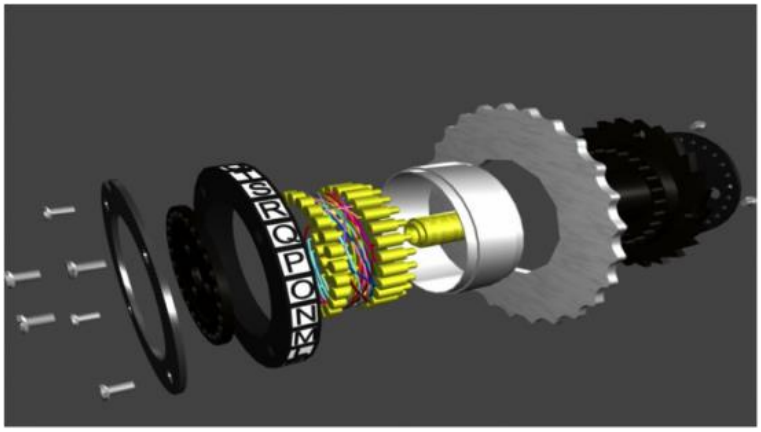
Machine Enigma

La machine Enigma, brevetée par l'ingénieur allemand Arthur Scherbius en 1918, est l'un des systèmes de cryptage les plus redoutables de l'histoire. C'est une machine à chiffrer électromécanique dont le chiffrement est à la fois simple et ingénieux : **Chaque lettre est remplacée par une autre mais le principe de substitution change d'une lettre à l'autre.**

Enigma, alimentée par une pile électrique, se compose de quatre éléments reliés les uns aux autres par un circuit électrique : un clavier permettant d'entrer les lettres du texte clair, un brouilleur pour chiffrer les lettres du texte clair, un réflecteur qui renvoie le signal par un autre chemin que celui de l'aller et un tableau lumineux pour afficher les lettres du texte crypté. Le brouilleur est la pièce maîtresse d'Enigma. C'est en réalité un tambour rotatif en matériau isolant portant sur chaque face des contacts électriques. Chaque fois qu'une lettre est tapée sur le clavier naît un courant électrique qui traverse le rotor activé par la dépression de la touche et circule à travers un réseau de fils jusqu'au réflecteur puis au tableau lumineux où s'éclaire la lettre cryptée correspondante. Le parcours du courant électrique change à chaque touche activée (donc la lettre A par exemple ne se convertit pas deux fois de la même façon) grâce à l'action de brouillage du rotor.

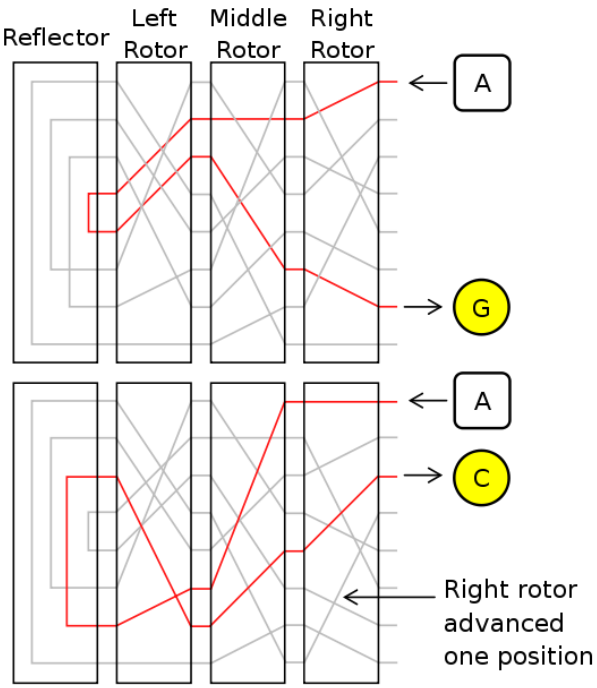


Vue en coupe d'un rotor

La rotation du brouilleur est l'innovation majeure de Scherbius. Pour complexifier la rotation d'1/26ème de tour chaque fois qu'une touche est activée, ce qui induit une régularité facile à déchiffrer pour un cryptanalyste, Scherbius ajoute un second, puis un troisième rotor au brouilleur, chacun possédant 26 positions. Chaque fois qu'une lettre est tapée, le premier rotor tourne d'un cran, les autres rotors restent immobiles. Une fois que le premier rotor a effectué un tour complet, le deuxième rotor tourne d'un cran. Le premier rotor recommence alors à tourner jusqu'à ce que le deuxième ait effectué un tour complet et soit revenu à sa position de départ. C'est ensuite au troisième rotor de s'amorcer. En multipliant le nombre de rotors, il devient

possible de concevoir une machine à crypter qui passe d'un alphabet à un autre, chaque fois différent, et d'obtenir une permutation quelconque des lettres. Ainsi, avec notre alphabet de 26 lettres, ces trois rotors procurent 26 X 26 X 26 soit 17 576 positions de brouillage.

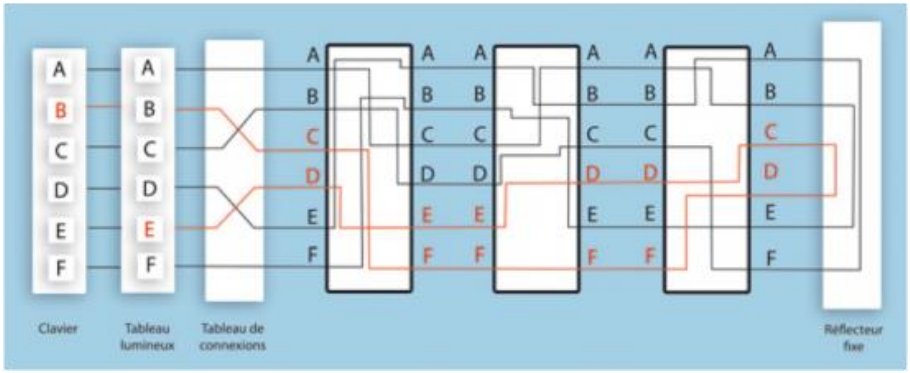
Ci-contre, un schéma simplifié de l'action de brouillage de la machine Enigma : la lettre A est entrée en clair, passe par le brouilleur composé de trois rotors, le réflecteur renvoie le signal pas un autre chemin, et la lettre G s'affiche finalement sur le tableau lumineux. Si l'on rentre à nouveau la lettre A en clair, le parcours du courant électrique est différent grâce à l'action de brouillage du premier rotor, qui a avancé d'un cran, et c'est cette fois la lettre C qui s'affiche sur le tableau lumineux :



C'est le positionnement des rotors qui constitue la clef du chiffrement. Afin de mieux protéger Enigma et sa cryptographie, Scherbius s'assure que les trois rotors sont mobiles et interchangeables, multipliant par 6 le nombre de clefs possibles. Il introduit également un tableau de connexions à 6 fiches entre le clavier et le premier brouilleur qui permet d'intervertir 12 lettres deux à deux avant que la lettre ne pénètre dans le rotor. 6 fois 2 lettres parmi les 26 lettres de l'alphabet peuvent être appareillées ainsi.

Chaque jour une nouvelle clef est définie, suivant un carnet de codes déterminés à l'avance spécifiant l'ordre de disposition des rotors, leur orientation et le branchement des connexions. La même clef sert à toutes les machines Enigma d'un même réseau, pour un jour donné. Pour crypter et envoyer un message, l'expéditeur fait tourner les trois rotors jusqu'à leur position de départ puis branche les connexions et rentre le texte clair dans la machine, notant pour chaque lettre la correspondante chiffrée qui s'allume sur le tableau lumineux. Il transmet ensuite le texte chiffré à son destinataire via un opérateur radio. Le récepteur du message chiffré peut le décoder à l'aide d'une machine Enigma similaire et du carnet de codes qui lui indique les positions du jour.

Ci-dessous, une schématisation du fonctionnement d'Enigma avec un alphabet à 6 lettres:



Le nombre total des clefs possibles de la machine Enigma s'élève à plus de 10 000 000 000 000 000, décomposé comme suit :

- 26 x 26 x 26 (orientation des brouilleurs)
- multiplié par 6 (disposition des brouilleurs)
- multiplié par 100 391 791 500 (nombre de branchements possibles)

Sans le carnet de codes le cryptanalyste devra vérifier toutes les clefs potentielles à la main… une mission impossible !

Si ce sont les connexions du tableau qui apportent le facteur multiplicatif le plus efficace, ce sont les rotors, leur rotation et leur disposition, qui, en tournant continuellement, rendent le texte chiffré imperméable à l'analyse des fréquences.

Durant les années 1930, l'armée allemande se dote de plus de 30 000 machines Enigma, le système cryptographique alors le plus sûr au monde. Enigma est appelée à jouer un rôle prépondérant dans la victoire d'Hitler. Contre toute attente, elle contribua à sa chute.

Les cryptologues allemands, afin de mieux protéger leurs messages, décident de ne pas appliquer la même clef de chiffrement à tous les messages du jour. Ils choisissent de changer l'orientation du brouilleur à chaque message. Or, ce changement d'orientation ne figurant pas dans le carnet de codes, ils doivent transmettre au récepteur du message la nouvelle orientation des rotors chaque fois qu'ils envoient une information. Celle-ci est chiffrée selon la clef du jour, tapée deux fois de suite afin que le destinataire s'assure qu'il n'y a pas eu d'erreur. Le principe de la rotation des brouilleurs permet de dissimuler cette répétition puisque les trois mêmes lettres tapées deux fois de suite ne donnent pas le même résultat crypté. La clef de chiffrement du jour ne sert donc plus qu'à transmettre la clef propre à chaque message.

Sentant l'invasion allemande imminente, la Pologne s'acharne à briser le code d'Enigma. En 1931, grâce à un délateur allemand, elle s'empare des plans de la machine et des carnets de codes de l'armée nazie. Marian Rejewski, âgé d'à peine 23 ans, est un des mathématiciens les plus doués du bureau du chiffre polonais. Il se lance tête baissée dans cette course contre la montre.

Très tôt il s'intéresse aux répétitions des messages envoyés par les Allemands, cherchant à en exploiter les failles. Il découvre que chaque message est précédé d'un message de 6 lettres et c'est sur ces 6 lettres qu'il concentre son attention pour déterminer la clef du jour. A l'autre bout, les Allemands, confiants d'avoir renforcé la sécurité d'Enigma, ne se rendent pas compte qu'ils l'ont en fait rendue vulnérable.

Pour chaque clef cryptée il existe une correspondance entre la 1ère et la 4ème lettre, entre la 2nde et la 5ème, entre la 3ème et la 6ème puisque ce sont deux chiffrements de la même lettre. Cette corrélation permet d'en déduire une indication sur le positionnement initial des rotors. Si suffisamment de messages sont envoyés dans la journée, Rejewski arrive à établir une correspondance complète entre l'alphabet de la première et celui de la quatrième lettre.

Rejewski s'intéresse aux chaînes de lettres qui lient les lettres du premier alphabet à celles du second. Il calcule ensuite le nombre de liens qui unissent chaque chaîne. Il fait de même avec les liens entre les alphabets de la 2nde et la 5ème lettre, entre ceux de la 3ème et la 6ème lettre. Ces chaînes changent tous les jours, parfois courtes, parfois longues, fluctuant en fonction de la clef du jour. Comment alors en déduire cette fameuse clef du jour ?

Rejewski réalise que si le tableau des connexions influe sur la composition des chaînes, il y a un élément de la chaîne qui dépend exclusivement du brouilleur, de son réglage et de son orientation: la longueur de la chaîne, c'est-à-dire le nombre de liens qui la composent. En effet, malgré la permutation des lettres du tableau de connexions, le nombre de liens reste inchangé.

Ainsi, plutôt que de chercher la clef du jour parmi les 10 000 000 000 000 000 clefs possibles, Rejewski n'a plus qu'à chercher les réglages du brouilleur parmi l'ensemble des réglages (6) et des orientations possibles (26 x 26 x 26) du brouilleur, soit 105 546 dispositions possibles. La tâche devient tout à coup moins ambitieuse. C'est donc ce qu'il fait, aidé d'une équipe chargée de répertorier toutes les longueurs de chaînes engendrées par chaque disposition. Au bout d'un an il obtient un répertoire exhaustif. Il peut dorénavant se référer à ce fichier pour retrouver l'agencement et l'orientation des brouilleurs correspondant à chaque clef du jour.

A partir de là il ne lui reste plus qu'à déterminer les branchements du tableau de connexions. Pour cela, Rejewski règle sa machine Enigma selon l'orientation des brouilleurs du jour et

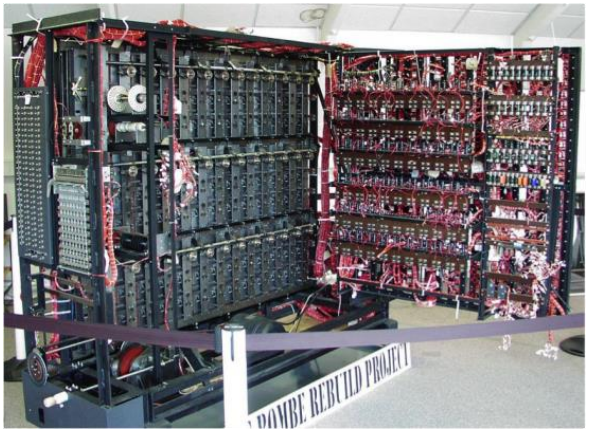
débranche les 6 câbles du tableau de connexions. Il entre ensuite le texte chiffré dans la machine. Le texte, une fois décrypté, n'est pas totalement lisible puisqu'il manque les branchements du tableau de connexions mais le message est tout de même déchiffrable et les branchements se déduisent de là. En quelques années, Rejewski réussit à rendre les communications allemandes totalement transparentes.

En parallèle il travaille à la conception de six machines électromécaniques, appelées " bombes ", qui permettent d'essayer rapidement des ensembles de clefs potentielles sur des blocs de communication d'Enigma. Elles peuvent, pour chaque position de réglage du brouilleur (soit 6), rechercher automatiquement son orientation. Ces bombes, conçues pour une attaque de force brute, fonctionnent toutes en même temps, comme une mise en série de plusieurs copies d'Enigma. Elles sont à l'origine de la mécanisation du cryptage.

Fin 1938, les Allemands renforcent la sécurité d'Enigma en ajoutant 2 rotors et 4 branchements supplémentaires au tableau de connexions. La Pologne, qui n'a plus les moyens de construire les " bombes " capables de décrypter la nouvelle Enigma et qui sait l'invasion allemande inéluctable, se tourne vers les Alliés, livrant à la France et à la Grande-Bretagne l'ensemble de ses travaux au cours de l'été 1939. Une bien belle surprise pour ceux qui pensaient Enigma indéchiffrable !

Les cryptanalystes anglais, réunis secrètement à Bletchley Park où est installée l'Ecole Gouvernementale du Code et du Chiffre, perfectionnent les découvertes de Rejewski, parvenant ainsi à décoder des informations décisives pendant la bataille d'Angleterre. Si le Polonais s'était intéressé aux faiblesses induites par la clef répétée au début de chaque message, Alan Turing, mathématicien de génie, se penche sur la structure type de certains messages en fonction de l'heure d'envoi et de l'opérateur.

En étudiant les messages décryptés, il se rend compte que les messages sont réglementés donc certains mots sont répétés. Ainsi, à 6 h 05, les messages envoyés contiennent presque toujours le mot " wetter " (" le temps "). A partir de ces " mots probables " (appelés " cribs "), qui sont en réalité devinés, Turing établit une correspondance plausible entre le texte clair supposé et le texte chiffré connu, liant les lettres en une boucle à la façon des chaînes de Rejewski. Il saisit rapidement que grâce à ces mots il va pouvoir venir à bout d'Enigma. Sa connaissance du fonctionnement d'Enigma et son exploitation des imprudences des chiffreurs allemands lui permettent de déduire le réglage des machines Enigma d'un même réseau pour un jour donné.



Reconstitution d'une bombe de Bletchley Park

Turing met au point une machine à chiffrer électromécanique composée de machines reliées électriquement entre elles qui répliquent le mouvement des rotors d'Enigma. Pour chaque réglage possible des rotors, la bombe de Turing effectue une chaîne de déductions logiques fondées sur les " cribs " et leurs boucles. Elle simule une correspondance entre texte clair et texte crypté pour essayer une clef. A chaque occurrence d'une contradiction la bombe écarte ce réglage et passe au suivant, modifiant les agencements de la machine. Lorsque toutes les connexions correspondent et ne donnent qu'une seule réponse, la clef est testée manuellement.

La machine de Turing est capable de chercher le réglage correct parmi les 159 milliards de milliards d'ajustements possibles (soit celles d'une machine Enigma contenant 5 rotors et 20 connexions) en moins d'une heure, abattant par jour le travail de 10 000 cryptanalystes. Les

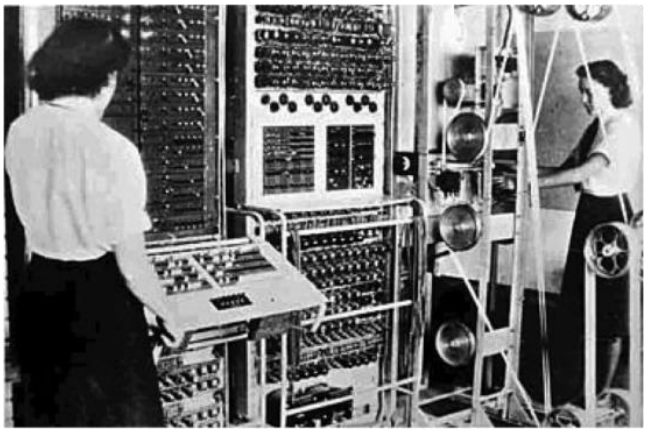
erreurs des opérateurs allemands permettent de réduire considérablement le nombre de clefs possibles. Plus efficace que la bombe polonaise, la bombe anglaise vient à bout du code de la machine allemande, jouant un rôle majeur dans l'affaiblissement du régime nazi.

Après la guerre, les percées des briseurs de code anglais et le décryptage d'Enigma restèrent classifiés secret défense jusque dans les années 1970. Les cryptanalystes de Bletchley Park furent pourtant à l'origine d'une des plus grandes révolutions technologiques de leur siècle : l'avènement de l'ordinateur programmable.

Parallèlement aux avancées de Turing, les cryptanalystes de Bletchley Park, parviennent à briser le chiffre de Lorenz utilisé pour coder les communications entre Hitler et ses généraux.

Bien que plus complexe qu'Enigma et se servant de chiffres plutôt que de lettres, la machine SZ40 de Lorenz fonctionne sur le même principe. Utilisant le code international de téléscripteur à 5 «bits», elle convertit chaque lettre du message clair en un code binaire, une suite de 0 et de 1. Chaque bit traverse ensuite deux clefs de chiffrement intermédiaires, l'une, appelée P, changeant à chaque opération, l'autre, appelée S, changeant au hasard. La somme de la lettre originale + P + S donne la lettre chiffrée. Le chiffre de Lorenz, trop subtile pour les bombes, doit être brisé manuellement. Il est percé à jour à la suite d'une erreur d'un opérateur allemand qui répète le même message deux fois de suite avec quelques étourderies en utilisant la même clef de chiffrement. A partir de ces deux textes chiffrés, John Tiltman trouve en janvier 1942 l'algorithme lui permettant de reconstituer le texte clair et son chiffrement.

Afin de mécaniser cette découverte, Max Newman met au point le premier calculateur électronique du monde, précurseur de l'ordinateur moderne : la machine Colossus. Il s'appuie sur la machine universelle de Turing conçue pour exécuter une suite d'opérations mathématiques données à l'aide de bandes perforées, comme celles utilisées pour les pianos mécaniques. Contre l'avis de l'Etat-major de Bletchley qui cherche à enterrer le projet, car jugé irréalisable, l'audacieux Tommy Flowers relève le défi et se lance dans la réalisation de Colossus qu'il termine fin 1943.



La machine Colossus, composée de 1 500 valves électroniques, est bien plus rapide que les bombes de Turing dont les commutations de relais électromécaniques sont assez lentes. Elle réalise 5000 opérations par seconde et le message crypté est en général cassé en quelques heures. Elle permet de retrouver le texte clair à partir du texte chiffré via un décryptage progressif sans qu'il soit nécessaire de récupérer la clef.

Si Colossus, comme les découvertes de Turing, reste classifié, il ouvre cependant la voie à une nouvelle orientation de la cryptographie qui peut dorénavant compter sur l'efficacité et la flexibilité des ordinateurs programmables, accélérant la course au code indéchiffrable et attisant la rivalité entre concepteurs et décrypteurs. La cryptologie rentre dans l'ère industrielle.

Le film : Imitation Game