7 septembre 2004

DESS-AIM

Contrôle des connaissances n° 3, 2003/2004: CRYPTOGRAPHIE

On peut utiliser les résultats d'un exercice dans un autre. On sera attentif à la précision de la rédaction. Les résultats devront toujours être justifiés que ce soit par une démonstration, un algorithme ou une vérification numérique. Les protocoles seront décrits précisément.

L'exercice VII sera traité sur une feuille séparée.

I

Quelle est la taille de la clé du crypto-système DES? Combien la clé génére-t-elle de sous-clefs et quelle est leur taille

Citer deux cryptosystèmes à clef publique.

II

Décrire un protocole de signature avec le système RSA.

III

Soit $p_a = 37$, $q_a = 41$, $q_b = 61$, $q_b = 67$ des nombres entiers. Montrez que ces nombres sont premiers.

IV

Calculez $7^{-1} \bmod 1440$.

Donnez une solution dans l'intervalle $[0, 1339] = \{x \in \mathbb{Z}; 0 \leq x \leq 1339\}$, une solution dans l'intervalle $[-1397, 42] = \{x \in \mathbb{Z}; -1397 \leq x \leq 42\}$ et une solution dans l'intervalle $[-927 \leq x \leq 512]$.

IV

Alice construit un cryptosystème RSA à partir des nombres $p_a = 37$, $q_a = 41$. Elle doit choisir sa clé publique dans la liste suivante

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13$$

Quels sont ses choix possibles.

Elle veut aussi un exposant aussi petit que possible. Quel sera son choix définitif que l'on notera e_a.

Quel sera alors l'exposant d_a de sa clé secrète? que publie-t-elle que garde-t-elle secret?

V

Bob construit un cryptosystème RSA à partir des nombres $p_b = 61$ et $q_b = 67$, il doit choisir l'exposant de la clé publique parmi les nombres

$$3,\ 4,\ 5,\ 48,\ 49,\ 50$$

Quel sera son choix? On note e_b son choix.

Calculez la clé secrète d_b de Bob.

VI

Alice veut envoyer le message, 3, codé et signé à Bob.

Envoyez à Bob le message crypté et signé par Alice.

VII

Soit a un entier, donner un algorithme qui trouve le plus petit entier tel qu'il n'y ai pas de nombre premier entre n et $n + a$, c'est-à-dire

$$\forall p \quad n < p < n + a \ \Rightarrow\ p \text{ n}'\text{est pas premier .}$$

Après avoir expliqué votre algorithme, le traduire dans le langage de votre choix. *Votre algorithme et sa traduction dans un langage de programmation devront éviter tout calcul inutile et couteux en temps.*