L’histoire de la rupture de l’Enigma commence en 1919. Après 123 ans de captivité, la Pologne renaissante, juste après la Première Guerre mondiale, doit à nouveau lutter pour sa liberté.

Le jeune État polonais doit se défendre et empêcher l’armée soviétique de prendre le contrôle de l’Europe, à l’époque du Bureau du Chiffre - la Section du Chiffrement fondée par le lieutenant Józef Serafin Stanślicki.

Déjà en 1919, juste après avoir recouvré son indépendance, Jan Kowalewski, organisateur et chef du département de la deuxième radio du bureau du chiffre du second département de l'état-major du commandement suprême en 1919-1924, avait brisé les premières clés de chiffrement de l'Armée rouge, permettant la lecture de la correspondance bolchevique sur les fronts de la guerre civile en Ukraine En janvier 1920, il commence à percer les chiffres allemands.

Le Bureau des chiffres a été l’un des premiers entretiens de l’histoire à renoncer aux linguistes, aux maîtres d’échecs et à d’autres, et a employé des mathématiciens de la célèbre école de mathématiques polonaise (Université de Lviv et Université de Varsovie), Stanisław Leśniewski, Stefan Mazurkiewicz et Wacław Sierpiński.

La célèbre école mathématique polonaise d'avant-guerre comprenait, entre autres, Stefan Banach, Hugo Steinhaus, Stanisław Mazur, Kazimierz Kuratowski et Stanisław Ulam - le créateur de la méthode de Monte-Carlo - avec le hongrois Edward Teller, ils créèrent la bombe thermonucléaire américaine.

Bydgoszcz ul. Wileńska, ici est née Marian Rejewski, n’avait que quelques années lorsque deux officiers de la marine néerlandaise Theo Van Hengel et Rudolf Sprengler construisirent en 1915 une machine de cryptage rotative. Les Pays-Bas sont un pays neutre et veulent cacher leurs informations à l'anglais et à l'allemand. Deux exemplaires de ces machines ont été construits et ont été utilisés dans l'est de l'Indonésie.

Les officiers néerlandais étaient réticents à déposer un brevet. Hugo Alexander Koch, un inventeur néerlandais, en fait la demande. Il obtint le brevet n ° 10 700 pour une machine à chiffrement rotatif, qu'il avait demandée aux Pays-Bas le 7 octobre 1919.

Hugo Alexander Koch n'était pas le seul à avoir déposé un brevet pour une machine à chiffrer en 1919. Artur Scherbius a également reçu un brevet pour une machine de cryptage électromécanique. La même année, il a fondé Ernst Richard avec Schebius & Ritterw, la société a également acheté les droits de brevet détenus par Hugo Koch.

En 1923, une machine à chiffrement rotative fabriquée par Scherbius & Ritterwas, connue sous le nom d'Enigma, est présentée pour la première fois. Initialement, il était vendu dans une version commerciale à quiconque souhaitait dissimuler sa correspondance.

En 1926, la marine allemande modifie l'Enigma civile et commence à chiffrer ses messages à l'aide de cette machine modifiée, tandis que la version civile d'Enigma est progressivement retirée du marché.

En juillet 1928, les stations de radio militaires allemandes ont commencé à diffuser les premiers messages cryptés avec Enigma. Les services secrets polonais interceptent la correspondance, mais les cryptologues de la section allemande du Bureau de chiffrement polonais ne sont pas en mesure de déchiffrer le code et de ne plus y travailler, de même que les services de renseignement français et britanniques.

En janvier 1929, le major Gwido Langer devient chef du département de recherche radio. Il est bientôt nommé chef du bureau du chiffrement, adjoint du major Langer et capitaine. Maximilian Heavy.

La direction de BS-4 ne veut pas accepter l'impossibilité de lire des messages cryptés de l'armée allemande. La même année, des employés du département Radio et Chiffrement, le major Franciszek Pokorny, le capitaine Maksymilian Ciężki, un employé du Bureau civil, Antoni Palluth et le professeur Zdzisław Krygowski dirigent un cours de cryptologie secrète. , pour certains étudiants en mathématiques de l’allemand à l’Université de Poznań.

L’Université de Poznań n’ayant pas été choisie par hasard, la direction du Bureau du chiffrement était consciente du fait que les étudiants locaux connaissaient parfaitement la mentalité, la culture et la langue d’un ennemi potentiel comme l’Allemagne. Le professeur Krygowski choisit parmi les étudiants des deux dernières années un groupe de 20 personnes qui participent à un cours de cryptologie secret. Après avoir terminé le cours, trois des étudiants les plus talentueux sont sélectionnés: Marian Rejewski, Jerzy Różycki et Henryk Zygalski, qui commencent à travailler pour la branche du bureau de Cipher de Poznań. Après deux ans, les Polonais tentent à nouveau de casser le code Enigma. En septembre 1932, la succursale de Poznań fut fermée et trois mathématiciens signèrent un contrat avec le bureau de chiffrement, en devinrent les employés civils et furent mutés à Varsovie. Ils travaillèrent intensément à briser le code Enigma.

Marian Rejewski à partir de matériaux (textes cryptés, livre de code des réglages de la machine à chiffrer pour septembre et octobre 1932) fournis au Bureau des chiffres par le général des services de renseignements français Gustave Bertrand, que les services de renseignement français ont achetés à l'espion allemand pour la France Hans-Thilo Schmidt, pseudonyme d'Asché, en utilisant la théorie des groupes, en particulier le théorème de permutation, a recréé les connexions internes des rotors et des cylindres inverseurs.

Marian Rejewski, dans ses mémoires de 1980, écrivait que les mêmes conclusions auraient pu être tirées sans les données obtenues des services de renseignement français, mais que cette méthode serait imprécise et fastidieuse et devrait s'appuyer fortement sur le hasard. Après que Marian Rejewski ait développé les connexions internes pour Enigma militaire, le bureau de chiffrement polonais a chargé AVA Radio Company de construire un équivalent d'Enigma conforme aux spécifications de Rejewski. Les premiers messages de l'armée allemande cryptés avec Enigma ont été cassés.

Marian Rejewski se souvient: nous avions maintenant une machine, mais nous n'avions pas les clés et nous ne pouvions pas demander au général Bertrand de les remettre tous les mois ... la situation était inverse. Il devint nécessaire de développer des méthodes pour trouver les clés quotidiennes.

L’amélioration constante de la procédure de chiffrement et de l’Enigma elle-même du côté allemand a obligé les mathématiciens polonais à créer de nombreuses méthodes de déchiffrement.

La première était une méthode manuelle fastidieuse à grille, supposant que seules six paires de lettres étaient échangées sur le connecteur de câble et que les quatorze lettres restantes étaient inchangées.

La méthode de l'horloge de Różycki en est une autre, qui permet de déterminer avec une grande probabilité quel rotor se trouve à la position la plus à droite de la machine un jour donné.

Après le 1 er octobre 1936, les Allemands ont modifié leurs procédures de codage en augmentant le nombre de connexions sur le tableau Enigma. En conséquence, la méthode de la grille perdit beaucoup en efficacité, mais inventée entre-temps, vers 1935 ou 1936, la méthode SDS était indépendante du nombre de connexions sur le tableau. Le catalogue de cartes a été construit à l’aide d’un dispositif développé par Rejewski, appelé cyclomètre, qui calculait les permutations cycliques. Après avoir sauvegardé toutes les caractéristiques du catalogue, il était possible de lire les permutations appropriées correspondant aux réglages du rotor pour un jour donné.

Le cyclomètre constitué de deux ensembles de rotors Enigma a été utilisé pour déterminer la longueur et le nombre de cycles de permutation générés par Enigma. Même avec l'aide de cet appareil, la création d'un catalogue complet de caractéristiques était une tâche difficile et fastidieuse. Pour chacune des 17576 positions dans lesquelles la machine a pu être configurée, il a fallu analyser six séquences d’alignement du rotor possibles, ce qui a donné 105 456 résultats. La préparation du premier catalogue a pris un an de travail, mais une fois achevée vers 1935, il était possible de déterminer la clé journalière en 12 à 20 minutes.

Au début du mois de novembre 1937, la partie allemande changea le rouleau inverseur Enigma, ce qui obligea tout le catalogue à être recalculé dès le début. Malgré ce changement intervenu en janvier 1938, le bureau du BS4 Cipher Bureau chargé de déchiffrer les chiffres allemands était en mesure de lire environ 75% des messages interceptés chiffrés avec Enigma. et, selon Rejewski, avec une légère augmentation des effectifs, il était possible de lire jusqu'à 90% des messages

À l'été 1937, le Bureau des chiffres est transféré dans un centre secret situé près de Pyr, dans la forêt de Kabacki, près de Varsovie. En août 1938, l’Allemagne introduisit de nouvelles règles pour l’encodage et l’envoi de clés journalières, qui rendaient toutes les techniques de décryptage d’Enigma obsolètes à l’époque. Les mathématiciens polonais développent de nouvelles méthodes pour trouver les paramètres et les clés Enigma. La bombe cryptologique de Rejewski est créée. Il s'agit d'un dispositif à moteur électrique créé à partir de la combinaison de six copies de la machine Enigma capable de trouver la clé journalière en environ 2 heures. Après l'introduction d'une autre modification du codage en janvier 1939 consistant à augmenter le nombre de connexions sur le tableau, la bombe perdit considérablement en convivialité.

Au même moment, Zygalski développa sa propre méthode basée sur des feuilles de papier perforées, appelées feuilles de Zygalski, indépendantes du nombre de paires de lettres remplacées sur le commutateur à câble. Cependant, à la fois la bombe de Rejewski et les feuilles de Zygalski ont de nouveau perdu leur utilité après que les Allemands ont introduit le 15 décembre 1938 une autre modification du codage consistant à étendre le jeu de rotors de deux nouveaux, ce qui complique à dix reprises le processus de déchiffrement. Pour pouvoir déchiffrer les nouveaux messages codés, il était nécessaire de construire 60 bombes cryptologiques et de créer autant de jeux de feuilles de Zygalski, mais le coût de la construction de nombreux outils a été 15 fois supérieur au budget du Cipher Bureau. En outre, une autre modification de codage introduite par les Allemands le mois suivant, consistant à augmenter le nombre de paires de lettres remplacées de 12 à 20 (passant à plus d'un millier de configurations possibles du commutateur), a encore réduit l'efficacité du décryptage des bombes.

En janvier 1939, lors d'une conférence à Paris, des représentants du Cipher Bureau rencontrent des services cryptologiques de Grande-Bretagne et de France. La partie polonaise est représentée par le colonel Gwido Langer et le capitaine Maksymilian Ciężki. La rencontre en France avait pour but de présenter la position des entretiens sur l’état d’avancement des travaux sur la rupture de l’énigme. Les représentants polonais restent silencieux, comme convenu précédemment dans le pays. La divulgation d'informations sur la fracture ne devait avoir lieu que si les parties française ou britannique réussissaient à déchiffrer l'Enigma. Les Britanniques et les Français n’ont pratiquement aucune connaissance en ce qui concerne la rupture de l’Enigma. Les Polonais ne sont pas impliqués dans la divulgation des résultats de leurs travaux.

L'été arrive, les invitations aux services de renseignement français et britanniques à la conférence Enigma sont envoyées à l'initiative du Bureau de chiffrement polonais. La réunion a lieu en juillet 1939, la partie française est représentée par Gustave Bertrand, l’anglais par Alastair Denniston Dillwyn Knox. Les deux délégations manifestent leur aversion et leur mépris pour la partie polonaise. Le 25 juillet 1939, les deux délégations se rendent à la station de radio de Pyry, où le colonel Gwido Langer et le capitaine Maksymilian Ciężki dévoilent le secret de la rupture de l'énigme avec le consentement du commandement de l'armée polonaise. Les mathématiciens polonais présentent des preuves mathématiques concernant la reconstruction de la machine et l'obtention de clés de réglage Enigma, ainsi que des dispositifs permettant le déchiffrement. À la fin de la réunion, ils déchiffrent le nouveau radiodepesh capturé.

L’anglais et le français reçoivent du polonais une copie d’Enigma ainsi que de la documentation permettant le déchiffrement. Le 15 août 1939, le GC & CS britannique s’installa dans le lieu ultra-secret de Bletchley Park, où le mathématicien britannique Alan Turing construisit une bombe cryptologique et décrypte Les chiffres allemands, qui, en fin de compte, changèrent considérablement le sort de la guerre, mais c'est une histoire complètement différente ........