$
   d. B chiffre le message M par la formule $C = M^N \pmod{N}$
   e. A trouve M en résolvant $M \equiv C^{P'} \pmod{Q}$ et $M \equiv C^{Q'} \pmod{P}$

1. expliquez comment et pourquoi ce schéma fonctionne
2. comment diffère-t-il du RSA ?
3. y a t'il quelque avantage particulier à ce schéma par rapport au RSA ?

7) Les utilisateurs A et B utilisent Diffie-Hellman avec p=71 et a=7
   a. Si la clé de l'utilisateur A est 5, que vaut Ya
   b. Si la clé de l'utilisateur B est 12, que vaut Yb
   c. Que vaut Kab ?

8) considérez un schéma Diffie-Hellman avec p=11 et a=2
   a. si Ya = 9, que vaut Xa ?
   b. si Yb = 3, que vaut Kab ?

Soit le schéma suivant :
Comme dans Diffie-Hellman, on choisit deux éléments publics : un nombre premier q et α une racine primitive (un primitif) de q. L'utilisateur A sélectionne une clé privée X_A et calcule une clé publique Y_A (comme dans Diffie-Hellman).
L'utilisateur A chiffre le texte M (< q) destiné à B de la manière suivante :
1. A choisit un nombre entier k tel que $1 \leq k \leq q-1$
2. A calcule $K = (Y_B)^k \pmod q$
3. chiffrement de M comme la paire d'entiers (C_1,C_2) où $C_1 = \alpha^k \pmod q$ et $C_2 = MK \pmod q$

L'utilisateur B déchiffre le message de la manière suivante :
1. calcul de $K = (C_1)^{X_B} \pmod q$
2. calcul de $M = (C_2/K) \bmod q$

9) Ce schéma fonctionne-t-il (inversibilité) ? Est-il équivalent à ElGamal ?

10) Si q = 71 et $\alpha = 7$
   a. si B a calculé comme clé publique $Y_B = 3$ et que A choisit k = 2. Que vaut C si $C = (C_1, C_2)$ sachant que M = 30 ?
   b. si maintenant A choisit une valeur pour k différente de telle sorte que le chiffrement de M = 30 donne $C = (59, C_2)$, que vaut C_2 ?