Bulletin de la Société Royale des Sciences de Liège, Vol. 71, 4, 2002, pp. 199-209

COMMENT PARLER A QUELQU'UN QUAND TOUT LE MONDE VOUS ECOUTE

Georges HANSOUL

PREAMBULE. La communication privée existe depuis que la communication existe. Son utilisation entre partenaires éloignés et à des fins plus ambitieuses que la simple conversation entre confidents a fait naître cette chose quelque peu étrange qu'est la cryptologie, tout à la fois un art et une science, servant autant le mal que le bien, elle se parfume d'un relent d'histoire d'espionnage et est en même temps enseignée dans les universités ; elle se nourrit de la puissance des plus grands ordinateurs alliée aux mathématiques les plus abstraites et ses heures de gloire lui furent données tout aussi bien par des grands stratèges que des scientifiques enfermés dans leur tour d'ivoire.

Dans cette courte note, nous envisagerons trois aspects généraux de la cryptologie :
1) à qui sert-elle ? (ce qui nous conduira à une brève histoire de la cryptologie à travers ses utilisateurs),
2) Comment sert-elle, quelles sont les procédures classiques et comment mesure-t-on leur efficacité ? (ce qui nous obligera à une incursion dans le monde des mathématiques, qu'elles surgissent des temps passés ou soient le fruit de découvertes récentes),
3) à quoi sert-elle (outre l'usage communément connu et évoqué dans le titre de cette note) ?

SECTION 1 *En guise de définition*

On résume souvent la cryptologie à l'étude des codes secrets. L'utilisation de codes pour transmettre une information n'est pas une caractéristique typique de la cryptologie. Toute information doit être codée pour être transmise. On pourrait même dire à la limite que l'information « à l'état pur » n'existe pas : elle est déjà codée en impulsions électromagnétiques que ce soit dans le cerveau de celui qui la détient ou dans la mémoire de l'ordinateur dans lequel elle est stockée. De plus, pour être transmise, elle doit être de nouveau codée : dans un langage qui peut être oral (et donc dit dans une langue spécifique), écrit (avec des symboles spécifiques), de programmation (double codage d'un langage machine lui-même transformé en impulsions électromagnétiques), ou autre

(gestuel, ...). Rien que ceci confère au transfert d'information un certain caractère secret, en tout cas inintelligible à certains (un message écrit n'est pas compris d'un analphabète, nous comprenons peu le langage des animaux, etc ...). Sans essayer d'être formel ni vouloir cerner de façon définitive un concept qui évolue sans cesse, nous considérons ici la cryptologie comme l'étude raisonnée des moyens d'assurer la sécurité de l'information alors qu'elle s'achemine entre deux parties au travers d'un canal réputé non sûr (on parle souvent à l'heure actuelle de *sécurité informatique*). Ce mot « sécurité » est à prendre au sens large, mais comporte deux aspects fondamentaux : l'information doit parvenir non altérée (authenticité) et uniquement aux personnes désignées (secret).

SECTION 2 *Les utilisateurs*

En Syrie, à Jerfel-ahmar, on a découvert des plaquettes en pierre gravées et l'on estime qu'il s'agit là des premiers écrits découverts à ce jour (ils ont été datés du X^{ème} millénaire avant J.-C.). Des tablettes semblables quoique plus récentes ont été retrouvées dans des bulles d'argiles qui accompagnaient les guides des caravanes lors de leurs longs périples, à but essentiellement commercial, entre la Mésopotamie et la Syrie. Ces tablettes faisaient en quelque sorte l'inventaire de la caravane : nature et quantité des produits transportés. Sans vouloir être définitif, on imagine aisément l'un des objectifs de ces tablettes : les esclaves ne sachant lire les tablettes ne pouvaient ni en déformer le contenu ni même en prendre connaissance. Les deux attributs de la cryptographie : secret et authenticité du message, étaient déjà présents à l'aube de la civilisation écrite.

Il faut ici parler de cryptographie et non de cryptologie, concept plus vaste qui ne s'occupe pas seulement des techniques d'encodage mais aussi des techniques de décodage vues du point de vue d'un intercepteur non légitime du message. Dans le cas que nous venons d'évoquer, cette dernière occupation est inexistante : la population est divisée en deux catégories : ceux qui savent lire et ceux qui ne savent pas. La volonté de secret n'est pas farouche mais découle naturellement d'un état de fait. Cette « cryptographie passive » se retrouve dans de nombreuses situations où une catégorie de soi-disant élus veut se distinguer de la masse. Ainsi les sociétés secrètes où toute une symbolique tient lieu de cryptogramme. Dans certaines civilisations Perses existait un parler distinct de la langue commune appelée « langage des rois ». Dans le même ordre d'idée, le latin utilisé au Moyen-Age distinguait les nobles du vulgaire qui ne le comprenait pas. Les argots et jargons de toutes sortes peuvent dans une certaine mesure être assimilés à un système cryptographique : pensons au verlan, au lenou, et même au jargon des mathématiciens ou pire encore celui des informaticiens.

Si l'on désire entrer plus en avant dans le vif de la cryptologie, là où des codes secrets sont spécifiquement conçus pour empêcher toute compréhension en dehors des personnes désignées, c'est tout naturellement vers l'armée que l'on se tourne, de tout temps utilisatrice privilégiée de communication secrète : la réussite d'une stratégie dépend de façon cruciale du fait que l'ennemi n'en soit pas informé. Les militaires, à côté de systèmes ingénieux mais peu reproductibles, furent les premiers à inventer des procédés systématiques de codage, faisant passer la cryptographie du stade artisanal à un stade de technique. Ainsi au V^{e} siècle avant J.-C., les militaires de Spartes utilisent un instrument appelé *scytale* : un papyrus long et étroit est enroulé autour d'un axe de bois ; le message est écrit parallèlement à l'axe, donc en recoupant toutes les bandes du papyrus. Dès lors le texte original se retrouve en bouts épars sur le papyrus déroulé. Les Grecs ont vraisemblablement mis au point plusieurs systèmes cryptographiques mais on sait peu de

leur utilisation effective et leur portée dans l'histoire. Les cryptologues ont cependant retenu le procédé dit du *carré de Polybe* où l'alphabet est écrit dans un tableau à double entrée et chaque lettre du message remplacée par les numéros de la ligne et de la colonne correspondante. Il s'agit d'un exemple simple du *procédé de substitution*, base de presque tous les chiffrements modernes : chaque lettre (substitution monoalphabétique) ou groupe de lettres (substitution polyalphabétique) est systématiquement remplacé par une lettre ou un groupe de lettres selon un encodage révélé uniquement au destinataire du message. Il est bien connu que Jules César lui-même - après avoir écrit ses messages en grec pour les soustraire à la compréhension des Gaulois - a utilisé un système de substitution mono alphabétique : chaque lettre est remplacée par la lettre située trois places plus loin dans l'ordre alphabétique.

Tout autant que la stratégie militaire, le monde des ambassades et des diplomates doit des succès retentissants à l'usage de correspondances cryptées. La papauté en Italie, Charles-Quint en Espagne, Richelieu puis Louis XIV en France, les Stuart en Angleterre et à un niveau plus intense encore dans la maison d'Autriche, tous les grands des XVI^{e}, XVII^{e} et XVIII^{e} siècles possèdent leurs cabinets secrets où sont cryptés et décryptés les écrits qui y transitent. La plupart des cryptosystèmes utilisés sont bâtards en ce qu'ils comportent à la fois une partie substitutive et ce qu'on appelle une partie codique : certains mots revenant souvent dans un message se voient attribuer un code, une succession de quelques lettres, le représentant. Ces codes sont consignés dans des répertoires gardés au secret (jusqu'au jour où ils sont dérobés par l'adversaire...).

L'histoire retiendra surtout les noms d'Antoine Rossignol, sans doute le premier cryptologue à temps plein, attaché à la cour de France ; de John Wallis, un des rares mathématiciens à s'intéresser à la cryptologie et finalement celui du Baron de Vigenère qui répertoria plus qu'il n'inventa de nombreux systèmes dont un porte son nom. Le chiffre de Vigenère n'est autre qu'un chiffre de César polyalphabétique : la valeur du décalage varie selon la position de la lettre dans le texte et est donnée par un mot clé. En voici un exemple, codé à l'aide du mot clé VIGENERE :

```
  LAVRAIERICHESSEESTLETEMPSQUELONPOSSEDE
+ VIGENEREVIGENEREVIGENEREVIGENEREVIGENE
  GIBVNMVVDKNIFWVINBRIGIDTNYAIYSETJAYIQI
```

(voir la section suivante pour une explication détaillée).

La petite histoire de la cryptographie ne manquera pas pour son compte d'épingler le nom de Casanova. Dans ses mémoires, celui-ci se flatte d'avoir séduit Madame d'Urfé en décryptant un texte qu'elle avait encodé sans dévoiler à quiconque le mot clé (qui était NABUCHODONOSOR et que Casanova détermina aussi).

On peut imaginer que Casanova procéda comme la plupart des cryptographes de son temps : intuition, ingéniosité, persévérance. En effet, peu de réels progrès théoriques sont faits pendant la période « des cabinets noirs ». Tout au plus voit-on se généraliser les substitutions polyalphabétiques et naître quelques machines à coder. La littérature cryptologique est d'ailleurs assez pauvre. Trois exceptions cependant : un traité de cryptanalyse (très en avance sur son époque) par l'arabe Qalqashandi (début du XV^{e} siècle, très vite tombé dans l'oubli), l'excellent travail de compilation de Vigenère et le traité de cryptologie militaire de Kerckhoffs (début du XIX^{e} siècle) qui inscrit son travail dans une réflexion théorique fort moderne.

Un peu plus tard, l'invention du télégraphe, en multipliant de façon extraordinaire le flux d'information échangée de par le monde, a considérablement élargi le spectre des utilisateurs de cryptographie, qui devient alors affaire d'état en temps de guerre comme en temps de paix. Cependant, il faut réellement attendre la deuxième guerre mondiale pour que la cryptologie devienne une discipline scientifique à part entière. Épinglons deux raisons qui nous semblent déterminantes à cet égard : l'impérieuse nécessité pour les belligérants de décoder les messages ennemis et la naissance des ordinateurs.

Dès la fin de la première guerre mondiale, les Allemands ont patiemment mis au point une machine à chiffrer performante appelée ENIGMA. Celle-ci se présente sous la forme d'une machine à écrire. Sous le clavier cependant trois *rotors*, sortes de disques plats où sont réalisées des connexions électriques entre les 26 positions d'une face et les 26 positions de l'autre. Les rotors peuvent tourner indépendamment les uns des autres, ce qui permet de réaliser un nombre extrêmement élevé de substitutions, rendant le décryptage par des moyens classiques quasi impossible. Cependant, l'équipe anglaise (et dans une moindre mesure les équipes françaises et polonaises) parvint à décrypter ENIGMA à tel point que les Allemands crurent être infiltrés. Or il n'en était rien. Mais l'équipe anglaise - pour ne parler que d'elle - avait la chance de compter parmi ses membres le mathématicien Alan Turing. Celui-ci, père de la calculabilité et pionnier de l'informatique, sut allier ses idées à la récupération de rotors allemands dans un sous-marin allemand coulé pour créer des machines de décryptement - les COLOSSUS - performantes.

Après la guerre, les progrès réalisés en informatique et en mathématiques font littéralement exploser le développement de la cryptologie, dans des directions qui dépassent de loin le cadre de cette note. La cryptologie envahit le domaine civil et s'occupe de sécuriser les transactions commerciales, industrielles, bancaires, ... Quelques aspects seront brièvement évoqués dans la section 4. Nous ne parlerons ici que de deux sigles qui firent date : DES et RSA.

Dans les années 60, la NSA (agence de sécurité des Etats-Unis) confie à la NBS (bureau des standards américains) la tâche de créer un système de chiffrement qui serait d'utilisation à la fois simple, rapide et sûre. Après six ans de travaux est présenté le système DES (data encryption standard) qui connaîtra un succès général - malgré les critiques qui lui furent adressées. Son principe est simple : la substitution caractère à caractère, mais non plus sur un alphabet de 26 lettres mais des unités de 64 bits (prenant chacun valeur 0 ou 1), ce qui donne 2^{64} unités possibles. Dans sa première version, la clé est donnée par une chaîne de 56 bits. Cette clé est mélangée au texte clair, puis subit une substitution et ce processus est recommencé 16 fois. Les 16 substitutions sont spécifiées dans 16 « boites noires » construites par la NBS. Depuis plusieurs années déjà, la puissance des ordinateurs augmentant rapidement, le DES ne résiste pas à une attaque dite de force brute où l'on essaye les clés une à une. La NBS a préconisé que l'on fasse 3 tours de DES pour crypter, triplant ainsi la longueur de la clé, mais il est clair que le DES a cessé d'être un système sûr. D'autres standards sont proposés par la NSA, tel le AES, mais on assiste à une libéralisation du marché dans ce domaine.

Le DES, tout comme tous les systèmes de cryptographie envisagés avant lui, souffre d'une faiblesse qu'on a crû longtemps inhérente à la cryptologie : la transmission des clés. Que celle-ci se fasse lors de rencontres secrètes, ou par la voie de la valise diplomatique, ou soit consignée dans des registres secrets..., rien n'est à l'abri d'un espion habile, d'une fouille bien menée, d'un interrogatoire musclé ou d'une découverte fortuite (pensez à ENIGMA)... Contre toute attente, en 1976, Diffie et Hellman décrivent un système de communications sécurisées entre plusieurs parties sans qu'aucune clé ne doive

être échangée. Le principe repose sur l'utilisation de fonctions unidirectionnelles dont nous parlerons dans la section suivante. Sur le même principe, en 1978, Rivest, Shamir et Aldeman publient un système appelé depuis RSA et qui est l'un des plus étudiés et l'un des plus usités à l'heure actuelle.

SECTION 3 *Quelques systèmes de chiffrement*

Sans vouloir être exhaustif, sans être trop technique et en essayant de décrypter le langage des spécialistes, nous allons présenter ici quelques exemples de systèmes cryptographiques afin de donner corps aux propos de la précédente section, de montrer comment des disciplines mathématiques classiques (théorie des nombres, algèbre, probabilités,...) viennent conjuguer leurs efforts pour aider le cryptologue et d'entrouvrir quelque peu le voile sur les défis mathématiques actuels lancés par la cryptologie moderne.

Nous l'avons déjà dit, une des idées de base de la cryptographie est la substitution : si je décide de remplacer A par H, B par Z, ..., M par A, N par C, O par I, P par S, Q par Y, R par E, ..., U par N, ... alors AMOUR devient HAINE, ce n'est pas plus compliqué. Certaines substitutions sont plus faciles à décrire que l'énumération fastidieuse de l'avatar subit par chaque lettre. L'ordinateur de bord du vaisseau spatial lancé vers Jupiter par Stanley Kubrik[1] a vu son vrai nom crypté en substituant à chaque lettre celle qui lui précédait dans l'alphabet (c'est pourquoi il se nomme HAL dans le film). Ce « chiffre de César » est facile à décrire, par la locution « décalage d'une place vers l'arrière » ou encore « décalage de -1 ». Il peut donc se traduire par l'équation $x \mapsto x-1$.

Avant de compléter la formalisation, posons nous la question suivante : dans le système précédent, que devient la lettre A ? Si l'on imagine les lettres de l'alphabet écrites sur un disque, Z précédera tout naturellement A (tout comme dans un décalage +5, la lettre X deviendra C, Y deviendra D etc ...). Autrement dit, si l'on représente les lettres par la position qu'elles occupent dans l'alphabet, le A est aussi bien la lettre de numéro d'ordre 0, que celle d'ordre 26, 52 ... Cette nouvelle conception de l'égalité (qui spécifie par exemple 0=26, 1=53, 20=-6 etc ...) donne lieu à une arithmétique fort amusante, appelée *arithmétique modulaire*, et dont nous allons donner ici un bref aperçu. Afin de pouvoir considérer des alphabets plus généraux que l'alphabet traditionnel, nous allons abandonner ce rôle privilégié joué par le nombre 26 et présenter l'arithmétique modulo N où N est un naturel quelconque.

Cette arithmétique comporte exactement N nombres différents, à savoir 0,1,2, ...,N-1, puisqu'à partir de N, tout recommence : N = 0, N+1 = 1, ... De façon plus précise, deux nombres sont égaux si leur différence est multiple de N, ce que l'on écrira $p = q \pmod N$ si et seulement si N divise $p-q$.

Ces nombres sont appelés entiers modulo N et leur ensemble noté Z_N. On peut évidemment les additionner ou les multiplier de la façon usuelle, mais cela donne lieu à des tables de multiplication surprenantes. Ainsi 7.10 = 70 mais comme 70 = 18 (mod 26), on écrira de façon standard 7.10 = 18 (mod 26).

La soustraction s'effectue sans problème mais la division exacte réserve des surprises. Évidemment, un nombre modulo 26 est divisible par 2 si et seulement s'il est pair. Par contre, tout nombre modulo 26 est multiple de 3, comme on le voit en écrivant la liste exhaustive des multiples de 3 : 0, 3, 6, 9, 12, 15, 18, 21, 24, 1, 4, 7, 10, 13, 16, 19, 22,

[1] Dans le film « 2001, odyssée de l'espace », évidemment.

25, 2, 5, 8, 11, 14, 17, 20, 23, qui épuise effectivement la liste des 26 nombres modulo 26. En particulier, 1 est multiple de 3 et l'on peut même préciser que 1=3.9 (mod 26), ce que l'on pourrait écrire $\frac{1}{3} = 9 (\mathrm{mod}\, 26)$ (on dit que 3 admet un inverse dans Z_{26}, à savoir 9).

Le résultat suivant est important : *le nombre a admet un inverse modulo N si et seulement si a est premier avec N*. Le seulement si se démontre facilement. En effet, si a et N admettent le facteur d en commun, il est clair que les multiples de a seront toujours des multiples de d, quelle que soit la façon dont on les écrit modulo N. Si d ? 1, aucun multiple de a ne peut être égal à 1. La réciproque est un peu plus ardue à démontrer, mais était déjà connue des mathématiciens arabes du XIII^{e} siècle.

Pour présenter un exemple simple de système cryptographique, nous allons utiliser le jargon usuel du cryptologue. C'est systématiquement la charmante Alice (pour A) qui désire envoyer un message à son ami Bob (pour B) sans que l'infâme Oscar (pour O), interceptant le message de façon illégitime, ne puisse en comprendre la teneur. À cette fin, le message clair M (décomposé en fragments ou unités claires $M = mm_1m_2\ldots$) est transformé par Alice en un message secret M' (obtenu en transformant les unités claires m en m', m_1 en m'_1, ...) par un procédé que seuls Alice et Bob connaissent. Alice enverra M' à Bob qui, connaissant, le procédé d'encodage $M \blacklozenge M'$, pourra inverser le procédé et retrouver le message originel M.

Une *substitution linéaire*, une fois les lettres encodées par leur équivalent numérique dans Z_N, s'exprime par une fonction du premier degré $m \mapsto m' = am + b$.

Étudions le cryptosystème linéaire du triple point de vue d'Alice, Bob et Oscar.

Tout d'abord, Alice ne peut pas choisir n'importe quels paramètres a, b pour confectionner son chiffre : il est nécessaire que des lettres différentes soient codées différemment pour que Bob puisse décoder sans ambiguïté. Le résultat est le suivant : *le chiffrement $m \mapsto am + b$ dans Z_N se décode sans ambiguïté si et seulement si a admet un inverse dans Z_N*.

Les paramètres a et b forment ce que l'on appelle la *clé* du cryptosystème. En effet, une fois la clé connue, tout le procédé de chiffrement est déterminé. C'est la clé qui sera choisie par Alice et transmise en secret à Bob. Celui-ci peut alors aisément décoder tout message venant d'Alice connaissant $m' = am + b$, il doit retrouver m qui vaut $\frac{m'-b}{a}$, puisque $\frac{1}{a}$ existe.

Tout différent est le travail d'Oscar : interceptant $M' = m'm'_1m'_2\ldots$, il doit retrouver $M = mm_1m_2\ldots$ sans connaître la clé. Cela s'appelle *briser* le code, et l'étude des techniques permettant de briser un code est la *cryptanalyse*.

Lorsque l'on étudie un cryptosystème du point de vue d'Oscar, on supposera toujours que celui-ci connaît au moins le type de système utilisé (c'est le premier des principes que Kerckhoffs avait énoncé dans son traité de cryptologie militaire). On distingue alors plusieurs niveaux de cryptanalyse selon les informations dont dispose Oscar : attaque à texte secret connu, attaque avec accès temporaire à la machine chiffrante, attaque avec accès temporaire à la machine déchiffrante. Les deux dernières attaques ne

sont à envisager que pour des cryptosystèmes évolués. Ici, nous nous contentons d'envisager une attaque de premier niveau. Si l'espace des clés n'est pas trop grand, Oscar peut se permettre d'essayer toutes les clés une à une (recherche exhaustive). C'est évidemment le cas pour une cryptanalyse informatique du cryptosystème linéaire (512 clés pour N = 26) qui n'est évidemment plus jamais utilisé.

Pour des espaces de clés dépassant la capacité des ordinateurs, des méthodes d'attaque plus sophistiquées existent. La plupart reposent sur des considérations statistiques que nous allons illustrer sur notre exemple linéaire.

Supposons qu'Oscar intercepte le message suivant :

N X L X P P D H X X P U Z Q C D Z O L X P P D H X Q X Q U X Q X Y A D P N V L A U X.

Conformément au principe de Kerckhoffs, il sait qu'on a utilisé une substitution linéaire dans Z_{26}. Monsieur Jacques de Chabannes en eût dit autant : la lettre se retrouvant le plus souvent dans ce texte secret est l'encodage de la lettre se retrouvant le plus souvent dans le texte clair. Depuis longtemps (l'arabe Qalqashandi abordait déjà ce problème dans son traité) on s'est aperçu que certaines lettres reviennent plus souvent que d'autres dans les textes courants. L'étude statistique globale de fréquence dépend très peu du texte lui-même (pourvu qu'il soit assez long et avec exception pour des sujets fort spécialisés) mais plutôt de la langue dans laquelle il est écrit, avec quelques variations dans le temps. Ainsi en français le E est le plus fréquent, puis assez loin derrière, les lettres S, A, R et T (plus ou moins dans cet ordre) et comme deuxième peloton I, N, U, L, O et C. Examinant le message secret. Oscar déduit que le E est devenu X (10 occurrences) et que le S est devenu P (6 occurrences). La fonction de codage $m' = am + b$ doit être telle que $m = 4$ (pour E) donne $m' = 23$ (pour X) et $m = 18$ donne $m' = 15$. On obtient le système suivant :

$$\begin{aligned} 23 &= 4a + b \\ 15 &= 18a + b \end{aligned}$$

Un peu d'arithmétique modulaire (amusante parce qu'elle nous force à repenser les routines de résolution implantées en nous depuis notre jeunesse) livre deux solutions : $a = 5, b = 3$ ou $a = 18, b = 3$. La deuxième est à rejeter : n'oublions pas qu'Alice a choisi une clé a admettant un inverse. Ainsi $m' = 5m + 3$ et quelques calculs livrent la fonction de décodage $m = 21m' + 15$ et donc la possibilité pour Oscar de décrypter le message illégitimement intercepté (il sera bien déçu).

On obtient des cryptosystèmes plus difficiles à briser en réalisant une substitution polyalphabétique : le texte est découpé en blocs de longueur fixe, disons k .et chaque bloc est encodé comme un vecteur $\vec{m} = (m, m_1, \ldots)$ dont les composantes sont des fonctions linéaires des composantes de $\vec{m}$: $m' = am + bm_1 + \ldots + c$, $m'_1 = \ldots$, ...

(En langage matriciel, on obtient une formule agréable $\vec{m'} = A\vec{m} + \vec{b}$). L'espace des clés est beaucoup plus vaste puisque une clé consiste en la donnée des $k^2 + k$ paramètres nécessaires pour décrire l'encodage.

Un cas particulier ($a = 1, b = 0, \ldots,$) est le système de Vigenère (avec mot clé $\vec{b}$) décrit dans la section précédente. À ce propos, il importe de décrire ici une adaptation intéressante de ce cryptosystème, d'ailleurs effectivement utilisée par les services secrets soviétiques. C'est un cryptosystème de Vigenère où le message est considéré comme un seul bloc, c'est-à-dire où la clé est aussi longue que le message lui-même. Ceci peut paraître aberrant puisque la transmission de la clé, qui pour des raisons de sécurité ne peut servir qu'une seule fois, pose exactement les mêmes problèmes que celle du message. Ce système est pourtant utilisable en pratique et même très performant dès lors que l'on parvient à concilier deux exigences contradictoires : la faisabilité (donner un algorithme simple générant la clé) et la sécurité (générer une clé aléatoire, impossible à deviner). De telles clés sont appelées pseudo-aléatoires et leur étude a débouché sur la naissance de théories passionnantes comme la *théorie de la complexité* où les problèmes sont tout aussi bien de nature philosophique (qu'est-ce que l'aléatoire) que pragmatique (combien de temps faut-il pour multiplier deux nombres).

Venons-en à la révolution cryptographique de 1976, où fut donnée une solution étonnante au problème délicat de l'échange des clés. Tout d'abord , la théorie de la complexité a permis d'affiner la perception que l'on peut avoir d'Oscar. La cryptographie moderne se préoccupe de la capacité de calcul d'Oscar : pour parler pompeusement, Oscar est assimilé à un *algorithme probabiliste polynomial*. Dans ces conditions a pu voir le jour l'importante notion de *fonction unidirectionnelle* : une fonction f dont l'évaluation (calculer $y = f(x)$ connaissant x) est facile (calculable pour Oscar) alors que son inversion (trouver x si $f(x) = y$ est donné) est difficile (non calculable pour Oscar). La cryptographie imaginée par Diffie et Hellman distingue la clé K de codage (donnant le codage c_K) de la clé de décodage K' (donnant le décodage $d_{K'}$) et impose que le passage de K' à K soit unidirectionnel. On procède alors de la façon suivante. Tout un pool d'utilisateurs potentiels s'assemblent pour réaliser un réseau de communications sécurisées. Chaque utilisateur : A(lice), B(ob), C(ésar), ... se choisit une clé de décodage $K'_A, K'_B, K'_C, \ldots$ calcule la clé de codage correspondante K_A, ... et la publie. (C'est pourquoi on parle de *système à clé publique*.) Lorsqu'Alice veut envoyer un message à Bob (dont la teneur doit être inconnue même de César), elle le code avec la clé de Bob (clé dont l'accès est public) qui, seul possesseur de sa clé de décodage, peut seul décoder le message.

Reste à donner quelques exemples de fonctions unidirectionnelles aux propriétés si bien venues. À vrai dire, aucune fonction unidirectionnelle n'est connue à l'heure actuelle et l'on doit se contenter de candidats (ainsi, la gloire - ou la gloire et la puissance - est acquise à l'heureux qui prouvera l'existence - ou la non-existence - de fonctions unidirectionnelles). Un bon candidat (sur lequel repose le système RSA) est la multiplication de deux nombres premiers :

$$p, q \mapsto pq.$$

Pour se convaincre de la difficulté de retrouver p et q connaissant leur produit pq, plaçons nous dans les conditions actuelles de l'usage de cette fonction : p et q sont de grands nombres premiers de l'ordre de 10^{100}, pris hors de tables connues de nombres premiers et assez éloignés l'un de l'autre, par exemple $p \cup 10^{90}$ et $q \cup 10^{110}$. Multiplier ces nombres prendra moins d'une minute à un bon ordinateur. Imaginons que l'on nous apporte $n = pq$ sur un plateau avec pour tâche de retrouver p et q. Nous sommes peu versés dans l'art de la factorisation et avons décidé d'effectuer les divisions de n par tous les impairs 3, 5, 7, ... jusqu'à trouver une division exacte : nous nous sommes mis $(1/2)10^{90}$ divisions sur le dos, quel pensum. Imaginons un ami[2], virtuose de l'informatique, capable d'effectuer 10^{20} opérations à la seconde et 10^{20} fois plus futé que nous. Il lui faudra alors $(1/2)10^{50}$ secondes pour trouver le facteur p (alors que l'âge de l'univers est moindre que 10^{19} secondes !).

D'autres candidats sont connus, la plupart faisant appel à l'arithmétique modulaire (cf. [4] et [5]).

SECTION 3 *Divers aspects de la sécurité informatique*

Dans cette brève section, nous allons énumérer quelques applications parfois surprenantes de la cryptologie.

1. À côté du caractère secret ou privé de la communication, les cryptosystèmes à clé publique ont augmenté l'attention à porter à l'authenticité du message. Rien n'empêche, dans le protocole proposé, à Oscar d'envoyer un message à Bob (seule la clé publique de Bob est nécessaire) en prétendant qu'il vient d'Alice.

Pour parer à cette fraude, Alice utilise la procédure dite du *message signé*, qui consiste à surcrypter le message m qu'elle veut envoyer, tout d'abord avec la clé publique de Bob (on obtient $c_{K_B}(m)$) et ensuite avec sa propre clé (elle envoie donc $m' = d_{K_A} c_{K_B}(m)$). Bob pour le décoder utilise, avant sa propre clé de décodage, la clé publique d'Alice, vérifiant ainsi que seule Alice pouvait l'envoyer.

2. Signer un document électronique de la façon usuelle est évidemment très facile à imiter. La procédure du message signé qui vient d'être décrite est infalsifiable, mais produit une signature aussi longue que le message. On utilise alors des fonctions spéciales dites de hachages qui compactent le message avant de le signer. Un des problèmes majeurs de la théorie des fonctions de hachage (hash functions) est d'éviter les collisions, c'est-à-dire la possibilité que deux textes distincts mènent à la même signature.

À côté de la possibilité de signer, des protocoles ont été mis au point pour prouver qu'une signature donnée est un faux, pour qu'une signature soit impossible à désavouer, pour que la vérification d'une signature requière nécessairement la participation du signataire etc...

3. Dans la pratique, utiliser un cryptosystème à clé publique comme RSA requiert beaucoup plus de temps qu'utiliser un protocole standard à clé secrète, comme DES ou

[2] Si à peu près personne n'a un ami ayant gagné € 250.000 à la loterie, à peu près tout le monde a un ami féru d'ordinateurs.

l'une de ses améliorations. La rapidité de l'une se combine avec la sécurité de l'autre si l'on utilise un protocole public d'échange de clés secrètes. Autrement dit, Alice et Bob vont communiquer à l'aide d'un système classique, utilisant une clé secrète K mais ne devront pas se la transmettre par un canal sécurisé : Alice va la donner à Bob en utilisant un cryptosystème à clé publique.

Nous présentons ici un protocole d'échange de clé dû à Diffie et Hellman. Il repose sur un résultat d'arithmétique modulaire et une conjecture.

Résultat. *Si p est un nombre premier, tout entier non nul modulo p est une puissance de l'un d'entre-eux convenablement choisi* (appelée *élément primitif* de Z_p).

Conjecture. Si p est un nombre premier et si α est primitif, *la fonction $y = \alpha^x$ est unidirectionnelle.*

Alice et Bob peuvent construire la clé secrète K avec laquelle ils vont communiquer de la façon suivante : 1) choix public d'un nombre premier p et d'un élément primitif α ; 2) Alice se choisit secrètement un exposant $x_A < p-1$, Bob se choisit secrètement un exposant x_B ; 3) Alice envoie α^{x_A} à Bob et Bob envoie α^{x_B} à Alice. La clé K est $K = \alpha^{x_A x_B}$. Alice peut la calculer car $K = (\alpha^{x_B})^{x_A}$ de même que Bob car on a aussi $K = (\alpha^{x_A})^{x_B}$. Oscar, même s'il a intercepté α^{x_A} et α^{x_B} ne peut calculer K car il ne peut retrouver ni x_A ni x_B tant que la conjecture énoncée précédemment tient le coup.

4. Assez curieusement, après tant de communications secrètes, Alice et Bob divorcent. Un point d'importance : qui garde le chien ? Alice (à Marrakech) et Bob (à Paris) décident de jouer cela à pile ou face. Mais comment jouer à pile ou face au téléphone sans possibilité de tricher ? Une procédure repose sur la difficulté de factoriser et le résultat suivant.

Résultat. *Si n est le produit de deux nombres premier, un entier modulo n qui admet une racine carrée en admet quatre, dont exactement deux comprises entre* 0 *et* $n/2$. *Si l'on connaît l'une d'entre-elles, la connaissance de l'autre est équivalente à la factorisation de n.*

Voici alors un protocole possible :
1) Alice choisit deux grands nombres premiers p et q et livre le produit $n = pq$ à Bob ;
2) Bob choisit un entier x modulo $n(x < n/2)$ et livre $c = x^2$ à Alice. À ce moment, Bob ne connaît pas l'autre racine y de $c(y < n/2)$ car il ne connaît pas p et q alors que Alice peut calculer les deux racines $(< n/2)$ de c.
3) Alice nomme une des racines. Si ce n'est pas x, elle perd et Bob le lui signale en lui révélant x. Si c'est x, elle gagne et Bob doit en convenir car il ne peut lui révéler l'autre racine et ne peut donc prétendre qu'il avait choisi cette autre racine !

À côté de cette utilisation quelque peu anecdotique, la cryptologie s'occupe aussi de sécuriser les cartes bancaires, l'Internet et les télécommunications en général ; elle donne les moyens de réaliser une télévision cryptée ; elle permet de se prémunir des copies frauduleuses d'images numériques de toutes sortes (tatouage) etc …, autant de domaines qui demanderaient de longs développements. Terminons ce bref aperçu par un dernier exemple, le partage de secrets.

5. Il n'est pas rare qu'une opération sensible (mise à feu de missiles, ouverture d'un coffre-fort, ...) requière la coopération de plusieurs personnes pour éviter les dérives que le pouvoir peut exercer sur une personne seule. Imaginons ici l'opération sensible matérialisée par la connaissance d'une clé K. Le but est de confier à Alice et Bob des informations K_A et K_B respectivement de façon que

1) la connaissance conjointe de K_A et K_B donne la clé K,

2) la connaissance de K_A ou de K_B seuls ne donne aucune information sur la clé K (ainsi donner à Alice et Bob des morceaux de clé ne convient pas car ce serait donner à Alice et à Bob des fragments d'information dont ils pourraient profiter).

La solution présentée ici brille par sa simplicité et ne demande que quelques rudiments de géométrie : la clé K est matérialisée par un point sur une droite d donnée publiquement. À Alice et Bob sont donnés secrètement des points K_A et K_B du plan tels que K soit à l'intersection de d avec la droite K_AK_B : les stipulations 1) et 2) sont visiblement satisfaites.

Bibliographie

[1] F. Bauer, Decrypted Secrets, Springer-Verlag, Berlin, 1997.

[2] D. Kahn, The Codebreakers, The Macmillan Company, New York, 1967.

[3] N. Koblitz, A course in Number Theory and Cryptography, Springer-Verlag, Berlin, 1987.

[4] A. Salomaa, Public-Key Cryptography, Springer-Verlag, Berlin, 1990.

[5] D. Stinson, Cryptography : theory and practice, CRC Press, Boca Raton, 1995.

Algèbre et Logique
Institut de Mathématiques (B37)
Université de Liège
4000 Liège