L'ENTRE-DEUX GUERRES : 1920 - 1945

Si l'on considère l'histoire des Transmissions, on constate qu'au cours de la seconde moitié du XIXe siècle, le télégraphe et les communications en alphabet Morse se sont généralisés dans le monde entier. Puis, au début du XXe siècle, l'invention de la radio a permis de développer considérablement le volume et surtout la vitesse de ces communications. A cette époque,les messages radio vont donc devenir le moyen de transmission par excellence. Inconvénient : ils peuvent se faire intercepter !

Du fait des interceptions massives de messages et du fantastique travail des cryptanalystes, les messages chiffrés par transposition, très utilisés fin XIXe et début XXe, ont été souvent décryptés (chiffre ADFGVX en 1918, voir Fiche n° 5). La fin de la Première Guerre mondiale va marquer la fin de l'utilisation de ces types de chiffrements. Puis, à partir de 1920, les militaires vont ressentir la nécessité d'utiliser des machines.

1. Enigma

En 1926, l'ingénieur allemand Arthur Scherbius breveta une machine conçue pour faciliter les communications sécurisées : *Enigma.* Au départ, Enigma fut conçue pour protéger le secret des communications commerciales. Mais cette version commerciale fut un échec. Dès 1926, en raison de sa facilité d'utilisation et de la complexité du chiffrement qu'elle permet, Enigma fut choisie par le gouvernement allemand pour coder les communications militaires. L'armée allemande fut dotée d' environ 100 000 machines entre 1926 et 1945.

En fait il existait une série de machines : chacun des trois corps de l'armée hitlérienne, la Luftwaffe (aviation), la Wehrmacht (armée de terre) et la Kriegsmarine (marine) avait la sienne.

La machine Enigma se présente comme une ancienne machine à écrire. Elle est constituée d'un clavier, d'un tableau lumineux de 26 lettres, de trois rotors et d'un réflecteur. La position des connexions entre les 3 rotors, qui sont modifiables, ainsi que la position de ces rotors, constituent la clef de chiffrement.

L'utilisation d'Enigma est relativement simple : l'émetteur dispose les connexions et les rotors en position de sortie, tels que spécifié par le livre des clefs pour ce jour-là. Puis il tape les lettres du message qui se trouve automatiquement chiffré. A chaque frappe d'une nouvelle lettre, un rotor tourne, modifiant le chiffrement. A la réception, le destinataire tape le message chiffré et la machine restitue les lettres en clair sur le clavier lumineux. Le système des rotors permettait plus de 10 millions de milliards de combinaisons, donc autant de clefs différentes. En pratique, la clef était changée chaque jour.

Si vous êtes intéressés, vous trouverez le fonctionnement détaillé d'Enigma dans les principaux livres cités dans la fiche n° 10 et sur de nombreux sites Internet. Expliquer ce fonctionnement dans le détail serait un peu fastidieux et sortirait du cadre de ces fiches, d'autant que ces livres et ces sites Internet l'expliquent parfaitement bien.
Ce fonctionnement d'Enigma est également expliqué dans la vidéo suivante (très courte) sur YouTube ainsi que sur d'autres vidéo.

https://www.youtube.com/watch?v=dTiqXrrH-oQ

On peut voir une Enigma au Musée de l'Armée à Paris ainsi qu'au Musée de la ville de Bletchley en Grande-Bretagne.

2. Casser Enigma

L'histoire de la cryptanalyse d'Enigma est un véritable roman d'espionnage.

En 1931, un fonctionnaire allemand du Bureau du Chiffre, Hans-Thilo Schmidt, trahit son pays pour de l'argent et fournit aux Français les tables de chiffrement et les manuels d'utilisation d'Enigma. Cet espion, Schmidt fut traité par un officier français , le capitaine Gustave Bertrand. (« traiter» un agent signifie assurer la liaison avec un agent étranger qui est source de renseignements).

Gustave Bertrand remit la précieuse documentation sur Enigma à ses collègues français de la Section du Chiffre, mais ils ne parvinrent pas à briser le cryptage de la machine. Sur ordre de sa hiérarchie, le capitaine Bertrand remit alors les mêmes documents au Bureau du Chiffre britannique, également sans succès. En décembre 1932, ll s'adressa alors au Bureau du Chiffre polonais et communiqua certains éléments au colonel Gwido Langer, le chef du Biuro Szyfrów (Bureau du chiffre polonais).

Dans ce Bureau du chiffre polonais travaillait une équipe de mathématiciens de très haut niveau. Parmi eux se trouvait *Marian Rejewski*, qui, grâce aux documents remis par Gustave Bertrand concentra les efforts des équipes sur le problème des clefs. Après quelques mois d'un dur labeur, il parvint à dégager 105 456 clefs, parmi les 10 millions de milliards de clés initiales possibles. Pour cela, les mathématiciens polonais construisirent une machine appelée « Bomba », qui générait toutes les positions possibles des rotors pour rechercher la clé du jour. En 1934, le Bureau de cryptanalyse polonais avait réussi à casser Enigma et pouvait déchiffrer un message en quelques heures.

Les Allemands ne savaient pas que les Polonais étaient parvenus à briser la sécurité d'Enigma. Pourtant, ils amélioraient constamment le système et en 1938, ils ajoutèrent deux rotors supplémentaires à la machine. Le nombre de clés possibles fut multiplié par 10. Ceci posa quelques problèmes aux cryptanalystes polonais.

Après la déclaration de guerre et la défaite de la Pologne face à l'Allemagne nazie, certains membres du Bureau du Chiffre polonais vinrent en France grâce à Gustave Bertrand. Ils échangèrent beaucoup d'informations avec les Anglais et leur permirent de travailler efficacement sur Enigma. En 1942, dans la France de Vichy, les Français et les Polonais poursuivirent conjointement leurs efforts de déchiffrement. Mais leur histoire devint dramatique : la Gestapo les traquait et le MI 6 (Military Intelligence section 6) tenta de les exfiltrer. Sur le point de passer en Espagne en 1943, ils furent arrêtés par une patrouille allemande et ne purent jamais se rendre en Angleterre.

3. Enigma vaincue : Alan Turing

Alan Turing naquit le 23 juin 1912. Après ses études secondaires, il fut admis en 1931 au King's College de Cambrige, haut-lieu de l'enseignement des mathématiques en Grande-Bretagne. Pendant ses études, en 1937, il publia son célèbre article *« On computable Numbers »*, article de logique mathématique sur la difficulté de discerner le vrai du faux. Dans cet article, il décrit une machine imaginaire capable d'enchaîner des opérations de calcul (un algorithme) : l'ancêtre de l'ordinateur.

Il existe différentes branches dans les mathématiques : la théorie des nombres, l'algèbre, l'analyse, la géométrie, la logique etc. Alan Turing est un logicien. Une petite histoire permettra de comprendre la notion de logicien :

Un biologiste, un physicien et un mathématicien sont dans un train en Écosse. Tout à coup, ils aperçoivent un mouton noir dans un pré qui borde la voie.
– Le biologiste dit : « Tiens, en Écosse, les moutons sont noirs.»
– Le physicien le corrige et dit : «Il faut s'en tenir à ce que l'on a observé : on peut dire qu'en Écosse, il existe au moins un mouton noir.»
– « Non, dit le mathématicien, on peut seulement dire qu'en Écosse il existe un mouton dont au moins un côté est noir.»

Revenons à nos propres moutons :

Au début de la Seconde Guerre mondiale, l'interception et le déchiffrement des messages de l'ennemi sont fondamentaux. Les sous-marins allemands règnent en maîtres sur l'océan atlantique et le ravitaillement de la Grande-Bretagne en nourriture et en armes est compromis. C'est la célèbre Bataille de l'Atlantique.
Les communications entre la terre et les sous-marins s'effectuaient avec Enigma. Décrypter ces transmissions est un enjeu vital. Connaître les positions des U-boots est fondamental pour que les bâtiments de ravitaillement les évitent et que ceux de la Royal Navy puissent les attaquer.
Des équipes de spécialistes en cryptographie furent réunies au début de la guerre à Bletchley Park, un grand manoir situé à 80 km au nord de Londres. A la déclaration de guerre en septembre 1939, Alan Turing fut invité à rejoindre Bletchley Park pour y diriger le service chargé de décrypter les messages de la Marine allemande. À cette époque, les Enigma de la Kriegsmarine ont 4 ou 5 rotors. Dans les premières années de la guerre, les Anglais posséderont une ou deux Enigma, récupérées difficilement sur des sous-marins en perdition.

Ces Enigma vont être étudiées par les experts de Bletchley Park et Alan Turing, dans la logique de son article de 1937 sur une machine qui calcule, fit construire un premier appareil de décodage automatique appelé « la Bombe ». Quinze bombes furent construites dans les huit mois suivants pour apporter des améliorations.

Enigma était utilisée par les armées, mais les communications entre les états-majors et la chancellerie d'Hitler étaient chiffrées par une machine appelée machine de Lorenz. Pour parvenir à la décrypter une machine de décodage plus puissante fut nécessaire. Ce nouvel outil découla lui aussi des travaux de Turing. Il s'agit d'un calculateur électronique de grande taille, appelé pour cette raison Colossus. Alimenté par câbles, Colossus effectue les opérations de déchiffrement en suivant une logique abstraite et universelle ; il est également capable de programmer d'autres machines et de s'arrêter lui-même après avoir inscrit ses résultats sur un ruban de papier. L'ordinateur est né.

La vie et les actions d'Alan Turing à Bletchley Park ainsi que sa fin tragique en 1954 appartiennent à l'Histoire avec un grand H. Là encore, nous laisserons les livres, les sites Internet et un très beau film (*Imitation Game*) raconter tout cela en détail.

Remarquons simplement quelques points importants ou méconnus :

- De nombreux historiens estiment que la cryptanalyse d'Enigma a permis d'écourter la durée de la Seconde Guerre mondiale d'environ deux ans.

- Toutes les activités de décryptage réalisées à Betchley Park pendant la Seconde Guerre mondiale ont été tenues secrètes jusque dans les années 1975 / 1980. Elles étaient classifiées « Top Secret », le plus haut niveau de classification (correspondant au « Très Secret - Défense » français) par les autorités britanniques. Tout s'est passé comme si ces événements n'avaient jamais existé. Colossus a été détruit après la guerre sur ordre de Winston Churchill.

- On a commencé à entendre parler d'Alan Turing dans les années 80. David Kahn évoque Enigma et Alan Turing dans son livre extraordinairement bien documenté « La guerre des codes secrets », publié en France en 1980. La première biographie qui lui a été consacrée, *Alan Turing : the enigma* d'Andrew Hodges, fut publiée en 1983. Ce livre a été édité en France en 1988 et réimprimé en 2014 et 2015 à la suite du succès de la sortie du film *Imitation Game*.

- En 1945, les Anglais ont récupéré de nombreuses machines Enigma dans les unités combattantes allemandes, dans les états-majors, les ministères etc. Très généreusement, ils en ont offert un grand nombre à des pays amis et en particulier aux pays du Commonwealth pour un usage diplomatique ou militaire. Il se trouve que par un malencontreux oubli, ils ne les ont pas informés qu'il savaient décrypter les messages…

****
*****
***
*