le 31 octobre 2003

DESS-AIM

Contrôle des connaissances 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 VIII sera traité sur une feuille séparée.

Soit $p_b = 29$, $q_b = 37$, $q_a = 23$, $q_a = 31$ des nombres fixés une fois pour toutes.

I

Montrez que ces nombres sont premiers.

II

Calculez

$$9^{-1} \bmod 16 \times 7$$
$$16^{-1} \bmod 7 \times 9$$
$$7^{-1} \bmod 9 \times 16$$

montrez que

$$25^{-1} \equiv 9 \bmod 112; \quad 25^{-1} \equiv -5 \bmod 63; \quad 25^{-1} \equiv 23 \bmod 144$$

III

Calculez

$$25^{-1} \bmod 1008$$

Donnez une solution dans l'intervalle $[0, 1007] = \{x \in \mathbb{Z}; 0 \leq x \leq 1007\}$, une solution dans l'intervalle $[-965, 42] = \{x \in \mathbb{Z}; -965 \leq x \leq 42\}$.

IV

Alice construit un cryptosystème RSA à partir des nombres $p_a = 23$, $q_a = 31$ et l'exposant de la clé publique $e_a = 7$. Quel est l'exposant d_a de sa clé secrète? que publie-t-elle que garde-t-elle secret?

Bob construit un cryptosystème RSA à partir des nombres $p_b = 29$ et $q_b = 37$ il doit choisir l'exposant de la clé publique parmi les nombres

$$24,\ 25,\ 26,\ 27,\ 28$$

Quel sera son choix? On note e_b son choix.

V

Calculez la clé secrète d_b de Bob.

VI

On choisit un alphabet à 5 lettres

$$O = 0, \quad U = 1, \quad I = 2, \quad ! = 4$$

Alice veut envoyer le message codé et signé **OUI!** à Bob. Quel sera le choix optimal de taille des blocs pour Alice.

Envoyez à Bob le message crypté et signé par Alice.

VII

Alice utilise la fonction de hachage suivante: si $x = x_0 + 5x_1$ est l'écriture d'un bloc de deux lettres en base 5, donc $0 \leq x_0 \leq 4$ et $0 \leq x_1 \leq 4$, on pose

$$h(x) \equiv x_0 + x_1 \bmod 5$$

Envoyez à Bob le message crypté et signé grâce à la fonction de hachage h par Alice.

VIII

Soit n un nombre entier, on appelle diviseur *propre* de n tout diviseur de n distinct de n. On dit qu'un entier est un nombre *parfait* si et seulement s'il est la somme de ses diviseurs propres.
Exemple 6 a pour diviseurs propres 1, 2 et 3 dont la somme est 6, il est donc parfait.
Écrire une fonction qui teste si un nombre est parfait. On vous demande de décrire votre algorithme en langage naturel, puis de l'écrire en C ou en langage algorithmique.
Votre algorithme devra surtout veiller à ne pas faire des calculs inutiles .