De Poznań à Bletchley Park : l'histoire du décryptement de la machine ENIGMA

Partie 2 : Bletchley Park : une usine de décryptement[1]

Marie-José Durand-Richard[2]

Traduction : Francis Bruckmann[3]

INTRODUCTION

Pendant la Seconde Guerre mondiale, les Alliés purent lire presque immédiatement la plupart des messages chiffrés allemands qu'ils interceptaient, ce qui leur procura un avantage qui eut un impact significatif sur le déroulement du conflit. Des films comme *Enigma* (1999) et *The Imitation Game* (2015) mettent en lumière le succès des travaux des Britanniques à Bletchley Park, et particulièrement de ceux du mathématicien Alan Madison Turing (1912-1954). Mais Turing n'a pas travaillé seul au décryptement d'Enigma à Bletchley Park ; et il est beaucoup moins connu que dans les années 1930, les Polonais avaient déjà accompli la prouesse de rendre transparentes les communications chiffrées entre l'armée allemande et son état-major [GUI]. Ainsi, l'histoire du décryptement d'Enigma est un peu plus compliquée que ce que montrent de tels films hagiographiques.

Dans cette perspective, cet article se concentre sur les différentes compétences à l'œuvre pour décrypter la machine Enigma. Dans la période de 1932 à 1942, les Français et les Britanniques ont donné la priorité au renseignement militaire plutôt qu'à la cryptanalyse mathématique pour surmonter le problème. Cependant, la situation politique et géographique des Polonais les a poussés à coordonner leurs efforts sur les plans à la fois technique, mathématique et politique. Cette synergie les a conduits à construire différents instruments et machines – cartes perforées, cyclomètres et *Bombas* – qui leur ont permis de surmonter les nouvelles difficultés sans cesse introduites par les armées allemandes dans leurs protocoles de chiffrement [CAR1].

Dès 1936, le cryptanalyste britannique A. Dillwyn (Dilly) Knox (1884-1943) entreprend manuellement la cryptanalyse de l'Enigma commerciale à la *Government Code and Cypher School* (GC&CS), et réussit à décrypter ses versions espagnole et italienne en 1937. La menace d'invasion par les Allemands conduit les Polonais à communiquer leurs résultats à leurs Alliés français et britanniques. Lorsque le GC&CS déménage à Bletchley Park au début de la guerre, le travail connaît un changement radical d'échelle, qui impose de déployer d'énormes moyens pour faire face à la quantité de communications de l'armée allemande engagée dans son tout nouvel art de la guerre, la *Blitzkrieg*. Bletchley Park devient une véritable usine de cryptanalyse, où les travaux

---

[1] Cet article est la traduction de la deuxième partie d'un article publié en anglais [DUR-GUI2]. La première partie, consacrée à la période polonaise de cette aventure, est relatée dans le bulletin de l'ARCSI n°42 [GUI].

[2] Maître de conférences honoraire, Université Paris 8 Vincennes-Saint-Denis. Chercheuse associée du Laboratoire SPHERE, UMR 7219 CNRS – Université Paris Cité. marie-jo.durand-richard@orange.fr

[3] Administrateur de l'ARCSI. francis.bruckmann@arcsi.fr.

de recherche sont menés collectivement, et développés tout au long de la guerre. L'analyse de tout ce trafic et les innombrables essais indispensables pour traiter le processus de décryptement auraient été impossibles sans l'aide de machines telles que les *Bombes* britanniques et états-uniennes. Cependant, ces machines auraient été inutiles, ou en tout cas inefficaces, sans à la fois un travail humain préalable et des opérations militaires.

La conception et la fabrication d'une autre machine, le Colossus, sont menées dans les dernières années de la guerre. Ce calculateur électronique, le premier au monde, est conçu pour s'attaquer à la machine de Lorenz qui chiffre les communications d'infrastructure, et non à la machine Enigma, dédiée aux communications tactiques. Colossus est produit principalement par une équipe dirigée par Maxwell Hermann Alexander – Max – Newman (1897-1984), avec l'aide de la *Post Office Research Station* à Dollis Hill. Au cours de cette période, et après son séjour aux États-Unis entre novembre 1942 et mars 1943, Turing s'intéresse davantage aux recherches sur un système avancé de sécurisation de la parole, pour le service de sécurité radio (*Radio Security Service*) des Services Secrets, situé à Hanslope Park près de Londres, en dehors de Bletchley Park. Tous ces travaux auront une grande influence sur le déroulement et la durée de la guerre, et marqueront fondamentalement l'avenir de la cryptologie.

LA CRYPTOLOGIE BRITANNIQUE DE L'ENTRE-DEUX-GUERRES

En Grande-Bretagne, le renseignement et la sécurité étaient organisés autour du GC&CS, qui deviendra en 1946 le *Government Communication Headquarters* (GCHQ). Le GC&CS réunit en 1919 deux agences de renseignement du signal (SIGINT) : la *Room 40*, fondée par l'Amirauté en 1914, et son homologue de l'Armée, le M.I.1b. Le commandant Alexander G. (Alistair) Denniston (1881-1961) en est le chef opérationnel jusqu'en 1942.

Pendant l'entre-deux-guerres, le GC&CS est transféré de l'Amirauté au ministère des Affaires Étrangères, où il est dirigé par les services secrets. Sa fonction officielle est d'assurer la sécurité des communications gouvernementales, et sa fonction secrète de lire les messages envoyés et reçus par les gouvernements étrangers. Son activité est si minime qu'elle est parfois surnommée la *Golf Club and Chess Society*. En 1935, il s'agit d'un département relativement restreint, avec un personnel de 90 personnes, dont 30 cryptologues qui s'occupent essentiellement du trafic diplomatique, et utilisent des méthodes cryptographiques classiques [KAH, pp. 95-96].

Depuis la Première Guerre mondiale, les méthodes de cryptanalyse utilisées par le GC&CS s'appuient davantage sur l'analyse du langage que sur les mathématiques. Par exemple, Knox est un érudit de Cambridge, recruté en 1914. Il a été impliqué dans le décryptement du télégramme Zimmermann en 1917, qui a conduit les États-Unis à s'engager dans la Première Guerre mondiale. Il est avant tout un spécialiste du grec ancien, et édite les textes des papyrus d'Hérodas en 1922. Il n'est féru « ni d'organisation, ni de technique », mais il est « avant tout un homme plein d'idées » [WEL1, p. 34]. En 1927, le CG&CS acquiert une machine commerciale Enigma, qui est évaluée par Hugh Foss (1902-1971, GC&CS 1924), spécialiste de japonais à Cambridge. Dans un rapport intitulé « The Reciprocal Enigma »[4], Foss établit que, malgré l'argumentaire de vente, une machine Enigma sans tableau de fiches peut être décryptée si un *crib* – qui est un texte en clair probable – peut être obtenu par d'autres moyens : « Si le câblage des rotors est connu, il suffit de quinze lettres pour trouver le réglage de la machine – c'est-à-dire les positions de départ correctes des trois rotors – mais, si le câblage des rotors est inconnu, 180 lettres au moins sont nécessaires » [BAT, p. 58].

[4] Foss nomme **«** Enigma réciproque **»** la machine équipée d'un réflecteur (*Urnkehrwalze*).

Vers 1936, les Allemands produisent la machine Enigma modèle K avec un câblage modifié. Ce modèle est fourni à différents clients en Allemagne et à l'étranger, en particulier en Italie et en Espagne. A l'issue de ses discussions avec Foss, Knox invente une méthode appelée *Rodding Method* pour trouver l'ordre et les positions des rotors. En 1937, il parvient à lire les messages chiffrés sur cette machine [BAT, p. 60-61]. Cette méthode s'appuie également sur des *cribs*. Cependant, elle ne fournit qu'une suite fragmentaire des caractères du message en clair. Il faut donc une bonne compétence linguistique pour parvenir à la découverte des parties manquantes, un peu comme dans les mots croisés. Féru de la logique du non-sens de Lewis Caroll[5], Knox excelle dans le jeu de mots, et il travaille toujours en linguiste, cherchant à découvrir les messages à partir de leur signification [BAT, p. 31-401]. Voyons brièvement le processus de *Rodding* dans l'exemple suivant [CAR2].

1. La méthode du *Rodding*

Le nom vient des *rod*s, mot qui désigne les bandes de papier sur lesquelles Knox inscrit des lettres. La méthode suppose que le câblage des rotors est connu.

Rotor positions

Contacts on the Imaginary disc	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
q	C	U	L	H	I	V	Y	R	P	S	D	M	T	K	W	G	B	J	B	F	X	N	O	Q	M	A
w	I	Q	J	O	B	X	T	Y	D	F	L	Z	P	E	H	N	K	N	G	C	M	A	W	L	S	V
e	W	K	A	N	C	Z	X	F	G	Q	U	Y	R	J	M	P	M	H	V	L	S	E	Q	D	B	O
r	P	S	M	V	U	C	G	H	W	I	X	T	K	L	Y	L	J	B	Q	D	R	W	F	N	A	E
t	D	L	B	I	V	H	J	E	O	C	Z	P	Q	X	Q	K	N	W	F	T	E	G	M	S	R	Y
z	Q	N	O	B	J	K	R	A	V	U	Y	W	C	W	P	M	E	G	Z	R	H	L	D	T	X	F
u	M	A	N	K	P	T	S	B	I	X	E	V	E	Y	L	R	H	U	T	J	Q	F	Z	C	G	W
i	S	M	P	Y	Z	D	N	O	C	R	B	R	X	Q	T	J	I	Z	K	W	G	U	V	H	E	L
o	L	Y	X	U	F	M	A	V	T	N	T	C	W	Z	K	O	U	P	E	H	I	B	J	R	Q	D
a	X	C	I	G	L	S	B	Z	M	Z	V	E	U	P	A	I	Y	R	J	O	N	K	T	W	F	Q
s	V	O	H	Q	D	N	U	L	U	B	R	I	Y	S	O	X	T	K	A	M	P	Z	E	G	W	C
d	A	J	W	F	M	I	Q	I	N	T	O	X	D	A	C	Z	P	S	L	Y	U	R	H	E	V	B
f	K	E	G	L	O	W	O	M	Z	A	C	F	S	V	U	Y	D	Q	X	I	T	J	R	B	N	S
g	R	H	Q	A	E	A	L	U	S	V	G	D	B	I	X	F	W	C	O	Z	K	T	N	M	D	P
h	J	W	S	R	S	Q	I	D	B	H	F	N	O	C	G	E	V	A	U	P	Z	M	L	F	Y	T
j	E	D	T	D	W	O	F	N	J	G	M	A	V	H	R	B	S	I	Y	U	L	Q	G	X	Z	K
k	F	Z	F	E	A	G	M	K	H	L	S	B	J	T	N	D	O	X	I	Q	W	H	C	U	P	R
p	U	G	R	S	H	L	P	J	Q	D	N	K	Z	M	F	A	C	O	W	E	J	V	I	Y	T	G
y	H	T	D	J	Q	Y	K	W	F	M	P	U	L	G	S	V	A	E	R	K	B	O	X	Z	H	I
x	Z	F	K	W	X	P	E	G	L	Y	I	Q	H	D	B	S	R	T	P	N	A	C	U	J	O	J
c	G	P	E	C	Y	R	H	Q	X	O	W	J	F	N	D	T	Z	Y	M	S	V	I	K	A	K	U
v	Y	R	V	X	T	J	W	C	A	E	K	G	M	F	Z	U	X	L	D	B	O	P	S	P	I	H
b	T	B	C	Z	K	E	V	S	R	P	H	L	G	U	I	C	Q	F	N	A	Y	D	Y	O	J	X
n	N	V	U	P	R	B	D	T	Y	J	Q	H	I	O	V	W	G	M	S	X	F	X	A	K	C	Z
m	B	I	Y	T	N	F	Z	X	K	W	J	O	A	B	E	H	L	D	C	G	C	S	P	V	U	M
l	O	X	Z	M	G	U	C	P	E	K	A	S	N	R	J	Q	F	V	H	V	D	Y	B	I	L	N

Rod square for Rotor I

Fig. 1. Le carré du *Rodding*. [RAC2, p. 2].

La première étape consiste à analyser l'effet du rotor de droite sur les 26 premières lettres du cryptogramme. La table du *Rodding* ci-dessus, formant un carré de 26 x 26, donne toutes les correspondances possibles entre les lettres d'entrée et de sortie à travers ce rotor, pour chaque position initiale.

Le rotor de droite tourne d'un cran à chaque introduction d'une lettre. Le tableau ci-dessus indique qu'en position 10, ce rotor relie la lettre *C* à la lettre *t*, et en position 15, la lettre *Z*

[5] L'historien Frank Birch – plus tard chef de la section navale – a écrit une pièce humoristique sur la *Room* 40, *Alice in ID 25*, avec des poèmes de Knox. Elle a été joué par les cryptanalystes à la fin de la Première Guerre mondiale [BAT p. 31].

à la lettre *v.* Dans toutes les diagonales du haut droit au bas gauche, les lettres suivent l'ordre des lettres QWERTZU du clavier allemand de la machine Enigma modèle K. Un jeu de 26 *rods* est constitué à partir des 26 colonnes de ce tableau. En fait, trois ensembles sont nécessaires, un pour chaque rotor, avec des couleurs différentes pour les distinguer.

Supposons qu'on sache que la lettre *V* d'un message chiffré représente la lettre *T* du message en clair, et que cette correspondance se produise lorsque le rotor de droite est dans sa 6ème position. Alors, en raison du principe de réciprocité [GUI, p. 83], les deux bornes *q* et *u* doivent être électriquement connectées par la partie restante de la machine – les deux autres rotors et le réflecteur. Et leurs *rods* correspondants peuvent être associés.

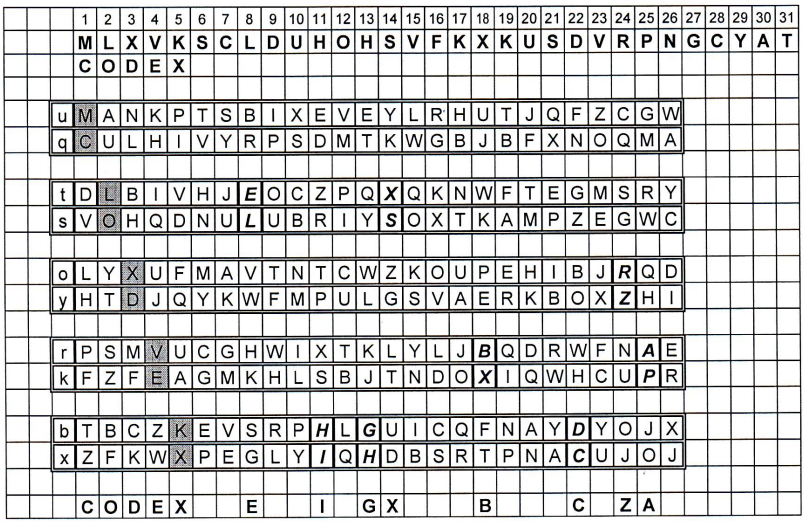
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
q	C	U	H	H	I	V	Y	R	P	S	D	M	T	K	W	G	B	J	B	F	X	N	O	Q	M	A
u	M	A	N	K	P	T	S	B	I	X	E	V	E	Y	L	R	H	U	T	J	Q	F	Z	C	G	W

Les lettres *q* et *u* sont appelées lettres de « couplage de *rods* ». L'association de ces deux *rods* donne donc d'autres lettres comparables entre le *crib* et le message chiffré. Par exemple, avec ce message chiffré :

MLXVK SCLDU HOHSV FKXKU SDVRP NGCYA T

et le *crib* de départ : 'CODEX', supposons d'abord que la bonne position de départ du rotor de droite a été déterminée en testant les 3 x 26 = 78 configurations possibles. On procède par vérification des incohérences entre leurs paires de *rods* correspondants, en utilisant le principe d'exclusivité [GUI, p. 83]. De la même façon, pour chacune des cinq premières lettres, les *rod*s qui peuvent être associés par paires**,** présentées dans le tableau ci-dessous, sont :

- celles pour *M* et *C* en position 1
- celles pour *L* et *O* en position 2,
- celles pour *X* et *D* en position 3,
- celles pour *V* et *E* en position 4,
- celles pour *K* et *X* en position 5.



Pour les lettres suivantes du cryptogramme, lorsqu'une lettre correspond à un *rod* quelconque, la lettre couplée correspondante donne une autre lettre possible pour le *crib.* Le *crib* peut ainsi être partiellement complété en bas de page, et donc aussi le texte clair fragmentaire qui en résulte, pas à pas, en devinant les lettres manquantes comme dans un jeu de mots croisés : ici CODEXBREAKING.

Dans ce processus, on suppose qu'il n'y a pas de rotation du rotor médian pour cette partie du message. Lorsqu'un tel changement de position se produit, la même procédure peut être poursuivie avec quelques complications supplémentaires.

Knox invente aussi la méthode dite du *Buttoning-up* (boutonnage) pour retrouver le câblage des rotors [CAR3]. Cette méthode permet de découvrir la première colonne de la table des *rods,* en partant de deux lettres adjacentes du message chiffré correspondant à deux lettres adjacentes du texte en clair, un cas que Knox nomme *beetle* (scarabée)[6]. Descendre depuis le *beetle* le long des diagonales QWERTZU permet de découvrir une paire de lettres « boutonnées » sur la colonne. La procédure nécessite de découvrir de nombreux *beetles*, de tester plusieurs hypothèses initiales possibles en comparant les différentes paires de lettres « boutonnées » et d'éliminer les hypothèses qui conduisent à des incohérences. Des diagrammes aident à analyser ces conclusions. Une fois la première colonne du tableau des *rods* découverte, le tableau entier peut être obtenu, car l'ordre des lettres de chaque diagonale est celui du clavier.

La méthode du *Rodding* et la méthode du *Buttoning-up* sont bien sûr très fastidieuses et longues. Elles sont effectuées à la main et ne permettent que de décrypter les messages un par un. Knox les présente comme une « sorte de jeu de mots que même un débutant peut faire sans savoir comment la machine fonctionne » [BAT, p. 113]. Ces méthodes ont néanmoins conduit à plusieurs réussites. Knox les utilise rapidement pour décrypter l'Enigma commerciale modifiée utilisée par les volontaires de la Légion Condor de la *Luftwaffe*, qui soutient les troupes du général Francisco Franco (1892-1975) pendant la guerre civile espagnole en 1937. Knox aide aussi l'Amirauté à décrypter les messages des quatre sous-marins que le président italien Benito Mussolini (1883-1945) a envoyés à Franco [BAT, p. 62-63]. Mais ces résultats ne sont pas communiqués aux Républicains espagnols.

Une fois les machines militaires Enigma équipées d'un tableau de fiches en 1930, Knox considère que ses méthodes peuvent encore être utilisées, même si elles nécessitent beaucoup plus de messages et beaucoup plus de temps pour être efficaces. Mais sur ce modèle militaire, la liaison entre le clavier et le rotor de droite a changé, et Knox imagine qu'elle obéit maintenant à un ordre aléatoire, mais ne le découvre pas.

Ainsi, lorsque la délégation britannique arrive à la réunion de Pyry, Knox a déjà une expérience des méthodes manuelles de décryptement sur des machines Enigma sans tableau de fiches. Mais les Britanniques n'ont pas développé le même niveau de mobilisation coordonnée que les Polonais dans les années 1930 entre le renseignement, les mathématiques et l'ingénierie. Néanmoins, les pratiques de Knox sont suffisamment efficaces pour être utilisées immédiatement sur les résultats communiqués par les Polonais dès juillet 1939.

2. L'héritage du décryptement polonais

Les cryptanalystes britanniques sont pleinement mobilisés depuis l'invitation de Gustave Bertrand (1896 - 1976) à rejoindre un conseil de guerre début novembre 1938 à Londres, où il apporte de nouveaux documents d'Asche [GUI, p. 86]. Denniston, Knox, John Tiltman (1894-1882) et Oliver Strachey (1874-1960) y assistent [BAT, p. 67]. Tiltman est un ancien officier de l'armée qui a décodé le trafic diplomatique russe avec l'Afghanistan et le Turkestan, et dirige maintenant la nouvelle section militaire. Strachey, du ministère des Affaires étrangères, est cryptographe en chef au GC&CS, et il continuera à diriger le département ISOS (*Illicit Service*

[6] Knox excelle à donner des noms spéciaux à ses procédures, depuis *crab* (crabe) ou *lobster* (homard) jusqu'à des noms spécifiques similaires utilisés lors du décryptement de l'Enigma de l' *Abwehr*. Comme on le verra plus loin, l'habitude se poursuivra dans le travail des *Huts* spécialisées.

Oliver Strachey) à Bletchley Park. Il fait partie du système *Double Cr*oss – composé d'agents doubles – que Churchill appelait le « bodyguard of lies » (le garde du corps des mensonges) [BAT, p. 153] – si important dans les préparatifs du débarquement de Normandie.

Lors de la réunion de Paris de janvier 1939 avec les Polonais [GUI, p. 90], la délégation britannique est conduite par Denniston, accompagné de trois cryptanalystes : Knox, Foss et Tiltman. Knox, alors expert sur l'Enigma commerciale, est d'abord très déçu par la présentation générale de Ciężki sur une machine qu'il connaît déjà sur le bout des doigts. Mais Knox présente ensuite sa méthode du *Rodding,* et commence ainsi à nouer une amitié durable avec le capitaine Henri Braquenié (1896-1976), le cryptologue en chef de Bertrand [BAT, p. 70]. Rejewski est impressionné par la présentation de Knox et insiste pour qu'il soit présent à la réunion de Pyry en juillet 1939. Rejewski commente :

> « Jusqu'à quel point Braquenié comprenait-il ? Je ne sais pas ; mais il ne fait aucun doute que Knox a tout saisi très rapidement, presque aussi vite que l'éclair. Il était évident que les Britanniques avaient vraiment travaillé sur Enigma. Ils n'ont donc pas eu besoin de beaucoup d'explications. C'étaient des spécialistes d'un genre différent » [WEL2, p. 217].

Knox apprend alors de Rejewski que la connexion entre le clavier et le rotor de droite n'est pas aléatoire comme il le pensait, mais relève d'une correspondance tout à fait élémentaire entre A et A, B et B et ainsi de suite. Il en est à la fois déçu et excité. Déçu car il avait rejeté cette idée comme trop simple, pourtant suggérée par une de ses jeunes assistantes – appelées les *Dilly girls* [BAT, p. 76] – et excité parce que ses méthodes redeviennent utilisables. Le *Rodding* et le *Buttoning-up* vont permettre de résoudre les cryptogrammes de l'Enigma de la marine italienne, et d'assurer la victoire de la *Royal Navy* lors de la bataille du cap Matapan[7] dans le Péloponnèse en mars 1941. Ces méthodes seront encore cruciales pour résoudre, en octobre 1941, les cryptogrammes de l'Enigma utilisée par *l'Abwehr* [BAT, p. 118-131].

La réunion de Pyry renforce donc la confiance de Knox dans ses propres résultats de 1937. Mais surtout, il observe les difficultés récurrentes rencontrées par les Polonais à chaque décision allemande de modifier la procédure de mise à la clé des messages. La méthodologie des Polonais repose en effet sur l'analyse de cet indicateur. Knox est rapidement convaincu que cette approche est trop hasardeuse. Son approche de linguiste lui fait préférer un travail sur le contenu des messages.

3. Le GC&CS recrute des mathématiciens et s'installe à Bletchley Park

Même si les Polonais n'ont rien révélé à Paris des moyens par lesquels ils ont résolu les codes d'Enigma, la réunion a alerté le GC&CS sur l'existence de menaces de plus en plus graves contre la paix. Cette conviction se trouve renforcée par *l'Anschluss*, l'annexion de l'Autriche par les Nazis le 13 mars 1938. En conséquence, le GC&CS décide de préparer des listes d'universitaires de Cambridge et d'Oxford susceptibles d'être recrutés. Deux séries de cours de cryptologie sont organisées à Londres, en septembre et à Noël 1938, réunissant une trentaine de participants, essentiellement des mathématiciens, des linguistes et des germanophones. Parmi les mathématiciens impliqués figurent Peter Twinn (1916-2004), de l'Université d'Oxford, et, pour Cambridge, W. Gordon Welchman (1906-1985), spécialiste de géométrie algébrique, John

[7] Comme les documents secrets n'avaient pas encore été déclassifiés lorsque Winterbotham a publié son livre sur Enigma, *The ULTRA Secret,* en 1974 [WIN], il y attribue à tort le succès de la résolution de l'Enigma de la *Luftewaffe* à la *Hut* 6. Il était le chef de la section de renseignement aérien du SIS, qui a supervisé la mise en place de la *Hut* 3 en 1939. En raison de la stricte division du travail à Bletchley Park, il « ne connaissait que le renseignement d'ULTRA sur l'armée de l'air allemande, et rien sur les Italiens » [BAT, p. 128].

Jeffreys (1916-1941), et Alan Turing (1912-1954) qui, en juillet 1938, rentre de deux années passées au Département de Mathématiques de l'Université de Princeton (New Jersey). Turing y a terminé sa thèse de doctorat sous la direction d'Alonzo Church (1903-1995), qui travaille lui aussi sur la calculabilité effective avec une approche différente. Depuis son retour, il est en contact avec Denniston et travaille régulièrement avec Knox qui, juste après la réunion de Pyry au tout début d'août 1939 [BAT, p. 80], lui fait découvrir ses propres méthodes. Turing partage bientôt la conviction de Knox qu'il serait plus sûr de travailler sur le contenu des messages chiffrés plutôt que sur leurs indicateurs – les clés du message –, qui sont toujours menacés d'évolution par de nouveaux protocoles de mise à la clé. Leur collaboration se poursuivra même après la spécialisation des activités de GC&CS, jusqu'à la mort de Knox en 1942 [BAT, p. 81, p. 102].

L'étape majeure suivante dans l'entreprise de décryptement est le déménagement du GC&CS en grand secret à Bletchley Park le 15 août 1939. Le parc et son lac ornemental entourent un grand manoir victorien de style gothique Tudor. La station X, comme on l'a appelé pendant la guerre, est idéalement située : à 80 km au nord-ouest de Londres, à la jonction des principales liaisons routières, ferroviaires, télégraphiques et de téléscripteurs vers toutes les régions du pays, en particulier Oxford et Cambridge. Afin de fournir plus d'espace de travail, des baraques en bois, les *Huts*, sont rapidement construites dans le parc, et plus tard des bâtiments en briques, les *Blocks*, pour des activités plus spécialisées. Twinn a déjà rejoint le GC&CS en février 1939, et au début de la guerre, Turing se porte volontaire pour intégrer Bletchley Park, avec Jeffreys et Welchman.

Désormais, les mathématiciens vont jouer un rôle majeur dans l'organisation de la Station X. Ces premiers recrutements ne sont que le début d'une implication continue essentiellement issue de Cambridge. Stuart Milner-Barry (1906-1995) s'y joint en janvier 1940 et recrute Hugh Alexander (1909-1974). Ils sont connus avec Turing et Welchman comme les « quatre oncles », ou les « affreux oncles »[8]. John William Jameson Herivel (1918-2011) est également recruté par Welchman au début des années 1940, tout comme Dennis Babbage (1909-1991) et Keith Batey (1919-2010). Ce dernier épouse Mavis Lever (1921-2013), ancienne assistante germaniste de Knox, qui a joué un rôle clé dans le décryptement du code de l'Enigma[9] de l'*Abwehr*[10]. Jack Good (1916-2009), recruté en 1941, continuera à travailler avec Turing après la guerre sur la conception d'ordinateurs et les statistiques bayésiennes à l'université de Manchester. Mais des linguistes sont également recrutés, dont Patrick Mahon (1921-1972), entré en 1941, spécialiste des langues modernes à Cambridge [COP1, p. 265]. Il dirige la *Hut* 8 à partir de 1944, et en a raconté l'histoire [MAH] en 1946. William Tutte (1917-2002) est également recruté en 1941, puis Max Newman en 1943. Tous deux, avec l'ingénieur Thomas H. Flowers (1905 -1998), vont contribuer à la conception du calculateur électronique Colossus. Dans les premières années, le recrutement des scientifiques et des mathématiciens découle essentiellement de relations personnelles. Dès le printemps 1941, le recrutement est confié à C. P. Snow, de Cambridge, qui suit souvent les suggestions de Welchman [WEL2, p. 223].

Cette organisation de Bletchley Park hérite du travail effectué par les Polonais, et il est important de comprendre les similitudes et les différences entre les deux approches pour décrypter Enigma. Leur bonne entente est soulignée par Welchman en 1982 lorsqu'il affirme :

---

[8] Le 21 octobre 1941, ils écrivent directement à Churchill une lettre demandant plus de ressources pour le décryptement. Conscient de l'importance du chiffre dès la Première Guerre mondiale, le Premier Ministre répond immédiatement par l'affirmative. Le GC&CS est ensuite réorganisé et Denniston remplacé par son adjoint, le commandant Edward Travis (1888-1956), qui dirigera plus tard le GCHQ.

[9] Plus tard, elle écrira un livre très vivant sur Knox : *Dilly, the Man who broke Enigmas* [BAT].

[10] L'organisation du renseignement militaire allemand.

> « Les Polonais nous ont fait pleinement profiter de leur brillant travail sur Enigma. Quand j'en viendrai à décrire ce qui s'est passé à Bletchley Park, il deviendra évident que ces cadeaux étaient d'une immense importance pour nous lancer sur la voie qui a conduit à *Hut* 6 *Ultra* » [WEL1, p. 13].

4. La coopération entre Bletchley Park, les Polonais et le PC Bruno

L'inestimable cadeau des Polonais comprend la réplique de la machine Enigma, les informations détaillées sur le câblage des rotors et leurs méthodes de décryptement, ainsi que la *Bomba* de Rosycki et les cartes perforées de Zygalski. Il arrive à la gare Victoria le 16 août 1939 et est immédiatement transmis à Bletchley Park. Knox et Turing se mettent tout de suite au travail sur ces matériaux.

Entre le déclenchement de la guerre et l'invasion de la France, Bletchley Park et le PC Bruno travaillent en étroite collaboration. Un officier de liaison GC&CS est stationné en permanence au PC Bruno, offrant au capitaine Bertrand un service direct de téléscripteurs avec Denniston à Bletchley Park. Braquenié vient travailler avec Knox en septembre 1939 [BAT, p. 90]. Douze mille livres sont immédiatement allouées pour construire des répliques d' Enigma.

Grâce à une machine spéciale construite à cet effet, le GC&CS commence à fabriquer le jeu de 1 560 cartes perforées rendues nécessaires pour trouver la clé du jour, suite à l'introduction par les Allemands des deux rotors supplémentaires en décembre 1938 [GUI, p. 90]. Ces cartes sont achevées en janvier 1940 sous la supervision de Jeffreys. Turing fait le voyage à Paris pour rencontrer l'équipe polonaise au château de Vignolles le 17 janvier 1940 et lui apporter ces cartes. Il transmet aussi des informations sur une machine Enigma de la *Reichsmarine* capturée par les Anglais sur un sous-marin, révélant l'existence sur ces machines d'un sixième et d'un septième rotor. En sa présence, et grâce aux cartes de Jeffreys, Rejewski décode un message datant du 28 octobre 1939 [BAT, p. 99]. De retour au GC&CS, les informations cruciales que Turing a apprises au château de Vignolles lui permettent de résoudre le code d'entraînement de la *Luftewaffe*, le 29 janvier 1940 [BAT, p. 102]. Knox veille à entretenir une relation fructueuse avec le PC Bruno : le premier à avoir élaboré les clés d'un jour donné transmet immédiatement l'information à ses homologues alliés [BAT, p. 101]. La proportion de messages décryptés par chacune des deux équipes – 17 % pour le PC Bruno et 83 % pour Bletchley Park – correspond à leurs ressources respectives [KAH, p. 134]. Welchman soulignera à plusieurs reprises le caractère essentiel de la transmission et de la coopération polonaises depuis la réunion de Pyry pour conduire les premiers succès de décryptement, ce qui a notamment permis à Bletchley Park de convaincre les autorités britanniques de développer le décryptement scientifique et, ce faisant, de surmonter la crise de mai 1940 [WEL1, p. 223].

En effet, le 1er mai 1940, les messages allemands ne peuvent plus être décryptés. La position de départ des rotors n'est plus répétée dans la clé du message, ce qui rend totalement inefficaces les méthodes fondées sur l'analyse des indicateurs. Le 10 mai 1940, l'armée allemande lance une grande offensive contre la Hollande, le Luxembourg, la Belgique et la France, offensive au cours de laquelle les messages chiffrés demeurent illisibles. Une solution de fortune est trouvée à Bletchley Park par Herivel, le *Herivel tip* (voir p. 14). Elle profite d'une négligence des opérateurs allemands qui ne modifient pas toujours la position des rotors d'un jour à l'autre. A partir du 21 mai, il redevient possible de lire certains messages.

La débâcle de l'armée française et les progrès de l'offensive allemande conduisent à la signature d'un armistice entre la France et l'Allemagne le 22 juin 1940. Le PC Bruno est évacué vers Alger via Oran le 26 juin 1940. Les services de renseignement français sont rétablis clandestinement par le général Weygand (1867-1965), ministre de la Guerre du premier gouvernement de Vichy. L'équipe franco-polonaise est reconstituée en zone libre, au Château des Fouzes près d'Uzès, sous le nom de PC Cadix. Les Polonais reçoivent le nom de code *Eksposytura*

300 – position 300 – et vivent clandestinement sous de faux noms : Marian Rejewski est Pierre Ranaud, professeur de mathématiques dans un lycée de Nantes. Ce centre résout des messages allemands avec les clés fournies par Bletchley Park. Le décryptement scientifique va maintenant être entièrement assuré par les Britanniques.

BLETCHLEY PARK, LE DÉCRYPTEMENT À L'ÉCHELLE INDUSTRIELLE

Dès le déclenchement de la guerre, le GC&CS connaît un changement radical d'échelle. D'abord petite structure, elle devient une organisation de très grande envergure mêlant méthodes manuelles et mécaniques. Bletchley Park est divisé en différentes sections et unités entre lesquelles une stricte division du travail est établie afin de préserver le secret.

Même si les mathématiciens, en tant qu'individus, considèrent souvent leur travail à Bletchley Park comme un jeu, et ne cherchent pas vraiment à « savoir quoi que ce soit sur ce qui se passe en dehors de [leur] propre domaine » [WEL1 p. 58], leurs recherches s'inscrivent dans une entreprise collective soutenue par une vaste structure, qui ne cesse de croître en effectifs et en influence tout au long de la guerre.

1. La réponse de Bletchley Park à la *Blitzkrieg*

Dans son *Hut Six Story*, Welchman caractérise la *Blitzkrieg* de Hitler par sa « vitesse d'attaque, soutenue par la vitesse des communications, [qui réalise] l'un des plus grands changements révolutionnaires de l'histoire militaire » [WEL1 p.19]. La rapidité des attaques des divisions *Panzer* et des *Stukas* est soutenue par une coopération très coordonnée entre toutes les forces allemandes. Enigma joue un rôle majeur dans la coordination sécurisée des flux d'informations, notamment entre l'armée de l'air et les forces terrestres, et entre les lignes de front et l'arrière, où les véhicules de commandement sont équipés des machines portables Enigma à batterie. Cette nouvelle situation « [n'est] pas une révolution technologique », précise Welchman :

> « C'était plutôt une attitude révolutionnaire quant à ce que les communications et la technologie cryptographique existantes pouvaient apporter au fonctionnement combiné des forces terrestres très mobiles et de leur soutien aérien. C'était une question d'organisation, de formation et d'ampleur de l'effort. [.....]. Parce que les Allemands avaient fait un si bon travail, les problèmes auxquels nous étions confrontés étaient sans précédent. Jamais auparavant la signalisation radio et la cryptographie n'avaient été utilisées à une aussi grande échelle pour établir des communications sur le champ de bataille » [WEL1 p. 20].

Les travaux de cryptanalyse du Bureau polonais du Chiffre avaient déjà témoigné de l'importance d'une coopération étroite entre les services de renseignement, les mathématiciens, les ingénieurs et les opérateurs chargés de mettre en œuvre les procédures accompagnant l'utilisation des équipements. Cette coopération ne put avoir lieu que grâce à des relations personnelles au sein d'un petit département, le *Biuro Szyfrów*. Ce qui est nouveau dans l'organisation de la cryptanalyse à Bletchley Park, c'est la mise en place d'une conception systématique, voire systémique, de son organisation, qui s'incarne clairement dans sa structure matérielle.

Le manoir est réservé au personnel d'encadrement. Pendant les premières semaines à Bletchley Park, la section de recherche, l'équipe de Knox, est localisée dans le Cottage – une partie des anciennes écuries sur le côté du manoir – avec Twinn, Turing, Jeffreys et Welchman. La

vingtaine de baraque*s* en bois, les *Huts*, rapidement construites sur tout le terrain, est beaucoup moins confortable, accueillant à la fois les cryptanalystes et le personnel de plus en plus nombreux nécessaire à la préparation de leur travail. Chacune de ces *Huts* est dédiée à une activité spécifique, en grande partie à la résolution du chiffre d'Enigmas spécifiques, mais aussi à la réception des messages depuis les stations d'interception, à la traduction des messages décodés et à leur transmission aux services de renseignement et aux autorités gouvernementales.

Le premier groupe de mathématiciens recrutés se répartit progressivement sur le site pour **c**onduire des recherches spécifiques dans différentes *Huts.* Par exemple:

- la *Hut* 7 s'occupe de la section navale japonaise. Elle est dirigée par Foss avant qu'il ne se rende aux États-Unis en 1944. L'unité va ensuite s'agrandir et déménager au bloc B.
- la *Hut* 6 est d'abord dédiée au chiffre Enigma de la *Wehrmacht* et de la *Luftwaffe*. A sa tête, Welchman met en place une organisation fondée sur ses conceptions originales de l'analyse du trafic (TA), avant de devenir directeur adjoint de la mécanisation à l'automne 1943.
- la *Hut* 8 traite la machine Enigma de la Marine allemande. Elle est dirigée par Turing, puis Alexander (1942) et plus tard Mahon (1944). Ce nom est conservé lorsque les *Huts* 3, 6 et 8 déménagent au bloc D en février 1943.
- la *Hut* 3 traite les messages envoyés par l'armée de terre et l'armée de l'air allemandes. Elle prépare les messages qui sont traités par la *Hut* 6 et, une fois les messages décryptés, assure leur traduction, leur interprétation et leur expédition aux différents services de renseignement à Londres. Peter Calvocoressi (1912-2010), qui écrira *Top Secret Ultra* (1980), dirige la section *Luftewaffe* de la *Hut* 3 [CAL]. En 1939, elle est supervisée par Frederick Winterbotham (1897-1990), l'auteur de *The Ultra Secret* (1974), qui organise les Unités Spéciales de Liaison (SLU) veillant à ce que les procédures de sécurité rigoureuses soient correctement suivies [WEL1, p. 160].
- la *Hut* 4 a le même rôle pour les messages de la *Hut* 8.
- Plusieurs des *Huts*, comme la *Hut* 1 et la *Hut* 11, accueilleront les *Bombes* britanniques.

La spécialisation du travail dans les *Huts* et les *Blocks* constitue la caractéristique essentielle de la nouvelle organisation de Bletchley Park, que Knox est pourtant particulièrement réticent à appliquer. Il menace Denniston à plusieurs reprises de démissionner car il n'est plus en mesure de surveiller l'ensemble du processus de décryptement, jusqu'à sa transmission au service de renseignement. Cette nouvelle structure ne correspond pas à son approche linguistique [BAT, pp. 133-134]. Welchman est très influent dans la mise en place de ce nouveau plan de structuration du travail. Avant la construction des *Huts*, il propose tout un plan d'organisation à Denniston et à son adjoint, le commandant Edward Travis (1888-1956), couvrant toutes les activités de Bletchley Park. Il estime nécessaire de travailler 24 heures sur 24, dans cinq salles aux activités étroitement coordonnées :

> « une salle d'enregistrement (*Registration Room*) pour effectuer l'analyse du trafic des messages Enigma en continu, sur la base des registres de trafic reçus par les téléscripteurs des stations d'interception ; une salle de contrôle d'interception (*Intercept Control Room*) qui .... [aiderait] à se concentrer sur le trafic le plus précieux ; une salle des machines (*Machine Room*) traitant les aspects cryptanalytiques en étroite collaboration avec [ces deux salles] ; une salle d'empilage des cartes (*Sheet-Stacking Room*) qui serait sollicitée par la salle des machines chaque fois que le trafic d'un jour donné sur une clé particulière mériterait qu'on tentât de la casser et enfin une salle de décodage (*Decoding Room*) pour gérer les messages dont la clé avait pu être cassée » [WEL1, p. 76].

Denniston et Travis apportent leur total soutien à ce plan, tout comme les chefs des sections des *Huts* qui traitent des messages de l'armée de terre et de l'armée de l'air. Un accord officiel est conclu pour le mettre en œuvre. Cette organisation est généralisée à toutes les *Huts*, même lorsque les cartes perforées de Jeffreys ne seront plus le principal outil de décryptement.

Welchman la considère comme sa « plus grande contribution à l'effort de guerre » [WEL1, p. 77]. Il est également conscient qu'un personnel considérable est nécessaire pour exécuter ce grand nombre de tâches distinctes, de la routine d'empilement des cartes de Jeffreys au travail des experts d'Enigma [WEL1, p. 75]. L'ensemble du personnel de Bletchley Park compte plusieurs centaines de personnes en 1940. Il passe à environ 10 000 en 1945, chacun prêtant un serment de secret absolu quant à ses activités. Des jeunes femmes sont également recrutées en grand nombre [WEL1, p. 86]. La responsabilité et la confiance sont les maîtres mots du travail de tous les participants, quel que soit leur rôle, plutôt que le respect traditionnel de la hiérarchie. De ce fait, même si Turing est souvent considéré comme un chercheur excentrique, il s'adapte très bien à ce type d'organisation. Le travail est très intense, et à partir de mars 1940, est mené sans interruption, en trois quarts de 8 heures [MAH, p. 27]. Irène Young, l'une des opératrices provenant de l'Université d'Edimbourg, affirme que dans la salle de décodage, elles doivent souvent sortir à cause du niveau sonore et du rythme de travail [YOU, p. 74].

Cette division du travail est ainsi adaptée à la profusion de messages à décrypter, à la nécessité d'un décryptement rapide et aux impératifs de sécurité. Par exemple, lorsque Welchman est chargé par Knox d'analyser le trafic intercepté dans les premiers mois de son recrutement, il ne sait rien du contenu du cadeau des Polonais [WEL2, p. 196-198] et il réinvente les cartes de Jeffreys, ce qui irrite Knox parce que Welchman s'est écarté de ce qu'il était censé faire. En fait, jusqu'aux préparatifs du débarquement de Normandie, il est tout à fait « extraordinaire [de voir] à quel point chacun en savait si peu sur la situation d'ensemble », et n'en avait qu'une « vision tunnel » [WEL2, p. 223].

2. L'organisation du travail à Bletchley Park

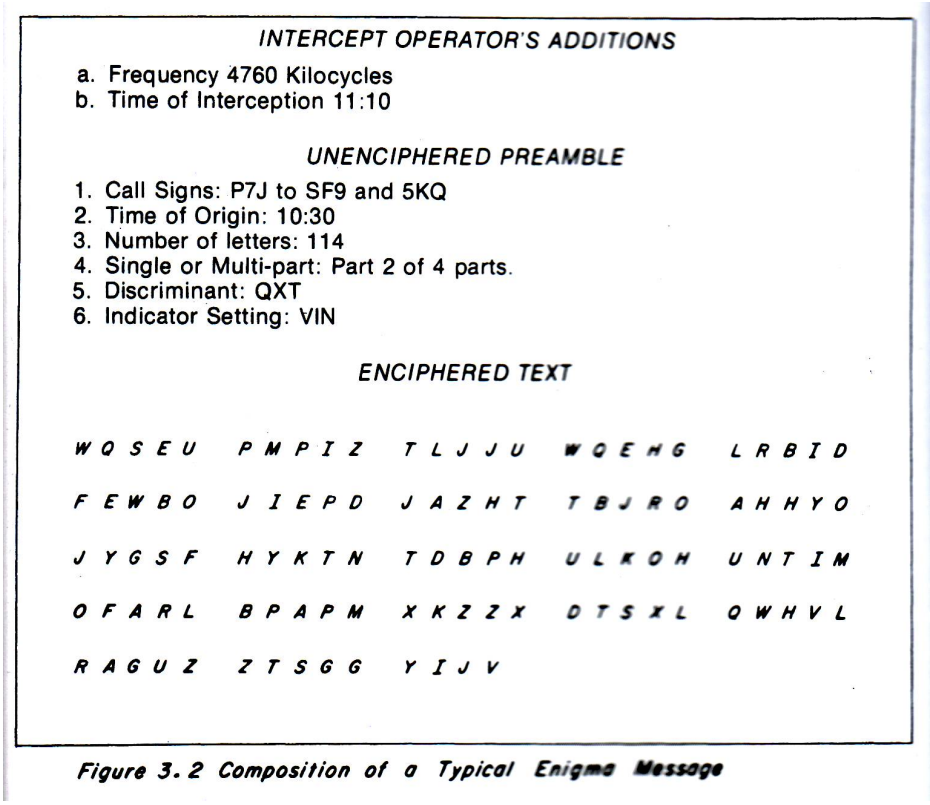
Le mode de fonctionnement de la recherche change radicalement. Dès les premiers mois à Bletchley Park, le trafic d'Enigma est analysé de manière très « méthodique ». Et Welchman souligne comment il a commencé à penser ses caractéristiques avec le même état d'esprit que dans ses propres recherches en géométrie algébrique, lorsqu'il lui fallait d'abord trouver une méthode, face « au problème consistant à saisir quelque chose sur quoi penser » [WEL1 p. 37].

Avant la mise en place de la *Hut* 6, Welchman quitte le Cottage pour s'installer à l'école voisine d'Elmer, où il « commence à analyser le trafic Enigma intercepté simplement comme du trafic – se souciant de la structure du système de communication plutôt que du contenu inconnu des messages qu'il transportait » [WEL1 p. 58]. Dès qu'il reçoit la première collecte de messages Enigma décodés – sans en connaître l'origine – il commence à comprendre que la cryptologie ne porte plus sur la question de traiter des énigmes inextricables dans des messages singuliers, mais que Bletchley Park est confronté à quelque chose de très différent. Il développe donc ce qu'il appelle « l'analyse du trafic », aujourd'hui qualifiée d'analyse des métadonnées. Il fait ainsi écho à la thèse d'Auguste Kerckhoffs (1835-1903) – auquel il fait référence – lorsqu'il envisageait les systèmes cryptographiques où les armées communiquent par télégraphe.

Comme c'est souvent le cas dans la recherche scientifique, Welchman commence à classer différentes informations, dressant des listes et des tableaux afin de trier les différentes sources des messages allemands. De nombreux éléments utiles proviennent de la station d'interception radio de l'armée à Chatham. Une étroite collaboration entre Welchman et le commandant M. J. N Ellingworth, chef de la station de Chatham, conduit à leur décision commune qu'un registre quotidien du trafic des téléscripteurs intercepté soit envoyé de Chatham à Bletchley. En analysant le préambule non chiffré des messages allemands qu'il reçoit, Welchman peut obtenir diverses indications précieuses telles que :

- les indicatifs des radios émettant et recevant les messages, car une même station envoie souvent des messages à plusieurs groupes,

- les discriminants, qui distinguent différents types de trafic Enigma, car les communications sont cloisonnées entre corps d'armée allemands,
- le réglage de l'indicateur, qui donne à l'opérateur à la réception la position de départ des trois rotors, – ici VIN (voir tableau ci-dessous) – à partir duquel le réglage du rotor – ici RCM – a été encodé deux fois, donnant les six premières lettres du message, qui est l'indicateur, ou le paramètre de message – ici WQSEUP.



INTERCEPT OPERATOR'S ADDITIONS

a. Frequency 4760 Kilocycles
b. Time of Interception 11:10

UNENCIPHERED PREAMBLE

1. Call Signs: P7J to SF9 and 5KQ
2. Time of Origin: 10:30
3. Number of letters: 114
4. Single or Multi-part: Part 2 of 4 parts.
5. Discriminant: QXT
6. Indicator Setting: VIN

ENCIPHERED TEXT

WQSEU PMPIZ TLJJU WQEHG LRBID
FEWBO JIEPD JAZHT TBJRO AHHYO
JYGSF HYKTN TDBPH ULKOH UNTIM
OFARL BPAPM XKZZX DTSXL QWHVL
RAGUZ ZTSGG YIJV

Figure 3.2 Composition of a Typical Enigma Message

Fig. 2. Un message chiffré avec Enigma et son préambule [WEL1, p. 36]
Avec l'autorisation des éditeurs M & M Baldwin.

La classification des messages à partir de ces préambules donne la structure du système allemand de chiffrement sur différentes machines Enigma. De plus, un système d'indexation est établi, par recoupement, à partir de chaque message décodé, de chaque correspondant, de chaque navire, de chaque unité, de chaque arme, de chaque terme technique, et de chaque locution stéréotypée telle que la forme de l'adresse, et de tout autre jargon militaire allemand, enregistrant ces informations sur des cartes pour faciliter l'interprétation des messages ultérieurs [WEL, p. 160]. C'est une étape indispensable pour allouer les messages aux différentes *Huts* où ils doivent être analysés et résolus. Welchman considère que :

> « Nous avions affaire à un système de communication complet qui devait répondre aux besoins des forces terrestres et aériennes allemandes. Les indicatifs d'appel prenaient vie en tant que représentants d'éléments de ces forces, dont les commandants à différents échelons devaient s'envoyer des messages. L'utilisation de différentes clés à des fins différentes, qui était connue pour être la raison des discriminants, suggérait des structures de commandement différentes pour les divers aspects des opérations militaires » [WEL1, p. 38].

Ainsi, l'analyse du trafic par Welchman résulte d'une approche consciente et systématique sur la manière de répondre à la nouvelle organisation allemande des communications secrètes.

Pour chaque message sont enregistrés : l'identifiant du réseau allemand, l'heure d'envoi du message, l'indicatif des stations émettrices et réceptrices, le discriminant et l'indicateur. Welchman a l'idée d'utiliser des couleurs pour distinguer les différents réseaux : le rouge pour le chiffrement principal de la *Luftwaffe*, le vert pour le chiffre utilisé par les districts militaires de l'armée allemande, et le bleu pour le chiffre d'entraînement de la *Luftwaffe*. Les messages correspondants peuvent donc être distribués à leurs *Huts* et *Blocks* respectifs, de sorte que des méthodes spécifiques peuvent leur être appliquées pour les décrypter [WEL1, p. 54].

Décrypter ne consiste pas uniquement à résoudre le chiffre de la machine Enigma. Une fois une suite cohérente et lisible de mots allemands obtenue par les cryptanalystes, le travail passe aux décodeurs, qui complètent la lecture grâce à la clé ; traducteurs et consultants doivent alors interpréter les abréviations et le jargon militaire. Ainsi, le succès du décryptement nécessite-t-il une coordination délicate entre toutes ces activités. À Bletchley Park comme en Pologne, le processus n'est pas toujours fluide et les messages chiffrés sont souvent décryptés des semaines, voire des mois après leur réception. Mais même dans ces cas, ils continuent à fournir des informations utiles sur l'ennemi.

MÉTHODES MANUELLES PRÉALABLES AU TRAVAIL DES MACHINES

Lorsque Turing arrive à Bletchley Park en septembre 1939, il rejoint la section de recherche et étudie les documents polonais reçus le 16 août 1939. Bien qu'il commence à concevoir les *Bombes* britanniques à l'automne 1939, les premiers prototypes ne sont construits qu'en mars 1940, et il n'y a pas suffisamment de machines avant la mi-1941 pour traiter tout le trafic allemand. Des méthodes manuelles et beaucoup de main-d'œuvre sont donc nécessaires pour commencer un décryptement et faire face au trafic. Cette situation perdure même lorsque les *Bombes* sont pleinement opérationnelles, et reste nécessaire pour ménager les *Bombes* et réduire leur temps de fonctionnement.

1. Méthodes spécifiques issues des faiblesses du chiffrement

Pour explorer les *cribs*, que ce soit manuellement ou mécaniquement, le point crucial est de réduire le grand nombre de positions des rotors à examiner. Les vulnérabilités du système cryptographique sont systématiquement analysées, donnant lieu à des méthodes spécifiques de travail sur les indicateurs.

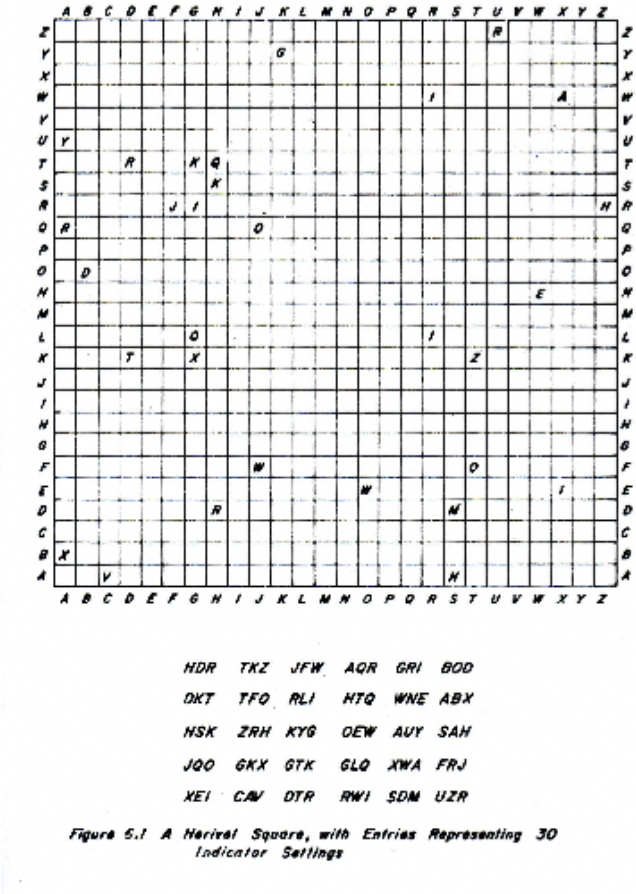
Très souvent, le manque de temps conduit les opérateurs radio allemands à commettre des négligences comme oublier de changer la clé du jour ou la clé du message, ou envoyer deux fois le même message. Il est courant que des messages de la Marine soient envoyés parallèlement avec le système de chiffrement des chantiers navals, qui est plus faible. Les cryptanalystes britanniques qualifient de *gardening* (jardinage) la collecte de telles vulnérabilités. Celles-ci reçoivent souvent des noms particuliers, comme *Cillie*s, qui désigne l'utilisation de touches faciles à deviner dans l'indicateur – par exemple AAA –, des lettres adjacentes sur le clavier – par exemple QWE ou ASD, ou des jurons courants [WEL1, p. 97-118].

1.1. Le *Herivel tip,* ou *Herivelius*

En février 1940, Herivel, recruté depuis janvier, observe que pour le premier message de la journée, les opérateurs allemands fixent parfois les réglages de bagues alors que les rotors sont déjà dans la machine [GUI, p.83**]** et utilisent simplement les lettres apparaissant à

l'ouverture de la machine pour le *Grundstellung* – position initiale des rotors – plutôt que de les choisir au hasard.

Dans ces conditions, ces lettres constituent le réglage de bagues lui-même, ou en sont très proches. Cette simple remarque devient une méthode, le *Herivel Tip* (pourboire) ou *Herivelius*, pour laquelle est créé le carré d'Herivel, afin d'affiner le nombre de trois lettres possibles pour un indicateur. La première lettre est lue horizontalement, la seconde verticalement et la troisième est écrite à l'intersection de la ligne et de la colonne correspondantes. Lorsqu'un groupe de lettres proches les unes des autres est reconnu, le nombre de réglages de bagues à tester passe de 17 576 à environ entre 6 et 30. *Herivelius* est ensuite combiné avec d'autres techniques, comme les *Cillies,* pour trouver l'ordre des rotors et les réglages du tableau de fiches [WEL1, p. 98-102].



HDR TKZ JFW AQR GRI BOD
DKT TFQ RLI HTQ WNE ABX
NSK ZRH KYG OEW AUY SAH
JQO GKX GTK GLQ XWA FRJ
XEI CAV DTR RWI SDM UZR

Figure 5.1 A Herivel Square, with Entries Representing 30 Indicator Settings

Fig. 3. Le carré d'Herivel [WEL1, p. 100]
Avec l'autorisation des éditeurs M & M Baldwin

Herivelius est conçu avant que les Nazis n'envahissent la France le 10 mai 1940, lorsque le double chiffrement des clés de message se trouve interrompu, rendant les cartes de Zygalski inutilisables. A ce moment précis, la méthode d'Herivel devient très efficace du fait de la négligence croissante des opérateurs allemands sous la pression de la situation militaire. Welchman note que Bletchley Park fut entièrement dépendant de *Herivelius* et des *Cillies* de mai 1940 au dernier *Eagle Day*, le 15 septembre 1940, qui marque la fin de la bataille d'Angleterre, lorsque Hitler renonce à ses plans d'invasion. « *Hut* 6 *Ultra* a révélé les plans de Goering pour cette journée critique et aidé la RAF à tirer le meilleur parti de ses capacités restantes » [WEL1, p. 102]. Les premiers prototypes des *Bombes* britanniques arrivent à Bletchley Park en août, mais sont encore expérimentales et bien trop peu nombreuses pour faire face à tout le trafic d'Enigma.

1.2. Les captures

La *Hut* 8 est chargée du décryptement de l'Enigma navale. En mai 1937, afin de renforcer la sécurité des communications entre les U-*boats* (sous-marins) et le commandant Karl Dönitz (1891-1980), la *Kriegsmarine* introduit une procédure plus hermétique pour chiffrer l'indicateur. En fait, les *Grundstellungs* sont fournis sur des listes de clés, et sont les mêmes pour tous les messages envoyés un jour donné. Mais les messages sont ensuite sur-chiffrés en utilisant des combinaisons de substitutions de bigrammes et de trigrammes, dont les tables sont rassemblées dans un livret, le *Kenngruppen Buch*, ou *K-book* en anglais. Même si Turing découvre la structure de ce nouveau système de chiffrement peu de temps après son arrivée à Bletchley Park, aucun travail ne peut être entrepris sans les *K-books*, qui ne peuvent être obtenus qu'à partir de la capture des *U-boats.*

Des opérations spéciales sont organisées pour dérober les *K-books* aux Allemands. Le 26 avril 1940, lors de la bataille de Narvik en Norvège, des documents sont saisis sur un patrouilleur allemand camouflé en chalutier hollandais, le Polares : des manuels d'instructions, un enregistrement de transmissions et des détails sur le système des indicateurs. Ces documents permettent une reconstitution partielle des tables de bigrammes, et des messages peuvent être analysés, certains rétrospectivement, et le dernier au moment même où la première *Bombe Victory* est installée en mars 1940 [COP1 , p. 259].

Compte tenu de la nécessité cruciale de ces tables de bigrammes et de trigrammes, de nombreux plans sont alors imaginés afin de les récupérer. La capture du *Lofoten* du 3 mars 1941 donne toutes les clés pour février, et d'autres encore, menées en juin et juillet 1941, sont une véritable aubaine, survenant juste au moment où les tables de bigrammes changent le 15 juin [MAH, p. 24-26].

1.3. *Banburismus*

Imaginer des méthodes pour accélérer la résolution du chiffrement d'Enigma conduit également à développer une approche probabiliste du problème. Lorsqu'il découvre le système d'indicateurs de l'Enigma navale, Turing invente une méthode appelée *Banburismus*, qui étend la méthode de l'horloge inventée par Różycki en Pologne dans les années 1930 [GUI, p. 87]. Ces deux méthodes sont un moyen plus efficace d'attaquer un chiffre par l'indice de coïncidence, conçu aux États-Unis par William Friedman (1891-1969) en 1920. Des cas comme celui-ci, où la même méthode ou théorie, ou une méthode similaire, est inventée indépendamment par plusieurs savants à peu près au même moment, se produisent très souvent dans l'histoire des mathématiques, et également en cryptographie.

Comme les *Grundstellungs* pour les messages de la *Kriegsmarine* sont identiques pendant une journée entière, il est possible que, pour une partie d'un message, les positions des rotors deviennent les mêmes que leurs positions de départ pour un autre message. Dans ce cas, les parties correspondantes des deux messages sont dites « en profondeur », et le taux de répétition des lettres entre les deux messages[11] est de 1/17. Afin de comparer deux messages en profondeur, chacun d'eux est perforé sur une feuille de papier aussi longue que le message, faisant parfois plusieurs mètres, et d'environ 25 cm de large.

Les lettres de l'alphabet sont écrites en colonnes successives tout le long de chaque feuille, et un trou est perforé successivement sur chaque colonne pour chaque lettre du message.

[11] Ce taux est légèrement différent de l'indice de coïncidence de la langue allemande, probablement du fait que les messages sont spécifiques au temps de guerre.

Deux feuilles sont superposées devant une lampe. La lumière les traverse en cas de lettres identiques**,** appelées *fit*, puisque les deux trous coïncident. Le nom *Banbarismus* provient de l'endroit où les feuilles sont fabriquées : Banbury, dans la région d'Oxford. Hugh Alexander, Jack Good et Joan Clarke – un moment fiancée à Turing – sont des *Banburistes* très efficaces, friands de ce « jeu intellectuel » [MAH, p. 20].

Turing décrit la méthode dans son *Treatise on Enigma*, un manuel connu sous le nom de *Prof's Book*, écrit en 1940 et regroupant les méthodes utilisées à Bletchley Park, à l'intention des nouveaux arrivants[12]. Bien qu'il soit un brillant mathématicien, il est trop brouillon, et dépourvu de sens de l'organisation pour superviser l'élaboration de la méthode [MAH, p. 24]. Environ 200 messages sont nécessaires pour la rendre efficace. Et un très important personnel doit être recruté, organisé et formé. Le *Banburismus* commence à être utilisé en mars 1940, et au début il s'avère plus difficile à employer que prévu. Il réussit d'abord sur les messages du 8 mai 1940, finalement décryptés par Hugo Foss en novembre. Par la suite, le 8 mai a été célébré comme le *Foss Day,* en reconnaissance de ce succès. L'automne 1941 marque le début de la pleine efficacité du *Banburismus*, la « période opérationnelle », traitant 400 messages quotidiens [MAH, p. 31, p. 48]. C'est « la méthodologie principale que la *Hut* 8 a utilisée » [MAH, p. 14] et ce jusqu'en septembre 1943, date à laquelle les *Bombes* sont assez nombreuses pour remplacer cette vaste entreprise manuelle collective.

2. Le rôle crucial des *cribs*

Voyant les difficultés rencontrées par les Polonais avec l'augmentation des changements d'indicateurs réalisés par les Allemands, Turing est désormais convaincu, tout comme Knox, qu'il faut s'attaquer au chiffre à partir du contenu des messages [CAR4, p. 5]. Dans cette approche, et comme c'était déjà le cas dans la méthode du *Rodding*, les *cribs* prennent de plus en plus d'importance, car ils réduisent le nombre de positions des rotors à tester, que ce soit manuellement ou mécaniquement. Ils sont absolument indispensables au fonctionnement des *Bombes,* qui seraient inutiles sans eux [WEL1, p. 120]. Ils proviennent de phrases ou de locutions allemandes stéréotypées fréquemment utilisées, souvent situées en tête ou en fin de message, comme les en-têtes hiérarchiques. Ils caractérisent également certains types de messages, comme les bulletins météorologiques. Mais ils résultent fréquemment de la négligence des opérateurs pris par l'urgence, ce que Welchman considère comme des erreurs de procédure [WEL1, p. 98]. Les *cribs* sont enregistrés de manière très systématique, afin d'optimiser leur utilisation et d'assurer une continuité maximale dans le décryptement.

Les cryptanalystes polonais avaient déjà utilisé des *cribs*, en particulier le FORTYWEEPYWEEPY. Lorsqu'un message se trouve à la suite d'un autre, il commence par FORT, l'abréviation du mot allemand *Fortsetzung* – qui signifie « suite » – et se répète quand le premier message est envoyé, encadré par la lettre Y qui sépare les mots. Pendant cette période, les chiffres sont représentés par les lettres de la rangée supérieure du clavier Q=1, W=2, etc.. Ainsi, le deuxième message envoyé à 23h30 commence par : FORTYWEEPYWEEPY. Cette méthode est particulièrement efficace lorsque le nombre de rotors et de lettres appariées (*steckered letters*[13]) est assez faible, puisque les cryptanalystes peuvent supposer assez justement que les lettres du *crib* ne sont pas affectées. Quoi qu'il en soit, cette méthode devient complètement inutile lorsqu'il est décidé d'écrire les nombres en toutes lettres [MAH, p. 14-16]. Dès que Turing et son équipe apprennent ce changement, après l'interrogatoire d'un opérateur radio allemand au début de 1940, ils reprennent d'anciens messages depuis novembre 1938 avec ces nouvelles informations

[12] Turing a écrit deux articles importants sur la théorie de cette approche probabiliste, intitulés « The Applications of Probability to Cryptography » [TUR1] et « Paper on Statistics of Repetitions » [TUR2]. Ils n'ont été remis aux Archives nationales du Royaume-Uni qu'en avril 2012.

[13] Les lettres appariées sont les paires de lettres reliées par le tableau de fiches.

sur des *cribs* qui semblaient auparavant incorrects[14]. Ils découvrent ainsi que 70% d'entre eux sont en fait corrects, ce qui leur permet de continuer à recueillir des renseignements sur les messages précédant l'introduction des 4ème et 5ème rotors [MAH, p. 1, p. 21].

Turing dresse alors un catalogue automatique avec tous les chiffrements possibles du mot *Eins* – « un » en allemand, le tétragramme le plus courant de tous les messages – pour toutes les positions possibles des rotors, avec leurs ordres et les lettres appariées possibles. Des *cribs* courts peuvent être utilisés, mais leur taille optimale est d'une trentaine de lettres. Les bulletins météorologiques sont une source très précieuse, en particulier ceux des ports de la Manche française jusqu'au printemps 1942, tout comme le rechiffrement des messages avec un chiffre plus faible. Les *cribsters* – les spécialistes des *cribs* – doivent être toujours aux aguets pour tester de nouvelles suggestions, avoir une bonne intuition pour reconnaître des messages similaires et des mots spécifiques, et leur expérience est une qualité irremplaçable [MAH, p. 44].

En 1940, les *cribs* sont fournis à la *Hut* 8 par la section navale. Cette transmission est une perte de temps et des tensions se produisent entre les deux équipes lorsque les *cribs* échouent. C'est pourquoi Milner-Barry met en place une *Cribbing room* dans la *Hut* 8, avec des *cribsters* qui savent exactement comment Enigma fonctionne, mais qui gardent néanmoins un contact étroit avec la section navale pour en recevoir des suggestions [MAH, p. 24]. Dans le même temps, le service de sécurité allemand surveille de près les éventuelles faiblesses de ses systèmes de transmission, les change régulièrement et envoie même des messages factices. Les *cribs* ne durent donc jamais très longtemps, et il faut non seulement en trouver toujours de nouveaux, mais aussi conserver tous les anciens, qui pourraient s'avérer efficaces ultérieurement avec de nouvelles combinaisons et des améliorations dans les méthodes de décryptement [MAH, p. 40].

Au-delà de toutes ces méthodes manuelles courantes, les *cribs* vont prendre une importance considérable du fait que les *Bombes* ne peuvent pas être utilisées sans eux. Ils seront présentés sous forme de schémas pour régler la machine avant sa mise en route, afin qu'elle puisse détecter s'ils sont corrects ou non. L'analyse des *cribs* va devenir le seul moyen d'attaque après l'introduction de l'Enigma à 4 rotors par la *Kriegsmarine* en février 1942.

LES *BOMBES* BRITANNIQUES

L'idée d'une machine pour aider au décryptement a déjà été envisagée par Knox, et plus encore après sa rencontre avec les cryptanalystes polonais. Turing en avait discuté avec lui [BAT, p. 95], mais la *Bombe* qu'il conçoit est très différente de la *Bomba* polonaise et introduit plusieurs innovations [CAR1, p. 4]. Elle peut en effet être utilisée pour déterminer si un *crib* est correct ou non, à partir d'hypothèses successives sur les lettres appariées. Les réglages de son circuit électrique concrétisent les relations entre les lettres du cryptogramme et le texte en clair. De ce fait, on peut dire que la machine effectue automatiquement des déductions logiques fondées sur une *reductio ad absurdum*, car elle indique si une hypothèse est juste ou fausse [HOD, p. 157-160].

1. Description de la *Bombe*

La *Bomb*e est un peu plus large que haute et mesure environ 2 m de haut sur 60 cm de profondeur. Elle est composée de rangées de douze ensembles de trois tambours rotatifs rangés l'un au dessus de l'autre avec le tambour le plus rapide en bas. Ils représentent les trois rotors

[14] La raison du choix d'une période si ancienne est que la méthode n'est plus efficace avec les deux nouveaux rotors introduits en décembre 1938.

d'une Enigma. Ainsi une *Bombe* correspond à trente-six machines. Dans celle rénovée maintenant au *National Museum of Computing* qui jouxte Bletchley Park, les tambours sont colorés pour indiquer lequel des huit rotors ils simulent : rouge I ; marron II ; vert III ; jaune IV ; brun V ; cobalt (bleu) VI ; jais (noir) VII ; argent VIII.

Fig. 4. La *Bombe* britannique, telle que reconstituée actuellement au *National Museum of Computing* de Bletchley Park.
Wikimédia Commons. Domaine public. Auteur : Alain Taveneaux.

La machine n'a pas de réflecteur et chacun des tambours porte un double système d'entrée-sortie de 26 lettres, qui peuvent être reliées entre elles de 26 manières différentes par des câbles. C'est pourquoi il y a tant de câbles à l'arrière de la machine. Le courant électrique peut les parcourir dans les deux sens. Il faut environ 20 minutes pour passer en revue toutes les 17 576 positions différentes de rotor possibles.

2. Comment la *Bombe* gère les menus

Pour former un circuit, la *Bombe* simule plusieurs Enigmas fonctionnant ensemble afin de tester des hypothèses sur les configurations possibles de la machine qui a chiffré le message. Douze sont câblées ensemble selon les instructions qui correspondent à un « menu », et 3 configurations différentes peuvent être testées ensemble pour un même menu. Celui-ci n'est autre qu'un *crib* présenté sous forme de schéma, et utilisant le principe de réciprocité du procédé de chiffrement. Ce menu est préparé par le cryptanalyste, et installé sur la machine par des

opérateurs, généralement des femmes, pour tester la cohérence des relations entre les lettres du *crib* et celles du cryptogramme [CAR4, p. 5].

Avec un *crib* comme celui ci-dessous, présenté par Turing au chapitre 6 de son *Treatise on Enigma* [TUR3, 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	H	**I**	Q	T

où le texte en clair signifie : « pas d'ajouts au rapport préliminaire », il y a ce qu'on appelle une boucle, ou une fermeture :

- entre les lettres *A* et *E*, en positions 2 et 5.
- entre les lettres *A*, *I* et *E*, avec les positions 5, 10 et 23,

et avec une lettre commune *A*.

Le menu correspondant indique la position des liens entre les lettres du message chiffré et le *crib*, et affiche les boucles. Turing établit que ces boucles sont indépendantes des valeurs appariées des lettres d'entrée et de sortie, c'est-à-dire que, ce qui est vu ici entre *A* et *E* par exemple, se produit également entre les valeurs appariées. Ainsi, le processus peut être utilisé pour les déterminer. Si la valeur appariée supposée de *A* est correcte, alors le fonctionnement de la *Bombe* fait apparaître la boucle.

Dans l'annexe I de son *Hut Six Story*, Welchman donne un exemple plus détaillé, mais avec un *crib* en anglais, où il illustre clairement la correspondance entre les boucles et le montage de la machine. Comme dans les exemples donnés pour la méthode du *Rodding,* celui-ci suppose que le rotor central ne tourne pas pendant le chiffrement du *crib*. Si cela se produit, aucune solution correcte n'est trouvée et d'autres positions doivent être testées.

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	M	Z	P	V	L	I	L	E	U	I	K	T	E	D	C	G	L	O	V	W	V	G	T	U	F	L	N	Z	P
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

L'un des trois menus extraits de ce *crib* est le suivant :

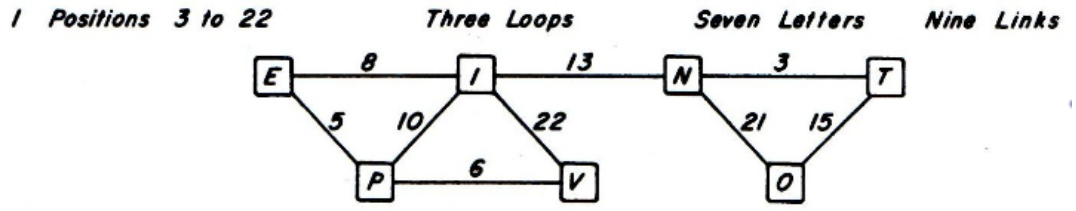


Fig. 5. Schéma de Welchman de ce menu [WEL1, p.240]
Avec l'autorisation des éditeurs M & M Baldwin

Comme on le voit sur la fig. 6, la même lettre est saisie comme valeur appariée supposée de la lettre *I* commune aux trois boucles, et chaque lettre de l'alphabet est testée successivement. La *Bombe* s'arrête chaque fois que la configuration des tambours identifie la boucle. Alors, les positions des tambours et la lettre de sortie pour chaque copie exacte sont notées.

La *Bombe* permet de tester simultanément trois configurations de rotors si l'on suppose qu'il ne faut pas plus de 12 Enigmas pour les boucles dans un *crib*. Chaque position correcte donnée par la machine pour le *crib* est ensuite testée dans une autre *Hut* sur une véritable

machine Enigma ou sur la machine de chiffrement britannique Type-X pour trouver l'intégralité du texte en clair.

L'idée de *Bombe* de Turing est vite améliorée par le tableau diagonal, conçue tout de suite par Welchman pendant la période de conception. Welchman soulignera plus tard sa propre contribution, ainsi que l'aspect collectif du travail [WEL1, p. 77-83]. Le tableau relie électriquement tous les couples symétriques sur un panneau carré de 26 par 26 fiches. Cela permet d'éviter d'avoir à utiliser de très longs *cribs*, et aussi d'utiliser moins de boucles, voire pas de boucle du tout. Ce tableau diagonal est conçu au début de 1940, avant même la livraison du premier prototype de la *Bombe*, et a un tel effet sur l'efficacité de fonctionnement que la nouvelle *Bombe* est d'abord appelée *The Spider* [TUR3, p. 323-331; CAR4, p. 16-23].

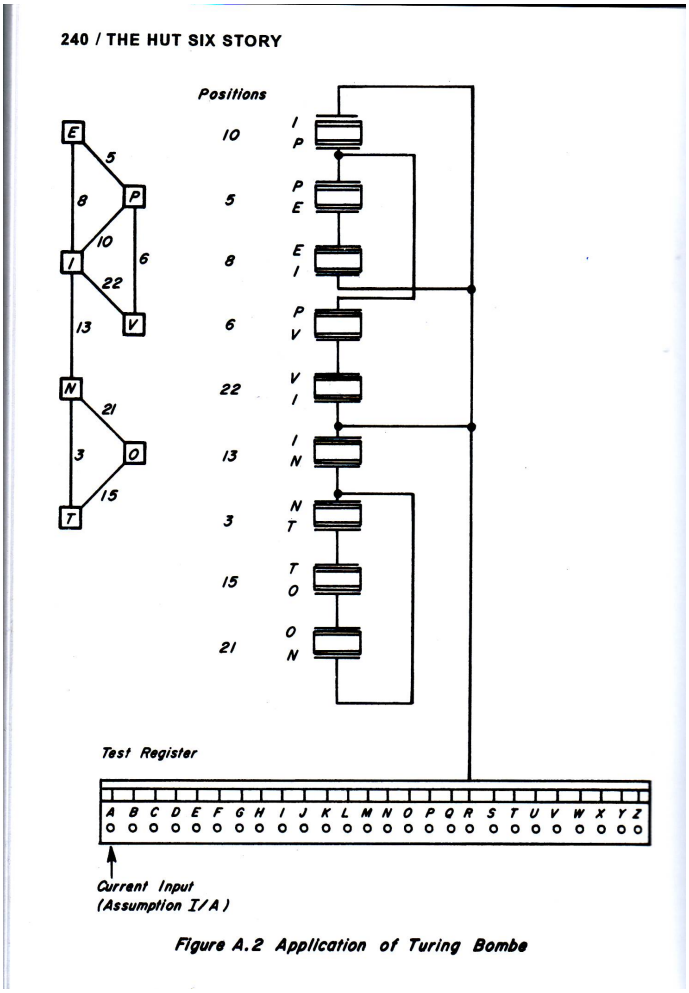


Fig. 6. Un menu de Welchman, et
le montage correspondant de la *Bombe* [WEL1, p. 240]
Avec l'autorisation des éditeurs M & M Baldwin

3. La construction des *Bombes*

Une somme de cent mille livres est affectée à la construction des *Bombes*, qui est confiée à la *British Tabulating Machinery Company* (BTM), une filiale d'IBM directement impliquée dans la mécanisation des ministères et des entreprises commerciales de l'entre-deux-guerres. La fabrication de *Bombes* pour Bletchley Park va être sa principale activité pendant la guerre. La construction est très efficacement gérée par Harold Keen, responsable de la conception et du

développement chez BTM. Il est surnommé *Doc* en raison de la sacoche de médecin dans laquelle il emporte toujours ses documents.

Le 18 mars 1940, le prototype *Victory* est installé dans la *Hu*t 1. Il est équipé par la suite d'un tableau diagonal. La forme complète de la *Bombe*, le *Spider*, est livrée le 8 août 1940 et appelée *Agnus D*ei, plus tard abrégée en *Agnes, puis Aggie.* Certains l'ont décrite comme une « déesse de bronze ». Au cours de l'année 1940, 178 messages sont lus sur les deux machines, presque tous avec succès. En juin 1941, cinq *Bombes* sont en service. À partir de la mi-1941, elles lisent chaque jour tout le trafic chiffré nazi.

Il y aura quinze *Bombes* en service en novembre 1941, vingt en septembre 1942, quarante neuf en janvier 1943, et jusqu'à 200 à la fin de la guerre. Elles seront indispensables pendant la bataille de l'Atlantique, et encore plus lorsque la *Kriegsmarine* introduira une machine Enigma à quatre rotors. Les *Bombes* sont installées sur différents sites autour de Bletchley Park pour des raisons de sécurité, et mobilisent environ 2 000 opérateurs, essentiellement les *WRENS* du *Women's Royal Naval Service*, qui travaillent sous la responsabilité d'un ingénieur de la RAF, le sergent Jones.

En 1942, environ 39 000 messages sont lus chaque mois à Bletchley Park, et ce nombre passe à environ 84 000 à la fin de 1943.

4. La résolution du chiffre ne se limite pas au travail des *Bombes*

Le travail des *Bombe*s permet aux cryptanalystes d'identifier l'ordre des rotors, leurs positions initiales et les lettres appariées par le tableau de fiches. Mais d'autres méthodes sont encore utilisées pour peaufiner le processus de décryptement, notamment pour traiter les arrêts erronés qui pouvaient être produits par les menus.

De plus, les *Bombes* sont relativement peu nombreuses, surtout au début, et leur utilisation doit être soigneusement rationnée entre les différentes sections de décryptement. Pour éviter de perdre du temps avec un nombre excessif de faux arrêts, Turing mène alors une longue analyse probabiliste – d'abord sans aide électronique – pour estimer le nombre d'arrêts de chaque ordre des rotors. L'utilisation des menus dont on estime qu'ils ne produiraient pas plus de quatre arrêts pour un rotor devient alors une pratique courante, qui conduit à normaliser la longueur des *crib*s, en fonction du nombre de leurs boucles.

LA COLLABORATION AVEC LES USA : DES *BOMBES* AU CODAGE DE LA VOIX

Avant l'entrée en guerre des États-Unis, une collaboration s'est établie avec la Grande-Bretagne pour attaquer le chiffre allemand. Denniston a rendu visite à Friedman qui le tient en haute estime [WEL2, p. 202]. Mais les Britanniques sont très prudents car il est crucial pour eux que les Nazis et leurs alliés ne devinent pas qu'Enigma est décryptée.

Des experts états-uniens sont envoyés à Bletchley Park en février 1941. Dès décembre 1941, du fait de l'intensification de la bataille de l'Atlantique, et avec l'adoption de la machine à 4 rotors par la *Kriegsmarine*, les États-Unis et le Royaume-Uni renforcent leurs relations. Les visites réciproques se multiplient : l'une de Tiltman à *l'US Navy Cryptanalysis Office* (OP-20-G) en avril 1942, et une autre de lieutenants de *l'US Navy* à Bletchley Park en juillet 1942. Un accord est signé le 2 octobre de cette année. Les Britanniques acceptent de fournir assistance et informations aux États-Unis. L'accord est limité à la construction de 100 *Bombes,* et la

coordination des travaux est laissée au GC&CS. Les *Bombes* sont construites par le *Naval Computing Machine Laboratory* de la *National Cash Register Corporation* (NCR) à Dayton, Ohio [HOD, p. 206].

Turing se rend aux États-Unis le 19 octobre 1942, où il reste jusqu'en mars 1943. Il est alors attaché à la *British Joint Staff Mission* à Washington, en raison de son expertise sur les *Bombes* et leur utilisation. Le 22 juin 1943, les deux premières machines, « Adam » et « Eve », résolvent des cryptogrammes très difficiles datés des 9 et 10 juin. En décembre 1943, 121 machines sont finalement installées [WIL, p. 18-55].

La coordination militaire entre le Royaume-Uni et les États-Unis nécessite également des communications orales entre les autorités politiques. Ces transmissions sont vulnérables à l'interception et des recherches sont rapidement menées pour chiffrer la voix. Au cours de ses six mois aux États-Unis, Turing passe beaucoup de temps aux *Bell Telephone Laboratories* et a un accès relativement libre pour étudier la sécurité des systèmes vocaux en cours de développement aux *Bell Labs,* en particulier la machine SIGSALY [*], et il rédige un rapport sur ces équipements daté du 4 mars 1943 [HOD, p. 215]. Ils sont développés dans le cadre d'un vaste système de recherche organisé en modules pour en assurer le secret.

De retour à Bletchley Park, Turing poursuit ce type de recherche pour le service de sécurité radio de Hanslope Park, qui travaille en étroite collaboration avec Bletchley Park pour développer ce nouveau type d'équipement. Il élabore la machine *Delilah* qui est un appareil numérique portable pour encoder les communications vocales, et qui, comme SIGSALY, fonctionne avec l'arithmétique modulaire et le système de chiffrement de Vernam [DUR-GUI1, p. 13-16]. Elle est opérationnelle en 1945 et Turing peut chiffrer et déchiffrer un discours enregistré par Churchill. Néanmoins, cette machine n'est pas utilisable pour les transmissions radio longue distance. Elle est achevé trop tard pour être utilisée pendant la guerre et a été rapidement oubliée.

L'ATTAQUE CONTRE LA MACHINE DE LORENZ PAR COLOSSUS

Même si les Nazis n'ont jamais soupçonné qu'Enigma avait été décryptée, ils ont systématiquement introduit de nouvelles méthodes de mise à la clé tout au long de la guerre. En juin 1941, ils commencent à chiffrer avec une nouvelle machine, la machine de Lorenz, qui est beaucoup plus sophistiquée et rapide qu'Enigma. Elle est destinée uniquement à l'usage du haut commandement nazi pour les communications militaires d'infrastructure. Les messages interceptés par les Britanniques sont au début totalement incompréhensibles, car ils ne ressemblent en rien à ceux chiffrés avec Enigma. Néanmoins, des messages chiffrés par Enigma, et décryptés, révèlent que ces messages incompréhensibles proviennent d'un système de transmission par téléscripteur sans fil appelé *Sägefisch* par les Nazis. À Bletchley Park, ces communications sont appelées *Fish* et chaque ligne de communication reçoit un nom de poisson. Par exemple, la ligne Berlin-Paris s'appelle *Jelly Fish* (méduse).

1. Chiffrement sur la machine de Lorenz

Le chiffre de la machine de Lorenz correspond au chiffre de Vernam. Il est fondé sur le code international Baudot utilisé pour les téléscripteurs. Dans ce code, chaque caractère en clair est converti en un groupe de 5 impulsions électriques produites par des roues à partir desquelles une marque ou un espace est imprimé sur une bande de papier (DUR-GUI1 pp. 14-16]. Une

[*] NdT : Voir l'article de Jon Paul paru dans le Bulletin de l'ARCSI [PAU].

marque, c'est-à-dire un trou dans la bande de papier, correspond à une impulsion. Ce qui est maintenant représenté par les symboles 1 ou 0 était alors désigné par une marque [pour 1] ou un espace [pour 0], et à Bletchley Park, par une croix [pour 1] et un point [pour 0]. Aujourd'hui, ces groupes de 5 impulsions sont représentés par des nombres de cinq chiffres binaires.

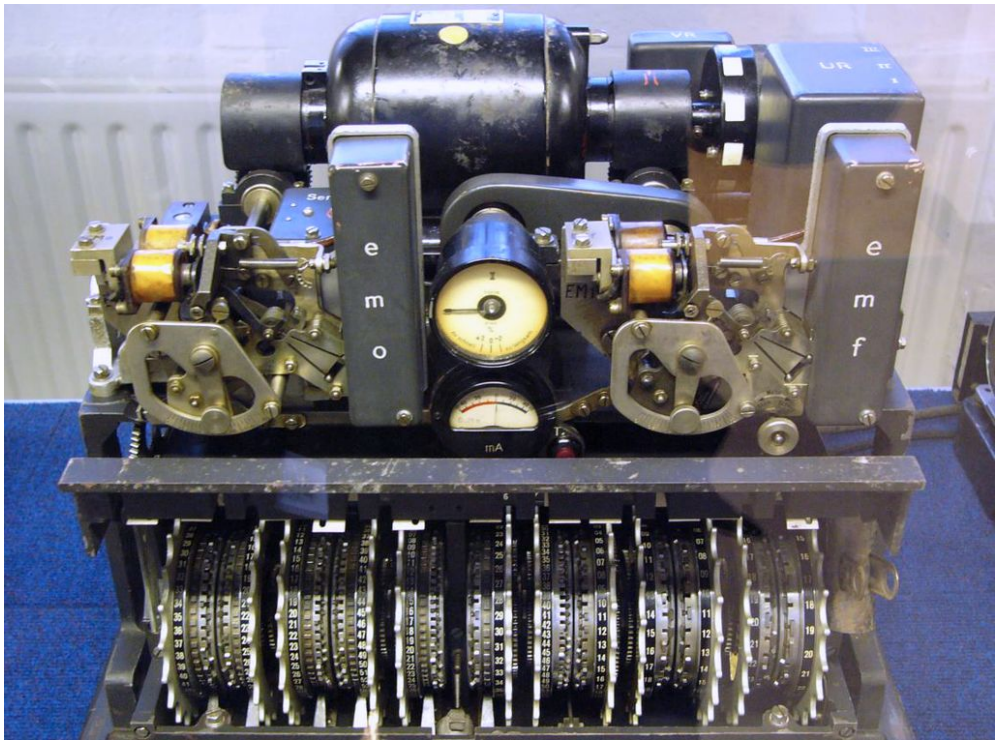


Fig. 7. La machine Lorenz SZ42 avec son couvercle retiré.
Musée de Bletchley Park. Auteur Math Crypto.
Wikimédia Commons. Domaine public.

Le système de Vernam chiffre automatiquement la séquence d'impulsions produite par le téléscripteur. Un mécanisme complexe, reposant sur divers agencements de cames sur 10 roues dentées lui permet de produire automatiquement les impulsions pseudo-aléatoires nécessaires[15]. Cette séquence chiffrante, d'une taille identique à celle du message, est ainsi générée automatiquement. La séquence chiffrante et le message sont combinés d'une manière qui est représentée aujourd'hui comme une addition modulo 2. Mais cette opération reste encore à cette époque représentée comme des règles sur des marques et des espaces, ou des croix et des points. La configuration de la machine est modifiée pour chaque message, afin de changer à chaque fois la séquence chiffrante. Mais elle n'est plus transmise sur une bande de papier [COP2, p. 36-51].

Un message commence par un préambule de 12 lettres représentées par des noms phonétiques :

A - Anton
B - Berte
C - César
D - Dora
etc.

[15] Les deux dernières roues étaient des roues motrices.

Il est rapidement supposé, et à juste titre, que chaque ensemble de ces 12 noms est un indicateur qui fournit les informations requises par les opérateurs de la station réceptrice pour régler leur machine de Lorenz à la même configuration qu'à la station émettrice [CAR5, pp. 2-9].

2. Résolution du système de Lorenz : le principe

Les cryptanalystes britanniques n'ont jamais vu de machine de Lorenz avant les derniers jours de la guerre en juin 1944. Mais ils ont réussi à en comprendre le fonctionnement et à construire une machine de simulation, appelée *Tunny.* Comme ce fut le cas pour la machine Enigma, une négligence classique des opérateurs a ouvert la voie au décryptement. En août 1941, une erreur d'exploitation dans la transmission permet d'intercepter deux longs messages, chiffrés avec le même indicateur. Ici encore, les deux messages sont dits en profondeur.

Appliquer deux fois la séquence chiffrante est une opération nulle. C'est pourquoi l'opération de chiffrement est identique à l'opération de déchiffrement. Lorsque deux caractères chiffrés sont obtenus avec le même caractère de la séquence chiffrante :

$$C_1 = P_1 + K \text{ et } C_2 = P_2 + K$$

où P_i désigne une lettre en clair et C_i la lettre correspondante du cryptogramme, l'addition de ces deux égalités modulo 2, donne : $C_1 + C_2 = P_1 + P_2$.

Il reste nécessaire de séparer les deux messages, et il n'y a pas de procédure systématique pour le faire. Cependant, si l'un des textes en clair peut être deviné par d'autres moyens, par exemple grâce à un *crib*, alors, l'autre peut en être déduit, encore une fois par addition modulo 2. Par cette méthode, John Tiltman (1894-1982) réussit à lire manuellement les deux messages, et l'équipe de recherche, dirigée par William Tutte, peut bientôt déduire la structure logique de la machine. En juillet 1942, Bletchley Park est régulièrement en mesure de lire des messages chiffrés sur la machine de Lorenz. Mais le rythme reste trop lent [CAR5, pp. 9-17].

3. Colossus

À la recherche d'une méthode pour casser le chiffre de Lorenz, Turing travaille d'abord sur la disposition de ses roues. Il conçoit une nouvelle méthode, un processus itératif connu sous le nom de *Turingery*, inspiré de *Banburismus*. Mais il est alors impossible de l'utiliser, en raison de la lenteur du travail à effectuer manuellement. Le processus pourra être appliqué sur la machine Colossus une fois construite. D'autres indications sur certaines régularités des cryptogrammes sont également testées. Mais Turing n'est pas impliqué dans la conception et la construction de Colossus, car il n'est plus à Bletchley Park à cette époque [COP2, p. 64-77].

Un premier prototype, appelé *Heath Robinson*, fonctionne à partir d'avril 1943, mais il est encore lent et rencontre de nombreuses difficultés liées à la synchronisation des bandes de papier. Colossus est développé par Newman, recruté en septembre 1942, et sa section *Newmanry,* qui travaille dans la *Hut* 11 à la recherche de moyens pour améliorer la machine initiale. Ce groupe réunit des hommes qui deviendront connus plus tard dans les domaines des mathématiques, de la cryptographie et de l'informatique, tels que Shaun Wylie (1913-2009), Jack Good (1916-2009), Donald Michie (1923-2007) et Charles E. Wynn-Williams (1903-1979). Newman est responsable de la recherche sur les méthodes mécaniques pour décrypter la machine de Lorenz. Tommy Flowers, l'ingénieur principal et chef du groupe de commutation à la *Post Office Research Station* de Dollis Hill, réunit cinquante personnes, dont dix ingénieurs. Flowers a travaillé sur des équipements de commutation automatique avant la guerre et a confiance dans les possibilités offertes par l'électronique. Il met à profit cette expertise pour la

conception de la machine, malgré quelques réticences à Bletchley Park, notamment de la part de Welchman [RAN, p. 60-65].

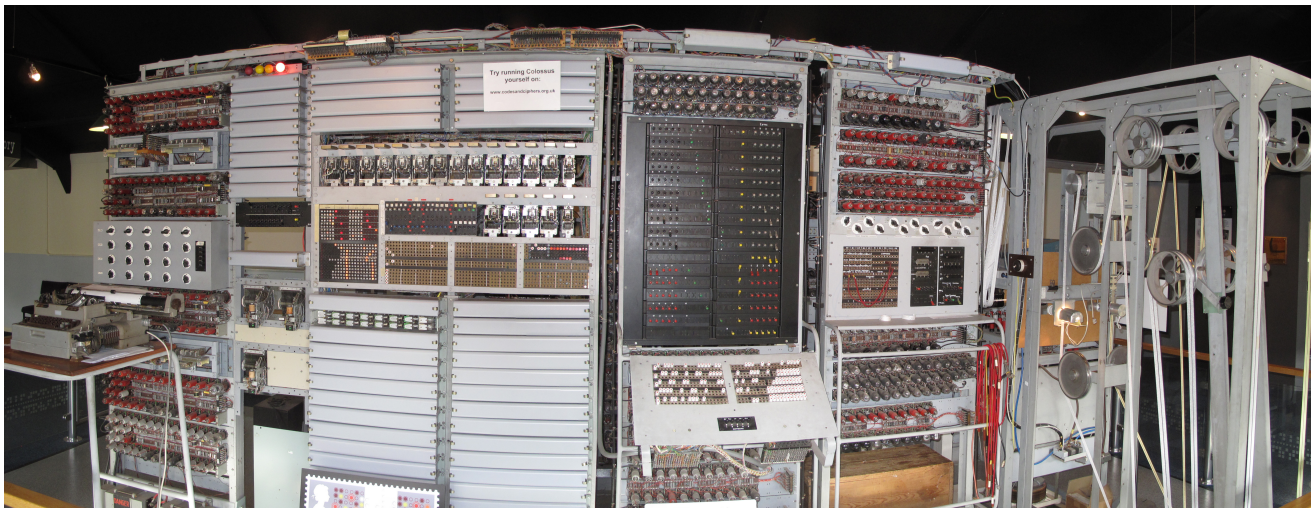


Fig. 8. Vue frontale de Colossus reconstruit au *National Museum of Computing,* Bletchley Park par Ted Coles. *Wikimédia Commons.* Domaine public.

Colossus est le premier grand calculateur électronique programmable au monde, antérieur à l'ENIAC. Construit à Londres, il est opérationnel en décembre 1943, puis déplacé à Bletchley Park en janvier 1944. Il utilise entre 1 500 et 2 400 tubes à vide, et est programmé à l'aide de prises et d'interrupteurs. Il exécute 5 000 opérations par seconde [CAR5, pp. 17-24].

A la fin de la guerre, 10 modèles opérationnels sont utilisés pour résoudre le chiffre de Lorenz. Sa conception continue à évoluer et chaque modèle diffère donc du précédent. Sa programmation est externe, mais utilise la commutation conditionnelle et le calcul sur les fonctions booléennes. La flexibilité de la nouvelle machine, du fait de son électronique, est rapidement apparue clairement à ses utilisateurs. La nature et l'importance de cette machine à Bletchley Park n'ont été révélées qu'en 2000, lorsque le gouvernement britannique a déclassifié 500 pages d'un document rédigé en 1945, « General Report on Tunny: With Emphasis on Statistical Method » [GOO]. Sur les dix machines Colossus d'origine, huit ont été détruites avec leurs plans après la guerre sur ordre de Churchill afin de garder l'opération secrète. Les deux derniers ont été détruits en 1960. Ce n'est qu'en 1975 que le secret a été partiellement levé.

Du fait de cette destruction, la machine britannique Colossus n'a pas eu le même succès, ni la même renommée que l'ENIAC aux États-Unis. Quelques plans illégalement conservés ont permis toutefois de le reconstruire en 1996, grâce à la mémoire des ingénieurs impliqués dans sa conception initiale. Et on peut voir un Colossus fonctionner aujourd'hui à Bletchley Park (Fig. 8).

CONCLUSION

Résoudre le chiffre d'Enigma a été un défi majeur pendant la Seconde Guerre mondiale. Son succès a été obtenu grâce à l'efficacité des travaux résultant de l'implication de mathématiciens et d'ingénieurs dans les pratiques de cryptanalyse militaire, fortement motivés par le contexte politique dès l'entre-deux-guerres. Certains procédés mécaniques avaient déjà été introduits en cryptologie dès les années 1930 par les Polonais. Ces améliorations se poursuivent ensuite à Bletchley Park, de manière industrielle, ce qui deviendra dès lors l'un des traits

caractéristiques de la cryptanalyse. Les méthodes de décryptement ont dû faire appel aux mathématiques et à la logique pour pallier l'augmentation considérable du nombre de combinaisons apportée par la mécanisation des procédés de chiffrement. Le succès de Bletchley Park prolonge les premiers efforts des Polonais sur les Enigmas militaires, et de l'équipe de Knox sur les machines commerciales. L'utilisation par Rejewski de la théorie des permutations, ainsi que celle par Turing des probabilités et de la logique, n'auraient pu être efficaces sans leurs *Bombes* respectives. La cryptologie est loin d'être le seul domaine où la relation entre mathématiques et ingénierie a été efficace au cours du 20ème siècle. La physique expérimentale s'est aussi beaucoup appuyée sur des machines mathématiques analogiques comme l'analyseur harmonique et l'analyseur différentiel pendant cette même période. Mais la cryptologie est ici un bel exemple où le traitement mathématique n'aurait pu être réalisé sans les performances de ces nouvelles machines.

Il est à noter que c'est le décryptement d'une autre machine à chiffrer, la machine de Lorenz, qui a conduit à la conception et à la construction d'un premier ensemble de calculateurs électroniques à programmation externe, le Colossus. Ces machines ont été détruites pour des raisons politiques après la guerre, afin que ces succès ne soient révélés ni aux ennemis, ni aux alliés de la Grande-Bretagne. Cependant, cette expérience a été investie par la suite dans d'autres projets britanniques. Après la guerre, la construction d'ordinateurs fut entreprise en Angleterre par trois groupes différents : l'un porté par Maurice V. Wilkes (1913-2010) au *Cambridge Mathematical Laboratory*, où a été construit l'EDSAC, achevé en 1949 ; un autre dirigé par Newman à Manchester, le *Manchester Mark I*, également achevé en 1949 ; et enfin celui dirigé par Turing au *National Physical Laboratory*, l'ACE, ou *Automatic Computing Engine*, dont seule une version réduite sera construite en 1950. La machine théorique conçue par Turing en 1936 ne prendra de l'importance que plus tard, lorsque les programmes deviendront des logiciels, avec le développement des langages de programmation.

Glossaire

Block	Bâtiment en brique construit dans le parc de Bletchley Park
Cillies	Séquences de touches faciles à deviner dans les indicateurs
Colossus	Premier calculateur électronique de l'histoire, développé en 1943
Crib	Mot probable du clair
Cyclomètre	Machine polonaise pour l'analyse des cycles des substitutions
Hut	Baraque en bois construite dans le parc de Bletchley Park. Chaque Hut avait un rôle particulier
Rodding method	Méthode de décryptement de l'Enigma commerciale inventée par Dilly Knox à Bletchley Park utilisant de bandes de papier appelées *rods.*

Références

[BAT] Batey, Mavis, 2009, Dilly, *The Man Who Broke Enigmas*, Londres, Dialogue.

[CAL] Calvocoressi, Peter, 1980, *Top Secret Ultra*, Londres, Littlehampton Book Service.

[CAR1] Carter, Frank, 1999, « The first Breaking of Enigma, Some of the pioneering techniques developed by the Polish Cipher Bureau », *Report n° 10, Bletchley Park Trust Reports*, Bletchley Park edition, pp. 1-35.

[CAR2] Carter, Frank, 2009, « Rodding », *Bletchley Park Trust Reports*, Bletchley Park edition, in Batey, pp. 174-188.

[CAR3] Carter, Frank, 2009, « Buttoning up, A method for recovering the wiring of the rotors used in a un-Stickered Enigma », *Bletchley Park Trust Reports*, in Batey, pp. 189-205.

[CAR4] Carter, Frank, 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. 1-40.

[CAR5] Carter, Frank,, 2008, « Codebreaking with the Colossus Computer », *Report n° 1* (2nd edition), *Bletchley Park Trust Reports*, Bletchley Park edition, pp. 1-34.

[COP1] Copeland, B. Jack, 2013, *The Essential Turing, Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life*, Oxford, Clarendon Press, 2nd edition.

[COP2] Copeland, B. Jack, 2006, *Colossus, the Secrets of Bletchley Park's Codebreaking Computers,* Oxford, Oxford University Press.

[DUR-GUI1] Durand-Richard, Marie-José et Guillot, Philippe, 2019, « How Mathematics Spread and Transformed Cryptographic Activities », *CIIT Lab Workshop on History of Cryptography*, Faculty of Electronic Engineering, Nis, Serbia. http://ciitlab.elfak.ni.ac.rs/kriptografija/ https://shs.hal.science/halshs-03949775

[DUR-GUI2] Durand-Richard, Marie-José et Guillot, Philippe, 2019, « From Poznań to Bletchley Park: The History of Cracking the ENIGMA Machine », *CIIT Lab Workshop on History of Cryptography*, Faculty of Electronic Engineering, Nis, Serbia.
http://ciitlab.elfak.ni.ac.rs/kriptografija/
https://shs.hal.science/halshs-03949790

[GOO] Good, Irving J. et Donald Michie, 1945, « General Report on Tunny with Emphasis on Statistical Methods », *UK National Archives,* www.AlanTuring.net/tunny_report.

[GUI] Guillot, Philippe, 2015, « Les mathématiciens polonais contre Enigma », *Bulletin de l'ARCSI,* n° 42, pp. 81-94.

[HOD] Hodges, Andrew, 1988, *Alan Turing, ou l'énigme de l'intelligence*, Paris, Payot.

[KAH] Kahn, David, 2012, *Seizing the Enigma, The Race to Break the German U-boats Codes 1939-1943*, Londres, Frontline Books. Revised edition.

[MAH] Mahon, A. P., 1945, *The History of Hut Eight*, http://www.ellsbury.com/hut8/hut8-000.htm, National Archives, Kew, Richmond, Surrey, TW9 4DU. Reference HW 25/2. Sa première partie se trouve également dans [COP1], pp. 267-312.

[PAU] Paul, Jon, 2017, « Le système de communication ultra-sécurisé SIGSALY à l'origine de notre monde numérique », *Bulletin de l'ARCSI,* n° 44, pp. 69-76, et en accès libre sur le site internet de l'Association https://www.arcsi.fr.

[RAN] Randell, Brian, 1980, « The Colossus », *A History of Computing in the Twentieth Century*, *in* N. Metropolis, J. Howlett et Gian Carlo-Rotta, London, Academic Press, pp. 47-92.

[TUR1] Turing, Alan M., 1941a, « The Applications of Probability to Cryptography », www.nationalarchives.gov.uk, HW 257.37.

[TUR2] Turing, Alan M., 1941b, « Paper on Statistics of Repetitions », www.nationalarchives.gov.uk, HW 257.38.

[TUR3] Turing, Alan M., 2013, « Bombe and Spider (1940) », *in* [COP1], pp. 313-335

[WEL1] Welchman, Gordon, 2017 (1982), *The Hut Six Story, Breaking the Enigma Codes*, Kidderinster, M & M Baldwin.

[WEL2] Welchman, Gordon, 1986, « From Polish Bomb to British Bomb : the birth of Ultra », *Intelligence and National Security*, vol. 1, n°. 1, publié par Franck Cass & Co, 900 Eastern Avenue, Ilford, Essex, England. Reproduit dans *The Hut Six story*, pp. 195-234.

[WIN] Winterbotham Frederik, 1974, *The Ultra Secret*, London, Weidenfeld & Nicolson.

[YOU] Young, Irene, 1990, *Enigma Variations: A Memoir of Love and War*, Edimbourg, Mainstream Publishing.