timbres-postes, monnaies et médailles

Par Daniel TANT

Les services postaux de tous pays, sont sensibles aux avancées technologiques, et le chiffre en fait partie.

William Friedman et la SIGABA

Inspiré par la machine à chiffrer allemande Hebern, William Friedman, directeur du *Signals Intelligence Service* de l'armée des U.S.A., invente un système de lecture de bande perforée qui déclenche un avancement des rotors.

C'est la M-134 dont la fragilité des rubans pose de gros problèmes sur les champs de bataille.

L'associé de William Friedman, Frank Rowlett apporte des améliorations sur le système d'avance des rotors.

La M-229 est alors utilisée avec la M-134, ce qui donne la M-134-C.

En 1937 leur invention est remarquée par le directeur du bureau *Office of Naval Intelligence* (espionnage naval). Encore améliorée, la machine devient la CSP-889 ou CSP-888. C'est en 1941 que l'armée de terre l'adopte également. Dès lors elle s'appelle SIGABA ou CSP-2900 et ne compte pas moins de quinze rotors. Elle se présente sous la forme d'un cube métallique noir, lourd et peu maniable.

Sur ce timbre espagnol émis en l'honneur de William Friedman une Sigaba figure à l'arrière plan.

Les zlotis

Craignant à juste titre son annexion par l'Allemagne ou par la Russie dès la fin de la Première guerre mondiale, la Pologne s'équipe d'un bureau du Chiffre, le Biuro Szyfrow qui, dès 1926, cherche à décrypter les messages allemands chiffrés avec l'Enigma.

En 1931 un Allemand aigri de son échec social et ancien chiffreur sur enigma, Hans-Thilo Schmidt est le frère du chef du service des signaux à Berlin et qui vient d'imposer cette machine à l'armée allemande. Jaloux de son frère, il se rend le 8 novembre en Belgique et

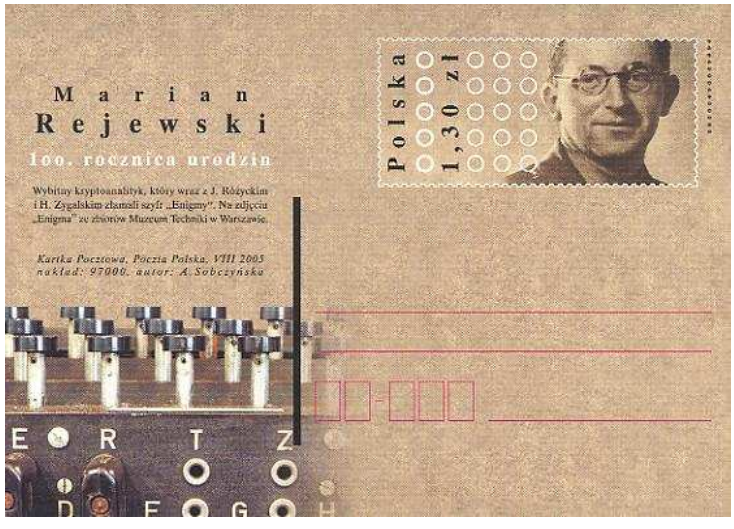
permet, pour 10 000 marks, que les plans de l'Enigma soient photographiés par un agent français. La France ne possédant pas de décrypteur efficace, les plans sont transmis à la Pologne. Le Biuro Szyfrow, plutôt que de recruter des linguistes, recrute par concours vingt mathématiciens qui parlaient tous parfaitement l'allemand.

L'un d'eux, Marian Rejewski alliant technique, science et intuition réalise une machine volumineuse qu'il baptise « bombe », capable de décrypter les messages allemands, du moins jusqu'en 1939 lorsque les Allemands modifient le nombre de clefs possibles qui s'élèvent désormais à 159 milliards de milliards !…

En juillet 1939, les Chiffreurs anglais et français sont invités à Varsovie et découvrent avec surprise l'existence de la « Bombe » de Rejewski et en reçoivent un exemplaire de cette machine pour chacun de nos deux pays.

L'origine du décryptement des messages d'Enigma pendant la Seconde guerre mondiale est dû principalement aux Polonais Marian Rejewski, Henryk Zygalski et Jerzy Rozycki. En leur mémoire, la Pologne a édité des pièces de 2 et 10 zlotis en forme de rotor avec leur nom inscrit et en 1983 un timbre commémoratif pour le 50è anniversaire.

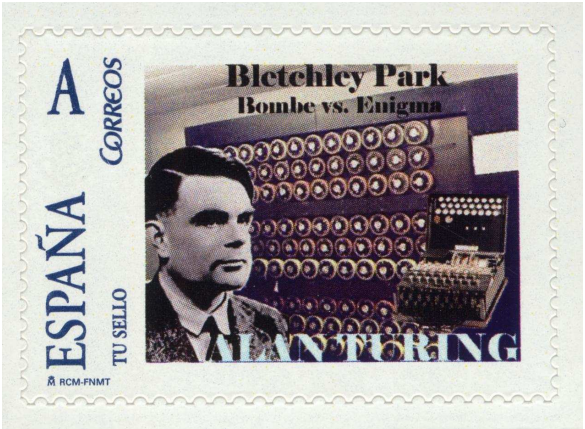
Une carte postale polonaise rappelle également le travail de Marian Rejewski.



Alain Turing et la Bombe

Alan Turing, le père de l'informatique a joué aussi un rôle primordial dans l'avancée de la cryptographie. Né le 23 mai 1912 à Londres il montre très tôt des capacités intellectuelles exceptionnelles, lui permettant par exemple, à 16 ans de comprendre les travaux d'Enstein. Il se trouve en 1937 et 1938 à l'université de Princeton puis retourne à Cambridge en 1939.

Pendant la Seconde guerre mondiale, il travaille à Bletchley Park sur le décryptement des messages de la machine allemande Enigma, à partir des études polonaises sur cette machine et crée avec Gordon Welchman et Richard Pendered une machine électromécanique appelée « bombe » comme son équivalent polonais, capable d'effectuer en une journée le travail de dix mille personnes. Nous lui devons également quatre autres éléments majeurs dans le décryptement des messages allemands. Son rapport sur les applications de la probabilité à la cryptographie et son document sur la statistique des répétitions ne sont déclassés que depuis avril 2012.

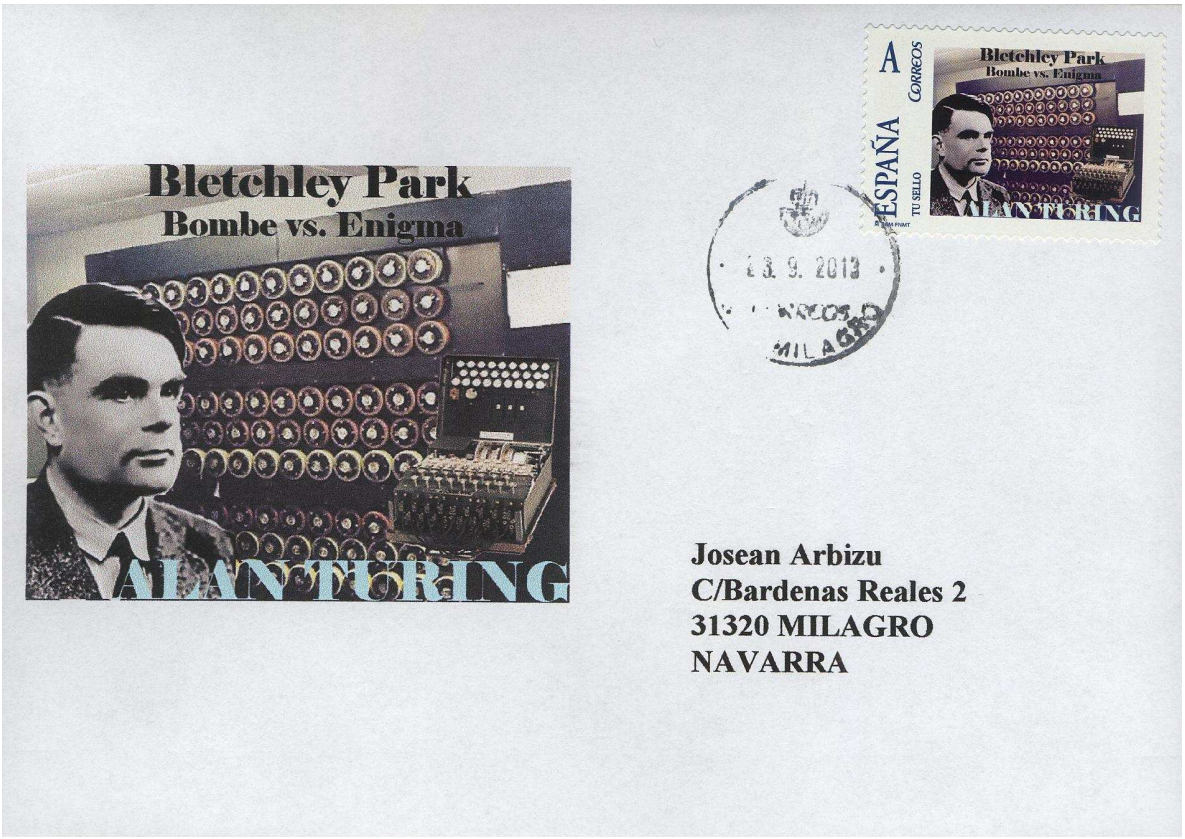


De 1945 à 1948 il travaille au National Physical Laboratory de Teddington (R.U.) sur la conception de l'Automatic Computing Engine (moteur de calculs automatiques) et en 1949 travaille sur la programmation du premier ordinateur : Manchester Mark I.

Membre de la Royal Society, Turing est mis à l'écart dès 1952 pour ses penchants homosexuels.

Il meurt par une pomme trempée dans du cyanure le 7 juin 1954. Le 10 septembre 2009 le Premier ministre anglais a présenté des excuses publiques au nom du gouvernement pour la manière ingrate avec laquelle Turing a été traité après la guerre.

Sur ce timbre émis par l'Espagne figurent Alan Turing au premier plan et une partie de la « Bombe » à l'arrière.



Le code Navajo

La Seconde guerre mondiale a révélé l'importance des messages chiffrés. Chaque belligérant cherchant à trouver un procédé a l'abri de tout décryptement du camp adverse. Non seulement les Japonais cassaient les messages américains, mais ils arrivaient même à en fabriquer de faux…

En 1942, un ingénieur américain Philip Johnston remarque que les étudiants allemands ont étudié toutes les tribus indiennes à l'exception du peuple navajo vivant dans les réserves du nord-est de l'Arizona, des régions contiguës du Nouveau-Mexique et de l'Utah. Il connaît ce peuple où il a vécu 24 ans.

Il part donc du principe que deux transmetteurs radios de cette tribu, parlant dans leur langue sont incompréhensibles par l'ennemi et même par les autres tribus. Il partage son idée avec le lieutenant-colonel James E. Jones qui demande une évaluation du projet.

Evidemment, le dialecte est adapté aux termes militaires. Les noms d'oiseaux remplacent les avions, les poissons aux bateaux, etc... A ce système est ajouté un alphabet pour épeler, ce qui représente, en tout, 411 termes. 420 Navajos sont affectés aux transmissions et leur courage au combat a été largement reconnu.

Ils ont participé aux batailles les plus sanglantes, d'autant plus qu'ils devaient être exécutés par les soldats américains s'ils risquaient de tomber aux mains de l'ennemi, afin qu'ils ne puissent dévoiler leur code qui n'a été déclassé qu'en 1968. En 1982 le gouvernement américain institue le 14 août journée nationale des radio-codeurs navajos. Le président Georges Bush remet à 29 Code Talkers la médaille d'or du Congrès, la plus haute distinction.

En plus d'une enveloppe commémorative, le congrès américain a autorisé en 2000 la frappe d'une médaille. A l'avers, deux transmetteurs Navajos communiquent par radio. Le revers est décoré des symboles des Marines américains et de la légende : « Diné Bizaad Yee Atah naayéé Yik'eh Deesdl » ce qui, comme tout le monde le sait, signifie : « Le Navajo est la langue qui a été employée pour vaincre l'ennemi ».

Médaille de la N.S.A.

Créée le 4 novembre 1952, la National Security Agency (N.S.A.) relève du département du ministère de la Défense des U.S.A . Elle a la mission de sécuriser les communications américaines et employait en 2009, 38000 salariés.

L'agence américaine de sécurité nationale outre le fort G. Meade dans le Maryland, est implantée en Angleterre, l'Australie, le Canada et la Nouvelle-Zélande avec qui elle partage les informations, grâce au système « Echelon » qui « épluche » tous les mails, communications téléphoniques, fax, à partir de certains mots spécifiques tels que « secret », « terroriste », « espionnage », « Hezbollah », et autres…. Ce réseau surveille également les groupes et partis politiques.

Entre autres, la NSA a saboté les procédés de chiffrement de la société suisse AG Crypto par l'intermédiaire de son fondateur Boris Hagelin, fait échouer deux contrats Airbus et permis la saisie de 12 tonnes de cocaine appartenant au cartel de Cali.