Bletchley Park, haut lieu de la cryptographie

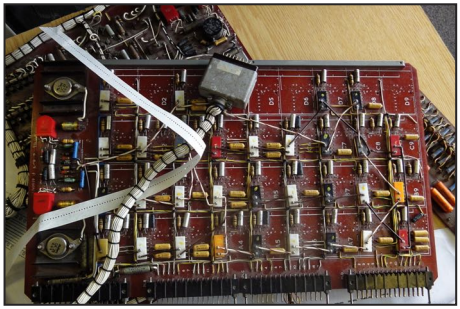
Laurent Bloch

En route pour Bletchley Park !

Bletchley Park est un site mythique de l'histoire de l'informatique : pendant la Seconde Guerre mondiale, *Bletchley Park* abrite le *Government Code and Cypher School* (GC&CS, qui deviendra le GCHQ en 1946), dont une mission de plus en plus importante sera le décryptement des messages codés des armées allemandes, et notamment des communications des sous-marins en opérations dans l'Atlantique contre les convois qui acheminaient de l'armement et d'autres marchandises vers le Royaume-Uni. À la fin de la guerre, ce sont des dizaines de mathématiciens et d'ingénieurs qui travailleront à *Bletchley Park*, ainsi que plus de 8 000 WRNS (*British Women's Royal Naval Service*) occupées pour la plupart à transcrire les traces d'interceptions de transmissions hertziennes sur ruban perforé en vue de leur compilation et traitement sur matériel mécanographique.

Ces opérations de décryptement, la recherche de procédés de nature à les automatiser, et la réalisation de machines capables de réaliser ces procédés, constituent des étapes majeures de la préhistoire de l'informatique, avec la participation d'Alan Turing, de Max Newman et d'autres précurseurs notables. Aussi, lorsque j'appris que l'ARCSI, dont j'ai l'honneur d'être membre, organisait une visite de *Bletchley Park*, je m'y précipitai, en entraînant mon épouse ; en effet, lors de notre visite des collections d'ordinateurs du *Science Museum* de Londres, nous avions été frustrés de n'y voir ni la Bombe ni le Colossus.

Ordinateur soviétique (*Science Museum*)

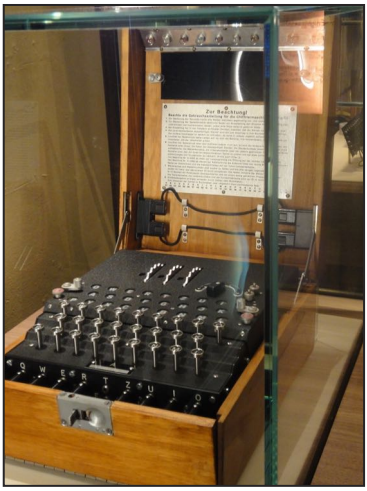


Ça c'est de la logique discrète !

Bletchley Park est à une heure de train de Londres-Euston, à 10 minutes à pied de la gare, c'est une excursion réalisable, que je ne saurais trop vous conseiller. En outre, juste à côté de *Bletchley Park* se trouve le *National Museum of Computing*, un des plus beaux musées d'informatique.

Merci à l'ARCSI d'avoir organisé cette visite passionnante, avec en supplément l'*Imperial War Museum* de Londres, également intéressant !

Machines de chiffrement allemandes



Enigma

Au début de la guerre, les procédures de décryptement étaient surtout manuelles, mais le nombre d'opérations répétitives conduisit à l'idée de les mécaniser. Les machines de chiffrement les plus utilisées par les armées allemandes étaient l'Enigma, puis les machines de Lorenz SZ40 et SZ42, plus perfectionnées. Les Allemands changeaient régulièrement la configuration de ces machines, ce qui modifiait le code et obligeait les cryptanalystes anglais à reprendre leurs efforts de décryptement depuis le début. La courbe qui trace le nombre de bateaux alliés coulés par les sous-marins allemands exhibe des pics qui correspondent aux dates de ces changements de code, suivis d'une diminution au fur et à mesure que les cryptanalystes progressent, ce qui conforte l'idée que le travail accompli à *Bletchley Park* a été une contribution majeure à la victoire alliée sur les forces de l'Axe.

Les Enigma civiles étaient en vente libre avant la guerre, mais les Enigma militaires étaient secrètes et plus perfectionnées. En 1931 les services secrets français avaient obtenu une copie de leur documentation et l'avaient communiquée aux services polonais, qui créèrent une équipe pour reconstituer et analyser la machine. C'est grâce au travail pionnier des mathématiciens polonais Marian Rejewski, Henryk Zygalski et Jerzy Różycki que la cryptanalyse des messages Enigma a pu commencer.

Automatisation du déchiffrement de messages codés

Devant un message chiffré selon un code inconnu, la première étape du travail consiste à trouver, mi par tâtonnement mi en profitant de la connaissance des principes de la machine de chiffrement, le chiffré d'un texte connu, par exemple un bulletin météorologique, type de message assez stéréotypé au vocabulaire pauvre et répétitif. On peut aussi tenter de retrouver les formules stéréotypées de début et de fin de message. En bref, on tente le décryptement avec une configuration de la machine, on regarde si on trouve un texte significatif, sinon on recommence avec une autre configuration. Il y a de nombreuses configurations possibles et elles sont de plus en plus compliquées au fur et à mesure que les Allemands perfectionnent leur matériel. Ce sont ces essais successifs à l'aveugle que l'équipe polonaise avait eu l'idée d'automatiser avec un matériel électromécanique baptisé « Bombe », matériel qui allait être réalisé et perfectionné progressivement par l'équipe de *Bletchley Park*.

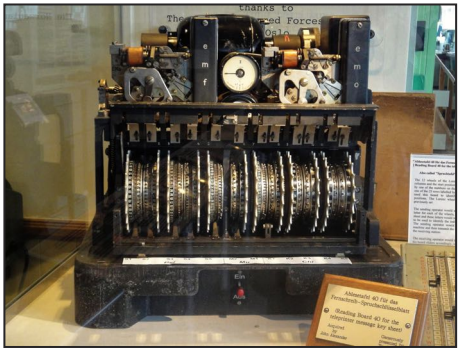
« Une machine Enigma standard employait un groupe de trois rotors, chacun pouvant être installé sur 26 positions. D'autres versions d'Enigma utilisaient 4 rotors. La Bombe essayait chaque position de rotor possible et appliquait un certain test. Le test éliminait

des milliers de positions des trois rotors ; les quelques solutions possibles étaient alors examinées manuellement. Pour utiliser une Bombe, cependant, un cryptanalyste devait d'abord produire une copie - une section de chiffrement pour lequel il pouvait deviner le décodage correspondant. » (Wikipédia, mais l'article en anglais est beaucoup plus complet et permet de comprendre vraiment le procédé).

« Les deux machines à rotor électromécanique allemandes, Enigma et la machine de Lorenz, dont les signaux sont décryptés à *Bletchley Park*, auraient été inviolables, à condition d'être correctement mises en œuvre. Les fautes de procédure [commises par quelques opérateurs allemands] permirent aux cryptanalystes du GC&CS de lire une partie des messages chiffrés de ces deux machines. » (Wikipédia).

Les équipes de Bletchley Park et leurs réalisations

De l'équipe de *Bletchley Park*, la postérité a surtout retenu Alan Turing, connu pour de nombreuses autres raisons, mais si ce dernier a effectivement été le contributeur principal à la conception et au perfectionnement de la Bombe et à l'élaboration des procédures logiques de test destinées à accélérer l'analyse, il serait injuste de laisser dans l'ombre les autres cryptanalystes : Gordon Welchman, Harold Keen, l'helléniste Alfred Dillwyn « Dilly » Knox, et d'autres. La fabrication des Bombes (plus de 200 exemplaires furent construits et dispersés sur différents sites pour diminuer le risque de destruction par un bombardement) était assurée par la *British Tabulating Machine Company* à Letchworth, Hertfordshire.



Machine de Lorenz…

… et son clavier

Les machines dites « de Lorenz », selon le nom de l'entreprise qui les fabriquait, utilisées par l'état-major allemand, étaient beaucoup plus compliquées que les Enigma. Ce sont les équipes de Ralph Tester et de Tommy Flowers qui, d'après les idées théoriques de Max Newman et en exploitant là encore des erreurs de manipulation de chiffreurs allemands, conçurent des automates qui aboutirent à la conception du calculateur électronique Colossus, capable de décrypter les messages chiffrés par une machine de Lorenz. Le Colossus britannique dispute à l'Eniac américain le titre de premier ordinateur électronique programmable, mais en fait ni l'un ni l'autre ne sont des ordinateurs au sens contemporain du terme : c'est le texte de John von Neumann *First Draft of a Report on the EDVAC* qui donnera la première formulation de l'ordinateur à programme enregistré, dont les premières réalisations effectives, toutes les deux Britanniques, seront

le *Manchester Mark I* et l'*Electronic delay storage automatic calculator* (EDSAC) à Cambridge. Avant von Neumann, programmer, c'était tourner des boutons de commutateurs et brancher des fiches dans des tableaux de connexion, après von Neumann, c'était écrire des textes, ce qui ouvrait la voie à la science informatique.

Conclusion

Cette visite nous a permis de découvrir des aspects de la guerre secrète dont certains sont restés confidentiels jusque dans les années 1970. Les techniques mises en œuvre ne relevaient pas encore de l'informatique au sens actuel du terme, mais elles lui ouvraient la voie. Et elles mobilisaient déjà des théories scientifiques toujours mises à contribution pour la cryptographie d'aujourd'hui, même après la révolution du chiffrement asymétrique dans les années 1970 par Diffie, Hellman, Merkle, Rivest, Shamir et Adleman.