Cryptographie publique

par Alain BOUVIER, IREM de LYON

Cryptographie : Code graphique déchiffrable par l'émetteur et le destinataire seulement.

(Petit Robert)

1. La cryptographie aujourd'hui

Chacun de nous, une fois dans sa vie au moins, a échangé avec un ou plusieurs camarades des messages secrets. Nous avons tous entendu parler des codes utilisés pendant la dernière guerre par les militaires, les agents secrets ou les résistants. En dehors de ces cas extrêmes, qui utilise encore des codes secrets aujourd'hui ? Pourquoi ce regain d'intérêt, depuis quelques années, pour la cryptographie ?

Bien sûr, on pense en premier lieu aux usages militaires contemporains: communications avec les sous-marins, avec les avions et les satellites chargés de la surveillance de territoires ou porteurs de bombes. On imagine très bien également que les messages entre agents secrets continuent à nécessiter l'usage de codes et qu'au niveau politique, les liaisons entre chefs d'état (type "téléphone rouge") ou entre un gouvernement et ses ambassadeurs ne se font pas "en clair".

Mais tout ceci reste discret; le grand public que nous sommes en connaît vaguement l'existence et le principe, sans plus.

L'engouement réçent pour la cryptographie semble venir surtout des milieux économiques. Ils désirent utiliser de plus en plus des procédés de codages pour échanger des informations commerciales (certaines d'entre elles seulement bien sûr): le courrier, le téléphone, la radio, le télex, les microfilms ne sont pas sûrs; tout peut être

intercepté compte tenu des moyens sophistiqués utilisables aujourd'hui et aucun code secret ne résiste longtemps à la sagacité des spécialistes, surtout depuis les prodigieux progrès des ordinateurs. Le problème de la transmission de messages codés inviolables devient d'autant plus important que l'informatisation sans cesse croissante de la société fait envisager des systèmes où des ordres, des consignes, seront transmis directement d'un ordinateur à un autre. Comment s'assurer que la bonne instruction sera transmise au bon destinataire ? Comment celui-ci pourra-t-il contrôler que le message reçu provient bien de l'émetteur supposé ? Sans précautions, nous risquons un jour de voir des comptes en banque débités de dépenses faites par d'autres, ou, bien pire, tel satellite lâcher sur nous une bombe qui ne nous était pas destinée.

La cryptographie est devenue un domaine particulier du calcul numérique. Alors qu'en 1940, les calculs sur machine coûtaient encore fort cher et surtout nécessitaient un temps considérable, aujourd'hui l'informatique a rendu impossible la construction de codes à la fois inviolables, d'emploi facile et bon marché. Devant cette situation, les spécialistes tentèrent de poser le problème d'une façon nouvelle que nous allons présenter et qui consiste à rendre le code connu de tous, dès le départ, puisque l'on ne peut pas garantir son inviolabilité.

Avant de nous livrer à cette description, rappelons brièvement comment on procédait jusque-là.

2. Cryptographie secrète

On appelle *cryptographie secrète* celle, que nous connaissons tous, où tout repose sur le secret du code. Cette terminologie l'oppose à la *cryptographie publique* dont le code est connu de tous.

La situation la plus simple met en scène deux personnes: un *émetteur* E et un *récepteur* R. Le premier souhaite transmettre au second un message M que l'on peut considérer comme un nombre (ou si besoin comme une suite de nombres). De plus, la situation classique nécessite trois ingrédients:

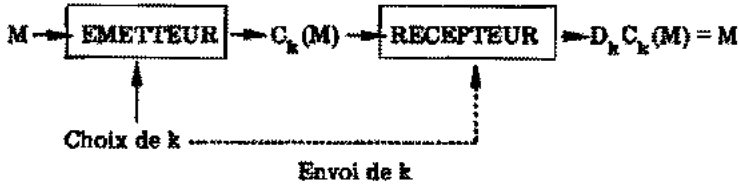
- des clés k ,
- des fonctions codages C_k ,
- des fonctions décodages D_k ,

de sorte que pour toute clé k et pour tout message M, on ait

$$D_k\, C_k(M) = M \quad .$$

La connaissance de la clé k permet de connaître aussi bien la fonction codage C_k que la fonction décodage D_k.

Figure 1



En pratique, le choix de la clé k suppose un accord préalable à l'émission entre l'émetteur et le récepteur. Ou bien le récepteur envoie à l'émetteur, par un canal particulier, la clé k qu'il doit utiliser pour son prochain message (et il y a risque d'interception de la clé) ou bien l'émetteur et le récepteur se mettent d'accord sur toute une famille $(k_i)_{i \in I}$ de clés et sur leur ordre d'utilisation.

Cette solution diminue le nombre d'envois relatifs aux clés. Mais l'unique échange peut, lui aussi, être intercepté — comme cela fut le cas à plusieurs reprises pendant la dernière guerre — et l'intercepteur, en possession de cette information, peut décoder les messages pendant une longue période sans que nul ne s'en doute.

L'inconvénient de ce système est clair: il nécessite *deux* circuits de transmission (figure 1); l'un, fréquemment utilisé pour transmettre les messages codés et qui en raison de sa fréquence d'utilisation ne peut pratiquement pas rester secret; un autre, pour la transmission de l'annuaire des clés $(k_i)_{i \in I}$ et donc des fonctions décodages correspondantes $(D_{k_i})_{i \in I}$. Ce dernier circuit doit impérativement demeurer secret.

De plus, rien n'empêche un intercepteur éventuel d'envoyer de faux messages qu'il aura lui-même codés en utilisant l'annuaire de clés intercepté. Comment le récepteur pourrait-il se douter de quelque chose puisqu'une fois décodés par ses soins, les faux messages auront du sens ?

Remarquons enfin que ce système exige un annuaire de clés par couple de correspondants. Il est donc particulièrement coûteux.

3. Principe de la cryptographie publique

Le principe initial de la cryptographie publique est simple: puisque la faiblesse du système classique tient au secret de l'annuaire des clés, secret de plus en plus difficile à assurer, inventons un système ayant les qualités requises habituellement (facilité d'utilisation, coût peu élevé, etc.) mais dans lequel l'annuaire des clés serait public, c'est-à-dire connu de tous, comme le sont aujourd'hui nos numéros de téléphone lorsqu'ils figurent dans l'annuaire des PTT.

Vous vous demandez sûrement comment, dans ce cas, on peut empêcher un intercepteur de décoder les messages qui ne lui sont pas destinés. Afin de répondre à cette question, entrons un peu plus dans les détails de la cryptographie publique.

Plaçons-nous à nouveau dans la situation d'un émetteur E et d'un récepteur R et supposons que l'on possède les ingrédients suivants:

- une fonction T ,
- une famille de fonctions codages $(C_y)_{y \in Y}$,
- une famille de fonctions décodages $(D_x)_{x \in X}$,

et supposons que pour tout x appartenant au domaine de définition de T, l'élément T(x) soit dans Y et que pour tout message M, on ait:

$$D_x \, C_{T(x)}(M) = M \quad .$$

Pour connaître C_y ou D_x , il faut connaître y ou x .

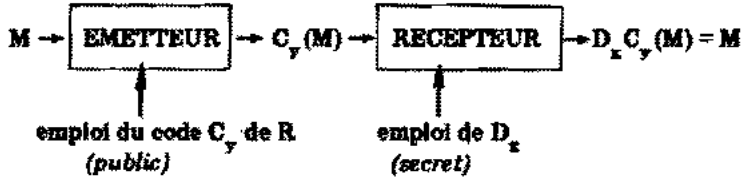
Lorsque le récepteur R veut recevoir un message de l'émetteur E, il choisit un élément x_1 (qu'il est donc *le seul* à connaître) et rend publique $y_1 = T(x_1)$. Puisque l'émetteur E connaît y_1 , pour envoyer son message M à R, il utilise le *code public* C_{y_1} , c'est-à-dire qu'il envoie $C_{y_1}(M)$.

Lorsque R reçoit ce message, il sait qu'il a été codé avec C_{y_1} (puisqu'il lui est destiné). Il le décode en utilisant la fonction D_{x_1} qu'il est *le seul* à connaître. On a bien, en effet:

$$D_{x_1} \, C_{y_1}(M) = D_{x_1} \, C_{T(x_1)}(M) = M \quad .$$

Cette nouvelle situation peut se schématiser ainsi:

Figure 2



Pour garantir le secret du message, il suffit que la connaissance de $y_1 = T(x_1)$ ne permette pas de retrouver facilement x_1. En pratique, le mot "facilement" signifie que le temps de calcul de x_1 à partir de y_1 doit être trop long pour que sa recherche présente le moindre intérêt militaire, politique ou économique.

Arrivés là, vous vous demandez probablement s'il existe des fonctions T, C_x et D_y possédant toutes les propriétés que nous venons de décrire. Le problème principal, qui consiste d'abord à trouver la fonction T (une telle fonction est dite "one way function" ou *fonction trappe*), a été résolu en 1978 par des chercheurs du MIT: R.I. RIVEST, A. SHAMIR et L. ADLEMAN. Leur solution n'utilise que des propriétés d'arithmétique élémentaire, voir [1].

4. Une fonction trappe en arithmétique

Etant donnés deux nombres premiers p et q, le calcul de leur produit à l'aide d'un ordinateur nécessite une fraction de seconde. Par contre, si l'on connaît le produit pq, la recherche des facteurs p et q demanderait à l'ordinateur le plus puissant plusieurs millions d'années lorsque p et q s'écrivent avec plus de cent chiffres.

On considère qu'en pratique, on ne peut pas factoriser les entiers qui s'écrivent avec plus de 40 chiffres sauf dans des cas très particuliers (voir l'article de C. POMERANCE). Pour être précis, Donald RIVEST estime à sept minutes *au plus* le temps nécessaire pour tester la primarité d'un nombre de 130 chiffres, voir [5]. Par contre, pour retrouver deux facteurs premiers de 63 chiffres à partir de leur produit (126 ou 127 chiffres), le temps de calcul (toujours d'après D. RIVEST) serait de un million de milliards d'années.

De même, lorsque l'on connaît p et q, il est facile de calculer

$$\varphi(pq) = (p-1)(q-1)$$

où φ désigne la fonction indicatrice d'Euler. Par contre, la connaissance de $\varphi(n)$, en ne connaissant que le produit $n = pq$, nécessiterait aussi un calcul de plusieurs millions d'années (à condition bien sûr de choisir p et q avec suffisamment de chiffres). Or, s'il n'est pas difficile d'obtenir d'un ordinateur des nombres premiers de cette taille, quelques minutes suffisent pour trouver un nombre premier s'écrivant avec 130 chiffres.

On sait (théorème d'Euler) que pour tout entier a étranger à n, on a :

$$a^{\varphi(n)} \equiv 1 \mod n$$

et donc, pour tout entier h

$$a^{h\varphi(n)+1} \equiv a \mod n .$$

Etant donné un entier $d \geqslant 2$ étranger à $\varphi(n)$, l'algorithme d'Euclide permet en quelques secondes à un ordinateur de trouver un entier e tel que

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

où $h \in \mathbb{Z}$.

Maintenant tous les personnages sont en place, la pièce peut commencer. Revenons à notre situation avec un émetteur et un récepteur. Le récepteur se choisit deux nombres premiers p et q et un entier $d \geqslant 2$. Il conserve *secret* le triplet

$$x = (p, q, d)$$

et rend *public*

$$y = T(x) = (n, e)$$

où n est le produit pq et e un entier tel que $ed - 1$ soit multiple de $\varphi(n)$.

Nous savons que la connaissance de $y = (n, e)$ rend pratiquement impossible la découverte de $x = (p, q, d)$ à condition d'avoir choisi des entiers premiers p et q assez grands.

Exemple: Sur cet exemple, les valeurs choisies pour p et q sont petites afin de nous permettre de suivre les calculs et le raisonnement. Supposons que l'émetteur ait choisi $p = 17$ et $q = 23$. Il calcule $n = pq = 391$ et $\varphi(n) = 16 \times 22 = 352$. Supposons maintenant qu'il choisisse $d = 101$: cet entier est bien étranger à $\varphi(n)$. Appliquons l'algorithme d'Euclide:

$$352 = 101 \times 3 + 49 \quad ,$$
$$101 = 49 \times 2 + 3 \quad ,$$
$$49 = 3 \times 16 + 1 \quad .$$

Cela nous confirme que 352 et 101 sont bien premiers entre eux et nous permet de trouver une relation de Bezout entre eux:

$$1 = 49 - 3 \times 16 = 49 - 16\,(101 - 49 \times 2) = 33 \times 49 - 16 \times 101$$
$$= 33\,(352 - 3 \times 101) - 16 \times 101 = 33 \times 352 - 115 \times 101 \quad .$$

Puisque $115 \times 101 = 33 \times 352 - 1$, l'émetteur peut choisir $e = 115$; il garde secret le triplet $x = (17 , 23 , 101)$ et rend public $y = (391 , 115)$.

Continuons à explorer ce nouveau dispositif. Supposons que l'émetteur E veuille transmettre à R un message M. Comme précédemment, M peut être considéré comme un entier, et si besoin, en le remplaçant par une suite de nombres, on peut supposer $M < n$. Pour coder M, l'émetteur va l'élever à la puissance e modulo n ; c'est-à-dire qu'il enverra à R le message

$$C_y(M) \equiv M^e \qquad \text{mod } n \quad .$$

Puisque $y = (n, e)$ est public, n'importe qui, en particulier l'émetteur, peut effectuer un tel calcul.

En possession du message codé $C_y(M)$, le récepteur pourra le décoder en appliquant la fonction D_x , qui consiste à élever le message codé à la puissance d modulo n (fonction qu'il est le seul à connaître). En effet:

$$D_x\, C_y(M) = D_x(M^e) = M^{ed} = M^{h\varphi(n)+1} \equiv M \qquad \text{mod } n \quad .$$

Exemple: Prenons à nouveau pour p et q de petites valeurs. Supposons par exemple que $p = 5$, $q = 11$. Alors, $n = pq = 55$ et $\varphi(n) = 40$. Si par exemple $d = 23$, alors $e = 7$. Donc, en résumé, est conservé secret par R le triplet $x = (5 , 11 , 23)$ et est rendu public le couple $y = (55 , 7)$.

Si maintenant E veut envoyer à R le message $M = 2$, il lui transmet, en fait, le message codé:

$$C_y(M) \equiv M^e \equiv 2^7 \equiv 18 \qquad \text{mod } 55 \, .$$

A la réception de ce message qu'il sait codé, R utilise D_x ;
il obtient:

$$D_x\, C_y(M) = (M^e)^d = 18^{23} = 18.18^2.18^4.18^{16} \equiv 18.49.36.26 \equiv 2 \mod 55.$$

Il retrouve bien le message original M que E voulait lui envoyer.

Supposons maintenant que la situation soit un peu plus complexe, qu'au lieu de deux personnes, on veuille organiser un réseau de communications secrètes entre s personnes $P_1, P_2, \ldots, P_s$. Chaque personne P_i se choisit deux entiers premiers p_i, q_i qu'elle conserve secrets, fait le calcul du produit $n_i = p_i q_i$, se choisit un entier d_i, fait le calcul comme plus haut d'un entier e_i tel que $e_i d_i - 1$ soit multiple de $\varphi(n_i)$ et rend public, par exemple au moyen d'un annuaire, $y_i = (n_i, e_i)$. Une personne P_j qui veut envoyer un message à P_i pourra utiliser le code public C_{y_i} de P_i. Seul ce dernier en possession de D_{x_i} pourra décoder le message codé ainsi envoyé.

Signalons que l'on peut trouver dans "Micro-Système" de janvier-février 1980, un programme (pour ordinateur) qui permet de chiffrer et de déchiffrer des messages selon cette méthode. Mais sans aller jusqu'à des solutions aussi perfectionnées, nous invitons nos lecteurs désireux de faire découvrir à leurs élèves la beauté et l'intérêt de l'arithmétique, à organiser au sein de leurs classes un réseau de relations secrètes basées sur la méthode que nous venons de présenter.

5. Signature d'un message

Deux précautions valent mieux qu'une, dit la sagesse populaire. On devine bien qu'un satellite artificiel ou un bombardier recevant un ordre, même convenablement codé, veuillent s'assurer, avant de passer à l'action, que l'ordre reçu provient bien de l'émetteur supposé. Cela exige que l'on soit en mesure de signer les messages d'une façon inimitable, parfaitement contrôlable par le récepteur.

La méthode précédente offre cette possibilité. Supposons que deux personnes P_1 et P_2 soient concernées et que P_2 ait à transmettre à P_1 un message M. L'émetteur P_1 va d'abord utiliser D_{x_1}, qu'il est le seul à connaître, avant d'appliquer C_{y_2} qui est public. Ainsi, il envoie à P_2 le message codé $C_{y_2}\ D_{x_1}(M)$.

Le récepteur P_2 suppose que ce message codé provient de P_1. Il peut trouver C_{y_1} dans l'annuaire public et il possède D_{x_2} (il est même le seul à le connaître). De la sorte, il peut retrouver M car:

$$C_{y_1}\ D_{x_2}\ C_{y_2}\ D_{x_1}(M) = C_{y_1}\ D_{x_1}(M) = M \quad .$$

Bien sûr, il suffisait d'y penser !

Les spécialistes considèrent qu'aujourd'hui, ce type de signatures apporte plus de sécurité que tout autre.

6. Ensuite ?

En supposant que la puissance de calculs des ordinateurs et la découverte de nouveaux algorithmes rendent raisonnable la recherche de x à partir de la connaissance de T(x), il suffira de changer de fonction trappe T et de renouveler les annuaires. Or d'autres fonctions trappes sont déjà connues et certaines d'entre elles ont trouvé des applications ailleurs qu'en cryptographie.

Bien que *théoriquement* inviolable, ce système possède des failles. Dans certains cas, des messages sont décryptables sans que l'on découvre la factorisation de $n = pq$. Un exemple explicite où p et q s'écrivent avec 30 chiffres est donné par C. POMERANCE dans [3]. Des précautions supplémentaires peuvent être prises pour éviter cet écueil, du moins semble-t-il, à l'heure actuelle.

*
* *
*

[1] Alain BOUVIER et Michel GEORGE, sous la direction de François LE LIONNAIS, *"Dictionnaire des mathématiques"*. PUF.

Les lecteurs qui voudraient en savoir plus sur la cryptographie publique pourront consulter avec profit:

[2] M.E. HELLMAN, *"An overview of public key cryptography"*. IEEE Communications society magazine. Novembre 1978. p. 24 - 32.

[3] C. POMERANCE, *"Recent developments in primality testing"*. The Math. Intel. Vol. 3, numéro 3 (1981). p. 97 - 105.

En particulier, l'article de POMERANCE explique comment l'étude des nombres pseudo-premiers fournit aujourd'hui des tests rapides de primalité.

Henri COHEN et Hendrik LENSTRA viennent de mettre au point un test qui permet en une minute environ de tester la primalité de nombres s'écrivant avec 90 chiffres; voir:

[4] M.E. HELLMAN, *"La mathématique de la cryptographie à clef révélée"*. Pour la Science, numéro 24 (1979). p. 114 - 123.

[5] D. LEGLU, *"La chasse aux nombres premiers"*. Sciences et Avenir, numéro 422, (1982). p. 70 - 76.

Je dois à Peter TAYLOR (Queen's University, Canada) de m'être intéressé à ce sujet. Je tiens à l'en remercier.

NDLR — Cet article est paru dans le numéro 28 de "Sans Tambour Ni Trompette", Bulletin IREM et APMEP de LYON.