TURING ET LA CRYPTANALYSE : MÉCANISATION ET PROBABILITÉS TURING AND CRYPTANALYSIS : MECHANIZATION AND PROBABILITIES

Marie-José Durand-Richard, Philippe Guillot

INTELLECTICA

NUMERO SPECIAL : *RETOUR A TURING : SON HERITAGE AUJOURD'HUI*

pour Intellectica, n° 72., 2020/1, ISSN n°0769-4113
Edité par Michel de Glas et Jean Lassègue

Marie-José DURAND-RICHARD
marie-jo.durand-richard@orange.fr
MCF honoraire, Université Paris 8 Vincennes Saint-Denis
Chercheuse associée, laboratoire SPHERE UMR 7219 CNRS-Université Paris Diderot
Philippe GUILLOT
philippe.guillot@univ-paris8.fr
MCF Université Paris 8 Vincennes Saint-Denis, département de Mathématiques et d'Histoire des Sciences.

TURING ET LA CRYPTANALYSE : MÉCANISATION ET PROBABILITÉS

TURING AND CRYPTANALYSIS : MECHANIZATION AND PROBABILITIES

RESUME :
La contribution d'Alan M. Turing (1912-1954) à la cryptanalyse est souvent ignorée ou mal connue. Il règne souvent une malencontreuse confusion entre la conception abstraite de Turing du calcul mécanique, sa conception des *Bombes* qui ont servi au décryptement d'*Enigma,* et la production du *Colossus*, premier calculateur électronique conçu et réalisé à Bletchely Park. Cette confusion peut s'expliquer à la fois par une vision trop souvent hagiographique des événements attachés à la vie et à l'œuvre de Turing, et par le secret qui a longtemps régné sur les productions de Bletchley Park. Cet article vise à resituer le travail de Turing dans le contexte de la vaste entreprise de cryptanalyse qu'a constitué Bletchley Park pendant la Seconde Guerre Mondiale, et à analyser les conditions du rapprochement irréversible ainsi engagé entre cryptanalyse, mécanisation du calcul et mathématiques. Si Turing n'a pas directement contribué à la construction du Colossus, il a développé l'approche probabiliste de la cryptanalyse, que Irving John Good (1916-2009) révélera plusieurs décennies plus tard, et qui est est aujourd'hui au fondement de l'analyse séquentielle.

MOTS-CLES : A. M. Turing, histoire de la cryptanalyse, mécanisation du calcul, *Enigma*, *Bombes*, *Colossus*, W. G. Welchman, I.J. Good, probabilités, facteurs de vraisemblance.

ABSTRACT :
The contribution of Alan M. Turing (1912-1954) to cryptanalysis is often overlooked or little known. There is often an unfortunate confusion between Turing's abstract conception of mechanical calculation, his conception of the *Bombes* which were used to break *Enigma*'s code, and the production of *Colossus*, the first electronic calculator designed and produced at Bletchely Park. This confusion can be explained both by an all too often hagiographic vision of the events attached to the life and work of Turing, and by the secret which has long reigned over the productions of Bletchley

Park. This paper aims to integrate Turing's work in the context of the vast cryptanalysis enterprise that Bletchley Park constituted during the Second World War, and to analyze the conditions of the irreversible relationship thus engaged between cryptanalysis, mechanization and mathematics. If Turing did not directly contribute to the achievement of the Colossus, he developed the probabilistic approach to cryptanalysis, which Irving John Good (1916-2009) revealed several decades later, and which is today at the foundation of sequential analysis.

KEY WORDS : A. M. Turing, history of cryptanalysis, mechanization of computation, *Enigma*, *Bombes*, *Colossus*, W. G. Welchman, I. J. Good, probabilities, likelihood factors.

INTRODUCTION

Le nom d'Alan M. Turing (1912-1954) est étroitement associé à la conception de la machine éponyme, élaborée en 1936-37 dans le cadre de ses recherches sur le problème de la décision (Turing, 1937). Il s'agit alors d'une machine abstraite, d'un concept théorique qui tend à préciser le caractère potentiellement universel du calcul. Mais cette conception théorique ne doit pas être confondue avec l'élaboration des grands calculateurs qui conduiront aux ordinateurs après la Seconde Guerre Mondiale, et qui s'enracine tout autant dans des recherches d'ingénierie et de mathématiques appliquées, essentiellement menées aux Etats-Unis et en Angleterre.

Pendant cette même période, les recherches de Turing abordent elles aussi des territoires plus concrets. Dès son retour des Etats-Unis en 1938, il est engagé à Bletchley Park auprès de la *Government Code and Cipher School* (GC&CS), qui est alors confrontée à l'impérieuse nécessité de décrypter les messages chiffrés des armées allemandes, et en premier lieu ceux de la machine *Enigma.* Il y fera des contributions majeures, qui ne doivent pas éclipser l'héritage des travaux des mathématiciens polonais au cours des années 1930. Il règne souvent une malencontreuse confusion entre la conception abstraite de Turing du calcul mécanique, sa conception des *Bombes* qui ont servi au décryptement d'Enigma, et la production du *Colossus*, premier calculateur électronique conçu et réalisé à Bletchely Park pour décrypter, non pas l'Enigma, mais la machine de Loretnz, et réalisé par l'équipe de Maxwell H. A. Newman (1897-1984), la *Newmanry.* Cette confusion peut s'expliquer à la fois par une vision trop souvent hagiographique des événements attachés à la vie et à l'œuvre de Turing, et par le secret qui a longtemps régné sur les productions de Bletchley Park. La documentation, déclassifiée au cours des dernières décennies, permet fort heureusement de mieux cerner les apports respectifs des cryptanalystes de Bletchley Park, et de mieux caractériser les spécificités de ce type de travail.

La Seconde Guerre Mondiale correspond à un moment essentiel dans l'histoire de la cryptologie, marquée par l'utilisation massive de machines à chiffrer, et par le recours de plus en plus prégnant aux mathématiques et aux machines dans les procédés de décryptement. Les relations entre mathématiques et ingénierie ne sont pas totalement nouvelles : elles se sont développées autour de machines mathématiques telles que l'analyseur harmonique ou l'analyseur différentiel avec les développements de la physique expérimentale dans la première moitié du 20ème siècle (Durand-Richard, 2019). Mais elles envahissent désormais le champ de la cryptologie, et s'établissent durablement et à une échelle industrielle lorsque la GC&CS s'installe à Bletchley Park en août 1939. Une entreprise collective de très grande ampleur s'y met en place, véritable « industrie » fondée sur une stricte division du travail légitimée par l'abondance du travail et l'obligation du secret. Si Turing en est un acteur de poids, son travail ne saurait être évalué indépendamment de toute cette

infrastructure, et des interactions permanentes qu'elle coordonne entre cryptanalystes, militaires, mathématiciens, linguistes, ingénieurs et opérateurs, où toute invention résulte de compétences multiples. Les Bombes marquent une première étape de ce changement radical d'échelle, qui installe de façon définitive la mécanisation des procédures de décryptement.

Le présent article entend analyser les contributions de Turing à la cryptanalyse en les resituant dans ce contexte, afin de mieux cerner leur impact dans l'évolution de ses propres conceptions. Une telle analyse suppose de préciser d'abord les difficultés, nouvelles en ce domaine, issues de l'adoption d'Enigma par les armées allemandes depuis 1926, et les acquis antérieurs à la guerre en matière de décryptement. Au déclenchement de la guerre, lorsque Turing est recruté au sein d'un groupe de mathématiciens, Bletchley Park bénéficie d'un double héritage : celui de son chef cryptanalyste Dilwyn Knox (1894-1943), qui a décrypté l'Enigma commerciale en 1937, et celui des mathématiciens polonais, qui décryptent l'Enigma militaire depuis 1933, grâce à des moyens tant mathématiques que mécaniques. Synthétisant ces deux approches, Turing va développer un autre type de machines électro-mécaniques que W. Gordon Welchman (1906-1985) améliorera. La méthode des *cribs* – ces mots probables sans lesquels les Bombes auraient été inutiles – leur conférera l'efficacité nécessaire pour décrypter l'Enigma, dont les conditions d'utilisation se sont complexifiées depuis le début de la guerre. Si ces Bombes ne sont en aucun cas des ordinateurs, elles représentent une matérialisation de raisonnements logiques concrétisés sous forme de diagrammes et de montages sur la machine.

Mais ces méthodes et ces machines ne se suffisent pas à elles-mêmes. Elles vont toujours de pair avec un travail systématique de classification des milliers de messages qui parviennent quotidiennement à Bletchley Park au plein cœur de la guerre. Turing initie des méthodes fondées sur la probabilité des causes énoncée par le théorème de Bayes pour optimiser le recours aux *cribs*. Ces méthodes probabilistes étayent notamment un mode d'attaque des messages, appelé *Banburismus*, utilisé à Beltchley Park jusqu'à ce que les Bombes soient assez performantes pour s'en dispenser. Les écrits théoriques de Turing qui les fondent, longtemps restés secrets, marquent le point de départ de l'analyse séquentielle, dont Irving John Good (1916-2009) lui reconnaît la paternité dès 1979 sans pouvoir alors détailler son travail. Cette analyse structure aujourd'hui bon nombre d'approches, des neurosciences au *deep learning*. Turing reconduit cette approche probabiliste avec sa méthode dite *Turingery*, ou *Turingismus*, lors des premières tentatives de décryptement des messages chiffrés par la machine de Lorenz. Mais, parti aux États-Unis pour six mois en octobre 1942 afin d'y suivre la construction de nouvelles Bombes suite à l'accord Holden avec la Grande-Bretagne, il ne participera pas à la réalisation des Colossus.

I. ENIGMA ET LA MÉCANISATION DE LA CRYPTOLOGIE

Appréhender le travail de Turing en cryptanalyse suppose de mesurer la complexité nouvelle qu'introduisent les machines à rotors dans le chiffrement au début du XX^{ème} siècle, ce qui passe par une présentation de leur implantation et de leur fonctionnement. Dès la Première Guerre Mondiale, plusieurs inventeurs ont proposé des mécanismes de ce type, et déposé des brevets pour réaliser un chiffrement pratique et sûr. C'est finalement l'ingénieur allemand Arthur Scherbius (1878-1929) qui produit la machine Enigma en 1923, d'abord à destination des milieux commerciaux. Son succès viendra des militaires (Guillot, 2015). Ces machines introduisent une si grande complexité du chiffrement que les meilleurs spécialistes, comme par exemple le général français Marcel Givierge (1871-1931), chef du Service du Chiffre pendant la Grande Guerre, les considèrent comme

mathématiquement inviolables (Givierge, 1923). Force est alors de recourir à une recherche exhaustive des clés possibles, voire de la mécaniser, dès lors que la lenteur des seuls moyens humains la rendrait vaine.

Quelques définitions spécifiques à la cryptologie

• Chiffre ou chiffrement : dissimulation de la signification d'un message au moyen de substitutions, transpositions, ou autres opérations littérales ou mathématiques.
• Message clair : message intelligible d'origine.
• Message chiffré ou cryptogramme : message qui a été soumis au chiffrement.
• Déchiffrement : activité du récepteur d'un cryptogramme, qui retrouve le message clair en connaissant son mode de chiffrement.
• Décryptement : activité d'un intercepteur étranger au système de communications, qui doit retrouver le message clair sans connaître la clé de chiffrement.
• Cryptographie : discipline qui recouvre toutes les activités de chiffrement.
• Cryptanalyse : discipline qui regroupe toutes les activités de décryptement.
• Cryptologie : discipline qui regroupe la cryptographie et la cryptanalyse.

Les avancées techniques ont joué un rôle fondamental dans l'évolution de la cryptologie. Longtemps fondée sur l'analyse du langage et de ses systèmes d'écriture, elle a connu une première mutation lorsque les armées ont commencé à transmettre leurs messages par télégraphe. Auguste Kerckhoffs (1835-1901) avait alors attiré l'attention des militaires sur la nécessité de renouveler les méthodes cryptographiques, en ne s'attachant plus au chiffrement des messages pris isolément, mais en produisant ce qu'il qualifie de « système cryptographique », caractérisé par son organisation d'ensemble (Kerckhoffs, 1883). Cependant, c'est seulement après la Première Guerre Mondiale que la marine allemande a pris pleinement conscience du problème. Elle a adopté Enigma dès 1926. L'armée de terre l'adoptera en 1928, et l'armée de l'air en 1935, lorsque Hitler, en violation du traité de Versailles, la rétablit et enclenche le réarmement de l'Allemagne. L'Enigma sera un élément essentiel de la *Blitzkrieg*, ce « changement révolutionnaire dans l'histoire de la guerre » (Welchman, 1982, p. 19). Chargée sur les camions ou dans les avions, elle sera au cœur d'un système de communications qui coordonne très rapidement les mouvements des forces terrestres et aériennes, entre l'arrière et la ligne de front, la vitesse des transmissions déterminant la vitesse de l'attaque.

L'Enigma est une machine électromécanique à rotors, munie de piles et transportable dans une mallette (fig. 1). Elle comprend :
- un clavier des 26 lettres de l'alphabet,
- un tableau de 26 ampoules,
- 3 rotors, dont chacun porte une bague pouvant être calée dans les vingt-six positions possibles
- et un réflecteur.

En 1930, elle sera renforcée par un tableau de fiches à l'avant de la machine, permettant de permuter certaines lettres par paires.
Le clavier ne comporte pas de signe de ponctuation. Les chiffres sont représentés par les lettres de la première ligne du clavier. Les mots sont séparés par des X, les phrases par des Y. La touche frappée ferme un circuit électrique (fig. 2). Le courant passe par le tableau de fiches, traverse chacun des rotors, rebondit sur le réflecteur et repasse par les 3 rotors et le tableau de fiches, avant d'allumer l'ampoule qui indique la lettre chiffrée. En même temps, l'action de la touche fait tourner d'un cran le premier rotor, puis le second au bout d'une rotation complète du premier et pareillement pour le troisième.

Fig.1. La machine Enigma. Wikimedia Commons. Domaine public
Museo scienza e tecnologia. Milan.

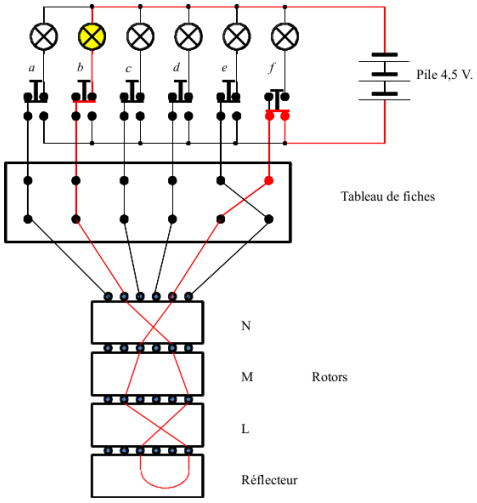

Fig. 2. Diagramme du chemin de chiffrement d'une lettre sur *Enigma.* Production des auteurs

L'intérêt majeur de cette machine est le nombre considérable de substitutions qu'elle est susceptible de réaliser, et qui changent pour chaque lettre chiffrée[1]. En ne comptant que les rotations successives des 3 rotors, le chiffrement réalise une substitution à chaque fois différente, parmi 25 x 26^2, et non pas 26^3 du fait d'un mécanisme appelé *double stepping* qui fait parfois tourner le second et le troisième rotor simultanément. Le cryptanalyste doit explorer 6 fois plus de combinaisons puisque l'ordre des 3 rotors peut être modifié. Ce nombre, qui dépasse déjà 10^{16} dès que 6 paires de fiches sont connectées, procurera aux Nazis une confiance quasi absolue dans la sûreté de leur chiffrement.

[1] Ce qui rend illusoire l'analyse des fréquences.

Au moment de son utilisation, la machine est d'abord configurée selon une « clé du jour », qui comporte le choix[2] et l'ordre des rotors, leur positionnement initial, le calage des bagues, et les paires de lettres connectées sur le tableau de fiches[3].

Datum [Date]	*Walzenlage* [Ordre des Rotors]	*Ringstellung* [Postion des bagues]	*Grundstellung* [Position initiale des Rotors]	*Steckerverbindungen* [Lettres appariées]
4 Mai	III-I-II	16-11-13	01-12-22	*CO DI FR HU JW LS TX*

Mais la machine est également configurée à partir d'une « clé du message », afin que les messages d'une journée ne soient pas tous chiffrés avec la même suite de substitutions. Une fois la machine configurée selon la clé du jour, l'opérateur choisit 3 lettres qu'il chiffre 2 fois. Les six lettres obtenues constituent l'entête du message, ou indicateur. Le corps du message est alors chiffré avec les rotors calés dans la position donnée par les trois lettres de départ. Le destinataire procédera de façon inverse pour retrouver ces trois lettres, positionner la machine et reconstituer le message en clair en tapant tout simplement le cryptogramme sur son clavier.

La structure même de cette machine impose désormais à la cryptanalyse de s'attaquer au système cryptographique tel que défini par Kerckhoffs en 1883.

2. LE TRAVAIL DES CRYPTANALYSTES POLONAIS

Hors des cercles de spécialistes, il est quasiment ignoré que la machine Enigma a déjà été décryptée en Pologne au cours des années 1930, grâce à une rencontre tout à fait spécifique de facteurs politiques, humains et scientifiques : plus concrètement, par la conjonction inédite de la mécanisation, du renseignement, et de compétences mathématiques et linguistiques. Face à une Allemagne qui ne cachait pas son intention de reprendre les territoires devenus polonais après le traité de Versailles, la Pologne avait organisé un Bureau du Chiffre, le *Biuro Szyfrów,* au sein de son service de renseignements[4]. Fort efficace depuis la guerre contre les Soviétiques (1919-1920), il fut tenu en échec à partir de l'adoption d'Enigma. Et l'identification de la machine elle-même ne suffira pas à en venir à bout.

Son décryptement réussira grâce au recrutement de trois mathématiciens en 1932, Marian Rejewski (1905-1980), Jerzy Rózycki (1909-1942) et Henryk Zygalski (1906-1978), à la contribution d'ingénieurs, et aux informations fournies par le renseignement français, sous l'égide du capitaine Gustave Bertrand (1896-1976). En mobilisant la théorie mathématique des permutations, Rejewski a pu reconstituer le câblage interne spécifique des rotors de la machine militaire, par l'observation minutieuse des cycles qui apparaissent dans les indicateurs des messages. Cette mobilisation des mathématiques est une première évolution significative des méthodes de la cryptanalyse. Grâce aux répliques de l'Enigma militaire réalisées par l'entreprise AVA – une quinzaine fin 1934 –, les messages allemands seront régulièrement déchiffrés dès janvier 1933.

Soucieux de retrouver les clés du jour sans l'aide du renseignement français, les cryptanalystes

[2] Les machines disposaient initialement de 3 rotors. Le 15 décembre 1938, ils seront choisis parmi 5 disponibles, puis parmi 8 au début de 1940.
[3] Le rythme des modifications de la clé du jour va suivre l'évolution des tensions politiques.
[4] Plusieurs mathématiciens de l'Ecole polonaise de logique y ont été impliqués avec succès au moment de l'offensive soviétique : Stefan Mazurkiewicz (1888-1945), Waclav Sierpinski (1882-1969) et Stanisław Leniewski (1886-1939).

polonais vont alors conjuguer méthodes manuelles et procédés mécaniques qui leur permettront de s'adapter aux modifications réitérées des modes opératoires introduits par les Allemands. Leur méthode dite *de l'horloge* s'appuie sur une ré-invention de l'indice de coïncidence[5] produit par William F. Friedman (1891-1969) aux États-Unis en 1920.
Une première machine, le cyclomètre, facilite l'élaboration d'un catalogue de toutes les structures cycliques possibles des indicateurs, qui renseignent sur l'ordre et la position des rotors, et donc sur une partie importante de la clé du jour. Le cyclomètre met en œuvre deux séries de rotors pour composer les permutations. Une fois établi ce catalogue aux 105 456 entrées (6×26^3), la recherche de la clé du jour ne prend que quelques minutes. Lorsque le câblage de l'Enigma militaire change en novembre 1937, le catalogue est mis à jour dès la fin décembre, si bien qu'au début de 1938, les Polonais décryptent au quotidien les messages de la *Wehrmacht* et de la *Luftwaffe*.
Les feuilles de Zygalski seront conçues pour faire face au changement du mode de chiffrement du 15 septembre 1938 – suite à l'Anschluss et à la crise des Sudètes – qui ne livre plus que des cycles de taille un, ou points fixes. Pour trouver la configuration des rotors qui donnent ces points fixes, Zygalski conçoit un système de $6 \times 26 = 156$ plaques perforées, chacune de 26×26 cases, avec un trou à l'emplacement d'un point fixe. Les messages dont l'indicateur comporte un point fixe permettent de sélectionner des plaques qui sont empilées dans une position convenable sur une table lumineuse. La lumière, lorsqu'elle les traverse toutes, indique une configuration possible des rotors pour la clé du jour. La recherche complète s'effectue en moins de deux heures.
Mais une étape supplémentaire est franchie avec la *Bomba*, une machine électromécanique imaginée par Rosycki et Rejewski, afin d'automatiser la recherche de la configuration des rotors compatible avec les points fixes observés. Un moteur fait tourner les 6 blocs de rotors qui la composent, et toutes les combinaisons sont explorées en 108 minutes. Un mécanisme à relais électromagnétiques gère l'arrêt de la machine sur la configuration idoine. Les pièces commandées à la manufacture AVA ont permis d'assembler six *Bombas* en grand secret dès novembre 1938. Les clés des messages allemands n'avaient alors plus de secret pour le Bureau du Chiffre[6].

Le 15 décembre 1938, deux nouveaux rotors sont mis en service. Le nombre de choix possibles pour l'ordre des 3 rotors passe de 6 à 60. Le câblage interne des deux nouveaux rotors a cependant pu être reconstitué. Mais il faudrait maintenant 10 fois plus de feuilles de Zygakski et de *Bombas* pour réussir le décryptement, ce que les Polonais n'ont ni le temps ni les moyens de faire alors que la guerre menace. Conscients de leur manque de moyens et de l'urgence de la situation, les Polonais organisent une rencontre a Pyry près de Varsovie, les 24 et 25 juillet 1939, où ils révèlent toutes leurs avancées aux délégations française et britannique abasourdies, offrant à chacune une réplique d'Enigma. Après l'invasion de la Pologne le 1er septembre 1939, toutes les traces du travail du *Biuro Szyfrów* sont détruites, mais Bertrand parvient à recueillir toute l'équipe. Elle est intégrée au PC Bruno, qui va travailler au château de Vignolle (Seine et Marne), en étroite collaboration avec la GC&CS des Britanniques, jusqu'à la signature de l'armistice le 22 juin 1940 entre la France et l'Allemagne. Alors que PC Bruno est évacué le 26 juin vers Alger, l'équipe franco-polonaise est reconstituée clandestinement au sein du PC Cadix, installé au château des Fouzes près d'Uzès, et elle continuera à coopérer avec les Britanniques jusqu'en novembre 1942, au moment de l'invasion de la zone sud[7].
Les mathématiciens et ingénieurs polonais ont ainsi mis en œuvre des interactions fructueuses entre

[5] Cette méthode utilise le fait que la fréquence des coïncidences de lettres pour 2 cryptogrammes chiffrés avec la même suite de substitutions est environ le double de celle observée sur des messages chiffrés avec des suites différentes.
[6] Quoi qu'il en soit, Rejewski visait un décryptement par les mathématiques et considérait cette recherche exhaustive comme un échec.
[7] Les Français gagnent l'Algérie par avion, et les Polonais fuient par l'Espagne, certains seront arrêtés.

procédés mécaniques et analyse mathématique (Guillot, 2015), que l'organisation de la cryptanalyse en Grande-Bretagne ne va systématiser qu'au moment de la guerre.

3. BLETCHLEY PARK : LE DÉCRYPTEMENT À ECHELLE INDUSTRIELLE

Au déclenchement de la guerre, la GC&CS, dirigée par Alastair Denniston (1881-1961) depuis 1919, est alors une petite structure d'environ 90 personnes, dont 30 cryptologues, recrutés plutôt parmi littéraires et linguistes. Ainsi Knox, le chef cryptanalyste, impliqué dans le décryptement du télégramme Zimmerman pendant la Première Guerre Mondiale, est un helléniste de Cambridge, éditeur de textes sur papyrus du British Museum, et féru de Lewis Carroll (Batey, 2009, pp. 31-40). La prise de conscience de la nécessité de recruter des mathématiciens dans cette structure n'est patente qu'après l'Anschluss du 13 mars 1938. La guerre va enclencher un changement d'échelle radical dans l'organisation de la GC&CS, et un renouvellement profond des méthodes.

3.1. La restructuration des moyens matériels et humains

En 1938, la GC&CS forme des listes d'universitaires susceptibles d'être recrutés. Deux séries de cours de cryptographie sont organisés à Londres en septembre et décembre 1938, rassemblant une trentaine de linguistes, germanophones et mathématiciens, et comportant une initiation à Enigma (Turing D., 2016, p. 93). Les mathématiciens recrutés sont essentiellement issus de Cambridge, dont Peter Twinn (1916- 2004), W. Gordon Welchman (1906-1985), John Jeffreys (1916-1941), et Turing[8], qui est déjà en contact avec Denniston[9] depuis son retour de Princeton en juillet 1938. L'effectif des mathématiciens ne cessera de s'étoffer au cours de la guerre.

Étape majeure du changement d'échelle qui s'amorce : le 15 août 1939, la GC&CS s'installe à Bletchley Park, un lieu d'une grande importance stratégique, à 80 km au Nord-Ouest de Londres. Ce manoir victorien se trouve à mi-chemin entre Cambridge et Oxford, à un grand carrefour de routes et de chemins de fer, et au cœur d'un système de communications par téléphone et téléscripteur. L'accroissement considérable du nombre des messages avec la guerre rend les débuts du travail assez chaotiques, du fait aussi de la mise en place de nouvelles méthodes de décryptement avides en personnel. Une vingtaine de baraques en bois, les *Huts*, sont rapidement construites dans le parc pour héberger chacune l'activité de décryptement relative à une Enigma spécifique : armée de l'air, armée de terre et marine pour l'Allemagne, mais aussi Italie, Espagne, Portugal, ainsi que le Japon. Il s'agit également de coordonner le travail avec les services de renseignement et le gouvernement. Plus tard, certaines *Huts* hébergeront des Bombes. La spécialisation des *Huts* est un élément essentiel du mode d'organisation. L'extrême division du travail est un facteur déterminant pour l'efficacité de l'entreprise et la garantie du secret des opérations : chacun œuvre sur une tâche très précise et ignore tout de ce qui se passe dans les autres *Huts*.

Dans ce processus d'organisation, Welchman joue un rôle majeur qu'il considère comme sa contribution la plus essentielle à l'effort de guerre. La mécanisation de la cryptographie a décuplé la puissance et la rapidité des attaques allemandes : puisque « jamais auparavant, les signaux radio et la

[8] Le recrutement se fait au début par relations personnelles. Twinn vient d'Oxford et fut le premier recruté en janvier 1939. Jeffreys, Turing et Welchman seront officiellement intégrés à la GC&CS le 4 septembre 1939.
[9] D'après la biographie d'Alan Turing écrite par son neveu Dermot Turing, des souvenirs familiaux font état de premiers contacts pendant son séjour d'été de 1937 en Angleterre (Turing D., 2016, p. 92).

cryptographie n'avaient été utilisés à une si grande échelle pour fournir des communications sur le champ de bataille » (Welchman, 1982, p. 20), les cryptanalystes doivent faire face à une production de masse, et la réponse doit être de même envergure. Avant même la construction des *Hut*s, Welchman remet à Denniston et à son adjoint Edward Travis[10] (1888-1956) un schéma organisationnel fondé sur cette stricte division du travail, fonctionnant 24h/24 en 3 équipes successives (Welchman, 1982, pp. 75-77). Mis en place en mars 1940, et généralisé à toutes les *Huts,* il matérialise l'attaque globale du système cryptographique de l'Axe dans son ensemble, de l'attaque cryptanalytique au traitement linguistique et à sa transmission à l'*Intelligence Service* (Hodges, 1984, p. 169).

En octobre 1941, à l'initiative de Wlechman, les quatre *Worked Uncles* – Welchman, Turing, Hugh O. D. Alexander (1909-1974) et P. Stuart Milner-Barry (1906-1995) – prendront la liberté d'écrire directement au Premier Ministre Winston Churchill (1874-1965), pour réclamer un accroissement en moyens matériels et humains. Celui-ci, conscient de l'importance de la cryptologie depuis la Première Guerre Mondiale, et du travail de Bletchley Park depuis sa visite en juin 1941, accordera immédiatement les moyens nécessaires pour tout le reste de la guerre (Turing & al, 1941). Les effectifs monteront jusqu'à 10 000 personnes, faisant de Bletchley Park une véritable industrie du décryptement.

3.2. L'analyse des messages, préalable à leur répartition dans les *Huts*

La première urgence quand les messages interceptés arrivent à Bletchley Park est d'identifier le corps d'armée d'où ils proviennent, et Welchman va se révéler particulièrement efficace dans ces questions d'organisation. Comme ses congénères, il ignore tout de la cryptologie quand il arrive à Bletchley Park, mais, en tant que chercheur en géométrie algébrique, il sait que le premier travail pour aborder un nouveau domaine est d'établir des classifications. Les messages interceptés par la station radio[11] militaire de Chatham, près de Londres, arrivent d'abord en vrac à Bletchley Park. Avec le commandant qui dirige la station, Welchman décide d'établir un rapport quotidien du trafic intercepté où sont systématiquement notées, pour chaque message la fréquence radio, l'heure d'interception, ainsi qu'un préambule composé :
- des signaux d'appel (*callsigns*) des stations d'envoi et de réception, car une même station peut recevoir des messages de plusieurs sources,
- des heures d'envoi et de réception,
- du nombre de lettres des messages,
- de l'indication qui précise si le message est complet ou s'il a une suite,
- des trois lettres (*discriminants*), qui distinguent les différents types de trafic Enigma,
- et de la position dans laquelle l'opérateur a disposé les 3 rotors (*indicator settings*) avant de choisir trois lettres pour constituer l'indicateur.

Welchman entreprend alors une analyse systématique des messages, aujourd'hui qualifiée d'analyse des méta-données[12], qui débouche sur leur classification selon les différents corps d'armées (Welchman, 1982, pp. 35-38). Il a pleinement conscience d'avoir à travailler sur un système cryptographique, et renvoie sur ce point au travail de Kerckhoffs :

[10] Il lui succédera à la tête de la GC&CS en 1942.
[11] Les stations radio sont appelées 'stations Y' (Welchman, 1982, p. 35).
[12] Ce terme renvoie à l'analyse qui est faite en cryptologie pour attaquer les messages électroniques chiffrés en travaillant, non pas sur le contenu, mais sur tout son environnement.

> « Previously, I suppose I had absorbed the common view that cryptanalysis was a matter of dealing with individual messages, of solving intricated puzzles, and of working in a secluded back room, with little contact with the external world. As I studied that first collection of decodes, however, I began to see, somewhat dimly, that I was involved in something very different. We were dealing with an entire system that would serve alive the needs of the German ground and air forces. The call signs came alive as representing elements of those forces, whose commanders at various echelons would have to send messages to each other. The use of different keys for different purposes, which was known to be the reason for the discriminants suggested different command structures for the various aspects of military operations » (Welchman, 1982, pp. 37-38).

La cartographie des messages permet à Welchman d'identifier les différents systèmes de clés, qu'il caractérisera par des couleurs, essentiellement le bleu pour la *Wehrmacht*, le rouge pour le trafic opérationnel de la *Lufftwaffe*, et le vert pour son trafic courant. À partir de ce classement, les messages pouvaient être répartis entre les différentes *Huts*.

Les messages des armées de terre et de l'air sont ainsi traités par la *Hut* 3, où la section de la *Lufftwaffe* est dirigée par Peter Calvocoressi (1912-2010), l'auteur de *Top Secret Ultra* (1980). Welchman crée la *Hut* 6, chargée de leur décryptement, le 20 janvier 1940. Sous sa direction, elle passe rapidement d'à peine une vingtaine à plusieurs centaines de personnes. Particulièrement compétent pour gérer cette production de masse, Welchman sera nommé Directeur adjoint pour la Mécanisation à la fin de 1943. Il transférera ses méthodes aux Etats-Unis lorsqu'il y émigrera en 1948. Il dirigera l'étude des applications du projet *Whirlwind*[13] au *Massachussetts Institute of Technology* (MIT) avant de travailler pour plusieurs compagnies d'informatique.

4. LES MÉTHODES

Les Bombe*s* sont à l'évidence l'étape majeure attribuée à Turing pour le décryptement d'Enigma. Construites à une autre échelle, elles prennent le relais des *Bombas* polonaises, qui ont inspiré à Knox l'idée de mécaniser le décryptement dès la rencontre de Pyry en juillet 1939. Il en discute très vite avec Travis et Turing, qu'il initie personnellement[14] aux acquis des mathématiciens polonais dès que les documents et la machine Enigma parviennent à Bletchley Park en août 1939 (Batey, 2009, p. 78). L'inestimable cadeau que constitue cet héritage des Polonais permet à Bletchley Park de démarrer efficacement le travail : 3 mois au lieu de 6, ce qui fut absolument crucial pour s'attaquer à Enigma avant l'occupation de la France par l'armée allemande (Welchman, 1982, pp. 13-14). Cet héritage est d'autant plus fructueux que les cryptanalystes britanniques bénéficient aussi du travail mené par Knox sur l'Enigma commerciale pendant l'entre-deux-guerres.

4.1. L'héritage des travaux de Knox sur l'Enigma commerciale

La méthode des mots probables fait partie des méthodes classiques en cryptanalyse, pour raccourcir et compléter l'analyse des fréquences (voir note 1). Elle fait aussi partie des méthodes manuelles des cryptanalystes polonais, et pendant l'entre-deux-guerres, elle a déjà donné quelques résultats probants à la GC&CS sur l'Enigma commerciale – sans tableau de fiches – acquise en 1927. Elle consiste à repérer un mot probable du message en clair en examinant certaines de ses caractéristiques – en-têtes,

[13] Le *Whirlwind* est le premier ordinateur à travailler en temps réel. Achevé en 1951 aux Etats-Unis, il constitue la base du système de défense aérienne, le système SAGE (*Semi-Automatic Ground Environmen system*) qui est le premier réseau couvent l'ensemble du territoire états-unien.

[14] Turing est même autorisé à emporter des documents sur Enigma au *King's Collège* de Cambridge.

signatures, termes météorologiques, formules convenues – et à tester le reste du cryptogramme à partir de cette hypothèse.

FORTYWEEPYWEEPY
Quand un message était la suite d'un autre, il commençait par FORT, abréviation du terme allemand *Fortzeitung*, qui signifie 'suite', puis il répétait l'heure d'envoi du premier message. Les chiffres étant représentés par les lettres de la première ligne du clavier, et les mots séparés par Y, un second message envoyé à 23 h 30 commençait donc par FORTYWEEPYWEEPY, et cette expression est devenue le terme générique de ce type de message à Bletchley Park.

Fig. 3. Exemple de *crib* du type déjà utilisé par les cryptanalystes polonais

En systématisant la recherche de *cribs*, Knox a produit en 1937 une méthode manuelle, la *rodding method*, du nom des *rods*, ces bandes cartonnées qu'il découpe pour associer les lettres du chiffré et du clair probable selon les mouvements successifs du premier rotor. Elle permet de déterminer le premier rotor et sa position de départ, dont les deux autres peuvent ensuite se déduire. Elle est décrite par Turing dans *A Treatise on Enigma,* ce manuel de cryptanalyse qu'il rédige en 1940 pour les nouveaux arrivants à Bletchley Park (Turing, 1940a) et détaillée par Frank Carter en 1970. Cette méthode ne donne que des fragments du texte. Cette étape du décryptement doit être complétée grâce à l'habileté linguistique des spécialistes des mots croisés qui trouvent des extensions successives du *crib* (Durand-Richard et Guillot, 2019).

Knox décrypte ainsi l'Enigma des volontaires allemands de la Légion Condor qui soutient l'offensive de Francisco Franco (1892-1975) en 1937, et celle des quatre sous-marins que Benito Mussolini (1883-1945) lui envoie[15]. En les combinant à ses propres méthodes[16] – Knox, secondé par une équipe féminine, les *Dilly's girls*, décryptera aussi l'Enigma de la marine italienne au moment de la bataille de Matapan en mars 1941, contribuant à la victoire de la *Royal Navy*. Le décryptement de l'Enigma de l'*Abwehr* en octobre 1941 relève des mêmes méthodes (Carter, 2009a-b, pp. 174-205).

Au vu des travaux polonais, Knox s'inquiète de ce qu'une méthode portant sur les indicateurs peut être anéantie à tout moment (Batey, 2009, p. 95). Sa propre expérience le convainc qu'il est préférable de travailler sur le corps du message, conviction partagée par Turing. Quoi qu'il en soit, la première urgence est d'exploiter les méthodes polonaises à plus grande échelle. 12 000 livres sont allouées pour la réalisation d'autres répliques d'Enigma, et avant même l'installation des *Huts*, Knox charge Jeffreys de la fabrication des 1560 feuilles de Zygalski, désormais nécessaires, et la division du travail proposée par Welchman est d'abord destinée à leur exploitation[17]. Une petite équipe y travaille jour et nuit dans la crainte permanente qu'un changement de procédure ne les rende inutiles (Batey, 2009, p. 98). Elles sont achevées le 7 janvier 1940. Turing en apporte un jeu au PC Bruno le 17 janvier 1941, en même temps que des statistiques établies par Knox, et promises aux Polonais depuis Pyry[18]. Le premier décryptement des Polonais en temps de guerre a lieu en présence de Turing sur un

[15] En 1936, Les Allemands ont vendu une Enigma commerciale aux Italiens et aux Espagnols de Franco.

[16] Ces méthodes – *rodding method*, *buttonning-up method* – permettent de retrouver le câblage des rotors utilisés dans une Enigma sans tableau de connexions.

[17] Welchman a aussi réinventé cette méthode, et à chaque étape du travail est attribuée une salle spécifique : enregistrement, contrôle des interceptions, mécanique, empilement des feuilles de Zygalski, décryptement (Welchman, 1982, p. 60-77). Jeffreys le secondera à la *Hut* 6 dès sa création en février 1940 et pendant 2 ans.

[18] Knox a eu à cœur de maintenir des relations étroites avec le PC Bruno : quiconque découvre des clés du jour les transmet immédiatement à l'autre partie. La proportion des messages décryptés de part et d'autre – 17% pour le PC Bruno, 83% par Bletchley Park – correspond à leurs ressources respectives.

message vert[19] du 28 octobre 1939, et sur celui du trafic bleu par Turing à Bletchley Park le 29 janvier 1940 (Batey, 2009, p. 102).

4.2. La nécessaire exploitation des vulnérabilités des modes de chiffrement d'Enigma

Les *Bombas* polonaises étant détruites, la première idée est de les reconstruire en les adaptant pour les faire travailler sur le corps du texte. Knox en étudie les plans depuis l'été avec Turing, qu'il appelle *my bombish boy* (Batey, 2009, p. 96). Leur conception est en marche dès septembre 1939. La section de recherche qui lance la fabrication, constituée de Knox, Twinn, Turing, Welchman et Jeffreys, se réunit le 1er novembre 1939, pour évaluer les différentes options, et Travis prend contact avec la *British Tabulating Company* à Letchworth. 100 000 livres sont attribuées à leur construction. Le prototype ne sera assemblé que le 18 mars 1940 dans la *Hut* 1, et la première Bombe, baptisée *Agnus Dei,* le sera le 8 août. Les Bombes ne maîtriseront le trafic allemand que de manière progressive. Il y en aura 15 en Novembre 1941, 20 en Septembre 1942, 49 en janvier 1943, et jusqu'à 200 à la fin de la guerre, mobilisant alors plus de 2000 opératrices, les WREN du *Women Royal Naval Service*.

En attendant, pour faire face à l'accroissement du trafic, il est indispensable de restreindre le nombre de combinaisons à exploiter pour trouver l'ordre et les positions de départ des rotors. Les vulnérabilités du mode de chiffrement d'Enigma vont être d'un grand secours. Elles proviennent massivement d'erreurs ou de négligence des opérateurs allemands, pris dans l'urgence du grand nombre de messages à traiter. Il arrive aussi qu'un même message soit envoyé deux fois à deux corps d'armée différents, avec un mode de chiffrement moins puissant pour l'un que pour l'autre.

L'exploitation de ces vulnérabilités débouche sur des méthodes manuelles qui continueront à fonctionner même quand les Bombes seront opérationnelles, car elles permettront de réduire leur temps d'utilisation. Les cryptanalystes parlaient de *gardening* pour designer la collecte de ces vulnérabilités, qui recevaient souvent des noms spéciaux. Les *Cillies* désignaient ainsi la présence de clés faciles à deviner dans l'indicateur, tantôt la répétition d'une même lettre, comme *AAA*, tantôt le choix de lettres adjacentes du clavier, comme *QWE* ou *ASD*, tantôt des mots doux ou des mots grossiers (Welchman, 1982, pp. 97-118).

Toutes ces astuces relèvent typiquement de l'art du cryptanalyste, associant observation et ingéniosité. Le *Herivel tip* par exemple, qui travaille encore sur les indicateurs, est conçu début mai 1940 dès que les Nazis changent la procédure de clé du message avant l'invasion de la France. Il en permet le décryptement le 21 mai. John W. J. Herivel (1918-2011), qui vient tout juste d'être recruté par Welchman, observe qu'au premier envoi du matin, les opérateurs choisissent parfois comme indicateur, non pas 3 lettres au hasard, mais la position des bagues, ou une position proche. Il les représente sur des plaques carrées, qui permettent de repérer leur proximité par des nuages de points. Le nombre de possibilités à tester peut ainsi passer de 26^3 à une petite trentaine.

Turing lui-même participe à cette collecte des *cribs.* Comme en témoigne Patrick Mahon (1921-1972) qui écrivit une histoire de la *Hut* 8 à la fin de la guerre, il établit un catalogue de tous les chiffrements du mot *Eins* – « un » en allemand, le tétragramme le plus fréquent de tous les messages – pour toutes les positions possibles des rotors, avec leur ordre et les lettres appariés (Mahon, 1945, p.44).

[19] Voir § 3.4.

Mais le trafic était considérablement plus important que celui que traitaient les cryptanalystes polonais pendant l'entre-deux-guerres. La mécanisation de l'analyse des *cribs* sur les Bombes va permettre de réguler le flux du décryptement.

5. LA RECHERCHE LOGICO-MÉCANIQUE OUVERTE PAR LES BOMBES

Si la machine dite « de Turing » définit abstraitement le concept de calcul mécanique, son auteur n'est nullement étranger aux questions concrètes de calcul et de mécanisation quand il arrive à Bletchley Park. Bien que la plupart des commentateurs retiennent essentiellement le concept abstrait de machine dans son travail sur le problème de la décision de 1936-37, il ne faut pas oublier qu'il y définit la calculabilité à partir de l'analyse de tables numériques. Pendant son séjour à Princeton, en 1937, comme en témoigne le physicien canadien qui lui a ouvert les portes de l'atelier de physique, Turing était alors préoccupé par les menaces de guerre et par les questions de chiffrement tel qu'il les imaginait à cette époque, et envisageait d'associer ainsi un message et une clé écrite en base 2. Il réalise pour ce faire un multiplicateur électrique binaire, construisant lui-même les commutateurs à relais qu'il ne trouve pas dans le commerce (Hodges, 198, p. 123-126)[20]. A son retour, il envisage aussi le recours à une machine pour tester l'hypothèse de Riemann relative à la fonction zêta, $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ où s est un nombre complexe, fonction qu'il a déjà abordée dans sa thèse de 1938. Il s'agissait de repérer si les zéros de cette fonction sont sur la droite $\mathrm{Re}(s) = ½$. Là où le mathématicien E. C. Titchmarsh (1899-1963), avant lui, avait eu recours au système de cartes perforées utilisé en astronomie planétaire, Turing s'inspire cette fois d'une machine analogique, le *Tide Predictor* de Liverpool (Durand-Richard, 2016) pour traduire physiquement par des combinaisons de roues dentées une sommation de logarithmes de fonctions circulaires, ou plutôt leur approximation par des fractions. Les plans sont réalisés, et les roues dentées fabriquées dès juillet 1939, mais la guerre va définitivement interrompre le projet (Turing D., 2016, p. 88-94).

À une époque où les mathématiques pures évoluaient grandement à l'écart des techniques et des applications, cet intérêt de Turing pour la conception et la construction de machines, antérieur à son engagement à Bletchley Park, est révélateur d'une démarche ouverte, toujours soucieuse des relations entre concret et abstrait. Loin d'avoir pour unique horizon les seules exigences de la logique symbolique ou d'un pur mécanisme, Turing est toujours prêt à confronter ses idées aux aléas comme aux contraintes de la réalité, et à s'aventurer sur des voies nouvelles hors de toute convention. De ce point de vue, Bletchley Park sera pour lui un lieu idéal, où l'ingéniosité a toute sa place. Le respect de la compétence l'emporte sur celui de la hiérarchie, et l'action collective y est plus essentielle que les originalités individuelles.

5.1. Description des Bombes de Turing

Une *Bombe* mesure environ 2 m de large et de haut, sur 60 cm de profondeur. Elle est composée de tambours répartis en 3 groupes de 12, simulant ainsi 12 Enigma à 3 rotors. Chaque triplet de tambours est positionné verticalement, le tambour le plus rapide étant situé en bas. Sur le modèle qui a été

[20] Nous ne suivrons pas Hodges qui considère ce multiplicateur comme la première réalisation concrète de la machine de Turing.

reconstruit au *National Museum of History of Computing* à Bletchley Park, les couleurs des tambours indiquent lesquels des 3 sont utilisés parmi les 8 mis en service par les Allemands :
Red I, Marron II, Green III, Yellow IV, Brown V, Cobalt (blue) VI, Jet (black) VII, Silver VIII.

Fig. 4. La Bombe de Turing, ici reconstruite au *National Museum of History of Computing*, Bletchley Park
Wikimedia Commons. Domaine public. Auteur : Alain Taveneaux

Chaque tambour, comme les rotors, porte un système d'entrée-sortie de 26 lettres. Les câbles qui les relient sont extérieurs à la machine, et peuvent être parcourus par le courant dans les deux sens car il n'y a pas de réflecteur. La Bombe prend 20 minutes pour parcourir les 17 576 positions possibles des rotors dans un certain ordre.

5.2. Les menus, outil d'analyse des *cribs*

Comme le répète Welchman à l'envi, les Bombes auraient été inutiles sans l'existence des *cribs* (Welchamn, 1982, p. 120). Ils vont donc prendre une importance majeure avec le développement des Bombes. Les *cribs* courts peuvent être utilisés, mais la taille optimale semblait être d'environ trente lettres. Les bulletins météo en sont une source très importante, en particulier ceux des ports de la Manche. Le même message pouvait y être traité avec des chiffres moins robustes.
La structure d'un *crib* est analysée et illustrée par un diagramme appelé *menu*, qui représente les relations numérotées entre les lettres du clair et celles du cryptogramme. Le menu est préparé par les cryptanalystes et monté sur la machine par des opératrices. Il permet de tester la cohérence logique

des relations entre les lettres du *crib* et celle du cryptogramme. Dans un *crib* tel que celui-ci, présenté par Turing dans son *Treatise on Emiga* (Copeland, 2013, p. 315) :

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
D A E D A Q O Z S I  Q  M  M  K  B  I  I  G  M  P  W  H  A  I  V
K E I N E Z U S A E  T  Z  E  Z  U  M  V  O  R  B  E  R  I  Q  T
```

où le texte clair signifie : « pas d'addition au rapport préliminaire », apparaissent des boucles (*loops* ou *closure*s) :
- entre les lettres *A* et *E*, dans les positions 2 et 5.
- entre les lettres *A*, *I* et *E*, dans les positions 5, 10 et 23,
et elles ont la lettre A en commun.

Les boucles apparaissent plus explicitement sur le menu, qui matérialise par des traits les relations entre les lettres des deux textes, en utilisant le principe de réciprocité[21] :

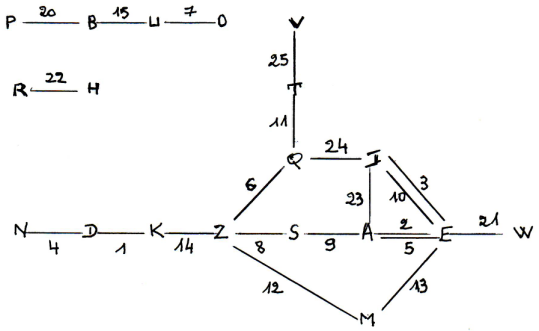

Figure 5. Menu propose par Turing dans son *Treatise on Enigma*
Reproduit de Copeland, 2013, p. 317

Turing établit que ces boucles sont indépendantes de l'appariement des lettres sur le tableau de fiches. Ce qui signifie que ce qui est observé ici entre *A* et *E* l'est aussi entre les lettres appariées s'il y en a. Le menu peut donc être utilisé pour les déterminer, car la Bombe indique les boucles qui correspondent aux lettres appariées correctes.

Dans l'annexe I de *Hut Six Story*, Welchman reconstitue un exemple plus détaillé, qu'il associe à un *crib* en anglais, et où il précise la correspondance entre les boucles, le montage de la Bombe et son fonctionnement.

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
C O N Z P V L I L  P  E  U  I  K  T  E  D  C  G  L  O  V  W  V  G  T  U  F  L  N  Z
T O T H E P R E S  I  D  E  N  T  O  F  T  H  E  U  N  I  T  E  D  S  T  A  T  E  S
```

Plusieurs enchaînements comprenant des boucles sont représentées sur le menu :
- entre *E*, *P* et *I*, en positions 5, 8 et 10,

[21] Le principe de réciprocité exprime le fait que sur la machine Enigma, si la lettre E est chiffrée par I, alors la lettre I est chiffrée par E.

- entre *I*, *P* et *V* en positions 6, 10 et 22,
- entre *N*, *T* et *O* en positions 3, 15 et 21.

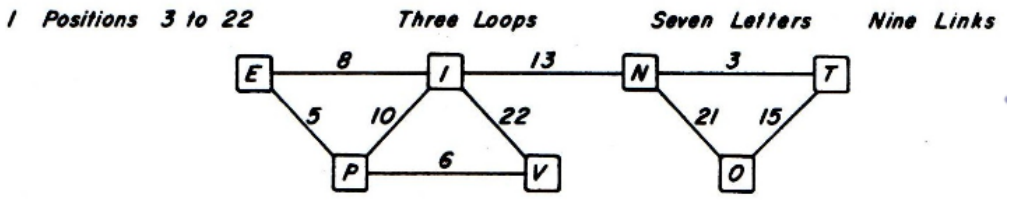

Fig. 6. Le diagramme de Welchman et son menu (Welchman, 1982 [2017], p.240)
Avec l'autorisation des éditeurs M. & M. Baldwin

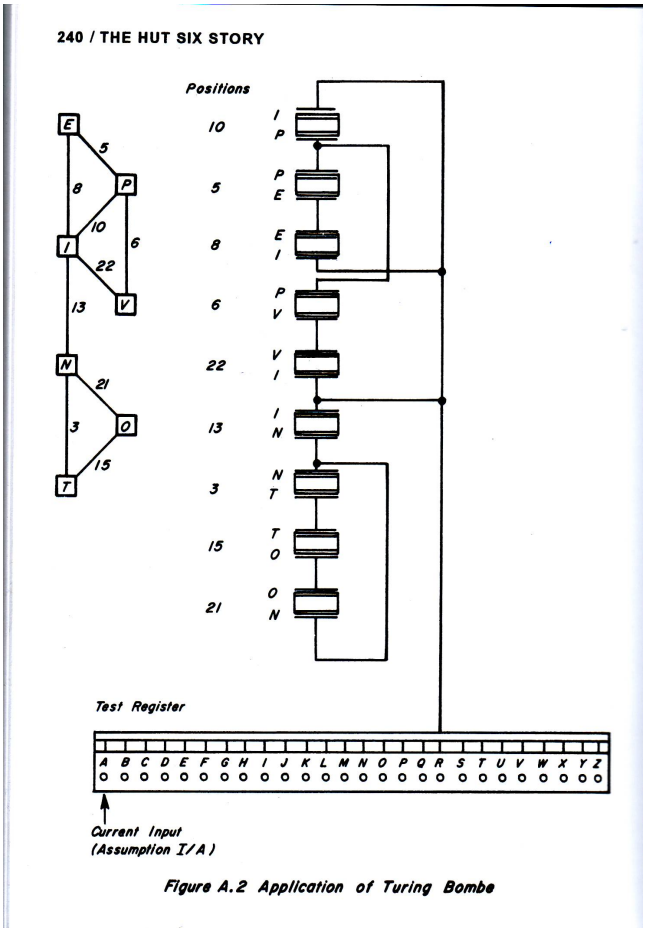

Fig. 7. Un menu et le montage associé de la Bombe (Welchman, 1982 [2017], p. 240)
Avec l'autorisation des éditeurs M. & M. Baldwin

Le montage d'une Bombe matérialise un menu. Comme le montre la fig. 7, chaque lettre de l'alphabet, en bas, est successivement testée comme lettre appariée à la lettre *I* qui est commune aux 3 boucles. La machine s'arrête à chaque fois que la configuration des tambours identifie une boucle. La course d'une Bombe permet ainsi de déterminer automatiquement la validité d'un *crib*, par une sorte de raisonnement par l'absurde : le passage ou non du courant dans la Bombe signifiant la présence ou l'absence de contradictions pour une hypothèse donnée sur les paires de lettres associées

par le tableau de fiches. Comme la *Bomba* polonaise, elle fonctionne sur le principe de l'arrêt. Chaque position correcte donnée par la machine est alors testée dans une autre *Hut*, sur une machine Enigma ou sur une machine britannique Type-X. Ce test sert également à éliminer les faux arrêts. Les Bombes étaient peu nombreuses, surtout au début, et leur utilisation soigneusement répartie entre les différentes sections. Pour éviter de perdre du temps avec un nombre excessif d'arrêts incorrects, Turing a procédé à une analyse probabiliste qui a conduit à la normalisation des *cribs*, et à adopter comme pratique standard de n'en pas utiliser de plus de quatre boucles.

La Bombe a été améliorée par l'installation d'un tableau diagonal, immédiatement conçu par Welchamn au début de 1940, avant même la livraison du premier prototype, et qui a eu un effet si marqué sur l'efficacité opérationnelle de la nouvelle Bombe que Turing l'a baptisée *The Spider* (Turing, 1940b, p. 323-331). Le tableau diagonal connectait électriquement tous les couples symétriques sur un panneau carré de 26 par 26 fiches. Cela permettait d'éviter d'avoir à utiliser de très longs *cribs* et d'utiliser moins de boucles, voire aucune. Welchman insistera beaucoup sur cette contribution, ainsi que sur le caractère collectif de ce travail (Welchamn, 1982, pp. 77-83).

Le travail des Bombes permettait d'identifier l'ordre des rotors, leur position initiale et les lettres appariées par le tableau de fiches. Le décryptement ne s'arrête pas à l'identification des clés du jour. Lorsque le *crib* est testé positivement, la Type-X reconstitue le message tout entier. Il reste à traduire le message en anglais, à en assurer la transmission aux services compétents, toutes tâches qui exigent une grande coordination entre les *Huts*.

Les Bombe*s s*eront indispensables à la bataille de l'Atlantique, surtout lorsque *la Kriegsmarine* a aura introduit une Enigma à 4 rotors en février 1942.

6. LES MÉTHODES PRATIQUES D'OPTIMISATION EN CRYPTANALYSE

L'utilisation systématique des *cribs*, et la montée en puissance des Bombes, ne suffisent pas à assurer un décryptement efficace des messages. Le travail doit être complété par des méthodes d'optimisation, fruit de l'ingéniosité des cryptanalystes, qui seront théorisées par Turing.

6.1. Le décryptement de l'Enigma navale et le *Banburismus*

Les premiers décryptements portaient surtout sur les messages de la *Luftwaffe* et de l'armée de terre. Ceux de la *Kriegsmarine* résistaient, car depuis le 1er mai 1937, pour renforcer la sécurité des communications entre les *U-boats* et l'amiral Karl Dönitz (1891-1980), elle avait introduit une procédure plus hermétique de chiffrement des indicateurs[22]. Ils étaient chiffrés deux fois, d'abord sur la machine selon la méthode classique, puis à la main, en utilisant des substitutions de bigrammes et de trigrammes, dont les tables et le calendrier étaient répertoriés dans un livre distribué régulièrement aux opérateurs, le *Kenngruppenbuch*, ou *K-book* en anglais (Copeland, 2013, p. 258). Au début de 1940 les 3 rotors sont désormais choisis parmi 8, d'où un nouveau total de 336 positions possibles [= 8x7x6] de l'ordre des rotors.

[22] Les cryptanalystes polonais avaient obtenu certains succès sur l'*Enigma* navale entre 1934 et 1937. Et le premier décryptement de Turing, en décembre 1939, concernait l'Enigma navale qui chiffrait plus simplement le réseau *Dolphin* – celui des eaux intérieures (*Home Waters*) : il portait sur 5 jours de messages interceptés en novembre 1928 (Smith, 2013, p. 27).

Quand la guerre éclate, Denniston est très pessimiste sur les possibilités de décryptement. Mais Turing s'y intéresse d'autant plus que le problème n'a pas encore été véritablement abordé. Il est bientôt rejoint par Twinn, Joan Clarke – l'éphémère fiancée de Turing – et Tony Kendrick, l'assistant de Knox. Turing va très vite assurer la direction de la *Hut* 8, entièrement dédiée au décryptement de l'Enigma navale. Alexander le secondera pour l'organisation du travail, et le remplacera au moment de son départ aux Etats-Unis en octobre 1942.

Reprenant les documents polonais, Turing découvre en quelques mois la structure de ce nouveau mode de chiffrement. Mais il montre aussi que cette découverte ne peut être exploitée sans connaître les tables de bigrammes. Des opérations militaires de la *Royal Navy* sont donc essentielles pour capturer des *K-books* et les nouveaux rotors. La première capture a lieu sur le U-33 le 12 février 1940. Les documents saisis lors de la bataille de Narvik en Norvège d'avril 1940 permettront une reconstruction partielle des tables de bigrammes et la lecture rétrospective en mai 1940 du trafic de la *Kriegsmarine*. Quelques opérations spéciales, comme celle des îles Lofoten en 1941, seront organisées pour capturer de nouveaux documents.

Aussi bien Good que Mahon ont insisté sur le rôle primordial de la méthode produite par Turing, le *Banburismus*, dans le succès de la *Hut* 8. Elle permet une identification partielle de l'ordre des rotors, et réduit considérablement le temps de travail des Bombes. Elle systématise la méthode de l'horloge[23] de Różycki. Comme les positions initiales des rotors pour les messages de la *Kriegsmarine* sont données pour la journée, il est possible que, pour une partie du message, les positions des rotors reviennent sur la position initiale d'un autre message. Dans ce cas, les parties correspondantes des deux messages sont dites « en profondeur » (*in depth*). Quand on les dispose l'une sous l'autre, le taux de répétition des lettres, qui est de 1/26 pour deux cryptogrammes quelconques, passe à 1/17 pour des messages en profondeur. Afin de les repérer plus facilement, chaque message est représenté sur une feuille de plusieurs mètres de long et de 25 cm de large, portant toutes les lettres de l'alphabet en lignes successives, avec un trou à l'emplacement de chaque lettre du message. Les deux feuilles de deux messages sont superposées au-dessus d'une lumière, qui les traverse lorsqu'une coïncidence a lieu. Esprit inventif s'il en fût, Turing avait besoin de l'organisation de Bletchley Park pour mettre en œuvre ses idées, celle-ci demandant un long et fastidieux travail de préparation et d'observation. Alexander, Good et Joan Clarke furent des experts du *Banburismus*[24], raffolant de ce « jeu intellectuel » (Mahon, 1945, pp. 20-24). Pour que la méthode soit efficace, il fallait environ 200 messages et un personnel considérable à recruter et à former. *Banburismus* commença à être utilisé en mars 1940, et n'obtint ses premiers succès qu'en novembre[25], sur un message du 8 mai 1940. L'automne 1941 marque le début de sa pleine efficacité, où environ 400 messages sont décryptés le jour même. Les informations recueillies permettent de dérouter les convois en Atlantique ; les succès allemands s'en trouveront réduits de plus de moitié (Hodges, 1988, p. 194). Ce sera la méthode fondamentale utilisée par la *Hut 8* jusqu'en septembre 1943, quand les Bombes seront assez nombreuses pour se substituer complètement à cette laborieuse méthode manuelle[26] (Mahon, 1945, p. 14, 31 et 48).

---

[23] Voir §2.

[24] L'appellation *Banburismus* provient du nom de la ville de Banbury, près d'Oxford, où les feuilles étaient fabriquées.

[25] Même les messages anciens pouvaient fournir des renseignements précieux. Ce décryptement fut l'œuvre de Hugh Foss (1902-1971), et le 8 mai désormais célébré comme le *Foss day.*

[26] Le début de l'année 1942 fut pourtant difficile, car l'amiral Dönitz introduisit un 4ème rotor, choisi parmi deux, sur l'Enigma navale, produisant un nouveau système de chiffrement baptisé *Shark.* Cette complication put être surmontée grâce à une capture, qui permit de reconstituer le câblage du 4ème rotor, et grâce à une erreur des opérateurs, qui révéla une faiblesse de son fonctionnement.

6.2. *Turingery* et le décryptement de *Tunny*

En juin 1941 parviennent à Bletchley Park des signaux interceptés qui diffèrent de ceux d'Enigma. Ils proviennent de messages transmis par télétype, chiffrés par la machine de Lorenz, qui assurent les contacts entre le Haut Commandement allemand et ses généraux, sur la liaison Berlin-Athènes/Salonique. Les messages sont plus rares, mais fournissent de précieux renseignements.

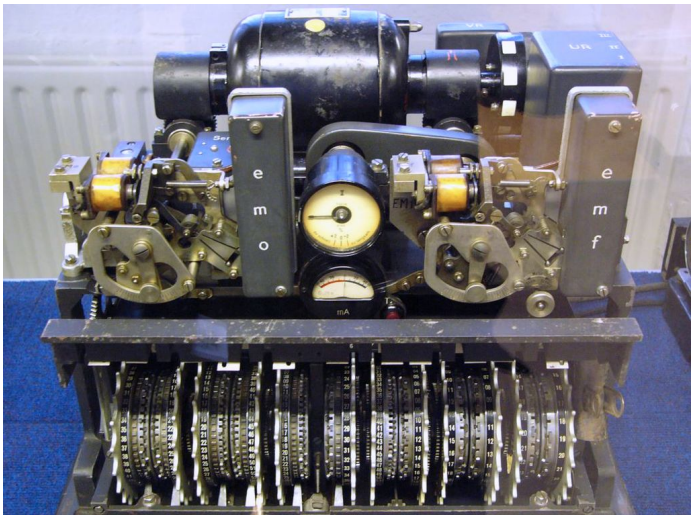

Fig. 8. La machine de Lorenz SZ42, modèle introduit en février 1943
National Museum for the History of Computing, Bletchley Park museum
Auteur Math Crypto. Wikimedia Commons. Domaine public

6.2.1. Le chiffrement des messages par la machine de Lorenz

Chaque lettre y est codée par cinq unités de base inscrites sur un ruban perforé. Les cryptanalystes de Bletchley représenteront un trou par une croix, une absence de trou par un point. Le chiffrement est automatisé. Un autre ruban, produit avec un système pseudo-aléatoire, constitue la clé. Les lettres de ce second ruban sont automatiquement associées aux lettres du premier selon les règles de Vernam (Durand-Richard, 2014, pp. 117-123), qui s'énonceront plus tard comme l'addition en base 2, si x est traduit par 1 et • par 0.

•	+	•	=	•
•	+	x	=	x
x	+	•	=	x
x	+	x	=	•

Un seul opérateur suffit. Il ne voit pas le résultat du chiffrement, qui est immédiatement transmis par le télétype. La transmission d'un indicateur du message permet à l'expéditeur et au destinataire de régler leur machine de la même façon, ce qui évite toute transmission matérielle de clé. L'application des mêmes règles permet à la machine de livrer directement le message en clair[27]. Personne à Bletchley Park n'a vu de machine de Lorenz avant la fin de la guerre. Les cryptanalystes en ont pourtant percé le fonctionnement et reproduit une machine semblable qu'ils ont appelée *Tunny*[28].

---

[27] En effet, la clé se trouve alors ajoutée deux fois, ce qui donne, modulo 2 : 1 + 1 = 0 et 0 + 0 = 0.
[28] Ils se réfèrent à l'ensemble de ces communications par le nom de *Fish*, et attribue un nom de poisson particulier à chaque liaison.

Les signes du code Baudot-Murray
Code télégraphique international

A x x • • •	B x • • x x	C • x x x •	D x • • x •
E x • • • •	F x • x x •	G • x • x x	H • • x • x
I • x x • •	J x x • x •	K x x x x •	L • x • • x
M • • x x x	N • • x x •	O • • • x x	P • x x • x
Q x x x — x	R • x • x •	S x • x • •	T • • • • x
U x x x • •	V • x x x x	W x x — — x	X x • x x x
Y x • x • x	Z x • • • x	3 • • • x •	4 • x • • •
8 x x x x x	(+)x x • x x	9 • • x • •	/ • • • • •

(3 = carriage return, 4 = line feed, 8 = letter shift, + = figure shift,
9 = space, / = null)

La génération de cette clé pseudo-aléatoire est réalisée par un système de 5 paires de roues, nommées χ et ψ à Bletchley Park, dont chacune porte un certain nombre de broches – différent de l'une à l'autre – uniformément réparties sur sa circonférence, et qui peuvent être activées ou non par l'opérateur. Les roues χ tournent d'une broche à chaque impulsion, elles produisent les lettres du message. Les roues ψ produisent les lettres de la clé, leur rotation est irrégulière, et contrôlée par 2 autres roues motrices latérales[29]. Les 12 roues agissent ensemble pour chiffrer une lettre du message. La disposition des broches selon qu'elles sont on non actives constitue le « schéma des roues », qui change tous les mois[30] à partir d'octobre 1942. Ce système permet de générer une clé très longue, évitant la répétition du même réglage sur une partie du message (Copeland, 2006, pp. 36-51).

Numéro de roue	1	2	3	4	5	6	7	8	9	10	11	12
Nom de roue BP	$\psi 1$	$\psi 2$	$\psi 3$	$\psi 4$	$\psi 5$	$\mu 1$	$\mu 2$	$\chi 1$	$\chi 2$	$\chi 3$	$\chi 4$	$\chi 5$
Nombre de cames	43	47	51	53	59	37	61	41	31	29	26	23

6.2.2. La découverte de la structure de la machine

Le 30 août 1941, un opérateur allemand commit l'erreur de transmettre deux longs messages de 3976 caractères avec le même indicateur, signalant aux cryptanalystes de Bletchley Park deux messages en profondeur. Le second était presque identique au premier, mal reçu à cause d'un brouillage. En additionnant les deux chiffrés – ce qui élimine la clé –, John Tiltman (1894-1982)[31] a pu déduire les deux textes clairs[32]. En testant un mot probable sur un des messages clairs, il a pu en déduire l'autre. Et l'addition d'un des deux textes clairs à son chiffré donnait une très grande longueur de clé (Carter, 1996, pp. 9-17).

---

[29] Si la roue motrice $\mu 1$ donne une impulsion, la roue ψ avance d'un pas. Elle reste immobile dans le cas contraire. Et la roue $\mu 1$ est contrôlée de la même façon par la roue $\mu 2$. Le mouvement des roues motrices se compliquera dans les modèles ultérieurs, faisant par exemple intervenir un autoclave, c'est-à-dire un mode de chiffrement où une partie du clair sert de clé (Copeland, 2013, p. 50).

[30] Ceux des roues motrices changent quotidiennement depuis juin 1941.

[31] Il avait servi dans l'armée indienne pendant l'entre-deux-guerres, et avait décrypté le trafic diplomatique soviétique passant entre Moscou, Kaboul et Tachkent.

[32] Voir note 27.

William Tutte (1917-2002), membre de la Section de Recherche, va analyser la succession des signes sur les caractères de cette clé. Il traite séparément chaque ligne d'impulsions, en essayant d'écrire les suites de croix et de points dans des colonnes de différentes hauteurs jusqu'à trouver des schémas récurrents. Faute d'avoir d'autres messages ayant le même indicateur, il fait aussi des essais avec des indicateurs proches. C'est en janvier 1942 qu'il découvre ainsi la structure de la machine, en particulier les paires de roues, leur nombre de broches, et leurs mouvements. C'est à ce moment-là qu'il les nomme χ et ψ.

6.2.3. Turingery *et la* Δ*-méthode*

Turing, alors détaché à la Section de Recherche, produit en juillet 1942 une méthode spécifique, la *Turingery*, ou *Turingismus*, pour trouver les schémas de roue à partir des messages en profondeur. Elle est destinée à séparer l'action des roues χ et ψ dans la production d'une lettre de la clé. Elle sera exploitée par Tutte, puis par l'équipe de Newman, sous le nom de Δ-méthode.

L'idée était la suivante : puisque les roues ψ n'avançaient pas régulièrement, la production d'un symbole (x) ou (•) avait de fortes chances d'être suivie du même symbole. De ce fait, en ajoutant une suite de lettres chiffrées à elle-même, mais en la décalant d'une position, la suite somme aurait une prédominance de (•). Ces (•) indiquent que la roue n'a pas tourné. Il faut alors tester les deux hypothèses possibles sur le symbole initial (x) ou (•). Cette procédure révélait ainsi des informations que ne donnait pas la suite initiale. Tutte calcula ensuite des statistiques sur cette méthode, afin d'apprécier dans quel cas semblable prédominance devenait significative[33]. Mais il s'agissait d'une méthode manuelle, qu'il s'avéra impossible de mettre en pratique efficacement à elle seule, en dépit d'essais concluants inspirés de *Banburismus* (Budiansly, 2006, pp. 57-59).

Armé de ces différentes méthodes, et d'autres types d'observation, un groupe intitulé la *Testery*, formé de membres de la Section de Recherche alors dirigée par le commandant Ralph Tester (1902-1998), a pu lire les messages de Tunny de juillet à octobre 1942, au moment où le réglage des roues ne sera plus indiqué en clair dans le préambule du message par une suite de 12 lettres, mais par un système de nombres communiqués aux opérateurs dans un livre appelé QED.

Fin 1942, Newman, a reçu le feu vert pour explorer l'idée de mécaniser une approche purement statistique de Tunny. La Δ-méthode, ainsi que d'autres observations sur la régularité des cryptogrammes, seront à la base de toutes ces méthodes utilisées pour trouver les réglages des roues[34]. Elles sont décrites dans le *General Report on Tunny*, écrit par Good, Donald Michie (1923-2007) et Geoffrey Timms (1903-1982) en 1945, et déclassifié en 2000. Elles seront investies sur la machine *Colossus* mise en point par l'équipe de Newman, la *Newmanry*, et réalisée sous la direction de l'ingénieur Thomas H. Flowers (1905-1998)[35], ingénieur en chef en télécommunications à la *Post Office Research Station*, qui imposera le recours à l'électronique. Turing est alors aux États-Unis et ne sera pas impliqué dans cette réalisation.

---

[33] Cette dénomination se réfère à la méthode des différences finies. La méthode fut aussi appelée *differencing.*

[34] À partir de décembre 1943, la *Newmanry* fut en charge de l'analyse des réglages des roues χ sur Colossus, et la *Testery*, manuellement, de celle des roues restantes (Copeland, 2013, p. 158).

[35] À la Libération, Churchill ordonna de détruire les 10 exemplaires réalisés de *Colossus*, 8 le furent effectivement dès 1945 les 2 derniers en 1960. Le secret fut maintenu jusqu'en 1975. Flowers coordonnera la reconstruction d'un Colossus, inauguré en 1996, et aujourd'hui exposé au *National Museum for the History of Computing* à Blechley Park.

Toutes ces méthodes relèvent en premier lieu de l'ingéniosité des cryptanalystes, sur laquelle vient s'articuler le recours aux mathématiques sans lesquelles leurs inventions ne seraient pas parvenues à leur pleine efficacité. Le travail théorique de Turing va s'enraciner sur ces pratiques, et sur sa réflexion personnelle de chercheur, pour développer de nouveaux concepts qui ouvriront un nouveau champ de recherche.

7. TURING ET L'ANALYSE BAYÉSEINNE

Outre les vulnérabilités provenant des négligences des opérateurs allemands, *Banburismus* et *Turingery* ont permis de développer une approche probabiliste que Turing va chercher à optimiser. Son travail figure dans deux textes inédits de 1940-41, mi-tapuscrits, mi-manuscrits, déclassifiés le 17 avril 2012, « *The Application of Probability to Cryptography* », et « *Paper on statistics of Repetition*s ». L'existence de ce travail a été révélée par Good en 1979. Celui-ci est aujourd'hui considéré comme le fondateur de l'analyse séquentielle, à partir des concepts bayésiens alors produits par Turing.

7.1. Le facteur de vraisemblance et sa mesure en *bans*

Esprit indépendant, Turing retravaille souvent par lui-même des résultats mathématiques déjà connus[36]. Il reprend ici le théorème de Bayes, qui établit une relation entre probabilités *a priori* et probabilités *a posteriori*. Le recours de Turing à cette approche bayésienne est alors tout à fait original, voire hérétique. Il s'écarte du courant alors orthodoxe de l'analyse fréquentiste par échantillonnage, soutenue à Cambridge par le statisticien R.A. Fisher (Turing D., 2016, p. 112 ; Zabel, 2012, p. 194). Le raisonnement bayésien est alors sujet à caution du fait que c'est à partir de l'observation d'événements partiellement connus qu'il calcule les probabilités de causes hypothétiques. C'est pourquoi les anti-bayésiens considèrent ces probabilités comme dépourvues de signification fiable. En fait, ce recours aux probabilités subjectives est ici parfaitement adapté à la pratique du cryptanalyste, qui doit déduire des clés possibles à partir d'hypothèses et de données partielles, et se livrer constamment à des approximations dont il doit évaluer la pertinence.

Le théorème de Bayes

Il s'appuie sur la commutativité de l'intersection de deux ensembles pour écrire que :

$$p(H \cap E) = p(H|E).p(E) = p(E|H).p(H)$$

où $p(H|E)$ est la probabilité de l'hypothèse H connaissant l'événement E, et $p(E|H)$ la probabilité de l'événement E connaissant l'hypothèse H.
Ce qui permet d'obtenir :

$$p(H|E) = p(H).\frac{p(E|H)}{p(E)}$$

où $p(H)$ est la probabilité *a priori* de H, indépendamment de E.
Cette probabilité $p(H|E)$ est interprétée comme une mesure de la connaissance subjective que nous percevons de *H.*

[36] Ce fut le cas déjà en 1934 lorsqu'il redémontra le théorème limite central de Gauss, qui lui ouvrit le *King's College* de Cambridge, et lui valut le *Smith Prize* en 1936, pour l'originalité de sa méthode. Il ignorait que ce théorème avait été démontré par J. W. Lindeberg en 1922 (Turing D., 2016, p. 66).

De fait, Turing travaille plutôt en termes de chance ou de pari en faveur d'un événement, qu'il définit comme le rapport $p/(1-p)$, ce qui lui permet de travailler sur les probabilités qu'un événement ait lieu dans les deux cas où l'hypothèse – qu'il appelle la théorie – est vraie ou fausse. Il établit ce qu'il appelle le « principe du facteur », qu'il appelle le « facteur de la théorie quand on prend en compte l'événement » (*factor for the theory on account of the data*), et que Good et ses successeurs appelleront le « facteur bayésien en faveur d'un événement *E* », ou « facteur de vraisemblance ». Turing écrit (Turing, 1941a, p. 4) :

Pari a posteriori de la théorie =
Pari a priori de la théorie x $\frac{\textit{Proba que l'événement ait lieu si la théorie est vraie}}{\textit{Proba que l'événement ait lieu si la théorie est fausse}}$

Turing cryptanalyste utilise des approximations qu'il justifie. Pour travailler sur des hypothèses concernant plusieurs lettres d'un message, il fait une approximation, en considérant ces hypothèses comme indépendantes. Dans ce cas, la vraisemblance totale de E vis-à-vis de l'hypothèse est le produit des vraisemblances individuelles. Et pour simplifier les calculs, Turing effectue un passage aux logarithmes – qui permettent de substituer des additions aux multiplications – et définit ainsi une mesure de la vraisemblance, qu'il appelle le *ban*[37]. De fait, il propose plutôt le *deciban*, défini en se référant au *décibel*, afin de pouvoir négliger les décimales. Good le convainc alors de travailler plutôt en demi-déciban (Good, 1984, p. 254).

Afin d'expliciter l'intérêt de son propos, Turing applique le principe du facteur à l'estimation d'hypothèses dans les attaques de différents systèmes cryptographiques. Dans le cas du chiffrement polyalphabétique de Vigenère par exemple[38], la formule devient, pour tester si *B* est la lettre de la clé qui donne le chiffré *D* :

Pari en faveur de la lettre B=
Pari a priori en faveur de B x $\frac{\textit{Proba d'obtenir D en chiffrant si la clé est B}}{\textit{Proba d'obtenir D en chiffrant si la clé n'est pas B}}$

ce qu'il évalue numériquement pour chaque lettre d'un cryptogramme donné. Mais le principe du facteur va surtout lui servir à tester la vraisemblance des *cribs*, et ainsi valider l'analyse des messages en profondeur[39], afin d'éviter un travail inutile sur des hypothèses que l'analyse révélerait peu vraisemblables. Dans ce dernier cas, une fois écrits les 2 messages l'un sous l'autre, Turing forme la « figure de répétition », formée de 0 et de X, où les X correspondent aux répétitions, et il analyse cette figure à partir du facteur de vraisemblance, en fonction de sa longueur et du nombre de X.

Cette théorisation de Turing, formalisée en termes de « vraisemblance » va ainsi être utilisée pour l'évaluation de *Banburismus* et de *Turingery* dans les recherches sur Tunny (Hodges, 1982, p. 230), ainsi que sur la *Heath Robinson*, qui précéda Colossus et nécessitait une évaluation statistique des

[37] Ce nom fait à nouveau référence à la ville de Banbury (voir note 24).
[38] Blaise de Vigenère (1523-1596) est l'auteur d'un *Traicté des Chiffres, ou Secretes Manieres d'escrire* (1586), où il définit le chiffrement polyalphabétique s'appuyant sur un mot-clé qui rend plus difficile l'attaque par analyse des fréquences. Ce chiffre ne sera décrypté qu'en 1854 par Charles Babbage (1791-1871) dans des travaux inédits, et en 1863 par F. W. Kasiski (1805-1881) dans un ouvrage publié, *Die Geheimschriften und die Dechiffrir-Kunst*. Mais les secrétaires chiffreurs lui préféreront longtemps les livres de codes plus faciles à utiliser.
[39] Turing n'utilise pas ce terme, mais dit que les messages s'accordent (*fit)*.

méthodes d'autant plus importante que ses tubes à vide tombaient souvent en panne (Hodges, 1942, p. 256).
En 1979, Good soulignera le fait que l'analyse du taux de répétition de Turing généralise les travaux de Corrado Gini (1884-1965) de 1912, et ceux de Friedman sur l'indice de coïncidence en 1920, et qu'il a lui-même appris cette notion de Turing (Good, 1979, p. 395).

7.2. Du facteur de vraisemblance à l'analyse séquentielle

Après la guerre, Good est l'un des fondateurs de l'analyse séquentielle. Invité à rejoindre Newman à l'Université de Manchester, il travaille avec Turing sur la statistique bayésienne et la conception du *Manchester Mark I*, avant d'être recruté par le *Government Communications Headquarters* GCHQ) qui a succédé à la GC&CS. Good, parti aux États-Unis en 1967, est nommé professeur de statistiques à la *Virgina Polytechnic Institute and State University*. Bon nombre de ses travaux étaient encore classifiés en 2009. Ils ont beaucoup contribué à installer l'analyse séquentielle comme discipline, et à faire basculer l'intérêt du côté de la théorie bayésienne, face aux méthodes fréquentistes encore dominantes au début des années 1990.

Lorsque le secret commence à se lever sur Bletchley Park, Good revendique les travaux de Turing comme premiers et donne une présentation historique du domaine, où il discute des apports respectifs des autres contributeurs de la discipline (Good, 1979 et 1984). Il insiste sur l'originalité du travail de Turing qui, comme à son habitude, développe ses propres idées à partir d'une recherche personnelle, sans se référer ni aux travaux de Thomas Bayes (1701-1761) – sans doute en raison de l'ostracisme dont il était l'objet à Cambridge – ni à ceux qui l'ont suivi comme ceux de Charles S. Peirce (1939-1914) en 1878, et ceux plus récents de Dorothy M. Wrinch (1814-1976) en 1921 et surtout Harold Jeffreys (1891-1989) en 1936 (Good, 1984, p. 252). Good revendique cette application à la cryptanalyse comme le premier exemple d'analyse séquentielle, et situe ses propres travaux dans le prolongement direct des travaux de Turing.

Good étend le travail de Turing à la comparaison d'hypothèses, qui deviendra cruciale dans les tests de décision. En 1979, il fait du principe du facteur un théorème fondamental : le facteur bayésien en faveur d'une évidence *H*, portant sur les paris O (*odd*) est égal au rapport des probabilités de l'événement *E*, l'une sachant *H* et l'autre sachant sa négation $\overline{H}$:

$$\frac{O(H|E)}{O(H)} = \frac{P(E|H)}{P(E|\overline{H})}$$

Le logarithme[40] de ce rapport définit alors le poids d'évidence d'une hypothèse H, fourni par E. Il le note W(H : E) et en fait le concept de base de ses analyses.

$$W(H:E) = \log \frac{P(E|H)}{P(E|\overline{H})}$$

Good en tire la définition du poids d'évidence d'une hypothèse H contre une hypothèse H', étant donné un événement E :

[40] Ce recours au logarithme, déjà utilisé par Turing pour définir le *ban*, est ici explicitement motivé par le souci de montrer que le concept de poids d'évidence est plus fondamental que celui de quantité d'information de Shannon.

$$W(H/H':E) = log\frac{P(E|H)}{P(E|H')}$$

Good estime que le concept de poids d'évidence est plus fondamental que d'autres définitions qui interviennent en théorie de la décision, et discute de la pertinence de sa terminologie par rapport à d'autres appellations possibles alors en usage dans ce nouveau champ de recherche en voie d'élaboration. Il insiste sur l'antériorité de cette « invention cryptanalytique vitale » sur les considérations d'un Karl Popper sur le degré d'acceptabilité d'une théorie (Good, 1984, p. 253). Les travaux de 1949 d'Abraham Wald (1902-1950) et de George A. Barnard (1915-2002) sont associés à cette fondation de l'analyse séquentielle, dont Good cherche à faire un outil d'analyse des théories de la connaissance, comme par exemple la théorie de l'induction.

La définition du *deciban* est doublement cruciale pour Good. D'abord, il la définit comme le plus petit changement du poids d'évidence qui soit directement perceptible à l'intuition. Il la voit comme une aide précieuse au raisonnement humain qui permettra d'améliorer efficacement les jugements des docteurs, des juristes et des autres citoyens, et conclut que « l'application principale du *deciban* est l'analyse séquentielle, non pas pour le contrôle de qualité, mais pour discriminer entre deux hypothèses, tout comme dans les essais cliniques ou les diagnostics médicaux » (Good, 1979, p. 394).

Mais surtout, le *deciban* lui permet de faire le lien avec la théorie de l'information de Shannon, élaborée elle aussi dans un contexte cryptographique pendant la Seconde Guerre Mondiale (Durand-Richard, 2014, pp. 133-142). Il insiste sur le fait que le logarithme intervient ici en base 10, parfois en base *e*, bien avant que Shannon ne définisse le *bit*. La notion de quantité d'information n'est pour lui qu'un cas particulier du poids d'évidence. En outre, Good considère ce dernier comme une notion plus intuitive et plus fondamentale que l'entropie.

CONCLUSION

La contribution de Turing sur les Bombes, tout comme celle de Newman et de son équipe sur Colossus, signe l'installation d'une relation irréversible entre cryptologie, mathématiques et mécanisation. Une telle relation existait déjà entre mathématiques et ingénierie autour de machines analogiques aussi importantes que l'analyseur différentiel. Mais la digitalisation des procédures, issue tant de la cryptologie que de l'électronique, marque en retour une recomposition des relations entre mathématiques dites pures et mathématiques appliquées, qui débouchera sur le développement des mathématiques effectives. Ni Bletchley Park, ni Turing ne sont uniques dans cette voie, comme en témoigne la démarche de Shannon qui, au même moment, mène en parallèle ses travaux sur la cryptologie et sur la théorie de l'information. Le contexte de la guerre est crucial, qui dynamise dans l'urgence ces différents types de collaboration. Turing y prend une part substantielle, et fort peu connue, qui va nourrir ses recherches ultérieures, rendant concrète son approche théorique de la mécanisation du calcul.

Le voyage de Turing aux États-Unis marque un tournant dans ses recherches, dont le parcours devient plus erratique. Parti pour coordonner la construction de nouvelles *Bombes*, il est également chargé d'analyser la sécurité des systèmes de codage de la parole, dont celui de l'importante machine SIGSALY ou Projet-X. Accueilli aux Bell Labs à partir de janvier 1943, il rédige un rapport le 4 mars sur la sécurité des équipements qu'il était chargé d'examiner, en vue d'un accord anglo-états-unien (Hodges, 1082, p. 215). Il revient en Angleterre initié à l'électronique, mais il ne retrouvera pas l'encadrement de travail de Bletchley Park. Alexander l'a remplacé à la direction de la *Hut* 8. Et c'est ailleurs, au service de sécurité radio des services secrets à Hanslope Park, qu'il élabore, avec

seulement un collaborateur, une machine de codage de la parole, la *Delilah.* Mise en service en 1945, elle est trop tardive et trop peu puissante pour servir aux communications militaires ou diplomatiques à grande échelle. La fin de la guerre voit alors Turing investi dans la construction effective de grands calculateurs automatiques à grande vitesse. Il travaille au *National Physical Laboratory* en 1945 sur un grand projet d'ACE (*Automatic Computing Engine*), dont seule une version pilote sera achevée en 1950, après son départ. Newman le recrute en 1948 pour élaborer des programmes pour le *Baby*, ou Manchester Mark I, premier calculateur digital électronique à programme enregistré en fonctionnement. Si l'histoire des ordinateurs a beaucoup été écrite à ses débuts comme s'enracinant exclusivement aux États-Unis, du fait du secret absolu qui a entouré les travaux de Bletchley Park, c'est pourtant en Angleterre que les premières machines de ce type ont été opérationnelles, du Manchester Mark I en 1948 à l'EDSAC de Cambridge en 1949.

Au sortir de la guerre, le travail de recherche n'est plus intégré à un système unique où chacun collabore à un même projet. La Grande-Bretagne ambitionne un programme nucléaire qui rend indispensable le recours à de grands calculateurs. Le reclassement des cryptanalystes fait éclater les équipes de recherche de Bletchley Park. Et plusieurs projets se trouvent en concurrence. La réalisation de ces machines automatiques à grande vitesse ne va pas sans difficultés. Elles sont liées tout autant au matériel technique à produire qu'à la conception de ces machines, axées tantôt sur la résolution de problèmes mathématiques cruciaux, tantôt sur celle d'un « cerveau électronique ». Quoi qu'il en soit, pendant et après la guerre, les interventions de Turing ne sont pas enfermées dans un travail de pure pensée. Elles manifestent le souci constant de confronter les données du problème aux élaborations théoriques, et de mobiliser tous les moyens à sa disposition, matériels aussi bien que conceptuels, pour traiter les questions abordées dans leur réalité propre.

Cette entreprise collective, sans cesse rythmée par une course contre la montre, fait passer la cryptologie et la mécanisation du calcul d'une échelle artisanale à une échelle industrielle, fortement marquée par la dimension politique de la guerre. Les technologies d'aujourd'hui héritent en grande partie de concepts et d'infrastructures mis en place dans ce contexte. Lorsqu'ils sont massivement transférés à la société civile, il y a lieu de se demander s'ils sont bien adaptés à la complexité des rapports sociaux, fondés sur bien d'autres valeurs que celles du contexte militaire.

BIBLIOGRAPHIE

Batey, M. (2009). *Dilly: The Man Who Broke Enigmas*, London, Dialogue.

Budiansky, S. (2006). « Colossus, Codebreaking and the digital Age », in Copeland, 2006, pp. 52-63.

Carter, F. (2009a). « Rodding », *Bletchley Park Trust Reports*, Bletchley Park edition, in Batey, pp. 174-188.

Carter, F. (2009b). « Buttoning up, A method for recoveiring the wiring of the rotors used in a un-Steckered Enigma », *Bletchley Park Trust Reports*, in Batey, pp. 189-205.

Carter, F. (1999). « The Turing Bombe, An Account of how the machine functioned, together with some illustrative examples » , *Report n° 16, Bletchley Park Trust Reports*, Bletchley Park edition, pp. 101-140.

Carter, F. [1996]. « Codebreaking with the Colossus Computer », *Bletchley Park Trust Reports*, Bletchley Park édition (2006).

Copeland, B. J. (2013). *The Essential Turing*, *Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life*, *O*xford, Clarendon Press, 2nd edition, 2013.

Copeland, B. J. (2006). « The German Tunny Machine », in Copeland et al., pp. 36-51.

Copeland, B. J. et al. (2006). *Colossus, the Secrets of Bletchley Park's Codebreaking Computers,* Oxford University Press.

Durand-Richard, M.-J. (2014). « Du message chiffré au système cryptographique », in Durand-Richard & Guillot, pp. 107-151.

Durand-Richard, M.-J. (2016). « De la prédiction des marées : entre calcul, observation et mécanisation (18311876) », in (dir.) Guy Boistel et Olivier Sauzereau, *Entre Ciel et Mer. Des observatoires pour l'enseignement de l'astronomie, des sciences maritimes et le service de l'heure, en France et en Europe, de la fin du XVIIIe au début du XXe siècle : institutions, pratiques et cultures, Cahiers François Viète, Série II, n°8-9.* http://www.cfv.unib-nantes.fr/146106738784400/fiche_pagelibre/&RH=1429711167616.

Durand-Richard, M.-J. (2019). « Historiographie du calcul graphique », in D. Tournès, *Histoire du calcul graphique*, Paris, Cassini, pp. 455- 530.

Durand-Richard, M.-J. et Guillot, Ph. (2014). *Cryptologie et mathématiques : une mutation des enjeux,* Paris, L'Harmattan.

Durand-Richard, M.-J. et Guillot, Ph. (2019). *From Poznań to Bletchley Park, the History of Cracking the Enigma Machine*, Nis (Serbia), Faculty of Electronic Engineering. http//\ciitlab.elfak.ni.ac.rs/kriptografija/

Friedman, W. F. (1920). *The Index of Coincidence and its Applications in Cryptography*, Riverbank Publications.

Givierge, M., (1923). « La cryptographie et les machines à cryptographier », *La science et la vie*, mars 1923, p. 223-231.

Givierge, M., (1925)., *Cours de Cryptographie,* Nancy-Paris-Strasbourg, Berger-Levrault.

Good, I. J. (1952). « Rational Decisions », Journal of the Royal Statistical Society. Series B (Methodological), Vol. 14, No. 1 (1952), pp. 107-11.

Good, I. J. (1979). « Studies in the History of Probability and Statistics. XXVII, A. M. Turing's statistical work in WWII », *Biometrica,* n° 68, 2, pp. 393-398.

Good, I. J. (1985). « Weight of Evidence : A Brief Survey », *Bayesian Statistics,* n° 2, pp. 249-270.

Good, I. J. (1983). *Good Thinking, The Foundations of Probability and its Applications,* Minneapolis, University of Minesota Press.

Good, J., Michie, D. et Timms, G. (1945),. *General Report on Tunny*, www.AlanTuring.net/tunny_report.

Guillot, Ph. (2015). « Des mathématiciens polonais à l'assaut de la machine ENIGMA », *Quadrature,* n° 98, pp. 28-38, et n° 99, pp. 20-29.

Hodges, A. (1988). *Alan Turing, ou l'énigme de l'intelligence*, Paris, Payot.

Kerckhoffs, A. (1883). « La cryptographie militaire », *Journal des Sciences Militaires*, tome 9, série 9, pp. 5-38 et p. 161-191.Paris, Imprimerie et Librairie Militaires, L. Baudouin & Co.

Mahon, A. P. (1945). *History of the Hut 8, 1939-1945*, http://www.ellsbury.com/hut8/hut8-000.htm, National Archives, Kew, Richmond, Surrey, TW9 4DU. Reference HW 25/2. Partiellement reproduit dans Copeland (2013). pp. 267-312.

Shannon, C. (1937). « A Symbolic Analysis of Relay and Switching Circuits », *Transactions of the American Institute of Electrical Engineering,* 57, pp. 713-23. Reproduit dans (eds) Sloane, N. J. & al., pp. 471-495.

Shannon, C. (1948). « A Mathematical Theory of Communication », *The Bell System Technical Journal,* vol. 27, pp. 379-423 et 623-656, july-october 1948. Reproduit dans (eds) Sloane, N. J. & al., pp. 5-82.

Shannon, C. (1949). « Communication Theory of Secrecy Systems », *The Bell System Technical Journal,* vol. 28, pp. 656-711. Reproduit dans (eds) Sloane, N. J. & al., pp. 656-711.

(eds) Sloane, N. J. A., & Wyner, Aaron D. (1993). *C. E. Shannon Collected Papers,* New York, John Wiley's & Sons.

Smith, M. (2006). « How it Began : Bletchley Park goes to War », in Copeland et al. (2006), pp. 27-35.

Turing, A. M. (1936-37). « On Computable Numbers, with an Application to the Entscheidungsprobelm », *Proceedings of the London Mathematical Society*, n° 42, pp. 230-65 et n° 43, pp. 544-46.

Turing, A. M. (1939). « Systems of Logic based on Ordinals », *Proceedings of the Loncon M.ahtematical Society*, n° 45, 1939, pp. 161-228

Turing, A. M. [1940a]. *A Treatise on Enigma,* The Turing Digital Archive, AMT/C/30. Partiellement reproduit dans Copeland (2013), pp. 313-335. http://www.turingarchive.org/browse.php/C/30.

Turing, A. M. [1940b]. Turing, Alan M., 2013, « Bombe and Spider », in Copeland (2013). pp. 313-335.

Turing, A. M. [1941a]. « The Applications of Probability to Cryptography », www.nationalarchives.gov.uk, HW 257.37.

Turing, A. M. [1941b]. « Paper on Statistics of Repetitions », www.nationalarchives.gov.uk, HW 257.38.

Turing, A. M., Welchman, G., Alexander, H., Milner-Barry, S. (1941). « Letter to Winston Churchill », in Copeland (2013). pp. 336-340.

Turing, D. (2016). *Prof, Alan Turing decoded,* London, Pitkin Publishing, Bletchley Park edition.

Welchman, G. [1982]. *The Hut Six Story, Breaking the Enigma Codes,* Kidderinster, M. & M. Baldwin, réédition 2017.

Welchman, G. (1986). « From Polish Bomb to British Bomb : the birth of Ultra », *Intelligence and National Security,* vol. 1, n°. 1. Reproduit dans *The Hut Six story,* pp. 195-234.

Zabel, S. (2012). « Commentary on Alan M. Turing : The Applications of Probability to Cryptography », *Cryptologia,* n° 36-3, pp. 191-214.