Au dessus de l'Enigma

Les « Geheimschreiber » allemands de la Seconde Guerre mondiale et les décryptements alliés

Gilbert Bloch

Malgré la persistance de quelques zones d'ombre, l'histoire de l'« Enigma » peut être désormais considérée comme bien connue.

Mais, si l'Enigma a été la machine à chiffrer la plus utilisée par les forces armées allemandes, elle n'a été ni la seule, ni la plus secrète. L'Enigma était employée au niveau « armée » et en dessous (corps d'armée, division, etc.) ; aux échelons supérieurs (groupes d'armées, grands commandements régionaux, états-majors des diverses armes, Oberkommando der Wehrmacht) le secret des communications reposait aussi sur d'autres engins de chiffrement, désignés de nos jours (à tort) par l'appellation générique de « Geheimschreiber » (« Imprimeurs Secrets »), qui prirent peu à peu une place prépondérante.

Jusqu'à une date récente, les renseignements disponibles sur ces machines, leur utilisation, leur décryptement (car, là aussi, Bletchley Park a remporté d'éclatants succès) étaient limités et fragmentaires. La publication du volume 3 de la monumentale Histoire du renseignement britannique au cours de la Seconde Guerre mondiale, réalisée sous la direction du professeur Sir Harry Hinsley (1) a permis de disposer d'informations (non techniques !) plus étendues et plus cohérentes. Du côté allemand, une étude d'ensemble sur les « Geheimschreiber » est actuellement en cours d'élaboration ; sa publication apportera certainement une contribution essentielle à nos connaissances (2).

Aucune documentation sur le sujet n'était jusqu'à présent accessible en français. Le présent texte, simple compilation des quelques documents cités dans la bibliographie, n'a pas la prétention de combler cette lacune. (Il ne comporte d'ailleurs aucune description technique des machines). Sa seule ambition est de fournir des indications sommaires sur quelques aspects des problèmes.

Les divers « Geheimschreiber »

A. Caractères généraux.

Le terme « Geheimschreiber » doit être entendu au pluriel. En effet, il recouvre plusieurs types de machines dont les techniques, les procédures d'emploi et les utilisateurs ont été différents.

Malgré ces différences, ces machines ont en commun certaines caractéristiques.

1. Destinés à être utilisés à des niveaux de hiérarchie militaire d'une mobilité géographique moindre que celle des unités dotées de l'Enigma, les « Geheimschreiber » sont plus volumineux et plus lourds (entre 100 et 200 kg).

2. Devant assurer la protection des communications les plus secrètes, les « Geheimschreiber » sont des engins plus sophistiqués que l'Enigma.

3. Tous les « Geheimschreiber » peuvent assurer le chiffrement et la transmission des messages. Il s'agit donc, à la différence de l'Enigma, de machines « on line ».

4. Tous les « Geheimschreiber », utilisent l'alphabet Baudot (5 « moments » pour chacun des 32 caractères de cet alphabet) et non l'alphabet Morse.

5. Les « Geheimschreiber » originellement conçus pour fonctionner en tant que téléimprimeurs sur (circuit filaire), vont être ultérieurement dotés de dispositifs leur permettant de fonctionner en « mode radio » (transmissions sur liaison radio). Ceci est généralement obtenu en incorporant aux machines des perforateurs de bandes : les perforations correspondent au texte chiffré — exprimé en alphabet Baudot — la bande perforée est ensuite « lue » par un lecteur modulant un émetteur radio, cette lecture s'effectuant soit à vitesse normale (50 bauds), soit à allure accélérée permettant de diminuer le temps de transmission. Un processus inverse est utilisé à la réception des messages.

B. Les divers types de machines.

Dans l'état actuel des connaissances peuvent être identifiés trois types de machines. Pour chaque type, plusieurs modèles, de plus en plus perfectionnés, se sont succédés au cours du temps (tout en restant, en général, « compatibles », afin que l'apparition d'un nouveau modèle n'implique pas la mise au rebut des modèles précédents).

1. Les « S.Z. » « 40 » et « 42 »

S.Z. est l'abréviation de « schlüsselzusatz » (pluriel « schlüsselzusätze ») c'est-à-dire, en français, « dispositif supplémentaire de chiffrement ». (Le terme « geheimzusatz » « dispositif supplémentaire de secret » est aussi utilisé).

Les « S.Z. », conçus et fabriqués par la firme C. Lorenz (3) ont comporté deux séries d'appareils — S.Z. 40 et S.Z. 42 — la dernière série elle-même subdivisée en modèles successifs A, B et C. Comme l'indique le terme « Zusatz » (supplément), les machines étaient construites pour être couplées à des téléimprimeurs ordinaires (c'est-à-dire sans système de chiffrement) produits par la firme Lorenz.

Dans un rapport en date du 5 septembre 1944, une commission d'experts, chargée d'étudier la sécurité des communications

allemandes, concluait que le S.Z. 40 et les S.Z. 42 A et B ne devaient être employés qu'en mode téléimprimeur, le S.Z. 42 C étant seul considéré comme suffisamment sûr pour être utilisé couramment en mode radio.

Les S.Z. étaient employés essentiellement par l'armée de terre (« Heer »), et furent donc les « geheimschreiber » les plus nombreux et les plus utilisés. Paradoxalement pourtant, les S.Z. — décryptés à partir de 1942 par les Britanniques — n'ont pas fait l'objet jusqu'à présent (à notre connaissance) d'une description technique accessible et détaillée.

2. Les « T 52 »

Les premières études et réalisations de cette machine furent entreprises à la demande de la Marine. Elles datent de la période 1930-1932 et sont dues à l'inventeur Erhard Rossberg (en collaboration avec les ingénieurs A. Jipp et E. Hettler). L'élaboration en fut faite par la firme Siemens & Halske, et tous les T 52 sortirent de ses ateliers. Les prototypes du T 52 étaient bâtis autour du téléimprimeur T type 25, fabriqué couramment par Siemens ; ultérieurement, les divers types successifs des téléimprimeurs Siemens furent employés (T 29, T 32, T 36, etc.). Les T 52 comportèrent les modèles successifs A (1930), B (1934), C, D (1938), E (1942-43) ; le modèle D fut celui construit en plus grand nombre. Un type F était en expérimentation à la fin 1944 et deux prototypes furent détruits à Spandau par un bombardement aérien en 1945.

Jusqu'à 1942, les T 52 furent désignés sous le terme « Geheimzusatz der Siemens Fernschreibmaschine » (dispositif supplémentaire de secret pour téléimprimeur Siemens) par la « KriegsMarine », et « Schlüsselzusatz der Siemens Fernschreibmaschine » (dispositif supplémentaire de chiffrement...) par la Luftwaffe.
Le 20 juillet 1942, les dénominations furent unifiées en « Schlüssel fernschreibmaschine T 52 » (téléimprimeur chiffrant T 52), en abrégé SFM T 52. Le modèle T 52 E reçut officiellement la désignation de « Geheimschreiber » — et son nom a été indûment étendu aux autres modèles de T 52 et aux autres types de machines.

Les T 52 furent essentiellement employés aux échelons supérieurs de la Marine (dès 1932) et de la Luftwaffe, mais l'armée de terre en utilisa également quelques-uns. Les T 52 A, B et C ne fonctionnaient qu'en mode filaire. A partir du T 52 D, l'utilisation en mode radio fut rendue possible. Le rapport du 5 septembre 1944 (précédemment cité à l'occasion des S.Z. 40 et 42) concluait à la sécurité du T 52.

Le T 52 est (à notre connaissance) la machine pour laquelle la documentation technique accessible est la plus fournie, Des études lui ont été consacrées, tant du côté britannique (par D.W. Davies) que du côté allemand (par W. Mache). On a pu estimer à plus de 1 000 le nombre de T 52 construits. Bon nombre survécurent à la guerre, et certains furent construits ou reconstruits, après guerre, pour le

compte d'acheteurs étrangers.

3. Le SFM T 43

La plus mystérieuse des machines à chiffrer allemande. Son existence fut révélée en 1981 par W. Mache, qui avait retrouvé l'année précédente dans les archives de la firme Siemens & Halske une description complète de l'appareil. Le SFM T 43 n'a été fabriqué (par Siemens) qu'à dix exemplaires dont, semble-t-il, quatre seulement ont été en utilisation suivie, à partir de 1943, par le ministère de l'Air, pour ses liaisons avec les quartiers généraux de la Lufwaffe situés respectivement à Paris et à Varsovie. Le système de chiffrement du T 43 était paticulièrement sophistiqué et équivalait à la « clé aléatoire une fois » (One time pad). Le dispositif de transmission radio utilisait les ondes décamétriques avec antennes directives.

La connaissance et le décryptement (partiel !) des « Geheimschreiber »

A. Les premières informations.

L'emploi aux plus hauts niveaux militaires allemands de téléimprimeurs munis de dispositifs de chiffrement n'était pas ignoré à l'étranger (4). Toutefois, les machines elles-mêmes et leurs procédures d'emploi restaient mystérieuses ; leur utilisation exclusive en mode téléimprimeur durant les années précédant la guerre avait interdit toute écoute. (On n'avait pas encore à l'époque l'habitude de se brancher sur les lignes... et, au surplus, on voit mal les « services » étrangers se livrer à cette activité à l'intérieur du IIIe Reich).

Par contre, Hinsley (Vol. 3, Part 1, p. 477) indique que, dès 1932, les stations d'écoute britaniques avaient suivi les expériences allemandes relatives à la transmission par radio de messages rédigés (en clair) selon l'alphabet Baudot réservé en principe aux transmissions par téléimprimeurs. Au cours du 2e semestre 1940 et du 1er semestre 1941, de tels messages — dûment chiffrés — furent interceptés occasionnellement ; ces interceptions se firent fréquentes à partir du 2e semestre 1941.

L'insuffisance sécurité d'un type de machine allemande et de ses procédures d'emploi se révéla dès 1940 de manière inattendue. Après l'occupation de la Norvège, les Allemands sollicitèrent de la Suède l'autorisation d'utiliser les câbles télégraphiques et téléphoniques suédois pour leurs liaisons militaires Berlin-Oslo, Trondjeihm, Narvik, et plus tard Berlin-Helsinki. Les autorités suédoises ne pouvaient qu'acquiescer, mais établirent une écoute sur les lignes. Les interceptions réalisées permettraient peut-être — les Suédois ne devaient guère y croire — de glâner quelques informations. A la surprise générale, le mathématicien et cryptologue Arne Beurling réussit, après un court délai (quelques semaines !) à décrypter les messages allemands transitant par la Suède ; ultérieurement, il construisit même une

sorte de « Bombe » suédoise pour faciliter son travail. La machine allemande — sans doute un T 52 du premier type — et ses procédures initiales d'emploi s'avéraient moins coriaces qu'on aurait pu le croire. Les décryptements suédois se poursuivirent jusqu'au 17 juin 1942, date à laquelle les Allemands, avertis de la « fuite » par l'attaché militaire de Finlande à Stockholm (la Finlande était alors alliée de l'Allemagne) changèrent leurs procédures. Il est certain que les Britanniques furent informés — par l'intermédiaire de leur mission diplomatique à Stockholm — de l'exploit suédois, probablement même des méthodes employées et de la teneur des messages interceptés et décryptés.

B. Le réseau allemand de transmissions « Fish »

Le succès suédois avait été conditionné par la possibilité de se brancher sur les liaisons par fil utilisées par les Allemands. A l'intérieur d'une Europe continentale sous contrôle germanique, les Britanniques se trouvaient dépourvus de semblables moyens d'interception. Mais la capacité des liaisons par fils devint rapidement insuffisante et, mettant en pratique les résultats de leurs expériences, les Allemands organisèrent progressivement à partir de 1942 un gigantesque réseau de télécommunications à l'intérieur duquel les liaisons par fils étaient doublées par des liaisons radio. Ces dernières devinrent rapidement prépondérantes : les ondes se jouaient des distances — et des sabotages affectant de plus en plus fréquemment les câbles terrestres utilisés par les transmissions allemandes. Mais la T.S.F. est indiscrète et les stations d'écoute permirent aux Britanniques de suivre pas à pas le développement du réseau. Celui-ci fut désigné par le nom de code générique « Fish » (Poisson) ; il comprenait « 6 liaisons en juillet 1943, 10 à l'automne de la même année, 26 liaisons à partir des premiers mois de 1944. Chacune des liaisons utilisait des configurations de machines qui lui étaient particulières » (Hinsley).

Les interceptions britanniques régulières débutèrent dès le milieu de 1941, lorsque les Allemands expérimentèrent une première liaison radio « Fish » entre Berlin et Athènes. L'étude de ces écoutes démontra aux Britanniques que les messages captés étaient chiffrés par une machine à laquelle les Anglais attribuèrent le nom de code « Tunny » (Thon) : il s'agissait du S.Z. 40, bientôt suivi du S.Z. 42. Un an plus tard, les écoutes révélaient l'existence d'une autre machine de chiffrement, utilisée notamment pour les transmissions dépendant de la Luftwaffe et de la Kriegs-Marine : le nom du code « Sturgeon » (Esturgeon) fut ainsi donné au T 52. Il fallut attendre janvier 1942 pour que Bletchley Park puisse reconstituer la technique du S.Z. 40 et son mode d'emploi, et l'été 1942 pour qu'il en soit de même du T 52. Au cours de l'année 1942, les combats en Afrique permirent la capture de plusieurs « Geheimschreiber » : toute incertitude fut ainsi levée pour les Britanniques en ce qui touche les machines elles-

mêmes ; restaient à trouver les moyens de reconstituer leurs configurations journalières, et de résoudre, au niveau de chaque « réseau » et de chaque message, les problèmes conditionnant le décryptement...

L'appendice 2 relatif aux « Geheimschreiber » inclus dans le volume 3, partie 1 de l'ouvrage d'Hinsley décrit le réseau « Fish » et en fournit (pour les liaisons « Tunny ») le schéma reproduit ci-joint, correspondant à son développement entre novembre 1942 et juillet 1944. Ce développement et la masse rapidement croissante des interceptions obligèrent les responsables britanniques à faire des choix et à établir des priorités.

C. Les décryptements.

1. Le décryptement des S.Z. 40 et 42.

Malgré l'expansion quantitative et qualitative de Bletchley Park, les Anglais ne disposaient pas pour le décryptement de moyens illimités. Il fallait donc allouer ceux-ci de la manière apparemment la plus profitable. A la fin 1941, il fut donc décidé de concentrer les efforts sur les transmissions de l'armée de terre allemande, c'est-à-dire sur les machines de types S.Z. Hinsley explique les raisons de ce choix : le décryptement — constant depuis le 22 mai 1940 — des messages Enigma de la Luftwaffe fournissait sur l'armée de l'air allemande des informations abondantes. En ce qui concerne la « KriegsMarine » l'essentiel était de décrypter les messages Enigma du « réseau » couvrant les communications des sous-marins allemands dans l'Atlantique (réseau « Triton » à partir d'octobre 1941). Par contre, la pénétration des réseaux Enigma de l'armée de terre s'était révélée difficile (les premiers décryptements opérationnels suivis et réellement utilisables ne débuteront guère qu'en juin 1942 sur le champ d'opération africain). De plus, le décryptement des messages « Fish » échangés entre les commandements du plus haut niveau de l'armée de terre assurait l'accès aux grandes synthèses et aux plans d'ensemble de la stratégie allemande.

Les succès obtenus par les Suédois constituaient un précédent de bon augure : là où un mathématicien suédois avait réussi, l'extraordinaire équipe de Bletchley Park devait pouvoir réussir également... Les conditions étaient pourtant beaucoup plus difficiles : les Allemands avaient perfectionné leurs machines et leurs procédures d'emploi. Les écoutes britanniques étaient rendues délicates par la faiblesse des signaux captés (faiblesse résultant de la distance séparant les stations d'interception britanniques des émetteurs allemands, et aussi du fait que les messages allemands étaient émis sur des antennes directives), par la longueur des messages et groupes de messages transmis (parfois plusieurs dizaines de milliers de caractères !), par les caractéristiques des messages rédigés en alphabet non Morse (à la vitesse normale de 50 bauds, chacun des 5 « moments » constitutifs d'un caractère de l'alphabet Baudot ne dure que 1/50^{e} de

seconde), enfin par l'emploi fréquent d'équipements permettant les transmissions à grande vitesse.

L'écoute et la transcription des messages « Fish » impliquaient le recours à des techniques particulières. Dans le cas des transmissions radio ordinaires (c'est-à-dire en Morse), la tâche était confiée à des opérateurs radio. L'emploi pour les messages « Fish » de l'alphabet Baudot impliquait la lecture sur téléimprimeur, mais la faiblesse des signaux captés ne permettait pas, au début, leur réception correcte. Il fallait utiliser un ondulateur inscrivant sur bande les signaux reçus puis, à l'aide de cette bande, reconstituer visuellement l'émission originale et la transcrire sur bande perforée. A la fin de 1942, une station d'interception spécialement consacrée aux écoutes « Fish » fut mise en service à Knockholt. Equipée de matériels perfectionnés, cette station permit de réduire progressivement la part des traitements manuels et d'aboutir finalement à une réception normale sur téléimprimeurs. Ceux-ci livraient directement des bandes susceptibles d'exploitation machine.

Quand au décryptement, il se heurtait à d'énormes obstacles, malgré la mise au point en juin 1942 d'un premier prototype primitif de machine. Les perfectionnements constants des machines et des procédures d'emploi allemandes démontrèrent aux Britanniques la nécessité de recourir à des procédés mécaniques reposant sur l'emploi de machines de formule entièrement nouvelle, fonctionnant à des vitesses jamais atteintes jusqu'alors.

L'étude des problèmes fut confiée à un groupe de mathématiciens placé sous la direction de Max Newman (de l'Université de Cambridge. Il avait rejoint Bletchley Park en septembre 1942). L'indispensable liaison entre la théorie et la pratique fut réalisée grâce à une collaboration étroite avec les services de recherches de l'Administration des Postes et le Laboratoire des télécommunications.

Un premier prototype de machine — baptisé « Heath Robinson » — fut construit et son fonctionnement jugé en mai 1943 suffisamment satisfaisant pour justifier la commande de 24 machines plus ou moins modifiées constituant la « famille Robinson » (« Peter Robinson », « Robinson & Cleaver », etc.). Ces machines ne connurent qu'une existence opérationnelle limitée — deux seulement effectivement employées — leurs performances étant complètement dépassées par un nouveau type d'engin. En effet, T.H. Flowers avait conçu en 1943 le premier « ordinateur » que le monde ait connu. Les tests eurent lieu à Bletchley à la fin de l'année et, en février 1944, le « Colossus » entrait réellement en service. La machine fut rapidement améliorée à la lumière des expériences. Le premier « Colossus II » fut réceptionné le 1er juin 1944 ; à la fin de la guerre, 10 Colossus perfectionnés étaient en service.

Ainsi, le décryptement des messages « Fish » issus des S.Z. 40 et 42

débuta au printemps 1942 grâce à l'utilisation de méthodes purement manuelles. Celles-ci purent faire place à des traitements mécaniques, utilisant jusqu'à mai 1943 des dispositifs assez primitifs. A partir de Mai 1943, le relais fut pris par les machines « Robinson » puis, à partir de février 1944, par les Colossus. L'existence de ceux-ci ne fut révélée qu'en 1976 (5) et leur mission exacte laissée initialement dans l'ombre. Aussi l'opinion les imagina comme un prolongement des « Bombes » utilisées contre l'Enigma... Il fallut un certain délai pour réaliser que le rôle des « Colossus » était l'attaque des machines de chiffrement du plus haut niveau, et que cette attaque avait été couronnée de succès.

Le décryptement des « S.Z. » fut une constante course entre les perfectionnements apportés par les Allemands à leurs machines et leurs procédures d'emploi d'une part, les améliorations des méthodes de décryptement britanniques d'autre part. Bletchley Park sortit vainqueur, mais on a de nos jours trop tendance à concidérer que cette victoire allait de soi et qu'elle fut acquise sans échecs partiels et temporaires. Il n'en est rien et les révélations faites récemment par Hinsley ne laissent aucun doute sur les difficultés éprouvées, en particulier à deux moments cruciaux. C'est ainsi qu'en février 1944, une modification des procédures allemandes entrava les décryptements (leur volume représenta la moitié seulement de celui atteint en janvier) pendant plusieurs semaines. Pire : si le premier exemplaire du « Colossus II » put entrer en service le 1er juin 1944 et permettre l'obtention, à la veille du débarquement, de renseignements d'une inestimable valeur, de nouvelles mesures de sécurité allemandes firent perdre à Bletchley Park à partir du 10 juin 1944 - 4 jours après le débarquement - la maîtrise du décryptement des messages « Fish » échangés entre l'OKW et le commandement allemand du front occidental. Les décryptements purent se poursuivre quelque temps encore sur d'autres liaisons (c'est ainsi que des informations intéressant le front de Normandie purent être obtenues par la lecture des messages échangés entre Berlin et le maréchal Kesselring, commandant le front italien) mais l'extension graduelle des nouvelles procédures allemandes à l'ensemble des liaisons « S.Z. » entraîna un « black out » angoissant. Au prix d'énormes efforts, Bletchley réussit à maîtriser les changements et à reprendre les décryptements : la situation fut rétablie (voire même améliorée) à la fin septembre 1944. Les décryptements « S.Z. » étaient alors complètement maîtrisés, et leur volume atteignit un maximum en mars 1945. Ce volume décrut ensuite, l'évolution même de la guerre entraînant l'élimination de certaines liaisons et la diminution sur les autres du nombre des messages émis.

2. Que s'est-il passé pour le T.52 ?

La décision britannique de concentrer les efforts sur les S.Z. 40 et 42 n'implique pas que le T 52 ait été complètement négligé. La prudence est une des

vertus du « Renseignement » britannique et il serait surprenant que, au cours même de la guerre, le T 52 n'ait pas fait l'objet d'une surveillance attentive et d'études approfondies. Ceci dit, il n'existe aucune preuve — et les Britanniques n'ont fourni à ce sujet aucune indication — que les messages allemands cryptés sur le T 52 aient été lus couramment avant la fin de la guerre.

Il semble bien qu'après 1945, les Anglais se soient attaqués — avec succès — au décryptement du T 52. Ils avaient pour cela de bonnes raisons. Après la défaite allemande, certains pays, découvrant l'ampleur et l'apparente sécurité des systèmes de cryptement allemands, adoptèrent pour leur propre usage les T 52 de modèles récents qu'ils pouvaient se procurer d'occasion — ou neufs, car la fabrication reprit ! Les Britanniques étaient intéressés à ces communications « secrètes » : le GCHQ « Government Central Headquarters », logé à Cheltenham, qui avait succédé à Bletchley Park, sut utiliser ses compétences.

3. Et le SFM 43...

Le Professeur Hinsley mentionne (op.cit. p. 477) « qu'une autre machine « Fish » introduite sur une liaison (baptisée « Thrasher ») resta impénétrable. Selon toute vraissemblance, « Thrasher » doit être identifié avec les liaisons de la Luftwaffe utilisant le SFM 43. Compte tenu du nombre très limité de ces liaisons et des machines utilisées, l'affirmation britannique paraît correspondre à la réalité. La question d'une étude, entreprise après la guerre, sur les possibilités de décryptement du SFM T. 43 reste entière.

L'importance et le rôle des décryptements.

Les messages diffusés sur les divers réseaux « Enigma » allemands (que les Britanniques ont progressivement décryptés pour aboutir, à partir de 1943, à la maîtrise pratiquement complète de l'ensemble du système) fournissaient essentiellement — compte tenu des niveaux auquels ils étaient échangés — des renseignements **tactiques** opérationnels utilisables dans le court terme.

Par les décryptements de messages échangés sur les liaisons « Fish » les Britanniques ont pu accéder aux renseignements **stratégiques** relatifs à la conduite générale de la guerre. Les synthèses de situation, l'examen des diverses options ouvertes, les choix finalement effectués devaient nécessairement figurer dans les messages circulant entre les plus hautes instances des forces armées allemandes.
Le décryptement — même partiel — de ces messages a certainement placé entre les mains des Anglo-Saxons des informations capitales. Les délais existants entre l'interception et le décryptement — d'après Hinsley, 3 jours en moyenne en 1943 et 1945, une semaine en 1944 — n'entraînaient pas de pertes graves de la valeur de l'information.

Le professeur Hinsley a (voir note

1 et bibliographie) fourni des renseignements sur les liaisons « Fish » qui furent décryptées, et sur les dates à partir desquelles les Britanniques les pénètrent. Les messages échangés à partir de 1941 sur la liaison expérimentale Vienne-Athènes purent être décryptés par des méthodes entièrement manuelles au printemps 1942. La première liaison opérationnelle — entre Berlin et le QG à Salonique du groupe d'armées E (Balkans), inaugurée le 1er novembre 1942, fut décryptée presque immédiatement. En janvier 1943, la liaison entre le QG du groupe d'armées C (Italie) à Rome et la 5e armée blindée en Tunisie, était lue à son tour — et devait l'être jusqu'à la fin de la campagne en mai 1943. En mai 1943, la liaison entre Berlin et le maréchal Kesselring, chef du groupe d'armées C (Rome) commençait à livrer ses secrets. A la fin d'Avril 1943, la liaison entre Berlin et le QG du groupe d'armées Sud sur le front russe était décryptée... [et les premiers décryptements fournirent les indications les plus détaillées de la contre-offensive allemande contre le saillant de « Koursk »]. (Hinsley) D'autres liaisons avec différentes portions du théatre d'opérations oriental suivirent.

Sur le front occidental, les Allemands inaugurèrent en janvier 1944 une liaison radio non Morse entre Berlin et le QG de Rundstedt : les décryptements commencèrent à fin mars. Comme il a déjà été signalé, ces décryptements s'interrompirent le 10 juin et les difficultés durèrent pendant trois mois. Quant aux nouvelles liaisons créées sur le front occidental après le débarquement, elles étaient toutes décryptées à partir d'octobre 1944. Ces succès étaient d'autant plus précieux qu'à partir de la même période — et jusqu'à la fin de la guerre — de nouvelles modifications apportées par les Allemands à leurs procédures rendaient plus difficile le décryptement des messages Enigma.

L'immense importance pour les Alliés du décryptement des messages chiffrés sur « Geheimschreiber » est évidente ; elle reste difficile à préciser. Aucun texte important de décryptement « Fish » (seuls quelques messages insignifiants sont connus), aucune « synthèse » obtenue à l'aide de ces décryptements n'ont été rendus publics par les Britanniques. Certes, le texte de la partie 2 du volume 3 d'Hinsley fait à de nombreuses reprises mention de renseignements dont l'origine est spécifiquement attribuée au décryptement de messages « Fish ». Cette précision n'est toutefois pas systématique et l'expression — très souvent employée — de « High Grade Sigint », couvre aussi bien les messages Enigma que ceux des « Geheimschreiber » (6). Tenter dans ces conditions de dresser une liste des renseignements obtenus et d'examiner l'exploitation qui en fut faite serait fort délicat. Au surplus, isoler **une** source de renseignements de l'ensemble des informations disponibles ne pourrait — sauf cas exceptionnels — que conduire à mésestimer dangereusement la réalité...

En effet, l'utilisation efficace des

renseignements implique la combinaison des informations provenant de toutes les sources (« Analyse du trafic », reconnaissance aérienne et terrestre, interrogatoires de prisonniers, etc., en plus des décryptements de tous ordres) ; cette synthèse ne doit pas trop privilégier les sources de haut niveau, quelle que soit la confiance — basée sur l'expérience antérieure — qu'il paraît légitime de leur attribuer. Manquer à cette règle c'est s'exposer à de graves mécomptes. Comme le firent remarquer les autorités de Bletchley Park au cours d'une enquête sur la faillite du renseignement allié avant l'offensive allemande des Ardennes en 1944 « Il y a des risques à trop dépendre du renseignement de haut niveau ; il était dangereux de croire que celui-ci serait toujours complet ; il était dangereux de croire qu'il serait toujours explicite. » (Hinsley, op. cit. p. 429). « Ultra » a rendu aux Alliés d'inestimables services, mais la valeur même qui lui fut légitimement accordée a parfois conduit à des erreurs... □

★

Notes

(1) Ce volume 3 de *British Intelligence in the Second World War* a été publié (voir bibliographie) en deux parties. La première, qui couvre la période allant de juin 1943 à juin 1944, fournit en tant qu'« Appendix 2 » (p. 477-482) une étude générale — vue du côté britannique — du problème des « Geheimschreiber ».

La deuxième partie — du débarquement de Normandie à la fin de la guerre — fournit de multiples indications sur le décryptement de leurs messages et l'exploitation des renseignements obtenus.

(2) Le Service Historique de l'Armée allemande a récemment (août 1987) demandé à un spécialiste de rédiger sur les « Geheimschreiber » une étude destinée à être ultérieurement publiée.

(3) Cette compagnie faisait partie du groupe international ITT, sous direction générale américaine. Bien entendu, le développement de l'appareil par la société allemande fut soigneusement caché au reste du groupe.

(4) En 1931, le major Evans (de l'U.S. Signal Corps), attaché militaire adjoint de l'Ambassade des Etats-Unis à Berlin fut convié par la Reichswehr à une démonstration des nouveaux engins de chiffrement. On lui présenta l'Enigma militaire... et le premier T 52 qui venait d'entrer en service au centre des communications de la Marine.
Le major Evans rendit compte à Washington dans un rapport parfaitement explicite daté du 2 juillet 1931 (voir à ce sujet R. Lewin. *Ultra goes to war*, chapitre 1).

(5) Par B. Randell, dans un *Report on Colossus*, publié par le Département des Statistiques de l'Université de Newcastle. R. Lewin est — à notre connaissance — le premier auteur qui, dans son livre *Ultra goes to war*, publié en 1978, ait tenté d'incorporer le « Colossus » à l'histoire d'« Ultra ».

(6) Par exemple, sous le titre *The sources of High Grade Sigint after D day*, l'Appendix 15 de la partie 2 du Volume 3 d'Hinsley (p. 845-857) est essentiellement consacré aux réseaux Enigma et reste très succinct sur les liaisons « Fish ».

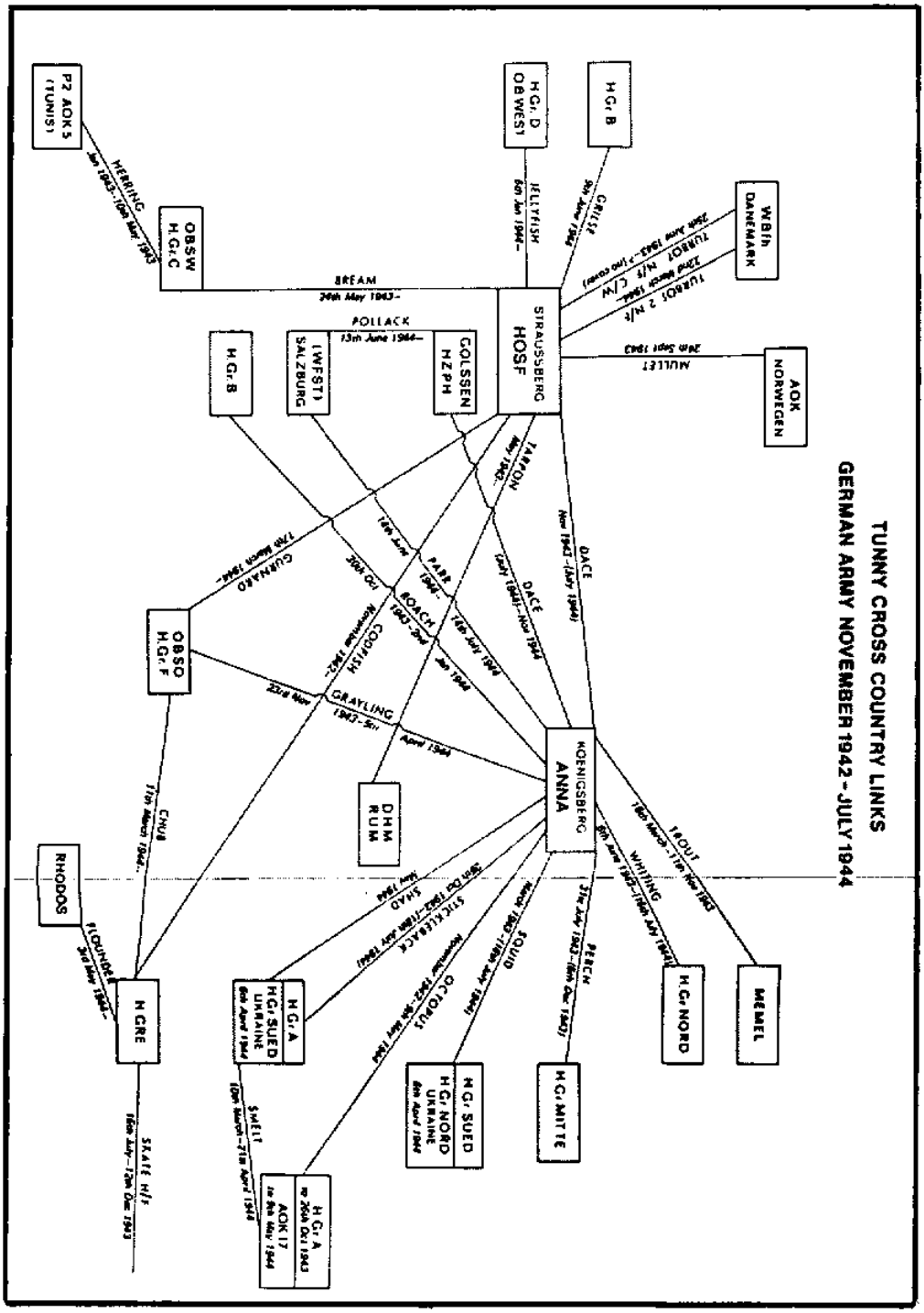
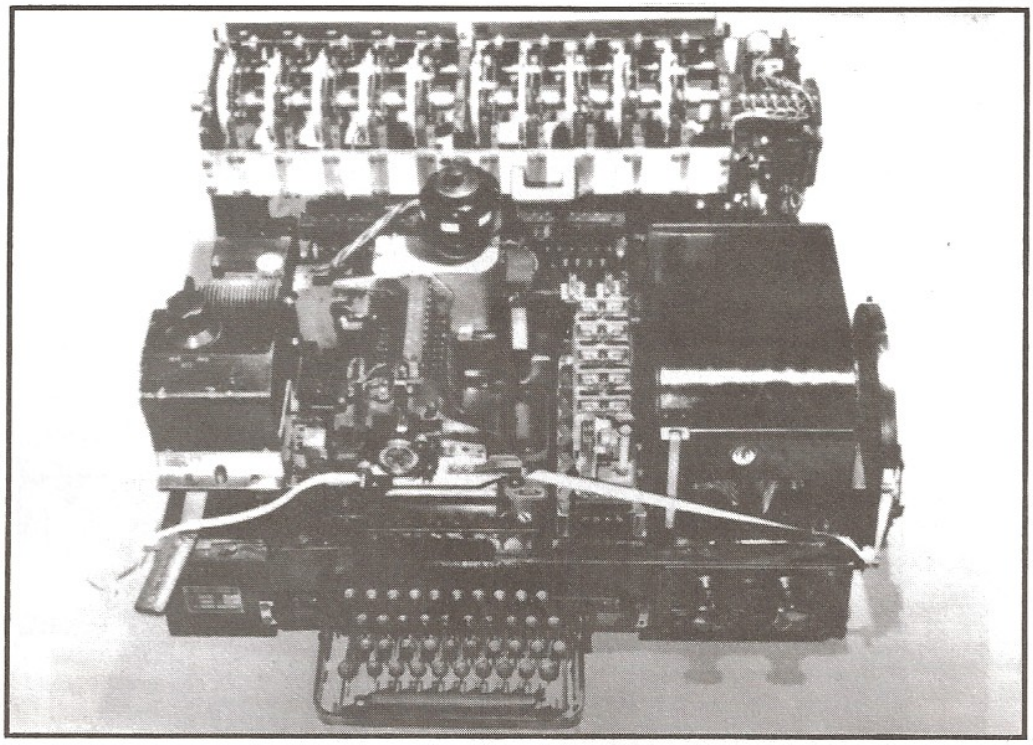
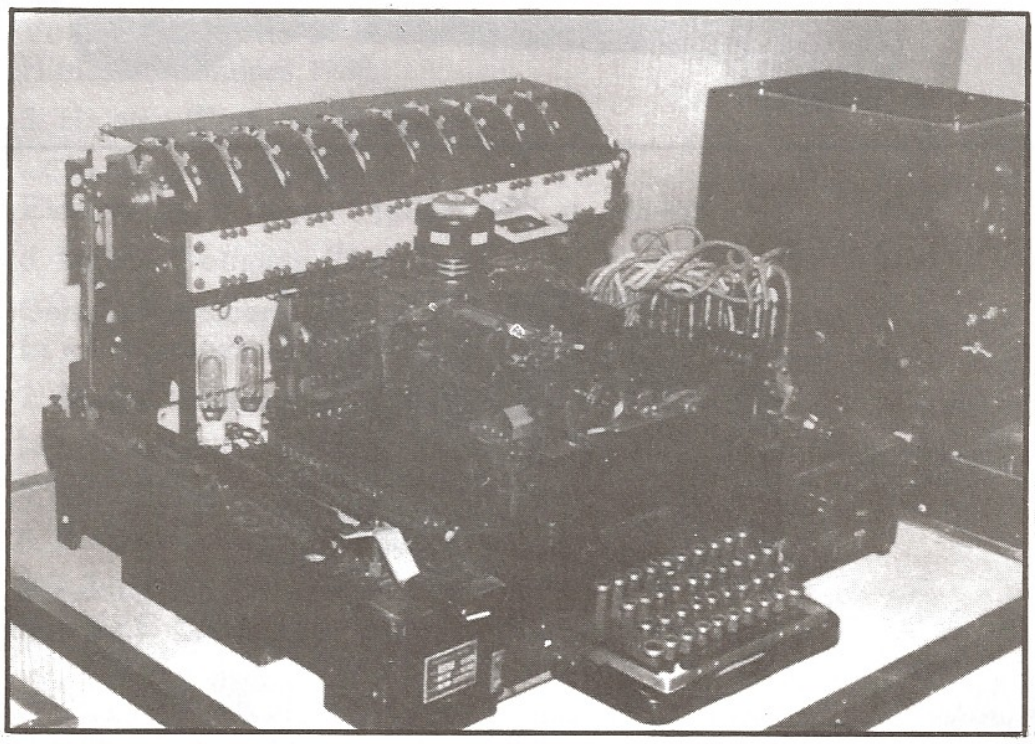


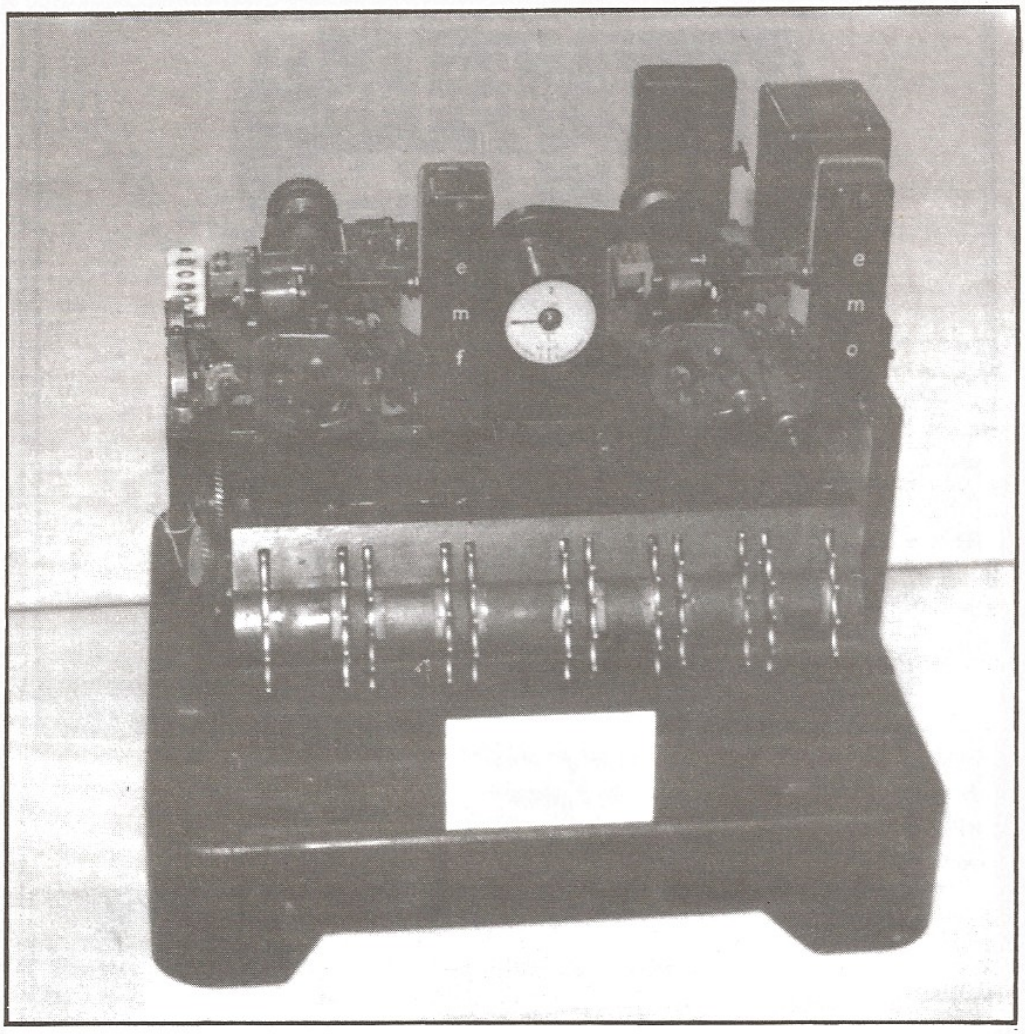
Schéma des liaisons allemandes « Fish » par SZ 40-42
(Evolution - novembre 1942 - juillet 1944)
Source : Hinsley - *British Intelligence in the Second World War*

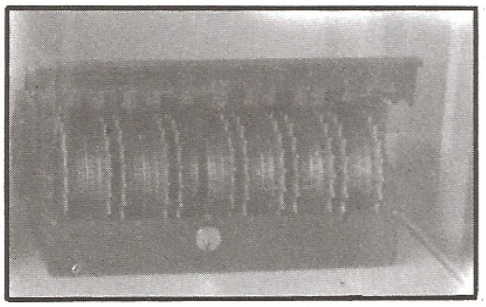


T 52 « E »



T 52 « D »





SZ 40-42

Bibliographie

1. D.W. Davies

a) The method of operation of the T 52 e cipher machine — One of the « Geheimschreibers », (29 pages).

b) The sequence of development of the Siemens and Halske T 52 cipher machine, (8 pages).

c) Port script to the report on the T 52 e cipher machine, (8 pages).

d) Second postscript to the report on the T 52 e cipher machine (3 pages). Tous ces documents sont dactylographiés.

2. D.W. Davies

The Siemens and Halske T 52 e cipher machine — In « Cryptologia », 6-1982, p. 289-308.

3. D.W. Davies

The early models of the Siemens and Halske T 52 cipher machine. In « Cryptologia », 7 - 1983 ; p. 235-253.

4. Hinsley (Prof. Sir F. Harry), E.E. Thomas, C.F. Ransom, R.C. Knight

British Intelligence in Second World War.
Volume 3 - Partie 1 - XV + 693 p.
H.M.S.O. Londres 1984.

Volume 3 - Partie 2 - XV + 1038 p.
H.M.S.O. Londres 1988.

5. Hinsley (Prof. Sir F. Harry)

« Cracking the Ciphers ».
Electronics & Power - juillet 1987, p. 453-455.

6. Mache Wolfgang (Dipl. Ing.)

Geheimschreiber.
In « Cryptologia », Octobre 1986, Vol. 10, N° 4, p. 230-241.

7. Mache Wolfgang (Dipl. Ing.)

British Intelligence in W.W. II and Siemens Cipher Teleprinters, 8 p. (dactylographiées).

8. Zorpette Glenn

Breaking the Enemy's Code.
In « EEE Spectrum », numéro de septembre 1987, p. 47-51.