Rubrique Historique de GUERRELEC N°37

« Si vous n'écrivez pas votre propre histoire, personne ne l'écrira pour vous »
Jean-Paul SIFFRE

Le décodage de la machine Lorenz à Bletchley Park (2e partie)

Dans la première partie de cette histoire, on a vu que durant la Seconde Guerre mondiale *Enigma* et *Lorenz* étaient deux systèmes allemands de codage vraiment différents et qu'ils avaient très peu de choses en commun. *Enigma*, avec l'image de Turing, comportait trois roues de codage, puis quatre, créant des messages utilisant les 26 lettres de l'alphabet. Elle pouvait avoir 150 millions de millions de codages différents. La *Lorenz SZ40/42,* utilisée par Hitler et les généraux et dont le cerveau était Bill Tutte, était beaucoup plus sophistiquée avec 12 roues dentées et 501 pointes (sur les roues dentées). Les messages étaient envoyés par téléscripteur sur des bandes de papier perforé. Les possibilités de codages étaient considérables (de l'ordre de 1,6 quadrillions de positions de départ, soit un million de trillions, soit 10^{24}). *Lorenz* était de loin bien plus complexe qu'*Enigma.* Ce fut un miracle que Bill Tutte parvienne à « casser » la *Lorenz* avec le peu d'éléments dont il disposait. Cette machine était employée pour envoyer des messages par téléscripteur qui pouvaient compter des milliers de caractères, espaces compris, alors que les messages *Enigma* ne pouvaient en comporter seulement 300.

Pourtant, bien que les Allemands aient changé souvent les codes au début de la guerre, puis chaque jour à partir de janvier 1944, *Lorenz* était plus facile à employer que *Enigma* et beaucoup plus efficace. *Lorenz* demandait seulement un opérateur à chaque bout de la ligne alors qu'*Enigma* avait besoin de trois personnes : une pour préparer le message, une pour le convertir en code morse et une troisième pour l'envoyer sur les ondes. Avec *Lorenz*, l'opérateur tapait simplement son message sur son clavier et la machine générait automatiquement le code automatiquement, puis l'envoyait.

Un événement extraordinaire intervint le 30 août 1941. L'opérateur « A » de la *Wehrmacht* en poste à Athènes envoya un message à son collègue, l'opérateur « B » à Salzburg en Autriche. L'opérateur « B » qui n'avait pas compris le message demanda à l'opérateur « A » de le renvoyer. Ce dernier s'exécuta mais commit deux erreurs rédhibitoires. D'abord, il ne changea pas la position des roues de codage, mettant ainsi sa

machine *Lorenz SZ40/42* dans la même position de codage de départ que lors de l'envoi du message mal reçu. Puis, lorsqu'il le renvoya, il comprima le message en employant les abréviations de certains mots allemands, chose qui n'avait pas été faite lors du premier envoi. Ce message comportait 4 000 signes et ces petits changements firent gagner quatre places vers la gauche, ce qui fit que les cryptographes de Bletchley Park purent comparer les deux messages. Cela leur permit de trouver le code de départ et, ensuite, de lire le message en clair.

En 1942, la première manifestation de la technologie pour « casser » la machine allemande *Lorenz* fut la *British Tunny machine* (pour casser le code allemand Tunny signifiant « Thon »). Elle fut construite par Ralph Tester, dans son laboratoire, la *Testery*, selon les spécifications de Bill Tutte, d'une taille complétement différente de la *Lorenz.* Elle mesurait plus de 2 mètres de haut pour un 1,20 mètre de large. Cette machine était servie par une équipe de vingt-quatre jeunes femmes ATS[1] au sein de la *Testery*. Une dizaine de machines furent installées. Les ATS « calaient » la position de la roue du jour et décodaient le message intercepté. La machine fut conçue à Bletchley Park et construite par la *Post Office Research Station* (laboratoire de la Poste) à Dollis Hill au nord de Londres.

Dans le même temps, Tutte travaillait au sein de la *Newmanry*, dont le chef était Max Newman, responsable d'une méthode de décodage. Ce laboratoire était situé dans le Block F avec la *Testery* (dont le chef était Ralph Tester aidé des jeunes femmes Wrens) pour mettre au point, à la mi-1943, une machine de deuxième génération, la *Heath Robinson,* capable de trouver la position de la roues *chi* (nom donné à la roue de gauche dans chaque couple de deux roues, *psi* étant donné à la roue de droite). Elle était également capable de trouver le code à raison de 2 000 caractères par seconde.

Puis, grâce à Tommy Flowers, vint le premier système de décryptage britannique, appelé *Colossus*, d'une taille impressionnante de 2,4 mètres de haut, 4,5 mètres de long et 3 mètres de profondeur et capable de scanner 5 000 caractères à la minute. Pour sa mise au point, Tommy Flowers fut aidé par Bill Tutte et Alan Turing.

Enfin, le 1er juin 1944, juste à temps pour le débarquement prévu le 6 juin, arriva la *Colossus Mk2* capable de scanner 25 000 caractères à la seconde. Il fallait passer par sept manipulations pour décoder un message allemand de la *Lorenz.* Après la découverte de la position du jour de la roue *chi* à la *Newmanry,* il restait cinq actions à la main pour les « casseurs de codes » de la *Testery* afin de lire, enfin, un message en clair (en allemand bien sûr, car il fallait encore le traduire en anglais).

Après la guerre, toutes ces machines furent démantelées sur ordre de Winston Churchill. Seuls deux *Colossus Mk2* furent préservées par le *Government Communications Headquarters (GCHQ)* et absolument personne n'y avait accès. Tous les plans furent (théoriquement) détruits… Tellement détruits qu'un ancien de Bletchley Park a réussi, selon de simples photos, à reconstituer une machine *Colossus Mk2.* Cette dernière fonctionne aujourd'hui parfaitement devant les visiteurs de ce lieu si mythique outre-Manche qu'est Bletchley Park.

[1] ATS : *Auxiliary Territorial Service*. C'était la branche féminine de la British Army durant la Seconde Guerre mondiale.

En résumé, il y eut trois héros à Bletchley Park :

- **Alan Turing**, qui participa à la réflexion sur l'ordinateur moderne et « cassa » le code de la machine *Enigma* de la *Kriegsmarine* (qui avait ajouté une quatrième roue de codage), ce qui aida les Britanniques à ne pas perdre la guerre en 1941 lors des attaques de convois dans l'Atlantique Nord ;
- **Bill Tutte**, qui « cassa » le système *Lorenz*, ce qui contribua à raccourcir la durée de la guerre ;
- **Tommy Flowers**, un des pères du *Colossus* britannique et de l'ordinateur moderne.

A ce sujet, nous pouvons ajouter que, au vu des archives qui depuis se sont ouvertes, les Britanniques ont volontairement expliqué « en long et en large » que Alan Turing avait été seul le concepteur de l'ordinateur moderne à partir de la machine *Colossus* Mk2. S'il y a probablement participé, c'est Tommy Flowers qui en est le « père » comme cité précédemment. Alors pourquoi ce détournement de la vérité historique ? Tout simplement parce que, dans les années 1970, lorsque le système de décodage *Ultra* de la machine *Enigma* a été révélé et publié, il fallait encore garder le secret sur le décodage de la machine *Lorenz* dont le véritable concepteur était Tommy Flowers. Secret bien gardé pendant trente années de plus, tout en orientant les chercheurs vers d'autres pistes. Rien n'est jamais fait au hasard chez nos amis britanniques, surtout dans le domaine du renseignement. Le code de cette machine réputée inviolable a été cassé entre 1942 et 1943.

La Grande-Bretagne fut extrêmement chanceuse d'héberger chez elle ces trois grands hommes oeuvrant dans un lieu comme Bletchley Park dans les heures les plus sombres de la Seconde Guerre mondiale. Le décryptage de la machine *Lorenz* a permis de lire une grande masse de messages, permettant d'apprendre les pensées stratégiques, les programmes et les décisions de l'ennemi. Les messages furent décodés pour aider à la résolution de situations critiques comme la bataille de Koursk en 1943, le nettoyage de la péninsule italienne en 1944 et les mois avant et après le débarquement en Normandie le 6 juin 1944.

Cette guerre a coûté environ 55 millions de vies humaines entre 1939 et 1945, mais le décodage de la machine *Lorenz* a, dit-on, réduit la durée de la guerre de deux ans environ, et a probablement a permis de sauver 20 millions de vies.

La machine Lorenz peut être considérée comme le précurseur d'un système de Guerre Electronique, même si son histoire extraordinaire est malheureusement peu connue, du moins jusqu'à ce jour.

Pierre-Alain Antoine