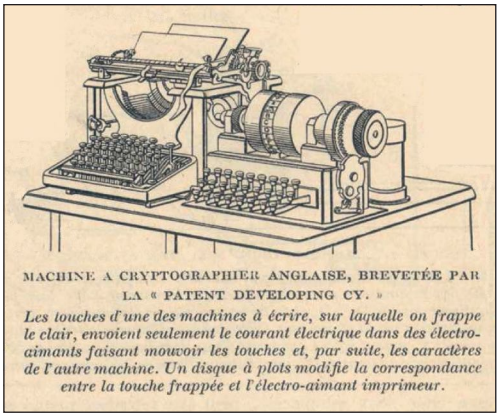
Les mathématiciens polonais contre Enigma

Philippe Guillot

Pendant la deuxième guerre mondiale, les messages chiffrés allemands étaient lisibles en clair presque simultanément par les Alliés, leur procurant un avantage qui a eu un impact notable sur le déroulement du conflit. À l'instar du film *The Imitation Game*, les récits de ce succès mettent en avant les travaux britanniques de Bletcheley Park. Pourtant, pendant la décennie 1932-1942, le bureau du chiffre polonais et son équipe de mathématiciens avait déjà accompli la prouesse de rendre transparentes à son État-major les communications chiffrées de l'armée allemande. Cet article est consacré au récit de cette passionnante épopée.

La machine Enigma dont se servaient les Allemands appartient à la famille des machines à chiffrer à rotor. Ces machines sont apparues au lendemain de la première guerre mondiale, dans un contexte de retour aux affaires après la fin des hostilités et de développement de la télégraphie sans fil. Plusieurs inventeurs ont déposé presque simultanément des brevets pour des machines semblables.



MACHINE A CRYPTOGRAPHIER ANGLAISE, BREVETÉE PAR LA « PATENT DEVELOPING CY. »

Les touches d'une des machines à écrire, sur laquelle on frappe le clair, envoient seulement le courant électrique dans des électro-aimants faisant mouvoir les touches et, par suite, les caractères de l'autre machine. Un disque à plots modifie la correspondance entre la touche frappée et l'électro-aimant imprimeur.

La science et la vie, mars 1923

L'américain Edward Hebern (1869-1952) avait d'abord imaginé, dès 1915, de relier deux machines à écrire électriques avec un câblage irrégulier de telle sorte qu'une touche actionnée sur une machine imprime une lettre différente sur l'autre machine. Ce procédé de substitution simple reproduit les régularités de la langue naturelle et est connu pour être facilement résoluble avec un peu d'entraînement. Hebern a corrigé cette faiblesse en insérant un tambour rotatif, qui tourne à chaque touche actionnée, faisant ainsi varier l'alphabet de chiffrement. Il dépose son brevet en 1918.

L'histoire des machines Enigma est digne des meilleurs romans d'espionnage économique. Dès 1915, en pleine première guerre mondiale et dans le plus grand secret, deux ingénieurs de la marine hollandaise, Theo van Hengel (1875-1939) et Rudolf Pieter Cornelis Spengler (1875-1955) mettent au point une machine à cryptographier à rotors. De retour à la paix, ils cherchent à breveter leur invention et s'adressent à une agence qui les fait patienter en attendant l'autorisation de la marine hollandaise. Avant que celle-ci n'arrive, Hugo Alexander Koch (1870-1928), beau-frère de l'employé de l'agence *Huybrecht Verhagen* dépose le 7 octobre 1919 le brevet d'une *machine à écriture secrète* au nom de l'entreprise, *Naamlooze Venootschap Ingenieursbureau « Securitas »* qu'il vient de fonder pour la circonstance. En 1927, il cède ses droits à l'ingénieur allemand Arthur Scherbius (1878-1929) qui avait auparavant déposé des brevets similaires. Scherbius a appelé ses machines *Enigma*. Les modèles A et B - étonnamment proches de la machine de Hengel et Spengler - comportent 4 rotors et sont lancés sur les marchés commerciaux, mais sans succès en raison de leur prix élevé. Le modèle C, est un modèle portatif et plus économique, avec trois rotors seulement. Le système d'impression est remplacé par un tableau d'ampoules. Le troisième rotor est relié à un tambour muni de contacts connectés entre eux sur une seule face et appelé réflecteur (*umkerhwalze*). L'impulsion électrique qui arrive sur ce tambour est alors réfléchie vers le rotor d'où cette impulsion est venue.

Apprenant en 1923 par l'ouvrage « *The World Crisis* » de Winston Churchill (1874-1965), que son dictionnaire de chiffrement, le *Signalbuch der Kaiserlichen Marine*, avait été compromis dès 1914, la *Reichsmarine* est à la recherche d'un chiffrement plus sûr et adopte l'Enigma en 1926. Elle est suivie par la *Reichswehr* en 1928.

En mars 1935, en violation du Traité de Versailles, Adolf Hitler (1889-1945) annonce le rétablissement du service militaire obligatoire et décide de porter l'effectif de l'armée de 100 000 à 500 000 hommes. La *Reichswehr* devient la *Wehrmacht*, la *Reichsmarine* devient la *Kriegsmarine*, la force aérienne la *luftwaffe* est rétablie et adopte à son tour l'Enigma. Le réarmement de l'Allemagne est en marche.

La machine Enigma, portable sur le front, d'un emploi facile, sera au cœur du nouvel art de la guerre allemand, la *Blitzkrieg*, et l'armée en fera fabriquer un grand nombre, dans cinq usines réparties sur tout le territoire afin de diversifier les sources. Selon les estimations, de 50 à 120 000 exemplaires seront produits jusqu'à la fin de la deuxième guerre mondiale. Une machine Enigma comporte un clavier de 26 touches qui permet d'écrire les 26 lettres. Il n'y a ni chiffre ni signe de ponctuation. L'espace entre les mots est représenté par un X, et la séparation des phrases par un Y. Au-dessus du clavier se trouve un tableau d'ampoules qui indique la lettre substituée.

Au-dessus du tableau d'ampoules se trouvent les trois rotors. Chacun comporte une couronne mobile qui peut se caler à l'aide d'un cliquet dans l'une des vingt-six positions.

Sur l'avant de la machine se trouve un tableau de fiches.

L'action d'une touche ferme un circuit électrique qui traverse le tableau de fiches, les trois rotors et un réflecteur qui renvoie le courant vers les trois rotors dans l'ordre inverse, puis à nouveau à travers le tableau de fiches pour finalement allumer une ampoule. En même temps, l'action sur la touche fait tourner le premier rotor d'un vingt-sixième de tour. Une fois que ce rotor a effectué une rotation complète, un ergot fait tourner

le second rotor d'un vingt-sixième de tour et pareillement pour le troisième rotor. La machine Enigma réalise ainsi une substitution polyalphabétique évolutive dont la période est $26 \times 26 \times 25 = 16900$ (et non pas 26^3 en raison d'un mécanisme qui faisait parfois avancer les deuxième et troisième rotors simultanément).

Machine Enigma le capot ouvert

L'action d'une touche coupe le circuit qui alimente sa propre ampoule. Une lettre ne peut pas être chiffrée par elle-même. C'est ce qu'on appelle le *principe d'exclusivité*.

Si l'action sur une touche, disons la touche *f* a pour effet d'allumer l'ampoule *b*, l'action sur la touche *b* a pour effet de faire circuler le courant dans le sens inverse jusqu'à allumer l'ampoule *f*. C'est le principe de réciprocité. Le chiffrement échange les lettres deux à deux, ce qui permet d'avoir la même machine avec le même positionnement pour chiffrer et déchiffrer. C'est d'une grande commodité du point de vue opérationnel, mais aussi une grave faiblesse que ne manqueront pas d'exploiter les cryptanalystes.

Chaque jour, l'opérateur doit configurer la machine dans une position donnée par la table des clés du jour. En voici par exemple un extrait au 4 mai 1937 :

Date	ordre	couronne	position
4 mai	III - I - II	16 - 11 - 13	01 - 12 - 22
fiches			
CO DI FR HU JW LS TX			

Ce jour, l'opérateur doit placer les rotors dans la cage dans l'ordre indiqué : le rotor III à gauche, le rotor I au milieu et le rotor II à droite. Il doit avoir calé les couronnes des trois rotors avec le cliquet calé dans la position indiquée : 16 pour le rotor de gauche, 11 pour celui du milieu et 13 pour celui de droite. Les rotors sont alors tournés pour faire apparaître le numéro indiqué par la quatrième colonne : 1 pour le rotor de gauche, 12 pour celui du milieu et 22 pour celui de droite. Les lettres indiquent les fiches à connecter entre elles sur le tableau de fiches : le *C* avec le *O*, le *D* avec le *I*, le *F* avec le *R*, etc.

Ensuite, avant de chiffrer un message, il y a un protocole bien précis à suivre, afin d'éviter que tous les messages d'une journée ne soient chiffrés avec la même séquence de substitutions. L'opérateur choisit trois lettres, par exemple *XFR* qu'il chiffre deux fois avec la clé du jour. Cela donne six lettres qui sont transmises dans l'en-tête du message et qui constituent la *clé de message*, cela peut donner par exemple *hui lkb*. Il positionne alors les rotors selon les trois lettres *XFR* qu'il a choisies, puis chiffre son message.

Au déchiffrement, l'opérateur procède de manière inverse. Il déchiffre l'en-tête *hui lkb*. Si tout s'est bien passé, il doit trouver deux fois *XFR XFR*. Il positionne alors les rotors selon ces trois lettres, puis déchiffre le reste du message.

Le traité de Versailles rend à la Pologne sa « Partition prussienne ». L'Allemagne ne cache pas son ambition de récupérer ces territoires à la première occasion, ce qui pousse les Polonais à se méfier de leur ambitieux voisin. Un centre d'écoutes est installé dans la ville de Poznań près de la frontière allemande. Les services de renseignements d'alors sont organisés autour d'un « *Bureau de renseignement des transmissions* » dirigé par Guido Langer (1894-1948) et d'un « *Bureau de cryptographie* » dirigé par Franciszek Pokorni, cousin de Hermann Pokorni, cryptologue qui a opéré dans l'armée austro-hongroise pendant la première guerre mondiale. Dans ce bureau, une section germanique BS4 est dirigée par Maksymilian Ciężki (1899-1951). Cette section résout tant bien que mal le chiffre rudimentaire des messages interceptés.

Mais à partir de 1926, l'adoption de l'Enigma change le chiffre et met en échec le BS4. Le trafic continue à être méthodiquement analysé, mais sans succès.

Un vendredi du début de l'année 1929, un incident survient au bureau des douanes dans lequel transite un colis en provenance d'Allemagne à destination d'une entreprise allemande de Varsovie. Un employé de cette entreprise insiste pour que ce colis, qui contient selon lui un équipement radio, soit retourné à l'envoyeur dans les plus brefs délais. Le bureau répond que cela sera fait dès lundi, le bureau des douanes étant fermé pour la fin de semaine. Mais l'insistance de cet employé met la puce à l'oreille des douaniers. Le doute n'est plus permis lorsque le consulat allemand lui-même intervient pour formuler la même requête. La douane fait alors appel au BS4 pour éclaircir cette affaire. Ciężki est appelé comme expert et requiert l'aide de deux anciens camarades qu'il a connu pendant l'insurrection de la Grande Pologne de 1918-1919, deux ingénieurs de la manufacture Radio AVA, par ailleurs radio amateurs passionnés d'ondes courtes : Ludomir Danilewics (?-1971) et Antoni Palluth (1900-1944). Cet événement scellera le début d'une coopération qui durera jusqu'en 1942. Les deux ingénieurs examinent le colis et se rendent compte que, contrairement à l'équipement radio annoncé, il contient une machine à chiffrer. Ils reconnaissent la machine Enigma qui était proposée sur le marché civil. Pensant trouver là la solution à leur problème, Ciężki s'en procure une. Mais le trafic ne parvient toujours pas à être décrypté.

Le bureau de cryptographie prend alors conscience de l'insuffisance de ses moyens. Le chiffre a changé de nature. Ce ne sont plus des substitutions ni des transpositions, mais une machine plus sophistiquée qui requiert d'autres compétences. Ils ont l'idée de recruter des mathématiciens, les seuls qui selon eux, pourraient apporter les idées nouvelles qui viendront à bout du problème.

En 1929, un cours de cryptographie est organisé à l'Université de Poznań, ouvert aux

étudiants en mathématiques. Ces cours sont assurés par Francizek Pokorni, qui s'appuie sur le cours de cryptographie de 1925 du Français Marcel Givierge (1871-1931), par Maksymilian Ciężki qui enseigne la résolution des chiffres allemands et d'Antoni Palluth, de la société Radio AVA. À l'issue de ce cours, trois brillants étudiants sont recrutés parmi la vingtaine d'inscrits : Marian Rejewski (1905-1980), Jerzy Różycki (1909-1942) et Henryk Zygalski (1906-1978). Le bureau de cryptographie tient ses trois recrues. L'année suivante, le cours de cryptographie n'est plus proposé.

Marian Rejewski (1905-1980)

Jerzy Różycki (1909-1942)

Henryk Zygalski (1906-1978)

Entre-temps, Les services de renseignements français ont confirmé auprès des Polonais, que l'armée allemande utilisait bien cette machine Enigma.

Le chiffre français avait connu de grands succès pendant la première guerre mondiale avec en particulier la résolution du « radiogramme de la victoire » qui a permis de faire connaître à l'État-major le lieu d'une offensive d'envergure aux alentours de Compiègne en juin 1918. Les dispositions avaient pu être prises pour la faire échouer. Mais après la guerre, ces services ont décliné et ne comportaient plus en 1923 que huit employés. Il devenait admis que les cryptogrammes produits par les nouvelles machines ne pouvaient plus être résolus par des attaques mathématiques, mais seulement par des opérations d'espionnage. Marcel Givierge lui-même, chef du chiffre de l'armée française de 1914 à 1917 admettait : « *De telles machines donnent des cryptogrammes que l'on peut théoriquement considérer comme indéchiffrables* ».

Le ministère de la guerre crée donc en 1930 une section D, chargé d'obtenir par tous les moyens des informations sur le chiffre des pays étrangers. À sa tête se trouve le capitaine Gustave Bertrand (1896-1976). Début juillet 1931, il reçoit de Rodolphe Lemoine (1871-1946), agent recruteur à Berlin, de son vrai nom Rudolf Stahlmann, alias Rex, agent double, une lettre émanant d'un certain Hans-Thilo Schmidt (1888-1943) lui proposant de « *négocier des documents de la plus haute importance* ». Le signataire est employé civil au *Chiffrierstelle*, ou *Chistelle*, le service du chiffre allemand, et frère de Rudolf Schmidt (1886-1957), Lieutenant-Colonel de l'armée Allemande par qui il a obtenu ce poste après un échec dans les affaires.

Une rencontre a lieu le 8 novembre 1931 à Vervier en Belgique où Schmidt montre aux Français plusieurs documents dont le manuel de la machine Enigma ainsi que son mode d'emploi pour les opérateurs. Ces documents sont estimés de grande valeur par Gustave Bertrand qui les photographiera en échange de la somme de 10000 marks, soit environ 24000 euros actuels.

Gustave Bertrand transmet les documents à ses collègues du service du chiffre mais reçoit une réponse très froide : « *Il s'agit d'une machine contre laquelle on ne peut rien faire, même avec vos documents* ».

Le 23 novembre, les documents sont transmis au représentant parisien des services de renseignement britanniques qui les envoie à Londres. Même réponse du *Government Code and Cipher School*, le GC&CS : « *Les documents n'ont pas la valeur suffisante pour que le GC&CS aide à en partager les coûts* ».

Bertrand se tourne alors vers ses contacts polonais, Gwido Langer et Maksymilian Ciężki, et là, l'accueil est enthousiaste. Les Polonais reconnaissent dans ces documents une solution pour remplir leur mission. Cela marque le début d'une coopération entre Bertrand, Schmidt, Langer et Ciężki. Hans-Thilo Schmidt sera désormais connu par son nom de code Asché (HE). Il fournira les clés du jour que différents services utilisaient pour l'Enigma. La coopération durera jusqu'en septembre 1938, date de la mutation d'Ashé au *Forschungsamt* (FA), le « bureau de recherche » où Ashé n'aura plus accès aux documents Enigma.

Les Britanniques ont aussi reçu ces documents, mais n'en n'ont rien fait jusqu'en 1938. Au début des années 1930, l'Allemagne n'était pas perçue comme une menace mais au contraire comme un rempart contre les bolcheviques.

L'agent recruteur Lemoine sera plus tard interrogé par l'Abwehr en février 1943. Pour sauver sa peau, il avouera la trahison de Hans-Thilo Schmidt. Ce dernier sera retrouvé mort en septembre 1943. Son frère Rudolf devenu général et malgré de brillants états de services, sera démis de ses fonctions et limogé de l'Armée.

La première mission des mathématiciens est de reconstituer le câblage interne de la machine utilisée par l'armée allemande qui diffère de la machine commerciale. Pour accomplir leur mission, ils ont à leur disposition les premiers documents d'Asché. Ils vont pour cela appliquer la théorie des permutations.

Rappelons que l'opérateur choisit trois lettres *a*, *b* et *c*. Ces trois lettres, sont répétées et subissent les six premières substitutions d'Enigma, qu'on note ici *A*, *B*, *C*, *D*, *E* et *F*. La clé de message est constituée des six lettres résultantes $x=A(a)$, $y=B(a)$, $z=C(c)$, $t=D(a)$, $u=E(b)$ et $v=F(c)$. Mais le chiffrement est réciproque, ce qui signifie que la substitution *A* transforme *a* en *x*, mais aussi *x* en *a*. Par conséquent, le produit de composition de *A* et *D* transforme *x* en *t*. Mais ici, *x* et *t* sont connus de l'intercepteur, car ces lettres font partie de la clé de message transmise dans l'en-tête du cryptogramme. De même, la composition de *B* et *E* transforme *y* en *u*, et la composition de *C* et *F* transforme *z* en *v*. En accumulant un nombre suffisant d'en-têtes de message, le cryptanalyste peut ainsi connaître entièrement les produits de composition *AD*, *BE* et *CF*. La solution au « *problème du collectionneur de coupon* » nous dit qu'il faut collecter en moyenne 74 messages pour récupérer la collection complète des 26 valeurs des substitutions *AD*, *BE* et *CF*.

Connaissant ces produits de composition il faut maintenant retrouver les permutations *A*, *B*, *C*, *D*, *E* et *F*. L'un des trois mathématiciens, Marian Rejewski, va utiliser un théorème qu'il a établi pour la circonstance :

Si deux permutations sont constituées de transpositions disjointes, ce qui est le cas des transformations opérées par Enigma, *alors leur produit contient un nombre pair de cycles disjoints*

de même longueur. Et réciproquement, si une permutation est constituée d'un nombre pair de cycles de même longueur, ce qui est le cas des produits *AD*, *BE* et *CF* connus, *alors elle est le produit de deux permutations constituées de transpositions disjointes*.

Mais la factorisation n'est pas unique. Par contre, le choix d'un élément et de son image dans deux cycles de même longueur impose les autres transpositions. Le nombre solutions possibles est assez limité, il vaut le produit des longueurs des cycles du produit.

Ici nos mathématiciens ont fait une supposition : les opérateurs, par facilité, choisissaient souvent des lettres identiques pour la clé de message, par exemple *jjj*, ou consécutives *abc*, ou voisines sur le clavier *qwe*. Cette hypothèse a été vérifiée assez souvent pour permettre de reconstituer les six premières substitutions *A*, *B*, *C*, *D*, *E* et *F*. La clairvoyance mathématique n'est pas la seule qualité du cryptanalyste. Rejewski écrira « *... le cryptanalyste ne connaît pas les préférences (des opérateurs), mais il essaye de compenser cette ignorance par de longs essais, de l'imagination et parfois un peu de chance* ».

Maintenant, notre équipe est en mesure de reconstituer le câblage interne du rotor de droite. Il fallait certes supposer qu'il était le seul à tourner pendant le chiffrement de la clé de message, mais cette hypothèse est vraisemblable. Selon la position de la couronne, elle se vérifie dans 20 cas sur 26. Il restait encore des inconnues pour exprimer la substitution réalisée par le rotor de droite. Cela a été résolu grâce aux clés du jour fournies par Ashé via les Français. Le câblage interne des autres rotors a pu être déterminé lorsque d'autres clés du jour les plaçaient à droite. Une fois les trois rotors connus, reconstituer le câblage du réflecteur est une formalité.

En janvier 1933, les plans de la machine sont fournis à la manufacture Radio AVA et une réplique *made in Poland* de la machine Enigma de la *Wehrmacht* est maintenant disponible au Bureau du Chiffre. Grâce encore aux clés du jour fournies par les Français, les messages interceptés sont maintenant régulièrement déchiffrés.

Mais ce résultat est insuffisant. Il faut pouvoir se passer des Français et trouver un moyen de reconstituer la clé du jour sans aide extérieure. L'équipe polonaise a tout d'abord, et pendant trois ans, de 1933 à 1936, appliqué des méthodes manuelles issues de la cryptanalyse classique. Citons l'une d'elle. Le comptage des lettres qui coïncident lorsqu'on superpose deux cryptogrammes, permet de décider si oui ou non ils sont issus de la même séquence de substitutions. En effet, si on superpose deux textes allemands l'un au-dessus de l'autre, on observe une lettre identique toutes les 13 lettres en moyenne. La même fréquence s'observe lorsque les deux textes ont subi les mêmes substitutions. Alors que si les textes sont des suites aléatoires de lettres, ou bien ont subi des substitutions différentes, on n'en observe qu'une sur 26 en moyenne. Compter les coïncidences sur des cryptogrammes différents permet de détecter le moment où le rotor du milieu a tourné. Supposons que le positionnement de la couronne du rotor de droite fait tourner le rotor du milieu lors du passage de *j* à *k*. Les positions des rotors seront par exemple *cli*, *clj*, *cmk*, *cml*, etc. Cette hypothèse sera validée en superposant un message dont la position initiale des rotors est *cmk* et en comptant les coïncidences. Cette méthode, découverte par Różycki, est appelée « méthode de l'horloge » à cause de la grosse horloge de la salle dans laquelle elle a été découverte. Les méthodes manuelles sont lentes, donnent un résultat partiel et incertain, et ne conduisent pas toujours à la clé du jour. Il fallait trouver autre chose.

Une percée a été accomplie en 1936. Les mathématiciens se sont rendu compte que la structure cyclique de substitutions *AD*, *BE* et *CF* pouvait caractériser l'ordre et la position initiale des rotors. Il existe six façons de disposer les trois rotors. Il existe 26 positions initiales possibles pour chaque rotor. Le nombre de combinaisons vaut 6 × 26 × 26 × 26 = 105 456. Si on pouvait disposer d'un catalogue qui, étant donné le nombre et la taille des cycles des permutations *AD*, *BE* et *CF*, pouvait indiquer les ordres et les positions initiales des rotors, il suffirait tout simplement de consulter ce catalogue pour en déduire une grande partie de la clé du jour. Constituer ce catalogue de plus de cent mille entrées a été un travail colossal. Il a fallu inventer un appareil qui puisse déterminer rapidement les cycles des substitutions *AD*, *BE* et *CF*. Cet appareil, appelé *cyclomètre* est constitué de deux jeux de rotors et du réflecteur. Son schéma électrique est d'une remarquable simplicité. L'action de l'un des vingt-six interrupteurs ferme le circuit électrique. Le courant passe alors dans un va-et-vient entre les deux jeux de rotors pour circuler alternativement dans un sens et dans l'autre et allumer les ampoules du cycle dans un circuit série. Il suffit de compter le nombre d'ampoules allumées pour connaître la taille du cycle. On actionne ensuite un interrupteur dont l'ampoule ne s'est pas encore allumée pour connaître la taille d'un autre cycle. Et ainsi de suite jusqu'à connaître toute la structure cyclique. Quelques secondes suffisent pour chaque combinaison. Une fois le catalogue établi, la clé du jour se retrouve en quelques minutes.

En novembre 1937, le câblage interne du réflecteur change. Un nouveau catalogue a dû être établi, ce qui a été fait avant la fin de l'année 1937. Début 1938, les Polonais décryptaient alors quotidiennement les messages de la *Wehrmacht* et de la *Luftwaffe*.

Mais le 15 septembre 1938, les messages devinrent à nouveau incompréhensibles. Après l'annexion de l'Autriche le 15 mars 1938, Hitler poursuit sa politique d'expansion et réclame le rattachement au Reich de la région des Sudètes, région germanophone de la Tchécoslovaquie. Avec cette montée de la tension, le mode opératoire d'Enigma change. Les Allemands voulaient éviter que toutes les clés de messages ne soient chiffrées avec l'unique position des rotors de la clé du jour. L'opérateur choisit désormais la position des rotors qu'il transmet en clair pour chiffrer la clé de message. Il chiffre ensuite deux fois les trois lettres qu'il a choisies comme position initiale des rotors pour le reste du message. Un en-tête de message pouvait par exemple être :

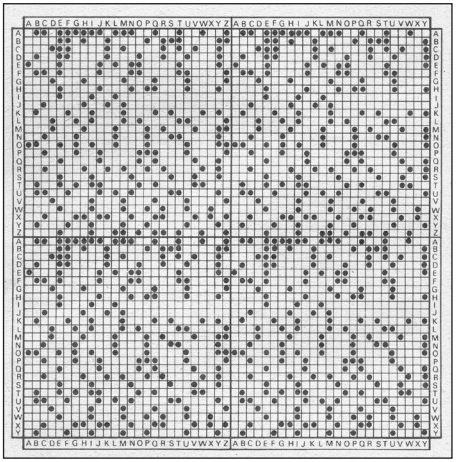
gkd wav wha.

Les trois premières lettres indiquent les positions des rotors pour le chiffrement de la clé de message et les six suivantes sont le résultat du chiffrement deux fois de la position des rotors pour le reste du cryptogramme. La position réelle des rotors reste inconnue du cryptanalyste, car elle dépend aussi du positionnement secret des couronnes. Par contre, l'information transmise en clair informe sur les positions relatives des rotors entre eux. Les permutations *AD*, *BE* et *CF* ne sont plus accessibles dans leur totalité, et le catalogue des cycles est inopérant.

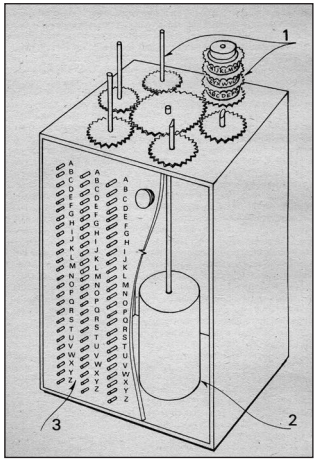
Les Polonais n'ont pas renoncé et ont poursuivi la démarche qui avait jusqu'alors conduit à leur succès. Dans l'exemple ci-dessus, on observe que l'image de *w* par la substitution *AD* est la lettre *w*. C'est un point fixe, c'est-à-dire finalement un cycle de taille 1. Les mathématiciens s'en sont contentés. Tout d'abord, un calcul de probabilités montre qu'environ une clé de message sur neuf comprend un point fixe dans l'une des 3 positions possibles. D'autre part, le catalogue a montré que l'observation d'un point fixe

permet d'éliminer 40 % des clés du jour. En interceptant environ 180 messages, on peut espérer disposer de l'information suffisante pour reconstituer l'ordre et la position initiale des rotors. Il fallait donc établir une sorte de catalogue des points fixes. Cela a d'abord été réalisé sous la forme de *plaques perforées* sur une idée d'Henryk Zygalski.

Il faut un jeu de plaques pour chaque ordre des rotors et pour chaque position initiale du premier rotor, soit un total de $6 \times 26 = 156$ jeux. Sur chaque plaque, l'abscisse représente la position du deuxième rotor et l'ordonnée celle du troisième rotor. Un trou est fait à cet endroit s'il existe un point fixe dans la permutation *AD* pour cette position. Pour avoir les points fixes de la permutation *BE*, il suffit de décaler la position du premier rotor d'un rang. Pour utiliser ces plaques, on récupère des messages dont l'en-tête présente un point fixe, c'est-à-dire une lettre identique à la 1re et 4e position, ou bien à la 2e et 5e position, ou bien à la 3e et 6e position. On empile les plaques perforées sur une table lumineuse en décalant les plaques selon les lettres données par le premier trigramme de la clé de message. S'il y a une perforation commune à toutes les plaques, c'est que la configuration des rotors correspondante réalise tous les points fixes observés. Cette configuration des rotors révèle la clé du jour. Avec cette méthode, la clé du jour peut être retrouvée en quelques heures.



Plaque perforée



Bomba

En même temps que cette technique de plaques perforées, Jerzy Różycki a imaginé une machine électromécanique : la *Bomba*. Ce terme signifie *magnifique*, *superbe*. Il désigne aussi une glace à la vanille nappée de chocolat à la mode à Varsovie à cette époque. Pour expliquer ce nom, on évoque aussi parfois le tic-tac que faisait la machine en fonctionnement, ou encore que cette machine allait détruire les cryptogrammes allemands.

Pour que cette machine fonctionne, il faut disposer de trois messages avec la même lettre comme point fixe. Peu importe que ce point fixe soit en 1re, 2e ou 3e position, mais il faut que ce soit la même lettre. Supposons par exemple avoir intercepté trois messages dont les en-têtes sont :

cku amt smu, *rtz mrk mpw*, *uyl mib msr*.

La lettre *m* est point fixe en deuxième position dans le premier message et en première position dans les deux autres. Le nombre de messages qu'il faut intercepter pour espérer avoir cette situation n'est pas si élevé. Il est donné par le *paradoxe des anniversaires*. En interceptant 144 messages, on a plus d'une chance sur deux de disposer de trois messages convenables. D'un autre côté, très peu de configurations des rotors peuvent conduire à cette situation, ce qui rend ce critère très discriminant. Une bomba comprend 6 jeux de rotors en trois paires qui détectent chacune un point fixe à la position observée. Un moteur fait tourner les rotors au rythme de 2,7 pas par seconde, ce qui fait qu'en 105 minutes, soit moins de deux heures, toutes les combinaisons sont explorées. Les pièces pour réaliser ces bombas sont commandées en octobre 1938 à Radio AVA. Elles sont livrées le 10 novembre. L'assemblage est réalisé dans le plus grand secret dans les locaux du BS4, et à partir de ce moment, les clés du jour sont systématiquement retrouvées en moins de deux heures!

Près de deux mois plus tard, le 15 décembre 1938, certains messages redevinrent incompréhensibles. Le renseignement polonais avait informé les mathématiciens de la mise en service de deux nouveaux rotors. Le nombre d'agencement des rotors passe de 6 à 60, soit dix fois plus. Par malheur les nouvelles procédures ne permettent plus de retrouver le câblage interne comme en 1932! Par chance le *Sicherheitsdienst*, le service de renseignements du parti Nazi n'a pas changé son mode opératoire et l'interception de ses messages a permis de reconstituer le câblage interne des deux nouveaux rotors.

Les plaques perforées ont dû être mises de côté. Il aurait fallu désormais 1560 jeux au lieu de 156 existants! Le travail pour les établir était hors de portée de moyens de l'équipe. Les Bombas pouvaient encore fonctionner, mais il aurait fallu en construire 60, ce qu'interdisaient les finances du bureau du chiffre. On pouvait toujours les utiliser les unes après les autres, mais la recherche d'une clé du jour pouvait prendre jusqu'à 17 heures.

Parallèlement, désespéré de n'avoir aucun retour, Gustave Bertrand a suggéré à Langer l'idée saugrenue d'utiliser des messages en clair obtenus par un agent informateur pour persuader les Allemands qu'Enigma était cassée et les conduire à abandonner son usage. Cette idée était bien sûr insupportable à Langer qui aurait vu s'effondrer près de dix années de travail. Il a réussi à persuader Bertrand de consulter les Britanniques avant de prendre cette mesure drastique. Une rencontre à l'initiative des Polonais, réunissant les responsables français, britanniques et polonais, s'est tenue les 9 et 10 janvier 1939 à Paris, dans les locaux du *Service de Renseignements* français aux Invalides. Mais les Polonais avaient ordre de ne rien révéler de leur savoir-faire. Dans son compte rendu, Dilly Knox a qualifié les Polonais de « sots ignorants ».

Mais ensuite, la situation internationale s'est encore dégradée: Invasion de la Tchécoslovaquie le 14 mars, Français et Britanniques assurent la Pologne de leur soutien en cas d'attaque allemande, en réponse, Hitler déclare nul et non avenu l'accord de non-agression signé en 1934, les discours d'Hitler se font de plus en plus anti-polonais. Le décryptement des messages allemands montre aux Polonais que les divisions de la Wehrmacht s'amoncellent aux abords de la frontière. Les Polonais organisent alors une deuxième rencontre avec les Français et les Britanniques les 24 et 25 juillet 1939 à Pyry, dans la banlieue de Varsovie. La délégation française était menée par Gustave Bertrand accompagné d'un cryptologue, le Capitaine Henri Braquenié. La délégation britannique comprenait

Alastair Denniston (1881-1961), chef du GC&CS et son principal cryptologue Dillwyn Knox (1884-1943), ainsi que le Commandant Humphrey Sandwith (1881-?), fondateur et chef des stations d'interception de la Royal Navy.

Devant un public ébahit, les Polonais ont alors tout raconté : comment ils ont reconstitué puis construit une réplique de la machine Enigma militaire, comment les plaques perforées et les bombas permettent de reconstituer la clé du jour. C'était le premier retour pour Gustave Bertrand qui a enfin appris à quoi ont servi les nombreux documents qu'il avait inlassablement continué à transmettre. Les Britanniques ont particulièrement apprécié cette réunion, cars ils avaient mis depuis peu une équipe en place pour résoudre Enigma, mais sans succès.

Cette rencontre de Pyry est « l'inestimable cadeau des Polonais » à leurs alliés. Ils leur ont offert deux répliques d'Enigma qui ont voyagé vers Paris par la valise diplomatique. Un exemplaire a ensuite traversé la manche le 16 août 1936 par le train Paris-Londres *Golden Arrow*. Pour ne pas éveiller les soupçons des services de renseignement allemands, elle a voyagé dans les valises de l'auteur dramatique Sacha Guitry (1885-1957) et son épouse la chanteuse et actrice Yvonne Printemps (1894-1977).

Les événements se précipitent. Le 1er septembre, les divisions blindées allemandes pénètrent en Pologne, en particulier, hasard de l'histoire, la 1re DB commandée par le Général Rudolf Schmidt, frère de Hans-Thilo Schmidt qui fournissait les Français en documents. Le 3 septembre, la France et la Grande Bretagne déclarent la guerre à l'Allemagne. Les défenses polonaises craquent face à la supériorité allemande. Le biuro szyfrow est évacué, et les traces de son travail sont détruites. L'équipe polonaise est évacuée pour atteindre un camp de réfugiés en Roumanie.

Les trois mathématiciens préfèrent prendre un train pour Bucarest où ils prennent tout d'abord contact avec l'ambassade britannique. Ils essuient un refus poli, les Anglais ayant fort à faire avec leurs propres ressortissant. Ils se tournent alors vers l'ambassade de France en se réclamant de Gustave Bertrand. Ce nom résonne comme un sésame. Les Français leur procurent papier, visa, argent et billets de train. Ils atteignent Paris le 25 septembre 1939 après un périple qui les fait passer par Belgrade, Zagreb, Trieste puis Turin. Un peu tard, les Britanniques leur ont proposé un refuge à Londres que les Français ont refusé, tout comme ces derniers ont décliné la proposition anglaise de monter un centre cryptologique commun en France. Gustave Bertrand part lui-même récupérer Langer et Cielski dans le camp de réfugiés en Roumanie et les ramène à Paris le 1er octobre 1939.

L'équipe polonaise est rassemblée dans un lieu tenu secret situé en banlieue parisienne à Gretz-Armainvilliers en Seine-et-Marne, au Château de Vignole. Elle a reçu le nom d'Ekipa Z. Ils disposent de trois répliques d'Enigma et commencent un travail de décryptement alimenté par les centres d'écoute français. L'ancien ingénieur de Radio AVA Antoni Palluth, membre de l'Ekipa Z, en démonte une pour en dresser les plans et passer commande à une entreprise française. Cette machine ne sera disponible qu'en juillet 1940.

Depuis 1938, les Anglais avaient pris conscience du danger que présentait l'Allemagne et ont reproduit presque à l'identique, mais avec davantage de moyens, ce que les Polonais avait mis en place six ans plus tôt. Ils ont organisé des cours de cryptologie à destination de mathématiciens comme John Jeffrey (1918-1944), Alan Turing (1912-1954) et Gordon Welchman (1906-1985). Le GC&CS est transféré en secret dans le manoir victorien

de Bletcheley Park à 80 km au nord de Londres. Après la révélation de Pyry, les Anglais ont alloué 12 000 livres à la réalisation de répliques d'Enigma et ont entamé la fabrication des 1 560 jeux de plaques perforées devenus nécessaires après la mise en place des deux rotors supplémentaires. Ces plaques seront achevées en janvier 1940. PC Bruno et Bletcheley Park travaillent alors en étroite coopération. Alan Turing fait le voyage pour Paris et rencontre l'équipe polonaise au château de Vignole le 17 janvier 1940 pour y apporter un jeu de plaques perforées et des informations sur une machine Enigma de la *Reichsmarine* capturée par les Anglais sur un sous-marin allemand, montrant l'existence, sur ces machines, d'un sixième et d'un septième rotor. Les deux équipes décryptent les messages. La proportion, 17 % pour PC Bruno et 83 % pour Bletcheley Park est à l'image des moyens alloués aux deux équipes.

Le 1er mai 1940, les messages allemands ne parviennent plus à être décryptés. La position initiale des rotors n'est plus répétée dans la clé de message, rendant totalement inopérantes les méthodes de décryptement.

Le 10 mai 1940, l'armée allemande engage une offensive d'envergure contre la Hollande, le Luxembourg, la Belgique puis la France. Pendant cette offensive, les messages restent illisibles. Une solution est trouvée à Bletcheley Park par John Herivel (1918-2011). À partir du 21 mai, certains messages redeviennent lisibles.

La débâcle de l'armée Française et les progrès de l'offensive allemande conduisent à la signature de l'armistice entre la France et l'Allemagne le 22 juin 1940. Le PC Bruno est évacué le 26 juin vers Alger via Oran.

Les services de renseignements se reconstituent de manière clandestine sous l'initiative du général Maxime Weygand (1867-1965), ministre de la guerre du premier gouvernement de Vichy. L'équipe franco polonaise sera reconstituée en zone non occupée, au château de Fouzes près d'Uzès sous le nom de PC Cadix. Les Polonais recevront le nom de code d'Eksposytura 300, le poste 300. Ses membres vivront clandestinement sous des noms d'emprunt. Marian Rejewski sera « Pierre Raneau », un professeur de mathématiques du lycée de Nantes. Ce centre déchiffrera les messages allemands avec les clés fournies par Bletcheley Park, l'activité scientifique de décryptement ayant alors été entièrement prise en charge par les Anglais.

Jerzy Różycki périra noyé lors du retour d'une mission à Alger le 9 janvier 1942.

Ce centre sera évacué en novembre 1942 suite à la détection d'une activité radioélectrique anormale par l'occupant allemand. Le matériel sera emmuré en catastrophe. Après de nombreuses péripéties, les Français seront évacués par avion vers l'Algérie, les Polonais fuiront à pied vers l'Espagne avec des fortunes diverses.

Les deux mathématiciens survivants traverseront les Pyrénées, ils seront arrêtés en Espagne puis s'évaderont avec la complicité de partisans polonais, ils gagneront le Portugal, puis l'Angleterre où ils passeront le reste du conflit au sein de l'armée polonaise libre. Apprenant l'arrivé des mathématiciens polonais en Angleterre, Bertrand s'est écrié « Quelle aubaine pour les Anglais ! ». Ils seront pourtant tenus à distance des travaux de Bletchley Park et n'auront plus aucun contact avec les cryptanalystes anglais qui étaient tenus au plus grand secret.

Les chefs Langer et Ciężki seront trahis par leur guide lors du passage en Espagne. Ils

seront internés au Stalag 122 à Compiègne, puis au camp d'internement de Schloss Eizenberg en Tchécoslovaquie. Découvrant qui ils étaient, la Gestapo (*Geheime Staatspolizei*, la police secrète d'état) les a interrogés en mars 1944. Ils ont dû avouer que les Polonais arrivaient à résoudre les messages allemands avant le conflit mais que leurs méthodes ne fonctionnaient plus avec les nouvelles procédures mises en place en 1938, rendant la machine Enigma réellement invincible. Leurs interrogateurs ont été satisfaits de ces réponses qui correspondaient à ce qu'ils voulaient entendre et n'ont pas poussé plus loin leurs investigations. Langer et Ciężki seront libérés par les troupes américaines en mai 1945 et rejoindront Londres où ils recevront un accueil très froid de la part de leurs compatriotes, accusés d'être responsables des échecs de l'évacuation du PC Cadix. Ils seront envoyés au camp des troupes des transmissions polonaises de Kinross en Écosse. Tous deux finiront leur vie misérablement en Grande Bretagne. Langer mourra le 30 mars 1948 et Ciężki le 5 novembre 1951 après avoir vécu les trois dernières années de sa vie des allocations du Bureau d'Assistance.

Les travaux ne seront révélés au public qu'en 1967 avec la publication en Pologne de l'ouvrage de Wladyskaw Kozaczuk, *Bitwa a tajemnic*e (Bataille secrète).

Gustave Bertrand continuera sa carrière militaire après la victoire des Alliés. Il sera promu Général et décoré par Charles de Gaulle au grade de Grand Officier de la Légion d'Honneur. Après sa retraite de l'armée en 1950, il sera élu maire de Théoule-sur-Mer dans les Alpes Maritimes. Il s'éteint à Toulon le 23 mai 1976 après avoir publié en 1973 son témoignage, *Enigma ou la plus grande énigme de la guerre 1939-1945*.

Henryk Zygalski est resté en Angleterre après le conflit, où il a enseigné les mathématiques au *Battersea Technical College* et à l'université de Surrey au sud-ouest de Londres. Il décède à Plymouth le 30 août 1978.

Marian Rejewski a été démobilisé en 1946 et est retourné en Pologne pour vivre avec sa famille aux côtés de ses parents dans la ville de Bydgoszcz. Il a choisi de ne pas reprendre le poste de mathématicien qu'on lui a proposé à l'Université de Poznań. Il a occupé divers emplois jusqu'à devenir comptable à l'Union Provinciale des Coopératives Ouvrières en 1954, poste qu'il a occupé jusqu'à sa retraite en 1967. Il est resté très discret sur son activité de cryptologue jusqu'à la révélation de son implication dans la cryptanalyse de la machine Enigma en 1973. Il a alors donné plusieurs interviews à la radio et à la télévision pour relater son aventure. Il a reçu ensuite plusieurs distinctions dont la très prestigieuse *Croix d'Officier de l'Ordre Polonia Restituta* – l'Ordre de la Renaissance de la Pologne. Il est le seul de l'équipe à avoir été officiellement reconnu de son vivant. Il meurt le 13 février 1980 à son domicile de Varsovie des suites d'une attaque cardiaque et est enterré avec les honneurs militaires au cimetière de Powązki à Varsovie.

Au regard des moyens modestes qui lui ont été alloués, l'équipe polonaise a connu de remarquables succès. Elle a su rapidement s'adapter aux différentes évolutions du mode opératoire. Un facteur essentiel de succès a été le travail d'une équipe constituée de mathématiciens formés à la cryptologie et d'ingénieurs concevant rapidement des moyens originaux de calcul : plaques perforées et bombas. Forts de moyens humains et matériels plus importants, les Britanniques de Bletchley Park suivront la voie tracée par les Polonais, sauront faire évoluer les idées et améliorer les solutions avec le succès que l'on connaît.

Bibliographie

Bauer Friedrich, *Decrypted Secrets*, New York, Springer, 2007.

Bertrand Gustave, *Enigma ou la plus grande énigme de la guerre 1939-1945*, Paris, Plon, 1973.

Gaj Kris & Orklowski Arkadiusz, *Facts and myths of Enigma: breaking stereotypes*, Eurocrypt 2003 Proceedings, Lecture Notes on Computer Science 2656, pp 106-122.

Garlinsky Jozef, Intercept, *The Enigma War*, Londres, Magnum book, 1979.

Kahn David, *The Codebreakers, The comprehensive History of Secret Communicationjs from the Ancient Times to the Internet*, New York, Scribner, 1996.

Kahn, David, *Seizing the Enigma, The Race to Break the German U-boats Codes 1939-1943*, Londres, Frontline Books, 1998.

Kozacsuk Wladyslaw & Straszak Jersy, *Enigma, How the Poles Broke the Nazi Code*, New York, Hippocrene Books, 2004.

Medrala Jean, *Les réseaux de renseignements franco-polonais, 1940-1944*, Paris, L'Harmattan, 2005.

Rejewski Marian, *An application of the Theory of Permutations in Breaking the Enigma Cipher*, Applicationes Mathematicae, 16, n°4, Varsovie, 1980.

Rejewski Marian, *Memories of my work at the Cipher Bureau of the General Staff Second Department, 1930-1945*, Adam Mickiewicz University Press, réédité en 2013.

Ribadeau Dumas Louis, *Les décryptements des machines Enigma allemand*es, Bulletin de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI), Numéro hors-série juillet 2005.

Stengers Jean, *Enigma, the French, the Poles and the British 1931-1940*, Revue belge de philologie et d'histoire. Tome 82, fasc. 1-2, 2004. Histoire médiévale, moderne et contemporaine, pp 449-466.

Winterbotham Frederik, *The Ultra Secret*, Londres, Weidenfeld & Nicolson, 1974.