Travail de maturité

Simulation et décryptage d'une machine Enigma

par Carl Johansson (carljohanpeter@me.com)

Route du Lac 7, 1026 Denges

Gymnase de Chamblandes, 3M2

sous la direction de M. Dessauges, Luc.

Année scolaire : 2017 - 2018

Remis le 6 novembre 2017.

Table des matières

Chapitre 1

Introduction

Le 23 mai 1945, l'Allemagne nazie capitula et mit fin à la deuxième guerre mondiale en Europe. La guerre fut combattue sur plusieurs fronts ; à la surface et sous la mer, sur la terre et dans les airs. Il y avait cependant encore un champ de bataille, qui restait longtemps inconnu ; celui des codes. Les Allemands étaient munis de la machine de cryptage la plus complexe jusqu'alors. Quelques décennies plus tard, il fut dévoilé que les Britanniques avaient décrypté des messages allemands dont ils se sont servis pour gagner la guerre. Cette histoire évoque plusieurs questions ! Comment fonctionne la machine Enigma ? Les Britanniques, étaient-ils vraiment les seuls à participer dans cette bataille du code ? Comment la machine Enigma a-t-elle été décryptée ?

Le premier but de ce travail de maturité est d'expliquer le fonctionnement d'une machine Enigma. Ceci sera accompagné d'une simulation, programmée en Python, qui met en évidence le fonctionnement de la machine. Le deuxième objectif sera d'explorer les différentes méthodes de décryptage et de simuler la stratégie de décryptage. En parallèle avec cet objectif, le contexte historique et les difficultés du décryptage seront mis en évidence.

Pour mon travail de maturité, je souhaitais traiter un sujet en lien avec la cryptographie, parce que je me suis toujours intéressé à ce sujet. Après avoir regardé le film "Imitation Game" [1], j'ai eu l'idée de travailler sur la machine Enigma en particulier.

1. TYLDUM Morten, *The Imitation Game*, 2014

Chapitre 2

Description d'Enigma

2.1 Fonctionnement d'Enigma

De part son aspect extérieur, une machine Enigma ressemble fortement à une machine à écrire surdimensionée. Elle comporte un clavier de 26 lettres, mais aussi 26 ampoules qui symbolisent chacune une lettre. Sur ces ampoules il y a une sorte de capot, qui crée donc un tableau d'affichage. Sous ce même capot, il y a un engin mécanique, que nous appellerons *le système de rotors*. Il y avait aussi des trous dans le capot qui permettent de voir la position de chaque rotor. Sur le devant de la machine se trouve le *tableau de connexion* dont nous aborderons le fonctionnement plus tard. Pour commencer, Enigma est constituée de deux parties, une partie mécanique et une partie électrique qui interagissent pour crypter le message.
Le fonctionnement de la partie électrique est très basique. Dès qu'une touche est appuyée sur le clavier, un circuit est fermé, une connexion électrique est établie et par conséquent une ampoule commence à briller. Si on a, par exemple, appuyé la touche C et que l'ampoule de la lettre Q s'allume sur le tableau d'affichage, cela veut dire que la lettre C a été cryptée en Q.

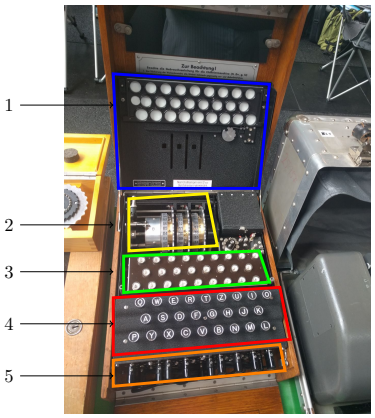

Photo prise à Friedrichshafen par Joël Wagnières.

Légende :
1. Capot
2. Système de rotors
3. Ampoules
4. Clavier
5. Tableau de connexion

FIGURE 2.1 – Légende d'une machine Enigma ouverte

Pour comprendre le fonctionnement de la partie mécanique qui est nettement plus sophistiquée, il faut premièrement se familiariser avec deux éléments de la machine : le rotor et le réflecteur.

Le rotor est, à première vue, un cylindre qui a un trou au milieu. Sur chaque face circulaire du rotor, il y a 26 contacts électriques et chaque contact est relié par un câble à un contact du côté opposé. En tout, il y a donc 26 câbles pour un rotor, qui forment ce que nous appellerons le *câblage* du

rotor. Dans les schémas qui suivent, nous allons supposer qu'un rotor a seulement six contacts de chaque côté.

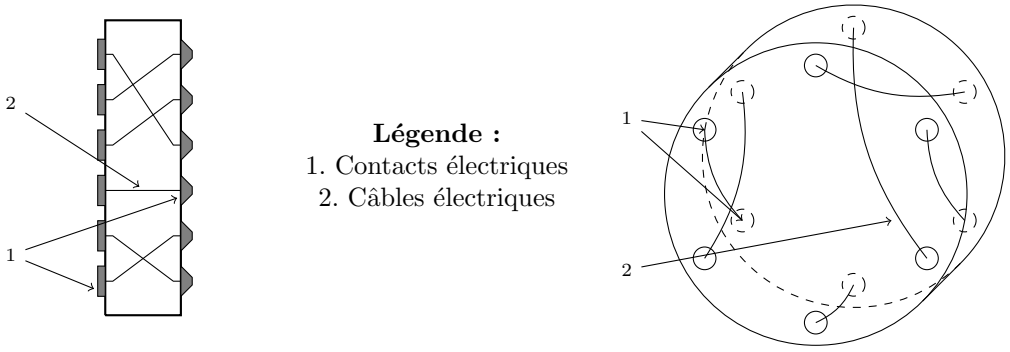

FIGURE 2.2 – Un rotor de côté et de face

Le réflecteur peut être décrit comme un demi-rotor. Tout comme le rotor, le réflecteur est un cylindre, mais contrairement au rotor, le réflecteur a 26 contacts électriques d'un côté, seulement. Il y a donc 13 câbles qui relient chacun des contacts à un autre.

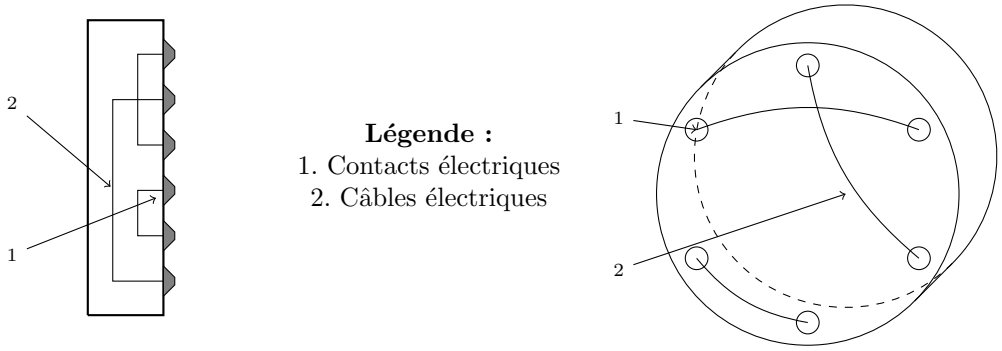

FIGURE 2.3 – Un réflecteur de côté et de face

Nous pouvons maintenant expliquer le fonctionnement principal de la machine en utilisant trois rotors et un réflecteur. Pour simplifier les schémas, nous dirons que la machine que nous construisons peut seulement écrire six lettres ; A, B, C, D, E et F. Sur les schémas qui suivent, les six interrupteurs visibles sont les six touches du clavier. De plus, nous dirons que les interrupteurs sont placés dans un ordre alphabétique, c'est-à-dire que l'interrupteur qui se trouve tout en haut est la touche A sur le clavier. Les six ampoules indiquent, comme nous l'avons déjà dit, la lettre cryptée qu'on obtient de la machine. Nous dirons que les ampoules sont, comme les interrupteurs, placés dans un ordre alphabétique. Le schéma suivant montre un exemple de machine où aucune touche n'est appuyée. Elle montre aussi que le courant parcourt premièrement les trois rotors pour ensuite passer dans le réflecteur qui lui permet de faire un aller-retour et de repasser une deuxième fois dans les trois rotors dans le sens inverse.

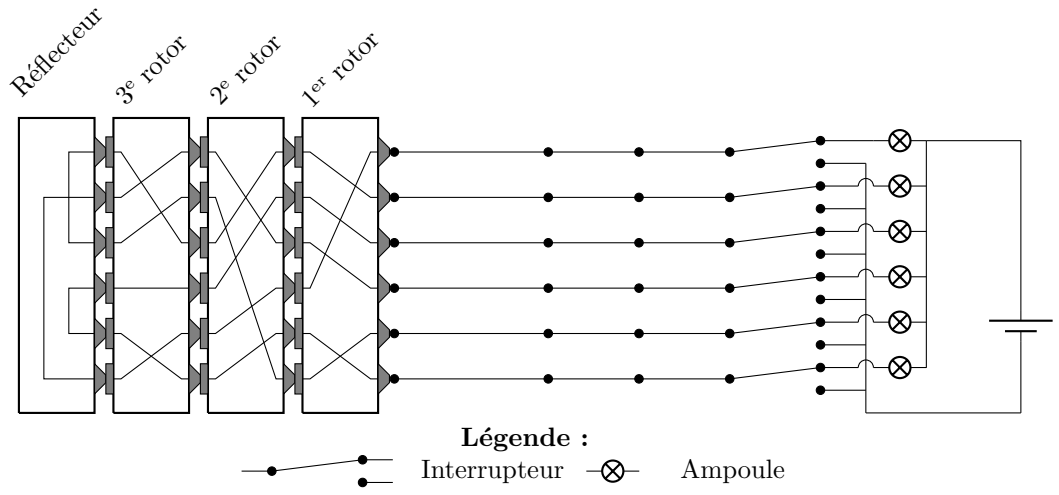

FIGURE 2.4 – Schéma d'une machine Enigma

La faille de cette construction est que chaque lettre est toujours cryptée en la même lettre et qu'il s'agit alors d'une simple substitution. Pour éviter ceci et compliquer le cryptage, les rotors sont mobiles et se déplacent à chaque fois qu'une touche est appuyée sur le clavier. Plus précisément, dès qu'une touche est appuyée, le premier rotor se déplace d'une position. Après avoir appuyé sur 26 touches, le premier rotor se retrouve donc à la même position. Pour faire varier encore plus le cryptage, le deuxième rotor se déplace d'une position pendant que le premier fait un tour entier et le troisième rotor se déplace d'une position pendant que le deuxième rotor fait un tour entier. Il faut donc appuyer sur $26^3 = 17576$ touches avant de se retrouver avec le même cryptage [1]. Pour permettre ce déplacement de rotors, il faut que chaque rotor entraîne le rotor suivant une fois pendant qu'il se déplace d'un tour. Nous dirons qu'un rotor a atteint sa position d'engagement si le déplacement suivant de ce rotor entraînera le déplacement du rotor à sa gauche. La figure 2.5 montre sous forme d'un graphe le fonctionnement du système de rotors. Une conséquence évidente de ce fonctionnement est que les rotors se déplacent à des vitesses différentes. Le premier rotor est le plus rapide en se déplaçant à chaque fois qu'une touche est appuyée. Le deuxième rotor est plus lent en se déplaçant dans $\frac{1}{26}$ des cas. Pour finir, le troisième et dernier rotor est le plus lent en se déplaçant dans $\frac{1}{26^2} = \frac{1}{676}$ des cas. Le réflecteur ne se déplace pas du tout.

1. Il peut bien-sûr arriver qu'on se retrouve avec le même cryptage avant d'avoir appuyée sur 17576 touches, mais pas de manière systématique.

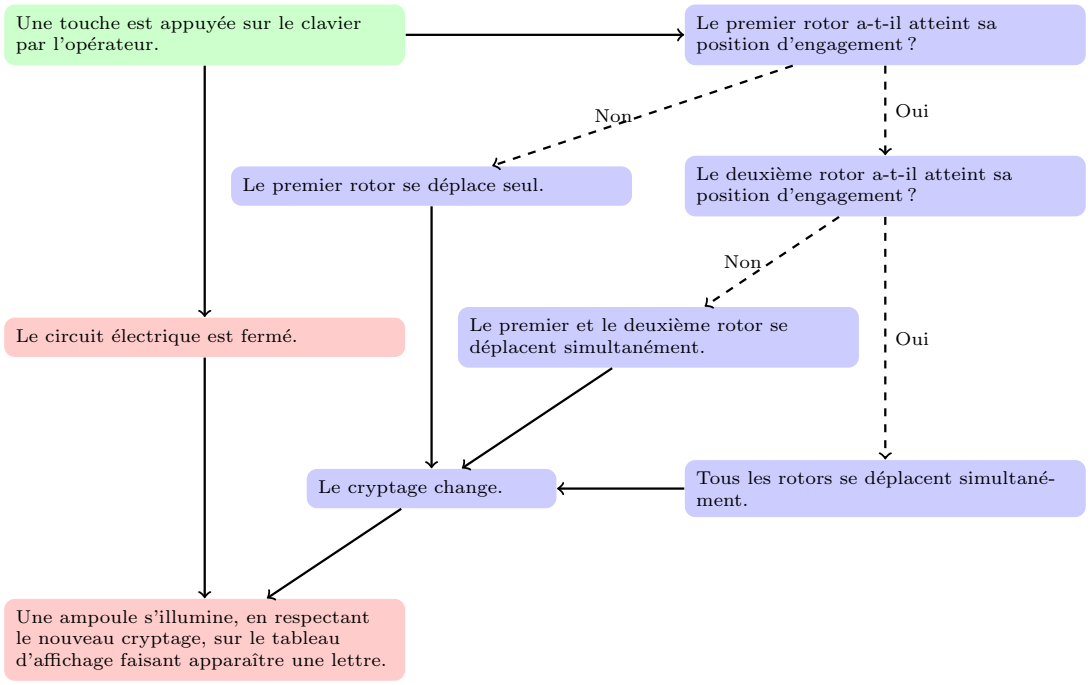

FIGURE 2.5 – Déplacement des rotors

Sur la figure qui suit, la touche de la lettre A est toujours celle qui est appuyée. Nous pouvons voir que quand la touche A est appuyé une deuxième fois, seulement le premier rotor se déplace et la troisième fois, le premier et le deuxième se déplacent simultanément.

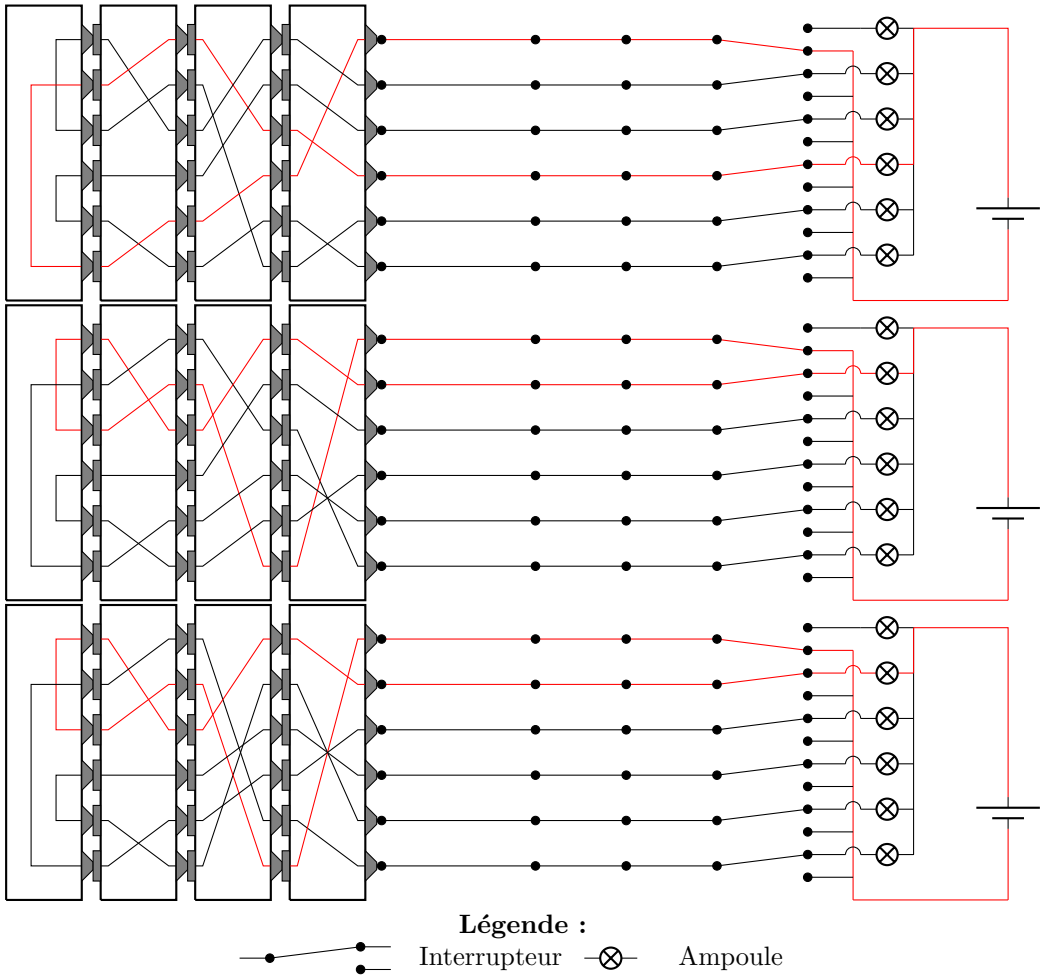

FIGURE 2.6 – Déplacement de rotors

Cette construction implique aussi qu'aucune lettre ne peut être cryptée en elle-même. Pour s'en convaincre, il suffit d'observer que la lampe correspondante à la lettre ne peut s'allumer à cause de la position de l'interrupteur.

Nous pouvons aussi remarque que la machine Enigma est son propre inverse. Si nous appuyions sur la touche A et que l'ampoule D commence à briller, alors si appuyions sur D, l'ampoule A qui commence à briller.

Sur notre machine simplifiée, il faut appuyer $6^3 = 216$ touches avant de revenir au cryptage du début. De même façon, sur la machine Enigma, il faut taper $26^3 = 17576$ touches avant de revenir au cryptage initial.

Nous comprenons maintenant le fonctionnement fondamental des rotors et il est donc temps d'aborder quelques aspects plus précis, tel que le tableau de connexion et le tambour d'entrée.

Le tableau de connexion permet de modifier les connexions entre les touches et le système de rotors et il est constitué, de 26 prises électriques qui peuvent, selon les paramètres de cryptage, être reliés entre eux par des câbles électriques.

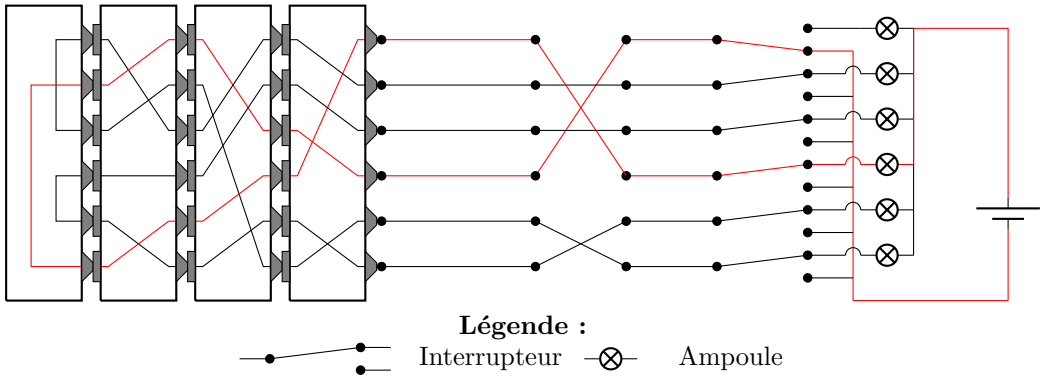

FIGURE 2.7 – Apparition du tableau de connexion

Le tambour d'entrée relie le système de rotors et le tableau de connexion entre eux en compliquant encore une fois les connexions. Sur la machine Enigma commerciale, ce tambour reliait dans l'ordre des lettres du clavier (Q, W, E, R, T, Z et ainsi de suite) à l'alphabet. C'est-à-dire qu'entre le tableau de connexion et le système de rotors, le câble symbolisant la lettre Q sortant du tableau de connexion est lié au câble symbolisant la lettre A dans le système de rotors. Ces connections continuent en liant W à B, E à C, R à D, T à E, Z à F et ainsi de suite.

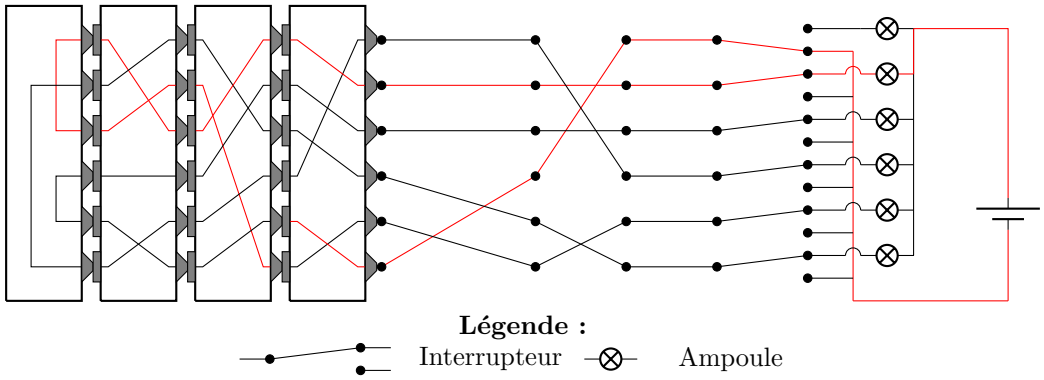

FIGURE 2.8 – Apparition du tambour d'entrée

Quand on regarde la figure précédente, on peut se demander quelle est la différence entre le tambour d'entrée et le tableau de connexions. Une première différence est que les connexions faites sur le tableau peuvent être facilement changées, tandis que le tambour d'entrée est fixe et ne peut pas être changé. Une autre différence est que le tableau de connexion a un caractère symétrique ; si A est relié à U, alors U est relié à A et inversement. Comme, nous pouvons le voir sur la figure 2.8, ceci n'est pas valable pour le tambour d'entrée.

2.2 Le Rotor

Nous allons maintenant explorer plus précisément le composant le plus important dans la machine. Comme nous l'avons déjà dit, il comporte 26 contacts électriques de chaque côté, reliés avec 26 câbles électriques. En plus de cela, il y a une bande blanche qui entoure le rotor. Sur cette bande, des nombres ou des lettres imprimées, qui permettent de définir la position du rotor dans la machine. La position du rotor dans la machine est simplement la lettre ou le nombre qui est visible à travers le trou dans le capot. Les données dans les tables de cette section peuvent être trouvées sur le site de Crypto Museum [2].

On peut donc penser que si on prend deux rotors, qui ont le même câblage et qui en plus se trouvent à la même position, agissent de la même manière. En réalité ce n'est pas le cas et ceci est dû à encore une complexité qui a été ajoutée dans le rotor. La bande blanche de positions, mentionnée auparavant, est mobile et peut être tournée autour du câblage du rotor. Avant d'utiliser le rotor, il faut néanmoins fixer la bande de positions à une des 26 positions possibles (correspondant au contacts sur la face des rotors). On appelle la position à laquelle la bande de positions est fixée le *ringstellung* Ce dernier permet donc de décaler le câblage par rapport à la bande de positions. Un rotor sur lequel la bande de positions à été décalée de 5 positions avec le ringstellung agit donc comme un rotor, inchangé par le ringstellung, se trouvant 5 positions plus loin.

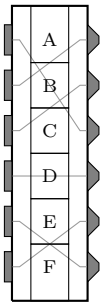

FIGURE 2.9 – Un rotor inchangé à la position A

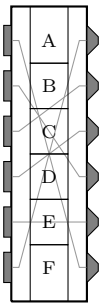

FIGURE 2.10 – Un rotor, décalé de 5 positions, à la position A

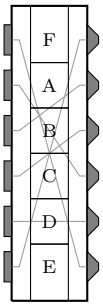

FIGURE 2.11 – Un rotor inchangé à la position F

En général, on décrit le ringstellung (c'est-à-dire le décalage de la bande de positions) par une lettre. On peut voir, en regardant le rotor, quel est son ringstellung. Si on a un rotor dont le ringstellung est B et que l'on souhaite qu'il ait le ringstellung E, alors il faut rendre mobile la bande de positions, la déplacer de 3 positons et la fixer.

Pour définir le câblage d'un rotor, on décrit à l'aide d'un tableau (table 2.1) la permutation effectuée par le rotor, depuis la droite jusqu'à la gauche. Pour définir la permutation du rotor, nous devons nommer les contacts électriques sur le rotor. Il est logique de les définir avec des lettres dans un ordre alphabétique. Il n'est pas vraiment important où l'on commence comme ceci donnera seulement un décalage. Sur la figure suivante nous avons choisi de nommer les contacts,

2. Crypto Museum. *"Enigma Wiring"*, http ://www.cryptomuseum.com/crypto/enigma/wiring.htm [consultée pour la dernière fois le 5 novembre 2017]. (Ce site donne des informations précises sur les rotors et les réflecteurs.)

selon la bande blanche qui entoure le rotor. La permutation R du rotor de la figure 2.12 donnera la permutation décrite par la table 2.1.

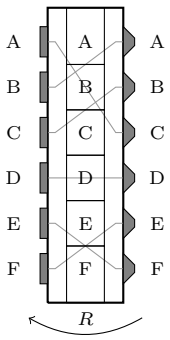

FIGURE 2.12 – Un rotor Enigma

A	B	C	D	E	F
B	C	A	D	F	E

TABLE 2.1 – Description de la permutation du rotor

Les tables suivantes montrent comment les trois premiers rotors de l'Enigma agissent dans le chiffrement d'un message. Il faut préciser qu'il s'agit de la permutation du rotor quand le courant va vers la gauche. Bien sûr, la permutation du rotor dépend du ringstellung et de la position du rotor, mais il s'agit seulement d'un décalage.

Rotor 1 :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J

Rotor 2 :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E

Rotor 3 :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O

TABLE 2.2 – Permutations faites par les trois rotors des premières versions de la machine Enigma

En ce qui concerne le mouvement des rotors, le tableau suivant montre, pour chacun des rotors, la position à laquelle chaque rotor entraine le suivant. Ici, il est important de noter que le mécanisme qui entraine le rotor suivant se trouve sur la bande de positions, c'est-à-dire qu'il dépend du ringstellung. Lorsqu'on utilise Enigma, cela veut dire que la position d'engagement d'un rotor dépend uniquement de la lettre que l'on voit à travers le trou du capot. C'est-à-dire que si la bande de positions est décalé de 17 positions par rapport au câblage, alors la position d'engagement est aussi décalé de 17 positions relativement au câblage du rotor.

Rotor	Position d'engagement
I	Q
II	E
III	V

TABLE 2.3 – Position d'engagement des rotors

Ceci veut dire que si un rotor de câblage II se déplace depuis la position E à F, alors le rotor à sa gauche se déplace simultanément avec lui.

2.3 Le tableau de connexions

Un autre composant, qui complique le cryptage, est le tableau de connexions. C'est une surface sur le devant de la machine avec 26 prises électriques, une pour chaque lettre de l'alphabet. L'opérateur peut connecter deux prises avec un câble électrique. S'il lie la prise de la lettre B à la prise de la lettre F, alors ceci veut dire que s'il appuie la lettre F, alors cela correspond à appuyer sur la touche B, sans le câble qui relie B et F. De la même façon, s'il appuie sur B, alors cela correspond à appuyer sur la touche F. Inversement, si la lettre B sort du système de rotors, alors l'ampoule de la lettre F brille. Au début de l'utilisation de l'Enigma, il y avait seulement six câbles qui reliaient des prises sur le tableau de connexion. Tout au long de la guerre, le nombre de câbles augmentait.

2.4 Utilisation de l'Enigma

Chaque opérateur allemand est muni du manuel des clés journalières qui indique l'ordre des rotors, le ringstellung pour chaque rotor, la position initiale de chaque rotor dans la machine et les connexions faites sur le tableau de connexion.

Dans le manuel, on pouvait par exemple lire [3] :

date	ordre	ringstellung	position	connexions
5 octobre	II - I - III	A - G - G	Z - L - T	XY IJ KL RT SV OP
6 octobre	II - I - III	U - A - J	Q - C - M	YZ AK LP WQ TS OJ

Quand un opérateur veut écrire un message, il met correctement le ringstellung de chaque rotor. Ensuite, il ouvre le capot de la machine et il place les rotors dans le bon ordre. Plus tard, il referme le capot et il tourne les rotors afin qu'ils atteignent les positions correctes. Finalement, il branche les câbles sur le tableau de connexion.
Il reste maintenant à l'opérateur de choisir une clé de trois lettres. Ensuite, il tape deux fois cette clé et il obtient un indicateur de six lettres qu'il écrit au début de son message. Puis, il place les rotors aux positions correspondant à sa clé et il peut maintenant commencer à écrire son message. Dès qu'il a son message crypté, un opérateur radio l'envoie en morse à un autre opérateur radio qui le donne à un opérateur Enigma. Comme la machine de ce dernier correspond aussi aux paramètres journaliers et comme l'Enigma est son propre inverse, il lui suffit d'écrire l'indicateur et il obtiendra la clé du message deux fois. Cela permet d'expliquer pourquoi la clé est écrite deux

3. Ce tableau est inspiré d'un tableau dans l'article GUILLOT Philippe. *"Des mathématiciens polonais au coeur du décryptement de la machine ENIGMA, 1932-1942"*, 34 pages.

fois. Ceci lui permet de vérifier qu'il possède la clé juste, car des erreurs arrivent. L'opérateur met ensuite les rotors aux positions correspondant à la clé qu'il vient d'obtenir. Maintenant, il ne reste plus qu'à écrire le message tel qu'il l'a reçu et le message déchiffré apparaitra sur les ampoules de la machine.

2.5 6'000 milliards d'années

Nous allons maintenant calculer le nombre de différentes configurations possibles sur une machine Enigma. Nous commençons par regarder de combien de façons différentes nous pouvons brancher les câbles sur le tableau de connexions. Pour le premier câble, le nombre de possibilités correspond au nombre de combinaisons de 2 éléments parmi 26, c'est-à-dire qu'il y a

$$C_2^{26} = \frac{26!}{2 \cdot (26-2)!}$$

possibilités. Pour le n-ième câble, il y en a

$$C_2^{26-2n+2} = \frac{(26-2n+2)!}{2 \cdot (26-2n)!}.$$

Comme le nombre de branchements différents est indépendant de l'ordre dans lequel on les choisit, il faut diviser par $n!$. Au final, il y a donc

$$\frac{1}{n!}(C_2^{26} \cdot C_2^{24} \cdot C_2^{22} \cdot ... \cdot C_2^{26-2n+2}) = \frac{1}{n!}(\frac{26!}{2 \cdot 24!} \cdot \frac{24!}{2 \cdot 22!} \cdot \frac{22!}{2 \cdot 20!} \cdot ... \cdot \frac{(26-2n+2)!}{2 \cdot (26-2n)!})$$

$$= \frac{1}{n!} \cdot \frac{26!}{2^n \cdot (26-2n)!} = \frac{26!}{2^n \cdot (26-2n)! \cdot n!}$$

possibilités. Ensuite, en ce qui concerne les rotors, il y a

$$\frac{m!}{(m-3)!}$$

façons différentes d'arranger trois rotors parmi les m rotors qui sont à disposition. Chaque rotor peut, en plus, se trouver à 26 positions différentes. De ce fait, il y a $26^3 = 17576$ possibilités pour l'ensemble des positions de trois rotors. En plus de ce grand nombre de possibilités, il y a pour chaque rotor 26 ringstellung différents. Pour tous les trois rotors de la machine, il y a donc autant de possibilités différentes d'arranger les *ringstellung* que de possibilités de positions de rotors différentes. On pourrait penser que le ringstellung n'a aucune influence, qu'il s'agit seulement d'un décalage et ce n'est pas complètement faux. Il est vrai que quand il s'agit du cryptage d'une lettre individuelle, il s'agit seulement d'un décalage. Il ne faut cependant pas oublier que la position d'engagement est fidèle au ringstellung. Si nous avons deux rotors dont un est décalé de 4 avec le ringstellung, alors ce dernier correspond au rotor inchangé à 4 positions plus loin, mais la position d'engagement n'est pas décalé relativement à la bande blanche de positions, ce qui les rends différents.

Au début de l'utilisation de l'Enigma, il y avait trois rotors et six câbles à disposition. Il y avait donc

$$\frac{26!}{2^6 \cdot (26-12)! \cdot 6!} \cdot 6 \cdot 17576^2 \approx 1.86 \cdot 10^{20}$$

configurations différentes. Si nous voulions décrypter un message en essayant toutes les configurations avec la machine Enigma. Imaginons que nous pouvions vérifier une de ces situations chaque seconde, il nous faudrait un peu moins de 6'000 milliards d'années avant de les avoir toutes vérifiées.

Chapitre 3

Les polonais font l'impossible

Après la première guerre mondiale, les Allemands ne cachaient pas leur intention de récupérer les terres cédées à la Pologne par le traité de Versailles. Les Polonais, de leur côté, savaient que le droit d'existence de leur nation allait être remis en question. Le service de renseignement polonais avait donc mis en place un centre d'écoute pour pouvoir intercepter les messages allemands. En 1926, le cryptage des messages commençait à changer et les méthodes de décryptage habituelles ne fonctionnaient plus. En 1929, les Polonais prirent connaissance de l'existence de la machine Enigma et ils choisirent donc d'en acheter une version commerciale, mais les messages allemands restaient indéchiffrables, car la machine militaire était différente de la machine commerciale. Pour décrypter les messages, il fallait donc reconstruire la machine et pour ce faire, le bureau de renseignements fit le choix de recruter des mathématiciens. Un cours de cryptologie fut mis en place à l'Université de Poznan, en Pologne, où les mathématiciens les plus brillants allaient être sélectionnés pour attaquer Enigma. Seulement trois étudiants réussirent à suivre le cours jusqu'au bout ; Jerzy Rózycki, Henrik Zygalski et surtout, Marian Rejewski. Ce dernier travailla à partir du premier septembre 1932 à plein temps au bureau de renseignement polonais.

Un officier du service de renseignement français, Gustave Bertrand, était persuadé que la nouvelle génération de chiffres, tel qu'Enigma, ne pourrait pas être résolue à l'aide de la pure cryptanalyse. Il proposa donc d'organiser un achat d'informations vendues par des Allemands. En 1931, Gustav Bertrand reçut une lettre d'une personne qui disait qu'elle avait accès à des informations sur Enigma. Dans cette lettre, il précisa que si ces informations l'intéressaient, il devait être contacté le premier octobre, à la Kaufhausgasse 2 à Bâle. Cette lettre intrigante était signée par Hans-Thilo Schmidt. REX était le pseudonyme de la personne qui s'occupait de cette affaire au service de renseignements français. Ce REX répondit, selon les ordres donnés, à la lettre de Schmidt en fixant un rendez-vous en novembre 1931 à Verviers en Belgique. Persuadé que Schmidt allait devenir espion, le service de renseignements français lui donna un pseudonyme : HE. Durant un prochain rendez-vous, HE échangea des photos du manuel d'utilisation d'Enigma (Gebrauchanweisung für die Chiffriermaschine Enigma) , qui décrivait comment il fallait utiliser correctement la machine, et du manuel de création de clés de la machine (Schlüsselanleitung für die Chiffriermaschine Enigma) contre 10'000 Marks.

Le manuel de création de clés précisait :

— L'ordre des rotors

— Le ringstellung de chaque rotor.

— La position du rotor en tenant compte du ringstellung.

— Les connexions faites sur le tableau de connexions.

Gustave Bertrand transmit donc ces documents au colonel Bassières, qui était l'un des cryptanalystes les plus connus en France, mais Bassières jugeait que ces documents ne présentaient que peu d'éléments intéressants. Il pensait donc que ces nouvelles informations ne permettraient pas de décrypter Enigma. Bertrand eut ensuite l'autorisation de transmettre ces informations aux Britanniques, mais eux jugeaient aussi que les informations n'étaient pas suffisantes pour permettre de progresser dans le décryptage d'Enigma. Plus tard, il transmit les mêmes documents aux Polonais qui disaient que ces documents permettraient avec beaucoup de temps et de travail de progresser dans le décryptage d'Enigma. Ces documents permirent aux Polonais de dire qu'il y avait un tableau de connexion, qui n'existait pas sur la machine commerciale. Les Polonais eurent accès aux configurations journalières pour les mois de septembre et octobre 1932. Le chef du bureau de cryptologie polonais, Ciezki, choisit de placer Marian Rejewski, seul, dans une chambre pour qu'il essaie de résoudre une de plus grandes énigmes du moment. Son incroyable travail sera décrit dans ce chapitre. Rejewski a lui-même décrit son travail dans l'article "An Application of the Theory of Permutations in Breaking the Enigma Cipher" [1].

Le travail de Rejewski ne consistait pas à décrypter les messages secrets allemands. En réalité, son travail était beaucoup plus spectaculaire. Grâce aux documents secrets qui lui étaient à disposition et des messages cryptés, Rejewski tentait de reconstruire la machine, en essayant de déterminer le câblage des rotors qui se trouvaient à l'intérieur de la machine. Seulement après avoir passé cette étape de reconstruction de la machine, le décryptage de messages pourrait commencer.

3.1 Notions fondamentales

Pour comprendre le travail de Rejewski, nous avons premièrement besoin de quelques notions mathématiques fondamentales très connues. Une *permutation* sur E est une bijection $\phi : E \to E$. On appelle le *groupe symétrique* S_n, l'ensemble de toutes les permutations sur un ensemble avec n éléments. Le groupe symétrique satisfait donc toutes les propriétés d'un groupe. Le *support* d'une permutation est, comme le nom l'indique, les éléments concernés par la permutation. Plus précisément, il s'agit de l'ensemble des éléments de S_n, qui ne sont pas envoyés sur eux-mêmes ; c'est-à-dire $supp(\phi) = \{x \in E \mid \phi(x) \neq x\}$ De plus, on dit que les supports de deux permutations ϕ et γ sont *disjointes* si et seulement si $supp(\phi) \cap supp(\gamma) = \emptyset$.

Il y a plusieurs méthodes pour représenter les permutations. Si nous prenons la permutation $\alpha \in S_5$ qui envoie 1 sur 3, 2 sur 1, 3 sur 2, 4 sur 5 et 5 sur 4, nous pouvons la représenter comme un graphe (voir figure 3.1).

1. REJEWSKI, Marian. *"An Application of the Theory of Permutations in Breaking the Enigma Cipher"* in Applicationes Mathematicae 16, n°4.

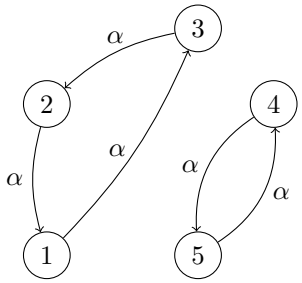

FIGURE 3.1 – Graphe de la permutation α

ou bien par l'écriture suivante, où l'élément du haut est envoyé sur celui du bas.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

Une *permutation cyclique* est une permutation $\phi \in S_n$,

$$\phi = \begin{pmatrix} x_0 & x_1 & x_2 & ... & x_k & ... & x_m \\ x_1 & x_2 & x_3 & ... & x_{k+1} & ... & x_0 \end{pmatrix}$$

qui envoie chaque élément x_k sur x_q tel que $q \equiv k+1 \pmod{m+1}$.

Remarque 3.1.1. Bien sûr, l'ordre d'écriture n'a aucune importance. C'est-à-dire que

$$\phi = \begin{pmatrix} x_0 & x_1 & x_2 & ... & x_m \\ x_1 & x_2 & x_3 & ... & x_0 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & ... & x_m & x_0 \\ x_2 & x_3 & ... & x_0 & x_1 \end{pmatrix} = ...$$

Nous dirons qu'une permutation cyclique de k éléments est un *k-cycle* et qu'un 2-cycle est une *transposition*. Pour simplifier l'écriture d'un cycle, nous écrirons

$$\phi = \begin{pmatrix} x_0 & x_1 & ... & x_m \\ x_1 & x_2 & ... & x_0 \end{pmatrix} = (x_0 x_1 ... x_m)$$

Remarque 3.1.2. Dans l'écriture simplifiée, chaque élément est envoyé sur celui qui se trouve à droite. Sauf, bien-sûr, pour l'élément qui est écrit tout à droite, qui est envoyé sur l'élément tout à gauche.

La permutation qui envoie chaque élément sur lui-même est appelée la *permutation identité*, notée Id. Le produit de deux permutations ϵ et γ, $\epsilon \circ \gamma$ est tout simplement la permutation γ suivie de ϵ. De plus, on écrit $\phi^r = \underbrace{\phi \circ \phi \circ ... \circ \phi}_{\phi \text{ apparait } r \text{ fois}}$. Il est important de noter que le produit de permutations n'est pas commutatif.

Proposition 3.1.1. *Pour toute permutation $\phi \in S_n$, il existe un entier $r > 0$ tel que $\phi^r = Id$.*

Démonstration. Soit $\phi \in S_n$, alors par définition de la permutation, il existe un inverse ϵ tel que $\phi \circ \epsilon = Id$. On montre premièrement par récurrence que $\phi^n \epsilon^n = Id$ pour tout $n \in \mathbb{Z}$. Pour $n = 0, 1$, c'est évident. Il nous suffit maintenant de supposer que $\phi^k \epsilon^k = Id$ ce qui implique que

$$\phi^{k+1} \epsilon^{k+1} = \phi(\phi^k \epsilon^k)\epsilon = \phi(Id)\epsilon = \phi\epsilon = Id$$

ce qui montre bien que $\phi^n\epsilon^n = Id$ pour tout $n \in \mathbb{Z}$. Comme le nombre de permutations dans S_n est fini, il existe deux entiers $x < y$, tel que $\phi^x = \phi^y$. On pose $r = y - x$ et on obtient

$$\phi^r = \phi^{y-x} = \phi^{y-x} \circ Id = \phi^{y-x}\phi^x\epsilon^x = \phi^y\epsilon^x = \phi^x\epsilon^x = Id$$

qui montre bien qu'un tel r existe. □

Cette proposition justifie la définition suivante.

Définition 3.1.1. On dit que *l'ordre* d'une permutation ϕ est le plus petit entier strictement positif tel que $\phi^r = Id$.

Pour pouvoir comprendre la proposition suivante nous avons besoin de définir ce que sont des *cycles disjoints*. On dit que deux cycles ϕ, γ sont disjoints si et seulement si leurs supports sont disjoints.

Proposition 3.1.2. *Toute permutation $\phi \in S_n$ peut s'écrire comme produit de cycles disjoints.*

Démonstration. Soit $\phi \neq Id$ une permutation sur E et supposons que $x_1^1 \in E$ tel que $\phi(x_1^1) \neq x_1^1$, alors il existe un x_2^1 tel que $\phi(x_1^1) = x_2^1$. Comme ϕ est bijectif, $\phi(x_2^1) \neq x_2^1$. Si $\phi(x_2^1) = x_1^1$, alors $(x_1^1x_2^1)$ est un cycle disjoint de la permutation. Sinon, on continue de la même manière en prenant $x_{n+1}^1 = \phi(x_n^1)$ jusqu'à ce que $\phi(x_{n+1}^1) = x_1^1$. On en conclut que $(x_1^1x_2^1...x_{n+1}^1)$ est un cycle. On dira que $\phi_1 = (x_1^1x_2^1...x_{n+1}^1)$. Il suffit de recommencer en prenant x_1^m qui n'est dans aucun des supports de $\phi_1, ..., \phi_{m-1}$ tel que $\phi(x_1^m) \neq x_1^m$ et obtient $\phi_m = (x_1^mx_2^m...x_y^m)$. On en conclut que $\phi = \phi_1 \circ \phi_2 \circ ... \circ \phi_m$ et il est évident que $\phi_1, \phi_2, ..., \phi_m$ sont des cycles disjoints. □

Exemple 3.1.1. Nous avons une permutation $\phi = (19856)(7651)$ dont les cycles sont non disjoints et nous allons tenter d'illustrer la proposition précédente. En effet, on a $\phi = (71)(598)$ sous forme de cycles disjoints.

Proposition 3.1.3. *Toute permutation $\phi \in S_n$ peut s'écrire comme produit de transpositions.*

Démonstration. Il suffit de monter qu'une permutation cyclique $(x_1x_2...x_k)$ peut s'écrire comme $(x_1x_2)(x_2x_3)...(x_{k-1}x_k)$. Pour $k = 2$, c'est évident. Maintenant, on suppose par récurrence que pour $k = n$, $(x_1x_2...x_k) = (x_1x_2)(x_2x_3)...(x_{n-1}x_n)$. Pour $k = n + 1$ on obtient

$$(x_1x_2...x_nx_{n+1}) = (x_1x_2...x_n)(x_nx_{n+1}) = (x_1x_2)(x_2x_3)...(x_{n-1}x_n)(x_nx_{n+1}).$$

Donc une permutation cyclique $(x_1x_2...x_k)$ peut s'écrire comme produit de transpositions pour tout k.
Par la proposition 3.1.2, toute permutation ϕ peut s'écrire comme produits de cycles disjoints $\phi = \phi_1 \circ \phi_2 \circ ... \circ \phi_m$ et chacun d'eux peut s'écrire comme produit de transpositions. On en conclut que toute permutation ϕ peut s'écrire comme produit de transpositions. □

Exemple 3.1.2. Si nous reprenons l'exemple précédent $\phi = (19856)(7651)$ qui peut s'écrire comme produit de cycles disjoints $\phi = (71)(598)$ qui peut s'écrire comme produit de transpositions $\phi = (71)(59)(98)$.

Nous avons encore besoin de quelques définitions qui auront une grande importance dans le travail de Rejewski.

Définition 3.1.2. On dit que deux permutations $\phi, \gamma \in S_n$ sont *conjuguées* s'il existe une permutation $\epsilon \in S_n$ tel que $\phi = \epsilon^{-1}\gamma\ \epsilon$.

Définition 3.1.3. La *structure orbitale* d'une permutation est le nombre de cycles disjoints et le nombre d'éléments dans le support de chaque cycle.

Exemple 3.1.3. Les permutations $(AB)(QCME)(XY)$ et $(BLDE)(MN)(AC)$ ont la même structure orbitale car les deux permutations ont trois cycles ; deux cycles de deux éléments et un cycle de quatre éléments.

Proposition 3.1.4. *Deux permutations $\phi, \gamma \in S_n$ sont conjuguées si et seulement si elles ont la même structure orbitale.*

Démonstration. Supposons pour commencer que ϕ et γ sont conjuguées, il existe alors par définition un ϵ tel que $\phi = \epsilon^{-1}\gamma\ \epsilon$. Si $\phi(x) = y$, alors $\gamma(\epsilon(x)) = \epsilon(y)$. Supposons que

$$\phi = (x_{00}x_{01}x_{02}...)(x_{10}x_{11}x_{12}...)...,$$

alors par ce qui vient d'être montré, on a notamment $\gamma(\epsilon(x_{00})) = \epsilon(x_{01})$. Pour finir, on a

$$\gamma = (\epsilon(x_{00})\epsilon(x_{01})\epsilon(x_{02})...)(\epsilon(x_{10})\epsilon(x_{11})\epsilon(x_{12})...)...,$$

donc ϕ et γ ont bien la même structure orbitale.
Supposons inversément que ϕ et γ ont la même structure orbitale. Disons que

$$\phi = \phi_1^2 \circ \phi_2^2 \circ \phi_3^2 \circ ... \circ \phi_1^n \circ \phi_2^n \circ \phi_3^n \circ ...$$

où ϕ_b^a est le b-ième cycle disjoint d'ordre a. De plus tous les cycles sont disjoints. Nous dirons que x_{bc}^a sont des éléments de $supp(\phi_b^a)$. Les x_b^1 sont les éléments qui sont envoyés sur eux mêmes. Ceci nous donne

$$\phi = (x_1^1)(x_2^1)(x_3^1) \circ ... \circ (x_{11}^2x_{12}^2)(x_{21}^2x_{22}^2) \circ ... \circ (x_{11}^nx_{12}^n...x_{1n}^n) \circ ...$$

Disons de manière similaire que

$$\gamma = \gamma_1^2 \circ \gamma_2^2 \circ \gamma_3^2 \circ ... \circ \gamma_1^n \circ \gamma_2^n \circ \gamma_3^n \circ ...$$

où γ_b^a est le b-ième cycle disjoint d'ordre a. Encore une fois, tous les cycles sont disjoints. Nous dirons que y_{bc}^a sont des éléments de $supp(\gamma_b^a)$. Les y_b^1 sont les éléments qui sont envoyés sur eux mêmes. Ceci nous donne

$$\gamma = (y_1^1)(y_2^1)(y_3^1) \circ ... \circ (y_{11}^2y_{12}^2)(y_{21}^2y_{22}^2) \circ ... \circ (y_{11}^ny_{12}^n...y_{1n}^n) \circ ...$$

Il suffit alors de prendre

$$\epsilon = \begin{pmatrix} x_{11}^1 & x_{21}^1 & x_{31}^1 & ... & x_{11}^2 & x_{12}^2 & x_{21}^2 & x_{22}^2 & ... & x_{11}^n & x_{12}^n & ... & x_{1n}^n \\ y_{11}^1 & y_{21}^1 & y_{31}^1 & ... & y_{11}^2 & y_{12}^2 & y_{21}^2 & y_{22}^2 & ... & y_{11}^n & y_{12}^n & ... & y_{1n}^n \end{pmatrix}$$

pour obtenir $\phi = \epsilon^{-1}\gamma\ \epsilon$. On en conclut que ϕ et γ sont conjuguées. □

Remarque 3.1.3. Dans la proposition précédente, il y a plusieurs ϵ possibles. Pour toutes les trouver, on peut échanger des cycles de même ordre dans une des permutations ϕ et γ. On peut aussi décaler l'écriture de chaque cycle.
Si ϕ et γ ont deux 13-cycles, alors ont peut écrire les cycles de 2 manières différentes. On peut en plus décaler l'écriture de chaque cycle pour obtenir 13 écritures différentes. Au total il y a donc $2 \cdot 13^2 = 338$ ϵ différents, qui satisfont $\phi = \epsilon^{-1}\gamma\ \epsilon$.

Exemple 3.1.4. Soient deux permutations $\phi = (AS)(ENIDHJTZ)$ et $\gamma = (AD)(QWERLPSV)$. Ensuite, nous cherchons une permutation ϵ, en procédant de la même manière que dans la démonstration de la proposition précédente(3.1.4). Nous obtenons

$$\epsilon = \begin{pmatrix} B & C & F & G & K & L & M & O & P & Q & R & U & V & X & Y & W & A & S & E & N & I & D & H & J & T & Z \\ B & C & F & G & K & I & J & O & M & N & H & U & T & X & Y & Z & A & D & Q & W & E & R & L & P & S & V \end{pmatrix}.$$

$$\epsilon = (LIEQNWZVTSDRH)(MJP)$$

Nous faisons le calcul

$$(HRDSTVZWNQEIL)(PJM) \circ (AD)(QWERLPSV) \circ (LIEQNWZVTSDRH)(MJP)$$
$$= (AS)(ENIDHJTZ)$$

qui montre bien que $\phi = \epsilon^{-1} \circ \epsilon$.

3.2 L'énigme du câblage des rotors

Pour pouvoir décrypter des messages allemands, Rejewski devait premièrement reconstruire et comprendre la machine et notamment, un des éléments les plus importants, le câblage de chaque rotor.

Pour commencer, Rejewski remarqua que tous les messages débutaient avec un indicateur qui transmettait la clé du message. Si par exemple la position des trois rotors précisée par le manuel des paramètres était ITP, alors l'opérateur les plaça correctement tel que la position du premier rotor soit I, le deuxième soit T et le dernier soit P. Ensuite, il choisit la clé de trois lettres du message ; par exemple MEP. Il écrivit deux fois cette clé sur sa machine et il obtint KLMLOP. Voici l'indicateur, qu'il écrivit au début de son message. Ensuite, il mit les rotors aux positions qui correspondent à cette clé, c'est-à-dire que le rotor le plus à droite était à la position P, celui du milieu à la position E et celui de gauche à la position M. Celui qui recevait ce message écrivit ensuite sur sa machine les six lettres de l'indicateur et il obtient MEPMEP. Ceci lui permettait de conclure que la clé du message est MEP et il plaçait donc ses rotors aux positions qui correspondaient à cette clé pour décrypter le message qu'il venait de recevoir. Plus d'informations sur la création de clés se trouvent à la section 2.4. Rejewski vit que tous les indicateurs qui commençaient par une même lettre (par exemple K) avaient tous la même lettre en quatrième position (par exemple L). Ceci était également vrai pour la deuxième et cinquième, et la troisième et la sixième lettre. Avec suffisamment de messages les trois fonctions qui donnaient la quatrième lettre en fonction de la première, la cinquième en fonction du deuxième et la sixième en fonction de la troisième pouvaient être déterminées.

Rejewski écrivit six équations massives, mais relativement simples qui décrivaient les six permutations impliquées dans le cryptage de la clé pour obtenir l'indicateur. De plus, il supposa que le deuxième et le troisième rotor demeuraient à la même position, respectivement, durant l'entier du cryptage de la clé. La probabilité de ceci était de $\frac{5}{26}$. C'est-à-dire que le premier rotor n'arrive jamais à la position d'engagement.

Dans ces six équations, $P = P^{-1}$ est la permutation faite par le tableau de connexion, E est la permutation du tambour d'entrée, R_1, R_2, R_3 les permutations des trois rotors et pour finir T est la permutation faite par le réflecteur. La permutation

$$\rho = (ABCDEFGHIJKLMOPQRSTUVWXYZ)$$

doit être présente parce que le premier rotor tourne. Si le rotor a tourné d'une position par rapport à la position d'origine et qu'un courant passe dans le fil A, alors, à la place d'entrer dans le contact A, il entrera dans le contact B. Si le courant sort du rotor par le contact A, alors le courant sort en réalité dans le fil Z. Pour s'en convaincre, il suffit de regarder la figure 2.6. Plus d'informations concernant ces différentes parties de la machine Enigma se trouvent dans le chapitre 2.

$$\Lambda_1 = P^{-1} \circ E^{-1} \circ \rho^{-1} R_1^{-1} \rho \circ R_2^{-1} \circ R_3^{-1} \circ T \circ R_3 \circ R_2 \circ \rho^{-1} R_1 \rho \circ E \circ P \tag{3.1}$$

$$\Lambda_2 = P^{-1} \circ E^{-1} \circ \rho^{-2} R_1^{-1} \rho^2 \circ R_2^{-1} \circ R_3^{-1} \circ T \circ R_3 \circ R_2 \circ \rho^{-2} R_1 \rho^2 \circ E \circ P \tag{3.2}$$

$$\Lambda_3 = P^{-1} \circ E^{-1} \circ \rho^{-3} R_1^{-1} \rho^3 \circ R_2^{-1} \circ R_3^{-1} \circ T \circ R_3 \circ R_2 \circ \rho^{-3} R_1 \rho^3 \circ E \circ P \tag{3.3}$$

$$\Lambda_4 = P^{-1} \circ E^{-1} \circ \rho^{-4} R_1^{-1} \rho^4 \circ R_2^{-1} \circ R_3^{-1} \circ T \circ R_3 \circ R_2 \circ \rho^{-4} R_1 \rho^4 \circ E \circ P \tag{3.4}$$

$$\Lambda_5 = P^{-1} \circ E^{-1} \circ \rho^{-5} R_1^{-1} \rho^5 \circ R_2^{-1} \circ R_3^{-1} \circ T \circ R_3 \circ R_2 \circ \rho^{-5} R_1 \rho^5 \circ E \circ P \tag{3.5}$$

$$\Lambda_6 = P^{-1} \circ E^{-1} \circ \rho^{-6} R_1^{-1} \rho^6 \circ R_2^{-1} \circ R_3^{-1} \circ T \circ R_3 \circ R_2 \circ \rho^{-6} R_1 \rho^6 \circ E \circ P \tag{3.6}$$

Soit xyz la clé que choisit l'opérateur et $abcdef$ l'indicateur du message, alors on a

$$\Lambda_1(x) = a, \Lambda_2(y) = b, \Lambda_3(z) = c, \Lambda_4(x) = d, \Lambda_5(y) = e, \Lambda_6(z) = f.$$

Comme la permutation faite par la machine est son propre inverse, on a $x = \Lambda_1(a)$, $y = \Lambda_2(b)$ et $z = \Lambda_3(c)$ et ceci nous permet de dire que $\Lambda_4(\Lambda_1(a)) = d$, $\Lambda_5(\Lambda_2(b)) = e$ et $\Lambda_6(\Lambda_3(c)) = f$ et il est donc possible de déterminer $\Lambda_4 \circ \Lambda_1$, $\Lambda_5 \circ \Lambda_2$ et $\Lambda_6 \circ \Lambda_3$

Théorème 3.2.1 (Théorème de Rejewski)**.** *Soit G l'ensemble de toutes les permutations $g \in S_{2n}$ tel que g est un produit de n transpositions disjointes. Soit $\alpha \in S_{2n}$. L'équation $XY = \alpha$, $X, Y \in G$, a une solution si et seulement si α a un nombre pair (éventuellement nul) de cycles disjoints de chaque ordre.*
De plus, si α possède $2m_i$ i-cycles tel que

$$2n = \sum_{i=1}^{n} 2m_i \cdot i$$

alors le nombre de solutions est

$$\prod_{i=1}^{n} \frac{i^{m_i} \cdot (2m_i)!}{2^{m_i} \cdot m_i!}$$

Démonstration. Cette démonstration est inspirée de la thèse "The Enigma History and Mathematics"[2] de Stephanie Faint.
Soit $X, Y \in G$ et prenons un élément a_1 et sa transposition $(a_1 b_1)$ dans X. Il existe forcément un a_2 tel que $(b_1 a_2)$ est une transposition de Y. Si $a_1 = a_2$, alors $(a_1 b_1)$ est une transposition de X et Y. Sinon, il existe un b_2 tel que $(a_2 b_2)$ est une transposition de X. Ensuite, nous prenons a_3 tel que $(b_2 a_3)$ est une transposition de Y. Si $a_3 = a_1$, nous avons que $(b_2 a_3) =$

2. FAINT, Stephanie. *"The Enigma History and Mathematics"*, Waterloo, Ontario, Canada, 1999, 75 pages.

(b_2a_1) et (b_1a_2) sont des transpositions de Y et que (a_1b_1) et (a_2b_2) sont des transpositions de X et leur produit $(b_2a_1)(b_1a_2)(a_1b_1)(a_2b_2) = (a_1a_2)(b_1b_2)$ donne deux 2-cycles disjoints de α. Sinon le processus continue, comme il a déjà été décrit, jusqu'à ce que nous trouvions un $a_k = a_1$. Alors $(a_1a_2...a_{k-1})$ et $(b_1b_2...b_{k-1})$ sont des $(k-1)$-cycles disjoints de α, parce que $(a_1b_1)(a_2b_2)..(a_{k-1}b_{k-1})...(a_2b_1)(a_3b_2)..(a_1b_{k-1}) = (a_1a_2...a_{k-1})(b_1b_2...b_{k-1})$. Nous obtenons deux cycles disjoints de même longueur. Nous en déduisons que si $XY = \alpha$ a une solution, alors α possède un nombre pair de cycles disjoints de même longueur, parce que X et Y sont disjointes. Prenons maintenant un α avec un nombre pair de cycles disjoints de même ordre. Il suffit de prendre deux cycles de même ordre $(a_1a_2...a_{k-1}a_k)$ et $(b_1b_2...b_{k-1}b_k)$ et nous pouvons facilement vérifier que $X = (a_2b_k)(a_3b_{k-1})...(a_1b_1)$ et $Y = (a_1b_k)(a_2b_{k-1})...(a_kb_1)$ sont des solutions, mais il est important pour la suite de noter qu'il y a k solutions pour X et Y. La figure 3.2 montre comment on arrive à cette solution. La raison pour laquelle il y a k solutions, est qu'on peut décaler l'écriture d'un des cycles k fois et obtenir des X et Y différents.

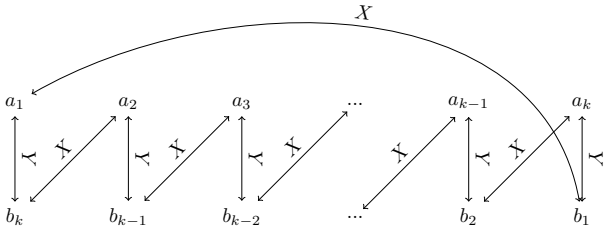

FIGURE 3.2 – Schéma du théorème de Rejewski

En ce qui concerne la deuxième partie du théorème, considérons tous les k-cycles de α. Il y a un total de $2m_k$ k-cycles et nous regroupons ces $2m_k$ objets par 2. Pour ce faire, il y a

$$C_2^{2m_k} = \frac{2m_k!}{2 \cdot (2m_k - 2)!}$$

possibilités différents et ensuite, il y a

$$C_2^{2m_k-2} = \frac{(2m_k - 2)!}{2 \cdot (2m_k - 4)!}$$

possibilités différentes et ainsi de suite. On obtient :

$$C_2^{2m_k} \cdot C_2^{2m_k-2} \cdot ... = \frac{2m_k!}{2 \cdot (2m_k - 2)!} \cdot \frac{(2m_k - 2)!}{2 \cdot (2m_k - 4)!} \cdot ... = \frac{(2m_k)!}{2^{m_k}}.$$

Mais, comme la solution est indépendante de l'ordre dans lequel nous choisissons les paires de k-cycles, nous obtenons :

$$\frac{(2m_k)!}{2^{m_k} \cdot m_k!}$$

Comme nous l'avons déjà démonté dans la première partie du théorème, il y a k solutions différentes X et Y, pour une paire de k-cycles et nous en déduisons qu'il y a

$$\frac{k^{m_k} \cdot (2m_k)!}{2^{m_k} \cdot m_k!}$$

possibilités pour l'ensemble des k-cycles. Jusqu'ici, nous avons traité les k-cycles, mais si nous considérons toutes les cycles de la permutation, nous obtenons

$$\prod_{i=1}^{n} \frac{i^{m_i} \cdot (2m_i)!}{2^{m_i} \cdot m_i!}$$

possibilités de solutions pour X et Y. □

Ce théorème nous permet donc de dire que les permutations $\Lambda_4 \circ \Lambda_1$, $\Lambda_5 \circ \Lambda_2$ et $\Lambda_6 \circ \Lambda_3$ ont toutes un nombre pair (éventuellement nul) de cycles disjoints de chaque ordre.

Remarque 3.2.1. L'ensemble G de la proposition précédente correspond à l'ensemble de toutes les permutations qui peuvent être effectuées par la machine Enigma.

Corollaire 3.2.1. *Quand la permutation $\alpha \in S_{2n}$ est composée seulement de cycles disjoints tel que pour tout i, le nombre de cycles d'ordre i est soit nul, soit égal à 2 (i.e. $m_i \in \{0,1\} \forall i$), alors le nombre de possibilités pour $X, Y \in G, XY = \alpha$ est*

$$\prod_{i=1}^{n} i^{m_i}$$

Démonstration. Pour tout i, m_i vaut 0 ou 1. Le résultat se démontre par un calcul simple :

$$\prod_{i=1}^{n} \frac{i^{m_i} \cdot (2m_i)!}{2^{m_i} \cdot m_i!} = \prod_{i=1, m_i=0}^{n} \frac{i^{m_i} \cdot (2m_i)!}{2^{m_i} \cdot m_i!} \cdot \prod_{i=1, m_i=1}^{n} \frac{i^{m_i} \cdot (2m_i)!}{2^{m_i} \cdot m_i!} = 1 \cdot \prod_{i=1, m_i=1}^{n} i = \prod_{i=1}^{n} i^{m_i}$$

□

Remarque 3.2.2. Pour connaitre le nombre de possibilités, lorsqu'on est dans une situation comme ci-dessus, il suffit de multiplier tous les ordres de chaque paire de cycles dans α. Si, par exemple, $\alpha = (AX)(WS)(ERTZ)(POIU)$, alors il y a $2 \cdot 4 = 8$ possibilités pour X et Y.

Exemple 3.2.1. Soit $\phi = (\text{QRLMO})(\text{ABCXY})$ et cherchons deux $\epsilon, \gamma \in G$ (chacun produit de cinq transpositions) tel que $\epsilon\gamma = \phi$. On peut écrire le schéma suivant pour trouver des solutions :

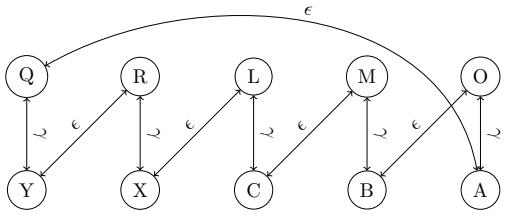

FIGURE 3.3 – Schéma du théorème de Rejewski

Ce schéma permet de reconstruire la solution donnée dans la démonstration du théorème de Rejewski et on obtient une solution $\epsilon = (\text{QA})(\text{RY})(\text{LX})(\text{MC})(\text{OB}) \in G$ et $\gamma = (\text{QY})(\text{RX})(\text{LC})(\text{MB})(\text{OA}) \in G$. En décalant l'écriture d'un des cycles du schéma (QRLMO) = (RLMOQ) = (LMOQR) = (MOQRL) = (OQRLM), on obtient un total de cinq possibilités de ϵ et γ différentes tel que $\epsilon \circ \gamma = \phi$. Ceci illustre le corollaire 3.2.1 parce qu'il y a, effectivement, deux cycles d'ordre 5.

Le théorème de Rejewski permet donc de limiter le nombre de possibilités pour les fonctions Λ_1, Λ_2, Λ_3, Λ_4, Λ_5 et Λ_6. Cette réduction de possibilités est donc possible grâce aux procédures de cryptage mis en place par les Allemands, qui crypte doublement la clé pour obtenir l'indicateur.

Exemple 3.2.2. Pour illustrer ce qui vient d'être dit, nous allons supposer que nous avons intercepté assez de messages avec des indicateurs différents pour déterminer que

$$\Lambda_4 \circ \Lambda_1 = (QX)(ET)(BDP)(KNC)(RZMJIV)(ALOWHU),$$

$$\Lambda_5 \circ \Lambda_2 = (EU)(LP)(XCGHYWRTQFS)(ZKVBOMJNADI)$$

et

$$\Lambda_6 \circ \Lambda_3 = (UFV)(XBC)(QWJGLEHYZA)(PDTOKSIMNR)$$

Grâce au théorème de Rejewski (3.2.1) et son corollaire, nous pouvons dire qu'il y a $2 \cdot 3 \cdot 6 = 36$ possibilités pour les permutations Λ_1 et Λ_4, $2 \cdot 11 = 22$ possibilités pour Λ_2 et Λ_5 et $3 \cdot 9 = 27$ possibilités pour Λ_3 et Λ_6.

De plus, il y avait chez les opérateurs allemands de mauvaises habitudes. Il y avait notamment des opérateurs qui choisissaient toujours la même clé, ou bien des personnes qui choisissaient des clés évidentes tel que par exemple AAA. Ceci permettait de réduire grandement les possibilités pour les permutations Λ_1, Λ_2, Λ_3, Λ_4, Λ_5 et Λ_6(voir l'exemple 3.2.3).

Exemple 3.2.3. Nous reprenons l'exemple précédent et imaginons qu'il y a un opérateur allemand ignorant qui est fermement convaincu que la machine Enigma est indéchiffrable. Il en est tellement convaincu qu'il choisit la même clé tous les jours pour tous les messages : AAA. Ceci peut être remarqué par le fait que ses indicateurs ne contiennent jamais la lettre A. Aujourd'hui, son indicateur est IYSVWI, ce qui nous permet de dire, en se servant du théorème de Rejewski, que la permutation Λ_1 doit contenir les cycles $(AI)(LJ)(OM)(WZ)(HR)(UV)$ et Λ_4 doit comprendre le cycles $(AV)(LI)(OJ)(WM)(HZ)(UR)$ en utilisant le théorème de Rejewski (3.2.1). De cette façon, nous avons réussi à passer de 36 possibilités à 6 parce qu'avec les cycles $(QX)(ET)(BDP)(KNC)$ on trouve 6 possibilités. Avec un raisonnement semblable, cela permet, pour les permutations Λ_2 et Λ_5, de diminuer le nombre de possibilités à 2. En ce qui concerne les permutations Λ_3 et Λ_6, le nombre de possibilités passent à 3.

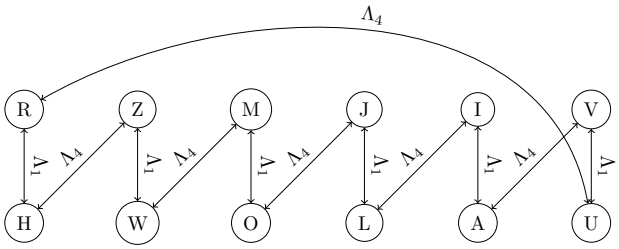

FIGURE 3.4 – Schèma de l'exemple

Remarque 3.2.3. Evidement, le cryptologue ne peut pas connaître les préférences de l'opérateur. Rejewski, dit lui-même que le cryptologue "essaie de compenser son ignorance par de longs essais, de l'imagination et parfois un peu de chance" [3].

3. REJEWSKI, Marian. *"An Application of the Theory of Permutations in Breaking the Enigma Cipher"* in Applicationes Mathematicae 16, n°4.

Après cette étape, Rejewski choisit de simplifier ses six équations en supposant que les permutations P et E étaient connues (en réalité E était inconnu). Il remplaça aussi $R_2^{-1} \circ R_3^{-1} \circ T \circ R_3 \circ R_2$ par Q pour simplifier l'écriture de ces équations massives. On obtient donc

$$\Lambda_1' = \rho^{-1} R_1^{-1} \rho \circ Q \circ \rho^{-1} R_1 \rho = EP \circ \Lambda_1 \circ P^{-1} E^{-1} \tag{3.7}$$

$$\Lambda_2' = \rho^{-2} R_1^{-1} \rho^2 \circ Q \circ \rho^{-2} R_1 \rho^2 = EP \circ \Lambda_2 \circ P^{-1} E^{-1} \tag{3.8}$$

$$\Lambda_3' = \rho^{-3} R_1^{-1} \rho^3 \circ Q \circ \rho^{-3} R_1 \rho^3 = EP \circ \Lambda_3 \circ P^{-1} E^{-1} \tag{3.9}$$

$$\Lambda_4' = \rho^{-4} R_1^{-1} \rho^4 \circ Q \circ \rho^{-4} R_1 \rho^4 = EP \circ \Lambda_4 \circ P^{-1} E^{-1} \tag{3.10}$$

$$\Lambda_5' = \rho^{-5} R_1^{-1} \rho^5 \circ Q \circ \rho^{-5} R_1 \rho^5 = EP \circ \Lambda_5 \circ P^{-1} E^{-1} \tag{3.11}$$

$$\Lambda_6' = \rho^{-6} R_1^{-1} \rho^6 \circ Q \circ \rho^{-6} R_1 \rho^6 = EP \circ \Lambda_6 \circ P^{-1} E^{-1} \tag{3.12}$$

Rejewski modifia encore une fois ces équations.

$$\Psi_1 = \rho \circ \Lambda_1' \circ \rho^{-1} = R_1^{-1} \rho \circ Q \circ \rho^{-1} R_1 \tag{3.13}$$

$$\Psi_2 = \rho^2 \circ \Lambda_2' \circ \rho^{-2} = R_1^{-1} \rho^2 \circ Q \circ \rho^{-2} R_1 \tag{3.14}$$

$$\Psi_3 = \rho^3 \circ \Lambda_3' \circ \rho^{-3} = R_1^{-1} \rho^3 \circ Q \circ \rho^{-3} R_1 \tag{3.15}$$

$$\Psi_4 = \rho^4 \circ \Lambda_4' \circ \rho^{-4} = R_1^{-1} \rho^4 \circ Q \circ \rho^{-4} R_1 \tag{3.16}$$

$$\Psi_5 = \rho^5 \circ \Lambda_5' \circ \rho^{-5} = R_1^{-1} \rho^5 \circ Q \circ \rho^{-5} R_1 \tag{3.17}$$

$$\Psi_6 = \rho^6 \circ \Lambda_6' \circ \rho^{-6} = R_1^{-1} \rho^6 \circ Q \circ \rho^{-6} R_1 \tag{3.18}$$

Ensuite, Rejewski eut l'idée de faire des produits de ces permutations et il obtint quatre équations

$$\Psi_2 \Psi_3 = R_1^{-1} \rho R_1 (\Psi_1 \Psi_2) R_1^{-1} \rho^{-1} R_1 \tag{3.19}$$

$$\Psi_3 \Psi_4 = R_1^{-1} \rho R_1 (\Psi_2 \Psi_3) R_1^{-1} \rho^{-1} R_1 \tag{3.20}$$

$$\Psi_4 \Psi_5 = R_1^{-1} \rho R_1 (\Psi_3 \Psi_4) R_1^{-1} \rho^{-1} R_1 \tag{3.21}$$

$$\Psi_5 \Psi_6 = R_1^{-1} \rho R_1 (\Psi_4 \Psi_5) R_1^{-1} \rho^{-1} R_1 \tag{3.22}$$

qui avaient comme seule inconnue $R_1^{-1} \rho R_1$. Comme Rejewski avait précédemment pu réduire grandement les possibilités, il lui suffisait d'essayer lesquels satisfaisaient ce système tel qu'un R_1 existe. Cette démarche permettait de déterminer R_1.

Remarque 3.2.4. Par la proposition 3.1.4, $\Psi_1\Psi_2$, $\Psi_2\Psi_3$, $\Psi_3\Psi_4$, $\Psi_4\Psi_5$ et $\Psi_5\Psi_6$ sont tous conjuguées entre eux. C'est-à-dire qu'ils ont la même structure orbitale. Si ces permutations n'ont pas la même structure orbitale, alors le deuxième rotor s'est déplace durant la création de l'indicateur.

Mais pour écrire les équations 3.7 à 3.12 qui sont à la base du raisonnement de Rejewski permettant de déterminer le câblage du premier rotor, les permutations P et E étaient supposés connues. Pourtant, ces permutations nous étaient complètement inconnues. La fonction P figurait néanmoins dans les documents mis à disposition par les Français (pages 14 à 15). La fonction E, au contraire, n'était pas précisée dans ces documents et était indéterminable. De plus, cette permutation n'était soumise à aucune contrainte, contrairement à P, ce qui impliquait qu'il y avait un total de 26! possibilités pour cette permutation E. Sur l'Enigma commerciale, la permutation E projetait tout simplement les lettres en suivant l'ordre du clavier (QWERTZ) sur l'alphabet, c'est-à-dire que Q était envoyé sur A, W sur B, E sur C, R sur D et ainsi de suite.

L'historien Frank Carter [4] dit que Rejewski avait essayé avec un grand nombre de permutations, avec l'énorme quantité de travail que cela implique et qu'après quelques temps, il essaya avec la permutation identité.

Rejewski remarqua alors qu'effectivement la permutation du tambour d'entrée est, en effet, la permutation identité. La réussite de Rejewski est sans doute un miracle, mais le choix trop évident de permutation par les ingénieurs allemands est naïf.

Cette démarche permettait seulement de déterminer le premier rotor et Rejewski avait seulement à disposition les clés pour les mois de septembre et octobre 1932. Heureusement pour Rejewski, les Allemands changeaient l'ordre des rotors entre ces deux mois et ceci lui permettait de déterminer le câblage de deux rotors. Malheureusement, il restait encore un troisième rotor dont il fallait déterminer le câblage avant de pouvoir reconstruire la machine.

Exemple 3.2.4. Cet exemple ne reprend rien des exemples d'avant. Le but de cet exemple sera de refaire le travail de Rejewski pour trouver le câblage du rotor de droite. Pour une question de longueur, nous imaginerons que nous sommes déjà arrivés à connaitre les fonctions suivantes en analysant les indicateurs du jour :

$$\Lambda'_1 = (AB)(CD)(EQ)(FS)(GX)(HR)(IL)(JK)(MO)(PN)(TV)(UY)(WZ)$$

$$\Lambda'_2 = (AY)(BF)(CD)(EL)(GJ)(HZ)(IR)(KX)(MU)(NW)(OQ)(PT)(SV)$$

$$\Lambda'_3 = (AQ)(BT)(CV)(DL)(EP)(FY)(GU)(HR)(IO)(JZ)(KS)(MX)(NW)$$

$$\Lambda'_4 = (AD)(BN)(CP)(EY)(FS)(GX)(HZ)(IO)(JL)(KV)(MW)(QU)(RT)$$

$$\Lambda'_5 = (AC)(BS)(DG)(EP)(FO)(HJ)(IU)(KW)(LT)(MQ)(NR)(VY)(XZ)$$

$$\Lambda'_6 = (AI)(BF)(CT)(DE)(GO)(HP)(JK)(LU)(MZ)(NX)(QS)(RW)(VY)$$

Ce qui nous donne, en calculant :

$$\Psi_1\Psi_2 = (ABMVFDYNTLSOU)(CXWQIKGPHERZJ)$$

$$\Psi_2\Psi_3 = (AYEONRIJUTHQM)(BLVGWFPCZSDKX)$$

$$\Psi_3\Psi_4 = (AZGDRYKIMHWXN)(BUFLTOQPVJESC)$$

$$\Psi_4\Psi_5 = (ALCHRXTBNOSJY)(DQUWMZPKGVFEI)$$

$$\Psi_5\Psi_6 = (AVZLFWQBCGMJT)(DKUOXEPYSHINR)$$

4. ROSE Stuart, *Heroes of War Poland : Cracking Enigma*, 2014.

Nous cherchons maintenant une permutation $R_1^{-1}\rho R_1$ qui envoie chacun de ces cycles sur un des cycles de la permutation suivante. Nous savons, grâce à la proposition 3.1.4 que cette permutation est un 26-cycle parce que ρ est un 26-cycle. Pour trouver $R_1^{-1}\rho R_1$, nous allons nous inspirer de la démonstration de la proposition 3.1.4. Par la remarque 3.1.3, il y a $13^2 \cdot 2 = 338$ permutations $R_1^{-1}\rho R_1$ différentes qui satisfont $\Psi_2\Psi_3 = R_1^{-1}\rho R_1(\Psi_1\Psi_2)R_1^{-1}\rho^{-1}R_1$. Il suffit de déterminer lesquels de ceci satisfont $\Psi_3\Psi_4 = R_1^{-1}\rho R_1(\Psi_2\Psi_3)R_1^{-1}\rho^{-1}R_1$, mais nous n'avons pas besoin de les essayer toutes. Nous considérons seulement les 26 fonctions différentes qui permettent d'envoyer le premier cycle de $\Psi_1\Psi_2$ sur un des cycles de $\Psi_2\Psi_3$. Pour envoyer le premier cycle de $\Psi_1\Psi_2$ sur le premier de $\Psi_2\Psi_3$ il s'agit des fonctions [5]

$$\begin{pmatrix} A & B & M & V & F & D & Y & N & T & L & S & O & U \\ A & Y & E & O & N & R & I & J & U & T & H & Q & M \end{pmatrix},$$

$$\begin{pmatrix} A & B & M & V & F & D & Y & N & T & L & S & O & U \\ Y & E & O & N & R & I & J & U & T & H & Q & M & A \end{pmatrix},$$

$$\begin{pmatrix} A & B & M & V & F & D & Y & N & T & L & S & O & U \\ E & O & N & R & I & J & U & T & H & Q & M & A & Y \end{pmatrix},$$

et ainsi de suite (en continuant à décaler la ligne du dessous). Pour envoyer le premier cycle de $\Psi_1\Psi_2$ sur le deuxième de $\Psi_2\Psi_3$ il s'agit des fonctions

$$\begin{pmatrix} A & B & M & V & F & D & Y & N & T & L & S & O & U \\ B & L & V & G & W & F & P & C & Z & S & D & K & X \end{pmatrix},$$

$$\begin{pmatrix} A & B & M & V & F & D & Y & N & T & L & S & O & U \\ L & V & G & W & F & P & C & Z & S & D & K & X & B \end{pmatrix},$$

$$\begin{pmatrix} A & B & M & V & F & D & Y & N & T & L & S & O & U \\ V & G & W & F & P & C & Z & S & D & K & X & B & L \end{pmatrix},$$

et ainsi de suite (en continuant à décaler la ligne du dessous).

Ensuite, nous essayons de déterminer lesquelles de ces fonctions pourraient être des solutions de $\Psi_3\Psi_4 = R_1^{-1}\rho R_1(\Psi_2\Psi_3)R_1^{-1}\rho^{-1}R_1$. C'est-à-dire que nous vérifions lesquelles de ces fonctions permettrait d'envoyer un des cycles de $\Psi_2\Psi_3$ sur un des cycles de $\Psi_3\Psi_4$ On trouve que

$$\begin{pmatrix} A & B & M & V & F & D & Y & N & T & L & S & O & U \\ C & Z & S & D & K & X & B & L & V & G & W & F & P \end{pmatrix}$$

est la seule fonction qui permettrait potentiellement d'envoyer le cycle

$$(AYEONRIJUTHQM)$$

sur un des cycles de

$$(AZGDRYKIMHWXN)(BUFLTOQPVJESC).$$

5. Dans chacune des parenthèses, la fonction envoie l'élément du dessus sur celui du dessous.

En effet, cette fonction envoie A sur C, Y sur B, O sur F, N sur L, U sur P, T sur U et M sur S. Le cycle

$$(AYEONRIJUTHQM)$$

donne donc

$$(\mathbf{CB}U\mathbf{FL}TOQ\mathbf{PV}JE\mathbf{S})$$

qui correspond à

$$(BUFLTOQPVJESC).$$

Ensuite, on cherche donc une fonction qui envoie le deuxième cycle des $\Psi_1\Psi_2$ $(CXWQIKGPHERZJ)$ sur l'autre cycle de $\Psi_2\Psi_3$ $(AYEONRIJUTHQM)$ tel que cette fonction envoie E sur U, I sur O, J sur Q, H sur J et Q sur E pour que cette fonction soit cohérente avec la precédente. Ceci nous donne

$$\begin{pmatrix} C & X & W & Q & I & K & G & P & H & E & R & Z & J \\ M & A & Y & E & O & N & R & I & J & U & T & H & Q \end{pmatrix}$$

Au final, on trouve, en combinant les deux fonctions trouvés, la permutation

$$\begin{pmatrix} A & B & M & V & F & D & Y & N & T & L & S & O & U & C & X & W & Q & I & K & G & P & H & E & R & Z & J \\ C & Z & S & D & K & X & B & L & V & G & W & F & P & M & A & Y & E & O & N & R & I & J & U & T & H & Q \end{pmatrix}.$$

Nous nous rendons compte que cette permutation satisfait toutes les équations et nous trouvons donc que

$$R_1^{-1}\rho R_1 = (DXACMSWYBZHJQEUPIOFKNLGRTV)$$

Pour R_1, il y a 26 possibilités, mais en utilisant des solutions différentes $R_1^{-1}\rho R_1$ trouvés des jours différents, nous pouvons tout de même déterminer R_1. Nous trouvons que

$$R_1 = (XBIQMENUOR)(YHKT)(ZJLV)(ACD)(FS)(GW)(P).$$

Le tableau suivant montre comment agit ce rotor. Nous pouvons aussi définir le câblage du rotor avec une suite de nombre que nous pouvons voir dans ce tableau. Le nombre correspond la distance entre les contacts liés.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G	B	H	J
2	7	1	23	9	13	17	3	8	2	9	10	18	7	3	0	22	6	13	5	20	4	10	4	9	10

Table 3.1 – Solution trouvée

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
4	9	10	2	7	1	23	9	13	17	3	8	2	9	10	18	7	3	0	22	6	13	5	20	4	10

Table 3.2 – Rotor 1

Si nous faisons la même chose avec la table du rotor 1, (qui se trouve aussi à la page 10) nous pouvons voir que ce R_1 correspond au câblage du rotor 1 décalé de quelques positions. En effet, le rotor est décale de 4 positions, mais cela ne veut pas dire que le ringstellung est D, car la solution trouvée dépend aussi de la position de départ du rotor.

3.3 Le troisième rotor

Il s'agit maintenant de déterminer le câblage du troisième rotor en connaissant deux rotors et les clés journalières pour deux mois.

La méthode que nous présenterons maintenant sera grandement inspiré de la thèse "The Enigma History and Mathematics"[6] de Stephanie Faint. On suppose que le rotor inconnu est à la troisième position. Comme nous l'avons vu dans la section précédente, on peut déterminer les permutations qui interviennent dans la création de l'indicateur.

En ayant à disposition le manuel de création de clés, on peut durant un mois trouver des Λ différents tel que :

$$\Lambda_0 = P^{-1}E^{-1} \circ \rho^{-n_0}R_1^{-1}\rho^{n_0} \circ \rho^{-m_0}R_2^{-1}\rho^{m_0} \circ \rho^{-z}R_3^{-1}\rho^{z} \circ T \circ \rho^{-z}R_3\rho^{z} \circ \rho^{-m_0}R_2\rho^{m_0} \circ \rho^{-n_0}R_1\rho^{n_0} \circ EP$$

$$\Lambda_3 = P^{-1}E^{-1} \circ \rho^{-n_3}R_1^{-1}\rho^{n_3} \circ \rho^{-m_3}R_2^{-1}\rho^{m_3} \circ \rho^{-z-3}R_3^{-1}\rho^{z+3} \circ T \circ \rho^{-z-3}R_3\rho^{z+3} \circ \rho^{-m_3}R_2\rho^{m_3} \circ \rho^{-n_3}R_1\rho^{n_3} \circ EP$$

$$\Lambda_6 = P^{-1}E^{-1} \circ \rho^{-n_6}R_1^{-1}\rho^{n_6} \circ \rho^{-m_6}R_2^{-1}\rho^{m_6} \circ \rho^{-z-6}R_3^{-1}\rho^{z+6} \circ T \circ \rho^{-z-6}R_3\rho^{z+6} \circ \rho^{-m_6}R_2\rho^{m_6} \circ \rho^{-n_6}R_1\rho^{n_6} \circ EP$$

$$\Lambda_9 = P^{-1}E^{-1} \circ \rho^{-n_9}R_1^{-1}\rho^{n_9} \circ \rho^{-m_9}R_2^{-1}\rho^{m_9} \circ \rho^{-z-9}R_3^{-1}\rho^{z+9} \circ T \circ \rho^{-z-9}R_3\rho^{z+9} \circ \rho^{-m_9}R_2\rho^{m_9} \circ \rho^{-n_9}R_1\rho^{n_9} \circ EP$$

Pour chaque Λ_n, on peut trouver un $J_n = \rho^{-m_n}R_2\rho^{m_n} \circ \rho^{-n_n}R_1\rho^{n_n} \circ E \circ P$ tel que $\Lambda_n = J_n^{-1}U_nJ_n$. On obtient :

$$U_0 = J_0A_0J_0^{-1} = \rho^{-z}R_3^{-1}\rho^{z} \circ T \circ \rho^{-z}R_3\rho^{z}$$

$$U_3 = J_3A_3J_3^{-1} = \rho^{-z-3}R_3^{-1}\rho^{z+3} \circ T \circ \rho^{-z-3}R_3\rho^{z+3}$$
$$U_6 = J_6A_6J_6^{-1} = \rho^{-z-6}R_3^{-1}\rho^{z+6} \circ T \circ \rho^{-z-6}R_3\rho^{z+6}$$
$$U_9 = J_9A_9J_9^{-1} = \rho^{-z-9}R_3^{-1}\rho^{z+9} \circ T \circ \rho^{-z-9}R_3\rho^{z+9}$$

Ensuite, on pose :

$$\Psi_0 = \rho^{z}U_0\rho^{-z} = R_3^{-1}\rho^{z} \circ T \circ \rho^{-z}R_3$$
$$\Psi_3 = \rho^{z+3}U_3\rho^{-z-3} = R_3^{-1}\rho^{z+3} \circ T \circ \rho^{-z-3}R_3$$
$$\Psi_6 = \rho^{z+6}U_6\rho^{-z-6} = R_3^{-1}\rho^{z+6} \circ T \circ \rho^{-z-6}R_3$$
$$\Psi_9 = \rho^{z+9}U_9\rho^{-z-9} = R_3^{-1}\rho^{z+9} \circ T \circ \rho^{-z-9}R_3$$

Comme pour la détermination du câblage des deux autres rotors, on essaie d'en déduire des équations avec seulement une inconnue, R_3. Les quatre équations précédentes permettent de dire que

$$\Psi_3\Psi_6 = R_3^{-1}\rho^{3}R_3(\Psi_0\Psi_3)R_3^{-1}\rho^{-3}R_3$$
$$\Psi_6\Psi_9 = R_3^{-1}\rho^{3}R_3(\Psi_3\Psi_6)R_3^{-1}\rho^{-3}R_3.$$

Ceci permet de réduire les possibilités pour $R_3^{-1}\rho^3R_3$, voire de le déterminer et par conséquent aussi déterminer R_3. Ici, nous avons supposé que nous avons trouvé des Λ différents à des intervalles de 3, mais on pourrait très bien trouver R_3 en se servant des Λ à d'autres intervalles.

6. FAINT, Stephanie. *"The Enigma History and Mathematics"*, Waterloo, Ontario, Canada, 1999, 75 pages.

Chapitre 4

Le décryptage peut commencer

Les Polonais réussirent à reconstruire la machine grâce à des messages cryptés, donc il suffirait de faire l'inverse pour décrypter des messages, pourrait-on penser. En réalité, ce n'est pas du tout si simple, parce que les Polonais n'avaient plus accès à la permutation P qui se trouvait dans les documents qu'ils recevaient de la part des Français. Les Polonais réussirent, à développer plusieurs techniques qui leur permettaient de déterminer la position journalière des rotors. Une des premières était de créer un répertoire qui permettait de déterminer rapidement la position correcte des rotors. Ce répertoire se révéla inutile quand les Allemands modifièrent leur procédé de création de clés. Jusqu'à maintenant, tous les opérateurs Enigma commençaient avec la même position de rotors lorsqu'ils tapaient doublement leur clé, ce qui permettait d'en faire les déductions que nous avons faites. En utilisant le nouveau procédé, l'opérateur plaçait les rotors dans un ordre bien défini par leur manuel qui indiquait aussi le *ringstellung* de chaque rotor. L'opérateur choisit ensuite la position de chaque rotor et il commençait son message par les trois lettres qui définissent la position de chaque rotor. Ensuite, il procédait exactement de la même manière qu'auparavant en tapant sa clé deux fois. Si l'opérateur choisit de positionner ses rotors aux positions RTN et qu'il tapait ensuite deux fois ALE qui lui donne WAR QLC, alors son message commençait par

RTN WAR QLC.

Pour réussir à décrypter ce genre de messages, Marian Rejewski eut l'idée de créer une machine.

4.1 Le répertoire

Comme nous l'avons déjà dit, une idée développée au début était la création d'un répertoire. Pour chaque ordre et positions des rotors différents, on note le nombre et la longueur des cycles de la permutation $\Lambda_{n+3} \circ \Lambda_n$ où Λ_n est une permutation de la machine Enigma avec les rotors à la position n (comme dans le chapitre precédent) et Λ_{n+3} est simplement la permutation Λ_n avec le premier rotor décalé de 3 positions. Si on reprend les permutations de l'exemple 3.2.2 à la page 23, alors obtient le répertoire suivant (tableau 4.1).

Ordre des rotors	Positions des rotors	Cycles obtenus
I, II, III	A, G, H	2, 2, 3, 3, 6, 6
I, II, III	A, G, I	2, 2, 11, 11
I, II, III	A, G, J	3, 3, 9, 9

TABLE 4.1 – Exemple répertoire

En utilisant la proposition 3.1.4, on peut dire que quelles que soient les connexions faites sur le tableau de connexion, la structure orbitale qui est spécifié dans le répertoire reste le même. Ceci permet donc d'ignorer complètement le tableau de connexion ce qui réduit considérablement le nombre de possibilités.

Il a tout de même fallu une année pour créer ce répertoire. Ceci s'explique par l'énorme quantité de configurations différentes à répertorier. Pour tout ordre de rotor, il y a $26^3 = 17576$ positions différentes et il y a $3! = 6$ ordres de rotors différentes. En tout, il y a donc $26^3 \cdot 6 = 105456$ possibilités à inscrire dans le répertoire. Alors, pour trouver la configuration du jour, il suffit de déterminer, chaque jour, les fonctions $\Lambda_4 \circ \Lambda_1$, $\Lambda_5 \circ \Lambda_2$ et $\Lambda_6 \circ \Lambda_3$, en particulier l'ordre de chaque cycle des permutations. Ensuite, il reste à comparer avec le répertoire pour y trouver trois configurations consécutives qui correspondent aux fonctions trouvées. Il se peut évidemment qu'on trouve plusieurs solutions, mais le nombre de solutions seront grandement réduites.

Malheureusement, pour le cryptologue, le ringstellung complique le procédé de décryptage. Le répertoire se base sur l'idée que seul le rotor de droite se déplace et que les deux autres restent immobiles. Si le premier rotor atteint sa position d'engagement durant le cryptage de la clé du message, le répertoire devient inutile. La probabilité que ceci arrive est d'environ 20%. Klaus Pommerening écrit dans son article "The Enigma" [1] que le taux de réussite du répertoire est de 50%, mais que la probabilité de 20% réduit le taux de réussite à 40%. Ceci peut sembler peu, mais chaque message qui peut être décrypté est une victoire pour les Polonais et une grande perte pour les Allemands.

Nous allons montrer comment, nous pouvons déterminer les connexions sur le tableau de connexion avec beaucoup de chance et en connaissant une partie du message. Nous supposons qu'il y ait cinq connexions sur le tableau de connexions. Imaginons que nous avons trouvé la position des rotors correcte et que nous recevons un message comme celui-ci :

WMPOC XJJPG ATVVX KFPPR JMROR SFMKG YXKLC VLRG

Quand nous tentons de décrypter le message avec la position des rotors correcte, nous obtenons le message suivant :

ZUEIA NGIFE JZEAH NKENJ EXYXI DRICH UVNHB REAQ

La raison pour laquelle ce message n'a aucun sens est que nous avons ignoré les connexions sur le tableau de connexion. Supposons que nous savons que ce message a été envoyé par un sous-marin qui a coulé deux bateaux et qui est ensuite parti en direction de Brest. Le message va probablement de contenir les mots, ZWEI, SCHIFFE, RICHTUNG et BREST. Les positions de ces mots peuvent être trouvés en cherchant des suites de lettres qui correspondent et en utilisant le fait qu'aucune lettre ne peut être cryptée en elle-même. Nous supposons que la manière dont nous avons disposé ces mots ci-dessous est correcte et nous essayons d'en tirer des conclusions.

1. POMMERENING, Klaus. *"The Enigma"*. Johannes-Gutenberg-Universität, Mainz, 1999, 40 pages.

WMPOC	XJJPG	ATVVX	KFPPR	JMROR	SFMKG	YXKLC	VLRG
ZUEIA	NGIFE	JZEAH	NKENJ	EXYXI	DRICH	UVNHB	REAQ
ZWEIS	CHIFF	E????	?????	?????	?RICH	TUNGB	REST

Nous pouvons dire que si deux lettres, qui apparaissent à la deuxième et troisième ligne à la même position, sont liés sur le tableau de connexion (ou libres de connexion, s'il s'agit de deux lettres identiques), alors la lettre à cette position à la première ligne est libre de connexion et inversémment. Quand nous regardons ces trois lignes, nous remarquons qu'il est probable que A et S soient liés, parce que cette paire apparait deux fois. La même chose est valable pour H et G. Ces deux paires sont en bleus sur le tableau ci-dessus. Ces deux dernières connexions impliquent que C, J, L et R sont libres de connexions. Nous pouvons aussi remarquer qu'il est probable que E, R et I (les paires de E, de R et de I sont en rouge) sont libres de connexions, parce que ces paires apparaissent deux fois, et ceci implique que P, O, J, F, M, V et L sont libres de connexions. Ensuite, dans les schémas suivants, nous avons 4 lignes, où la première est le message crypté, la deuxième est le message après avoir fait la permutation du tableau de connexion, la troisième est le message après avoir le système de rotors et, pour finir, la quatrième est le message après avoir traversé toute la machine, c'est-à-dire, le message décrypté. Avec les déductions que nous avons faites au sujet des connexions, nous pouvons écrire le schéma suivant.

WMPOC	XJJPG	ATVVX	KFPPR	JMROR	SFMKG	YXKLC	VLRG
?MPOC	?JJPH	S?VV?	?FPPR	JMROR	AFM?H	???LC	VLRH
??EIA	CGI??	E????	?????	?????	?RICG	???H?	REA?
ZWEIS	CHIFF	E????	?????	?????	?RICH	TUNGB	REST

Maintenant, nous pouvons utiliser la machine Enigma sans les connexions correctes pour remplir encore plus le schéma.

WMPOC	XJJPG	ATVVX	KFPPR	JMROR	SFMKG	YXKLC	VLRG
UMPOC	TJJPH	S?VV?	?FPPR	JMROR	AFMKH	???LC	VLRH
YUEIA	CGIFF	E?EA?	?KENJ	EXYXI	NRICG	???HB	REAX
ZWEIS	CHIFF	E?ES?	??E?J	E???I	?RICH	TUNGB	REST

Ceci nous permet de dire que K est libre de connexions et en plus X et T, U et W, Y et Z sont liés sur le tableau de connexions. Nous avons donc trouvé toutes les cinq connexions sur le tableau de connexions, ce qui nous permet de dire que tous les autres contacts sont libres de connexions.

WMPOC	XJJPG	ATVVX	KFPPR	JMROR	SFMKG	YXKLC	VLRG
UMPOC	TJJPH	SXVVT	KFPPR	JMROR	AFMKH	ZTKLC	VLRH
YUEIA	CGIFF	EHEAW	NKENJ	EXYXI	NRICG	XWNHB	REAX
ZWEIS	CHIFF	EGESU	NKENJ	ETZTI	NRICH	TUNGB	REST

Nous obtenons donc, pour finir, le message

ZWEI SCHIFFE GESUNKEN JETZT IN RICHTUNG BREST,

mais nous savions déjà ce que contenait ce message. Ce que nous ne savions pas, par contre, étaient les connexions faites sur le tableau de connexions. Grâce à ce message, nous avons réussi à déterminer ces connexions et comme ces connexions restent les mêmes pendant une journée, nous pouvons les exploiter pour décrypter d'autres messages.

En réalité, il est beaucoup plus difficile de déterminer les connexions, parce qu'il est rare de connaitre, comme nous l'avons supposé, autant d'éléments contenus dans le message. Les cryptologues durent, contrairement à nous, faire plusieurs tentatives pour déterminer les connexions faites sur le tableau de connexions.

4.2 La Bomba polonaise

Pour exploiter les nouvelles techniques de cryptage, les Polonais construisirent aussi un moyen électrique pour décrypter des messages, la Bomba. Cette machine qui leur permettait de décrypter les messages, était composé de 6 machines Enigma. Les indicateurs étaient encore une fois exploités, comme avec le répertoire, mais ce qui était nouveau est l'idée de créer une machine. Durant la recherche de solution, les rotors des 6 Enigmas tournaient et un courant passait à travers ses 6 Enigmas.

Chapitre 5

Les Britanniques prennent le relais

Le succès des Polonais prit fin le 15 décembre 1938 et les messages allemands demeuraient secrets. La raison était que les Allemands avaient ajoutés 2 nouveaux rotors. Avant, les Polonais avaient besoin de $3! = 6$ Bombas (la machine polonaise composée de 6 machines Enigma), mais, lorsque la machine Enigma était accompagnée de 5 rotors, il fallait $\frac{5!}{2!} = 60$ Bombas. Malheureusement, il était impossible de financer l'énorme quantité de matériel nécessaire.

Les Polonais rencontrèrent une première fois les Britanniques et les Français pour discuter de l'Enigma. Les Polonais avaient l'ordre de ne rien dévoiler de leur réussite. Comme ni les Britanniques, ni les Français avaient accompli quoi que ce soit, ils n'apprirent rien concernant les extraordinaires exploits des Polonais. Quand la relation entre la Pologne et l'Allemagne devint plus hostile et que leur accord de non-agression fut dénoncé, les Polonais choisirent de partager ce qu'ils avaient accompli. Le 24 juillet, les cryptologues polonais montrèrent à leurs homologues français et britanniques leur reconstruction de la redoutable Enigma. Un cryptoloque anglais, Knox, demanda comment était relié le clavier au premier rotor. On lui répondit simplement que c'était lié de la manière suivante : A sur A, B sur B, C sur C et ainsi de suite. Mais ce n'était pas tout ; les Polonais leur montrèrent aussi leurs Bombas qui leur permettaient de trouver, en deux heures, la clé journalière. Les Polonais avaient préparé deux répliques d'Enigma, une pour les Français, une pour les Anglais, qui furent livrés, non sans difficultés, dans chacun des pays respectifs.

Le bureau du chiffre britannique, Gouvernment Code & Cypher School, fut créé après la première guerre mondiale et avait, depuis sa création, décrypté un grand nombre de systèmes de cryptage. Le système de cryptage allemand, Enigma, demeurait, néanmoins, une énigme. Quand les cryptologues du GS&CS se rendirent compte que le système de cryptage allemand était fait par une machine, cela leur causa d'ignorer les messages allemands pendant un siècle.

Un des mathématiciens les plus brillants au GS&CS était Alan Turing, qui inventa un nouvel engin de décryptage des messages. En s'inspirant de la Bomba polonaise, il créa une Bombe de Turing. Cette machine cherchait, contrairement à la Bomba de Rejewski, à exploiter des mots qui apparaissaient de manière répétitive dans les messages allemands. Cette Bombe fut ensuite

perfectionnée par Gordon Welchmann qui eut l'idée d'ajouter un tableau diagonal qui permettait de trouver la solution correcte plus rapidement.

5.1 Utilisation d'un crib

Pour casser le code des Allemands, les Britanniques utilisaient la connaissance de certains mots qui devaient être dans le message. C'est cette connaissance et ses implications que nous appelons un crib. Pour trouver un crib, nous utilisons le fait que sur une machine Enigma, aucune lettre ne peut être cryptée en elle-même.

Dans l'exemple suivant, nous imaginons que nous avons reçu un bulletin météo et nous savons donc qu'il doit contenir le mot WETTERBERICHT. De plus, nous supposons que ce crib doit se situer entre la position 40 et 58 dans le message (voir table 5.1). Si ce mot commence à la position 40, alors les W et T coïncident aux positions 40 et 43. S'il commence à la position 41, alors les T et E aux positions 43 et 48. Si, pour terminer, le mot commence à la position 42, aucunes lettres coïncident, ce qui veut dire que la machine Enigma a pu écrire ceci. Evidement, nous pouvons continuer à vérifier, jusqu'à la position 58, mais la seule possibilité est que le mot commence à la position 42.

40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
W	R	G	T	H	I	T	Q	E	U	T	E	I	R	E	L	A	O	T
W	E	T	T	E	R	B	E	R	I	C	H	T						

40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
W	R	G	T	H	I	T	Q	E	U	T	E	I	R	E	L	A	O	T
	W	E	T	T	E	R	B	E	R	I	C	H	T					

40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
W	R	G	T	H	I	T	Q	E	U	T	E	I	R	E	L	A	O	T
		W	E	T	T	E	R	B	E	R	I	C	H	T				

TABLE 5.1 – Localisation de la position d'un mot dans un message

Maintenant que nous avons trouvé la position du mot, nous pouvons créer un graphe qui décrit le cryptage. Pour une question de simplicité, nous dirons que la 42^{e} permutation est en effet la première. Deux lettres qui sont reliées par une flèche numéroté montre que cette permutation permutent ces deux lettres. Nous pouvons voir dans la figure 5.1 un graphe de Turing qui décrit le crib trouvé.

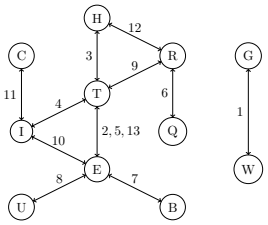

FIGURE 5.1 – Graphe de Turing

5.2 Notions mathématiques

Nous allons définir la permutation du système de rotors à la position i comme ξ_i et P la permutation du tableau de connexions. La permutation de l'Enigma quand le système de rotors est à la position i est par conséquent $\Lambda_i = P^{-1}\xi_i P$. Nous dirons que la séquence $\beta_n\beta_{n+1}...\beta_m$ est un message crypté et nous supposons que $\alpha_n\alpha_{n+1}...\alpha_m$ est le message clair, décrypté, correspondant, alors

$$\Lambda_i(\alpha_i) = \beta_i = P^{-1}\xi_i P(\alpha_i)$$

De plus, nous dirons que $\widetilde{\alpha_i} = P(\alpha_i)$ et $\widetilde{\beta_i} = P(\beta_i)$ ce qui nous permet de dire que $\widetilde{\beta_i} = \xi_i(\widetilde{\alpha_i})$ et comme $\xi_i^{-1} = \xi_i$, nous avons également $\widetilde{\alpha_i} = \xi_i(\widetilde{\beta_i})$.

Proposition 5.2.1. *Si dans un graphe de Turing, on a une composition de permutations de G*[1] *tel que* $\Lambda_{x_n}...\Lambda_{x_2}\Lambda_{x_1}(\alpha_j) = \alpha_j$*, alors* $\xi_{x_n}...\xi_{x_2}\xi_{x_1}(\widetilde{\alpha_j}) = \widetilde{\alpha_j}$ *(il s'agit de cycles dans les graphes de Turing).*

Démonstration. Cette proposition se démontre par un simple calcul.

$$\Lambda_{x_n} \cdot ... \cdot \Lambda_{x_2}\Lambda_{x_1} = P^{-1}\xi_{x_n}P \cdot ... \cdot P^{-1}\xi_{x_2}P \cdot P^{-1}\xi_{x_1}P = P^{-1}\xi_{x_n} \cdot ... \cdot \xi_{x_2} \cdot \xi_{x_1}P$$

Ce qui implique que

$$P^{-1}\xi_{x_n} \cdot ... \cdot \xi_{x_2} \cdot \xi_{x_1}P(\alpha_j) = \alpha_j \Rightarrow \xi_{x_n} \cdot ... \cdot \xi_{x_2} \cdot \xi_{x_1}(\widetilde{\alpha_j}) = \widetilde{\alpha_j}$$

□

Après avoir été correctement configuré, la Bombe peut chercher un point fixe dans une suite de permutations de G $\xi_{x_1} \cdot \xi_{x_2} \cdot ... \cdot \xi_{x_n}$. Avec notre exemple de graphe de Turing (figure 5.1), nous obtenons notamment les trois compositions de permutations G suivants

$$\xi_5\xi_2(\widetilde{E}) = \widetilde{E} \quad \xi_{12}\xi_9\xi_3(\widetilde{H}) = \widetilde{H} \quad \xi_{13}\xi_{10}\xi_4(\widetilde{T}) = \widetilde{T}$$

La probabilité qu'une composition de ξ_i contienne un point fixe est de $\frac{1}{26}$. Avec nos trois cycles, la probabilité qu'une possibilité particulière soit correcte est de $(\frac{1}{26})^3$. Les trois cycles que nous avons trouvés dans notre exemple nous permettent donc d'éliminer $1 - (\frac{1}{26})^3 = 99,99\%$ des possibilités.

5.3 La Bombe de Turing

En s'inspirant de la Bomba polonaise, Turing créa une machine qui utilisait le crib trouvé pour détérminer les configurations possibles de la machine Enigma. Lorsque la Bombe trouva une telle configuration, le cryptologue pouvait regarder la Bombe afin de prendre connaissance de la configuration. Il pouvait ensuite vérifier à l'aide d'une machine Enigma s'il s'agissait bien de la configuration du jour.

1. Il s'agit de l'ensemble de toutes les permutations que peut effectuer la machine Enigma comme dans la remarque 3.2.1 à la page 22

La machine que Turing créa en s'inspirant de la Bomba polonaise était composé de plusieurs simulateurs d'Enigma. Ces derniers ressemblaient à des machines Enigma, mais contrairement aux machines Enigma, les rotors avaient 54 contacts de chaque côté dont 26 pour le courant allant en direction du réflecteur. Les 26 autres étaient évidemment là pour le courant s'éloignant du réflecteur. Nous pouvons nous demander pourquoi il était nécessaire de doubler le nombre de contacts et par conséquent aussi le nombre de câbles dans le rotor. La raison est que Turing voulait exploiter les cycles que nous avons trouvés dans le graphe de Turing (figure 5.1) et il est donc obligatoire de savoir distinguer ce qui est entrant de ce qui est sortant. La figure 5.2 (cette figure s'inprire d'un dessin de Tony Sale [2]) montre une partie de la machine ; cette partie permettait de trouver un point fixe dans une composition de trois permutations. Dans ce cas il s'agit de la composition $\Lambda_{12}\Lambda_9\Lambda_3(H) = H$. Le système de rotors supérieur est la permutation ξ_3, le système du milieu représente la permutation ξ_9 et le système inférieur correspond à la permutation ξ_{12}. Heureusement, la Bombe de Turing pouvait faire ce genre de recherche sur plusieurs compositions de permutations en même temps, ce qui permettait de trouver la solution correcte plus rapidement.

Pour configurer la Bombe, afin qu'elle cherche un point fixe de $\xi_{12}\xi_9\xi_3$, il fallait arranger le premier système de rotors de manière arbitraire, il fallait décaler le deuxième système de 6 positions et décaler le troisième système de rotors de 3 positions par rapport au deuxième. Une fois que tous ces systèmes de rotors étaient correctement arrangés, la machine était démarrée et tous les systèmes de rotors commençaient à tourner de manière identique pour essayer toutes les positions possibles. C'est-à-dire que le premier rotor de chaque système tourne constamment, le deuxième se déplace d'une position à chaque fois que le premier a fait un tour complet et le troisième lorsque le deuxième a fait un tour entier. Le détecteur de coïncidence faisait passer un courant dans les fils du système de rotors et détectait si le courant revenait dans le fil correspondant à celui d'où il était parti. Lorsque les détecteurs de toutes les compositions de permutations repéraient une coïncidence, tous les systèmes de rotors arrêtaient de tourner. Le cryptologue pouvait alors vérifier, sur une machine Enigma, si la configuration trouvée était bien de la configuration journalière.

2. The Late Tony Sale's Codes and Ciphers Website. *"Virtual Wartime Bletchley Park by Tony Sale"*, https ://www.codesandciphers.org.uk/virtualbp/tbombe/tbombe.htm [consultée pour la dernière fois le 5 novembre 2017]. (Ce site donne des information sur les Bombes.)

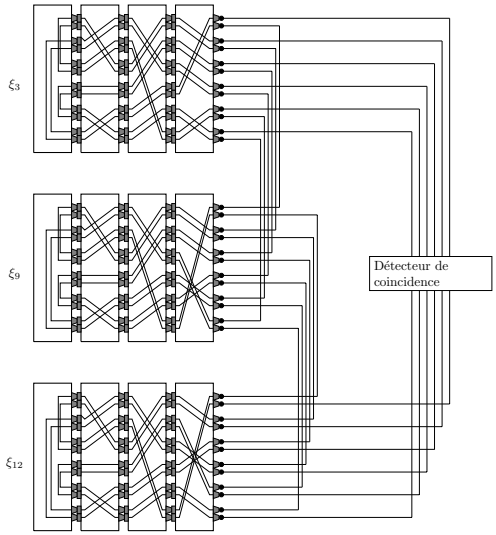

FIGURE 5.2 – Schéma d'une partie d'une Bombe de Turing

L'utilisation de cette machine comporte une difficulté majeure. Si nous reprenons l'exemple de la composition de permutations $\Lambda_{12}\Lambda_9\Lambda_3(H) = H$, nous avons supposé auparavant que seul le premier rotor se déplace entre les permutations Λ_3 et Λ_{12}. En réalité, il se peut que durant cet intervalle, le deuxième rotor se déplace (et même le troisième). Pour explorer cette possibilité, il faut, lorsque nous configurons la Bombe, déplacer le deuxième rotor sur un des simulateurs d'Enigma. Si nous pensons que le deuxième rotor s'est déplacé entre les permutations Λ_9 et Λ_{12}, alors il faut arranger le premier simulateur de manière arbitraire. Ensuite, pour le deuxième simulateur, nous décalons le premier rotor de six positions et pour le troisième simulateur, nous décalons le premier rotor de trois positions et le deuxième rotor d'une position par rapport au deuxième simulateur.

5.4 Le tableau diagonal

Plus tard, le tableau diagonal a été inventé par Gordon Welchmann. Cet ajout à la Bombe permettait d'exploiter quelques implications de la solution trouvée par la Bombe de Turing. D'un point de vue logique, il s'agit simplement de se servir du fait qu'il existe un tableau de connexion. Ceci avait été ignoré jusqu'alors. On reprend la 5.1 du graphe de Turing qui permet de dire

$$\Lambda_3(H) = T, \quad \Lambda_9(T) = R \text{ et } \quad \Lambda_{12}(R) = H.$$

On cherche donc avec la Bombe de Turing un point fixe de la composition de permutations $\Lambda_{12}\Lambda_9\Lambda_3(H) = H$. Si la machine trouve, en essayant toutes les configurations possibles, que $\xi_{12}\xi_9\xi_3(Q) = Q$, alors ça nous permet de déduire que $\widetilde{H} = Q$. De plus, on suppose que la machine trouve que

$$\xi_3(Q) = B, \quad \xi_9(B) = H \text{ et } \quad \xi_{12}(H) = Q.$$

En connaissant ceci, on peut en conclure que

$$T = \Lambda_3(H) = P\xi_3P(H) = P\xi_3(Q) = P(B).$$

De la même façon, on peut trouver que $R = P(H)$, ce qui nous montre bien que la configuration trouvée est fausse parce que

$$P(H) = R \neq Q = P(H).$$

La figure 5.3 illustre le raisonnement logique du tableau diagonal.

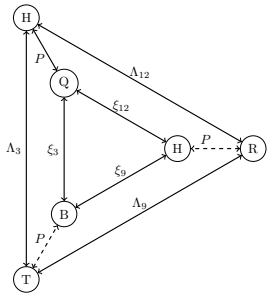

FIGURE 5.3 – Logique du fonctionnement du tableau diagonal

L'utilisation de cette logique permet même d'utiliser l'entier du graphe de Turing, plutôt que d'utiliser seulement les cycles du graphe de Turing. Maintenant, nous supposons que la machine de Turing trouve un autre point fixe A tel que

$$\xi_3(A) = B \quad \xi_9(B) = R \quad \xi_{12}(R) = A \text{ et } \quad \xi_6(H) = X$$

qui permet de dire que

$$P(H) = A \quad P(T) = B \quad P(R) = R \text{ et } \quad P(X) = Q.$$

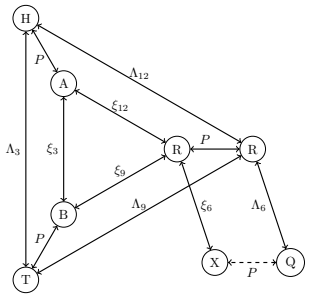

FIGURE 5.4 – Logique du fonctionnement du tableau diagonal

Pour finir, nous dirons que la machine a trouvé,

$$\begin{array}{cccc} \xi_1(D) = Z, & \xi_2(B) = Y, & \xi_3(A) = B, & \xi_4(B) = I, \\ \xi_5(B) = Y, & \xi_6(H) = X, & \xi_7(Y) = T, & \xi_8(T) = E, \\ \xi_9(B) = R, & \xi_{10}(I) = Y, & \xi_{11}(I) = C, & \xi_{12}(R) = A \\ \text{et} & \xi_{13}(B) = Y. & & \end{array}$$

ce qui nous permet de faire la figure (fig. 5.5) suivante. La permutation P contient donc les cycles $P = (BT)(LU)(YE)(QX)(AH)....$

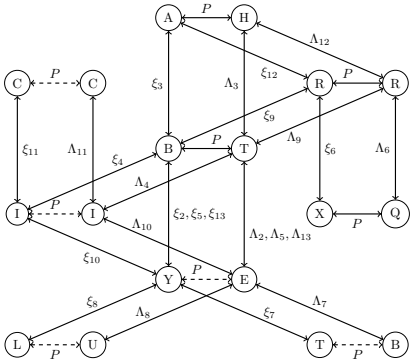

FIGURE 5.5 – Logique du fonctionnement du tableau diagonal

Comme le fait de supposer que la solution est correcte ne mène à aucune contradiction, il est probable qu'elle soit juste. De plus, on peut en déduire une grande partie de la permutation de P. En utilisant cette méthode, nous pouvons exploiter beaucoup plus d'implications du crib. De plus, cette méthode nous permet de déterminer, partiellement ou entièrement, la permutation P. Il s'agit maintenant de créer une machine qui puisse exploiter cette méthode.

5.5 Construction et fonctionnement d'une Bombe de Turing-Welchmann

Dans cette section, nous allons voir comment les cryptologues britanniques exploitaient le raisonnement fait dans la section précédente. D'abord nous construirons la Bombe de Turing d'une différente manière que dans la section 5.3. Puis, nous rajouterons le tableau diagonal à cette Bombe de Turing pour en faire une Bombe de Turing-Welchmann. Pour trouver la configuration correcte, la machine se sert d'un crib et la machine s'arrête lorsqu'elle a trouvé une configuration correspondante au crib.

Les figures des Bombes dans cette section sont inspirées de figures de Graham Ellsbury [3]. Nous allons maintenant imaginer comme dans le chapitre 3 que l'alphabet comporte seulement 6 lettres ; A, B, C, D, E et F. La Bombe de Turing, inspiré par la Bomba polonaise, a 6 câbles qui contiennent chacun 6 fils. Chacun des câbles représente une lettre et chacun des fils dans un câble représente une lettre. Sur les figures suivantes, les fils de chaque câble sont disposés dans un ordre alphabétique. C'est-à-dire que le fil le plus à gauche de chaque câble représente A, le fil à sa droite représente B et ainsi de suite. Les câbles sont aussi placés dans un ordre alphabétique, comme nous pouvons le voir sur les figures. Nous obtenons une machine que l'on peut voir dans la figure 5.7. Ensuite, nous pouvons brancher un simulateur d'Enigma (figure 5.6) entre deux câbles. Dans les figures suivantes, chaque carré orange représente un simulateur de

3. Graham Ellsbury. *"How the Bombe Worked"*, The Turing Bombe, http ://www.ellsbury.com/bombe4.htm [consultée pour la dernière fois le 5 novembre 2017]. (Sur ce cite, on trouve des informations précises sur le fonctionnement et la construction de Turing-Welchmann.)

machine Enigma dont nous avons déjà vu le fonctionnement dans la section 5.3. Dans la figure 5.8, un simulateur() a été branché entre le câble A et C.

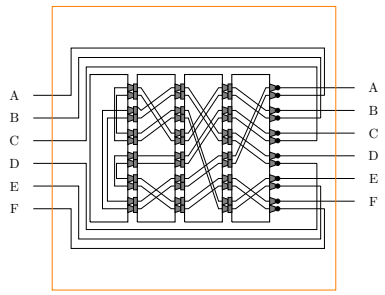

FIGURE 5.6 – Un simulateur d'Enigma

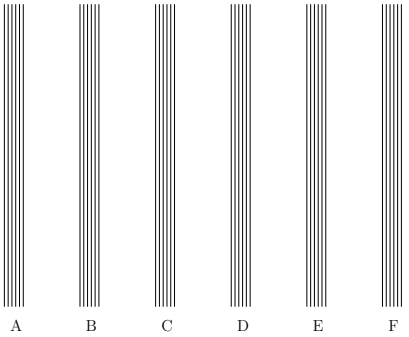

FIGURE 5.7 – Une Bombe de Turing sans simulateur

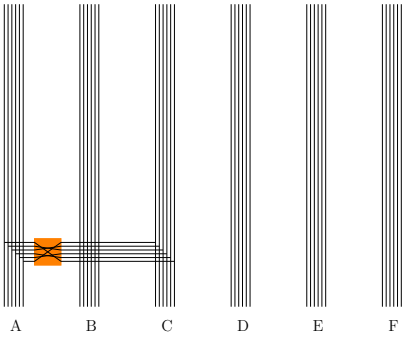

FIGURE 5.8 – Une Bombe de Turing muni d'un simulateur

Nous supposons que nous avons obtenu le graphe de Turing qui se trouve dans la figure 5.9

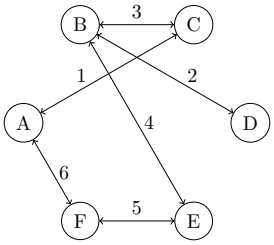

FIGURE 5.9 – Graphe de Turing

Maintenant, nous devons brancher les simulateurs d'Enigma aux câbles. Pour chaque simulateur d'Enigma, nous le branchons entre les deux câbles des lettres qu'il permute. La première permutation, par exemple, échange les lettres A et C, alors on branche les 6 fils d'un côté du simulateur aux fils correspondants de la lettre A. Les 6 fils de l'autre côté sont branchées aux

fils de la lettre C. Plus précisement, les deux fils A sortant du simulateur Enigma sont branchés aux fils A des câbles A et C de la Bombe. Les deux fils B sortant du simulateur sont branchés aux fils B des câbles A et C de la Bombe et ainsi de suite. Ensuite, après avoir branché tous les simulateurs, les rotors commencent à tourner. En même temps, on fait passer un courant dans un des fils des câbles. En ce faisant, on suppose que la lettre du fil est liée sur le tableau de connexion à la lettre du câble. Si, comme nous avons dit avant, la première permutation échange A et C et qu'en plus de cela nous supposons que B est lié à A sur le tableau de permutation, alors on fait passer un courant dans le fil B du câble A, qui entre dans le simulateur d'Enigma en tant qu'un B. Si après avoir passé dans l'Enigma, le courant sort en tant qu'un F, ceci implique qu'un courant passe dans le fil F dans le câble C. Ceci nous permet de dire que F est lié à C sur le tableau de connexion.

Dans la figure 5.10, un courant passe dans le fil A du câble A, c'est-à-dire que nous supposons que A est libre de connexion. Si nous regardons la figure, nous voyons que la Bombe montre que le fait qu'en faisant passer un courant dans le fil A du câble A, en supposant que A est libre de connexion, implique qu'un courant passe dans le fil E du câble A ; c'est-à-dire que A est lié à E sur le tableau diagonal. Ceci est évidemment contradictoire et il y a maintenant deux possibilités. Premièrement et probablement, il est possible que la position des rotors soit fausse. Deuxièmement, il se peut que la position des rotors soit juste, mais que l'hypothèse de connexion soit fausse, c'est-à-dire que A n'est pas libre de connexion. Nous supposons que nous nous trouvons dans le deuxième cas et choisissons de transmettre un courant dans le fil B. Nous remarquons que ceci est une solution possible car nous ne trouvons aucune contradiction.

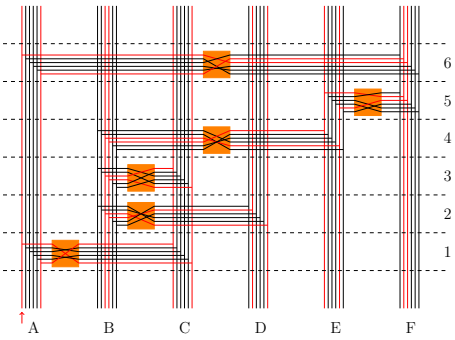

FIGURE 5.10 – Le courant passe dans le fil A du câble A.

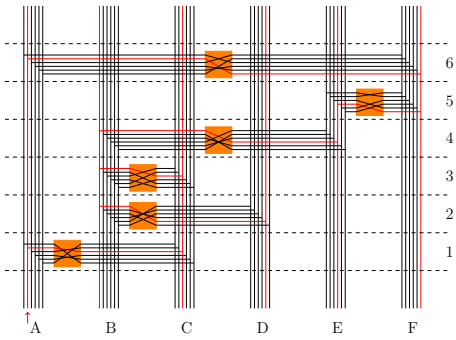

FIGURE 5.11 – Le courant passe dans le fil B du câble A.

En regardant les figures 5.10 et 5.11, nous nous rendons compte de la ressemblance avec la machine dans la section 5.3. Cette machine exploite, tout comme l'autre machine, la présence d'un point fixe.

Un mathématicien, Gordon Welchmann, eut l'idée d'ajouter encore un élément à la Bombe de Turing, qui permettait d'exploiter encore quelques implications de la position des rotors. L'idée de Gordon Welchmann est en réalité très simple. Il s'agit de se servir du fait que si A et lié à E sur le tableau de connexion, alors E est lié à A. Ceci justifie le choix de connecter le fil A du câble E au fil E du câble A, et ainsi de suite pour toutes les autres fils. Si on regarde la figure 5.12, on peut facilement comprendre pourquoi on appelle cette ajout le tableau diagonal. Nous pouvons aussi remarquer que le fil A du câble A, le fil B du câble B et ainsi de suite ne sont liés à rien sur le tableau diagonal. La raison est tout simplement qu'il faudrait le lier à lui-même.

Si on reprend la figure 5.11 et que nous ajoutons le tableau diagonal, alors nous obtenons les figures 5.12 et 5.13. Dans la figure 5.12, nous transmettons un courant dans le fil B du câble A et nous pouvons voir que la position des rotors peut être correcte et dans ce cas l'hypothèse de connexion est aussi juste. Si, au contraire, le courant est transmis dans le fil A du câble A (figure 5.13), alors le courant parcourt tous les fils, sauf ceux qui étaient parcourus par un courant dans la figure 5.12. Ces deux figures nous montrent que si la position des rotors est correcte, alors il y a deux possibilités. Si l'hypothèse de connexion est juste, alors le courant passera seulement dans un fil (en réalité, il ne circulera pas du tout). Si l'hypothèse de connexion est fausse, alors le courant passera en général tous les fils sauf ceux de l'hypothèse correcte.

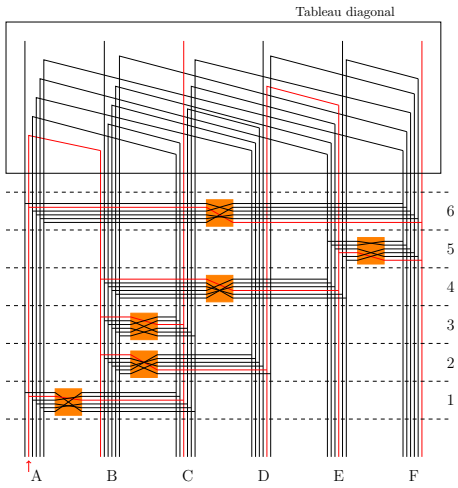

FIGURE 5.12 – Positions correctes et hypothèse juste

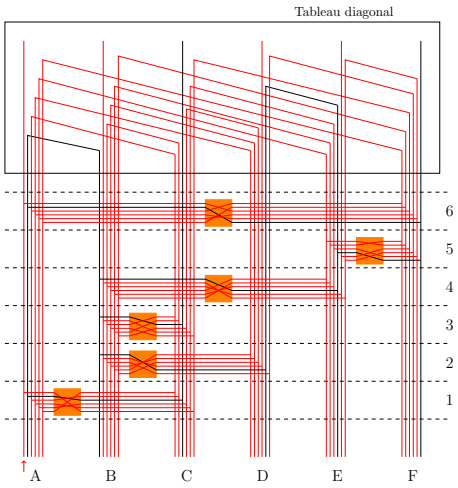

FIGURE 5.13 – Positions correctes, mais hypothèse fausse

Nous pouvons maintenant dire que si tous les fils sont parcourus par un courant, alors la position des rotors sera forcément fausse. Pour s'en convaincre, il suffit de regarder la figure 5.14 où un courant est transmis dans le fil A du câble A et en conséquence tous les fils sont parcourus par un courant. Cela veut dire que si nous transmettons un courant dans n'importe quel des autres fils du câble A (par exemple le fil D comme dans la figure 5.15), alors un courant passera aussi dans le fil A et donc dans tous les fils. Nous en concluons donc que la position des rotors est fausse, parce que quel que soit le fil à travers lequel nous faisons passer un courant, il y aura des contradictions.

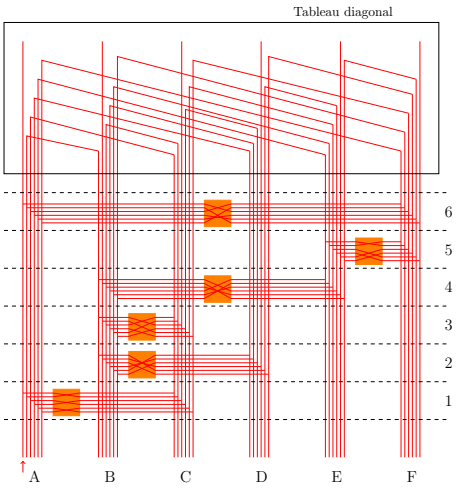

FIGURE 5.14 – Le courant passe dans le fil A du câble A losrque la position des rotors est fausse.

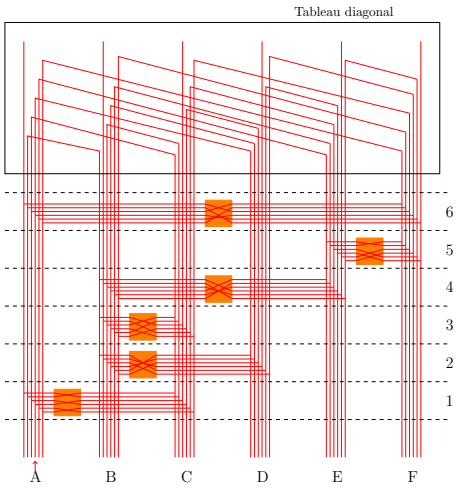

FIGURE 5.15 – Le courant passe dans le fil D du câble A losrque la position des rotors est fausse.

Les mathématiciens britanniques conçurent donc la Bombe de telle sorte que si tous les fils d'un câble étaient parcourus par un courant, alors les rotors continuaient de tourner. Du moment qu'il y avait un fil qui n'était pas parcouru par un courant, les rotors de la Bombe s'arrêtaient ceci permettait au cryptologue de voir la solution trouvée. Cependant, ceci n'était pas forcément la solution correspondant aux paramètres journaliers. Pour pouvoir le déterminer il fallait tout simplement configurer la machine Enigma en fonction de la solution trouvée et vérifier si les messages décryptés avaient du sens. Si le cryptologue découvrait que la solution trouvée n'était pas juste, il lui suffisait de redémarrer la Bombe pour qu'elle puisse continuer à chercher la solution.

La Bombe de Turing-Welchmann comporte la même difficulté que la Bombe de Turing. Il est impossible de savoir si le deuxième rotor s'est déplacé durant le cryptage du crib trouvé. S'il s'est déplacé, alors il est encore une fois impossible de déterminer à quel moment il s'est déplacé. D'un point du vue stratégique, un crib court est avantageux car il est peu probable que le deuxième rotor se soit déplacé durant cet intervalle, mais il y a aussi un désavantage. Un crib court est évidemment soumis à moins de contraintes. La machine s'arrêtera donc plus souvent sans pour autant trouver la solution. Inversement, un crib long est soumis à plus de contraintes, mais la probabilité que le deuxième rotor se soit déplacé est plus grande. La Bombe de Turing-Welchmann s'arrêtera donc moins souvent, mais il faudra essayer plus de configurations différentes de la machine, pour prendre en compte toutes les possibilités de mouvements des rotors.

Chapitre 6

Conclusion

Ce travail de maturité met en évidence le fonctionnement de la machine Enigma ainsi que ses propriétés les plus importantes. Nous avons observé qu'aucune lettre ne peut être cryptée en elle-même et qu'Enigma est son propre inverse, c'est-à-dire qu'on utilise la même machine, avec les rotors positionnés de manière identiques, pour crypter et décrypter. Nous avons vu que la machine Enigma a une quantité énorme de configurations différentes.

Quant au décryptage, nous avons remarqué que les méthodes de cryptage et de décryptage évoluent parallèlement, mais avec un certain décalage. Lorsque les Allemands s'étaient munis d'une machine de cryptage, les Britanniques, inspirés par les Polonais, inventèrent une machine qui leur permettaient de décrypter les messages allemands. Nous avons aussi pu voir comment, même si l'Enigma comporte une grande quantité de configurations différentes, beaucoup d'entre elles peuvent être ignorées. Avec la Bombe de Turing-Welchmann, toutes les possibilités d'arranger les connexions sur le tableau de connexions, ne devaient pas être essayées. En se servant de la propriété qu'aucune lettre ne peut être cryptée en elle-même, un crib pouvait être trouvé. Ce dernier permettait ensuite de trouver la position correcte de rotors.

En plus des idées incroyables des cryptologues, une des raisons de la réussite du décryptage était les choix faits par les ingénieurs allemands. Premièrement, il est envisageable de penser que si les Allemands n'avaient pas choisi d'utiliser la permutation Id comme permutation E, alors Rejewski n'aurait pas réussi à déterminer le câblage des rotors. Deuxièmement, nous nous rendons compte que si les Allemands avaient fait le choix de créer une Enigma où une lettre peut être cryptée en elle-même, il serait impensable d'essayer de déterminer les mots dans le message. Ceci aurait fait de la Bombe de Turing-Welchmann, une machine inutile.

Finalement, le décryptage massif et organisé de messages allemands permit de réduire considérablement la durée de la guerre et sauva un grand nombre de vies, à la fois alliées et allemandes. Malheureusement, tous ces brillants mathématiciens, qui ont permis ce décryptage, n'ont été reconnus que très tardivement pour leurs exploits. Marian Rejewski vécut toute sa vie en Pologne et ne publia son premier article sur Enigma qu'en 1980. Alan Turing fut condamné pour son homosexualité en 1952 et se suicida le 7 juin 1954, en mangeant une pomme empoisonné, après avoir été forcé de suivre un traitement hormonal.

Bibliographie

[1] KAHN, David. *The race to break the german u-boat codes, 1939 - 1943.* Frontline Books, 1998.

[2] SINGH, Simon. *A l'attaque d'Enigma in Histoire des codes secrets.* Londres : Fourth Estate Limited, 1999.

[3] LEHNING, Hervé. *Les rouages d'Enigma et Les mots probables de Turing* in *Cryptographie & codes secrets, L'art de cacher*, Bibliothèque Tangente. Paris : Editions POLE, 2006 (augmentée 2013).

[4] REJEWSKI, Marian. *"An Application of the Theory of Permutations in Breaking the Enigma Cipher"* in Applicationes Mathematicae 16, n°4.

[5] POMMERENING, Klaus. *"The Enigma"*. Johannes-Gutenberg-Universität, Mainz, 1999, 40 pages.

[6] POMMERENING, Klaus. *"Permutations and Rejewski's Theorem"*. Johannes-Gutenberg-Universität, Mainz, 2008, 10 pages.

[7] KUHL, Alex. *"Rejewski's Catalog"* in Cryptologia 31 : 326-331, 2007.

[8] GUILLOT Philippe. *"Des mathématiciens polonais au coeur du décryptement de la machine ENIGMA, 1932-1942"*, 34 pages.

[9] FAINT, Stephanie. *"The Enigma History and Mathematics"*, Waterloo, Ontario, Canada, 1999, 75 pages.

[10] ROSE Stuart, *Heroes of War Poland : Cracking Enigma*, 2014.

[11] Crypto Museum. *"Bombe"*, http ://www.cryptomuseum.com/crypto/bombe/ [consultée pour la dernière fois le 5 novembre 2017]. (Ce site donne des informations sur le fonctionnement et l'utilisation des Bombes.)

[12] Crypto Museum. *"Enigma Wiring"*, http ://www.cryptomuseum.com/crypto/enigma/wiring.htm [consultée pour la dernière fois le 5 novembre 2017]. (Ce site donne des informations précises sur les rotors et les réflecteurs.)

[13] Graham Ellsbury. *"How the Bombe was Plugged Up"*, The Turing Bombe, http ://www.ellsbury.com/bombe3.htm [consultée pour la dernière fois le 5 novembre 2017]. (Sur ce cite, on trouve des informations précises sur l'utilisation et la construction de la Bombe de Turing-Welchmann.)

[14] Graham Ellsbury. *"How the Bombe Worked"*, The Turing Bombe, http ://www.ellsbury.com/bombe4.htm [consultée pour la dernière fois le 5 novembre 2017]. (Sur ce cite, on trouve des informations précises sur le fonctionnement et la construction de la Bombe de Turing-Welchmann.)

[15] The Late Tony Sale's Codes and Ciphers Website. *"Virtual Wartime Bletchley Park by Tony Sale"*, https ://www.codesandciphers.org.uk/virtualbp/tbombe/tbombe.htm [consultée pour la dernière fois le 5 novembre 2017]. (Ce site donne des information sur les Bombes.)

[16] Vestergaards Matematik Sider, *"The German cipher machine Enigma"*, http ://www.matematiksider.dk/enigma_eng.html [consultée pour la dernière fois le 5 novembre 2017]. (Sur ce cite, on trouve des informations générales sur la machine Enigma, son fonctionnement, le décryptage et le Bombes.)

Remerciements

J'aimerais premièrement remercier chaleureusement, mon mentor, Luc Dessauges, sans qui ce travail n'aurait pas pu être réalisé. Je remercie également Joël Wagnières, Déborah Baumgartner, Jean-Marie Droz et Taras Pavliv pour avoir lu et commenté certaines parties de ce travail de maturité.

Annexe A

Marche à suivre du simulateur d'Enigma

A.1 Démarrage de la simulation

Pour démarrer le simulateur de la machine Enigma, il suffit de lancer le programme "Main.py" en Python 3 (3.5.3).

A.2 Utilisation de la simulation

Lorsque le programme a été démarré, vous pouvez configurer la machine en ouvrant la fenêtre "Paramètres de cryptage" en appuyant sur "Enigma → Paramètres de cryptage" sur la barre de menu. Sur la première ligne, il faut choisir le type de rotor à mettre à chaque position. Il a 5 rotors différents et pour en choisir un, il suffit d'écrire ce nombre dans l'espace dédié. Ensuite, il faut écrire le ringstellung et la position initiale de chaque rotor en écrivant la lettre correspondante. Pour finir, il faut préciser les connexions sur le tableau de connexions (pour des raisons évidentes, on ne doit pas taper la même lettre plus d'une fois) et appuyer sur "OK". Si on ne veut plus changer les configurations durant la session, on peut fermer la fenêtre, sinon, on peut la garder ouverte. Pour que la machine apparaisse sur l'écran, il faut cliquer sur la fenêtre "Simulateur d'Enigma" et ensuite taper une fois sur ENTER.

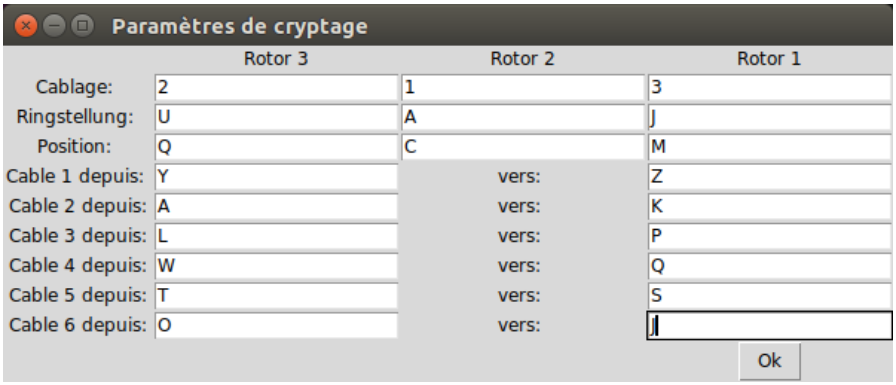

FIGURE A.1 – Une fenêtre “Paramètres de cryptage” complétée correspondant à l’exemple du 6 octobre à la page 11

On peut maintenant commencer à écrire le message. Il est important de noter que pour écrire, il faut se trouver dans la fenêtre principale “Simulateur d’Enigma” (avoir cliqué sur cette fenêtre). On voit alors sur l’écran comment fonctionne la machine et la lettre crypté obtenue lorsqu’on appuie sur une lettre du clavier. Les suites de lettres sur les côtés des rotors symbolisent la bande de positions. La lettre qui est entouré d’un carré rouge en haut de chaque rotor est sa position, c’est-à-dire la lettre qu’on verrait à travers le trou de capot sur une véritable machine Enigma.

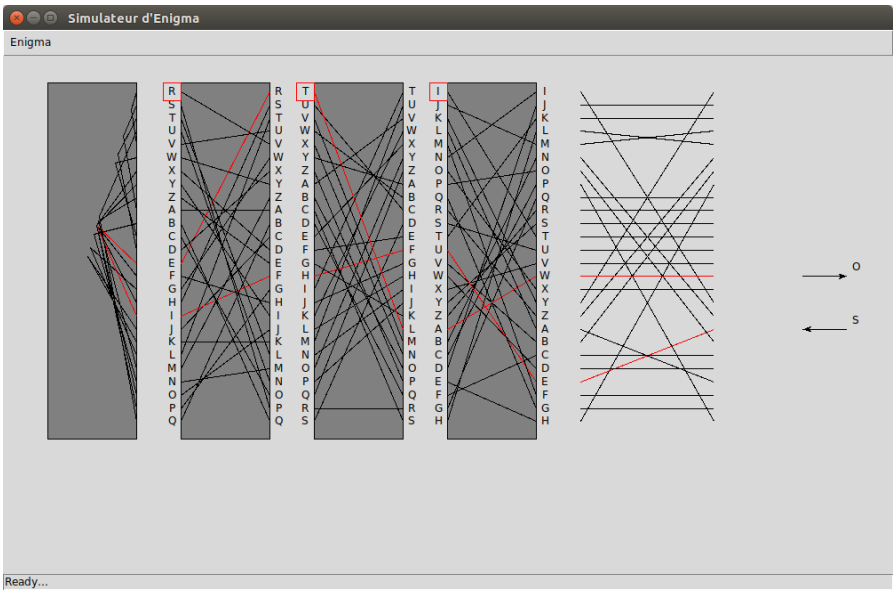

FIGURE A.2 – Une fenêtre “Simulateur d’Enigma”

Si on veut voir l’entier du message écrit et crypté, il faut ouvrir la fenêtre “Message crypté” en appuyant sur “Enigma → Voir le message crypté” sur la barre de menu. Dans cette fenêtre, on voit, en haut, le message clair et, en bas, on voit le message crypté. Le message crypté est

organisé en bloc de 5 lettres comme un véritable message Enigma. Dans le message clair, on peut écrire des espaces, afin d'organiser ce message comme on souhaite. Ces espaces ne seront pas pris en compte par la machine Enigma et n'apparaîtra pas dans le message crypté.

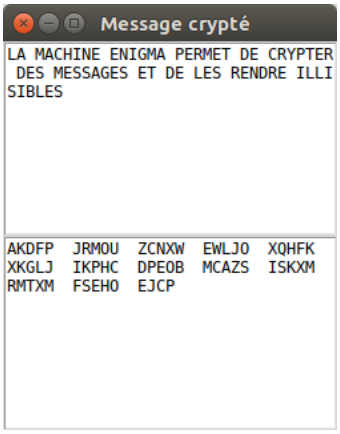

FIGURE A.3 – Une fenêtre "Message crypté"