Le chiffre d'hier et de demain

A l'occasion du 80e anniversaire de l'ARCSI

L'Association des réservistes du chiffre et de la sécurité l'information, l'Arcsi[1], a organisé un colloque sur la cryptologie et son histoire le 10 octobre dernier. Le sujet du chiffre reste aujourd'hui au cœur des solutions de sécurité des systèmes d'information.

[1] www.ssi.gouv.fr/fr/arcsi/index.html

Le colloque relate l'histoire du chiffre avec des exemples qui remontent aux Égyptiens (hiéroglyphes inconnus datant de 1900 ans avant Jésus-Christ), aux Lacédémoniens (la Scytale) ou aux Romains (le chiffre de Jules César) reposant sur les deux grands procédés cryptographiques : la substitution et la transposition (à distinguer des procédés stéganographiques visant à dissimuler un secret dans une masse d'informations anodines).
Les besoins de chiffrement sont donc anciens et bien antérieurs à l'informatique. Le porteur d'un message peut tomber dans une embuscade, par exemple, et il faut ainsi protéger le contenu du message en cas d'interception. Le chiffrement disparaît toutefois durant de nombreux siècles pour ne réapparaître qu'à la Renaissance. La France dispose alors de réelles compétences et d'un véritable service du chiffre. Celui-ci disparaît à nouveau sous la révolution. Le milieu du 20e siècle voit apparaître le chiffre dans une dynamique commerciale et littéraire, mais ignore le chiffre militaire. On y remarque la célèbre lettre de George Sand à Alfred de Musset, qui se lit en ignorant les lignes paires (voir ci-contre). Le procédé est simple, mais le chiffrement du contenu réel.

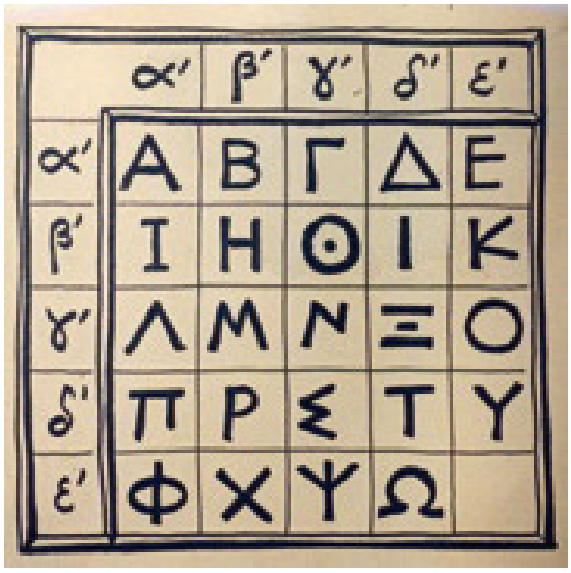
Lettre de George Sand

Je suis très émue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit là une preuve que je puisse être aimée par vous. Je suis prête à vous montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir aussi vous dévoiler sans artifice mon âme toute nue, venez me faire une visite. Nous causerons en amis, franchement. Je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde comme la plus étroite en amitié, en un mot la meilleure preuve dont vous puissiez rêver, puisque votre âme est libre. Pensez que la solitude où j'habite est bien longue, bien dure et souvent difficile. Ainsi en y songeant j'ai l'âme grosse. Accourrez donc vite et venez me la faire oublier par l'amour où je veux me mettre.

Lire une ligne sur deux pour avoir la clé de déchiffrement

> Outil stratégique dans les conflits

Ce n'est qu'à la fin du 20e siècle que l'on retrouve les travaux sur les codes de Louis XIV, et que les services de l'État recommencent à se doter de compétences en cryptographie.
L'histoire des interceptions est riche. On cite la bataille de Tannenberg, fin août 1914, gagnée par les Allemands qui avaient intercepté les messages transmis en clair par les généraux russes. Puis, l'interception et le décryptement en 1917 par les Britanniques d'un message allemand (télégramme dit Zimmermann) qui révélait le projet d'une offensive sous-marine totale et prônait des attaques du Mexique et du Japon contre les États-Unis. C'est d'ailleurs ce télégramme qui va provoquer l'entrée en guerre des Américains.
Côté français, on n'est pas en reste... En 1918, le lieutenant Painvin, qui était sorti major de l'École Polytechnique en 1905, décrypte en quelques jours le « radiogramme de la victoire » et permet au général Mangin de mobiliser les dernières troupes de réserves pour bloquer et repousser la dernière offensive allemande.
A l'issue de la seconde guerre mondiale, Winston Churchill rend hommage au service du chiffre britannique en



Bien antérieurs à l'informatique, les plus anciens exemples de cryptographie remonte à l'époque des Égyptiens (-1900 ans av. J.-C.), Lacédémoniens et Romains.

des termes proches de ceux qu'il a utilisés après la bataille d'Angleterre durant laquelle 900 aviateurs britanniques ont repoussé les attaques de plus de 2 500 avions allemands : « *Jamais dans l'histoire, un si petit nombre d'hommes n'a tenu entre ses mains le destin d'un si grand nombre.* » La maîtrise du chiffre apparaît comme un paramètre clé dans les conflits.
A côté des succès, il y a aussi des déconvenues du côté Français. On cite ainsi la perméabilité des transmissions du Quai d'Orsay avec son ambassade à Londres lors des discussions sur l'entrée de la Grande-Bretagne dans le marché commun : le *Foreign Office* lisait toute la correspondance française, car la machine de chiffrement rayonnait (effet Tempest)... Autre histoire à la fin des années 60, des machines françaises piégées par Moscou avec l'implantation, non sans un certain humour de la part des services russes, au cœur de la machine de trois petits fils : bleu, blanc, rouge !

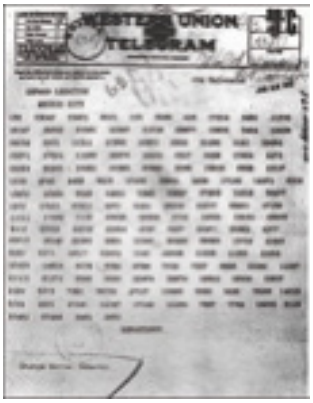
> Une course à l'anticipation

Les procédés de chiffrement sont multiples. Les plus simples ne sont pas les moins solides. Par exemple, l'utilisation d'une bande aléatoire et de la fonction XOR (ou exclusif) est un procédé symétrique extrêmement solide si les bandes aléatoires sont conservées secrètes et convenablement utilisées. Ces systèmes sont employés avec un code supplémentaire : « FTG »[2], qui s'inscrit comme exigence vitale des services du chiffre. Les machines à rotor permettent d'accélérer l'opération de chiffrement dans les années 30. La machine allemande Enigma est la plus connue. D'autres fondées sur le même principe seront commercialisées sous le nom d'Hagelin. Les modèles B211 et C36 équiperont notamment l'armée française jusque dans les années 50. Ces machines, jugées insuffisantes dès 1941 par une note de l'armée française, seront pourtant utilisées bien après cette date, mais rejetées en 1956 par les Britanniques durant l'expédition de Suez. Dans le cadre d'un plan de rénovation du chiffre français coïncidant avec le lancement d'un appel d'offres de l'OTAN, la Défense, avec le concours de la société Thomson-CSF, élabore le système Myosotis, première machine électronique de chiffrement. Myosotis n'emporte pas le concours OTAN, mais est évaluée et approuvée au niveau « NATO Secret ». Pour obtenir ce label, tous ses plans sont fournis à l'agence de sécurité américaine, la fameuse NSA (*National Security Agency*).
Les machines Hagelin sont remplacées par des Tarec (Transmission automatique régénératrice et chiffrante) produites par la Sagem et fonctionnant avec des bandes aléatoires pour un chiffrement symétrique. Elles seront utilisées jusque dans les années 90. Le principe, très sûr comme on l'a vu, sera utilisé pour protéger le « téléphone rouge » entre les US et l'URSS. Ce téléphone était alors en fait... une ligne télégraphique.
Cependant, subsisteront encore plusieurs années des « codes », c'est-à-dire des dictionnaires confidentiels utilisés soit directement pour coder les messages, ce qui est plutôt déconseillé, soit en surchiffrant le code obtenu par un autre procédé.

> *Jamais dans l'histoire, un si petit nombre d'hommes n'a tenu entre ses mains le destin d'un si grand nombre*
> *Winston Churchill*

Entre temps, la NSA a été créée et musclée en 1952. Elle succède à l'*Armed Forces Security Agency* qui avait été constituée dès 1949. La commission *Church* du Congrès révèle, dès 1975, que 150 000 messages sont analysés chaque mois. La loi américaine interdit l'espionnage des citoyens américains mais le considère légitime pour les étrangers. Cette agence comptera, au plus fort de la guerre froide, environ 100 000 personnes. Les attaques du 11 septembre 2001 ont conduit à accroître encore ses capacités à recueillir des renseignements d'origine technique.

[2] Traduit élégamment lors du colloque par l'expression « Ferme ta bouche ».



Ci-contre :
Ci-dessus, à gauche : le télégramme Zimmermann.
Ci-dessus, à droite : la machine Hagelin C36.

> L'avenir est aux clés RSA

La principale évolution cryptographique, pour ne pas dire révolution, à été la découverte des systèmes d'échange asymétrique en 1976 avec les notions de clés publiques et clés privées. Il a fallu 20 ans pour les utiliser à très grande échelle. C'est aujourd'hui chose faite. Le chiffrement symétrique repose sur l'usage d'un même secret connu de l'émetteur et du destinataire. Le problème est de transmettre ce secret entre ces deux personnes. Le chiffrement asymétrique repose, lui, sur le principe des fonctions à sens unique : il est facile de calculer y=f(x), mais il est très difficile de trouver x en connaissant y. Le trio Ron Rivest, Adi Shamir et Len Adleman propose en 1977 le système RSA (leurs initiales), une solution reposant sur la difficulté de factoriser le produit de deux grands nombres premiers.

Les systèmes ne sont pas pour autant incassables : la DCSSI[3] préconise désormais l'usage de clés RSA de plus de 2048 bits et l'abandon de l'algorithme de hachage SHA-1[4].

On notera toutefois que ces calculs ne sont valables qu'avec l'hypothèse que le calcul de la fonction inverse demeure un problème difficile. Une avancée mathématique pourrait éventuellement invalider cette hypothèse. Cela ne fait que 30 ans que les mathématiciens confirment la difficulté actuelle. C'est sur la base de celle-ci que les cryptologues bâtissent des systèmes de chiffrement dont ils peuvent « prouver » mathématiquement la sécurité.

Plus récentes, les techniques basées sur les courbes elliptiques permettent de réduire la taille des clés, mais ne bénéficient pas du même volume d'études cryptanalytiques que les fonctions RSA. Les algorithmes ECDSA pour la signature, ECDH pour l'échange de clés, et ECIES pour le chiffrement sont de même intéressants, notamment pour des applications RFID.

Les travaux de Shamir en 1984 proposent également des possibilités de résistance aux attaques MITM[5]. Basée sur l'identité, cette solution se réfère à une autorité. S'il n'y a pas de clé publique, l'attaque MITM n'est pas possible. Revers de la médaille, l'autorité dispose d'absolument toutes les clés, ce qui peut poser un problème de confiance.

> Sécurité des cartes à puce

Le colloque se penche également sur la sécurité des systèmes de cartes à puce. Il est nécessaire de chiffrer le bus de transmission entre la partie calculateur et la mémoire de la puce, afin qu'il ne soit pas possible d'extraire les données en se branchant sur le bus avec des micro-aiguilles. Cela conduit à ajouter des composants logiques pour assurer le chiffrement puis le déchiffrement. Sauf que si on passe le tout dans un logiciel d'optimisation d'architecture, ce dernier retire les opérations qui, selon lui, ne servent à rien : par exemple un chiffrement suivi du déchiffrement ! C'est une histoire vraie qui est arrivée à un industriel !

Le cassage des clés RSA: nombre d'opération temps de calcul

TAILLE DE LA CLÉ RSA(LF)	NOMBRE D'OPÉRATIONS À EFFECTUER	MIPS.YEAR
512 bits	2^{58}	2^{13}
1024 bits	2^{80}	2^{35}
2048 bits	2^{111}	2^{66}
4096 bits	2^{149}	2^{104}
8192 bits	2^{201}	2^{156}

La DCSSI recommande de passer à des clés de plus de 1500 bits, et pouvoir supporter des clés de 2048 bits.

[3] Direction centrale de la sécurité des systèmes d'information, entité du secrétariat national de la Défense nationale au sein des services du Premier ministre.

[4] En aparté lors de la RSA Conference à Londres fin octobre, les experts indiquent que l'on peut envisager de casser les clés RSA de 1024 bits en quelques semaines. Il faut en revanche un nombre d'années considérable pour casser une clé de plus de 2000 bits.

[5] *Man in the middle* : on croit avoir établi un tunnel chiffré entre deux équipements, mais en fait un tiers s'est interposé pour établir un tunnel chiffré avec chacun des deux équipements et lit, voire change, tout le contenu de la communication. Cette attaque permet, par exemple, de casser les tunnels https.

Autre question sur les cartes à puce : comment connaître toutes les fonctions noyées dans le silicium ? Il n'existe pas de code source fourni. Dès lors, comment s'assurer que la carte ne dispose pas d'un moyen de livrer une clé en réponse à une question tellement bizarre qu'aucun test ne permettra de s'assurer de l'absence d'une telle fonction. Or, les États ont besoin d'assurer la souveraineté de leurs titres d'identité. Une telle « porte dérobée » permettrait au fournisseur ou à son commanditaire de produire de vrais faux-titres d'identité.

Il faut donc introduire un prédateur sur la carte, que l'on nomme « Quine » (du nom de Willard van Orman Quine), et qui a pour objet d'imprimer son propre code, de se dessiner lui-même. On mesure ensuite les cycles machines utiles pour lire les données. S'il existe un programme malveillant, celui-ci devra, à un moment ou un autre, faire un test et allongera le temps d'exécution.

Toutefois, la bataille entre l'épée et la cuirasse pourrait prochainement donner un avantage très fort à la cuirasse, avec l'avènement de la cryptologie quantique, fondée sur l'altération inéluctable d'un photon qui serait intercepté indûment. Il convient toutefois de faire attention à ses certitudes. Le général Jean-Louis Desvignes, président de l'Arcsi rappelle que Roland Moreno avait promis, en 2000, une prime d'un million de francs à quiconque parviendrait à lire les données de ses cartes à puce. A l'époque, indique-t-il, les attaques de type DPA (analyse de la consommation électrique du composant) était encore peu connues. Un laboratoire de FT R&D, travaillant en tant que CESTI, savait notamment trouver en quelques minutes le code secret d'une carte bancaire non sécurisée. Le général regrette en souriant de ne pas avoir profité de ce défi, une aubaine pour améliorer l'ordinaire de son service...

> *« Les États ont besoin d'assurer la souveraineté de leurs titres d'identité »*

La course entre les chiffreurs et les déchiffreurs va donc se poursuivre. Il faut de la sécurité, tout le monde en convient. Mais, souligne le général Desvignes, pariant, non sans réalisme, que la lutte entre le glaive et le bouclier ne s'achèvera jamais, rappelle qu'un ministre a déclaré qu' « *heureusement, au cours de la seconde guerre mondiale, on vait pu fabriquer de faux-papiers d'identité et ainsi, sauver de nombreuse vies humaines* ». Aussi, conclut-il : « *Entre les back-doors imposées par certains gouvernements et celles laissées accidentellement par des concepteurs, les possibilités de frauder les systèmes d'information subsisteront certainement toujours, pour le meilleur et pour le pire...* » ■

Dominique Ciupa

En 1918, le lieutenant Painvin décrypte en quelques jours le « radiogramme de la victoire ».

Le Livre blanc de la Défense nationale

Pour conclure le colloque de l'Arcsi, Patrick Pailloux, directeur de la DCSSI présente les travaux réalisés autour du Livre blanc de la Défense nationale[1]. Les attaques informatiques sont officiellement inscrites dans la doctrine des USA et de la Chine. Elles ne sont pas difficiles à réaliser, peu dangereuses pour l'attaquant, peu coûteuses et potentiellement dévastatrices. Leur probabilité est donc élevée sur les 15 ans à venir et l'impact potentiel très élevé. La DCSSI doit donc se transformer en agence et se préparer à répondre à ces menaces. Il s'agit de former et de préparer la population et les entreprises dès le plus jeune âge.

Le besoin dépasse de très loin le seul périmètre du ministère de la Défense. Il y a des besoins de communication, de sensibilisation et d'animation d'une population.

Le général Desvignes, président de l'Arcsi, pose alors la question de clôture : *Ne faut-il pas penser à disposer de « cyber-troupes de réserve » pour renforcer, si besoin était, les capacités de riposte de l'État ?* L'Arcsi pourrait alors contribuer à une telle démarche...

[1] Voir les numéros de Mag Securs n°19 et 20.