Transmission de messages secrets grâce à l'arithmétique

(d'après R.L. Rivest, A. Shamir, L. Adleman)

Les discours secrets doivent être regardés comme des pensées.
Voltaire (Pol. et lég. Relat. mort de la Barre)

L'oeuf qui a reçu une quantité appropriée de chaleur se transforme en poussin, mais la chaleur ne peut transformer une pierre en poussin, car leurs bases sont différentes.
Mao Tsé-Toung (De la Contradiction, août 1937, oeuvres choisies, tome I)

I. La notion de système cryptographique à clef publique.

Ce schéma a été introduit par Diffie et Hellman [1] . On considère un ensemble d'individus i, j, k ... qui veulent communiquer entre eux. Mais, lorsque j envoie un message à i , seul i doit pouvoir le déchiffrer.

A chaque individu i correspondent deux procédures, l'une E_i (1) qui est publique, l'autre D_i , secrète, connue seulement de i (en principe !). La liste des procédures E_i figure tout simplement sur un annuaire.

Si l'individu j veut envoyer un message M à l'individu i , il procède ainsi : Il consulte l'annuaire pour trouver la procédure E_i . Il calcule $M' = E_i(M)$ et envoie M' à i . Pour déchiffrer M' , i calcule $D_i(M')$.

Ce schéma est caractérisé par les propriétés suivantes :

a) Décodage : Pour tout i et tout message M, on a $D_i(E_i(M)) = M$. En calculant $D_i(M') = D_i(E_i(M) = M$, i déchiffre le message qui lui est destiné.

b) Simplicité : Le travail de codage et décodage imposé par les procédures E_i et D_i n'est pas trop compliqué.

c) Secret : La connaissance de E_i ne permet pas de découvrir facilement la procédure D_i.

Ainsi, seul i peut déchiffrer le message qui lui est envoyé. Mais un plaisantin ou un individu malveillant peut lui communiquer de fausses nouvelles. Donc, dans de nombreux cas, on souhaite que l'expéditeur du message puisse être identifié avec certitude : le message doit être signé. Ceci est réalisé, de façon élégante, si la propriété suivante a lieu.

d) Signature : On suppose de plus $E_i [D_i(M)] = M$, pour tout i et tout M.

Supposons que j veuille faire parvenir à i un message M "signé". Il calcule $S = D_j(M)$, puis $S' = E_i(S)$. Il envoie S' à i. Alors i calcule $S = D_i(S')$, puis $E_j(S) = E_j [D_j(M)] = M$. (2)

Quiconque a connaissance de S et de M peut se convaincre que l'expéditeur est bien j, en vérifiant la relation $E_j(S) = M$.

Le papier de Diffie et Hellman ne comportait qu'un seul défaut, il ne proposait aucun exemple de telles procédures E_i et D_i. Un tel exemple a été fourni par Rivest, Shamir et Adleman, nous l'étudierons dans un prochain paragraphe.

II. Interlude arithmétique.

Les quelques faits élémentaires suivants nous seront utiles.

LEMME 1. - Soit p un nombre premier. Soit k un entier congru à 1 modulo (p-1). Alors tout entier x vérifie la congruence

$$x^k \equiv x \pmod{p} .$$

> Lorsque p divise x c'est banal, puisque les deux membres sont alors congrus à zéro modulo p. Si p ne divise pas x, le petit théorème de Fermat [2], énoncé en 1640, affirme que l'on a

$$x^{p-1} \equiv 1 \mod p ,$$

donc, comme k est de la forme $\ell(p-1)+1$, on a bien

$$x^k = (x^{p-1})^{\ell} x \equiv x \pmod{p} .<$$

LEMME 2 (Théorème chinois). - Soient a et b deux entiers premiers entre eux, alors il existe un isomorphisme naturel entre les anneaux $\mathbb{Z}_{/ab\mathbb{Z}}$ et $\mathbb{Z}_{/a\mathbb{Z}} \times \mathbb{Z}_{/b\mathbb{Z}}$.

> Ce résultat était connu, au langage près, des astronomes chinois de l'Antiquité. En voici une preuve.

Considérons l'application naturelle

$$\mathbb{Z} \to \mathbb{Z}_{/a\mathbb{Z}} \times \mathbb{Z}_{/b\mathbb{Z}}$$

qui a un entier x fait correspondre le couple $(x \bmod a,\ x \bmod b)$. Du fait que l'on peut ajouter et multiplier des congruences membre à membre, il s'agit d'un homorphisme d'anneaux. Son noyau est constitué par les entiers congrus à zéro modulo a et modulo b, donc par les multiples de ab. D'où un homomorphisme injectif

$$\mathbb{Z}_{/ab} \to \mathbb{Z}_{/a\mathbb{Z}} \times \mathbb{Z}_{/b\mathbb{Z}} .$$

Pour conclure qu'il s'agit en fait d'une bijection, il suffit de noter que les ensembles de départ et d'arrivée comptent tous deux ab éléments. <

THEOREME 1. - Soient $p_1, \ldots, p_\ell$ des nombres premiers distincts et $n = p_1 \cdots p_h$. On pose $\varphi(n) = (p_1 - 1) \ldots (p_h - 1)$. Soit k un entier congru à 1 modulo $\varphi(n)$. Alors, tout entier x vérifie

$$x^k \equiv x \pmod{n} . \qquad (3)$$

>Par application répétée du lemme 2, on voit que les anneaux $\mathbb{Z}_{/n\mathbb{Z}}$ et $\mathbb{Z}_{/p_1\mathbb{Z}} \times \cdots \times \mathbb{Z}_{/p_h\mathbb{Z}}$ sont isomorphes ; par conséquent, il suffit de vérifier que l'on a toujours

$$x^k \equiv x \pmod{p_i} \quad \text{pour} \quad i = 1, \ldots, h .$$

Ces congruences résultent immédiatement du lemme 1.<

III. L'exemple de Rivest-Shamir-Adleman ([4]).

A chaque individu i, associons des entiers e_i, d_i, n_i tels que e_i et n_i figurent dans l'annuaire, tandis que d_i est tenu secret, seul i le connaît. Les messages M envoyés à i sont des entiers modulo n_i (ce qui n'ôte rien à la généralité de cette méthode). Les procédures E_i et D_i sont définies par

$$E_i(M) = M^{e_i} \quad \text{modulo } n_i ,$$
$$D_i(C) = C^{d_i} \quad \text{modulo } n_i .$$

Chaque entier n_i est le produit de deux nombres premiers distincts p_i et q_i. Le choix des entiers d_i et e_i sera précisé plus loin.

Oublions les indices i provisoirement.

1 - Pour réaliser la condition a), il faut que l'on ait

$$D(E(M)) = (M^e)^d = M^{ed} \equiv M \pmod{n} .$$

Le théorème 1 montre que cette condition a lieu lorsque e et d vérifient

$$ed \equiv 1 \pmod{\varphi(n)} , \quad \text{où} \quad \varphi(n) = (p-1)(q-1) .$$

2 - C'est un truc bien connu des informaticiens que le calcul de x^k nécessite au plus $2 \log_2(k)$ multiplications. La preuve formelle est la suivante : on écrit k en base deux,

$$k = \sum_{i=0}^{\ell} \epsilon_i 2^i \quad (\text{avec } \ell \leq \log_2 k) ,$$

et on a

$$x^k = x^{\Sigma \epsilon_i 2^i} = \prod_{i=0}^{\ell} (x^{2^i})^{\epsilon_i} . \qquad (4)$$

Ceci prouve que les temps de calcul de E et D sont polynomiaux en fonction de Log n , donc possibles même pour de très grandes valeurs de n .

3 - La condition c est-elle réalisée ?

On suppose que p et q sont deux grands nombres premiers secrets. On calcule alors $n = p\,q$ et $\varphi(n) = (p-1)(q-1)$. On choisit ensuite un entier d secret,assez grand et premier avec $\varphi(n)$ (il suffit de prendre d premier $> \max\{p, q\}$) . Grâce à l'algorithme d'Euclide du calcul du p. g. c. d de d et $\varphi(n)$, on calcule ensuite e tel que $ed \equiv 1 \mod \varphi(n)$. Le temps de ce calcul est encore polynômial en fonction de Log n . Comme nous l'avons déjà vu, cette congruence assure que la condition a) est vérifiée.

Rappelons que seuls n et e sont publics. Dans ces conditions, comment peut-on trouver d ?

. Si on sait factoriser n , on trouvera p et q , puis $\varphi(n)$ et enfin la clef d en résolvant $ed \equiv 1 \mod \varphi(n)$. Mais - à ce jour - personne

ne sait factoriser rapidement un entier arbitraire. La méthode élémentaire en quelques $\sqrt{n}$ opérations a été améliorée, cependant même avec les meilleures méthodes connues on estime que la factorisation d'un entier de l'ordre de 10^{100} nécessite en général 75 ans de calcul avec les ordinateurs les plus puissants et celle d'un entier de l'ordre de 10^{200} nécessite 4 millions d'années ! On choisit donc p et q supérieurs à 10^{50}.

. La factorisation de n n'est pas nécessaire, il "suffit" de calculer $\varphi(n)$. Mais, c'est aussi difficile que de factoriser n, puisque la connaissance de $\varphi(n) = n-(p+q)+1$ et $n = pq$ permet de retrouver facilement p et q.

. Aucune procédure efficace de résolution de l'équation

$$x^e \equiv a \pmod{n}$$

ne semble connue pour un entier e général.

4 - Du fait que les entiers n_i sont distincts, la condition d) n'est réalisée que dans "la moitié" des cas. En effet, pour $n_j > n_i$, le domaine de définition des fonctions D_j et E_j n'est pas contenu dans celui de E_i et D_i. On trouvera dans [4] deux suggestions simples pour remédier à cet inconvénient. Mais L. M. Kohnfelder [3] a proposé une solution plus élégante à ce problème. Supposons que j veuille envoyer à i un message M signé.

- Si n_j vérifie $n_j < n_i$ alors j procède comme indiqué au premier paragraphe.

- Si n_j vérifie $n_j > n_i$, cette fois j envoie $T = D_j(E_i(M))$ et i décode le message en calculant $M = D_i(E_j(T))$. Pour authentifier le message, il suffit de vérifier que l'on a $E_j(T) = E_i(M)$.
- Cette procédure n'est pas ambigüe puisque les entiers n_i et n_j sont connus, n'importe qui peut donc les comparer.

IV. Remarques.

. Le théorème 1 montre qu'il n'est pas nécessaire de choisir des entiers n égaux au produit de deux entiers premiers distincts, il suffit que n ne soit pas divisible par le carré d'un nombre premier. (5)

. Dans [4], le théorème 1 n'est démontré que pour $h = 2$. De plus, la démonstration donnée ici évite l'étude de cas qui figure dans [4].

Références.

[1] W. Diffie, M. Hellman. - New directions in cryptography, I.E.E.E. Trans. Inform. Theory IT-22, nov. 1976, n°6, p. 644-654.

[2] P. de Fermat. - Oeuvres, ii. 209.

[3] L. M. Kohnfelder. - On the signature reblocking problem in public-key cryptosystems, Com. A.C.M., fev. 1978, v.21, n°2, p. 179.

[4] R. L. Rivest, A. Shamir, L. Adleman. - A method for obtaining digital signatures and Public-Rey cryptosystems, Com. A.C.M., fev. 1978, v.21, n°2, p. 120-126.

Maurice Mignotte
Centre de Calcul
7, rue René Descartes
67084 STRASBOURG Cédex

N O T E S : Il a semblé nécessaire à la rédaction de l'ouvert d'ajouter quelques notes au texte de M. Mignotte pour une meilleure compréhension.

(1) E pour "encodage" et D pour "décodage".

(2) M est un message quelconque ou un simple mot du message. On peut toujours supposer après remplacement des lettres par un nombre à deux chiffres correspondant à leur rang dans l'alphabet, que M est un nombre entier.

(3) Ce théorème n'est qu'une généralisation du théorème bien connu des élèves de terminale C : $x^{p-1} \equiv 1 \pmod p$ où p est un nombre premier. (Théorème de Fermat).

(4) Par exemple, pour calculer x^{15} on calcule successivement : x^2 , x^4 , x^8 , $x^{8+4} = x^{12}$, $x^{12+2} = x^{14}$ et enfin x^{15} ce qui nécessite finalement 6 multiplications.

(5) En effet, si $n = p^2q$, en prenant $M = pq$ on voit que $M^2 \equiv 0 \pmod n$ et par suite M et 0 ont la même image ce qui prouve que le codage n'est pas bijectif (ce qui est source d'incompréhension !)

UN EXEMPLE :

Prenons $n = 3\,691 \times 3\,989 = 14\,723\,399$
alors $\varphi(n) = 3\,690 \times 3\,988 = 14\,715\,720 = 2^3 \times 3^2 \times 5 \times 41 \times 997$
choisissons comme valeur de d : 1 999 qui étant premier et plus grand que le plus grand facteur de $\varphi(n)$ est premier avec lui.

Il nous faut trouver e tel que :

$$ed \equiv 1 \pmod{\varphi(n)}$$

Comme d et $\varphi(n)$ sont premier entre eux, d'après le théorème de Bezout, il existe deux constantes e et f telles que :

$$ed + f\varphi(n) = 1$$

En prenant les reste modulo $\varphi(n)$ des deux membres de cette égalité, on voit que e est bien le nombre cherché.

Voici la construction de e pour $d = 1\,999$ et $\varphi(n) = 14\,715\,720$; l'application de l'algorithme d'Euclide donne :

14 715 720	=	7 361	x	1 999 + 1 081	- 233
1 999	=	1	x	1 081 + 918	+ 126
1 081	=	1	x	918 + 163	- 107
918	=	5	x	163 + 103	+ 19
163	=	1	x	103 + 60	- 12
103	=	1	x	60 + 43	+ 7
60	=	1	x	43 + 17	- 5
43	=	2	x	17 + 9	+ 2
17	=	1	x	9 + 8	- 1
9	=	1	x	8 + 1	

Dans la colonne de droite on a choisi, à partir du bas, des coefficients multiplicatifs de manière à pouvoir effectuer les simplifications indiquées après addition membre à membre des différentes égalités. Il vient alors :

$$-233 \times 14\,715\,720 + 126 \times 1\,999 = -233 \times 7\,361 \times 1\,999 + 1$$

Soit encore :

$$-233 \times 14\,715\,720 + 1\,715\,239 \times 1\,999 = 1$$

D'où la valeur de e :

$$e = 1\,715\,239$$

Nous laissons le soin aux ordinateurs pour encoder ou décoder les messages !

L ' O U V E R T : responsable de la publication : Jean Lefort
24, rue A Schweitzer
Wintzenheim 68000 Colmar

impression : Irem de Strasbourg
10, rue du général Zimmer
67084 Strasbourg Cédex