Enigma
et la
Seconde guerre mondiale

GUILLAUME MUNCH JULIEN MILLI

Août 2004

Table des matières

Introduction

Lors de la Seconde guerre mondiale, *Enigma* bouleverse le monde de la cryptographie en assurant la confidentialité des communications allemandes, sur laquelle le III^{ème} Reich comptait dans la mise en œuvre de sa stratégie. Cette machine permettait aux allemands de crypter les messages militaires, en se basant sur un dispositif électro-mécanique de chiffrement.

Cet évènement dans l'histoire de la cryptographie a poussé les pays belligérants à mener une véritable guerre du renseignement dont dépendra la vie de dizaines de milliers d'Hommes. En effet, la réaction des Alliés à cette invention ne se fit pas attendre. Ainsi, les Polonais, puis les Anglais à Bletchley Park, ont rassemblé les mathématiciens les plus éminents pour venir à bout d'Enigma et par la même occasion gagner la bataille de la cryptanalyse.

Comment la machine des nazis, héritage des méthodes antiques de cryptographie mais innovation par la mécanisation du codage, a-t-elle influencé le sort de la guerre ? L'utilisation de la machine Enigma par les Allemands sera traité dans une première partie. Mais l'influence d'Enigma est aussi celle de son décryptage par les Alliés, aussi ne peut-on pas ne pas nous intéresser aux efforts qu'on fourni les alliés pour briser le chiffre.

Première partie .

Enigma, les cryptographes allemands dans la guerre

Avant de devenir le symbole du décryptement allié, Enigma était surtout un outil efficace pour sécuriser les commmunications, que les Allemands ont parfaitement su intégrer à leur stratégie militaire. Cette partie retrace l'histoire de la machine : son invention, son utilisation et son fonctionnement.

1. L'invention d'Enigma et ses origines

La machine à crypter Enigma est née de la nécessité pour les Allemands de posséder un système de communication sûr à la veille de la Seconde guerre mondiale. Elle reprend le principe du cryptage par substitution expliqué dans ce chapitre.

1.1. Les origines de la cryptographie

Depuis des millénaires, les rois, les empereurs et les généraux ont dû se doter de moyens de communication efficaces pour gouverner leur pays ou commander leurs armées. Etant conscients des risques encourus si leurs messages tombaient dans les mains d'un ennemi, cela les a poussés à des codes pour que seul le destinataire puisse les lire. Ainsi, dans un souci de confidentialité, les nations ont créé des services secrets chargés d'assurer la sécurité des communications par la mise en place des meilleurs codes possibles. C'est donc essentiellement dans un cadre militaire et diplomatique que se sont développées les écritures sécrètes.

Pour dissimuler un texte, différentes techniques ont été inventé, parmi lesquels on distingue deux procédés principaux : la *stéganographie* et la *cryptographie*.

La stéganographie désigne toutes les techniques visant à cacher l'existence du message. Il s'agit d'une technique employée aujourd'hui pour insérer dans un fichier-image des informations relatives aux droits d'auteur. On peut en effet cacher un texte dans une image numérique, en codant le texte par d'invisibles variations de valeurs des pixels de l'image. La modification apportée à l'image reste invisible, puisqu'une image numérique peut représenter plus de couleurs que l'oeil humain n'en distingue.

La première trace de stéganographie remonte à la Grèce antique, au IV^{ème} siècle avant Jésus-Christ : on raconte qu'un citoyen avait rasé le crâne de son esclave pour y écrire un message. Il attendit ensuite que les cheveux repoussent avant de l'envoyer chez le destinataire. Mais la stéganographie n'est pas efficace pour assurer la confidentialité d'une communication : une personne soupçonnant une communication aura vite fait de mettre à jour le stratagème.

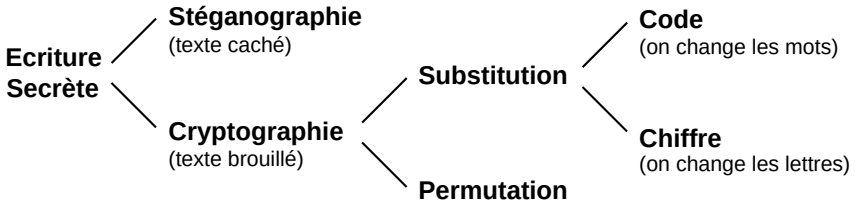


FIG. 1.1.: Schéma des moyens de dissimulation d'un texte

ALPHABET CLAIR	ABCDEFGHIJKLMNOPQRSTUVWXYZ
ALPHABET CHIFFRÉ	NBVCXWMLKJHGFDSQPOIUYTREZA

TAB. 1.1.: Alphabet pour une substitution monoalphabétique

La cryptographie, méthode bien plus sûre, consiste à rendre incompréhensible un texte pour tout lecteur qui ne serait pas son légitime destinataire. Cette méthode laisse le choix entre substituer une lettre par une autre, voire substituer un mot entier par une lettre : c'est la cryptographie par substitution ; ou bien permuter les lettres au sein d'un texte ou d'un mot : c'est la cryptographie par permutation.

Bien que le mot *code secret* est souvent utilisé pour désigner toute écriture secrète, il désigne à l'origine un système de cryptographie par substitution qui remplace un mot ou une phrase par une lettre ou un symbole. Il se distingue du *chiffre* qui effectue une substitution au niveau de chaque lettre (cf. FIG. 1.1). Ainsi, lorsqu'on se sert d'un code, on utilise les termes coder et décoder, et pour un chiffre, on utilise les termes chiffrer et déchiffrer. Plus généralement, les verbes crypter et décrypter s'appliquent à tous les procédés de cryptographie.

1.2. Le cryptage par substitution

La substitution monoalphabétique

La cryptographie par substitution *monoalphabétique* fut inventée par le cryptographe le plus célèbre de l'Antiquité, un certain Jules César. Elle consiste à faire correspondre à chaque lettre de l'alphabet une lettre chiffrée. L'*alphabet chiffré* du cryptage permet de représenter les correspondances entre les lettres claires et celles cryptées. Pour crypter un message, il suffit de remplacer chaque caractère par celui qui lui correspond dans

LETTRE	E	S	A	...	Z	K	W
FRÉQUENCE	17,66%	8,50%	7,47%	...	0,13%	0,02%	0,00%

TAB. 1.2.: Fréquence d'apparition de quelques lettres dans la langue française.

ALPHABET CLAIR	ABCDEFGHIJKLMNOPQRSTUVWXYZ
ALPHABET CHIFFRÉ N°1	NBVCXWMLKJHGFDSQPOIUYTREZA
ALPHABET CHIFFRÉ N°2	MLKJHGFDSQPOIUYTREZANBVCXW

TAB. 1.3.: Alphabets pour une substitution polyalphabétique

l'alphabet codé. Par exemple, avec l'alphabet chiffré du tableau 1.1, le mot `GUERRE` devient `MYXOOX`.

Comme toutes les méthodes de cryptage, la substitution monoalphabétique combine un *algorithme* et une *clef*. L'algorithme est ici le remplacement de chacune des lettre par une autre, et la clef, l'alphabet chiffré utilisé pour cette substitution.

La substitution monoalphabétique est-elle une méthode sûre ? Le nombre de clefs possibles, c'est-à-dire le nombres de possibilités de former un alphabet désordonné, vaut $26!$ soit plus de 4×10^{26} possibilités. Un espion qui met une seconde à essayer une clef mettrait plus de 10^{19} années à tester toutes les combinaisons[1].

Pour autant, cette méthode est-elle infaillible ? Non, mais la preuve n'en est venue que bien après la chute de l'empire romain, pendant le Moyen-Age et l'apogée de la civilisation arabe. Al-Kindi publie vers 1400 les premières méthodes de cryptanalyse de ce chiffre. Il remarque que suivant la langue, toutes les lettres n'ont pas la même fréquence d'apparition dans un texte. A titre d'exemple, les fréquences d'apparitions de quelques lettres de la langue française sont représentées dans le tableau 1.2.

Ainsi, en se basant sur ce tableau, les messages chiffrés par substitution monoalphabétique reprennent leur sens : grâce à l'analyse statistiques des lettres d'un texte crypté assez long, on peut en déduire à quelques erreurs près le texte clair.

La substitution polyalphabétique

Pour pallier à la faiblesse du chiffre de substitution monoalphabétique, les cryptologues de la Renaissance, dont le plus célèbre est le français Blaise de Vigenère, vont mettre au point un chiffre plus efficace : la substitution *polyalphabétique*. Le principe en

[1] A titre de comparaison, notre galaxie est apparue il y a $1,5 \times 10^{10}$ années.

est simple : Vigenère a voulu empêcher les cryptanalystes de se baser sur l'analyse des fréquences de lettres. Il a donc imaginé d'utiliser non plus un alphabet chiffré mais plusieurs.

Considérons les deux alphabets chiffrés du tableau 1.3. Nous voulons crypter le mot `GUERRE`. Le cryptage d'un message avec deux alphabets chiffrés consiste à utiliser le premer alphabet codé pour toutes les lettres de rang impair et à utiliser le second pour toutes les lettres de rang pair. Ainsi pour crypter notre mot, on chiffrera le `G` avec l'alphabet codé n°1, le `U` avec l'alphabet codé n°2, etc. Notre mot devient : `MNXEOH`. L'intérêt de ce nouveau cryptage est que l'emploi d'une analyse statistique directe est impossible. Notre exemple nous le démontre : les deux `R` consécutifs ne sont plus codés par la même lettre.

Le chiffre polyalphabétique était efficace, si bien qu'il ne fut brisé qu'au XIX^{ème} siècle, par Charles Babbage. La technique de décryptement consiste tout d'abord à chercher le nombre d'alphabets chiffrés utilisés, pour ensuite employer la méthode d'analyse statistique d'Al-Kindi, mais sur des lettres situées à une distance égale au nombre d'alphabet utilisés, qui par conséquent ont été cryptées de la même manière.

Cependant, cette méthode ne pouvait donner des résultats que sur des textes assez long par rapport au nombre d'alphabets chiffrés employés pour son cryptage. Un cryptage polyalphabétique idéal utiliserait autant d'alphabets chiffrés qu'il y a de lettres dans le message. Mais les techniques disponibles au XIX^{ème} siècle limitaient ce nombre pour des raisons pratiques évidentes : il serait effroyablement long et compliqué de crypter et de décrypter un texte en employant plusieurs dizaines d'alphabets chiffrés différents si l'on n'est muni que de crayon et papier, sans compter la difficulté pour parvenir à transmettre la clef au destinataire du message !

1.3. L'invention de la machine

Devant la difficulté qu'ils éprouvent à assurer la sécurité des communications au début du XX^{ème} siècle, les cryptologues s'accomodent des nouvelles techniques, et imaginent des dispositifs automatiques pour permettre un cryptage par substitution polyalphabétique qui, autrement, serait fastidieux. Presque simultanément, quatre inventeurs de pays différents inventèrent des machines de chiffrement électro-mécaniques, ayant pour principe la génération de nombreux alphabets chiffrés grâce à des cylindres rotatifs que traversent des circuits électiques : l'américain *Edward Hugh Hebern* commercialisa sa machine en 1917, la destinant aux militaires, mais déposa le bilan

quelques années plus tard. Le hollandais *Hugo Alexander Koch* déposa son brevet en 1919, en même temps que le suédois *Arvid Damm*.

Chiffriermaschinen AG

Le quatrième inventeur, à l'origine de la machine *Enigma*, est un inventeur allemand, Arthur Scherbius. Il déposa le brevet pour sa machine en 1918, et fonde avec un ingénieur du nom de Richard Ritter la société *Chiffriermaschinen AG* en 1923, pour commercialiser sa machine. Malheureusement pour lui, il n'a pas pu proposer sa machine aux militaires en raison de l'Armistice de 1918. Il se tourna alors vers les milieux financiers et les banques : pour cela, il fit des démonstrations publiques dès 1923 à Bonn, puis en 1924 à Stockholm lors du *Congrès Postal International*. En 1927, il acheta les brevets de la machine de Koch.

FIG. 1.2.: Arthur Scherbius

La machine de Scherbius présentait des avantages, non seulement par la force du cryptage qu'elle opérait, mais aussi par sa simplicité d'utilisation. Seules les machines Enigma pouvaient être munies d'un *réflecteur*. Alors que dans les autres machines, il pouvait être nécéssaire de retourner le dispositif pour permettre le décryptage des messages, ce dispositif facilitait l'utilisation de la machine en permettant au décryptage des messages de se dérouler exactement de la même manière que le cryptage. Mais Scherbius perdit ses clients potentiels, découragés par les prix excessifs des machines.

L'obsolescence des moyens de cryptage allemands de l'époque

Si la machine était un fiasco dans sa version destinée aux civils, elle allait acquérir sa renommée grâce à l'usage qu'en firent les militaires.

Dans les années 1920, l'armée allemande se vit forçée de reconnaître la piètre sécurité offerte par son système de cryptage ADFGVX. Ce changement d'état d'esprit se fit suite à la parution de deux livres, l'un de l'amiral anglais John Fisher, l'autre intitulé *The world crisis* écrit par Winston Churchill qui était alors à la tête de la marine anglaise. Ces deux ouvrages mettaient en avant l'avantage décisif de la Grande-Bretagne dans la première guerre mondiale grâce aux succès des cryptanalystes britanniques sur les messages allemands.

FIG. 1.3.: Version anglaise d'une brochure publicitaire d'un modèle commercial d'Enigma

L'armée allemande, mise devant le fait accompli, mena une enquête et conclut à la nécessité de s'équiper en Enigma. Ce fut tout d'abord la nouvelle marine allemande, la *Reischmarine*, en 1926 ; puis l'armée régulière, la *Reichswehr*, en 1928 ; et enfin l'armée de l'air, la *Luftwaffe*, en 1935. Mais il faut attendre l'accession de Hitler au pouvoir en 1933 pour que l'armée allemande s'équipe massivement en Enigma. Ce sont près de 200 000 machines qui furent construites jusqu'en 1945, cette production ayant été déléguées à plusieurs firmes allemandes.

Néanmoins, Scherbius ne vécut pas assez longtemps pour connaître l'extraordinaire ampleur de son invention pendant la deuxième guerre mondiale. En 1929, il mourut des suites d'un accident sur un attelage conduit par des chevaux.

2. L'utilisation d'Enigma durant la guerre

L'armée allemande s'est servie d'Enigma tout au long de la guerre, jusqu'à sa défaite. Un tel usage était nécéssaire en raison de la nouvelle manière de faire la guerre apparue avec la Seconde guerre mondiale. Cette section permet de se faire une image de l'emploi d'Enigma dans la guerre.

2.1. La cryptographie : une nécéssité pour la stratégie allemande

La *Blitzkrieg* mise en œuvre par les Allemands au cours de la Seconde guerre mondiale fut une innovation stratégique, permise par les nouvelles inventions dans les domaines de l'armement et des communications survenues depuis le début de la Première guerre mondiale : le char d'assaut et la radio.

Ce qui changea par rapport à la Première guerre mondiale

La Première guerre mondiale était une *guerre de position*, où les avancées d'une armée ne pouvaient qu'être lentes. Les champs de batailles étaient creusés de tranchées disposées face à face, dans lesquels les soldats des deux camps étaient cantonnés. Il était difficile pour le front de se déplacer, car lorsque les soldats se retrouvaient exposés, lors de la charge, ils étaient la cible des tirs d'artillerie et des mitrailleuses. Ces situations donnèrent lieu à des batailles interminables, à l'origine de nombreuses morts.

Les chars d'assaut et les avions ne constituaient pas une force majeure en eux-même. Les premiers étaient encore rudimentaires et peu nombreux à la fin de la guerre, tandis que les seconds n'avaient pour seule fonction la reconnaissance aérienne. La communication des armées se faisait encore à l'aide de pigeons voyageurs, de messagers à

cheval et de la télégraphie. Ce n'est que plus tard, avec l'entrée des Etats-Unis dans la guerre, que l'on s'est servi de la T.S.F., ancêtre de la radio.

Dans le domaine qui nous intéresse, la cryptologie, les méthodes employées étaient là aussi rudimentaires : le code ADFGVX qu'utilisaient les Allemands pour crypter leurs télégrammes se faisait encore à la main, et ne pouvait donc pas être employé à très grande échelle comme ce fut le cas pour Enigma. Mais déjà, les Anglais avaient tiré un avantage stratégique en fournissant les efforts nécéssaires à la cryptanalyse du code.

Le concept de guerre de mouvement

Juste après la Seconde guerre mondiale, pour ne plus avoir affaire à la guerre des tranchées dont les deux camps pâtissaient, on inventa le concept de *guerre de mouvement*. En 1920, des généraux anglais prédisaient que les tanks, en plus de leur puissance de tir écrasante, pouvaient tirer parti de leur mobilité en rompant à travers le front ennemi et en s'attaquant à leur positions reculées, où se trouvaient l'artillerie et le ravitaillement, ce qui saperait par la même occasion le moral des troupes ennemies.

Des officiers des armées de terre de tous les pays se sont intéressés à ce concept, comme De Gaulle, ou encore Heinz Guderian. Celui-ci en écrivit plusieurs articles, et reçut l'attention d'Hitler. Il fut promu au grade de général et se vit recevoir le commandemant de blindés avant l'invasion de la Pologne. Il pouvait donc appliquer sa nouvelle stratégie au conflit qui allait suivre.

Cette stratégie, la Blitzkrieg, guerre-éclair, a été conçue pour vaincre rapidement, sans que la guerre des tranchées n'ait le temps de s'installer. Pour la mettre en pratique, l'armée allemande s'est dotée à partir de 1933 d'une force de frappe importante, composée de blindés, les *Panzer*, et de bombardiers *Stuka*, pour éléments essentiels.

Description de la Blitzkrieg

La Blitzkrieg consiste en une attaque rapide des positions ennemies, par les différentes armées coordonnées entre elles : l'infanterie, les blindés de la *Wehrmacht*[1] et les bombardiers de la *Luftwaffe*[2] :

1. Les unités aériennes attaquent le front, l'arrière et la logistique ennemie, de manière à les affaiblir.

[1] Armée de terre allemande.
[2] Armée de l'air.

2. L'infanterie attaque le front sur une étendue vaste : de cette manière, l'ennemi ne peut pas savoir où l'offensive majeure aura lieu et sera pris par surprise.
3. Les tanks attaquent de manière massive et groupée les lignes de défense principales, et progressent dans le territoire ennemi, tandis que l'infanterie, continue d'attaquer l'ennemi pour l'empêcher d'organiser une défense efficace, avant de l'encercler.
4. Les unités mécanisées progressent et paralysent les positions arrières de l'ennemi pour l'empêcher de se replier.
5. Les différentes forces se rejoignent pour en finir avec l'ennemi.

Son principe fait que la Blitzkrieg doit son efficacité à de plusieurs éléments tactiques nécéssaires, que l'on peut faire correspondre avec des contraintes concernant les moyens de communication allemands.

En tout premier lieu, la Blitzkrieg est une coordination de toutes les armées. L'Allemagne a donc dû se doter d'un système de communication très vaste entre chaque unité et leur quartier général.

Deuxièmement, la Blitzkrieg se doit d'être rapide, et cette rapidité doit se retrouver dans la transmission des ordres. Une formation de Panzer avait beau aller vite, elle se mettait en danger et mettait en danger les autres unités si elle se mettait en route trop tard, à cause d'un ordre en parvenu en retard.

Ces deux premiers critères étaient parfaitement remplis par la radio, celle-ci pouvant être déployée à grande échelle et permettant de comuniquer rapidement, profitant de la célérité des ondes. Mais par sa nature même, les messages qui étaient transmis pouvaient être recueillis par n'importe qui disposant d'un récepteur réglé sur la bonne fréquence. L'effet de surprise, qui est le troisième élément tactique de la Blitzkrieg, aurait été inexistant si le camp adverse avait eu accès au contenu des messages, et nécéssitait d'être préservé.

L'intérêt d'Enigma

C'est à la nature dispersive des ondes radio que la machine Enigma doit sa participation à la guerre mondiale. Elle occupa la place centrale dans la sécurisation des communications allemandes en permettant de crypter les messages de nombreuses unités avant qu'ils ne soient envoyés. Elle multiplie les points forts : Rapide, la machine était plus simple à utiliser que d'autres procédés de cryptages, puisqu'elle faisait intervenir un dispositif électro-mécanique automatique pour le cryptage, et évitait

donc aux opérateurs l'effort qu'aurait nécéssité un cryptage se faisant avec crayon et papier. Petite, elle était transportée aisément, ce qui augmentait le nombre de situations où elle pouvait se rendre utile, et permettait aussi de ne pas entraver la mobilité des unités, point clef de la stratégie de la Blitzkrieg. Enfin, les Allemands ont pu établir un réseau très vaste de postes de TSF équipés de machines Enigma, puisqu'ils en étaient équipés de 30 000 au début de la guerre, pour un total de 200 000 machines construites à la fin de la guerre.

Pour les Allemands, la machine Enigma était tout ce dont l'armée avait besoin, en ce qui concernait la confidentialité de ses communications, pour la mise en œuvre de la Blitzkrieg. L'allemagne nazie a eu une confiance aveugle en cette machine pour sécuriser les communication de toutes leurs armées et de certains des services en pensant que la machine était telle que l'avait vanté son concepteur Arthur Scherbius : invincible.

2.2. Les différentes machines

Il faut savoir que lorsqu'on parle de la machine Enigma, en réalité, on parle d'un ensemble de machines parfois très différentes entre elles sur le plan cryptographique. Chaque armée disposait d'une version particulière d'Enigma. Les plus célèbres d'entre elles sont les machines de type *M3* et *M4* dont se servait la marine allemande, à cause de leur implication dans la Bataille de l'Atlantique et l'impact de leur décryptement sur la Seconde guerre mondiale[3]. Mais qu'existe-il comme machines autres que M3 ou M4, et en quoi différaient-elles ?

Toutes les variantes d'Enigma possèdent des *rotors* assemblés en un *brouilleur* comme pièce électro-mécanique servant de base au cryptage. Ce sont les caractéristiques de ce brouilleur qui différencient les machines entre elles, ainsi que l'adjonction ou non d'un *tableau de fiches*. La complexité du cryptage effectué par la machine augmente avec ces différents dispositifs. Nous reviendrons sur leur fonctionnement à la section 3.1.

La machine Enigma *standard* : Il s'agit de la machine employée par les armées de terre et de l'air allemandes, qui était la plus courante (cf. FIG. 2.1). Elle était dans son fonctionnement presque identique à la machine *Enigma D* vendue dans le commerce. Trois rotors étaient alignés dans le brouilleur.

[3]Ce point est abordé en détail dans la partie II.

FIG. 2.1.: Une machine Enigma standard, employée par la Wehrmacht.

La machine Enigma M3 : La marine allemande (*Reichsmarine* devenue *Kriegsmarine*) employait cette machine à partir de 1933. Elle était sensiblement plus difficile à décrypter que la machine standard, car bien qu'elle disposait du même nombre de rotors alignés simultanément dans le brouilleur, ceux-ci étaient choisi parmi un lot plus grand, proposant deux rotors en plus des trois initiaux.

La machine Enigma M4 : Cette machine remplaça la machine Enigma M3 en 1942 dans les sous-marins et dans les stations sur la côte, et était beaucoup plus complexe d'un point de vue cryptographique : quatre rotors étaient alignés simultanément dans le brouilleur de celle-ci, les trois premiers étant choisis parmi un lot de huit rotors, et le dernier étant choisi parmi deux autres.

La machine Enigma G ou *Abwehr Enigma* : elle était utilisée par les services secrets allemand. Il s'agit également d'une version à quatre rotors, mais démunie d'un tableau de fiches. La rotation des rotors a été choisie rapide, ce qui était perçu comme un difficulté supplémentaire pour d'éventuels cryptanalystes. Mais il s'avère que cette particularité a ajouté une faille supplémentaire à la machine, une aubaine pour les décrypteurs de Bletchley Park.

La machine Enigma des chemins de fer allemands ou *Raildienst Enigma* : celle-ci différait peu de la machine vendue dans le commerce, elle était utilisée par les services ferroviaires allemands.

Mais Enigma n'était pas le seul système de chiffrement utilisé par les Allemands durant la guerre. Enigma était utilisé pour la plupart des communications en morse, mais d'autres systèmes existaient, comme *Fish* qui codait les communications des téléscripteurs. Il commença à être développé en 1940, mais ce n'est que dans la seconde moitié de l'année 1941 qu'il vit son utilisation se répandre, surtout dans la *Luftwaffe*. Ce code a également été brisé par les Alliés, aidés du premier ordinateur électronique programmable, *Colossus*. Contrairement à l'histoire la plus répandue, le premier ordinateur, construit à Bletchley Park, n'a pas servi à décrypter Enigma.

Il est intéressant de noter que les différences fonctionnelles entre les machines ont eu deux conséquences. D'une part, les machines ne pouvaient pas se déchiffrer entre elles, à l'exception des machines M4 capables de communiquer avec les machines M3 avec un réglage du quatrième rotor spécifique. D'autre part, certaines machines se sont révélées être, pour les Alliés, très faciles à décrypter ; tandis que d'autres effectuaient un cryptage beaucoup plus fort.

2.3. La procédure de cryptage et d'émission d'un message

Les opérateurs chargés du cryptage des messages devaient suivre une procédure précise établie par l'état-major allemand, concernant le cryptage des messages d'une part, et l'envoi des messages d'autre part.

Comment un opérateur allemand faisait-il pour envoyer un texte tel que celui-ci en l'ayant préalablement crypté à l'aide d'Enigma ?

> *Auf Befehl des Obersten Befehlshabers sind im Falle, zur Zeit unwahrscheinlichen, Französischen Angriffs die Westbefestigungen jeder zahlenmässigen Überlegenheit zum trotz zu halten.*

Il s'agit d'un extrait de message authentique, envoyé par le commandant en chef allemand des armées en septembre 1938. Il signifie :

> *Sur ordre du commandant en chef, en cas d'attaque des fortifications à l'ouest*[4] *par les Français, bien que cela soit improbable pour le moment, ces fortifications doivent être défendues à tout prix, même contre des forces supérieures en nombre.*

[4] Le message fait probablement allusion à la *ligne Siegfried*, une ligne de fortifications allemandes faisant face à la ligne Maginot.

Comment crypter ce message sur une machine dont le clavier ne contient que les 26 lettres de l'alphabet ? Tout d'abord, les signes de ponctuation sont codés par des lettres peu fréquentes en allemand, `X` et `Y`, `X` correspondant à un point, et `Y` à une virgule. Ensuite, les nombres sont écrits en toutes lettres, et les caractères accentués ä, ö et ü, fréquents dans la langue allemande, sont remplacés par `AE`, `OE` et `UE`, et CH est remplacé par `Q`. Enfin, les abréviations sont possibles, pourvu que le texte reste intelligible. Zur Zeit deviendra par exemple `z.Zt`. Notre texte sera donc crypté sous cette forme :

```
AUF BEFEHL DES OBERSTEN BEFEHLSHABERS SIND IM FALLE
Y Z X ZT X UNWAHRSCHEINLICHEN Y FRANZOESISQEN
ANGRIFFS DIE WESTBEFESTIGUNGEN JEDER ZAHLENMAESSIGEN
UEBERLEGENHEIT ZUM TROTZ ZU HALTEN X
```

Le cryptage des textes requérait deux opérateurs, de manière à éviter les erreurs de saisie et à gagner du temps. Un opérateur chargé du cryptage crypte le texte lettre à lettres en ayant préalablement réglé la machine sur une clef de trois lettres, qu'il choisit et garde en mémoire. A chaque fois qu'une lettre est cryptée, un opérateur radio la note et récupère ainsi le message crypté entier. Ensuite, l'opérateur chargé du cryptage crypte la clef qu'il a gardé en mémoire à son tour, en se servant d'une *clef du jour*[5] partagée par tous les opérateurs de son armée, et répertoriée sur des documents d'instructions mensuels pour le réglage de la machine Enigma.

Ces documents étaient distribué aux unités de manière secrète, et les officiers devaient tout faire pour qu'ils ne tombent pas dans de mauvaises mains, car si un service de renseignements étranger y avait eu accès, celui-ci aurait été capable de déchiffrer tous les messages allemands.[6]

La clef maintenant cryptée constituait l'indicateur, que l'on ajoutait au message crypté avec la date et la désignation du destinataire, pour former le message qui allait être envoyé.

Enfin, l'opérateur radio envoie le message en morse, sur une fréquence radio qui lui était attribuée :

```
AN HEERESGRUPPENKOMMANDO 2= 2109 -1750 - FRX FRX -
HCALN UQKRQ AXPWT WUQTZ KFXZO MJFOY RHYZW VBXYS IWMMV
```

[5] On appelle la clef du jour ainsi car elle changeait le plus souvent toutes les vingt-quatre heures, mais la durée durant laquelle elle était valide n'était pas la même d'armée en armée et a changé au cours de la guerre. Certaines étaient gardées deux jours, d'autres huit heures seulement.

[6] On retrouve le principe de la cryptographie à clef privée, qui pose le problème de la transmission de la clef de l'émetteur du message à son destinataire.

```
WBLEB DMWUW BTVHM RFLKS DCCEX IYPAH RMPZI OVBBR VLNHZ
UPOSY EIPWJ TUGYO SLAOX RHKVC HQOSV DTRBP DJEUK SBBXH
TYGVH GFICA CVGUV OQFAQ WBKXZ JSQJF ZPEVJ RO -
```

Ceci n'avait évidemment aucun sens pour quiconque ne possédant ni la machine Enigma, ni la clef du jour.

Pour le destinataire du message, la procédure était analogue à celle du cryptage. Les deux opérateurs qui reçoivent le message chiffré décodent tout d'abord l'indicateur avec le clef du jour. Ils disposent alors de la clef qui a servi à crypter le message. Le décryptage est tout aussi simple : une fois l'orientation des rotors réglées sur la bonne lettre, le premier opérateur entre une à une les lettres du message chiffré. En effet, les opérations de cryptage et de décryptage sont les identique, le procédé de chiffrement étant "*symétrique*". Le seconde opérateur recueille ainsi le texte clair, contenant les ordres pour son unité.

Les messages allemands voyageaient sur des fréquences différentes, et cryptés par des versions d'Enigma différentes. Les messages étaient donc dirigés directements vers l'unité apropriée, et cela garantissait aussi qu'un officier de l'armée de terre allemand, par exemple, ne puisse pas avoir accès aux communications d'un officier de la marine. Non seulement parceque cela n'avait pas de sens, pour un char allemand, de décoder un message destiné à un sous-marin, mais en plus, certains messages très secrets n'étaient destinés qu'aux officiers les plus haut-gradés...

3. Le fonctionnement d'Enigma

Ce chapitre explique de quoi se compose Enigma et quel processus permet à partir d'une lettre en clair d'obtenir une lettre cryptée. Des propriétés d'Enigma telles le nombre de clefs possibles ou encore la réciprocité entre le codage et le décodage, seront également démontrées à l'aide d'outils mathématiques.

3.1. Explication du fonctionnement

Vue globale de la machine

La machine Enigma reproduit un chiffrage par substitution polyalphabétique rendu complexe pour éviter tout décryptement. Nous allons procéder à l'explication du système électo-mécanique d'un Enigma standard, celle utilisée dans la *Wehrmacht*. Dans ce modèle, elle se compose de trois éléments reliés par des cables électriques (cf. FIG. 3.1) :

- Un clavier pour entrer le texte clair.
- Un dispositif de cryptage qui remplace chaque lettre du texte clair par une lettre chiffrée.
- Un tableau lumineux qui affiche la lettre chiffrée.

Ainsi, lorsqu'on appuie sur une touche du clavier, un courant électrique issu du clavier traverse le dispositif de cryptage et allume une diode du tableau lumineux qui correspond à une lettre chiffrée (cf. FIG. 3.2).

Le dispositif de cryptage

Le dispositif de cryptage se compose de deux éléments distincts, qui tour à tour vont substituer la lettre provenant du clavier par une autre. Une première substitution est effectuée au niveau du tableau de fiches et une seconde au niveau du brouilleur.

Le tableau de fiches permet de substituer une lettre par une autre. Concrètement, il existe des fiches, c'est-à dire des fils électriques, qui permettent de permuter le cir-

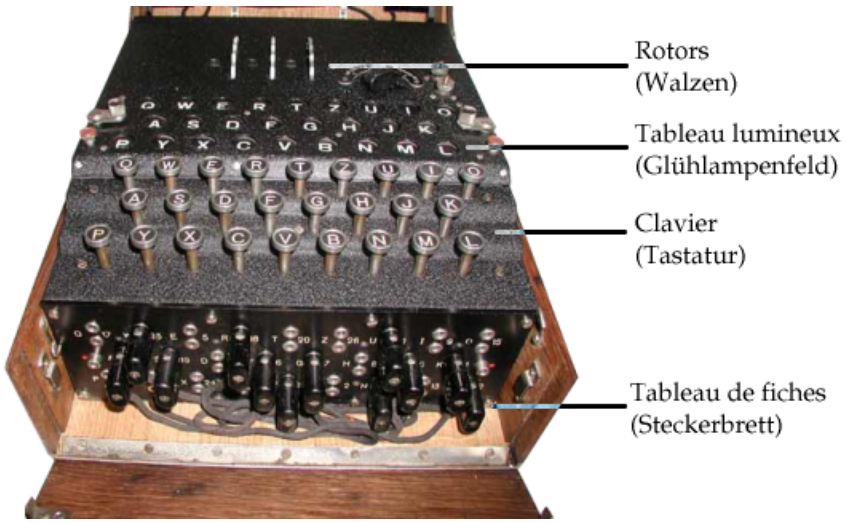


FIG. 3.1.: Les composants d'une machine Enigma standard.

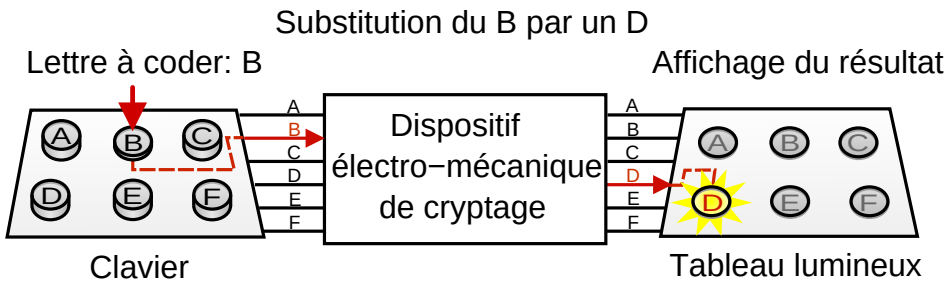


FIG. 3.2.: Le codage d'un message avec Enigma se fait lettre à lettre : on entre la lettre sur un clavier et la machine indique la lettre codée correspondante sur un tableau lumineux. Exemple avec une machine disposant d'un alphabet de six lettres.

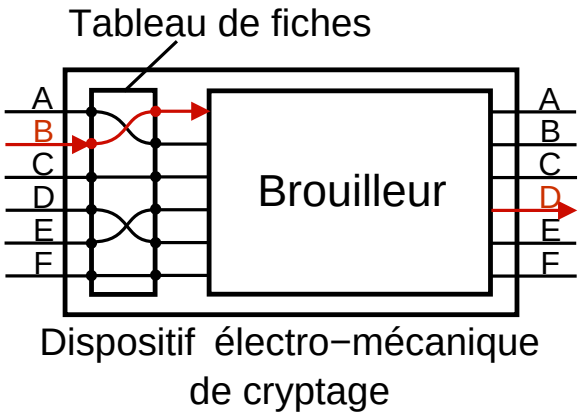


FIG. 3.3.: Le dispositif de cryptage de la machine Enigma, composé du tableau de fiches et du brouilleur.

cuit d'un fil avec celui d'un autre. A titre d'indication, les clefs du jour de l'armée demandaient de brancher dix fiches, ce qui entraînait la permutation de 20 lettres, chiffre qui était constant, mais dans d'autres utilisations, moins de fiches pouvaient être utilisées (cf. FIG. 3.3).

Le brouilleur

C'est l'élément esseniel du dispositif de cryptage. Dans une Enigma standard, il se compose de trois rotors et d'un réflecteur.

Qu'est-ce qu'un rotor ?

Un rotor est un disque composé d'un matériau isolant, de la taille d'un palet de hockey, et qui peut tourner selon un axe. Un rotor est pourvu de vingt-six contacts électriques sur chaque face. Les contacts de l'une des face sont reliées aléatoirement aux contacts de l'autre face par des fils électriques qui passent à l'intérieur du corps du rotor. Ainsi si chaque contact correspond à une lettre, un rotor correspond à un alphabet codé. Une impulsion électrique qui arrive au rotor par le contact d'entrée représentant une lettre claire, par exemple A, émergera du rotor par le contact de sortie représentant une lettre chiffrée, par exemple C. Un rotor effectue donc une substitution monoalphabétique, attribuant à chaque lettre claire une lettre chiffrée.

Enfin, le rotor est muni d'une bague non solidaire des câblages interne des rotors, sur laquelle des lettres sont gravées pour permettre à l'opérateur de repérer l'orientation

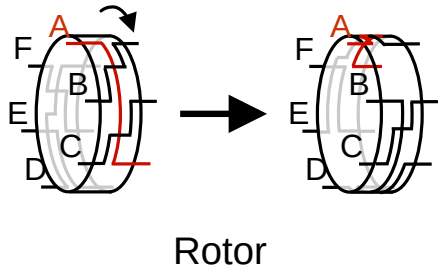


FIG. 3.4.: Un rotor du brouilleur, avant et après avoir tourné : la correspondance entre lettres change après le cryptage d'une lettre.

du rotor lorsqu'il règle sa machine[1]. Si cette bague n'est pas solidaire des câblages, c'est pour ajouter à la complexité du cryptage d'Enigma. La bague devra être réglée au préalable sur la bonne position, mais ce système ne rend pas ce cryptage beaucoup plus fort, c'est pourquoi l'on n'entrera pas dans les détails.

Pourquoi un rotor pivote-t-il ?

L'un des principaux rôles du rotor est de tourner autour de son axe. Lorsque le rotor tourne, la correspondance entre circuit d'entrée et circuits de sortie est modifiée. Pour reprendre l'exemple précédent, si le circuit A est relié au circuit C via le rotor, une fois que celui-ci ait tourné d'un cran, les connexions sont décalées d'un cran et donc le circuit A n'est plus relié au circuit C mais à un autre circuit, F par exemple (cf. FIG. 3.4).

Un rotor peut pivoter vingt-six fois sur lui-même avant de retrouver sa position initiale. Un rotor seul définit donc vingt-six alphabets chiffrés différents : il effectue une substitution polyalphabétique.

Pourquoi y a-t-il trois rotors dans une Enigma standard ?

La substitution polyalphabétique, au même titre que la substitution monoalphabétique, comme nous l'avons vu en section 1.2, a été décryptée. Le décryptement d'une telle substitution repose sur le fait qu'un alphabet chiffré est utilisé à plusieurs reprises pour crypter les lettres du texte clair. Ici, un rotor engendre vingt-six alphabets chiffrés qui sont fonction du câblage interne du rotor et de son orientation autour de son axe ; autrement dit, les vingt-six premières lettres d'un message peuvent être chiffrés

[1]Sur les premières machines, l'orientation des rotors n'était pas repérée par une lettre mais par un nombre.

d'une manière différente, mais inéluctablement, l'alphabet utilisé pour crypter la vingt-septième lettre du message sera le même que celui utilisé pour la première lettre, et ainsi de suite. Avec un seul rotor, un message plus long que 26 lettres pouvait facilement être décrypté.

Pour éviter cela, Scherbius a eu l'idée d'aligner l'un derrière l'autre trois rotors numérotés de un à trois, chacun ayant des cablages internes différents, c'est-à-dire engendrant alphabets codés différents. Il a conçu le brouilleur de manière à faire tourner les trois rotors tel un compteur : le rotor situé le plus à droite dans le brouilleur, le plus éloigné du réflecteur, est le rotor *rapide*, et tourne dès qu'une lettre est cryptée. Une fois qu'il a effectué un tour complet, le rotor adjacent tourne d'un cran, et de même, une fois que celui-ci a achevé sa rotation complète, le troisième rotor tourne d'un cran et le cycle continue. La partie mécanique de la machine Enigma est là pour remplir cette fonction.[2]

Au total, comme les rotors ont tous trois vingt-six positions possibles, il y a $26 \times 26 \times 26 = 17\,576$ alphabets chiffrés différents. Autrement dit, on retrouvera la même position des rotors donc le même alphabet codé à la 17 577$^{\text{ème}}$ lettre du message clair[3]. Les opérateurs manipulant Enigma avaient pour consigne de séparer les messages long en plusieurs messages courts, si bien qu'aucun message n'atteignait cette quantité de caractères, ce qui aurait été de toute manière difficile. Scherbius, par cet ingénieux système de trois rotors, a su éviter la redondance d'un alphabet chiffré.

Le réflecteur

A ce stade des explications, on sait crypter une lettre à l'aide de la machine, mais l'on ne peut, à partir de la lettre chiffrée, retrouver la lettre originale. Il existe un dernier élément à la machine permettant de résoudre ce problème : le réflecteur. Grâce à lui, le chiffrement et le déchiffrement sont "*symétriques*", c'est à dire si F est codé B alors pour une même position des rotors, B est codé F.

[2] A cause de ce mécanisme, la rotation est légèrement plus compliquée que présentée ici : lorsque le dernier rotor tourne, le rotor n°2 doit tourner deux fois de suite à cause d'un engrenage qui reste enclenché. Ce phénomène se nomme le *double-stepping* et ne survient pas sur le modèle G.

Dans d'autres modèles que celui présenté en exemple, certains rotors sont conçus pour tourner plusieurs fois durant le tour du rotor qui l'entraîne. C'est le cas de l'Enigma G ainsi que des trois rotors supplémentaires introduits avec l'Enigma M4.

[3] En réalité, à la 16 901$^{\text{ème}}$ à cause du *double-stepping*. Sur les modèles G et M4 entre autres, le cycle peut être raccourci considérablement, à cause de la rotation des rotors conçue pour être plus rapide. Dans le cas de la machine M4, il faut y ajouter le fait que le quatrième rotor, prévu pour accroître la sécurité du codage, ne tournait pas lors du chiffrement d'un message.

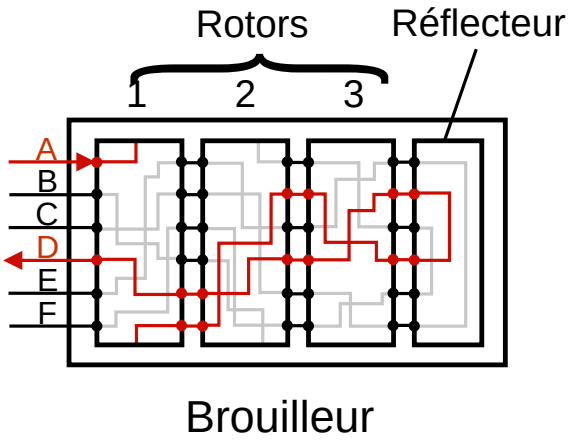


FIG. 3.5.: Les détails du brouilleur : trois rotors et un réflecteur reliés en série.

Le réflecteur fait partie du brouilleur et est situé après les trois rotors. Lorsqu'on enfonce une touche du clavier, un courant électrique qui lui est issu traverse le tableau de fiches puis les trois rotors, le rôle du réflecteur est de renvoyer l'impulsion électrique en sens inverse dans les trois rotors puis de nouveau dans le tableau de fiches, avant qu'elle n'arrive au tableau lumineux pour afficher la lettre correspondante — cryptée ou décryptée (cf. FIG. 3.5).

Cependant, le réflecteur a également généré une faiblesse de la machine Enigma largement exploitée plus tard par les cryptanalystes alliés : *une lettre ne peut pas être codée par elle-même*. On se propose de démontrer ces propriétés en section 3.3.

3.2. La force d'Enigma

La force d'Enigma réside dans le nombre immense de clefs imaginables pour tenter de décrypter un message : si l'on connait le fonctionnement et les câblages internes de la machine, mais si l'on ne connait pas la clef avec laquelle il a été crypté, le seul moyen pour parvenir à le lire serait *a priori* d'essayer toutes les combinaisons possibles. Cela s'appelle le décryptage par la *force brute*. L'exemple d'une Enigma M3 navale nous montre qu'il serait impratiquable.

La clef

La clef d'un message se décompose en plusieurs données. Tout d'abord, il faut connaître les composantes de la *clef du jour*, qui changeaient en général toutes les vingt-quatre heures et étaient les mêmes pour toute une armée, c'est-à-dire :

- **L'ordre dans lequel les rotors étaient positionnés :** Trois rotors sont choisis sur cinq disponibles, numérotés de `I` à `V`, et placés sur la machine dans un ordre bien déterminé.
- **Le placement de la *bague* :** Chaque rotor placé a un décalage de la bague déterminé, chaque bague d'un rotor pouvant être mise dans vingt-six positions différentes. Etant donné que la bague ajoute peu à la force du cryptage, on ne la prendra pas en compte pour calculer le nombre de clefs. En effet, même si l'on ne connaît pas son réglage, on pourra retrouver des portions de texte clair, étant donné qu'elle n'introduit qu'un décalage au niveau de l'orientation des rotors et de leur rotation.
- **Les couples de lettres interchangés :** Le tableau de fiches était également fixé pour la journée. Dix fiches sont ainsi branchées lors de l'utilisation de la machine.

Enfin, il faut connaître la composante de la clef propre au message. Il s'agit de **l'*orientation des rotors*** : chaque rotor était tourné de telle sorte à ce que dans une fenêtre laissant aparaître les lettres inscrites sur la bague, aparaisse une lettre constituante de la clef. Vingt-six alignements étaient donc possibles par rotor.

Nombre de réglages possibles pour l'orientation des rotors et de leurs bagues

Le nombre d'orientations des rotors s'élève à 26^3, car l'on a 26 positions pour chacun des trois rotors.

$$\text{nombre d'orientations des rotors} \quad = \quad 26^3$$

Nombre de réglages possibles au niveau de l'ordre des rotors

Ce nombre correspond au nombre de choix différents existant de trois éléments d'un ensemble en contenant cinq. On utilise une formule mathématique de *dénombrement*[4]. Il s'agit du nombre d'*arrangements* de 3 parmi 5 :

[4]Les formules sont expliquées en annexe B auf Seite 83.

$$\begin{aligned} \text{nombre d'ordres des rotors} &= \mathsf{A}_5^3 \\ &= \tfrac{5!}{(5-3)!} \\ &= 60 \end{aligned}$$

Nombre de réglages possibles au niveau du tableau de fiches

Dix fiches étaient branchées au niveau du tableau de chiffres. On considère ce chiffre constant, car si l'on prenait en compte le fait qu'on pouvait brancher autant de fiches que l'on voulait, on obtiendrait un nombre de combinaisons bien plus important, mais qui ne correspondrait pas à l'utilisation réelle que les militaires faisaient d'Enigma.

Si l'on branche dix fiches au tableau de fiches, on va choisir dix couples de lettres toutes différentes entre elles. On va chercher à dénombrer ces choix possibles, sachant que l'ordre dans lequel le choix a été effectué ne compte pas. On utilise une autre formule du dénombrement, le nombre de *combinaisons de p parmi n* C_n^p, avec lequel l'ordre du choix n'a pas d'importance.

Prenons n pour nombre de fiches que nous nous apprêtons à brancher. On va tout d'abord choisir les $2n$ lettres qui seront reliées parmi les vingt-six. C_{26}^{2n} possibilités se présentent à nous pour ce choix. Parmi ces $2n$ lettres, nous choisissons la première paire, choix pour lequel nous avons C_{2n}^2 possibilités. Pour la deuxième paire, nous avons $\mathsf{C}_{2(n-1)}^2$, et ainsi de suite jusqu'à la n-ième paire, pour laquelle nous disposons de C_2^2 possibilités. Mais n'oublions pas que l'ordre dans lequel les fiches ont été choisies ne compte pas. On doit donc diviser le nombre de paires par le nombre de duplicata dans notre dénombrement. Nous avons choisi n paires, chacune de ces paire a été dénombrée de $n!$ manières différentes, et l'on doit donc diviser notre résultat par ce nombre. Le nombre de possibilités lors du choix des $2n$ lettres à brancher, puis lors du choix de chacune des n paires, se multiplient entre elles, et l'on obtient, pour un cas général, le nombre de possibilités pour brancher n fiches au tableau de fiches :

$$\text{nombre de réglages de } n \text{ fiches} = \frac{\mathsf{C}_{26}^{2n} \times \prod_{i=0}^{n-1} \mathsf{C}_{2(n-i)}^2}{n!}$$

On obtient le compte final pour dix fiches après une simple application numérique :

$$\begin{aligned}
\text{nombre de réglages de } 10 \text{ fiches} &= C_{26}^{20} \times \prod_{i=0}^{9} C_{2(10-i)}^{2} \times \frac{1}{10!} \\
&= \frac{26!}{20! \times 6!} \times \left(\frac{20 \times 19}{2} \times \frac{18 \times 17}{2} \times \ldots \times \frac{2 \times 1}{2} \right) \times \frac{1}{10!} \\
&= \frac{26!}{20! \times 6!} \times \frac{20!}{2^{10}} \times \frac{1}{10!} \\
&= \frac{26!}{6! \times 2^{10} \times 10!} \\
&= 1\,507\,382\,749\,377\,250
\end{aligned}$$

Nombre de clefs différentes possibles

On multiplie les nombres de possibilités de chaque composante pour obtenir le nombre de clefs possibles.

$$\begin{aligned}
\text{nombre de clefs} = \ & \text{nombre d'ordres des rotors} \\
& \times \text{nombres de réglages de } 10 \text{ fiches} \\
& \times \text{nombre d'orientations des rotors}
\end{aligned}$$

On obtient ainsi que le nombre de clefs qui existent pour une Enigma M3 est de 16 milliards de milliards. Si l'on parvenait à tester toutes les clefs une à une à raison d'une par seconde, le message serait décrypté au bout de cinq mille milliards d'années ! Ce chiffre impressionnant est obtenu grâce à l'adjonction d'un tableau de fiches qui augmente considérablement le nombre de clefs, mais la véritable force de la machine vient du brouilleur, car sans lui, la machine n'effectuerait qu'un cryptage monoalphabétique, que l'on savait déjà décrypter cinq siècles plus tôt.

Comparatif de différentes machines Enigma

D'après les chiffres du tableau 3.1, cela pouvait sembler insensé de tenter le décryptage du code Enigma. Cela était-il pourtant irréalisable ? Tout comme nous l'avons vu précédement[5], le fait qu'un code ait un nombre immense de clefs possibles ne signifie pas qu'il est invincible : le chiffrement par substitution monoalphabétique a beau proposer 4×10^{26} clefs différentes, il est l'un des moins sécurisés. Il en va de même pour Enigma, qui possédait des failles qui permirent aux alliés de le briser.

[5] cf. section 1.2.

Version de la machine Enigma	C	Wehrmacht	M3	M4
Utilisation	Version vendue dans le commerce	Version utilisée par la Wehrmacht et la Luftwaffe	Version utilisée par la Kriegsmarine	Remplaça l'Enigma M3 en 1942
Nombre de rotors alignés	3 *(le réflecteur tourne également)*	3	3	4 *(le dernier est choisi à part parmi deux)*
Nombre de rotors total	3	3	5	8
Nombre de fiches branchées	0 *(version sans tableau de fiches)*	10	10	10
Agencement des rotors	6	6	60	672
Orientations des rotors	456 976	17 576	17 576	456 976
Réglages des fiches	1	$1,51 \times 10^{14}$	$1,51 \times 10^{14}$	$1,51 \times 10^{14}$
Nombre de clefs	$2,74 \times 10^{6}$	$1,59 \times 10^{19}$	$1,59 \times 10^{20}$	$4,64 \times 10^{22}$
En testant une combinaison par seconde...	**1 mois**	$\mathbf{5,04 \times 10^{11}}$ **ans**	$\mathbf{5,04 \times 10^{12}}$ **ans**	$\mathbf{1,47 \times 10^{15}}$ **ans**

TAB. 3.1.: La complexité de différentes versions de la machine Enigma

3.3. Démonstration des propriétés d'Enigma

La théorie mathématique des *permutations* s'avère efficace pour démontrer certaines caractéristiques de la machine Enigma apparues avec l'installation du réflecteur :

- Expliquons pourquoi le chiffrement et le déchiffrement d'un message se déroulent de la même manière.
- Démontrons qu'une lettre ne code jamais pour elle-même.

L'annexe B page 83 apporte des précisions sur les outils mathématiques utilisés.

La théorie des permutations

Dans cette théorie, nous disposons de fonctions mathématiques qui opèrent des permutations entre les *éléments* d'un *ensemble* donné, en associant à chacun des éléments de cet ensemble un autre élément de l'ensemble, et ce de manière réversible, à l'instar des substitutions de lettres effectuées par les rotors d'une machine enigma. Ces fonctions s'appellent des *permutations*. Prenons un exemple :

Soit l'ensemble $E = \{1, 2, 3, 4\}$.

Soit $f : E \to E$ tel que :

$$\begin{cases} f(1) = 2 \\ f(2) = 4 \\ f(3) = 3 \\ f(4) = 1 \end{cases}$$

f est une permutation.

Ici, notre f se note :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

f possède pour *point fixe* 3, car 3 est permuté avec lui même et restera 3 si on lui applique cette permutation.

Composition

On peut *composer* les permutations. La composition de fonctions consiste en l'application successive de deux fonctions, de la même manière que la substitution effectuée

par deux rotors que l'on branche en série. Elle se note avec l'opérateur $\circ$. Si σ et τ sont deux permutations, alors$\sigma \circ \tau(k) = \sigma(\tau(k))$. Ainsi, $\sigma \circ \tau$ est une nouvelle permutation.

Permutation réciproque

Par la définiton même de la permutation, chacun des éléments peut être obtenu par l'intermédiaire d'une permutation. Toute permutation f admet donc une réciproque que l'on note f^{-1} permutant les éléments de manière contraire à f. Avec le f de notre exemple précédent, on peut écrire f^{-1} de la manière suivante :

$$f^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Réciproque d'une fonction composée

Un résultat est important concernant la réciproque d'une permutation composée : elle est égale aux réciproques des permutations la composant, mais que l'on compose dans un ordre contraire.

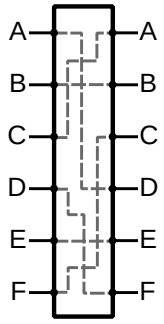
$$(\sigma \circ \tau)^{-1} = \tau^{-1} \circ \sigma^{-1}$$

La modélisation des composants d'Enigma

On peut modéliser les différentes parties de notre machine par ces fonctions. En effet, la substitution des lettres d'un message par d'autres lettres effectuée par la machine Enigma n'est rien d'autre qu'une succession de permutations s'appliquant lettre par lettre dans le message, effectuée tour à tour par chacun des dispositifs. Si dans notre exemple de permutations, nous avions des chiffres, nous pouvons très bien avoir une permutation opérant sur des symboles, comme les lettres de l'alphabet.

Modélisation d'un rotor

Voici un exemple de modélisation d'un rotor par une permutation r avec un alphabet de six lettres :



$\longrightarrow$

$$\begin{array}{lcl} A & \to & D \\ B & \to & B \\ C & \to & A \\ D & \to & F \\ E & \to & E \\ F & \to & C \end{array}$$

$\longrightarrow$ $r = \begin{pmatrix} A & B & C & D & E & F \\ D & B & A & F & E & C \end{pmatrix}$

Rotor électromécanique	Subtitutions cryptologiques	Permutation mathématique

Bien sûr, les substitutions effectuées changeant lorsque le rotor tourne[6], r n'est plus la même après la substitution d'une lettre. La modélisation ne correspond qu'à une clef quelconque donnée et une orientation quelconque des rotors donné, mais cela nous suffit pour démontrer les propriétés intéressantes, car elles sont valables pour n'importe quel orientation.

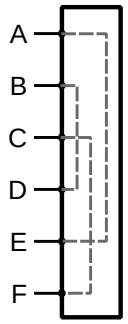
Si r_1, r_2, r_3 modélisent les trois rotors placés dans le brouilleur, leur bout à bout peut être modélisé à l'aide de compositions par :

$$r_3 \circ r_2 \circ r_1$$

La modélisation du réflecteur

Le réflecteur possède quant à lui des propriétés particulières. On le modélise par R.

[6] cf. section 3.1.



$\longrightarrow$

A $\rightarrow$ E
B $\rightarrow$ D
C $\rightarrow$ F
D $\rightarrow$ B
E $\rightarrow$ A
F $\rightarrow$ C

$\longrightarrow \quad R = \begin{pmatrix} A & B & C & D & E & F \\ E & D & F & B & A & C \end{pmatrix}$

Réflecteur électromécanique	Subtitutions cryptologiques	Permutation mathématique

Premièrement, le réflecteur reliant des fils électriques entre eux, si un courant provenant de A aboutit en C, un courant provenant de C aboutirait en A. La permutation modélisant le réflecteur est donc nécéssairement une *involution*, c'est à dire que cette permutation et sa réciproque sont identiques. Démonstration :

Soient k et l deux lettres de l'alphabet du réflecteur tels que $R(k) = l$.

$$\begin{aligned} & (R(k) = l \quad \Leftrightarrow \quad R(l) = k) \\ \Rightarrow \quad & R(R(k)) = R(l) = k \\ \Rightarrow \quad & R = R^{-1} \qquad \text{par définition} \end{aligned}$$

Deuxièmement, comme le circuit électrique nécéssite d'être fermé, une liaison à l'intérieur du réflecteur ne peut pas se faire entre une connection et elle-même. Le réflecteur n'associe donc jamais une lettre à elle-même et la permutation le modélisant n'a pas de point fixe :

$$\text{pour toute lettre } k \text{ de l'alphabet} \quad R(k) \neq k$$

Démontrons que la machine Enigma toute entière possède ces propriétés.

Modélisation d'Enigma

Pour les besoins de la démonstration, on modélise la machine Enigma de la manière suivante :

– La permutation modélisant la machine Enigma, qu'on nomme e, opère sur l'ensemble α, l'aphabet :

$$\alpha = \{\mathsf{A}, \mathsf{B}, \mathsf{C}, \ldots, \mathsf{Z}\}$$

– La machine Enigma se compose, pour ce qui est du dispositif de chiffrement, d'un tableau de fiches, d'un réflecteur et de rotors, comme nous l'avons détaillé dans les chapitres précédents. f modélise le tableau de fiches et r_1, r_2 et r_3 modélisent les trois rotor placés dans le brouilleur. On considère la substitution effectuée lors du passage dans le tableau de fiches puis dans les trois rotors comme une permutation unique σ. On a :

$$\sigma = r_3 \circ r_2 \circ r_1 \circ f$$

– R modélise le réflecteur.

– Le réflecteur a pour but de renvoyer l'information électrique dans les rotors puis dans le tableau de fiches. Une dernière substitution intervient alors, elle est égale à la réciproque de chaque permutation effectuées lors du premier passage, s'effectuant dans l'ordre inverse de celui survenu à l'aller :

$$\begin{aligned} f^{-1} \circ r_1^{-1} \circ r_2^{-1} \circ r_3^{-1} &= (r_3 \circ r_2 \circ r_1 \circ f)^{-1} \\ &= \sigma^{-1} \end{aligned}$$

– Ainsi, on obtient que e est le composé de ces permutations :

$$e = \sigma^{-1} \circ R \circ \sigma$$

Démonstrations des propriétés

Le cryptage et le décryptage sont identiques

On parvient à démontrer que e est une involution.

$$\begin{aligned} e^{-1} &= (\sigma^{-1} \circ R \circ \sigma)^{-1} \\ &= \sigma^{-1} \circ R^{-1} \circ \sigma \\ &= \sigma^{-1} \circ R \circ \sigma && \text{car } R \text{ est une involution} \\ &= e \\ \Leftrightarrow \quad & e \text{ est une involution} \end{aligned}$$

Ainsi, avec une clef donnée, si Enigma chiffrait une lettre par une autre, elle *dé*chiffrait cette lettre par la première. Cela montre pourquoi pour décoder un texte crypté, un opérateur allemand devait effectuer la même procédure que celle qu'avait employé, pour le crypter, l'opérateur qui lui avait envoyé le message.

Une lettre ne peut jamais être codée par elle-même

On parvient également à démontrer que e n'admet jamais de point fixe :

Raisonnons par l'absurde. Supposons que e admette un point fixe.

$$\begin{aligned}
e \text{ admet un point fixe} &\Leftrightarrow \text{il existe } k \in \alpha \text{ tel que } && e(k) = k \\
&\Leftrightarrow \text{il existe } k \in \alpha \text{ tel que } && \sigma^{-1} \circ R \circ \sigma(k) = k \\
&\Leftrightarrow \text{il existe } k \in \alpha \text{ tel que } && \sigma \circ \sigma^{-1} \circ R \circ \sigma(k) = \sigma(k) \\
&\Leftrightarrow \text{il existe } k \in \alpha \text{ tel que } && R \circ \sigma(k) = \sigma(k) \\
&\Leftrightarrow \text{il existe } k \in \alpha \text{ tel que } && R(\sigma(k)) = \sigma(k)
\end{aligned}$$

Cela est absurde car R n'admet pas de point fixe : Il n'existe aucun $\sigma(k) \in \alpha$ tel que $R(\sigma(k)) = \sigma(k)$. e n'admet donc pas de point fixe.

Ce résultat était important pour le décryptage d'Enigma. En effet, le fait que e n'admette pas de point fixe nous montre que la machine Enigma ne pouvait pas coder une lettre par elle-même. Il s'agit de la faille d'Enigma qui permit aux anglais de décrypter des messages chiffrés par Enigma. L'installation du réflecteur, bien qu'elle facilita le décodage des messages pour les opérateurs allemands, avait donc cet effet secondaire.

Deuxième partie .

Bletchley Park, la guerre vue par les décrypteurs Alliés

Bien qu'étant le cryptosystème le plus sûr de son temps, les Alliés ont mis tous les moyens possibles en jeu pour essayer de briser le chiffre d'Enigma, tant leur intérêt dans les communications allemandes était grand dans une période durant laquelle l'Europe était presque entièrement sous le contrôle du Reich. Cette partie rend hommage aux briseurs de code polonais et britanniques en analysant les méthodes de décryptage et les conséquences de celui-ci sur la guerre.

4. La cryptanalyse d'Enigma

Les Alliés ont réussi à force de courage et d'opinatreté à décrypter certains messages Allemands codés avec Enigma. Ce tour de force a été réalisé tout d'abord par les Polonais avant le déclenchement de la guerre puis par les Anglais à Bletchley Park de 1940 à 1945, aidés par la suite des Américains.

4.1. L'activité du bureau du chiffre Polonais

Après la première guerre mondiale, presque tous les pays belligérants avaient établi des services de renseignements et continuaient à lire les codes des états voisins comme en temps de guerre. Toutefois, en 1926, les messages allemands interceptés par ces services de renseignements les déroutèrent tout à fait : Enigma était rentré en action. La rapidité avec laquelle les cryptanalystes alliés renoncèrent à briser Enigma contrastait avec la persévérance qu'ils avaient déployée pendant le premier conflit mondial, travaillant nuit et jour à déchiffrer les messages allemands. A croire que la peur d'une invasion est la meilleure motivation pour attaquer des codes avec succès.

Une nation toutefois ne pouvait se permettre pareil relâchement : la Pologne. Ce petit pays remembré après le traité de Versailles en 1919 était constamment sous la menace de ses voisins : ses frontières longues de 5 400 km étaient bordées par des états hostiles et étaient souvent difficiles à défendre. Ainsi le territoire de *Cieszyn* (Teschen) fut partagé en juillet 1920 entre la Pologne et la Tchécoslovaquie dans des conditions qui les mécontentèrent toutes deux. La question des frontières orientales était encore plus délicate. Profitant de la guerre civile en Russie, la République polonaise voulait récupérer les territoires possédés par le royaume lors de sa plus grande extension au XVIe siècle. Aussi refusa-t-elle la *ligne Curzon* et lança-t-elle vers le sud-est une offensive qui conduisit ses troupes à Kiev en mai 1920. La contre-offensive soviétique les fit reculer jusqu'aux abords de Varsovie. Aidée par les Occidentaux, elle contre-attaqua à son tour et incorpora à la Pologne une partie de la Biélorussie et de l'Ukraine occidentales avec Lwów. A l'Ouest, l'Allemagne rêvait de reconquérir le corridor de Dantzig

qui séparait la Prusse Orientale du reste du pays selon la décision prise à Versailles, menace qui s'est d'autant plus affirmée avec la montée du nazisme.

L'instinct de survie poussa donc la Pologne à garder ses dangereux voisins sous surveillance : en 1920 fut fondé le Bureau du Chiffre (*Biuro Szyfròw*). Dans cette seule année, il permit de déchiffrer plus de quatre cent messages en provenance de Russie, tout en contrôlant toujours efficacement les communications allemandes. Quand en 1926, les cryptogrammes allemands changèrent, l'analyse des nouveaux messages allemands fut confiée à trois spécialistes de la langue germanique dont le capitaine Maksymilian Ciezki. Celui-ci observa que les nouveaux messages étaient tous précédés d'un mot-clef de six lettres mais ne pu établir de liens entre eux et le message. Les cryptanalystes furent bientôt convaincus que ces textes avaient été chiffré à l'aide d'un machine à crypter et non plus à la main comme il était alors d'usage. Les Polonais achetèrent alors une version commerciale de l'Enigma, ce qui leur permit de connaître le principe de l'invention de Scherbius. Mais la version commerciale différait de la version militaire de par les câblages internes des rotors, par conséquent les cryptographes polonais n'avaient aucune chance de déchiffrer les messages allemands à partir de cette simple machine.

FIG. 4.1.: Hans-Thilo Schmidt, allemand espionnant pour le compte des Alliés

C'est en fait grâce à un espion allemand du nom de Hans-Thilo Schmidt que le bureau du chiffre polonais put se lancer à l'assaut d'Enigma.

Schmidt avait fait carrière dans l'armée, il avait notamment participé à la Première guerre mondiale mais il ne put être maintenu à son poste après la réduction drastique des effectifs militaires de l'Allemagne conformément au traité de Versailles. Il tenta alors de se faire un nom dans les affaires mais son usine de savon ne put résister à la dépression des années 30. Ses échecs lui étaient rendus d'autant plus pénibles par les succès de son frère aîné Rudolph, lui aussi combattant de la Première guerre mondiale mais qui avait été gardé dans l'armée. Celui-ci finit par être promu en 1925 à la tête du Corps des Signaux, c'est-à-dire responsable de la sécurité des communications allemandes. Ayant une famille à charge, Hans-Thilo fut contraint de demander de l'aide chez son frère et ses parents, et Rudolph lui trouva un emploi à Berlin au *Chiffrierstelle*[1], le bureau du

[1]plus connu à l'époque sous le nom de *Chistelle.*

chiffre chargé de gérer les communications cryptées allemandes. C'était le poste de commande d'Enigma.

Grâce à cela Hans-Thilo Schmidt parvenait juste à subvenir aux besoins de sa famille — son épouse et ses deux enfants restés en Bavière. Il vécut donc seul à Berlin, pauvre et isolé, jaloux de son frère et animé d'un profond ressentiment envers une nation par laquelle il se sentait rejeté. Le résultat était prévisible : en vendant des informations secrêtes sur Enigma à des puissances étrangères, Hans-Thilo Schmidt pouvait à la fois gagner de l'argent et se venger en portant préjudice à la sécurité de son pays et en minant l'organisation dirigée par son frère. Hans-Thilo Schmidt prit contact avec les services de renseignement français et rencontra le 8 novembre 1931 en Belgique, à Verviers, un agent secret français, Rodolphe Lemoine, dont le nom de code était Rex, et Bertrand, cryptographe français. En échange de 10 000 marks, Schmidt, rebaptisé *Asche* pour plus de discrétion, permit à Rex de photographier des documents secrets : *Gebrauchsanweisung für die Chieffriermaschine Enigma*, les instructions pour l'utilisation de la machine Enigma, et *Schlüsselanleitungen für die Chieffriermaschine Enigma*, les directives pour fixer une clef sur Enigma. Pourtant les cryptographes français jugèrent assez vite que ces documents ne les aidaient en rien à déchiffrer Enigma, tout au plus leur permettaient-ils de connaître les éléments constitutifs une clef d'Enigma. Bertrand mit alors les Anglais au courant de ces informations, qui eux non plus ne surent en tirer profit, puis en désespoir de cause, les Polonais par l'intermédiaire du Biuro Szyfròw. Les Polonais ne savaient comment remercier Bertrand tant ces informations avaient de valeur à leurs yeux. Il découvrirent que la machine avait trois rotors comportant chacun une bague rotative ou était inscrit l'alphabet et que le réflecteur ne tournait pas. Qui plus est, les documents révélèrent la présence d'un tableau de fiches, qui n'existait pas sur la version commerciale. Les seuls éléments qui leur manquaient encore était les câblages internes des rotors, et bien sûr les ordre des rotors et les séries de fiches branchées au niveau du tableau qui constituait les clef d'Enigma. Ils ne connaissaient pas non plus la position de la bague alphabétique et par conséquent l'alignement des rotors mais pensaient être capables de les découvrir par l'analyse si les Français et Anglais consentaient à mettre en commun leurs avancées dans ce domaine. Bertrand, embarrassé, reconnu que la France et l'Angleterre n'avaient guère progressé dans la cryptanalyse d'Enigma... Toutefois en décembre 1931, une nouvelle rencontre entre Asche, Rex et Bertrand fut programmé à Verviers. L'entrée récente de Hans-Thilo Schmidt au parti nazi ne l'empêcha pas de fournir à Bertrand les carnets de code d'Enigma pour

Datum	Walzenlage	Ringstellung	Steckerverbindungen
30.	I V III	07 25 13	JT IV KE LR GU
29.	III II V	05 23 17	BQ WA IU YX ZP
28.	IV III I	26 18 16	LT FG ND KG JM
...	...	...	...

Datum : Jour du mois.

Walzenlage : Agencement des rotors dans le brouilleur.

Ringstellung : Réglage de la bague.

Steckerverbindungen : Couples interchangés au niveau du tableau de fiches.

Le tableau présenté est fictif : en réalité, les liaisons au niveau du tableau de fiches étaient souvent au nombre de dix et une information supplémentaire était indiquée, les discriminants (*kenngruppe*), qui permettaient de choisir la clé initiale en fonction du type de message que l'on voulait envoyer.

TAB. 4.1.: Extrait d'un carnet de code allemand

FIG. 4.2.: Marian Rejewski, du Bureau du Chiffre polonais

le mois de décembre. Les carnets de code étaient valables un mois et indiquaient les clefs d'Enigma spécifiques à chaque jour du mois (TAB. 4.1).

Cela ne l'empêcha pas non plus de retrouver Rex et Bertrand trois fois en 1932 : le 8 mai à Verviers, les 2 et 3 août à Berlin et les 19 et 20 octobre à Liège en Belgique. A chaque fois, Asche leur fournit, en plus d'autres informations, les clefs quotidiennes d'Enigma, pour mai puis de septembre à décembre.

La méthode de décryptage de Marian Rejewski

En 1929, le Bureau du Chiffre polonais, pour s'adapter à la mécanisation du codage, recruta à la place des traditionnels linguistes et autres spécialistes des formes de con-

struction de la langue, des mathématiciens. Parmi eux se trouvait Marian Rejewski (1905-1980), jeune étudiant de 23 ans, le plus doué. Il se lança à l'assaut d'Enigma et fit une découverte importante pour le décryptage d'Enigma. Sa stratégie se basait sur le fait que chaque jour, les six premières lettres de tous les messages d'un armée étaient chiffrées avec la même clef d'Enigma[2]. En effet pour plus de sécurité, les opérateurs allemands utilisaient la clef du jour pour transmettre un nouvel alignement des rotors qu'ils utilisaient pour la suite du message. Cet indicateur de trois lettres était répété deux fois au début de chaque message pour éviter les erreurs de transmissions en morse. Chaque message allemand avait donc sa propre clef qui était annoncée en début de message en utilisant la clef du jour. Ainsi Rejewski pouvait par exemple recevoir quatre messages commençant par les indicateurs suivants :

1er message	`LOKRGM...`
2ème message	`MVTXZE...`
3ème message	`JKTMPE...`
4ème message	`DVYPZX...`

Pour chaque message, la première et la quatrième lettre sont deux chiffrements de la même lettre, à savoir la première lettre du message-clef. De même pour la deuxième et la cinquième lettre, ainsi que pour la troisième et la sixième lettre, qui chiffrent respectivement la même lettre. Prenons par exemple le premier message : `L` et `R` chiffent la même lettre. Cette lettre est chiffrée différemment car entre ces deux cryptages, le brouilleur a tourné trois fois.

Rejewski découvrit que ce lien entre `L` et `R` dépendait du positionnement initial de la machine, il releva alors toutes les relations entre la première et la quatrième lettre dans un tableau. En considérant les quatre messages ci-dessus, on peut reconstruire ce tableau :

1ère lettre	`ABCDEFGHIJKLMNOPQRSTUVWXYZ`
4ème lettre	`---P-----M-RX------------`

Si Rejewski avait accès à suffisamment de messages, il pouvait compléter l'alphabet des relations. Il aboutissait alors à un tableau comme celui-ci :

1ère lettre	`ABCDEFGHIJKLMNOPQRSTUVWXYZ`
4ème lettre	`FQHPLWOGBMVRXUYCZITNJEASDK`

[2]C'est-à-dire le même branchement des fiches de connexions, le même ordre des rotors et la même orientation des rotors et de la bague.

C'est là que Rejewski eut une inspiration. Si la clef du jour utilisée pour coder ces messages avait été différente, ce tableau aurait été lui aussi entièrement différent. Il remarqua aussi que ce qui crée la complexité de la machine, c'est son tableau de connexions augmentant de $1,5 \times 10^{14}$ fois le nombre de clefs possibles pour coder un message. Il cherchait donc un moyen d'annuler les permutations effectuées au niveau du tableau de connexions. En fin de compte, il se pencha sur un modèle qui impliquait des chaînes de lettres. Dans le tableau ci-dessus, le A de la rangée supérieure est lié au F de la rangée du bas, aussi se reporta-t-il au F de la rangée supérieure. Il est lié au W, aussi chercha-t-il le W de la rangée supérieure. Ce W est lié au A, qui est justement la lettre avec laquelle il avait commençée. La boucle était bouclée.

Avec les autres lettres de l'alphabet, Rejewski généra d'autres chaînes, il les nota toutes ainsi que le nombre de liens pour chacune d'entre elles. Il aboutit à quatre chaînes :

- A→F→W→A : *3 liens*
- B→Q→Z→K→V→E→L→R→I→B : *9 liens*
- C→H→G→O→Y→D→P→C : *7 liens*
- J→M→X→S→T→N→U→J : *7 liens*

Jusqu'ici, nous n'avons considéré que les liens entre la première et la quatrième lettre des six lettres formant le message-clef. Rejewski, lui, répéta cet exercice pour les relations entre les deuxième et cinquième lettres et les troisième et sixième lettres, établissant pour chaque cas le nombre de chaînes et de liens dans chaque chaîne. Il remarqua que le nombre de chaînes changeait chaque jour de même que le nombre de liens dans chaque chaîne.

Toutefois il remarqua en construisant ces chaînes qu'il ne pouvait y avoir que 3 configurations différentes, encore appelées structures cycliques :

- 2 chaînes de 13 liens chacun.
- 6 chaînes respectivement de 9, 9, 3, 3, 1 et 1 liens chacun.
- 6 chaînes de 10, 10, 2, 2, 1 et 1 liens chacun.

Notons que l'exemple précédent qui contient 4 chaînes de 9, 7, 7 et 3 liens chacun ne correspond donc pas à une authentique structure cyclique. A partir d'ici, Rejewski s'écarte réellement des anciennes méthodes de décryptage s'appuyant des analyses statistiques et pour la première fois une théorie mathématique sera utilisée : la théorie des permutations dont nous nous sommes servis lors de la démonstration des propriétés de la machine Enigma, section 3.3.

En de simples termes le théorème employé par Rejewski dit :

$t \circ e \circ t^{-1}$ a la même structure cyclique que e

Dans le chiffrement d'Enigma, t peut représenter la permutation effectuée par le tableau de fiches sur les lettres entrantes en provenance du clavier et t^{-1} celle effectuée sur les lettres sortantes après leur passage à travers le brouilleur. De même on peut considérer que e est la permutation effectuée au niveau du brouilleur. Le résultat précédent permet donc de conclure que la structure cyclique d'Enigma dépendait uniquement du brouilleur et que le tableau de fiches n'avait sur elle aucune influence. En d'autres termes les cryptanalystes polonais pouvaient désormais ignorer le tableau de fiches, ce qui leur simplifiait grandement la tâche puisque c'est essentiellement le tableau de fiches qui créait la complexité en multipliant par un facteur de 1 507 382 749 377 250 le nombres de possibilités différentes pour coder un message (cf. section 3.2).

La structure cyclique que Rejewski avait découverte était produite par la substitution générée par le rotor le plus à droite dans le brouilleur encore appelé rotor rapide car c'est celui qui tourne d'un cran à chaque fois qu'une lettre est tapée sur le clavier. En effet dans 21 cas sur 26 les rotors du milieu et de droite restaient fixes pendant que l'opérateur tapait les six lettres du mot-clef, on peut donc raisonnablement les supposer immobile. Rejewski utilisa alors ces structures cycliques pour établir six équations qui, une fois résolues, mettraient à jour les câblages internes du rotor rapide. Mais les inconnues de ces équations n'étaient pas si simples et pour cause : il s'agissait de collections de 26 éléments chacune. Il s'attacha alors à résoudre ce système fort complexe mais le nombre d'inconnues le submergea. Il devint clair à Ciezki, qui lui rendait visite de temps en temps dans son bureau solitaire, que Rejewski ne trouverait pas la solution tout seul. Ciezki se résolu alors à lui fournir les informations de Hans Thilo Schmidt, qu'il lui avait volontairement cachées afin de ne pas rendre la cryptanalyse polonaise dépendante des dons de la France.

La connaissance des carnets de code permit immédiatement de dévoiler certaines inconnues et de simplifier le reste des équations. Mais elles restaient complexes et Rejewski continua de se débattre avec elles pendant plusieurs semaines. Un jour il se rendit compte que ses suppositions sur les câblages entre le clavier et la plaque d'entrée (*Eintrittswalze*, en amont du brouilleur) pouvaient être erronées. Il avait en effet supposé que la lettre `Q` du clavier était reliée à la lettre `A` de la plaque d'entrée, la lettre `W` à la lettre `B`, et ainsi de suite dans l'ordre des lettres sur le clavier, selon les observations qu'il avait faites sur la version commerciale de l'Enigma achetée par le Biuro Szyfròw.

Peut-être que la lettre A du clavier était simplement reliée à la lettre A de la plaque d'entrée. Il ajusta alors ces équations et des solutions satisfaisantes se présentèrent : le cryptanalyste polonais venait de mettre à jour le câblage interne du rotor rapide, nous étions en décembre 1932. Mais ce succès ne permettait pas encore de reconstruire une machine Enigma car seul un rotor était maintenant entièrement connu. Par chance, à cette époque-là les Allemands changeaient l'ordre des rotors dans le brouilleur tous les trois mois. Ainsi Rejewski put de servir de la même technique que précedemment, en même temps que des informations fournies par l'espion allemand, pour découvrir les câblages des autres rotors lorsqu'ils occupaient la position de droite dans le brouilleur.

Le long travail du Bureau du Chiffre

Une fois les rotors connus, le bureau du chiffre polonais pu construire une réplique d'Enigma. Mais cela ne lui permit pas encore de lire les messages allemands car l'atout d'Enigma réside dans le fait que même en possession d'une machine, un ennemi ne pourrait lire un message crypté sans en connaître la clef. Rejewski et son équipe de cryptanalystes étaient donc maintenant face à un nouveau défi. Utilisant les clefs fournies par Hans Thilo Schmidt, ils avaient pu reconstruire Enigma, et maintenant, utilisant leur réplique, ils avaient à retrouver les messages-clefs quotidiens pour pouvoir déchiffrer les messages comme le faisaient chaque jours des milliers d'opérateurs allemands. L'équipe du Biuro Szyfròw commença alors à répertorier les structures cycliques qu'engendraient chacune des 105 456 dispositions initiales du brouilleur. Cela lui prit un an pour terminer ce répertoire, mais à l'issue de ce travail, les cryptogrammes allemands étaient en mesure d'être décryptés. Chaque jour, Rejewski collectait le maximum de messages allemands et notait les six premières lettres qui constituaient le message-clef pour ensuite dresser des chaînes comme nous l'avons vu précédemment. Il pouvait alors consulter son répertoire qui contenait toutes les dispositions du brouilleur indexées suivant les sortes de chaînes. Il en déduisait la clef du jour concernant l'agencement et l'orientation des rotors. Il lui restait alors à trouver les connexions du tableau de fiches : il entrait un message crypté dans la machine Enigma avec la disposition correcte du brouilleur et effectuait ensuite une analyse statistique des fréquences de lettres pour retrouver la permutation effectuée par le tableau de connexions.

Ainsi, les travaux de Rejewski avaient rendu les communications allemandes transparentes. Ils constituent l'une des plus importantes réalisations de la cryptanalyse pendant la Seconde guerre mondiale.

Les Polonais utilisèrent cette méthode pendant plusieurs années. Lorsque les Allemands apportèrent une modification au brouilleur, tout le répertoire de Rejewski devint inutilisable. Loin de se décourager, le bureau du chiffre polonais conçut alors une version mécanisée de son système de répertoire qui en fonction des longueurs de chaînes donnait les réglages du brouilleur. Cette machine était capable de vérifier les 17 546 alignements possibles des rotors assez rapidement : en quelques heures, voire un jour. Six machines furent construites afin de vérifier en même temps les six placements possibles des rotors. Ces machines furent baptisées *bombes* polonaises (*Bomby*[3]). Pendant une partie des années 1930, Rejewski et ses collègues travaillèrent donc sans répit à la recherche des clefs d'Enigma...

Toutefois en décembre 1938, les Allemands renforcèrent la sécurité d'Enigma. Elle possédait alors trois rotors alignés choisis non plus parmi trois mais parmi cinq possibles. Il existait donc maintenant soixante agencements des rotors possibles dans la machine Enigma. Rejewski était alors débordé : non seulement il devait construire dix fois plus de bombes, ce qui correspondait à quinze fois le budget du Bureau du Chiffre polonais, mais il devait également retrouver les câblages internes des deux nouveaux rotors...

4.2. L'activité de Bletchley Park

Un manoir victorien pour les cryptanalystes

Devant la nouvelle invincibilité d'Enigma et la guerre qui approchait à grands pas, les Polonais mirent au courant Français et Anglais de leurs avancées, et leur donnèrent une copie de la machine Enigma qu'ils avaient fabriquée, espérant qu'ils auraient plus de moyens pour parvenir au déchiffrement.

FIG. 4.3.: Le manoir de Bletchley Park

Pendant treize ans, Britanniques et Français avaient tenu pour acquis qu'Enigma était intouchable, et voilà donc que l'espoir renaissait. Les révélations polonaises avaient fait apparaître des failles dans le chiffrement d'Enigma, ce qui remonta le moral des Al-

[3]Leur nom vient peut-être du cliquetis qu'elles émettaient lorsqu'elles étaient en fonctionnement, mais cette version des faits est sujette à controverse.

liés. Certes les avancées polonaises avaient été contrées par les nouveaux rotors mais Enigma n'était plus tenu pour un chiffre parfait.

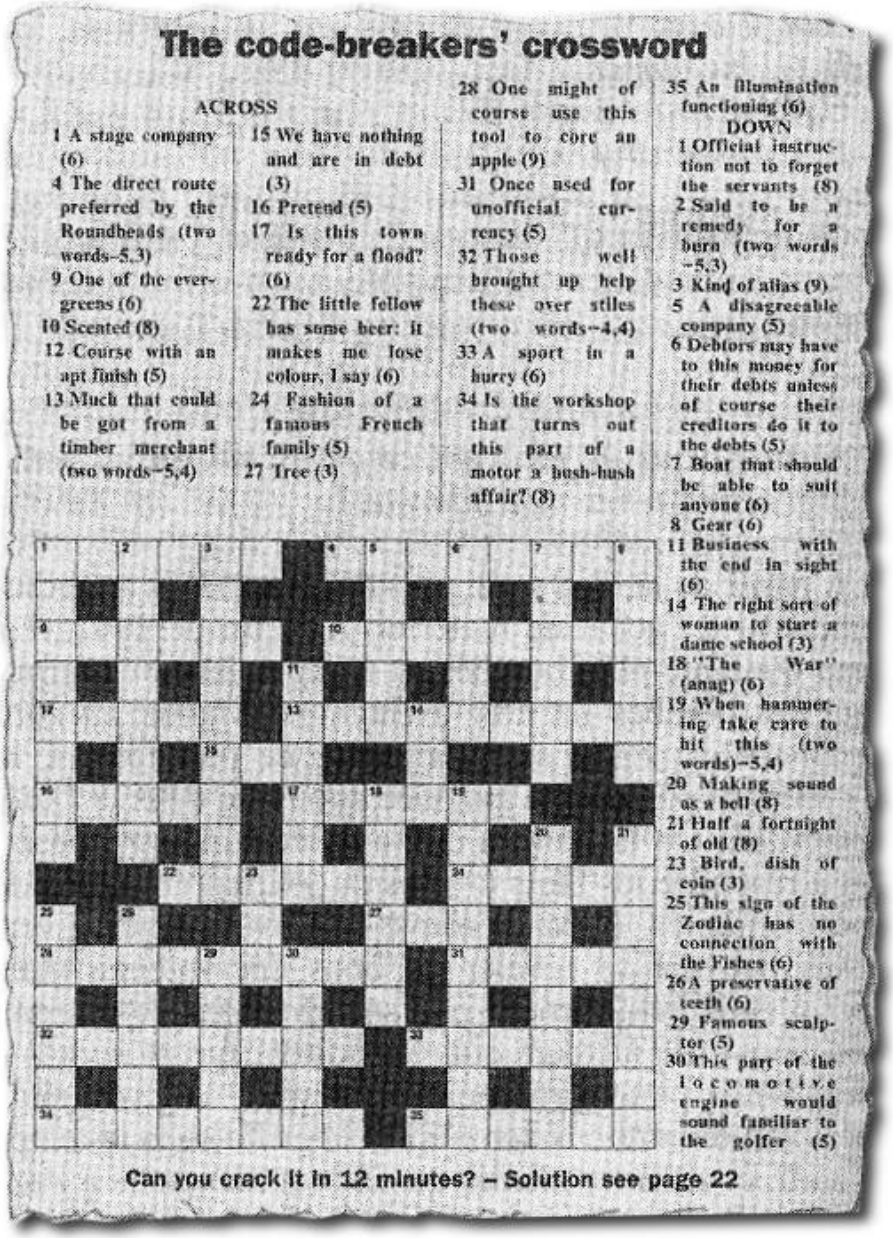
C'est ainsi qu'en Angleterre, les dirigeants du Bureau 40 (*Room Forty*[4]) s'activèrent pour rattraper leur retard sur Enigma, recrutèrent des mathématiciens, notamment parmi les meilleurs étudiants des universités de Cambridge et d'Oxford (Trinity College, King's College...) et fondèrent la *GC&CS*[5] à *Bletchley Park* dans un grand manoir de style victorien, seul lieu ayant la capacité d'accueillir tous ces cryptographes.

Les scientifiques et mathématiciens britanniques se familiarisèrent avec le chiffre d'Enigma et avec les méthodes polonaises et découvrirent eux-mêmes des raccourcis pour trouver les clefs d'Enigma. Bletchley Park disposait de plus de ressources et de personnel que le Bureau du Chiffre polonais et put donc s'attaquer à la cryptanalyse d'Enigma. Les équipes de cryptanalystes effectuaient les *3/8*[6] pour ne pas être débordés par le flot incessant de cryptogrammes allemands captés par des stations de contrôle sur la côte et envoyés sans tarder à Bletchley Park. De nouvelles recrues avaient été embauchées grâce à des mots-croisés publiés dans le *Daily Telegraph* : quiconque terminait des mots-croisés tel que celui présenté en figure 4.4, en moins de douze minutes, était invité à se présenter à Bletchley pour subir des tests d'entrée.

Turing à l'oeuvre

Les Allemands avaient remarqué que la répétition des clefs en début de message constituait un point faible à la sécurité d'Enigma. C'est pourquoi ils supprimèrent cette répétition dès le déclenchement de la guerre. C'est alors qu'Alan Turing (1912-1954), étudiant à l'Université de Cambridge venu à Bletchley Park, mis au point une nouvelle technique de décryptage appelée le *mot probable*. En étudiant de nombreux cryptogrammes allemands, il remarqua qu'on pouvait souvent prédire une partie du contenu d'un message ou au moins quelques mots. Par exemple, les Allemands émettaient chaque jour un bulletin météo chiffré avec Enigma qui contenait presque à coup sûr le mot *Wetter*. Il restait alors à deviner la position de ce mot probable en s'appuyant sur le fait qu'*une lettre n'est jamais codée par elle-même*. Turing appliqua alors la même stratégie que Rejewski : sachant qu'il était impossible de tester toutes les clefs imaginables d'Enigma, il voulut séparer la question des réglages des rotors de la question

[4] voir lexique.
[5] *Government Code & Cipher School*.
[6] Trois équipes travaillent huit heures d'affilée en se relayant, ce qui permet de garder une activité vingt-quatre heures sur vingt-quatre.



The code-breakers' crossword

ACROSS

1 A stage company (6)
4 The direct route preferred by the Roundheads (two words–5,3)
9 One of the evergreens (6)
10 Scented (8)
12 Course with an apt finish (5)
13 Much that could be got from a timber merchant (two words–5,4)
15 We have nothing and are in debt (3)
16 Pretend (5)
17 Is this town ready for a flood? (6)
22 The little fellow has some beer: it makes me lose colour, I say (6)
24 Fashion of a famous French family (5)
27 Tree (3)
28 One might of course use this tool to core an apple (9)
31 Once used for unofficial currency (5)
32 Those well brought up help these over stiles (two words–4,4)
33 A sport in a hurry (6)
34 Is the workshop that turns out this part of a motor a hush-hush affair? (8)
35 An illumination functioning (6)

DOWN

1 Official instruction not to forget the servants (8)
2 Said to be a remedy for a burn (two words –5,3)
3 Kind of alias (9)
5 A disagreeable company (5)
6 Debtors may have to this money for their debts unless of course their creditors do it to the debts (5)
7 Boat that should be able to suit anyone (6)
8 Gear (6)
11 Business with the end in sight (6)
14 The right sort of woman to start a dame school (3)
18 "The War" (anag) (6)
19 When hammering take care to hit this (two words)–5,4)
20 Making sound as a bell (8)
21 Half a fortnight of old (8)
23 Bird, dish of coin (3)
25 This sign of the Zodiac has no connection with the Fishes (6)
26 A preservative of teeth (6)
29 Famous sculptor (5)
30 This part of the locomotive engine would sound familiar to the golfer (5)

Can you crack it in 12 minutes? – Solution see page 22

FIG. 4.4.: Des mots-croisés du Daily Telegraph publiés à des fins de recrutement

FIG. 4.5.: Alan Turing, un génie des mathématiques qui n'avait que 23 ans !

des connexions du tableau de fiches. En effet, même si le nombre de clefs est gigantesque, le nombre de combinaisons possibles pour les rotors est *seulement* de 105 456, ce qui est à la portée des machines telles que les bombes de Rejewski. En s'inspirant de celles-ci, Turing mit au point lui-même les plans de ces nouvelles bombes. Grâce à la connaissance des alignements des rotors, il put ensuite en déduire assez facilement les connexions du tableau de fiches.

L'organisation du travail à Bletchley Park

Pour acceuillir autant de mathématiciens, cruciverbistes, linguistes et autres joueurs d'échec reconvertis dans la cryptanalyse, ainsi que de matériel, des *huttes* avaient été construites autour de Bletchley Park. Chaque hutte était spécialisée dans un domaine précis. Ainsi, une hutte s'occupait de la réception des cryptogrammes, de leur stockage et de leur transmission aux équipes chargés de les déchiffrer ; d'autres huttes étaient spécialisées dans la recherche de mots probables ou tout autre moyens de s'attaquer aux cryptogrammes ; et d'autres encore déchiffraient ces messages cryptés à l'aide des bombes de Turing.

En 1940, seize bombes furent mises en service à Bletchley Park. Quand tout allait bien, une bombe pouvait trouver la clef d'Enigma en une heure mais souvent il fallait changer le mot probable et recommencer, ce qui pouvait prendre parfois deux jours. Pourtant, lorsqu'un message était décrypté, on pouvait en déduire la clef du jour et tous les messages envoyés le même jour pouvaient être décryptés. Il faut toutefois relativiser cette affirmation puisque chaque armée allemande avait développé son propre

FIG. 4.6.: Les Stations Y : Imaginez-vous assis huit heures par jour avec de lourds écouteurs collés sur les oreilles à répertorier des suites de lettres qui n'avaient aucun sens puisqu'elles étaient chiffrées !

système de communication, c'est-à-dire ses propres carnets de code pour chaque mois, et parfois sa propre machine Enigma. Par exemple l'*Afrikakorps* de Rommel en Afrique du Nord avait son propre réseau et ses opérateurs n'utilisaient pas la même clef du jour que les armées allemandes sur le front russe. Identifier la clef du jour pour l'Afrique du Nord permettait de déchiffrer les messages envoyés par les troupes de Rommel mais ne servait à rien en ce qui concerne les messages transmis en Europe. De même, la *Luftwaffe*, la *Kriegsmarine* ou les sous-marins aux ordres de l'Amiral Doenitz avaient chacun leur propre réseau.

Le réseau de la Kriegsmarine était le plus difficile à pénétrer, car la marine allemande utilisait une version plus sophistiquée d'Enigma où quatre rotors étaient alignés choisis parmi un nombre de rotors plus grand, ce qui porte le nombre de possibilités de les placer différemment à 672. Il s'agit de l'Enigma M4, c'est celle qui a donné le plus de fil à retordre aux Britanniques et celle dont l'enjeu a été le plus important pour la guerre.

Les Stations Y

Les messages transmis par l'armée allemande étaient interceptés par des stations d'écoute situées sur les côtes anglaises et connues sous le nom de *Stations Y*. Ces stations interceptaient plusieurs centaines de messages ennemis chaque jour et les envoyaient directement à Bletchley Park où ils étaient décryptés. Elles comportaient d'immenses paraboles qui étaient capables d'entendre des signaux radios provenant de Russie et même du Japon. Des équipes d'opérateurs spécialisés dans le code morse travaillaient ici vingt-quatre heures par jour, leur tâche était de traduire les signaux morses en let-

tres puis d'écrire les enchaînements de lettres du message codé. Une seule erreur de leur part pouvait rendre impossible toute la cryptanalyse du message.

5. L'influence d'Ultra sur la guerre

La cryptanalyse d'Enigma, lorsqu'elle était possible, a permis aux Alliés de connaître les faits et gestes des armées allemandes pendant certaines opérations de la guerre, comme la bataille de l'Atlantique, les combats en Afrique du Nord ou même le débarquement en Normandie.

5.1. La bataille de l'Atlantique

Les messages décryptés à Bletchley Park étaient copiés sur place et triés. Les plus compromettants étaient envoyés à l'*OIC* (*Operational Intelligence Center*) qui transmettaient ensuite les informations aux différents ministères concernés — au ministère de la guerre, de l'air, à l'amirauté... — sans préciser qu'elles provenaient de la cryptanalyse d'Enigma : la source d'information qu'était Enigma avait pour nom de code *Ultra* et peu nombreux étaient ceux qui savaient à quoi ce nom référait. Ainsi, Ultra influençait directement les décisions militaires prises par la Grande-Bretagne pendant la Seconde guerre mondiale. Exemple de la bataille de l'Atlantique.

L'importance de cette bataille

Le destin de la bataille de l'Atlantique a été véritablement influencé par la cryptanalyse d'Enigma, assez paradoxalement puisque l'Enigma navale utilisée par les *U-Boote*, les sous-marins allemands qui sillonnaient l'Atlantique à la recherche de convois alliés, était aussi la plus coriace de toutes les versions car elle possédait un rotor de plus.

Les Etats-Unis ayant signé la loi *prêt-bail* avec la Grande-Bretagne en 1941, des convois américains approvisionnaient régulièrement l'île britannique en matières premières, carburant, armes et nourriture pour lutter contre la pénurie grandissante qui était apparue avec le début des hostilités. A l'heure où l'Angleterre, après la débâcle de Sedan, était seule face à l'Axe, il était d'une importance capitale pour elle de maintenir ce lien vital et donc de protéger ces convois contre d'éventuels agresseurs. Le destin du pays

était alors très lié à celui des convois ; sans quoi, par exemple, les avions de la *Royal Air Force* n'auraient pas eu suffisamment de carburant pour défendre leur île lors de la bataille d'Angleterre. On comprend donc l'enjeu de la bataille de l'Atlantique.

Cette lutte entre les bateaux alliés apportant du ravitaillement, et les sous-marins allemands, cherchant à briser ce dernier lien qui empêchait encore l'Angleterre de capituler, a été la plus longue bataille de la guerre car elle commença le premier jour pour se terminer le dernier. Winston Churchill l'évoque ici :

> "*La bataille de l'Atlantique fut tout au long de la guerre un élément de première importance. Pas un seul instant, nous ne pouvions oublier, que tout ce qui passait ailleurs, sur terre, sur mer ou dans les airs, dépendait en fin de compte de son aboutissement.* [...] *Dans un torrent d'événements tragiques, une angoisse dominait. Des batailles pouvaient être gagnées ou perdues, des mouvements pouvaient rencontrer le succès ou l'échec, des territoires pouvaient être conquis ou abandonnés, mais ce qui nous permettait de continuer la guerre, ou simplement de rester vivants, était notre maîtrise des voies maritimes et la possibilité d'entrer et de sortir librement de nos ports.*"

Le décryptement de l'Enigma navale

Jusqu'au début de l'année 1942, l'Enigma M3 était en service et les cryptanalystes de Bletchley Park étaient en mesure de déchiffrer les cryptogrammes allemands dans un délai convenable. Une chambre spéciale appelée *Submarine Tracking Room* avait été créée et centralisait toutes les données concernant la localisation et les mouvements des U-Boote. Ce bureau possédait une immense carte de l'Atlantique sur laquelle était positionnée des sous-marins et bateaux miniatures indiquant la position des convois anglo-saxons. Grâce à cette immense carte qui s'appuyait non seulement sur Ultra mais aussi sur la reconnaissance aérienne, sur des échos sonars et sur la radiogoniométrie, l'état-major pouvait ordonner à des convois de changer de cap pour contourner une meute de sous-marins.

Ainsi jusqu'en 1942, les informations fournies sur l'emplacement des U-Boote permirent de limiter le nombre de navires torpillés. Pourtant, dès le début de l'année 1942, l'Allemagne entre véritablement dans une industrie de guerre, construit plus de U-Boote, et l'amiral Karl Doenitz, inquiété du peu d'efficacité de ses sous-marins, renforce la sécurité des communications entre eux en complexifiant la machine à crypter. L'Enigma M3 disparait donc au profit de l'Enigma M4 dans les sous-marins allemands.

Le black-out de 1942 et ses conséquences

Confronté à cette nouvelle version d'Enigma, l'équipe de cryptanalystes de Bletchley Park est déconcertée. Pendant toute l'année de 1942 la hutte 8 ne déchiffra seulement trois clefs du jour, chacune nécessitant plusieurs semaines de travail ! La Submarine Tracking Room affirma en 1942 être incapable de connaître la position des sous-marins allemands, pour la première fois depuis le début de la guerre. Alors qu'en 1941, pendant que Ultra était utilisée pour détourner les convois alliés des meutes de U-boote, seul un convoi sur dix était repéré, ce nombre passa à un sur trois en 1942 pendant le black-out. Par conséquent, le tonnage coulé dans l'Atlantique nord, qui atteignait 600 000 tonnes durant les six derniers mois de 1941, a été multiplié par plus de quatre dans la deuxième moitié de l'année 1942, atteignant le record de 2 600 000 tonnes ! Et chacun des cinq cent bateaux coulés durant ces six mois entraînait moins de nourriture pour la population, mois de munitions pour les soldats, mois de carburant pour les avions et la perspective de prolonger encore toutes ces misères... La crainte que l'impuissance des services de renseignements, associée au nombre croissant de sous-marins, ne provoque la perte de plus de navires que l'Amérique ne puisse en produire atteint son paroxysme fin 1942. C'est pourquoi l'OIC fit pression sur Bletchley Park pour qu'elle trouve à tout prix le moyen de mettre un terme à ce black-out.

Dans l'impossibilité de trouver les clefs du jour, Bletchley Park eut alors l'idée de les subtiliser par la force. C'est ainsi que des opérations visant à capturer l'Enigma navale et ses livres de code furent mises sur pied. Ces attaques devaient être très rapides pour surprendre l'équipage des sous-marins afin qu'ils n'aient pas le temps de détruire les documents secrets et de jeter la machine par-dessus bord. De plus, elles ne devaient absolument pas suggérer aux Allemands que leur code avait été compromis...

La plus célèbre de ces captures a été celle du U-559, forcé de faire surface en octobre 1942 au large de la Méditerranée. Le courage et l'obstination de Fasson et Grazier, deux marins de la Royal Navy, leur permirent de ramener intacte une Enigma M4, ses carnets de code, et le code météo utilisé par les U-Boote. Ils n'assistèrent toutefois pas aux formidables conséquences de leur acte puisqu'ils périrent noyés avec le U-559 sans qu'ils n'aient eu le temps d'en sortir. Tous ces documents saisis per-

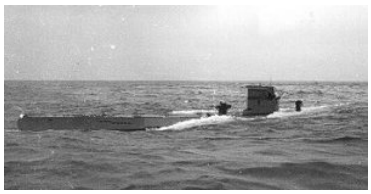


FIG. 5.1.: Un U-Boot allemand

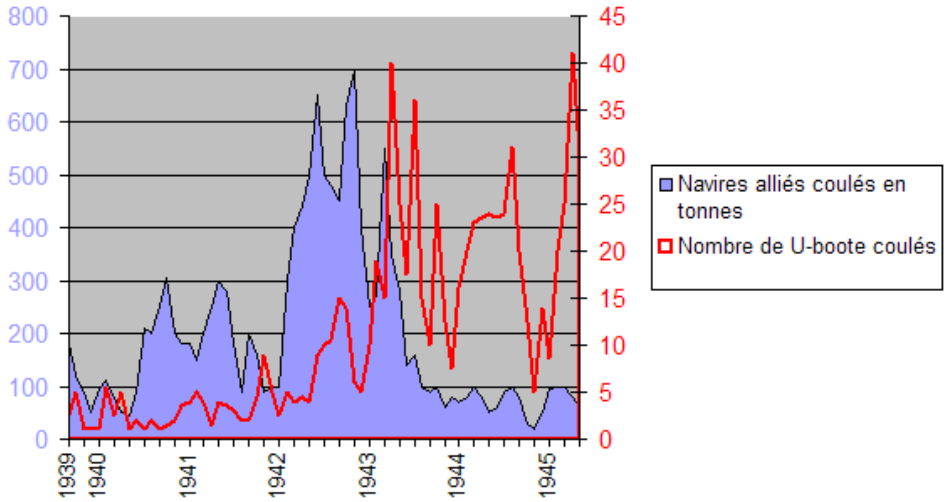


FIG. 5.2.: Diagramme comparant les pertes de navires alliés aux pertes de sous-marins allemands au cours de la guerre

mirent aux cryptographes de Bletchley Park de briser le chiffre de l'Enigma navale, et en 1943 les pertes des navires alliés baissèrent à nouveau.

A partir de 1943, on assiste à un spectaculaire renversement de situation dans la bataille de l'Atlantique. Non seulement les communications adverses sont à nouveau transparentes mais les convois bénéficient des dernières technologies de guerre : le radar centésimal en plus de l'habituel *ASDIC*[1], des grenades anti-sous-marines plus puissantes et une protection aérienne plus efficace grâce aux bombardiers *B-24 Liberator* à long rayon d'action. Les U-Boote ne sont plus les chasseurs mais sont devenus des proies. Sur 1170 U-Boote en action pendant la seconde guerre mondiale, 780 furent détruits, tuant dans des conditions effroyables 2700 marins (cf. FIG. 5.2). L'échec pour Doenitz est total : ils n'ont pu empêcher les liaisions entre les Etats-Unis et la Grande-Bretagne.

Bilan

Les historiens s'accordent pour dire qu'Ultra a été un facteur déterminant dans la victoire anglaise de la bataille de l'Atlantique. Sans cette source d'informations, les Allemands auraient conservé une plus grande flotte de sous-marins et davantage de capacités d'intervention. Cela aurait compromis le lien vital avec l'Amérique et les

[1]Sonar.

Alliés auraient dû consacrer des moyens humains et financiers considérables à la construction de nouveaux bateaux. Les historiens estiment les plans alliés auraient été retardés de plusieurs mois et le débarquement repoussé au moins à l'année suivante.

5.2. Les prouesses ponctuelles du décryptage d'Enigma

Bien que les avantages de la cryptanalyse d'Enigma se soit énormément fait sentir, et cela tout au long de la guerre, dans la bataille de l'Atlantique, le décryptage des messages allemands encodés avec Enigma a également permis des prouesses plus ponctuelles lors de certains évènements de la guerre.

La bataille d'Angleterre

Le 8 août 1940, Hitler lance la Luftwaffe contre la Royal Air Force. Le nombre inférieur de chasseurs anglais face aux appareils allemands est alors compensé par les messages quotidiennement interceptés et déchiffrés à Bletchley Park. A cette époque, il existe une ligne directe entre Bletchley et le centre de commandement de l'aviation à Stanmore dont le trafic journalier est de près de deux cent messages, indiquant à quelques heures près la connaissance détaillée des plans et cibles d'attaques allemandes. Cela permit aux Anglais, en combinant ces informations avec celles obtenues par leurs radars, de faire un usage plus efficace de leurs escadrilles d'aviation, leur évitant du même temps d'être submergés par l'aviation allemande.

Ainsi, le 15 septembre 1940, Hermann Goering ordonna une attaque massive avec 328 bombardiers et 769 chasseurs qui devait constituer le coup final de la bataille d'Angleterre. Prévenu par Bletchley Park, le commandement suprême de l'armée de l'air mit sur pied un comité d'accueil réunissant tous les appareils encore en état de combattre, et put déjouer l'offensive allemande. Deux jours plus tard, Bletchley décrypta l'ordre d'abandonner l'opération *Seelöwe* et de mettre fin à la bataille d'Angleterre.

L'Afrique du Nord

L'implication de Bletchley Park dans la guerre en Afrique du Nord débuta dès 1941 lorsque le général Rommel ayant envahi la Libye et commençant son offensive vers l'Egypte utilisait la machine Enigma pour crypter les communications de ses unités.

En septembre 1941, Bletchley Park fit une avancée majeure en parvenant à décrypter la version d'Enigma utilisée par l'*Afrikakorps* de Rommel. Ce fut un atout de grande importance sur le théâtre des opérations car la bataille était incertaine et le front avança et recula jusqu'à six fois pendant la campagne. Pour être plus efficace, Bletchley Park détacha même un de ses centres au Caire. Le décryptement des communications allemandes fournit aux britanniques des informations sur les navires de l'Axe ravitaillant l'Afrikakorps en munitions et en carburant. Cela permit en partie aux Alliés de couler quarante-sept navires de ravitaillement, donc de paralyser temporairement l'Afrikakorps. La nomination du général Montgomery à la tête de la 8ème Armée britannique qui accumulait plus de trois fois plus de matériel que l'ennemi précipita encore la retraite de l'armée allemande jusqu'en Tunisie. Rommel s'était alors plaint auprès d'Hitler que son armée était épuisée, et les tentatives de ravitaillement trop sporadiques et totalement inadéquates.

Les armes de la terreur : V1 et V2

En Allemagne à Peenemünde, des scientifiques allemands faisaient des recherches secrètes sur des combustibles liquides qui permettraient d'envoyer des bombes volantes sur des cibles déterminées à l'avance. Malgré les quelques témoignages reçus par le gouvernement anglais sur l'activité de la base de Peenemünde, les autorités britanniques se refusaient à croire que de telles performances étaient possibles dans un futur proche et ne considéra pas la menace au sérieux.

Encore une fois, l'aide du décryptage d'Enigma fut précieuse puisqu'elle permis de mettre en lumière les projets des Allemands et de connaître leur avancement, ce qui, cette fois-ci, alerta les autorités anglaises. Ces dernières envoyèrent des avions de reconnaissance patrouiller sur la côte Baltique, qui confirmèrent l'existence de cette base secrète. En raison de la menace sérieuse que ces armes représentait pour la Grande-Bretagne, des raids aériens massifs furent organisés sur Peenemünde en août 1943, ce qui retarda les expérimentations et productions des V1 et V2 d'au moins au mois, et obligèrent les Allemands à déplacer leurs usines de production.

De plus, en avril 1943, Hitler se préparait à construire des rampes de lancement sur les côtes françaises. Ultra intercepta les ordres d'Hitler visant à établir un quartier général près d'Amiens pour contrôler les opérations de lancement des fusées V1, ce qui confirma aux Alliés qu'il leur fallait lancer au plus vite les opérations de débarquement avant que les rampes de lancement ne soient prêtes.

Opération Overlord : le débarquement en Normandie

L'aide apportée par Ultra pour les opérations du débarquement s'est notamment fait ressentir dans la campagne d'intoxication menée par les Alliés visant à persuader les Allemands que le débarquement aura lieu dans le Pas-De-Calais, connue sous le nom d'*Operation Fortitude*. En effet, connaissant les craintes des Allemands d'un débarquement dans le Pas-De-Calais grâce à Ultra, les Alliés ont tout fait pour entretenir cette crainte et tromper les Allemands quant au véritable lieu du débarquement : la Normandie. Par exemple un QG imaginaire entouré de chars gonflables et d'engins factices est mis sur pied dans le Kent, en face du Pas-De-Calais, pour duper la reconnaissance aérienne allemande.

De plus, un concours de circonstances a permis aux Alliés grâce à Ultra d'en savoir plus long sur la disposition des armées allemandes dans le nord-ouest de la France. En effet, un désaccord entre Hitler et ses généraux a fourni des détails de première importance sur l'organisation de la défense allemande le long des plages normandes. Rommel est convaincu que la seule façon de battre les Alliés sera de les arrêter sur le rivage avant qu'ils ne puissent consolider leur tête de pont. Aussi demande-t-il que les divisions de Panzer tiennent position le plus près possible des côtes. Son supérieur hiérarchique, le vieux maréchal Von Rundstedt est pour sa part d'un avis diamétralement opposé. Il estime qu'un groupe de divisions blindées doit se tenir largement en retrait du front afin d'être engagé dans une contre-offensive décisive qui rejettera les assaillants à la mer. Quoi qu'il en soit, tout au long du printemps 1944, la discussion fit rage, ce qui assura à Bletchley Park de nombreux messages compromettants, révélant notamment que trois divisions de Panzer sous les ordres de Rommel seront sur la côte, que deux divisions seront placées au nord de la Seine et que quatre autres sont en réserve près de Paris sous le commandement personnel d'Hitler.

Grâce à Ultra, le décors du théâtre des opérations de Normandie est donc à peu près révélé. C'était alors aux soldats de faire leurs preuves.

6. Le décryptage d'Enigma

Dans ce chapitre est expliquée une méthode de décryptage d'Enigma qui n'aurait pu être mise en œuvre durant la Seconde guerre mondiale : elle n'est permise que par la puissance actuelle des ordinateurs.

6.1. L'indice de coïcidence

Nous allons utiliser ici une approche plus moderne que celle utilisée par Turing et Rejewski pour décrypter un message d'Enigma. Cette méthode est plus simple que celle mise au point par les britanniques et les Polonais car elle ne nécessite pas de trouver au préalable des boucles ou des mots probables comme c'était le cas pendant la Seconde guerre mondiale. Elle s'appuie sur un outil linguistique puissant : l'*indice de coïncidence*.

L'indice de coïncidence

L'indice de coïncidence (IC) est la probabilité que deux lettres choisies aléatoirement dans un texte soient identiques. Il fut inventé en 1920 par William Friedman. Pour calculer cet indice, on utilise les notations suivantes :

- N est le nombre de lettres du texte dont on cherche à calculer l'IC
- n_1 est le nombre d'apparitions de la lettre A
- n_2 est le nombre d'apparitions de la lettre B
- n_3 est le nombre d'apparitions de la lettre C
- ...
- n_{26} est le nombre d'apparitions de la lettre Z

La probabilité de tirer deux A parmi les N lettres du texte est :

$$\frac{C_2^{n_1}}{C_2^N} = \frac{\frac{n_1!}{2!\times(n_1-2)!}}{\frac{N!}{2!\times(N-2)!}} = \frac{\frac{n_1\times(n_1-1)\times(n_1-2)!}{(n_1-2)!}}{\frac{N\times(N-1)\times(N-2)!}{(N-2)!}} = \frac{n_1(n_1-1)}{N(N-1)}$$

Français	Anglais	Allemand	Espagnol	Italien	Texte Aléatoire
0,074	0,065	0,072	0,074	0,075	0,038

TAB. 6.1.: Valeur moyenne de l'IC suivant la langue

La probabilité de tirer deux lettres identiques est la somme des probabilités de tirer deux même lettres pour chacune des 26 lettres :

$$\mathrm{IC} = \sum_{i=1}^{26} \frac{n_i(n_i-1)}{N(N-1)}$$

La principale propriété de l'indice de coïncidence est d'être d'autant plus grand que les fréquences d'apparitions des lettres sont déséquilibrées. Ainsi, pour un texte français assez long, cet indice vaut environ 0,074. Sa valeur varie légèrement suivant la langue du texte, voir tableau 6.1. En revanche pour une suite de lettres aléatoires où chaque lettre a la même fréquence, l'IC vaut environ 0,038. Cet outil peut donc s'avérer utile pour le décryptage d'Enigma puisque l'on pourrait :

1. Déchiffrer un texte avec un certain réglage du brouilleur d'Enigma, sans se soucier du tableau de fiches.
2. Calculer l'IC du texte décrypté.
3. Si sa valeur se situe aux alentours de 0,038, cela signifierait que le réglage initial de la machine n'est pas correct. On recommence alors en tournant les rotors d'un cran...

6.2. Le décryptement pas à pas d'un message

Pour ne pas alourdir l'explication, nous ne tiendrons pas compte ici du réglage de la bague, qui pourrait néanmoins être déterminé par un raisonnement analogue à celui présenté ci-dessous. De plus, l'exemple présenté dans les paragraphes qui vont suivre traite d'une Enigma M3 à trois rotors.

Déterminer l'ordre des rotors

La cryptanalyse d'un message Enigma nécessite :

– De trouver quels rotors sont utilisés pour crypter le message parmi les 5 possibles, en ce qui concerne la version M3.

– De connaître leur orientation initiale, par exemple `FIM`.
– De savoir quels fiches ont été reliées sur le tableau de fiches.

Laissons les fiches pour plus tard et considérons tout d'abord l'agencement et l'orientation des rotors. Nous avons démontré en section 3.2 qu'il existe 60 façons différentes de placer les cinq rotors et 17 576 possibilités pour les orienter différemment. Cela porte donc le nombre de combinaisons à tester à un peu plus d'un million au total. Ce nombre est raisonnable comparé au total des clefs d'Enigma possibles et un ordinateur actuel est en mesure de passer en revue toutes ces possibilités.

Voici comment on procède : on retire toutes les fiches du tableau de connexions de la machine Enigma, on choisit un ordre des rotors par exemple `I-II-III` et pour chaque alignement des rotors, en allant de `AAA` à `ZZZ`, on décrypte le message codé et on calcule l'indice de coïncidence. Dès lors que tous les alignements des rotors ont été testés, on change l'ordre des rotors — on met par exemple `I-II-IV` — et on recommence, et ainsi de suite pour les 60 façons possibles de placer les rotors. Au final, l'ordre et l'alignement des rotors pour lequel l'indice de coïncidence est le plus grand correspond au réglage initial du brouilleur. Une partie de la clef d'Enigma a donc été découverte...

Prenons un exemple pour mieux comprendre. On considère le texte suivant qui a été crypté avec Enigma, et l'on ne connait pas la clef qui a été utilisée pour le crypter :

```
GVJAT MQJTB FASCG CXDLW SKYLY YKTKV WBAYZ YKLQX ZXWZA NLFSG
IEBBQ PYDOO ABGRV QYLYV AQWEL PGZCC WBEEB ZWYUH EBKBO GHQDT
DBSRO PVEEU TURIQ VZNIT NDOWS WOKSZ NBBYY MIIDO KWWZE LOUUK
GCYEB ZXJPV URUGG GMVXP KTKVH KYBOB XHOGA SIIBL MNKHO OHEAY
NRKKS VBEBY ZAYMQ KNHJD NWMZV QZGGK DBPXG NPXJF GJYKG PZFWQ
YIXXF IPQNX MCHBO DYSJJ DVUOY THWLM IZYRU YLFRS ANDVG CRXKW
ZNGJN GPDKI DIPID VMUGV JRYMV FPMNS RTQFI XGXKL CDSEP NPYVM
IHBKI GYDEG OJJJE BBQMI WWIVC QYQBL RXRQA SHOBK MZBNZ HJTCF
MLUAC KQBEC YUMDI CQWUB TKRSW EPANF HKMKP DZZOZ PPQIY HPHRK
JIWLN FIKHL MQWIK SDPWT GRWLK IXYGY GGCCL YXCZY QWMMV KUVPC
MOLYS OKVXL RWPJM IFBMZ HPNRK SYOWD NTSWS IEJSQ WISJG EIWTU
SVBJS VWKJN YMITY LWKFK ASAIJ KLUCW EPZRV KGLCD TDZVL UEVWZ
BWQSL IXILO PVNSS GXLFL VVYTH WRIJV CWTBF ISTJE FVUDH OTFID
SWXSZ GADPH TXYME BPFME BCEXY IMZFR PZKLV VZKBQ JIMPF LQILQ
AHQVL PDVUJ SPRHE FYYKV AWWYV JQRIV KKEAK TCANA INWZX JKXSW
YZHKB JWKAA YIBHD MBXXA WHBMX MQBYY FYUIW PTILE TGQLR HEVBM
RSZHA ZQRWV SVXOV GOXVW QCOVZ OBVJG HURWZ AUGFE SIAGD VRXZO
FXXHY LCRFW BOFYE XOZNN PCTEN AFQZL JBFQK XZXTK KEUQH MKSKH
FOHZK YZJQQ VPJJB JPYPO QMOBX EOBNA YBVWW UNFAP JOGGL PQZCP
QJWCB QCUKE TWWDJ IEUUK XDVZK AWSXX HWWAU OFSZZ RSLTB GHRKV
HMLLM RYUWE MWXEU ANYGC SEWCQ LYZSM AIARV REDVB XLXDK FXZEG
```

```
VBFWN MTSIW JWYYA SXCYK ZMINH BAJOJ VXOPT XEPVF MJSVA YXIIN
BFCKU JWBBN FCLNB PDXYL IEBXT WQLTF UBJHS SRTUQ DQRWD MRMBY
LWIZK GQQKC WTJNF WXSDW NASZS XGMBI OKRWB ACRTN LRBLQ IPWLV
YLARY UXYCQ UOQUM PZOGA RIVEL SOVDO JISKG RINJW KAJYH LPGMB
DHT
```

Grâce à un programme informatique simulant Enigma, nous pouvons alors décrypter le message avec Enigma pour une position des rotors donnée et il est facile de calculer l'indice de coïncidence selon la méthode expliquée précédement. Il suffit alors de faire tourner le programme en boucle pour qu'il teste toutes les positions possibles des rotors et relève à chaque fois l'indice de coïncidence. Nous avons consigné une partie des résultats de cette boucle dans le tableau ci dessous :

Agencement des rotors	Alignement des rotors	IC
	...	
`I II III`	`BTA`	0,0386
`I II III`	`BTB`	0,0648
`I II III`	`BTC`	0,0386
`I II III`	`BTD`	0,0386
`I II III`	`BTE`	0,0385
	...	

On constate que pour l'ordre des rotors `I-II-III` et l'alignement `BTB`, l'indice de coïncidence est nettement supérieur à celui des autres réglages. On peut donc en déduire sans risque que pour chiffrer le message, les rotors utilisés sont `I-II-III` dans cet ordre et ils sont alignés sur `BTB`. L'indice de coïncidence est toutefois inférieur à la valeur moyenne d'un texte français car les branchements du tableau de fiches ne sont pas encore connus. En effet un simple cryptage par substitution monoalphabétique ne modifie pas la valeur de l'IC car les fréquences des lettres prises dans leur ensemble restent les mêmes. Or ici il faut rappeler que le tableau de fiches n'effectue pas qu'une simple substitution monoalphabétique car chaque lettre est permutée au niveau de fiches à l'entrée du brouilleur mais aussi à sa sortie ! D'où un IC légèrement inférieur à 0,074.

La détermination des fiches branchées

La dernière étape du décryptage est de déterminer quelles fiches ont été branchées et quelles lettres sont donc permutées. Il s'agit tout d'abord de décrypter le message

avec l'ordre et la position des rotors découverte à l'étape précédente et en ne branchant aucune fiche. Puis on s'aide du cryptogramme partiellement décrypté et on y cherche des bribes du texte clair. En effet toutes les lettres ne sont pas permutées au niveau du tableau de fiches car les armées allemandes utilisaient au maximum dix fiches sur les treize possibles ce qui signifie qu'au moins six lettres du tableau de connexions n'étaient pas branchées ; il subsiste donc des portions du texte clair...

Reprenons notre exemple précédent. Nous allons tout d'abord le décrypter avec les rotors `I-II-III` alignés sur `BTB`. Puis nous recherchons des portions de mots qui seraient compréhensibles parmi ce qui semble à première vue un charabia dénué de tout sens... Voici ce que l'on obtient :

LERML UTYOZ SSLJ**C RYPTO GRJPH FE**PJR SUDSY FTUTF QZJAQ MRNFT
QOMMP EUZEL STTEC OZTFZ HELLE EZXRE **CRYPT AGRJP HESET DECRY**
PTEUR SJLOR FGFZE LILXR KPTOG RJPHQ HGJGZ EZDLJ PRESF EREBJ
TJFLL GEZFZ VEZTJ OTDJZ SLJZT FQUFT EUZES EAKOD EHMPJ RJBTE
FECHF IIRED AFESJ RWUQQ EJCDQ UDLKF ZDFZE PUFZK LBURT RCQJF
LNUFO SFG**OP ERER**E TJBYT TLJCO ZIFDE NMFJL FTZDE RROMM UZFCJ
AGOZF AUSQC JVEOU EBJBB AGEDE WOUIR EUZYV YECDE **DECRY QTER**L
LSUBZ TFTUT FSZZO LYJLW HJSET FQUEJ LJUBM DUXFX EFEXS ENLED
J**CRKP TOGRJ PHFE**N TJFTD ODCDJ ZSVJW POSSF BVEFB EDEBE TJBLF
BEESM OAETD ESCVM MUZFC JTFOZ ZDEPL USJVE CLFNV EZTFO ZDELJ
TSITE LEGRJ PHFYS SNSIJ LLPZE **CESSF** MEDUZ NRWPT JLERU RWEIJ
FSJWT DEPBV SEZ**PL US**SNZ WFHBC DECLE ZCEEM EZTDE LJVEC OZDEO
UERRE AOZDF JLXMF TEZDU MFERE LEPQE TJRDU OJZEC DDOMJ FZRR**L**
ORSQC EOJTS I**PROC UR**HFT DESIJ GFGIT EBDEC OQMUZ GLJTI OTLET
WOZCJ USSFF FZTER SEPTF LZSPJ UDETE VEZUU ELFFZ ZFMXS **DESCO**
DHSUT ZLFTQ SAJRL ESMFH FTJFR ESETJ IERLP EUFFJ BLESE TRJPF
DEYEZ ADECH FIIRE SCEST LECJC DUCLD EJLLT FJZCJ DFPVX PJRWX
MMPLE GRJPE JUEJC TFCPU ESDUS TNEAU ZOGDO ZNEJU XSERV FCESD
CRENS EBMME ZTDXE BJMJA ESTEE TJUUV JPTUR EXQVL ZVRES DESOD
EALLE MJMDL ESBRQ DJZZF **QUE**BE MJFEZ TJUPO UMJNF DESMO UVEME
ZTS**DE TROUP E**DELJ HGEEJ LLEMJ ZDBHE DDIUS EMEZT **POURL** TSORY
PTVGU JPHTS PLSZU IUREV XPCML OYZJC ROUVE RUZEW OZUTG OZMDB
RYETJ HLFRO GSETR **ETDES** ROMMU ZFCJH FOZSB FEZOB LFGES DJBJX
DOZNE RLEUR MEVPN DEJVE EFRBY OZETN JPFER NLSSL DJPTE QEZTJ
UXWEC HZOLO GFESL EOPLY SBECE ZTESP LZRBR OTKXL EMIES **MESSJ**
GES

On remarque notamment que dans la première bribe du texte : `CRYPTOGRJPHE` et dans la dernière bribe : `MESSJGES`, la lettre `J` correspondrait à un `A`. On va donc brancher relier par une fiche la lettre `A` et `J` au niveau du tableau de connexions et essayer de décrypter le message pour vérifier si cette intuition est bonne. Après décryptement,

il s'avère que nous avons progressé par rapport à précédemment puisque l'indice de coïncidence du texte partiellement décrypté vaut maintenant 0,0638 alors qu'il valait 0,0603 lorsqu'aucune fiche n'était branchée. Nous sommes donc assurés que cette fiche est correcte : elle a bel et bien été utilisée pour chiffrer le message.

Il nous reste alors à faire de même pour déduire les autres fiches branchées. Nous ne décrirons pas les étapes ici car elles sont exactement identiques à celle utilisée précedemment. On trouve finalement que en plus de la fiche `AJ`, deux autres fiches ont été branchées : `FI` et `ZN`. On obtient alors un texte entièrement clair dont l'indice de coïncidence vaut 0,0733. Le voici :

> "L'évolution de la cryptographie par substitution apparaît comme une lutte continuelle entre cryptographes et décrypteurs. A l'origine, les cryptographes gagnent la première bataille en inventant dans l'Antiquité une méthode imparable, le chiffre de César, jusqu'à ce qu'Al-Kindi ne ruine leur travail. Puis Vigenère rétablit la confidentialité des communications jusqu'à ce que Babbage découvre un moyen de décrypter la substitution polyalphabétique. A l'aube du XIX^{ème} siècle, la cryptographie était donc dans l'impossibilité de rétablir le secret des communications. De plus, avec l'invention de la TSF (télégraphie sans fil), la nécessité d'un cryptage sûr se faisait de plus en plus sentir. Le déclenchement de la Seconde Guerre Mondiale mit en lumière les retards dans ce domaine : alors que la TSF procurait des facilités de communications et donc aussi d'interceptions par des éventuels ennemis, les codes utilisés par les militaires étaient peu fiables et rapidement déchiffrés, c'est le cas du code allemand ADFGVX. Par exemple, grâce aux activités du bureau 40, nom donné aux services de renseignements de sa majesté, et aux captures de livres de code allemand, les britanniques étaient au courant des mouvements de troupe de l'armée allemande. Heureusement pour les cryptographes, ils ne furent pas long à trouver une solution pour rétablir le secret des communications. Bien obligés d'abandonner leur méthode avec crayon et papier, ils s'adaptèrent aux technologies les plus récentes pour brouiller les messages."

Conclusion

Enigma, plus qu'un simple outil de cryptage utilisé par l'armée hitlérienne, a bel et bien joué un rôle considérable pendant la Seconde guerre mondiale. Son invention en 1918 constitue une véritable innovation technologique puisqu'Enigma est le premier système électromécanique de cryptage. Tenant en échec les agences cryptographiques d'Europe occidentale, le déclenchement de la guerre en 1939 lui offrit l'occasion de faire ses preuves : Enigma changea le visage du conflit, le transformant réellement en guerre du renseignement opposant les armées allemandes, utilisatrices de la machine à chiffrer, aux cryptanalystes de Bletchley Park, où avait été établi le centre de décryptement allié. A l'aide des travaux des Polonais, les Anglais réussirent au terme de longues recherches, et parfois seulement grâce à la capture d'une Enigma et de ses documents secrets lors de raids contre la Kriegsmarine, à briser le chiffre de l'Enigma allemande. Ultra, cette nouvelle source d'informations, procura un avantage net aux Alliés sur les théâtres du conflit.

Que Bletchley Park ait ou non joué une un rôle décisif dans la victoire des Alliés reste prétexte à controverses. Ce qui est certain, c'est que les briseurs de code de Bletchley ont sensiblement écourté la guerre. C'est particulièrement évident lorsqu'on reconstitue la bataille de l'Atlantique et qu'on se présente comment les choses se seraient passées sans l'aide d'Ultra. Pour commencer, les Allemands auraient conservé une plus grande flotte de sous-marins et davantage de capacités d'intervention. Cela aurait compromis le lien vital avec l'Amérique, et les Alliés auraient dû consacrer des moyens considérables à la reconstruction de nouveaux bateaux. Le débarquement aurait été repoussé au moins à l'année suivante. L'historien David Kahn résume ainsi le rôle du succès sur Enigma :

> "*Cela sauva des vies, pas seulement des vies russes et alliées, mais aussi des vies allemandes, italiennes, japonaises.* [...] *Voilà la dette que le monde a envers les briseurs de codes : c'est la récompense en valeur humaine de leur triomphe.*"

Pour autant, même si les briseurs de codes de Bletchley Park avaient été entièrement inefficaces, même si la guerre avait été prolongée trois mois ou plus à cause de leur incapacité, un autre élément aurait influencé le destin des événements : la bombe atomique. Si l'Allemagne avait pu continuer à se battre à l'été 1945, la première bombe atomique n'aurait probablement pas explosé sur Hiroshima mais sur Berlin, et la guerre se serait terminée quoiqu'aient pu faire les cryptanalystes de Bletchley Park.

D'autres chiffres ayant eu une influence moindre ont également été employés pendant le second conflit mondial. C'est le cas du code japonais Purple qui est un chiffre électromécanique inspiré d'Enigma, ou du code Navajo utilisé par les Etats-Unis lors de la reconquête des îles du Pacifique.

Après la guerre, les prouesses de Bletchley Park restèrent un secret bien gardé. Alors que ceux qui étaient allés au front pouvaient parler de leurs luttes héroïques, ceux qui avaient mené des batailles intellectuelles d'une portée aussi importante si pas supérieure, étaient dans l'obligation d'éviter les questions ou de mentir dans leurs réponses. Un des jeunes cryptanalystes de la hutte 6 de Bletchley reçut par exemple une lettre insultante de son professeur, qui l'accusait d'avoir évité de se battre et d'être une honte pour son école.

Marian Rejewski, réfugié en France puis en Angleterre après l'invasion de la pologne, fut tenu à l'écart des travaux de Bletchley Park durant la guerre, à cause du grand secret qui entourait le lieu. Il avait poursuivi son travail de décryptement en aidant les services de renseignements français ; et son expérience aurait été un atout inestimable pour les Anglais. Mais il n'apprit l'importance de ses travaux que bien plus tard.

Alan Turing quant à lui, ne vécut pas assez longtemps pour recevoir une reconnaissance publique et, au lieu d'être acclamé comme un héros par son pays, fut persécuté pour son homosexualité. C'est pour cela qu'à quarante-deux ans, l'un des plus grands cerveaux de la cryptanalyse, père de l'ordinateur, mit fin à ses jours.

Après trente années de silence, le voile fut finalement levé sur Bletchley Park au début des années 70. Ceux qui avaient tellement contribué à l'effort de guerre pouvaient maintenant recevoir la reconnaissance qu'ils méritaient.

Annexes

A. Lexique cryptologique

Bletchley Park : Lieu près de Londres où a été établi le centre de décryptement d'Enigma et des autres codes employés pendant la Seconde Guerre Mondiale réunissant des mathématiciens, linguistes, cruciverbistes dans un manoir victorien reconverti ; connu également sous le nom de GC&CS.

Bombe : Machine électromécanique utilisée par les cryptanalystes pour déterminer la clef d'Enigma ayant servi à crypter un message allemand. Les premières bombes ont été inventé par les Polonais et Alan Turing en a également mises au point point par la suite.

Bureau 40 : Le bureau 40 (*room forty*) fut fondé en 1914 lors du déclenchement de la Première guerre mondiale par les services secrets de Sa Majesté, et ce afin de collecter puis décrypter les cryptogrammes allemands. Le bureau 40 resta en place pendant l'entre-deux-guerre et fut déménagé à Bletchley Park au début de la Seconde guerre mondiale.

Chiffre : N'importe quel système appliqué pour dissimuler le sens d'un message en remplaçant chaque lettre du message d'origine par une autre.

Chiffre de substitution : Cryptosystème dans lequel chaque lettre du message est remplaçé par un autre caractère mais conserve sa place dans le message.

Chiffre de transposition : Cryptosystème dans lequel chaque lettre du message reste inchangée, mais mise à une autre place.

Chiffrer : Transformer le message d'origine en message chiffré.

Clef : Paramètres qui spécifient l'état la machine Enigma lorsque l'on chiffre un message. Une clef comprend notamment les fiches branchées, l'agencement des rotors utilisés et leur orientation initiale.

Clef privée : La cryptographie à clef privée base la confidentialité des messages sur celle de la clef utilisée pour coder les messages. Celle-ci doit être partagée entre l'émetteur et le destinataire du message, ce qui pose le problème de la communication de la clef. Ce principe s'oppose à celui de la clef publique, plus récent.

Un système qui suit ce principe est le chiffrement *RSA*, avec lequel la clef utilisée pour crypter les message est différent de celle avec laquelle on les décrypte. Dans un système à clef publique, on peut donc divulguer la clef de cryptage de manière publique sans qu'on puisse craindre qu'on s'en serve pour déchiffrer les messages que l'on nous envoie.

Code : Système pour dissimuler le sens d'un message en remplaçant chaque mot ou phrase du message par un caractère ou un ensemble de caractères. Par abus de langage, un code peut également désigner n'importe quelle forme de cryptage.

Coder : Remplacer les mots d'un texte par les symboles correspondant dans le code en question.

Cryptanalyse : Sciences des techniques qui permettent de retrouver le sens d'un texte crypté sans en connaître la clef.

Cryptologie : Science de l'écriture secrète sous toutes ses formes, englobant à la fois la cryptographie et la cryptanalyse.

Déchiffrer : Transformer un message chiffré en un message clair conforme à l'original. Ce terme s'applique en principe au destinataire qui connaît la clef nécessaire pour obtenir le texte clair, mais on l'utilise aussi dans le cas d'un intercepteur ennemi qui opère le déchiffrement par la cryptanalyse.

Décoder : Transformer un message codé en message clair conforme à l'original.

Décrypter : Déchiffrer ou décoder.

Force brute : Le décryptage par la force brute est une méthode de cryptanalyse qui consiste à essayer toutes les combinaisons de clef possible. Il s'agit de la méthode la plus évidente, mais les systèmes sont bien sûr conçus pour disposer d'un nombre de clefs trop grand pour un tel décryptement systématique.

General Code & Cipher School (GC&CS) : Centre de déchiffrement basé à Bletchley Park.

Stéganographie : Technique pour cacher l'existence d'un message, par opposition à la cryptographie qui en dissimule le sens.

Symétrique : Un cryptage symétrique se sert de la même clef pour le cryptage et pour le décryptage. L'emploi du terme *symétrique* relève en fait dans ce dossier d'un abus de langage, puisqu'il est employé pour qualifier le caractère de chiffrement d'Enigma qui fait que le procédé de cryptage est similaire à celui du décryptage.

Texte chiffré : Message obtenu après le chiffrement.

Texte clair : Message original avant le chiffrement.

Ultra : Nom donné à la source des informations issues du décryptage d'Enigma, mais peu de gens en savaient l'origine.

B. Lexique mathématique

Arrangement : A_n^p est le nombre d'*arrangements* de p éléments parmi n. Il s'agit de choisir une liste de p objets tous différents dans un ensemble en contenant n. Un arrangement est un choix ordonné, c'est-à-dire que deux choix des mêmes objets mais dans un ordre différent compte pour deux choix différents. Ce choix peut être réalisé de manière simple : on choisit le premier objet parmi les n de l'ensemble, n possibilités se présentent à nous. Ensuite, on choisit le deuxième objet, $n-1$ possibilités se présentent à nous parmi les objets restants. Et ainsi de suite jusqu'au $p^{\text{ème}}$ objet, pour lequel nous avons $n-p+1$ possibilités. Le nombre de possibilités pour ces choix successifs équivaut donc à :

$$\mathsf{A}_n^p = n \times (n-1) \times \ldots \times (n-p+1) = \frac{n!}{(n-p)!}$$

Combinaison : C_n^p est le nombre de *combinaisons* de p éléments parmi n. Comme pour l'arrangement, nous allons choisir p objet, mais sans que l'ordre dans lequel le choisi a été fait ne compte pas, c'est-à-dire que deux choix des mêmes objets mais dans un ordre différent compte pour un seul et même choix. En ce sens, puisqu'il existe $p!$ manières d'ordonner une liste de p objets, il y a $p!$ fois moins de combinaisons que d'arrangements de p parmi n. Les mathématiciens disposent donc de la formule :

$$\mathsf{C}_n^p = \frac{n!}{p! \times (n-p)!}$$

D'après la nouvelle notation du programme de terminale, C_n^p se note $\begin{pmatrix} n \\ p \end{pmatrix}$.

Composition : La *composition* est une opération qui prend deux fonctions et en donne une autre consistant à l'application successive de ces deux fonctions. Elle se note à l'aide de l'opérateur "rond" $\circ$. $f \circ g$ est une fonction définie telle que pout tout k

d'un ensemble donné, $f \circ g(k) = f(g(k))$, pourvu que f et g soient deux fonctions et que la fonction f travaille sur les objets que donne g.

Dénombrement : Le dénombrement s'intéresse à établir le compte des éléments d'un ensemble donné, ou des possibilités qui s'offrent à nous lors d'un choix donné. Dans des situations qui peuvent être complexes, les mathématiciens disposent de formules générales. Voir arrangement et combinaison.

Element : Un *élement* d'un ensemble est un objet appartenant à cet ensemble. Si l'élément k appartient à l'ensemble E, on note $k \in E$. Voir ensemble.

Ensemble : Un ensemble mathématique est une collection d'objets. On peut représenter un ensemble fini en énumérant la liste de ses *éléments* entre accolades. Par exemple, l'ensemble des nombres entiers naturels pairs inférieurs à 7 peut s'écrire $\{0, 2, 4, 6\}$. Des ensembles célèbres sont $\mathbb{N}$, l'ensemble des nombres entiers naturels, $\mathbb{Z}$ qui contient les nombres de $\mathbb{N}$ et leurs opposés, et $\mathbb{R}$, qui contient tous les nombres réels.

Factorielle : $n!$ est un nombre nommé *factorielle* n, n étant un nombre entier. Une manière simple de le décrire est de dire qu'il s'agit du produit des nombres entiers non-nuls inférieurs ou égaux à n, avec la convention que $0!$ vaut 1. Ainsi $3! = 1 \times 2 \times 3 = 6$. On peut le définir formellement par récurrence :

$$n! = \begin{cases} 1 & \text{pour } n = 0 \\ n \times (n-1)! & \text{pour } n \geq 1 \end{cases}$$

Involution : Une *involution* est une fonction mathématique qui est égale à sa réciproque, si bien qu'en l'appliquant deux fois à un objet, on retrouve l'objet initial. Voir réciproque.

Notation scientifique des nombres : Lorsqu'un chiffre est très grand, il peut être utile pour des raisons pratiques de n'en représenter qu'une valeur approchée, en donnant ses premiers chiffres et son ordre de grandeur. Ceci peut être accompli grâce à la notation $a \times 10^b$ avec $1 \leq a < 10$ et $b \in \mathbb{Z}$. Si l'on veut écrire *quatre millions cinq-cent mille*, on le pourra avec $4,5 \times 10^6$, puisque 10^6 vaut dix multiplié six fois par lui-même, c'est à dire un million.

Permutation : Une permutation est une fonction mathématique particulière. Pour qu'une fonction soit une permutation, il faut qu'elle opère d'un ensemble quelconque dans le même ensemble, et qu'elle soit *bijective*, c'est-à-dire que les images respectives de deux objets différents par une permutation ne peuvent pas être

identiques. Il existe une notation particulière pour les permutations, où les correspondances entre éléments sont représentées en colonnes. Par exemple, si l'on considère la permutation f qui associe b à a, c à b et a à c, on note :

$$f = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

Point fixe : Le ou les *point(s) fixe(s)* d'une fonction sont les valeurs qui ne sont pas modifiées par l'application de celle-ci. Si $f(a) = a$ alors a est un point fixe de la fonction f.

Produit Π : La notation du produit par l'opérateur $\prod$ se fait pour simplifier l'écriture de produits ayant beaucoup d'opérandes. $\prod_{i=n}^{m} f(i)$ équivaut au produit des opérandes $f(i)$ pour chacun des nombres entiers i allant de n à m. Par exemple :

$$\prod_{i=1}^{3} 2 \times i = (2 \times 1) \times (2 \times 2) \times (2 \times 3) = 48$$

Réciproque : La *réciproque* f^{-1} d'une fonction f est une fonction telle que si $f(a) = b$, alors $f^{-1}(b) = a$.

Somme Σ : Tout comme pour le produit, il existe une manière simple d'écrire des somme à nombreux termes avec l'opérateur $\sum$. $\sum_{i=n}^{m} f(i)$ est la somme des termes $f(i)$ pour chacun des nombres entiers i allant de n à m.

Théorie des permutations : Cette théorie se propose de modéliser des phénomènes où des objets, symboles ou autres, sont échangés entre eux. C'est pour cela que les Polonais s'en servirent pour décrypter les messages cryptés à l'aide d'Enigma avant la guerre.

La théorie des permutations est sous-jacente à la *théorie des groupes*, qui propose des résultats de base pour n'importe quelle opération mathématique associée à un ensemble sur lequelle elle fonctionne, pourvu que cette opération vérifie certaines propriétés. L'opération qui nous intéresse ici est la *composition*, qui opère sur l'ensemble des permutations possible d'un ensemble donné. En effet, pour toutes permutations f, g et h de cet ensemble, la composition vérifie les propriétés nécéssaire pour rentrer dans le cadre de la théorie des groupes :

- Associativité : $f \circ (g \circ h) = (f \circ g) \circ h$
- Element neutre : $f \circ Id = Id \circ f = f$
- Inverse : $f \circ f^{-1} = f^{-1} \circ f = Id$

L'élement neutre Id est l'identité de l'ensemble, ou la fonction qui laisse tous les éléments de l'ensemble inchangés. Nous avons choisi dans ce dossier de ne pas employer la notation multiplicative conventionnelle mais de conserver l'emploi de l'opérateur $\circ$. Voir permutation, composition, réciproque, involution, point fixe.

Bibliographie

Livres

HARRIS, R. (1996). *Enigma*, Plon.

HINSLEY, F.H. & A. STRIPP (1993). *Codebreakers : the inside story of Bletchley Park*, Oxford University Press.

KAHN, D. (1996). *Seizing the Enigma : The race to break the german U-boats Codes 1939-1943*, Arrow Books.

KEMP, A. (1994). *6 juin 1944 le débarquement en Normandie*, Découvertes Gallimard.

SEBAG-MONTEFIORE, H. (2000). *Enigma the battle for the code*, Phoenix.

SINGH, S. (1999). *Histoire des codes secrets : de l'Egypte des Pharaons à l'ordinateur quantique*, JC Lattès.

"Pologne" dans *Encyclopédie Universalis* no. 9.

Journaux et périodiques

Cryptologia, *G-312 : An Abwehr Enigma, Vol. XXIV*, janvier 2000.[1]

Les Cahiers de Science & Vie, L'origine des nombres, n°57, juin 2000.

Le Monde, Les mystères d'Enigma, 26 juin 2000.

Science & Vie Junior, La seconde guerre mondiale, Hors-Série n°38, octobre 1999.

Science & Vie Junior, Les codes secrets, Hors-Série n°53, juillet 2003.

[1]Ce document se trouve sur internet, à l'adresse http://www.eclipse.net/~dhamer/pubs.htm.

Sites Internet

La date de première visite est indiquée entre parenthèses.

A propos de l'invention et de l'utilisation d'Enigma par les Allemands

http://www.securiteinfo.com/attaques/divers/steganographie.shtml (29/06/04)
http://www.memorial.fr/archives/collec_obj_hist_5.asp (12/10/03)
http://en.wikipedia.org/wiki/Rotor_machine (29/06/04)
http://www.smithsrisca.demon.co.uk/crypto-modern.html (29/06/04)
http://www.deutsches-museum.de/ausstell/meister/e_enigma.htm (29/06/04)
http://www.achtungpanzer.com/blitz.htm (12/10/03)
http://f.home.cern.ch/f/frode/www/crypto/tbombe.html (29/06/04)

A propos du fonctionnement d'Enigma

http://www.mlb.co.jp/linux/science/genigma/enigma-referat/enigma-referat.html (23/11/03)
http://www.enigma-replica.com/ (23/11/03)
http://w1tp.com/mcpu.htm (09/02/04)
http://www.swimmer.org/morton/enigma.html (09/02/04)
http://www.pbs.org/wgbh/nova/decoding/enigma.html (09/10/04)
http://www.vectorsite.net/ttcode5.html (29/06/04)

A propos du décryptement allié et ses conséquences

http://www.nsa.gov/publications/publi00016.cfm (02/07/04)
http://en.wikipedia.org/wiki/Marian_Rejewski (02/07/04)
http://www.cl.cam.ac.uk/Research/Security/Historical/hinsley.html (19/01/04)
http://pan.net/history/enigma/index.htm (12/10/03)
http://home.earthlink.net/~nbrass1/enigma.htm (16/11/03)
http://uboat.net/technical/enigma_breaking.htm (23/12/03)
http://www.bletchleypark.org.uk/ (13/01/04)
http://www.iwm.org.uk/online/enigma/eni-intro.htm (19/01/04)

A propos des méthodes utilisées pour décrypter Enigma

http://members.fortunecity.com/jpeschel/gillog1.htm (03/01/04)
http://www.armyradio.com/publish/Articles/The_Enigma_Code_Breach/ (28/12/03)
http://webhome.idirect.com/~jproc/crypto/bombe_us.html (23/11/03)
http://www.enseignement.polytechnique.fr/profs/informatique/Jean-Jacques.Levy/00/pi/poupard/enigma.html (06/10/03)

A propos de programmes simulant Enigma

http://home.t-online.de/home/grey-wolf/urudel.htm (12/10/03)
http://www.xat.nl/enigma/ (23/12/03)
http://homepages.tesco.net/~andycarlson/enigma/about_enigma.html (29/01/04)

Informations sur ce dossier

Ce dossier fait partie d'un projet plus vaste, comportant également un simulateur de la machine Enigma, que l'on peut trouver à cette date en intégralité sur le site internet http://diabo.free.fr/enigma/. Ce site Internet a été réalisé par Julien Milli et Guillaume Munch, initialement dans le cadre de leur TPE. Nous étions tous deux élèves du Lycée Louis Armand de Mulhouse, en Alsace, France, en classe de terminale S_2 durant l'année scolaire 2003-2004.

Les TPE, Travaux Personnels Encadrés, en classe de terminale, sont une épreuve du Baccalauréat consistant en une recherche documentaire et en la réalisation d'un projet en groupe restreint d'élèves, s'étalant sur plusieurs mois. Il s'agit de traiter d'un sujet faisant intervenir plusieurs disciplines, et de présenter oralement son projet devant un jury composé de professeurs enseignant ces disciplines. Le projet dont ce dossier fait partie s'est vu attribuer la note de vingt sur vingt par le jury des TPE au Baccalauréat.

Version du dossier

Nous avons décidé d'améliorer et d'apporter des précisions à ce dossier. Nous avons en partie réécrit et complété celui qui a été présenté à l'épreuve du Bac. Cette version a été mise en ligne le 29 août 2004.

Contact

Vous pouvez nous faire part de vos questions sur le déroulement des TPE, remarques et impressions éventuelles sur notre réalisation en nous contactant par e-mail à l'adresse suivante :

tpeenigma@free.fr

Remerciements

Nous tenons à remercier l'ensemble des professeurs qui nous ont aidés à réaliser notre TPE initial, en particulier M^{me} Oudenot, professeur d'Histoire-Géographie, et M. Chrétien, professeur de Mathématiques, pour avoir bien voulu répondre à nos questions.

Dans un tout autre domaine, nous remercions les auteurs des logiciels *libres* dont nous nous sommes servis, pour la qualité de leurs créations : *PHP*, *Gimp*, *Sketch*, *Lyx*. Ces logiciels nous ont permis respectivement de programmer notre simulateur d'Enigma, de traiter les images, de réaliser les schémas présents dans ce dossier et enfin d'écrire notre dossier sous cette forme.

Nous vous remercions également, pour l'intérêt que vous portez à notre dossier en le lisant jusqu'au bout et vous invitons à visiter notre site Internet si vous ne l'avez déjà fait :

`http://diabo.free.fr/enigma/`

Informations sur notre T.P.E.

Série : Scientifique.

Période de réalisation : Le TPE initial a été réalisé entre septembre 2003 et mars 2004. Il a ensuite été modifié et complété de juin à août 2004.

Thème abordé : *Hériter et innover*.

Sujet du TPE : La machine à crypter Enigma.

Disciplines impliquées : Histoire et Mathématiques.

Problématique : *Comment Enigma a-t-elle influencé la Seconde guerre mondiale ?*

Projet de réalisation finale : Un site Internet proposant un dossier répondant à la problématique et un programme informatique simulant le cryptage d'Enigma.