Club Math

Centre informatique
pédagogique (CIP)
Rue Théodore-de-Bèze 2
Case Postale 172
1211 GENÈVE 3
Tél: (022) 318.05.30
Fax: (022) 781.03.50
Responsable:
Raymond Morel

Lettre nº 25

Lundi 1er novembre 1993 à 17 h

Top secret !

Bernard Vuilleumier

Jusqu'à un passé récent, le code d'un message secret devait être connu d'au moins deux personnes: l'expéditeur et le destinataire du message

Dans un système à clefs publiques, une seule personne détient le code d'un message secret

Pour parvenir à briser le code d'un message, il faut être capable de factoriser de très grands nombres, ce qui est une tâche impossible en pratique

La prolifération des moyens de communication et le besoin croissant d'envoyer des informations confidentielles - déclarations d'amour, transferts bancaires, instructions d'achats ou de ventes, données diplomatiques ou militaires - ont rendu nécessaire le développement de méthodes cryptographiques sûres. Jusqu'à un passé récent, les codes étaient tenus secrets et n'étaient connus que des personnes qui envoyaient le message et de celles qui le recevaient. Mais il était toujours possible d'intercepter un message, de l'étudier et de découvrir le code, ce qui pouvait donner lieu à des situations désastreuses, en temps de guerre notamment.

De grands progrès ont été réalisés en cryptographie avec l'avènement du *système à clefs publiques*. Les caractéristiques principales de cette méthode sont: la simplicité, la clef publique et l'extrême difficulté à briser le code. L'idée de ce système a été proposée en 1976 par Diffie & Hellman [(1)]. L'implémentation fut achevée en 1978 par Rivest, Shamir & Adleman. Depuis, ce crypto système est appelé système RSA.

Dans le système RSA, chaque lettre ou signe, y compris l'espace blanc, correspond à un nombre à trois chiffres. Un message M peut donc être converti en un entier positif. Chaque utilisateur du système donne, dans un répertoire public, sa clef, qui consiste en une paire d'entiers positifs (n, e). Le premier entier, n, est égal au produit de deux nombres premiers p et q qui ne sont connus que du possesseur de la clef. Le deuxième entier, $e < pq$, est premier relativement à $p-1$ et à $q-1$.

Lorsqu'un utilisateur A veut transmettre un message à un utilisateur B dont la clef publique est (n, e), il doit procéder ainsi:

• convertir le message en un entier N (cet entier doit être inférieur à n);

• coder le nombre N en calculant N^e modulo n.

A peut alors envoyer son message à B sur une ligne totalement publique. Lorsque B reçoit le message, il le décode en faisant les opérations suivantes:

• décoder le nombre reçu en l'élevant à la puissance d modulo n, où d est l'inverse de e modulo $(p-1)(q-1)$;

• convertir l'entier N en une chaîne de caractères pour obtenir le message.

Si p et q sont des nombres premiers suffisamment grands, disons de 100 chiffres ou plus, et s'ils sont choisis au hasard, la factorisation de n est pratiquement impossible avec les méthodes connues actuellement. Vous pouvez donc envoyer sans risque - sur n'importe quelle ligne publique - des messages confidentiels à toute personne dont vous connaissez la clef, à condition bien sûr, de les coder à l'aide du système RSA!

(1) Diffie, W. & Hellman, M. E. New directions in cryptography. *IEEE Trans. on Inf. Th., IT-22,* 1976.

Travaux pratiques

Exercice 1

a) Décrivez les différences principales entre les systèmes de codage traditionnels (ceux utilisés durant la dernière guerre mondiale notamment) et le système de Rivest, Shamir & Adleman [(2)].

b) Dans le système RSA, la qualité du codage dépend-elle de la clef de celui qui envoie le message ou de la clef de celui qui le reçoit ?

Exercice 2

a) Ecrivez un programme permettant de transformer une chaîne de caractères (un message) en un nombre entier.

b) Ecrivez un programme permettant de retrouver le message à partir du nombre entier qui lui correspond.

Exercice 3

a) Définissez une fonction permettant d'obtenir le premier nombre premier supérieur à un nombre entier *m* donné.

b) Construisez une clef (*n*, *e*) à l'aide de deux nombres premiers *p* et *q*

Rappel: *n* est égal à *pq* et *e* doit être premier relativement à *p* -1 et à *q* -1.

Exercice 4

Vous souhaitez envoyer le message «Je vous aime» à une personne dont la clef est: (121576654590569289237414895290322022784 1, 135841).

a) Quel nombre lui faites-vous parvenir ?

b) Quel temps faut-il à la (au) destinataire pour décoder le message ?

Indication: p = 10000000000000000039, q = 12157665459056928919.

c) Si un indiscret interceptait le message codé, quel temps lui faudrait-il pour le décoder ?

Exercice 5

Vous interceptez le message suivant: 290072633447605769898707693.

Ce message est destiné à une personne dont la clef est: (113884547528651448182021814 1, 181).

Essayez de décoder ce message. Quel temps cela vous a-t-il pris ?

Constatations? Commentaires ?

[(2)] Rivest, R. L., Shamir, A. & Adleman, L. M. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM, 21*, 1978, 120-126.

Prochaine réunion: lundi 6 décembre 1993 à 17 h.