L’histoire de la ~~rupture de l~~ cryptanalyse d’Enigma commence en 1919. Après 123 ans ~~de captivité~~ d'occupation , 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 à cette époque nait le Bureau du Chiffre - la Section du Chiffrement fondée par le lieutenant Józef Serafin Stańslicki.

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 (ce n'est pas très clair) (oui !)

en dans les années 1919-1924, avait ~~brisé~~ cassé 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~~ casser les chiffres allemands.

Le Bureau des chiffres a été l’un des premiers ~~entretiens~~ services (?? à vérifier) services de renseignement 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), comme 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.

~~À Bydgoszcz, Wileńska, Ulica, ici est~~ Marian Rejewski est né rue Wilenska à Bydgoszcz. Il 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~~ chiffrement rotative. Les Pays-Bas sont un pays neutre et veulent cacher leurs informations ~~à l'~~ aux anglais et ~~à l'~~aux allemands. 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.~~

Il obtint le 7 octobre 1919 aux Pays-Bas le brevet n ° 10 700 pour une machine à chiffrement rotatif.

Hugo Alexander Koch n'était pas le seul à avoir déposé un brevet pour une machine à chiffrer en 1919. Artur Scherbius en a également ~~reçu~~ obtenu un ~~brevet~~ pour une machine de ~~cryptage~~ chiffrement électromécanique. La même année, il a fondé Ernst Richard avec Schebius & Ritterw Scherbius & Ritterwas avec Ernst Richard, 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~~ elle était vendue 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~~ chiffrés avec Enigma. Les services secrets polonais interceptent la correspondance, mais les cryptologues de la section allemande du Bureau de chiffrement polonais Polonais du Chiffre ne sont pas en mesure de ~~déchiffrer~~ décrypter le code et de ne plus y travailler cessent d'y travailler (je n'ai pas compris), de même que les services de renseignements 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 du capitaine Maximilian Heavy, le remplaçant du major Langer et chef de la section allemande BS-4 étant alors le capitaine Maksymilian Ciezki.

La direction de BS-4 ~~ne veut pas accepter l'impossibilité de~~ n'accepte pas de ne pas pouvoir lire ~~des~~ les messages ~~cryptés~~ chiffrés 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 secret de cryptologie ~~secrète~~, pour certains étudiants ~~en~~ de mathématiques ~~de~~ en ~~l'~~ allemand de langue allemande en mathématiques à l'Université de Poznań.

L'Université de Poznań n'a ~~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 secret de cryptologie ~~secret~~. Après avoir terminé le cours, trois des étudiants les plus talentueux sont sélectionnés: Marian Rejewski, Jerzy Różycki et Henryk Zygalski. ~~, qui~~ Ils commencent à travailler pour la branche du bureau ~~de Cipher~~ du chiffre la délégation du Bureau du Chiffre de Poznań. Après deux ans d'interruption, les Polonais tentent à nouveau de casser le code Enigma. En septembre 1932, ~~la succursale~~ l'annexe la délégation du Bureau du Chiffre de Poznań fut fermée et trois mathématiciens signèrent un contrat avec le bureau ~~de chiffrement~~ du chiffre le Bureau du Chiffre, en devinrent les des 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, en s'appuyant sur les matériaux (textes cryptés, livre de code, etc de septembre et octobre 1932) fournis au Bureau du Chiffre par le général français du renseignement Gustave Bertrand, lequel renseignement les a acheté à l'espion allemand Hans-Thilo Schmidt, pseudonyme Asché, en utilisant le théorie des groupes et en particulier le théorème de permutation, a établi les connexions internes des rotors et des cylindres inverseurs.

Marian Rejewski en utilisant la théorie des groupes, en particulier le théorème de permutation, a recréé les connexions internes des rotors et des cylindres inverseurs, 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~~ du chiffres par le général des services de renseignements français Gustave Bertrand, matériaux que les services de renseignements français ont achetés à l'espion allemand pour la France Hans-Thilo Schmidt, pseudonyme d'Asché.

Marian Rejewski, dans ses mémoires de 1980, écrivait que les mêmes conclusions auraient pu être tirées sans les données obtenues des services de renseignements français, mais que cette méthode ~~serait~~ aurait été imprécise et fastidieuse et ~~devrait~~ aurait dû s'appuyer fortement sur le hasard. Après que Marian Rejewski ait développé les connexions internes pour Enigma militaire, le bureau de chiffrement polonais Bureau du Chiffre 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~~ décryptage.

La première était une méthode manuelle fastidieuse à grille, supposant que seules six paires de lettres étaient échangées sur le connecteur de câbles 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~~ pouvait être configurée, il ~~a fallu~~ fallait analyser six séquences d'alignement du rotor possibles, ce qui ~~a donné~~ donne 105 456 résultats. La préparation du premier catalogue a pris plus d'un an de travail, mais une fois achevée vers 1935, il était possible de déterminer la clé journalière en 12 à 20 minutes.