Définitions

Cryptologie = « Science du secret »

Elle possède deux composantes :

- La **cryptographie**, du grec *krupos* (caché, secret) et de *graphein* (écrire), est « la science des écritures secrètes ». Étude et conception des procédés de chiffrement des informations.
  La cryptographie diffère de la **stéganographie**, du grec *stéganos* (couvert, abris) qui est « la science des écritures couvertes ». La cryptographie transforme un message clair en un message inintelligible le « **cryptogramme** » ou message **chiffré**, alors que le but de stéganographie est de dissimuler l'existence même du message (encre sympathique, micros-points, texte noyé dans un programme ou une image numérique…)
- La **cryptanalyse** ou décryptement à pour objet de percer l'écran logique derrière lequel sont cachés les informations chiffrées.

Historique

- **Claude Shannon** – *Communication theoryof secrecy system* – article publié en **1949** Un seul système de chiffrement est théoriquement indécryptable : le système « à clé une fois aléatoire » ou **one time pad**. (Voir **Vernam**.)
- **Al Kindi** - لا كيندي - (savant arabe) premier traité de cryptanalyse au IX^{e} siècle (utilisant la fréquence des lettres et des bigrammes) « *Du déchiffrement des messages crypographiques* » (découvert en 1987 dans les archives ottomanes d'Istanbul). (Voir fréquence lettres.)
- **Whitfield Diffie** et **Martin Helman** (Université de Standford) imagine le concept de cryptographie à clé publique en **1976** dans l'article *Les nouvelles voies de la cryptographie*.
- Système **RSA** (basé sur le principe de Diffie et Helman est inventé en **1977** par **Ron Rivest**, **Adi Shamir** et **Leonard Adleman**.

Antiquité

Hérodote : histoire des tablettes recouverte de cire pour prévenir le roi Léonidas de l'attaque de Sparte par les troupes perses de Xerxès (480 av JC) et du Grec Histaïus qui, pour encourager un soulèvement contre les Perses envoya une missive écrite sur le crâne rasé d'un serviteur et attendit que les cheveux repoussent avant de l'envoyer vers son destinataire. Ceci relève plus de la stéganographie que de la cryptographie.

Plutarque rapporte qu'à Sparte au IV^{e} siècle av JC les Éphores et les chefs des armées communiquaient avec la **scytale**. A la même époque paraissent des ouvrages en Grèce comme en Inde donnant des ''recettes'' pour crypter des messages.

50 ans avant notre ère Jules César décrit dans *La guerre des Gaules* le procédé portant son nom.

Moyen âge

L'obscurographie

A l'époque où Al Kindi écrit sontraité de cryptanalyse (IX e siècle), utilisant la fréquence des lettres et des bigrammes « *Du déchiffrement des messages crypographiques* », l'église en France prohibe l'usage du chiffrement dans lequel elle voit une action démoniaque.

On a recourt aux vielles recettes de l'antiquité, l'écriture elle-même constitue un crytage accessible à peu de personnes. Utilisation des alphabets grec ou hébreu, lettres remplacées par des symboles (voir exemple de Charlemagne).

La Renaissance

L'éveil cryptologique

C'est la diplomatie qui va donner naissance à la cryptographie d'état tout d'abord en Italie puis en France. Au cours du XIV e les grandes cités italiennes, Venise, Florence, Milan, Naples et la curie instituent des ambassadeurs permanents et veulent protéger les correspondances diplomatiques – création de la fonction de « secrétaire-chiffreur ».

Les chercheurs en cryptologie :

- Alberti, célèbre architecte de Florence
- L'abbé Trithème, savant lettré consulté dans toute l'Europe
- Le physicien napolitain Porta
- Le mathématicien milanais Cardan

En 1586 le diplomate français **Blaise de Vigenère**, alors secrétaire de Charles IX, fait la synthèse de tous ses travaux dans « *Le traité des secrètes manières d'écrire* ». Il y décrit le chiffre « indeschiffrable » (substitution poly-alphabétique), c'est-à-dire indécryptable qui porte son nom encore aujourd'hui.

Le procédé de chiffrement de Vigenère résistera jusqu'au milieu du XIX e travaux de Charles Babbage (1854) et de Friedrich Kasiski (test de Kasiski 1863).

Le chiffre à la cour de France aurait été introduit par Louis XII à la suite de son expédition en Italie en 1495.

François 1er avait comme secrétaire-chiffreur Philibert Babou , il utilisait en 1558 un chiffre de substitution mono-alphabétique agrémenté d'adjonction de lettres nulles, de symboles spéciaux pour les bigrammes et pour certains mots. (Il bénéficiait des largesses du roi mais on ne sait si elles récompensaient les talents de Philibert ou ceux de son épouse qui était la maîtresse du roi…).

Viète (le mathématicien) était le cryptologue d'Henri IV (qui s'occupé lui-même de cryptographie). Le roi d'Espagne, ayant appris, en 1595, par une naïve indiscrétion de Viète au cours d'un repas copieux (et sûrement bien arrosé…) que son courrier avec la Ligue était lu par celui-ci et connu d'Henri IV, déposa plainte auprès du pape et accusa Viète de sorcellerie. Viète sauva sa tête car il était protégé du roi et parce que le pape savait très bien

qu'il n'y avait pas d'histoire de sorcellerie puisque lui-même utilisait le même procédé pour lire la correspondance du roi d'Espagne…

Juste avant sa mort en 1603 Viète adresse à Sully son ''testament cryptographique'', sous forme d'un traité : « *La manière de découvrir les Chiffres d'Espagne et d'Italie pour le bien du service du Roy et de l'Estat de la France* ».

Le Grand Chiffre de Louis XIV

Antoine et Bonaventure Rossignol

Antoine Rossignol le père (1600-1682), créateur du Grand Chiffre de Louis XIV et célèbre pour ses décryptages (d'où le nom donné au passe).
Au service de Louis XIII et de Richelieu qui le recommandera à Mazarin, Rossignol organise le service du chiffre français qu'il va diriger pendant 50 ans.
Montée en puissance du **Cabinet Noir** (créé par Henri IV) sous l'impulsion de Louvois. Il restera longtemps un des tous premier d'Europe et sera complété sous Louis XV par « Le secret du Roi » embryon d'un service de renseignement.
Système à substitution syllabique.
Cryptanalyse en 1890 par Étienne Bazeries (il partit de l'hypothèse que la suite de nombres 124-22-125-46-345 répétée dans plusieurs documents pouvait remplacer « les-en-ne-mi-s » pour reconstituer le chiffre de proche en proche).

Le déclin des XVIII^e^ et XIX^e^ siècles

Après les Rossignol la science cryptologique française décline, en témoigne le chiffre utilisé par les émigrés contre-révolutionnaires pour communiquer avec leurs partisans (simple substitution moins complet que celui de Philibert Babou en 1558…).
Napoléon lui-même ne dispose que d'un chiffre de type césar et encore toutes les lettres ne sont pas cryptées. Berthier en charge des communications de l'empereur privilégiait plus la rapidité que la confidentialité.

Entrée de la cryptographie dans la littérature en 1839 Edgar Poe dans « *le scarabée d'or* » (énigme sous forme de cryptogramme dont il livre le décryptement, inspirait de l'histoire de la duchesse de Berry qui en 1832 tente de soulever la Vendée contre Louis-Philippe, ses messages ayant étés interceptés et décryptés), Balzac en 1846 dans « *La philosophie du mariage* » texte encore non décrypté … ? Enfin Jules Verne dans de nombreux ouvrages.

Cela ne s'améliore pas sous la restauration et le second empire. Le maréchal Bazaine se plaint de n'avoir pas de moyen de chiffrement, Napoléon III lui fournir un vieux code diplomatique exempt de termes militaires.

Le réveil de la fin du XIX^e^ et de la guerre de 14-18

Le chiffre du livre :

L'apparition de la télégraphie électrique en 1844 va relancer la cryptographie. Le coût des communications taxées au mot entraîne l'utilisation de codes commerciaux (par exemple le Sittler en 1868). On peut numéroter les pages et le code d'un mot sera obtenu en concaténant le numéro de la page et le numéro de la ligne correspondant à ce mot dans la page. Ces codes seront utilisés jusqu'en 1930.

L'activité du décryptement renaît à la fin du siècle comme le prouvent certaines affaires : les messages des anarchistes décryptés présentés au procès de Ravachol en 1892, le décryptement des dépêches chiffrés du duc d'Orléans et du parti royaliste en 1899, le fameux télégramme Panizzardi en 1894 dans l'affaire Dreyfus. Mais on fait preuve de peu de ''professionnalisme'' comme le prouve l'affaire Caillaux (président du conseil)en 1910, accusé, sur un message décrypté par les services français, d'entretenir des relation avec l'Allemagne, il alla brandir les fameux messages à l'ambassade d'Allemagne, les service allemand changèrent leur code et il fallut attendre 1914 pour pouvoir de nouveau les décrypter.

Le radiogramme de la victoire : Georges Painvin (1886-1980)

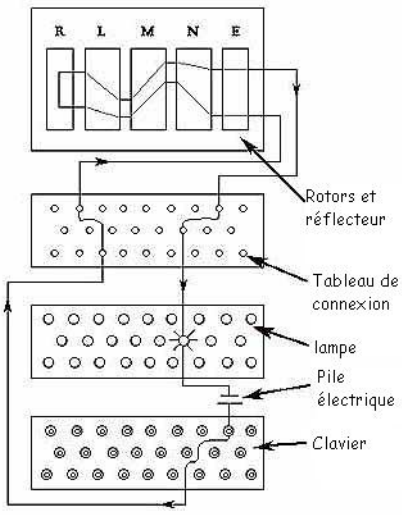
Vernam (One-time-pad) 1917
Claude Shannon – *Communication theory of secrecy system* – article publié en **1949**
Un seul système de chiffrement est théoriquement indécryptable : le système « à clé une fois aléatoire » ou **one time pad**.

La mécanisation

Enigma (1918)

L'Enigma se présente sous la forme d'une caisse en bois de 34×28×15 cm, et pèse une douzaine de kilos. Elle est composée :

- d'un clavier alphabétique
- d'un tableau de connexion
- de 3 rotors mobiles à 26 positions
- d'un rotor renvoi à 26 positions (le réflecteur)
- d'un tableau de 26 ampoules correspondant aux 26 lettres de l'alphabet.



Le principe de fonctionnement de l'Enigma est à la fois simple et astucieux. A chaque fois que l'on presse une lettre, un circuit électrique est fermé, et s'éclaire une ampoule qui correspond à la lettre codée. En même temps, un ou plusieurs des rotors mobiles tourne, changeant la substitution qui sera opérée à la prochaine touche pressée. De plus, le chiffrage est réversible : si en tapant A vous codez D, si vous aviez tapé D, vous auriez codé A. Ainsi, si le commandement allemand et le sous-marin ont le même réglage de départ, il suffit à l'opérateur du sous-marin de taper directement le message codé pour obtenir le message clair.

Le nombre de clés est gigantesque (de l'ordre de 10^{20}), et les allemands ont une confiance totale en la machine Enigma, dont ils fabriqueront 100.000 exemplaires. Au su et au vu de tous, ils s'échangeront des communications radios cryptées, persuadés que jamais les Alliés ne les comprendront.

La Pologne s'est trouvée ressuscitée en 1919 par le traité de Versailles. Craignant son voisin allemand (à juste titre!), elle se dote d'un très performant service du chiffre, et se tient à l'écoute des communications allemandes. Avec l'aide d'une Enigma "civile" (l'Enigma était destinée dans sa première forme aux banques), de renseignements fournis par les services secrets français, et grâce au remarquable travail du mathématicien Rejewski, elle parvient à fabriquer une copie conforme de l'Enigma militaire. Même, dans le milieu des années 1930, la Pologne dispose de méthodes pour déchiffrer les messages allemands.

Las. En 1938, les allemands changent le protocole d'envoi de leurs messages, et surtout font passer de 3 à 5 le nombre de rotors de leurs Enigma. La Pologne perd le contact. Devant la gravité de la situation internationale, les Polonais font parvenir aux Anglais et aux Français en 1939 une Enigma, ainsi que l'ensemble de leurs découvertes.

Bletchley Park

Les Anglais ont compris assez tard l'intérêt de la machine Enigma. En 1939, le service du chiffre décide de s'éloigner de Londres, et des futurs bombardements, pour s'installer, en toute discrétion, au manoir de Bletchley Park, dans la paisible campagne à 60km au nord-ouest de Londres. Devant l'urgence de la situation, les meilleurs mathématiciens, linguistes, et même joueurs d'échecs sont appelés à Bletchley Park, où plusieurs milliers de personnes se cotoieront.

Parmi eux, Alan Türing, un logicien et mathématicien, qui, quelques années plus tôt, a conçu une machine universelle qui formalise la notion d'algorithme et est le précurseur des ordinateurs modernes. Il conçoit les *Bombes*, des machines programmables qui permettent après une vingtaine d'heures de calcul, de décrypter les messages allemands. Le progrès est considérable. Du premier au second semestre 1941, le tonnage coulé chute de moitié (de 2,9 millions de tonnes à 1,4 millions).

Alan Turing (1912-1954)

En février 1942, une nouvelle version de la machine Enigma est mise en service, provoquant un nouveau trou noir dans le décryptage des messages. Grâce à des documents récupérés sur un sous-marin allemand, et à l'aide technique des Etats-Unis, Bletchley Park retrouve mi 1943, toujours sous l'impulsion de Türing, la faculté de décrypter les messages allemands. En 1944, le premier ordinateur de l'histoire, le Colossus, leur garantira une puissance de calcul suffisante jusqu'à la fin de la guerre : la bataille de l'Atlantique est gagnée ! Cela, d'autant que les allemands ne se douteront jamais que leurs messages sont décryptés. Ils pensent, à juste titre, que les hommes ne peuvent venir à bout d'un travail aussi titanesque. Ils ne se doutent pas qu'à Bletchley Park, dans un manoir, une étrange machine réalise cette prouesse!

Le travail d'Alan Türing pour déchiffrer les messages allemands a profondément changé le cours de la seconde guerre mondiale. Plusieurs centaines de navires, leur équipage et leur cargaison, furent sauvés. Le débarquement de l'été 1944 a pu être préparé en toute sérénité... Grâce au génie d'un mathématicien !

Déclaration de Churchill peu après la fin de la guerre : « Trois formations ont sauvé l'Angleterre : la R.F.A., la *Home Fleet*, et le service cryptographique. ». D'après les historiens

la cryptographie a permis d'écourter la guerre d'un an dans le Pacifique et de deux ans en Europe.

R. POMES