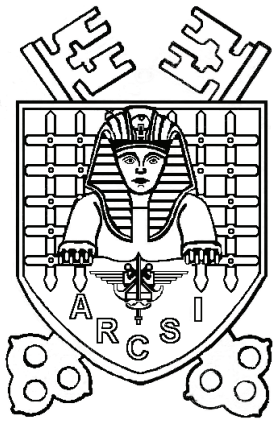

ASSOCIATION des RESERVISTES du CHIFFRE et de la SECURITE de L'INFORMATION

Nouvelle série
n° 28 - 2000

Document interne à l'Association
Réservé aux adhérents

7 . Alan TURING et L'ENIGMA

Alan TURING a écrit un mémoire ou un rapport sur l'ENIGMA ou plutôt sur le décryptement des divers modèles d'ENIGMA, dont un exemplaire se trouve aux archives nationales américaines. C'est Monsieur Ralph ERSKINE, bien connu par ses études de l'ENIGMA Marine qui l'a retrouvé et ce document m'est parvenu par notre ami Gilbert BLOCH. Il est d'une lecture difficile, car assez mal dactylographié, sans doute sur une machine fatiguée et avec un ruban usé, avec des corrections manuscrites souvent illisibles ; il manque des pages et semble ne pas avoir été achevé. Enfin TURING dominait tant la question que certaines de ses affirmations et même ses raisonnements sont difficiles à comprendre, avec une terminologie particulière ; c'est pourquoi certaines des explications suivantes peuvent demeurer hermétiques. D'après son contenu, ce mémoire aurait pu être écrit fin 1940 ou début 1941. Il soulève une première question : quand TURING a-t-il commencé à travailler sur l'ENIGMA ? On sait que le service anglais (GC and CS) a fait appel à lui et à quelques autres lors de l'alerte de 1938, qu'il a suivi une sorte de stage à la Noël 1938 et qu'il fut appelé définitivement à la mobilisation de 1939. Certains renseignements qu'il donne sont largement antérieurs mais ils ont dû lui être communiqués par le Dr KNOX.

En 1938, le GC and CS avait réussi à décrypter les machines commerciales et certaines machines utilisées en Allemagne (chemins de fer en particulier) par des méthodes manuelles classiques (mots probables et méthode dite des bâtons). Il avait aussi de ce fait su rétablir les câblages des rotors et du réflecteur dans certains cas. Mais il avait totalement échoué, comme la section du chiffre française avec la machine de la WEHRMACHT. On connaissait son existence, son mode d'emploi, la présence de fiches modifiant en partie les alphabets d'entrée et de sortie par une substitution simple, grâce aux documents remis par SCHMIDT au commandant BERTRAND qui les avait communiqués aux Anglais comme aux Polonais à partir de 1931.

Ce n'est qu'en juillet 1939 que les Polonais firent connaître aux Anglais comme aux Français la structure exacte de la machine, les câblages des rotors et des réflecteurs et leurs méthodes et moyens de décryptement, ce qui permit aux Anglais d'avancer.

Le mémoire de TURING repose sur ces connaissances dans ses chapitres relatifs à l'ENIGMA WEHRMACHT, mais il n'en indique pas la provenance.

Les prémices

Dans ses premiers chapitres, TURING rappelle les caractéristiques des diverses ENIGMA, avec les points communs : chiffrement symétrique et mouvement des roues en compteur ; ce qui a des conséquences multiples sur la structure des messages notamment.

Son moyen initial consiste à mettre la machine à plat, sur papier avec des bandes mobiles simulant les rotors (avec une longueur de 52 caractères, pour permettre les 25 décalages possibles) ; ceci suppose la connaissance des câblages des rotors et du réflecteur, connaissance dont, rappelons-le, TURING n'indique pas l'origine.

On se reportera pour bien se rappeler le fonctionnement et le mode d'emploi des machines à l'opuscule diffusé avec le bulletin de 1987, que l'auteur de ces lignes espère pouvoir remettre à jour et rediffuser en 2001 ou 2002.

Procédés manuels

TURING rappelle l'existence des cycles résultant du chiffrement d'une lettre ou plus sur deux positions de la machine, trouvaille initiale des Polonais ; le nombre et la longueur des cycles ne varient pas avec l'emploi des fiches de substitution sur la machine de la WEHRMACHT (les Polonais en avaient tiré des catalogues réalisés avec leur cyclomètre). TURING tire de ce fait certaines conclusions et une méthode d'examen des transformations successives du chiffrement dues au 1er rotor. On peut ainsi, dit-il, décrypter pas à pas, mais c'est très long et un très grand nombre d'essais sont à faire. L'avancement d'un pas du 2ème rotor n'apporte qu'une substitution simple.

On peut heureusement utiliser une méthode plus pratique, si l'on dispose de mots probables longs (50 à 70 lettres par exemple) ou de recouvrements importants entre deux ou plusieurs messages. Il y a tout de même un grand nombre d'hypothèses à tester, avant de parvenir au résultat (hypothèses concrétisées par le glissement des bandes de papier du modèle à plat). La reconnaissance du succès s'appuie sans doute sur la fréquence des lettres.

Un autre problème est de déterminer quand le second rotor tourne ; on s'en aperçoit assez facilement en considérant les bigrammes fréquents. Cette méthode permet aussi de déterminer les rotors utilisés et leur ordre. On peut aussi parvenir à rétablir le câblage des rotors quand il n'y a pas de fiches de substitution, mais le nombre des essais à faire est très important ; on peut étudier les alphabets de correspondance des rotors sur un tableau.

Avec la machine WEHRMACHT à fiches (dont on connaît les câblages des rotors et du réflecteur par les Polonais), quand peu de fiches sont utilisées, ce qui était le cas dans les premières années, on travaille comme s'il n'y en avait pas, en notant les coïncidences et on en déduit les substitutions produites par les fiches.

Malheureusement cette méthode échoue très souvent ; un palliatif est d'utiliser l'HERIVELISMUS : HERIVEL avait remarqué que les chiffreurs modifiaient de peu la position des roues entre deux messages et, surtout, qu'elle était proche de la position de base (GRUNDSTELLUNG) dans les premiers messages d'une cryptopériode (1). On peut aussi exploiter des négligences dans le choix des groupes-clés, qui permettaient de découvrir rapidement l'ordre des rotors.

Les services n'utilisant pas la machine de la WEHRMACHT, ABWEHR, SD, chemins de fer, administration, commerce, ENIGMA/K, posent un autre problème. L'analyse du trafic et des réseaux permet de savoir à quelle machine on a affaire ; les méthodes décrites précédemment s'appliquent, mais l'avancement plus fréquent des rotors et le réflecteur parfois mobile posent quelques problèmes.

Procédés manuels améliorés

Des améliorations de la méthode générale ci-dessus ont été apportées pour les machines n'ayant pas de fiches de substitution. Le texte de TURING suppose que l'on connaît

déjà les câblages des rotors et du réflecteur et que l'on a déjà décrypté des messages donc que l'on connaît des mots probables, notamment en début ou en fin de message.

On fait alors des essais avec un seul rotor et ses divers points de départ (25) toujours en utilisant la simulation de la machine par le tableau à bandes ; on parvient ainsi à trouver le point de départ du premier rotor, en s'appuyant sur la fréquence des bigrammes et la symétrie de la machine. On fait ensuite intervenir les autres rotors qui, s'ils ne tournent pas, n'apportent qu'une substitution simple, laissant subsister la fréquence des bigrammes. On arrive ainsi à caler ces rotors ; quand le second avance, il faut procéder par tâtonnements.

Cette méthode, comme la méthode précédente est longue et on a cherché les moyens de l'accélérer.

D'abord on a utilisé un masque à perforations. Un tableau représente le chiffrement d'un rotor (carré de 26 x 25 lettres) et on écrit au dessous le mot probable. On perce alors sur un transparent 2 trous correspondant à la première lettre et à son chiffrement. On fait glisser le masque aux positions correspondant aux points de départ, pour trouver le bon grâce aux coïncidences.

S'il y a le même mot probable dans différents messages ou à différentes places dans le même message, il peut être utile de faire des statistiques sur le chiffrement de ce mot probable selon sa position.

Pour revenir à la méthode initiale avec la machine à bandes mobiles, la position de celles-ci donnant les coïncidences voulues permet de se repérer et d'utiliser des feuilles ou tableaux de correspondance facilitant le travail. Les explications qu'en donne TURING sont assez sibyllines pour tout autre que lui ou ceux qui les ont utilisées.

Les tableaux du type BRUESSEL (d'ou vient ce nom ?) comprennent diverses lignes correspondant aux premières lettres du message chiffré et à leur chiffrement par un rotor à ses diverses positions, on y compare le mot probable ; les coïncidences observées peuvent mener à la solution.

2 autres types de tableaux furent aussi utilisés.

- Ceux de TURING comprenant 25 lignes basées sur les premières lettres du message chiffré, comme les précédents, mais 25 colonnes correspondant aux distances possibles de coïncidence. En plaçant le message aux diverses positions de départ, on peut découvrir la bonne position grâce aux coïncidences.
- Ceux de KENDRICK où les colonnes correspondent aux lettres successives du message et dont l'efficacité est très bonne quand on a une présomption sur la position de départ.

Il semble, mais TURING ne le dit pas, que le résultat où les comparaisons réalisées étaient bonnes à une substitution simple près (celle apportée par les autres rotors et le réflecteur) décelée par les fréquences des lettres et des bigrammes et que cela ne fonctionnait, comme il le dit, qu'avec des mots probables longs.

Enfin on avait remarqué que beaucoup de messages comprenaient une proportion importante de X, environ 30 %. (La même remarque avait aussi été faite par nos décrypteurs

en 1914). On peut alors essayer un texte clair ne comprenant que des X. Sur une suite de 25 lettres, il y a 3,7 coïncidences si le point de départ est bon, 2 seulement dans le cas contraire (cf. la loi de FRIEDMAN, que TURING ne cite pas).

Les divers procédés parviennent à faire trouver la position de départ du 1er rotor ; il faut ensuite trouver celle du 2ème ; cela se fait soit en examinant les bigrammes soit avec des catalogues adéquats.

Les catalogues

Les catalogues sont obtenus, d'après TURING, en chiffrant les 13 paires d'un rotor aux différentes position de celui-ci (26), il s'agit sans doute des paires de correspondance entre l'entrée et la sortie (symétriques). Ce tableau-catalogue permet de trouver les couplages et le point de départ de ce deuxième rotor.

La procédure diffère, selon que le réflecteur peut tourner ou non. Dans le second cas, on utilise le mot probable pour rechercher les paires correspondantes du catalogue ; dans le premier il faut disposer autrement ce tableau-catalogue avec des diagonales.

Le système très simple ne permet pas de trouver dans tous les cas les positions des 2ème et 3ème rotors et du réflecteur : pour répondre à tous les cas, il faut utiliser un catalogue de 13 feuilles à 26 x 26 cases (TURING ne dit pas comment elles sont constituées ni à quoi elles correspondent, on peut penser que ces 13 feuilles proviennent de 13 positions du réflecteur, nombre suffisant du fait de la symétrie).

JEFFREYS (ou JEFFRIES selon d'autres auteurs) a aussi inventé des feuilles avec perforations sur lesquelles TURING ne donne aucune indication. JEFFREYS avait piloté la fabrication en Angleterre des feuilles perforées de ZYGALSKI basées sur les lettres "neutres" qui permirent les décryptement en France et en Angleterre à partir de janvier 1940 ; ces lettres neutres résultaient du double chiffrement de la clé du message qui était aussi utilisé par les services autres que la WEHRMACHT. Ces nouvelles feuilles étaient peut-être basées sur le même principe.

TURING indique enfin que l'on peut utiliser le même genre de perforations avec les feuilles de TURING citées plus haut. Le résultat, positif, s'obtient plus rapidement avec de telles feuilles.

L'ENIGMA WEHRMACHT avec fiches de substitution

Méthodes manuelles

On peut appliquer les méthodes précédentes si l'on connaît la disposition des fiches ou s'il y en a peu d'utilisées. L'essentiel est de disposer d'un mot probable. Celui-ci peut être fourni par l'analyse du trafic réalisé antérieurement (TURING ne cite pas cette source, à laquelle HINSLEY et WELCHMAN accordent une grande importance), par les agissements fautifs des chiffreurs ou le BANBURISMUS (2).

Si le nombre des fiches de substitution est faible, le mot probable est peu affecté et il est possible de trouver la clé manuellement, par exemple en utilisant les feuilles de TURING ou de JEFFREYS, en déplaçant le mot probable.

Ces méthodes ont donné de bons résultats mais ne sont plus praticables lorsque le nombre des fiches en service est élevé (sans doute plus de 6) ou lorsque le nombre de rotors est notable (cas de la machine de la WEHRMACHT avec ses 5 rotors et de la machine de la Marine avec ses 7 puis 8 rotors).

Méthode mécanique

La BOMBE

Nous ne reprendrons pas ici les explications données dans l'opuscule "Les décryptements de la machine ENIGMA des Armées allemandes" diffusé avec le bulletin de 1987 et auquel il convient de se reporter (pages 4-4 à 4-12). TURING, dans son mémoire, développe d'ailleurs peu le principe de la machine, mais s'étend plus sur le problème de l'arrêt quand une solution est possible.

Les hypothèses à faire sur le 1er rotor (5 dans le cas de la machine de la WEHRMACHT), son point de départ (26) et l'impact des fiches sont considérable.

La solution est d'éliminer au moins partiellement l'impact des fiches, en utilisant les boucles qui se produisent dans le mot probable chiffré (pages 4-4 et 4-5 de l'opuscule susvisé) et en chiffrant le texte avec les décalages adéquats.

Il n'y a plus qu'à faire les hypothèses sur le 1er rotor utilisé et son point de départ, le reste de la machine n'apportant qu'une substitution simple facile à résoudre grâce à la fréquence des lettres et des bigrammes du mot probable.

La première machine réalisée selon les indications de TURING est baptisée LETCHWORK ENIGMA ; elle faisait les mêmes opérations que l'ENIGMA, mais plus rapidement, munie d'un clavier et d'un dispositif de sortie permettant de la relier à une autre machine ou à une imprimante. Elle était sans doute équipée avec des rotors de TYPEX. Sa mise en œuvre était manuelle. Quoique TURING n'indique pas la date de sa livraison à BLETCHEY PARK, son texte permet vraisemblablement de lever un coin du voile du mystère de la date d'apparition de la bombe, exposé par Mr. Gilbert BLOCH dans son opuscule "ENIGMA avant ULTRA", pages F2 et F3, diffusé avec le bulletin de 1986.

On sait maintenant que BLETCHEY PARK reçut le prototype de la LETCHWORK ENIGMA le 18 mars 1940 (l'incertitude demeure sur le nombre de machines simulées et sur le mode d'entraînement, manuel ou plus vraisemblablement par moteur) et a donc pu s'en servir pour remonter les clés de mai et juin 1940. Les premières BOMBES de série furent livrées en août (la première le 8 août) et septembre 1940 et étaient munies du tableau diagonal de WELCHMAN.

Ces bombes comportaient l'équivalent de 30 ENIGMA donc permettaient des recherches parallèles sur plusieurs messages.

Comme la TYPEX, les rotors des bombes avaient deux séries de contacts mais l'une servait à l'aller, l'autre au retour (et non pour une inversion des signes comme sur la TYPEX, car l'ENIGMA n'avait pas une telle inversion) ; cela simplifiait les câblages des tableaux d'entrée et de sortie et les raccordements.

Mais le problème d'un décryptement rapide n'était pas résolu par cette machine assez simple, car en plus du temps nécessaire à l'inscription du menu (lettres à entrer et décalages des machines successives) on s'aperçut que la coïncidence des lettres d'entrée et de sortie se produisait fréquemment et qu'il était nécessaire d'éliminer les "faux amis".

L'ARAIGNEE

TURING décrit assez longuement dans son mémoire les dispositions utilisées à cet effet, de façon à produire un arrêt automatique de la bombe à la position donnant la solution du décryptement, bon 1er rotor et bon point de départ de celui-ci, le reste du travail, détermination des 2ème et 3ème rotors et de leurs points de départ pouvant se faire manuellement par tâtonnements dans la baraque (HUT) chargée de rétablir la clé complète.

C'est là la clé du succès des bombes britanniques ; la connaissance de la solution des Polonais avec la Bomba y aida peut-être, mais TURING ne le dit pas.

La lettre espérée à l'entrée et à la sortie est connectée à un relais dans chaque panneau de sortie des machines faisant les essais et les contacts "positifs" de ces relais sont mis en série avec une batterie ; la machine s'arrête quand le courant passe par tous ces relais. Une autre solution est de relier entrées et sorties identiques de la bombe. En un tour, tous les résultats possibles sont examinés.

Ces examens de coïncidence n'étaient pas un problème mécanique, mais un problème de logique (spécialité de TURING) auquel on donnait une solution électrique (relais et branchements). Un autre problème était un arrêt de la machine sur la bonne position, sans délai, car le fonctionnement des relais n'est pas immédiat. On utilisa donc des circuits avec thyratrons pour commander les relais, car ces tubes réagissent sans retard à un changement de potentiel, avec un courant de plaque intense agissant efficacement sur les relais (encore nécessaires à l'époque où les transistors n'existaient pas !)

Ce système fut enfin complété par le tableau diagonal, inventé par WELCHMAN, basé sur la réciprocité des fiches et de la machine, qui multipliait le nombre de chaînes utilisables et permettait d'utiliser des chaînes courtes.

Cet ensemble de détection du résultat fut appelé SPIDER, araignée.

Mais on ne s'arrêta pas là et on continua à améliorer ce système, en particulier pour éliminer les coïncidences erronées toujours trop nombreuses.

Les premières bombes livrées comprenaient 30 ENIGMA et 3 tableaux diagonaux, ce qui permettait de tester 3 chaînes en même temps donc d'éliminer des contradictions (étude de WELCHMAN et KEEN).

Il sembla aussi possible de faire tester ces contradictions par la machine elle-même, non pas en modifiant les câblages et l'araignée, mais en ajoutant un dispositif qui vérifiait l'homogénéité du système de fiches trouvé. Ce dispositif fut baptisé "mitrailleuse" (à cause du bruit de ses relais ?). Le fonctionnement global était un peu ralenti, rallongeait l'essai de 5 minutes, mais, en éliminant les arrêts erronés, on gagnait du temps.

L'amélioration de la machine continua.

Mr. KEEN inventa un autre dispositif basé sur une modification du câblage des relais. Le but était que la machine ne s'arrête que dans deux cas : un seul relais ou tous les relais étaient activés. Cela pouvait faire manquer quelques solutions, mais c'était particulièrement efficace, quand le nombre des coïncidences donnant lieu à des arrêts erronés était grand. Ce dispositif était en cours d'essai quand TURING rédigea son mémoire et il n'en connaissait ni les détails ni les résultats. Un complément de disposition des câblages permit d'éliminer les cas ou il y avait contradiction entre les positions trouvées pour les fiches. Le matériel du Post Office permit de le faire (relais à plusieurs contacts). La machine peut alors commander une imprimante (téléimprimeur), donner les positions des rotors et la disposition des fiches jugées bonne.

D'autres améliorations étaient enfin prévues au moment où TURING rédigeait son document :

- le branchement sur le tableau diagonal d'un tableau à fiches de 325 points (13 x25) permettant d'inscrire les branchements des fiches de substitution non valables (les Allemands proscrivaient les mêmes branchements de fiches d'un jour au suivant à cette époque ce qui limitait le nombre de branchements à 6 ou 7),
- si l'on ne dispose pas d'un mot probable donnant une ou plusieurs chaînes, mais si l'on constate la répétition d'un même groupe de 6 lettres, on peut utiliser les bombes, mais il faut éliminer les nombreux arrêts erronés qui se produisent,
- quant on utilise l'HERIVELISMUS (HERIVEL avait découvert que des opérateurs choisissaient des positions de départ peu éloignées de la position résultante du calage des couronnes sur les rotors, au début d'une cryptopériode) un dispositif permet d'éviter les arrêts intempestifs loin de cette position.

L'ENIGMA de la KRIEGSMARINE

Ce que dit TURING dans son mémoire concerne le chiffre de la KRIEGSMARINE à partir de 1931. Or le GC and CS ne fut en mesure de commencer les décryptements qu'en 1939 après que les Polonais lui eurent communiqué leurs trouvailles.

Cela montre que les Anglais avaient soigneusement enregistré le trafic allemand depuis 1931 et se mirent à le décrypter en 1939. WELCHMAN, comme HINSLEY, insiste sur l'importance des informations provenant de l'analyse du trafic (même non décrypté) et des messages déchiffrés (structure et mots probables).

De 1931, dit TURING, en fait de 1934 au 30/04/37, le chiffre naval allemand a utilisé la machine WEHRMACHT avec la même procédure que les autres armées, toutefois la position de départ était choisie dans une liste de trigrammes, (1700 dit TURING, 17576 d'après d'autres sources), dont des lots affectés à chaque station par une feuille périodique, et un trigramme utilisé ne devait pas être repris. La faiblesse de ce système résidait dans le fait qu'il donnait des indications sur la position de base (GRUNDSTELLUNG) servant à chiffrer la position de départ, en utilisant les marquants où les 1^{ere} et 4ème lettres, 2ème et 5ème ou 3ème et 6ème étaient identiques. Les Polonais en avaient fait usage (catalogue établi par le cyclomètre, des positions donnant une telle possibilité pour chaque position de base et feuilles de ZYGALSKI). Le petit nombre des fiches de substitution utilisé permettait de retrouver

facilement leurs branchements. On pouvait aussi utiliser les feuilles de TURING mentionnées ci-dessus. Le banburismus pouvait aussi s'appliquer.

Il reste ensuite à trouver la RINGSTELLUNG (position des couronnes sur le noyau des rotors) ce qui était facile du fait qu'à la période considérée la disposition des rotors et la RINGSTELLUNG n'étaient changées que toutes les 2 semaines. Quand ce changement survenait, le décryptement était facile car dans les messages en plusieurs parties dont les indicatifs et les signatures étaient les mêmes, chaque partie commençait par le groupe date-heure (chiffré) de la précédente, ce qui donnait un mot plus que probable.

En mai 1937 les préambules changent et comprennent 2 groupes de 4 lettres (comme indiqué dans l'opuscule de 1987, page 1-7). On trouva la position des dicordes pour les 2, 3, 4, 5 et 8 mai et on put lire une centaine de messages et donc analyser les préambules. Les positions des rotors étaient indiquées par 3 bigrammes (tirés d'un tableau de correspondance) plus un bigramme inutile, soit directement soit après chiffrement sur la position de base.

Dans la réalité, un torpilleur n'avait pas reçu son tableau de correspondance et utilisa l'ancien système jusqu'au 3 mai, ce qui permit de remonter la disposition des rotors et de la GRUNSTELLUNG et d'opérer les décryptements et remontages indiqués ci-dessus.

Durant l'été 1937, le réflecteur A fut remplacé par le réflecteur B et en décembre 38, deux nouveaux rotors particuliers à la Marine , VI et VII avec 2 ergots d'avancement furent mis en service.

En novembre 1939 un prisonnier révéla que les nombres étaient insérés entre deux Y et que les chiffres étaient épelés en totalité. Furent examinés en conséquence tous les messages enregistrés depuis 1937 et en particulier les lettres ne paraissant pas altérées par le chiffrement (cette assertion de TURING parait étrange puisque la machine, symétrique ne peut chiffrer une lettre par elle-même, mais concerne sans doute les lettres non affectées par les fiches de substitution). On en déduisit que 70% des mots probables utilisés (chiffres) étaient bons. Ceci pouvait donner de bons résultats sur le trafic échangé jusqu'en août 1939 ; on constata que deux clés seulement étaient utilisées, l'une pour la Baltique, l'autre pour les autres mers et océans.

Les clés du 28 novembre 1938 et des jours voisins furent remontées. Le nombre des dicordes de substitution était de 6 ; l'ordre des rotors et la position des couronnes semblait demeurer fixe pendant une semaine. On aurait pu trouver toutes les clés de cette époque si le trafic avait été plus important.

En fait les décryptements ne purent se faire à partir de 1939 que grâce à la capture de documents sur les navires allemands (voir tableau page 4 - 18 de l'opuscule de 1987 qui indique la capture du patrouilleur VP 2523 le 26 avril 1940). Cette première capture fournit des clés et l'instruction sur la confection des préambules, dont le changement avait rendu le décryptement impossible faute de disposer des tableaux de correspondance des bigrammes.

On inventa alors (en 1939 ou 1940 ?) un système basé sur la fréquence des E. Une longue bande perforée contenait le chiffrement du E aux diverses positions de la machine. Une bande comportant le message chiffré était alors placée en regard. Le nombre des coïncidences donnait le nombre des E dans le message clair. Toutes les positions relatives de

ces deux bandes donnant un nombre de E supérieur à un certain niveau pouvaient alors être essayées. Mais ce système ne fut jamais employé car un autre plus simple fut trouvé.

Quand on parvint à lire les messages de 1938, on s'aperçut de la grande fréquence du mot EINS (Primo en allemand). On fit donc un catalogue du chiffrement de EINS sur les diverse positions de la machine en les classant par ordre alphabétique (25 feuilles de A à Z, le E étant exclu du fait de la réciprocité). On réalisa ensuite ce catalogue par cartes perforées (utilisables sur machines mécanographiques), ce qui facilitait les recherches.

En fait le programme du décryptement était le suivant : quand on disposait de l'ordre des rotors, de la position des couronnes et des dicordes pour un jour donné (TURING ne dit pas comment cela était obtenu, sans doute à la suite de captures de documents), on faisait le catalogue des EINS correspondants et on l'utilisait pour extraire les paires de messages ayant le même bigramme respectivement aux 2ème et 3ème place du préambule. Si 4 cas de cette espèce étaient relevés, on pouvait retrouver la position de base (GRUNDSTELLUNG) et le décryptement pouvait être obtenu avec la bombe.

CONCLUSION

Le mémoire de TURING a paru intéressant à analyser, malgré ses difficultés, car il montre l'ampleur des travaux effectués par les scientifiques de BLETCHEY PARK, et TURING en premier, leur progressivité et leur rapidité relative, comme ce fut aussi le cas en Pologne.

Il était connu à BLETCHEY PARK sous le nom de PROF'S BOOK, comme le rappelle Alan STRIPP dans le livre CODEBREAKERS co-écrit avec le professeur HINSLEY, paru en 1993, et dont il a été rendu compte dans le bulletin 22 de 1994.

Il met bien en lumière la créativité, le grand nombre de pistes et les méthodes à explorer, l'amélioration à apporter continûment à celles-ci ; tout cela est à la base des succès des décrypteurs de tous les temps, mais les connaissances en mathématiques, logique et informatique sont devenues maintenant indispensables.

Louis RIBADEAU DUMAS

(1) Un sous-officier du Chiffre avait remarqué en 1958 que la même "paresse" sévissait dans le choix de la clé de chiffrement des préambules des messages chiffrés en M. 209, où les lettres choisies étaient proches de l'espace. Le bureau Chiffre dut prendre des mesures contre cette tendance.

(2) Ce procédé, BANBURISMUS, consiste à utiliser des feuilles sur lesquelles on a répété l'alphabet par colonnes successives. Le texte du message chiffré était perforé, colonne par colonne, avec des décalages de - 25 à + 25, et on comparait les feuilles 2 à 2. Le nombre de coïncidences verticales était noté et on parvenait ainsi, d'après ce nombre à déterminer le 1er rotor et des mots probables. Le mot BANBURISMUS vient de BANBURY, localité où les feuilles étaient confectionnées et perforées. Les alphabets en question étaient, d'après certaines sources, des alphabets normalement ordonnés mais pouvaient aussi être ceux fournis par un rotor. Ce procédé permettait de déceler les recouvrements.