Un nouveau livre sur les décryptements britanniques pendant la Seconde Guerre mondiale

Le professeur Hinsley et Alan Stripp ont publié l'an dernier « *Code breakers - The inside story of Bletchey Park* » aux éditions Oxford Press (Décrypteurs : histoire interne de Bletchey Park). Le professeur Hinsley est bien connu comme l'auteur principal de la somme que constituent les quatres tomes du « Renseignement anglais pendant la 2e guerre mondiale », avec plus de 3 000 pages. Alan Stripp est l'auteur de « Décrypteur en Extrême Orient » dont il a été rendu compte dans le bulletin n° 19 de 1991. Tous deux ont fait partie de la GC and CS, le premier ayant exercé ses fonctions dans les cellules s'occupant du chiffre naval allemand, le second ayant opéré aux Indes, contre les armées de terre et de l'air japonaises à partir de l'été 1944.

Le livre commence par une étude du professeur Hinsley sur l'influence qu'ont exercé les décryptements sur le déroulement de la 2e guerre mondiale (elle nous servira de conclusion) puis comprend 30 articles écrits par des anciens de Bletchey Park. Certains font surtout ressortir l'atmosphère non conformiste qui y régnait mais beaucoup apportent, contrairement au symposium dont il a été rendu compte dans le bulletin 21 de 1993 des indications complémentaires ou même nouvelles sur les décryptements obtenus et les méthodes employées, en particulier pour les translations chiffrantes SZ40 et SZ42. Ces articles sont classés en 5 parties dont il a été essayé de tirer l'essentiel dans les lignes suivantes.

1re partie : La production des renseignements Ultra.

La baraque 3 (Hut 3) avait pour cible les messages ENIGMA de l'armée de terre et de l'armée de l'air allemandes, les clés de déchiffrement étant fournis par la Hut 6. Toute une série d'opérations s'y succédaient : déchiffrement, traduction, évaluation, mise en forme et envoi, chacune faite par des personnels spécialisés. En même temps on tenait à jour un ordre de bataille et un index où étaient enregistrés des renseignements de toute nature, mots nouveaux ou techniques notamment.

Un officier américain de liaison fut affecté à la Hut 3 durant l'automne 1943 et recruta quelques jeunes officiers de son pays parlant allemand pour la renforcer. Au début de 1944 il proposa de former une vingtaine d'officiers américains en 6 à 8 semaines

pour gérer le trafic ULTRA dans les commandements américains, ce qui fut agréé, et le général Eisenhower en fit bon usage (1). En ce qui concerne la Marine, FH Hinsley était à la fin de 1939 l'expert principal sur les réseaux radios de la Kriegsmarine. L'analyse des réseaux, de leur trafic et la radiogoniométrie étaient les seules sources d'information. Il releva en particulier un trafic accru et inhabituel en Baltique avant l'invasion de la Norvège. L'Amirauté britannique ne sut pas exploiter ce renseignement. Peu après le porte-avion *Glorious* fut coulé par le *Scharnorst* et le *Gneisenau* dont le départ de la Baltique avait été signalé. L'Amirauté prit alors conscience de l'importance de tels renseignements : Hinsley passa un mois à l'OIC (Centre de Renseignements Opérationnels de l'Amirauté) avec une visite au PC de la Homefleet et dès lors une bonne liaison exista entre BP et l'OIC. L'analyse du trafic permit en 1941 de déceler la présence et l'existence des chalutiers météorologiques ; l'Amirauté organisa leur capture qui fournit les premiers éléments du décryptement de l'Enigma navale, comme cela a déjà été raconté dans le bulletin.

2e partie : les machines ENIGMA

Tant de renseignements ont déjà paru sur le décryptement de l'Enigma qu'il semblerait ne plus rien avoir à découvrir. Les 5 articles qui y sont consacrés apportent cependant des précisions ou même des nouveautés. Le sérieux allemand faisait que, sur un mois, une configuration donnée de rotors n'était jamais répétée, et qu'aucun rotor ne se trouvait à la même place que la veille. Cette certitute diminuait le nombre des essais à effectuer.

Les divers articles insistent sur les ouvertures données par les adresses et signatures *in extenso* dans les messages de la Luftwaffe quoiqu'un des auteurs ait fait une légère confusion entre le banburisme et la méthode des lettres constantes de Zygalski parce que toutes deux utilisaient la coïncidence de perforations. On peut se faire une meilleure idée du premier. Les feuilles de « banbury » comportaient un grand nombre d'alphabets ordonnés parallèles en colonnes verticales et les lettre successives des messages étaient perforées sur ces colonnes. La superposition de feuilles deux à deux, en recherchant le « bon » décallage permettait, en recherchant les coïncidences des perforations :

- de reconnaître des recouvrements (adresses et signatures en particulier)
- surtout de déterminer les ruptures dues à l'avance du 2e rotor ce qui, comme l'avaient déjà vu les Polonais, donnait l'identité du 1er rotor et dans certains cas, en poursuivant l'étude, celle du deuxième. Cette méthode réussissant assez souvent, grâce à l'expérience et au flair des décryptements avec l'Enigma marine et permettait de réduire le nombre d'essais sur les bombes et de faciliter l'établissement du menu. Ceci fut très important car, jusqu'en 1944 le nombre des bombes et leur vitesse étaient insuffisants pour répondre à l'ampleur

des besoins. Avant les bombes, une petite machine fut utilisée dès l'été 1940, dénommée Baby, c'était une ébauche de bombe, à fonctionnement manuel. Elle permettait, connaissant l'ordre des rotors et la substitution des dicordes et en essayant le chiffrement du mot EINS (un) à toutes les positions des rotors, d'obtenir la position de départ des messages. Il semble qu'elle ait été utilisée quand les clés étaient connues par les captures (chalutiers météorologiques).

L'Enigma de la Reichsbahn (chemins de fer allemands)

La rareté des résultats obtenus par la HUT 8 avant 1941 fit lui confier aussi les messages de la Reichsbahn. C'était une machine type civil, sans dicordes de substitution, et il y avait beaucoup de recouvrements. Ceci permit de rétablir les câblages des rotors, par la méthode connue avant 1939 et le décryptement se fit avec une machine appelée Litchworth Enigma dont le bloc rotors était semblable à celui des bombes et où les mouvements se faisaient à la main. Ces machines servirent aussi plus tard à la vérification des résultats des bombes.
Le travail sur la Reichsbahn fut passé à la Hut 6 quand le décryptement des messages Marine commença en février 1941.

L'Enigma de l'Abwehr

La machine Enigma des réseaux de l'Abwehr posa plus de problèmes. Elle n'avait pas de dicordes de substitution, mais le réflecteur tournait comme les autres rotors, ceux-ci ayant respectivement 11, 15 et 19 ergots (sur l'anneau de repérage de position et non sur le corps du rotor comme dans la machine Wehrmacht. Il n'y avait heureusement que 3 rotors différents.
Son décryptement fut pris en charge en 1941. Le préambule comprenait 8 lettres indiquant la position de départ répétée, ce qui donna l'ouverture nécessaire, comme aux Polonais après 1931. Dilly Knox analyse la machine, reconstitue les rotors et met au point la méthode de décryptement juste avant sa mort (27.2.43). A cette époque il y avait 4 réseaux, 2 à l'Est et 2 à l'Ouest. Il y eut à plusieurs reprises modification du câblage des rotors.

3e partie : les translations chiffrantes Lorenz SZ40 et SZ42.

L'histoire de ces machines a été publiée dans le bulletin n° 16 de 1988. Le gros intérêt des articles les concernant réside dans une description détaillée de ces machines et de leur réplique britannique, ainsi que dans quelques indications sur l'emploi du Colossus pour les décryptements. Ces translations chiffrantes se plaçaient entre les téléimprimeurs, équipés éventuellement de perforations et de lecteurs de bande, et le dispositif de modulation des émetteurs ou récepteurs radios. Elles produisaient une clé additive (modulo 2) pseudo-aléatoire au moyen de 12 roues à ergots mobiles (comme celles de la C 35 ou de la M 209). Ces 12 roues étaient articulées en 3 groupes. Le premier groupe de 5 roues K (longueurs 23, 26, 29, 31 et 41 ergots)

avançait de façon régulière, pas à pas, fournissant un signe du code CCITT n° 2 fonction de la position des ergots, avec une période de 2,2 10^7. Le second groupe de roues S (longueurs 43, 47, 51, 53, 59 ergots) fournissait lui aussi un signe du code CCITT n° 2, additionné avec celui fourni par les roues K. L'avancement des roues S était commandé par la 11e roue M 37, à 37 ergots, suivant la position de l'ergot présenté, l'avancement de la roue M 37 étant lui-même commandé par la dernière roue M 61 à 61 ergots.
La période de l'ensemble SM était de l'ordre de 3 10^2 (en admettant l'équiprobabilité des positions des ergots sur les roues M) et en définitive de 6 10^{19} environ pour la machine entière. L'équation de chiffrement était C = c + k avec k = K S, en addition modulo 2 comme dans les translations à bandes aléatoires. 3 modifications furent apportées aux SZ pendant la guerre :

1 - modification de l'avancement de la roue M 37 , sa commande étant faite par la combinaison des ergots de la 2e roue K (K_{25}) et de la roue M 61.

2 - modification analogue par combinaison des ergots de la 1re roue S (S43) et de la roue M 61.

3 - autoclave en combinant le 2e moment du signe clair antépénultien avec l'ergot de la roue M 61, mais cette modification fut annulée en raison des très nombreuses erreurs résultant de fautes de transmission.

On sait, comme M. Llopis l'avait démontré dans les années 60, qu'on parvient à rétablir la clé d'un tel système de chiffrement de proche en proche, en utilisant des recouvrements ou des mots probables, en tenant compte des fréquences des lettres et des moments correspondants.
Le travail fut d'abord effectué en Suède (voir bulletin n° 16) ; M. Beurling avait mis au point une méthode générale à l'aide de machines sur lesquelles aucun renseignement n'a été divulgué. On sait aussi que les Suédois avait donné quelques informations aux Anglais, mais on ignore leur nature, opérationnelle ou technique, et le livre analysé ici n'en dit mot. Les informations anglaises indiquent que la première entrée dans le système eut lieu parce qu'un chiffreur allemand avait utilisé le même jour la même position de départ pour 2 messages, ce qui permit la restitution des clairs et de la clé. W.T.TUTTE réussit après quelques mois à en déduire la structure de la machine, y compris la longueur de chacune des roues. Une partie de son travail permettait aussi de remonter l'ergotage des roues lorsqu'on disposait d'une longue suite-clé. Le problème posé était en effet de restituer la clé du jour (position des 501 ergots soit 2^{501} ou plus de 10^{150} possibilités) et la position de départ (1,5. 10^{19} possibles environ).

Dans le même esprit que pour l'Enigma, les Anglais eurent pour objectif de créer des machines, d'une part des machines simulant les SZ40 et 42, pour déchiffrer, ce furent les TUNNY, d'autre part des machines pour rechercher les

clés.
La première de cette seconde catégorie de machines fut la Heat Robinson. On comparait un message chiffré et une suite fonction d'un ergotage des roues. Ces deux bandes de longueurs premières entre elles progressaient à la vitesse de 5 000 bauds environ (100 fois plus vite que la transmission normalisée) et étaient lues et comparées optiquement. On comptait le nombre de fois où une certaine fonction booléenne des signes comparés était égale à 1. La faiblesse de cette machine résidait dans l'entrainement mécanique des bandes qui leur causait des dégradations et/ou des décalages par rapport aux lecteurs optiques.

Le premier Colossus fut installé en 1943. Le principe était le même que pour le Heat Robinson, mais les bandes n'étaient lues qu'une fois, leurs signaux étant enregistrés électroniquement ; la machine comportait à cet effet 1 500 thyratrons (2 500 pour les Colossus 2 livrés, en 1944) ; la fiabilité de ces tubes était assuré pourvu qu'ils soient alimentés en permanence (comme les tubes des répéteurs téléphoniques).

Le programme du Colossus était fixé par un grand nombre de fiches. Ce menu (même dénomination que pour les bombes) avait été élaboré en premier lieu en tenant compte des fréquences des lettres et des moments en langue allemande. Il avait été reconnu que le 3e moment était le plus significatif : une addition du texte chiffré avec la séquence EUWE répétée donnait beaucoup de renseignements. On utilisait aussi vraissemblablement des mots probables (adresse notamment) pour remonter les clés. Les résultats obtenus, il convenait de rétablir l'ergotage des roues, selon la méthode initiée par WT TUTTE ; ce travail était fait d'abord à la main, mais on s'aperçut que le Colossus pouvait le faire avec un programme adéquat.

On trouva aussi après la guerre que le Colossus pouvait faire des opérations arithmétiques en base 10, servir à l'équilibrage des volants des machines tournantes etc. Le Colossus était donc le premier des calculateurs électroniques.

La réplique TUNNY des SZ fut commandée aux laboratoires du Post Office, comme les Heat Robinson et Colossus. 10 exemplaires avaient été livrés lors de l'arrivée du Colossus 1.
Ils étaient constitués essentiellement de sélecteurs de téléphonie automatiques à 25 points (plusieurs étaient combinés pour représenter les roues de longueur supérieure à 25) et de relais.
L'addition modulo 2 des moments était faite par des groupes de 4 relais télégraphiques Siemens, les autres relais n'étant pas assez rapides. La base de temps était obtenue à partir d'un circuit résistance-capacité commandant une lampe.

La vérification du bon fonctionnement de l'ensemble était assurée par l'appareil classique de contrôle des téléimprimeurs (vitesse, distorsion, marge). L'ergotage consistait en l'alimentation des contacts des sélecteurs et était

obtenue au moyen d'un panneau de fiches.
Cette machine n'était cependant pas parfaite. L'opérateur devait faire à la main les opérations de retour-chariot et d'interligne. Le passage lettres-chiffres ne fonctionnait pas non plus ; après le symbole indiquant l'inversion chiffres, l'opérateur devait traduire les signes, selon la concordance de l'alphabet CCITT n° 2.
L'article de Gil Hayward donne des renseignements très précis, avec schémas à l'appui des circuits de TUNNY, mais il n'a pas paru nécessaire de les reproduire, laissant le soin aux intéressés d'aller consulter le livre.
La section du professeur Newman qui avait la charge du décryptement avait été baptisée Newmanry et celle du major Tester qui opérait les déchiffrements la Testery.

4e partie : les chiffres tactiques

Divers auteurs racontent leurs expériences sur les chiffres tactiques allemands et japonais ; il a paru nécessaire d'en rendre compte d'une façon assez détaillée, car cela montre la difficulté de protéger le secret avec des systèmes relativement simples, utilisables sur le champ de bataille.
On commencera d'abord par Henry Dryden, dont le parcours est un excellent exemple du déroulement de la vie d'un décrypteur pendant cette guerre.

4.1. Henry Dryden
Après une courte instruction en septembre 1938 lors de la crise des Sudètes, Henry Dryden, qui était un diplomé de Cambridge, fut recruté par la GC and CS en février 1939. Son premier travail concerna un code (surchiffré) italien dont beaucoup de groupes étaient déjà connus du fait de son utilisation pendant la guerre civile espagnole. Ensuite il travailla sur un système allemand à double transposition (sans doute déjà utilisé par les formations allemandes en Espagne) basé sur des clés journalières de longueur 25 qui était fournies aux anglais par la France (2) mais fort peu de messages étaient interceptés. En juin 39 il s'occupe aussi d'un système de l'aviation japonaise en Mandchourie mais lors de l'attaque allemande contre la Pologne, on lui confie le trafic de la police allemande, il s'agissait encore de transposition. J Tiltman mit au point une méthode simple de rétablissement. Les Français (2) avaient également obtenu de bons résultats et une coopération fut organisée chaque pays prenant en charge un jour sur deux et communiquant ses résultats.

Lors de la réussite du décryptement de l'Enigma (Janvier 40) il fut affecté à la HUT3 puis en avril 40 comme adjoint de Mac Farlan auprès du Commandant Bertrand, mais le changement de méthode du chiffrement des clés de message Enigma ne laissait plus de possibilités à partir du 1er mai. H Dryden fut alors envoyé en liaison auprès du corps expéditionnaire anglais (BEF). Les Anglais avaient capturé des codes de groupe de 3 lettres utilisés par les avions de reconnaissance allemands, et celà, avec les messages clairs interceptés permit de don-

ner quelques indications utiles lors du repli rapide de la BEF. Il fut renvoyé à La Ferté, prit part au repli sur Briare et fut évacué en priorité par Bordeaux.

Revenu à BP, il fut affecté à la HUT3 où il participa à divers travaux :
- sur un code naval français, dont un exemplaire avait été remis aux anglais par un marin français après Dunkerque,
- sur un système de transposition de l'Abwehr, difficile parce que les lignes de son tableau avaient des longueurs variées,
- sur un système de l'aviation italienne avec un code à 3 chiffres assez facile,
- enfin sur l'Enigma de la Reichsbahn (voir plus haut) dont le décryptement fut facile à cause de nombreux recouvrements. Dès le début de 1941, l'importance des transports ferroviaires vers l'est fut détecté et signalé.

Henry Dryden fut alors envoyé en Egypte car Rommel avait débarqué en Libye et personne au Moyen-Orient n'avait l'expérience des chiffres allemands. Son départ par mer fut retardé à cause d'une panne du navire prévu et il n'arriva au Caire que le 30 avril, via Freetown.
Heliopolis s'était déjà occupé des messages italiens tactiques et y avait réussi pleinement.
Les interceptions de messages allemands ne commencèrent à donner des résultats que le 20 mai, lors de l'invasion de la Crête ; les messages tactiques étaient chiffrés par transposition selon la méthode utilisée par la police allemande (voir plus haut). Les messages Enigma interceptés étaient transmis à BP d'où ils revenaient déchiffrés mais par précaution le texte clair subissait une substitution simple avant le chiffrement par Typex, de façon à éviter les indiscrétions éventuelles des chiffreurs au départ comme à l'arrivée.

La Luftwaffe n'était pas la seule à transmettre des messages codés surchiffrés à 3 lettres, la 33e unité de reconnaissance de la 15e Panzerdivision en faisait autant.
On mit alors en place auprès de la 7e division blindés britannique un groupe d'interception et de décodage. C'était excellent mais ce groupe avait de grosses difficultés pour suivre et joindre le PC en période de mouvement. Aussi limita-t-on, pour El-Alamein (octobre 42) et ensuite, aux échelons Armées et Corps d'Armée la mise en place de détachements (interception). Au printemps 1942 le code à 3 lettres fut remplacé par un code à 3 chiffres, surchiffré au moyen de feuilles journalières ; cela ne présentait pas de difficultés quand le trafic était notable mais demandait plus de temps. Depuis le 1er juillet 1941, les Allemands utilisaient aussi un double Playfair en particulier entre les îles de la mer Egée, et on continua à intercepter et à décrypter jusqu'à l'automne 1944. A l'été 1942, le Caire, avec des machines récupérées sur les Allemands se met à déchiffrer les messages des officiers de liaison Air de Rommel qui utilisaient d'anciennes clés, envoyées précédemment par BP et dont l'emploi était caractérisé par un indicateur extérieur au message.

Après la victoire d'El Alamein, la vieà Heliopolis devenait plus calme (d'autant plus que H. Dryden, devenu chef du service avait mis en place des détachements à la 8e armée et aux corps d'Armée.
En mai 1944, Henry Dryden fut rappelé à BP, en prévision du travail résultant du débarquement en préparation.

4.2. Les chiffres tactiques de l'armée de terre allemande.

Comme cela a déjà été cité, les Allemands, qui avaient décrypté le Playfair anglais pendant la guerre 1914-1918 à partir de mai 1915 utilisaient un Playfair double, avec des alphabets entièrement désordonnés. Ils plaçaient un X entre chaque mot et STOP entre chaque phrase et complétaient le message à 5 par des X. Les clés changeaient chaque jour à minuit, les signatures et les chiffres épelés. il y avait en plus un code d'abréviation pour certains mots usuels (chars, camions etc.).

Le décryptement, dont Noël Currer-Brigs donne une exemple commença en 1941, sur des messages du front Est et fut tout à fait au point en 1942. L'auteur fut envoyé en Afrique du Nord dès novembre 1942, à la tête d'un détachement de décryptement et fut averti au cours de son voyage par BP que les Allemands avaient changé leur système. En plus ils avaient modifié leur procédure de transmission, employant une fréquence à l'émission et une à la réception, ce qui compliquait le travail des intercepteurs mais, heureusement, les particularités de manipulation subsistaient. Il y eut aussi des messages donnant en clair des noms et des désignations d'unités lors de leur débarquement en Tunisie, et il s'avéra enfin que les Allemands utilisaient toujours le même système, n'ayant modifié que la fréquence des changements de clé.

Ce détachement qui eut à souffrir des mauvaises conditions climatiques et de plusieurs déplacements inconfortables au cours de la campagne de Tunisie, s'appliqua ensuite à rétablir l'ordre de bataille en Sicile, Sardaigne, Italie du Sud et Balkans et y réussit, toujours grâce aux messages tactiques. Mais il travailla aussi sur ce que l'auteur appelle les chiffres exotiques des partisans yougoslaves, albanais etc. Il peut sembler que les résultats eurent de l'influence sur le transfert de l'aide anglaise de Mihailovitch à Tito.

4.3 Les chiffres navals allemands et italiens

Les Anglais ont répertorié environ 27 chiffres navals allemands dont la majorité put-être déchiffrée régulièrement. Ce succès eut beaucoup d'importance car il fournissait des mots probables pour l'Enigma, en particulier les messages météo émis avec la même rédaction sur plusieurs réseaux.
Le plus utilisé fut le *Werft Schlussel* (chiffre des chantiers navals) qui n'était pas seulement utilisé par les chantiers et les essais de navires, mais aussi pour les communications entre navire, et dans les convois et aussi pour la météo-

rologie, sauf dans la Manche.

Le premier message fut décrypté quelques mois après avril 1940 grâce à un document capturé puis à partir de mars 1941, les textes furent rétablis de façon courante. En 47 mois, 30 000 des 33 000 messages interceptés purent être lus. Le système de chiffrement était le suivant, le texte était écrit horizontalement sur cinq colonnes. Le chiffrement se faisait sur chaque colonne, successivement, par bigrammes, suivant une table de substitution qui changeait pour chaque colonne. Au début le chiffreur disposait de 20 tables, changées tous les deux mois, à la fin de 30, changées chaque mois. La substitution bigrammatique était réciproque et aucune des lettres claires ne pouvait apparaître dans le bigramme substitué, Outre les mots probables des messages stéréotypés, les bigrammes fréquents donnaient des entrées. Lorsque des difficultés surgissaient, des opérations de minage étaient montrés avec l'Amirauté pour obtenir des mots probables. Un autre chiffre naval d'assez haut niveau était le système H, lu, de septembre 1939 à mai 1941, utilisé par les navires de commerce intégrés dans la Marine allemande. C'était encore un système de substitution par bigrammes, sur antigrammes produits avec un code international. A la mi-1941 le système devint plus complexe et indéchiffrable. Le Flugmeldeldesignal, émis par les navires allemands pour signaler la présence d'un avion ennemi permit de travailler sur la grille de référence géographique allemande.
Enfin le moyen de secours en cas de panne de l'Enigma était le eserve Handverfahren (procédé manuel de réserve) : le message était inscrit sur une grille horizontalement (l'auteur ne dit pas si la longueur des lignes était variable ou s'il y avait des cases nulles, comme dans d'autres systèmes allemands) puis relevé verticalement par bigrammes, chiffrés eux-mêmes par des tableaux de substitution (4). Ce système fut d'abord lu en juin 1941 grâce à un document capturé puis ensuite par des méthodes cryptographiques. Le volume moyen était de 12 messages par jour. Les sous-marins disposaient de grilles particulières ainsi d'ailleurs que les navires en Méditerranée où le trafic pouvait atteindre 1 000 messages par mois à la fin de la guerre. En avril 1944, un raid sur l'île de Myconos permit de capturer tous les documents de ce réseau.

La section Marine de Bletchey s'occupa de chiffres spéciaux en Manche. A noter aussi un chiffre utilisé par un agent de l'Abwehr qui surveillait de La Linea le trafic de Gibraltar, avec une simple clé additive, ce qui fournit pendant quelque temps des entrées dans un réseau Enigma de l'Abwehr.

Enfin, le décryptement de la machine Hagelin C38 de la Marine italienne fut un facteur très important de la résistance anglaise à l'Afrikakorps, car il permit de couler beaucoup de navires de ravitaillement et en particulier des pétroliers.
Au début de la guerre, la Marine italienne utilisait un code ordonné à 5 chiffres, surchiffré par une clé

additive dont le GC and CS avait pu rétablir une bonne partie de 1937 à 1940. Mais son entrée en guerre entraîna un changement des clés et aussi de certains codes et aucun résultat ne fut obtenu avant une capture à la mi-41 ; de nouveaux changements introduits en février 1942 firent abandonner les essais de décryptement. En effet les Italiens utilisaient la C38 depuis décembre 1940, c'était une machine dérivée de la C36, avec six roues-clés mais on ne sait pas s'il y avait des cavaliers comme sur la M209 (C41 de Hagelin). Le système fut percé dans l'été de 1941 et lu ensuite de façon courante à BP, Alexandrie et Malte.

Christopher Morris termine son article sur les chiffres navals allemands par quelques réflexions sur la circulation de l'information et les relations entre les services de décryptement et les organismes chargés du renseignement dans les états-majors. C'est ainsi que le *War Office* qui avait la responsabilité de l'établissement de l'ordre de bataille ne reçevait pas les informations relatives aux transports en Baltique, réservés à l'Amirauté. Certaines identifications ou localisations obtenus par le Werftschluessel n'étaient transmises par BP à l'Amirauté que lorsqu'elles étaient confirmées par l'Enigma. Ce genre de choses atteignait parfois le moral des décrypteurs d'autant plus que les officiers de l'Amirauté comprenaient difficilement leur mode de travail, leur attitude souvent plus civile que militaire (voir ce que rapporte à ce sujet Hinsley à la fin de la 1re partie), etc. Et comme toujours le succès paraissait normal, dû, et l'insuccès entraînait des récriminations.

4.4 Les chiffres tactiques de la Luftwaffe.

Pour ses liaisons à grande et moyenne distance, en graphie manuelle, la Luftwaffe utilisait un code ordonné à 3 chiffres, surchiffré avec une carte de substitution faisant correspondre à chacun de ces 1 000 nombres un trigramme littéral constitué de façon aléatoire. Utilisé dès avant la guerre et pratiquement inchangé, ce code avait été reconstitué avant 1940 par la GC and CS. Au début de la guerre, les messages interceptés à Cheadle étaient retransmis à BP où on reconstituait les cartes de substitution et d'où on envoyait les déchiffrements au ministère de l'air. Quatre étudiants de Cambridge, formés à BP furent envoyés en 1940 à Cheadle où ils déchiffraient les messages avec les clés fournies par BP et en envoyaient le résultat aux commandements intéressés. Mais rapidement, à cause des messages stéréotypés envoyés notamment chaque matin par des avions de reconnaissance météo, et malgré le changement journalier de la carte de substitution, ces déchiffreurs devinrent, sans autorisation formelle de BP des décrypteurs et pouvaient faire parvenir aux commandements anglais (*Coastal Commando* par exemple), les messages déchiffrés pratiquement en même temps qu'ils touchaient leurs destinataires.

Le seul changement apporté à ce système au cours de la guerre fut le remplacement des cartes de tri-

grammes littéraux par des tables numériques à 3 chiffres réciproques (pour n'avoir qu'une liste à utiliser), ce qui facilitait encore plus le décryptement. Ces interceptions ne fournirent pas beaucoup d'informations, mais permettaient cependant de signaler des décollages et d'améliorer la connaissance de l'ordre de bataille aérien allemand.

4.5 Les chiffres navals japonais

Les Anglais se sont attaqués assez tardivement aux systèmes japonais et n'ont pu y consacrer que des moyens faibles, au regard de l'effort américain après Pearl Harbour.
La Marine japonaise utilisait un assez grand nombre de codes à 4 à 5 chiffres, surchiffré au moyen de suites additives longues.
Les codes les plus utilisés étaient, pour la marine marchande le JN 11 à 4 chiffres et le JN 40, pour la marine de guerre le JN 25.
Les suites additives étaient changées plus fréquement que les codes, ainsi en 1944, le JN 25 en était à sa 12^{e} édition, tandis que c'était le 53^{e} carnet d'addition qui était en service.

L'article de Monsieur Bloch paru dans nos bulletins 18 et 19 (1990 et 1991) fait le point sur les résultats obtenus par les Américains.
Après un changement de code ou de suite additive, il fallait attendre deux semaines pour les premiers résultats et deux semaines supplémentaires pour les premiers décryptements utilisables.
Après la perte de Hong-kong puis de Singapour, le service britannique s'installa au Kenya puis en 1943 à Colombo ; il comprenait en mai 1945, 33 personnes qui traitaient de 150 à 200 messages en JN 25 par jour, alors que d'autres groupe s'occupaient des JN 11 et JN 40. Il est précisé qu'il y avait beaucoup d'échanges d'informations avec les Américains et les Australiens pour reconstituer codes et carnets de clés.

4.6. Les chiffres de l'armée de terre japonaise.

Beaucoup de renseignements ont déjà été fournis par le livre d'Alan Stripp, dont il a été rendu compte dans le bulletin 19 de 1991.
Les deux articles traitant du sujet apportent quelques précisions. Le colonel Tiltman réussit dans l'été 1942 à décrypter le système utilisé par les attachés militaires japonais (dénommé JMA). C'était un code transformant les syllabes Kana en bigrammes littéraux (675), surchiffrés par une transposition assez compliquée sur une grille. La difficulté venait surtout de disposer d'assez de linguistes pour comprendre les messages.

En ce qui concerne le code 3366 (ou 6633 selon les auteurs), le travail de décryptement proprement dit était effectué à Bletchey Park ; un échange d'informations et une discussion avait lieu entre les intéressés (tous les jours à 17 heures, alors que presque tout le code avait été rétabli, un exemplaire en fut capturé aux îles Salomon.
Les clés découvertes étaient envoyées de BP à New-Dehli, où était Alan Stripp. Ce dernier complète les renseignements sur les décryptements réalisés par les Japonais ; ceux-ci en raison de la

faiblesse de la sécurité des autorités chinoises, décryptaient le trafic entre Mountbatten et Chungking, celui de la 36e division et de certaines patrouilles. Ils interceptaient aussi les conversations entre les pilotes américains et les tours de contrôle, ce qui leur permettait d'évaluer la force et les objectifs des raids aériens, en particulier vers le Japon.

5. Pour terminer, nous rappelerons les conclusions du Professeur Hinsley sur l'importance des renseignements apportés par le décryptement sur le déroulement de la guerre.

L'influence majeure a surtout concerné les batailles en Méditerranée, Afrique du Nord et Atlantique. En 1941, les préparatifs faits en Crête n'ont pu sauver l'île mais les pertes allemandes furent telles qu'Hitler ne put recommencer de semblables opérations (Malte par exemple). De juin 41 à juillet 42, le ravitaillement conditionna les actions de Rommel ; si environ 50 % de ses approvisionnements n'avaient pas été coulés, il aurait certainement pu atteindre le Nil puis le canal de Suez en 1941 ; on peut en imaginer les conséquences et les possibilités d'exploitation.
La bataille de l'Atlantique a été racontée dans de nombreux livres, dont celui de David Kahn dont il a été rendu compte dans le bulletin n° 19 de 1991.

Le professeur Hinsley estime que sans les informations apportées par le décryptement des réseaux de la Kriegsmarine du cours du 2e semestre 1941 puis à partir de la fin de 1942, les pertes de tonnage maritime alliées auraient retardé d'au moins un an et sans doute de deux la possibilité de réussir un débarquement en Normandie.
On ne peut que se rallier à cette opinion bien étayée, tout en laissant son imagination vaguer aux hypothèses plus ou moins plausibles.

Après avoir lu et étudié cet ouvrage, on ne peut qu'en recommander la lecture, car il apporte vraiment des renseignements inédits qui répondent à des questions que l'on pouvait se poser ou à des trous dans l'information déjà publiée. On ne peut que féliciter le Professeur Hinsley et Alan Stripp d'avoir eu l'initiative de cette publications.

L. Ribadeau Dumas

Additif,

« Mes camarades de Cambridge », (3) livre écrit par Youri Ivanovitch Modine un russe, ancien du KGB, donne quelques précisions sur les cinq anciens de l'Université de Cambridge recrutés au profit de l'URSS. Si l'histoire des quatre premiers, Anthony Blunt, Philby, Burgerss et Mac-Lean est bien connue, celle du 5e, qui file actuellement de vieux jours paisibles sur la Côte d'Azur l'est moins. L'action de Cairncross n'a été dévoilée que très récemment. Henry Dryden confirme qu'il fut à BP (HUT 3) pendant près d'un an, en 42-43 et Modine confirme qu'il communiqua aux Russes des informations obtenues notamment à BP. On peut penser que, grâce à l'extrême cloisonnement qui régnait à BP, il n'a pas transmis de renseignements concernant les techniques de décryptement.

(3) Un des rares livres sérieux traduits en français, aux éditions Robert Laffont dont la lecture peut être recommandée.

Rappel de note concernant le chapitre

(1) La participation américaine aux décryptements anglais ne ressort pas très nettement des livres britanniques. Elle vient de faire l'objet d'un livre paru en Amérique puis en Angleterre sous ce titre « The ULTRA MAGIC DEALS » qu'on peut traduire par les échanges ou les trafics ULTRA-MAGIC, par Bradley F.S Smith. Ce livre insiste sur l'importance des renseignements et moyens fournis par les Américains à BP (machines RED et PURPLE dès 42, renseignements sur les chiffres japonais, personnels, bombes américaines travaillant 6 fois plus vite que les dernières bombes anglaises. Il insiste aussi sur les réticences anglaises dues à un certain laxisme américain initial dans le domaine de la sécurité.

(2) il s'agissait vraisemblablement de l'équipe espagnole recrutée par le Cdt Bertrand.