Du XVIe au XIXe siècle

Philippe Guillot

Le propos de ce premier texte est de présenter un choix nécessairement incomplet de personnages dont l'activité a été cruciale pour le développement de la cryptologie en France depuis la renaissance et jusqu'aux débuts de la première guerre mondiale.

Avant tout, il faut rendre hommage aux mathématiciens français comme Fermat, Fourier, Laplace, Poincaré ou Poisson, qui ont œuvré à concevoir les outils d'analyse mathématique, de statistiques ou encore de traitement du signal dont l'importance n'est plus à démontrer pour le développement de la cryptologie moderne et des médias numériques.

Le premier personnage choisi est **François Viète**. De formation juridique, François Viète (1540-1603) a été l'avocat de grandes familles protestantes avant de devenir conseiller au parlement de Rennes sous Charles IX, puis maître des requêtes ordinaires de l'hôtel du roi sous Henri III. Il devient membre du conseil du roi Henri IV, puis son déchiffreur attitré. Parallèlement à ces charges au service de l'État, il mène une carrière de mathématicien qui le fera reconnaître comme un fondateur de l'algèbre symbolique. Fort du succès de ses premiers décryptements, il doit traiter une quantité toujours croissante de dépêches chiffrées, jusqu'à plus d'une dizaine de liasses par mois. Ce nombre le conduit à se faire aider pour préparer les transcriptions. Il est le premier cryptologue à proposer une méthode analytique systématique pour révéler une partie des alphabets de chiffrement. Il est par ailleurs sans doute l'auteur de nombreux codes utilisés à cette époque (code de Sully de 1599, code de Henri IV de 1604).

Sa méthode analytique repose sur l'assertion suivante qu'il appelle « règle infaillible » :

Parmi trois lettres consécutives, on trouve toujours l'une des trois voyelles A, E, I, O ou U.

En d'autres termes, jamais trois consonnes ne se suivent. Cette propriété est presque toujours satisfaite en Espagnol. Elle l'est un peu moins en Français, mais sa vraisemblance est suffisante pour commencer un décryptement. Le premier travail de Viète face à un cryptogramme sera donc de rechercher les voyelles avec une méthode systématique réalisable par un clerc. C'est sans doute son expérience de décrypteur qui, dans l'élaboration de son algèbre symbolique, l'a conduit à désigner les inconnues par des voyelles, convention qui sera remplacée par l'usage actuel, introduit par Descartes, d'utiliser les lettres x, y et z.

À ce stade, Viète ne pouvait pas entièrement ignorer leur signification. Une fois les voyelles déterminées, le sens commun, l'intuition, la spéculation et un long travail acharné sur le contexte et le sens des messages étaient encore nécessaires.

Le second personnage est **Antoine Rossignol**. Après des études de mathématiques, Antoine Rossignol (1600-1682) se passionne pour la cryptologie qu'il apprend dans des livres italiens. En avril 1628, le prince Henri de Condé mène le siège de la ville protestante de Réalmont. Il fait venir Rossignol pour résoudre un message intercepté sur un paysan qui tentait de fuir la ville. Le message contenait un poème d'une telle pauvreté que Rossignol a eu l'idée d'appliquer une grille de Cardan à partir de mots probables. Le message demandait de l'aide aux Huguenots de Montaubant en indiquant que Réalmont était à court de munitions. La ville s'est rendue le lendemain. Fort de ce succès, il est appelé par Richelieu et décrypte pour lui en octobre 1628 les messages émis par les protestants assiégés à La Rochelle qui attendaient l'approvisionnement par la mer de la part de leurs alliés anglais. La Rochelle a capitulé après 13 mois de siège. Rossignol dirigera le premier service français du chiffre. Il travaillera au décryptement des messages au sein du *cabinet noir* chargé de l'interception des dépêches postales.

L'œuvre principale de Rossignol est la création du *Grand Chiffre de Louis XIV*, premier nomenclateur désordonné de 587 mots ou groupes de mots qui gardera son secret plus de 200 ans. Un *petit chiffre* de 265 groupes était destiné aux subalternes. L'utilisation de ces chiffres nécessite deux tables. L'une ordonnée par les mots pour le chiffrement et une autre ordonnée selon les codes pour le déchiffrement.

Son fils Bonavanture Rossignol prendra la relève, puis ultérieurement son petit-fils Antoine.

Le troisième personnage choisi dans cette sélection est **Claude Chappe** (1793-1805). Il a donné son nom au télégraphe optique qui maillera le territoire de France métropolitaine et les colonies d'Afrique du Nord pendant la première moitié du dix-neuvième siècle. Le principe du télégraphe aérien est connu depuis l'antiquité. Dès le deuxième siècle avant l'ère commune, Polybe décrit un système de torches qui permet d'« *instruire à trois ou quatre journées de là, et parfois même à une plus grande distance* ». D'autres inventeurs ont expérimenté à partir du dix-septième siècle des dispositifs optiques de communication à distance, mais c'est l'adoption en 1793 de l'invention de Claude Chappe par la Convention qui signera le véritable succès du télégraphe. Chaque station comprend trois bras articulés peints en noir : un bras central appelé régulateur et deux bras latéraux appelés indicateurs. L'information est portée par la position relative du régulateur et des indicateurs selon l'une des 184 positions possibles. Une première ligne Paris Lille achevée en 1795,

constituée de 16 stations permet de transmettre un message de 25 mots en 15 minutes. La position des bras est visible par tous, ce qui rend nécessaire l'usage d'un code confidentiel. Le secret repose sur une organisation très hiérarchique avec une discipline militaire. Le livre des codes est maintenu secret et la signification n'est connue que par les directeurs de stations situés aux extrémités des lignes. Le message reste incompréhensible pour tous les intermédiaires.

Toutefois entre 1834 et 1836, le télégraphe a été exploité par des banquiers de Bordeaux, Louis et François Blanc qui ont eu l'idée d'exploiter la rapidité du télégraphe pour jouer en Bourse et transmettre des informations d'achat ou de vente selon la tendance avant que l'information officielle n'arrive par la poste.
Voici comment la *Gazette des tribunaux* du 10 décembre 1836 décrit l'opération :

> Un agent de Paris transmettait à Tours, poste restante des effets, tels que gants, etc., et la couleur de ces objets indiquait la hausse ou la baisse. Sur le vu de ces objets, l'employé du télégraphe donnait un signal convenu (…) L'employé de Tour donnait le signal indicatif du mot *erreur*, lequel se répétait sur toute la ligne, et ne figurait pas, par conséquent dans les dépêches officielles.

Informés par l'entremise d'un troisième agent, nos deux comparses avaient la certitude de gagner et pouvaient rémunérer grassement leurs complices. L'affaire a été révélée suite aux nombreuses erreurs *commises exprès* constatées par l'administration des Télégraphes.

Sa dernière utilisation est une version légère, transportable à dos de mulet, au service des opérations militaires de la guerre de Crimée (1853 – 1856) et qui permet un déplacement des stations au gré des opérations militaires.

Premier système de télécommunication organisé, le télégraphe de Chappe disparaît peu à peu à partir 1847 pour être définitivement remplacé en 1855 par le télégraphe électrique qui a l'avantage de fonctionner aussi la nuit et par temps de brouillard et dont les câbles sous-marins permettent de traverser les mers.

Notre sélection ne saurait faire l'impasse sur **Auguste Kerckhoffs** dont la contribution est sans conteste la plus importante. Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhof (1835-1901) est né en 1835 en Hollande. Il est issu d'une grande famille d'un duché Flamand, commence des études religieuses au petit séminaire d'Aix-la-Chapelle, puis étudie les langues anciennes et modernes. Il s'intéresse à l'histoire, à l'archéologie, aux mathématiques. Il commence à être en contact avec le milieu militaire comme titulaire de la chaire d'Allemand à l'école militaire, poste qu'il perdra rapidement, un employé ayant omis de signaler sa récente naturalisation. En 1883, à 47 ans, il publie son fameux article « la cryptographie militaire » qui fera date.

Il y tire les leçons de la défaite française de 1870 et bâti les fondements de ce que sera la cryptologie à l'aube de la première guerre mondiale. L'article est un véritable cours complet de cryptographie, incluant un rappel historique, l'usage de la cryptographie dans le contexte de l'utilisation du télégraphe, ainsi que l'analyse des différents procédés en usage à son époque.

Il montre combien l'absence d'un système de communications fiable et discret entre Paris et les généraux de Province a aidé les Prussiens en 1870. Mais surtout, avec le télégraphe, l'usage de la cryptographie change. Il ne s'agit plus de protéger les échanges entre deux acteurs déterminés, mais de protéger un « système de communications ».

Il faut bien distinguer entre un système d'écriture chiffrée imaginée pour un échange momentané de lettres entre quelques personnes isolées et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'Armée.

Il énonce les exigences que doit satisfaire un tel système cryptographique. La plus paradoxale est celle du non secret.

L'administration doit absolument renoncer aux méthodes secrètes.

La valeur d'un système de cryptographie destiné aux besoins de la guerre est en raison inverse du secret qu'exige son maniement ou sa composition (…) un chiffre n'est bon qu'autant qu'il reste indéchiffrable pour le maître lui-même qui l'a inventé : Ars ipsi secreta magistro.

Cette exigence exclut les livres de code, grilles ou autre cadrant qui perdent toute sécurité dès lors qu'ils sont capturés par l'ennemi. La sécurité doit s'appuyer sur une clé aisément modifiable au gré des correspondances. En cas de compromission, c'est la clé qui doit changer et non pas le mécanisme. Cette exigence sera assez peu respectée par l'Empire allemand durant la première guerre mondiale permettant aux Anglais et aux Français d'accéder aux contenus des messages chiffrés allemands.

Kerckhoffs attache également une très grande importance au décryptement, c'est-à-dire au déchiffrement sans la clé, et son rôle prépondérant pour éprouver la solidité d'une méthode de chiffrement.

Je suis stupéfait de voir nos savants et nos professeurs enseigner et recommander pour les usages de la guerre des systèmes dont un déchiffreur tant soit peu expérimenté trouverait certainement la clé en moins d'une heure de temps.

La première exigence est qu'un système doit être « *matériellement sinon mathématiquement indécryptable* », le terme *matériellement indécryptable* doit être ici compris comme *indécryptable* en pratique, au regard du temps du secret de la dépêche qui, dans le contexte militaire, n'est jamais très long. La faiblesse mathématique n'est pas un problème si cette faiblesse n'est pas pratiquement exploitable. Dans l'article, chaque procédé décrit est systématiquement assorti d'une méthode d'attaque et d'une étude de sa difficulté pratique.

L'article de Kerckhoffs va avoir une riche postérité en France et susciter des travaux en cryptologie qui vont placer la France dans une position dominante dans les années 1870-1918. Entre 1883 et 1914, 24 ouvrages ou brochures sur la cryptologie seront publiés en France contre seulement 6 en Allemagne. Il se crée une véritable école française de cryptologie autour de l'école polytechnique. Citons quelques contributeurs de cette école :

Étienne Bazerie (1846-1931) améliore le cylindre de Jefferson. Il est un grand cryptanalyste pratique. Il résout le grand chiffre de Louis XIV, le télégramme Panizzardi pendant l'affaire Dreyfus ainsi que le chiffre utilisé par les conspirateurs de 1892 pour le procès Ravachol.

Paul-Louis Eugène Valério publie dix articles dans le journal des sciences militaires ainsi qu'un ouvrage en deux volumes « de la cryptographie, essai sur les méthodes de chiffrement ». Il intervient comme expert dans le procès Dreyfus et décrypte la correspondance du Roi Henri IV.

Félix-Marie Delastelle (1840 – 1902) est l'auteur d'un chiffre publié en 1893 dans son ouvrage « la cryptographie nouvelle ». Ce chiffre se compose d'une substitution et d'une transposition. Il est également l'auteur en 1901 d'un « traité élémentaire de cryptographie ».

Gaétan De Viaris (1847, 1901) met en équation les procédés polyalphabétiques.

À l'aube de la première guerre mondiale, la France était dans une position de force dans le domaine de la cryptologie.

Je cède maintenant la parole à Agathe Couderc qui vous racontera comment cet avantage a été exploité.

Étienne Bazerie

Paul-Louis Eugène Valério

Félix-Marie Delastelle

Gaétan De Viaris