ESI ECOLE NATIONAL SUPÉRIEURE D'INFORMATIQUE

Sécurité Informatique

1CS

Contrôle Final

Partie Exercices

Exercice1 *(9 points)*

Alice construit un cryptosystème RSA à partir des nombres premiers p_a = q_a = 31. Alice doit choisir l'exposant de sa clé publique e_a parmi les nombres suivants : 9, 12, 13 et 63. Et calculer sa clé privée d_a.

1- Quel sera alors son choix pour e_a? (Justifier) (

2- Quelle est la valeur de sa clé privée d_a? (Justifier) (2

Bob ne disposant pas de clé publique dans l'annuaire, pas de canal sécurisé entre et Alice et veut solliciter Alice pour lui envoyer une information confidentielle.

3- Que doit faire Bob ? (En deux étapes) (1p

Bob décide enfin de construire un cryptosystème RSA à partir des nombres p_b = 67 et q_b = 37, il doit choisir l'exposant de la clé publique parmi les nombres suivants :

45, 46, 47, 48, 49.

4- Quel sera son choix ? (Justifier) (0.5pt)

On note e_b son choix. Bob doit choisir sa clé secrète d_b parmi les valeurs suivantes :

451, 453, 455, 457.

5- Quelle sera la clé secrète d_b de Bob ? (Justifier) (1pts)

Alice veut envoyer le message ***SECRET*** à Bob. Elle utilise un codage des lettres sur 8 bits comme suit : {A = 00_H, B= 01_H .... Z = 19_H}.

6- Donner le code, en Hexadécimale, du message qu'Alice veut chiffrer. (0.5pt)

Alice doit découper son message en blocs pour pouvoir le chiffrer à Bob.

7- Quel sera alors le choix optimal de la taille de ces blocs (en bits)? (justifier) (1pt)

8- Donner le cryptogramme du premier bloc chiffré. (2pts)