Si seulement Enigma tournait moins vite, ou cryptanalyse d'Enigma avec un rotor faible

Nicolas T. Courtois

On a tous entendu parler de l'histoire du cassage de l'Enigma militaire doté d'un tableau de fiches (*stecker*). C'est le sujet principal du formidable livre « X, Y & Z », dans sa version anglaise, écrit par Dermot Turing. Ce livre est également paru en France en 2019 [12]. Monsieur Turing lui-même s'exprime en français à chaque fois que l'occasion se présente, il a tissé ces dernières années des liens étroits avec la France et l'ARCSI. Il est venu nous voir aux Archives Nationales, il nous a reçus à Bletchley Park et il a effectué des recherches très pointues dans les archives du Service Historique de la Défense à Vincennes.

Sir Dermot Turing et Jean-Louis Desvignes lors de l'exposition « Le secret de l'État » (Archives nationales - 2015-2016)

Il raconte dans ce livre cet exemple exceptionnel de collaboration des spécialistes et des services de renseignement de 3 pays, désignés sous les pseudonymes XYZ, qui a commencé avant l'arrivée de Hitler au pouvoir. On connaît son rôle légendaire [2,4], dans la défaite de l'Allemagne Nazie.

Il est essentiel de ne pas confondre l'Enigma commerciale sans le tableau de fiches, de l'Enigma militaire, infiniment plus complexe. Cette Enigma avec le *stecker* est entrée en service en 1930. Les Polonais ont été les premiers à décrypter les messages

codés avec Enigma, très tôt et dès 1932, avec l'aide inestimable des services de renseignement français et d'un certain Gustave Bertrand. Quand la guerre éclate en 1939, les cryptologues polonais se retrouvent à Gretz-Armainvilliers, sous l'œil de Bertrand, qui sera promu général bien plus tard. Ensuite on sait comment cet effort allié de cryptanalyse a évolué, jusqu'à devenir une véritable industrie à Bletchley Park, avec 211 « bombes » de Turing-Welchman qui ont permis de décrypter, selon les sources, entre 2,5 et 5 millions de messages de l'armée allemande. Il existe des raisons profondes pour lesquelles les Polonais et eux seuls, ont eu tant de succès avant le début de la guerre. En fait deux ruptures technologiques majeures interviennent : un saut brusque dans la complexité du chiffrement introduit par le *stecker*, accompagné d'une rupture dans les techniques de cryptanalyse qui vont s'enrichir et devenir plus mathématiques.

Avant d'une Enigma montrant le tableau de fiches(*stecker*)

Alfred Dillwyn "Dilly" Knox

Dans les années 1930 en Angleterre, Alfred Dillwin Knox, connu en tant que *Dilly*, a élaboré (en collaboration avec Hugh Foss) la célèbre attaque connue sous le nom de l'attaque des Bâtons (ou *Rods*). Ce nom en français et de nombreuses sources semblent indiquer que cette attaque a également été connue en France, ceci bien avant le début de la deuxième guerre mondiale. Mavis Batey [1] confirme que « tout le monde » est arrivé à cryptanalyser l'Enigma plus ou moins de la même façon. Cette technique a aussi probablement été connue aux États-Unis bien que Batey semble en douter [1]. On sait bien que Friedman, et toute la crypto mondiale ont suivi de près l'Enigma commerciale dès le début des années 1920. Nous avons très peu d'informations sur le travail de Dilly Knox et la cryptanalyse d'avant la guerre. Nous savons toutefois que Foss a été le mentor de Knox dans son travail sur l'Enigma commerciale, sans *stecker*. Ensuite

l'histoire se répète : Knox a été le mentor de Turing pour le cassage de l'Enigma avec *stecker*, et ceci au moins 6 mois avant que Turing n'arrête son travail universitaire et arrive à Bletchley Park (voir page 107 dans [1]), soit bien plus tard, début septembre 1939. Turing arrive en effet très peu de temps avant que la commande de la première bombe soit passée. Cela donne à penser que celui-ci a travaillé sur ce problème pendant au moins 6 mois avant son arrivée à Bletchley Park.

Batey explique que pendant que les Polonais décryptaient l'Enigma, durant les années 1932-1937, Bletchley Park n'avait pas encore accès aux orignaux des messages allemands interceptés, ce qui arrive nettement plus tard vers 1937. En janvier 1940, date de la visite de Turing en France, de grands doutes existaient en Angleterre sur certaines questions clés, y compris sur les spécifications exactes des versions d'Enigma vraiment opérationnelles, après tous les changements de procédure de 1938 et 1939. Il n'était pas assuré non plus, que les méthodes polonaises marchaient encore. Il faut savoir que Knox a brandi sa menace de démission, auprès de sa hiérarchie, par écrit et dans une lettre dactylographiée, pour que le voyage en France de son poulain, Alan Turing, puisse enfin être autorisé. Le but de ce voyage fut un véritable échange entre services : les Britanniques fournirent un jeu complet des feuilles perforées de Zygalski, fabriqué en Angleterre par Jeffreys et sous supervision de Knox. De son côté, Rejewski fit, en présence de Turing, une démonstration de décryptement, du premier message allemand décrypté en temps de guerre, le 17 janvier 1940. C'est seulement quelques jours après le retour de Turing en Angleterre, que Bletchley Park commença à décrypter les messages allemands.

Si on revient à l'avant 1937, il est bien connu que Knox a bloqué sur des questions pratiques, tel que QWERTZU, la permutation d'entrée. Sur le plan théorique, c'est différent. Avant 1937, et d'après Denniston et Batey [1], Knox aurait travaillé sur ces méthodes avec un certain succès. Batey suggère que Knox était capable d'y arriver, et que pour Knox la complication introduite par le tableau de fiches n'aurait été qu'une permutation de plus. Batey s'oppose à nos versions plus récentes et aux affirmations de Denniston de l'époque, selon lesquelles Turing et Welchman sont allés beaucoup plus loin. Ici il faut souligner le rôle joué par les mathématiques et les mathématiciens. Nous savons que les Polonais pendant des années ont caché leurs exploits, et donc que Bertrand a dû solliciter l'aide de Dilly, et qu'il a fourni à celui-ci en 1938, des exemples clair/chiffré authentiques datant de 1932 pour travailler. Il faut souligner toutefois que dans ces exemples le *stecker* était tout simplement déjà connu et fourni par Bertrand [1]. Il faut donc penser que Dilly, n'a jamais eu accès ni eu la possibilité, de travailler sur de véritables challenges plus récents. Dilly a été bloqué sur la question de la permutation d'entrée présumée secrète, le célèbre « QWERTZU ». Or cette permutation aurait pu être aléatoire, avec en théorie 26 ! possibilités, l'équivalent de 88 bits d'entropie, ne laissant donc aucun espoir de la deviner. Or celle-ci s'avéra être « ABCDE », ce que les Polonais ont caché aux autres Alliés pendant des années, et l'ont finalement révélé à Pyry (en banlieue de Varsovie) en 1939. Batey écrit que Dilly et Denniston ont estimé que les Allemands n'étaient sûrement pas assez stupides pour faire un choix aussi facile à deviner [1]. Dans cet article nous allons montrer un autre grave problème, aussi incroyable que vrai, remontant également aux années 1920, et qui n'a pas encore été mis en évidence par des chercheurs.

Nous avons ici une différence d'opinions classique entre deux générations de casseurs de codes. L'ancienne génération insiste sur le côté linguistique, et pense pouvoir y arriver. Puis vient la nouvelle génération, avec les Polonais, puis Turing et Welchman, avec les mathématiques. Un autre élément majeur émerge seulement avec le temps : une augmentation considérable de l'effort de calcul nécessaire rend la cryptanalyse impossible, non seulement pour l'ancienne génération, mais pour quiconque ne dispose pas d'une puissance de calcul suffisante. Il est maintenant clair que Knox et plus tard Turing lui-même, ont sous-estimé la difficulté posée par le *stecker* et l'Enigma militaire, puis navale avec 4 rotors. On peut facilement s'en convaincre si on réfléchit au fait qu'examiner toutes les positions possibles de 3 rotors d'Enigma dans une Bombe (donc plus tard, par exemple en 1941), revient à faire une recherche systématique ou par force brute, avec des rotors mécaniques à parties amovibles, sur un espace de 14 bits. Ceci aurait déjà coûté une fortune : 211 bombes, au prix unitaire d'un demi-avion de combat. Alors peut-on espérer explorer un espace d'environ 36 bits en 1937 quand Knox s'avoue en difficulté, puis d'environ 47 bits pour le *stecker* avec 10 paires, tel qu'il a été mandaté en janvier 1939 ? Faut-il multiplier le budget déjà gargantuesque de Bletchley Park par un facteur de plusieurs milliards ? Ou fallait-il inventer et construire un autre Colossus pour résoudre ce problème, avec la technologie des tubes cathodiques, plus rapide ?

Non, car le but d'une attaque est bien entendu d'éliminer le *stecker*, de trouver une façon intelligente de travailler en contournant cette difficulté majeure. Batey explique ici que Knox aurait aussi indépendamment pensé à travailler sur des lettres qui se répètent à 3 lettres d'intervalle, connues en tant que « femelles ». Knox aurait comparé ces notes avec des cryptologues Polonais à Pyry, en 1939. Il semble que Knox ait imaginé une solution à lui, de type catalogue/statistique, qui aurait été moins performante que celle de Zygalski [1]. Il est intéressant de voir, que les sources anglaises attribuent le concept de « femelles » aux Polonais, alors que les Polonais l'attribuent… aux Anglais, sans doute ayant échangé avec Knox en personne sur ce sujet. Il faut aussi ajouter que la méthode d'attaque de Zygalski a été la principale technique, et quasiment la seule réellement opérationnelle pour décrypter quoi que ce soit, avant l'invasion de la France en mai 1940. Ceci aussi bien pour les Polonais en France, que pour les Anglais à la même période. Les méthodes de Herivel et de Sillies ont été celles de la période d'après, fort difficile, de la deuxième moitié de 1940.

Toutes les méthodes connues de cassage de l'Enigma militaire, différent principalement sur cette question, la plus essentielle : comment peut-on éviter ou éliminer le *stecker* d'une façon ou d'une autre ? Par exemple, la *bomba* polonaise (avec 6 machines Enigma), est devenue obsolète quelques mois après son invention, quand les Allemands sont passés à 10 paires de fiches en janvier 1939. En revanche la méthode de Zygalski basée sur des points fixes, une propriété qui ne change pas du tout avec une permutation de plus, celle du *stecker*, a fonctionné parfaitement jusqu'en mai 1940 et parfois après cette date. Un autre exemple est la bombe version Turing, qui exploite des cycles courts entre les lettres du clair et du chiffré dans un graphe que l'on appelle le menu. La bombe de Turing-Welchman va ensuite faire mieux, en exploitant le fait que le *stecker* est une permutation réciproque, les lettres étant connectées par paires. Ainsi on pourra cryptanalyser Enigma avec un clair probable nettement plus court, avec moins de cycles dans le menu, et parfois en absence totale de cycle.

Il faut donc croire que Dilly a eu en effet quelques idées de plus, peut être perdues à tout jamais, peut-être communiquées à Turing. En fait la lecture de Batey confirme notre idée que Dilly, a certainement vu, dès son voyage en Pologne en 1939, que tôt ou tard, les méthodes polonaises cesseraient de fonctionner. Ceci quand les Allemands changeraient les procédures, ce qui est arrivé d'après tous les récits, quelques jours avant l'invasion de la France. La date plus précise du 2 mai est donnée par Paillole [9]. Il semble donc que dès son voyage en Pologne en 1939, Knox a demandé à Turing de travailler précisément sur cette question, ce qui aurait été un retour des attaques à clair connu, chères au casseur de codes et linguiste hors pair qu'était Dilly. C'était une question stratégique de tout premier plan, et Dilly était bien placé pour le voir très clairement. L'ironie de l'histoire veut que ce retour de la cryptanalyse linguistique faisant appel aux clairs probables (ou *cribs* en anglais), et leur rôle essentiel dans le succès des attaques, avec une activité importante dans la *crib Room* de la Hutte 8 et dans le bloc C, se produit et revient en force bien plus tard, quand Knox commence à s'affaiblir. Il meurt d'un cancer en février 1943. Dans tous les cas il faut rejeter l'idée de Batey [1] selon laquelle pour Knox l'Enigma militaire aurait été cassable, car après tout il ne s'agissait que d'une permutation de plus. Une complication plutôt énorme.

On s'est souvent posé la question, si Dilly Knox n'a pas été le véritable inventeur de certaines idées aujourd'hui attribuées à Turing. Dans son ouvrage connu en tant que Prof's book, Turing utilise clairement des méthodes et une terminologie plus ancienne [10]. Il faut se rappeler que, bien que dépassée depuis 1932 pour l'Enigma militaire, la méthode des bâtons de Knox n'était clairement pas connue de Rejewski en 1939. Il y a sans doute des chapitres entiers sur le décryptement d'Enigma, et ceci même après 1940, quand ces questions ont continué à être très importantes. Il s'agit par exemple de l'Enigma Suisse, sans *stecker*, cassée par les Polonais en France, ce qui a été communiqué aux Suisses en 1941. De plus, un sujet encore délicat et obscur à ce jour, concerne la cryptanalyse de l'Enigma de l'Abwehr. Celle-ci était sans *stecker*, mais avec un mouvement de rotors plus complexe. Toutefois dans le dernier guide bleu de Dermot Turing vendu à Bletchley Park [11], écrit en collaboration avec David Kenyon (qui a été notre hôte pendant la visite de l'ARCSI), on apprend que l'Enigma de l'Abwehr n'a pas été très solide. La preuve en est, que seulement 2 bombes sur 211 lui ont été dédiées en 1943, dans une section à part qui portait le nom de « signaux illicites » de Knox, alors que Knox n'était plus de ce monde. Un début d'explication pourrait être, que si deux rotors tournent de façon simultanée, ce n'est pas tellement plus complexe que si un seul rotor tourne, car la permutation qui résulte de leur composition sera fixe.

On arrive ici à une considération essentielle que le mouvement est relatif, que l'on retrouve un peu partout en cryptanalyse et dans son histoire. Par exemple il est connu que dans le Lorenz SZ-42, le système de chiffrement de Hitler et des généraux allemands, les 5 roues Psi tournent toutes les 5 à la fois, ou pas du tout, les autres possibilités arrivant nettement moins souvent. De même dans la machine à chiffrer Est-allemande T-310, il y a une cascade d'additions avec un effet similaire.

Ô temps suspend ton vol, si seulement une machine à chiffrer quelconque pouvait tourner moins vite, un peu comme un « *one time pad* », quand il est utilisé deux fois de suite. On aurait alors certainement trouvé un moyen pour la casser. Par exemple

avec des corrélations renforcées par la répétition, ou une élimination de certaines variables.

Il est donc facile de se convaincre que tourner moins vite, implique de s'exposer à une cryptanalyse beaucoup plus efficace. À tel point que l'on pourrait envisager une attaque à clair inconnu, exploit jamais réalisé pendant la deuxième guerre mondiale et connu dans le cas de l'Enigma, seulement dans les articles très récents [8]. Ces nouvelles attaques sont des attaques probabilistes basées sur le fait que 6 lettres dans le *stecker* sont toujours transformées en elles-mêmes, ce qui peut laisser transpirer certaines propriétés statistiques du clair en langue Allemande. Cette question aurait été essentielle pour les anciens tel Knox, avant que le travail soit divisé, fractionné, organisé à la perfection, entre différentes tâches et différentes personnes. La réponse se trouve dans les articles récents : oui on peut [8] mais ceci nécessite une certaine puissance de calcul et un message suffisamment long. Par conséquent, certains messages Enigma courts originaux, même ceux datant de la deuxième guerre mondiale, n'ont toujours pas été décryptés [8].

Dans cet article nous allons y apporter une réponse nouvelle et originale, sous un angle nouveau. Considérons le cas où l'un des rotors de l'Enigma est faible. Cela peut paraître impossible ou incroyable, mais c'est pourtant vrai pour l'un des rotors datant du tout début de l'Enigma militaire. Le rotor en question, contient une sorte de backdoor installée par inadvertance ou pour d'autres raisons. Il n'a pas été généré de façon à obtenir une permutation aléatoire, mais il est très particulier, et en fait, il va s'avérer très faible. En apparence ce rotor faible va tourner rapidement. En revanche, il ne changera pas de sa position de toute la journée, et de nombreux messages chiffrés avec le même ordre de rotors vont être transmis. Nous allons voir qu'avec un rotor faible, on peut casser l'Enigma plus facilement. L'attaque est suffisamment simple pour être contenue dans cet article. Cette attaque est nouvelle et n'a jamais été publiée. Elle est pourtant pratique et réaliste. Elle nécessite une très faible puissance de calcul, elle aurait donc pu être inventée pendant la guerre.

On a su par la suite, avec la compromission de l'unité de cassage de codes allemande de Rommel en Afrique du Nord, que les Allemands aussi, étaient capables de lire les codes des Alliés. On a appris aussi lors de la dernière conférence CCH de la NSA en 2019 aux États-Unis, que les Allemands ont su décrypter quasiment tous les messages du gouvernement polonais exilé à Londres. Tout ceci est documenté dans les archives de Berlin, ouvert à ceux, tellement peu nombreux, qui s'intéressent à la véritable histoire de la crypto, basée sur les archives. On apprend tout ceci avec pas mal de détails de Rozwadowski, un chercheur Américain, économiste de profession. Cet auteur a avoué, pendant son exposé, être le fils d'un autre Rozwadowski, un polonais issu d'une famille célèbre depuis fort longtemps dans le domaine militaire, qui a autrefois dirigé un réseau de renseignements de 1 700 personnes, sur le territoire français occupé [7]. Le travail minutieux de Medrala cité ici, qui est extrêmement bien documenté dans les archives militaires françaises, apporte aussi quelques éclairages sur l'Enigma. En fait les cryptologues polonais ne faisaient pas du tout confiance à Bertrand, et ont dissimulé énormément de renseignements aux Français. Ces décryptements ont été transmis [sûrement] aux Anglais à Bletchley Park, et [probablement] aussi au gouvernement polonais en exil. Il faut alors se demander si De Gaulle avait une capacité de communiquer avec ses

collaborateurs ou autres Alliés de façon sûre. Leo Marks raconte en effet dans son livre avoir pu casser le code secret de correspondance de De Gaulle à Londres [6]. Il dit aussi très clairement, que les Polonais ont (bizarrement) été le SEUL gouvernement étranger exilé à Londres, autorisé à utiliser sa propre cryptographie. Ceci avec les résultats catastrophiques mis en évidence en 2019.

Il n'y a donc pas de doute que les Allemands n'ont pas été en retard dans le domaine de la cryptographie, ni en 1929, ni en 1939. Au contraire, en 1929 ils arrêtent d'utiliser une Enigma sans *stecker*, ce que les Suisses feront véritablement vers 1946 avec NEMA. C'est donc l'Allemagne qui a été le pays le plus avancé. Par ailleurs dans les sources Internet [cryptomuseum.com] on apprend qu'en plus des Polonais (qui ont eu le mérite d'avertir la Suisse en 1941 et de ne rien demander en retour, ce que Bertrand a regretté), les Américains, et pire encore, les Allemands, ont également été capables de décrypter les communications de la Suisse, à tout moment semble-t-il entre 1939 et 1945. On peut donc penser que l'Allemagne pouvait prétendre avoir environ 15 années d'avance en cryptographie, comparé à tous les autres pays du monde. Ceci si on pense juste à la complexité énorme apportée par le tableau de fiches. Il faut aussi savoir que dans le Typex Britannique il n'y avait pas de *stecker* non plus, celui-ci a été ajouté seulement pour pouvoir émuler l'Enigma.

On peut aussi penser que c'était une question d'ambition. Un pays qui veut conquérir le monde doit s'en donner les moyens, ou être très prudent au point de tomber dans la démesure. Par exemple les machines à chiffrer T-310 de fabrication Est-Allemande des années 1980, ont une complexité et un coût 10 000 fois plus grand, que des systèmes de chiffrement commerciaux actuels tels que le triple DES ou l'AES [3]. Une supériorité matérielle et un excès d'ambition incroyables pour mieux sécuriser les communications militaires ! Ce degré de paranoïa est peut-être lié au fait que des décennies plus tôt, l'Allemagne a fait preuve d'une naïveté sans limite, concernant la sécurité, supposée sans faille, de l'Enigma militaire. Ceci à tel point que les 3 premiers rotors de l'Enigma datant de 1929, étaient encore en service en 1945. Puis encore, au moins jusqu'en 1956, dans certains cas en Allemagne de l'Est. Ce fait est important dans cet article car il s'avère que le rotor III de 1929, cache quelques mauvaises surprises.

Pour s'en convaincre nous allons montrer juste quelques lignes du tableau qui montre la permutation originale de ce rotor, et la même permutation obtenue quand on déplace ce rotor d'un cran, et puis de deux, dans la machine Enigma.

i		$C^{-i} \circ R_{III} \circ C^{i}$
		ABCDEFGHIJKLMNOPQRSTUVWXYZ
0		BDFHJLCPRTXVZNYEIWGAKMUSQO
1		CEGIKBOQSWUYMXDHVFZJLTRPNA
2		DFHJANPRVTXLWCGUEYIKSQOMZB

Il y a ici comme un problème grave, qui va au-delà de 3 premières lignes du tableau.

Le problème concerne en fait, TOUTES les 26 positions possibles de ce rotor. Un ordre étrange et fort, qui n'est certainement pas accidentel, règne dans le coin en haut à gauche de ce tableau, qui va ensuite se déplacer dans le coin en bas à droite. Nous avons récemment rencontré au cours d'une conférence HistoCrypt à Smolenice en Slovaquie, des descendants de la famille d'entrepreneurs qui ont fabriqué des machines Enigma pour l'armée Allemande. En Pologne, nous avons rencontré un mathématicien très connu dans le pays, dont le grand-père a travaillé chez AVA, à la fabrication même des clones de la machine Enigma, fabriqués en Pologne à l'époque, exclusivement pour les besoins des services de renseignement polonais, dont un exemplaire a été donné à Bertrand, et un autre a été transporté à Londres dans le plus grand secret par Sacha Guitry en personne.

Ici nous constatons un fait étrange, il est possible que ce rotor ait été généré par un humain qui s'amusait à écrire BCDEFGHIJKL, il est bien connu que les hommes ne sont pas de bons générateurs d'aléa ! La probabilité pour les 20 lettres en rouge dans les 2 premières lignes qu'on soit toujours du côté gauche du tableau, est déjà de 1 chance sur un million. On n'est pas de loin de pouvoir gagner 1 million à la loterie. Il faut toutefois rejeter l'hypothèse d'un simple défaut concernant deux versions du même rotor. En fait, il y a là une structure encore plus forte, loin d'être apparente, si on regarde un tableau complet avec 26 lignes, pour toutes les positions possibles du rotor III. On remarque alors qu'il y a une sorte d'alternance plus approximative, mais qui reste forte. Certaines de nos lettres en rouge vont migrer de droite vers la gauche et vice versa, mais elles ont globalement tendance à aller tout le temps d'un côté à l'autre, un mouvement systématique et périodique. Nous avons devant nous, probablement, un cadeau posthume d'un cryptologue allemand anonyme, qui a peut-être cherché à nuire à la sécurité du chiffrement allemand. Ceci est assez étonnant, car ce rotor était déjà fabriqué avant l'arrivée de Hitler au pouvoir. Il est possible que les concepteurs aient pris en compte le traité de Versailles, qui imposait à l'Allemagne de ne pas développer de technologie militaire moderne. Ou que les concepteurs ont été payés par une puissance étrangère, une de celles qui auraient auparavant acheté les machines Enigma commerciales, pour compromettre la cryptographie allemande de l'intérieur. Probablement un employé a eu la possibilité de faire ce qu'il voulait, et il n'y avait pas de contrôle de qualité sur la qualité cryptographique de connexions dans ces rotors. Laissons ces questions de côté, car les faits sont tellement anciens qu'on ne connaîtra probablement jamais la réponse.

Il se trouve donc que notre rotor produit certaines lettres avec un biais considérable qui ne dépend que d'un bit de sa position i modulo 26. Et ce n'est pas seulement une affaire de **ABC**. Dans les 26 lettres de l'alphabet il n'y en a en fait pas moins de 16 qui ont tendance à fournir de l'information sur la valeur de **i** modulo 2. Ces lettres sont : **B**, **I**, **K**, **M**, **O**, **V**, **X**, **Z**, **A**, **C**, **J**, **L**, **N**, **P**, **W**, **Y**. Par exemple la lettre **B** aura la tendance à être beaucoup plus souvent dans la moitié droite pour **i** pair, et le plus souvent dans la moitié gauche pour **i** impair. Dans la table ci-dessous nous allons écrire **B=20R**, qui indique qu'avec une probabilité 20/26, la lettre **B** sera à droite quand **i** est pair (et à gauche pour **i** impair). En même temps, la lettre **A** sera très souvent dans l'autre moitié. Les déviations par rapport à 13/26 sont considérables pour un nombre considérable de 16 lettres sur un total de 26 :

B=20R I=17R K=20R M=21R O=20R V=17R X=20R Z=21R

A=22L C=17L J=19L L=21L N=22L P=17L W=19L Y=21L

Ceci est assez proche des techniques des bâtons de Dilly. Nous travaillons sur le même contact interne entre le rotor rapide et deux rotors lents. Produire des tables 26x26 qui montrent comment un rotor sera transformé par la rotation, est une des façons connues d'implémenter l'attaque des bâtons. Cette propriété aurait pu toutefois échapper à Knox et Turing, qui ont ordonné ces tables différemment et avec l'ancien ordre d'entrée QWERTZU.

Le résultat est que, en quelque sorte, le rotor III, s'il est en position 3, devient partiellement transparent pour l'attaquant. Ensuite, peu importe que ces lettres soient encore transformées par le *stecker*. Des corrélations aussi fortes qui concernent un grand nombre de lettres, vont sans problème survivre à la complication du *stecker*. Ceci parce que 6 lettres sont inchangées, ce qui est exploité également dans les attaques récentes sur Enigma [8]. Si l'on additionne dans une démarche d'attaque statistique les probabilités de type f/26 des lettres les plus probables, avec plutôt les 1-f/26, pour les lettres qui sont corrélées dans le sens opposé, on peut obtenir des statistiques robustes qui fonctionneront avec et malgré le *stecker*, qui sera partiellement transparent. Ensuite on peut deviner des connexions du *stecker* une par une, et voir si la propriété statistique devient plus nette.

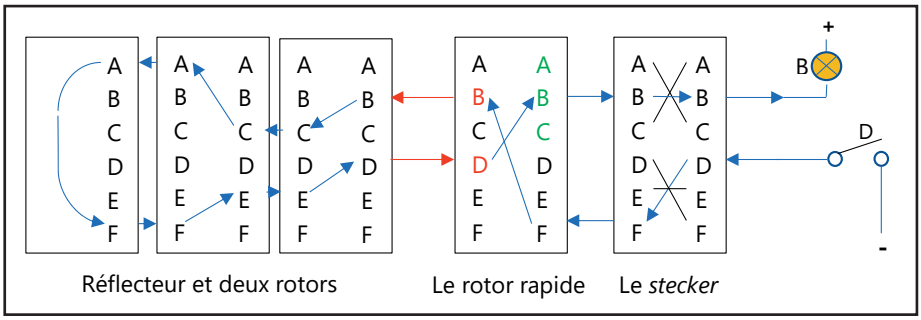

Fig. 1. Enigma : l'attaquant travaille sur les valeurs probables des lettres internes en rouge

Si seulement les rotors d'Enigma pouvaient tourner moins vite… on pourrait casser Enigma facilement, correct ? Oui, c'est quasiment la même chose. Il suffit pour l'attaquant d'inverser la parité pour une lettre sur deux, et une analyse de fréquence des différentes lettres nous donnera une information partielle sur la valeur interne, en rouge sur notre dessin, entrant ou sortant des rotors qui ne bougent pas très vite. Le 3e rotor devient donc partiellement transparent pour l'attaquant, du moins pour un bit d'information interne (une partition de l'espace de 26 lettres). Tout comme s'il s'arrêtait de tourner, cessant d'alterner 26 permutations différentes très complexes.

Dans notre attaque l'attaquant essaie de « voir » si la lettre active entre les 2 rotors lents et le rotor rapide (voir les deux valeurs internes en rouge dans Fig. 1), appartient à un certain ensemble avec une partition de l'espace de lettres. Le Rotor III distingue les premières 13 lettres de l'alphabet entre A et M. Ceci nous rappelle étrangement un célèbre article de Shamir de 1985 qui montre l'existence d'un biais très fort également de type moitié gauche-droite dans le DES [13]. Cet article a ensuite permis aux chercheurs d'inventer la cryptanalyse linéaire, initialement étudiée par Henri Gilbert et Anne Tardy-Corfdir, ensuite revue par Matsui pour le DES com-

plet à 16 rounds en 1993. Toutefois la cryptanalyse linéaire est clairement encore plus ancienne. En Allemagne de l'Est, les approximations linéaires des fonctions booléennes ont déjà été étudiées en 1973 sous le nom de « *Statistische Struktur* » [4]. Dans les documents originaux de 1973, on a l'impression que c'est déjà un travail de routine, standardisé, qui mérite d'être fait pour toute fonction booléenne. Ensuite les attaques par corrélation, sont bien évidemment encore plus anciennes. Il ne faut pas oublier l'attaque Britannique de Colossus de 1943 sur Lorenz SZ-42, le fameux système de chiffrement de Hitler, qui est également tombé, grâce à des attaques avec des corrélations binaires, entre un bit de message chiffré et un bit d'une certaine séquence périodique. Plus encore, pour notre rotor 3, on doit se poser la question suivante. Si notre propriété avec une corrélation forte a été conçue de façon délibérée, par le concepteur du rotor III dont le nom n'est pas connu, alors il faut imaginer qu'une attaque par corrélation complète aurait pu être étudiée encore 15 ans plus tôt, en 1929.

Sachant qu'au temps des bombes, il avait 8 rotors possibles dans l'Enigma de la Wehrmacht et celle de la Luftwafe, et seulement deux de plus dans celle de la marine, il est facile de voir que la sécurité des Enigma pendant en moyenne 1 jour sur 8, donc disons 4 jours par mois, a été plus proche de la sécurité d'une Enigma à 2 rotors. Ici il faut penser que Dilly aurait eu sa chance avec ses méthodes anciennes, ou alors on aurait pu inventer et implémenter une autre attaque par corrélation rapide. Ainsi peut-on imaginer que les bombes de Turing-Welchman auraient été au chômage technique pendant 1/8^{e} du temps. Ceci est considérable, car si les Britanniques avaient économisé environ 26 bombes, ils auraient pu commander 13 bombardiers supplémentaires.

Une autre interprétation est qu'on aurait pu, pour certains jours du mois, casser l'Enigma navale à 4 rotors au prix d'une Enigma normale à 3 rotors, et donc sans les bombes américaines à 4 rotors. Il faut savoir aussi que les Britanniques ont également construit pas moins de 13 bombes à 4 rotors, sous le nom de code Cobra (ce qui est décrit en page 69 [11]). Il est donc possible qu'une Enigma à 5 rotors serait également cassable, si le rotor III qui est si faible, est placé en dernière position.

La conclusion de cet article est qu'on peut encore, en 2020 trouver une attaque totalement nouvelle sur l'Enigma, et que la question des backdoors et des rotors faibles, n'a pas encore été étudiée. Par contre, des questions de ce type sont très souvent étudiées pour le chiffrement par blocs. Dans un article très récent de 2020 accepté à la publication dans Cryptologia, l'auteur montre comment on peut introduire une backdoor dans le système de chiffrement par blocks du T-310. Ce monument de la cryptographie de la guerre froide, a pendant plus d'une décennie été utilisé pour sécuriser l'essentiel des communications par téléscripteurs en Allemagne de l'Est [3]. Dans notre article on montre que la clé à long terme, qui était changée tous les ans, peut être l'objet d'une modification volontaire entièrement compatible avec les machines à chiffrer originales. Ceci affaiblit le système d'origine, à tel point qu'une propriété invariante se propage avec certitude, elle ne faiblit pas, pour un nombre illimité de rounds. Cette attaque marche avec la fonction booléenne d'origine du T-310, sans aucune modification.

Ici les fonctions booléennes ou les S-boxes du DES, sont le parfait équivalent logique d'un rotor de l'Enigma. Shamir a montré en 1985 que toutes les huit S-box

du DES ont le même type de faiblesse, également une corrélation très forte entre 1 bit d'entrée et les valeurs de sortie [13]. Ce qui est nouveau ici, c'est qu'un rotor d'Enigma, et un seul suffit en fait, est également vulnérable à ce même type de faiblesse.

Dans notre travail sur le T-310, il n'y a aucune faiblesse véritable connue dans la fonction booléenne du T-310. On aurait pu trouver une attaque similaire pour toute autre fonction booléenne. C'est différent pour l'Enigma et le DES. Les faiblesses de Shamir ont été la base des attaques linéaires dans les années 1990. Avec Enigma c'est encore plus flagrant. Il est évident que le rotor III de l'Enigma et seulement ce rotor, est exceptionnellement faible, et que cela n'arrive pas par accident. On ne saura probablement jamais s'il s'agit d'un acte de malveillance, ou d'une manie mal placée d'ordonner les lettres d'une façon parfaitement régulière dans un coin de tableau. Mais il est étonnant que ce tableau, qui aurait pu être inventé par Knox dans le cadre de son attaque des bâtons sur l'Enigma commerciale en 1937, ait été étudié bien avant, par les personnes qui ont organisé cette hasardeuse plaisanterie en 1927. Aucune source ne semble indiquer, à quelle date la méthode des bâtons a été connue dans les différents pays. Avec notre découverte, il est permis de penser que les spécialistes Allemands qui ont décidé de la spécification du rotor III, auraient pu avoir connaissance d'une attaque similaire. Il est en effet probable que les Allemands ont analysé d'une certaine façon l'Enigma commerciale bien avant Dilly Knox. D'après Foss [5], Knox aurait acheté une première machine Enigma commerciale à Vienne en 1925. Puis, Knox aurait trouvé l'attaque seulement une décennie plus tard, probablement peu avant le décryptement de l'Enigma Espagnole de Franco en 1937. On peut douter si les Allemands auraient pu étudier ce type d'attaque avant 1929. Mais alors pourquoi la table 26x26 qui sert dans cette attaque, contient de telles régularités ? De même, il faut à nouveau se reposer la question POURQUOI les Allemands ont rendu obligatoire le *stecker* en 1929-1930, alors que les autres pays comme la Suisse ne l'ont pas fait avant 1946. L'explication est peut-être que l'attaque des bâtons inventée par Knox vers 1935, et toujours inconnue des Polonais en 1939, est en fait encore plus ancienne. Il faut comprendre que les Américains dans TICOM n'ont pas pu interroger tous les cryptologues allemands. Certains ont disparu, et il est parfois dit, que certains auraient passé une décennie en Union soviétique, puis sont retournés en Allemagne de l'Est communiste pour travailler dans une université. Nous avons la certitude, et ceci est un message également de la part de vétérans allemands que nous avons personnellement rencontrés, que la cryptologie allemande cache encore bien des mystères.

L'histoire de l'Enigma dans l'immense travail sur XYZ de notre ami Dermot Turing, montre que c'est seulement en comparant les sources venant de pays différents, qu'on peut construire une version plus proche de la vérité, mais jamais parfaite, de l'histoire de la cryptologie. Que faire quand il n'y a plus de documents, et quand les témoins des événements ne sont plus là ? Il reste encore des faits mathématiques et cryptographiques. Forts en termes de probabilités, et dans leur application réduisant la difficulté de l'attaque. Certaines propriétés apparaissent trop peu probables pour penser qu'elles sont accidentelles. Le Rotor III avec sa propriété cachée nous apporte un message limpide : attention aux backdoors ! Semblable à une bouteille jetée à la mer par un cryptologue inconnu que l'on redécouvre 90 années plus tard.

Bibliographie

[1] Mavis Batey, *Dilly Knox - A Reminiscence of this Pioneer Enigma Cryptanalyst*, Cryptologia, 32: 2, 104-130, 2008.

[2] Gustave Bertrand, *Enigma ou la plus grande Enigme de la guerre 1939–1945*, Paris, Librairie Plon, 1973.

[3] Nicolas Courtois, Jörg Drobick, Klaus Schmeh, *Feistel ciphers in East Germany in the communist era*, Cryptologia, vol. 42, Iss. 6, pp. 427-444, 2018.

[4] Nicolas Courtois, Maria-Bristena Oprisanu & Klaus Schmeh, *Linear Cryptanalysis and Block Cipher Design in Eastern Germany in the 1970s*, Cryptologia, vol. 43, Iss 1, p.2-22 2019.

[5] Hugh Foss, *Chapter 3 : Reminiscences on the Enigma*. In Erskine, Ralph, Smith, Michael (eds.). *The Bletchley Park Codebreakers*. Biteback Publishing. pp. 35–39. Nouvelle version remise à jour du livre *Action This Day* … de 2001.

[6] Leo Marks, *Between Silk and Cyanide: A Code Maker's War, 1941-45*, the history Press Ltd, Octobre 2007.

[7] Jean Medrala, *Les réseaux de renseignements franco-polonais: 1940-1944*, l'Harmattan, 412 pages, Mars 2005.

[8] Olaf Ostwald, Frode Weierud, *Modern breaking of Enigma ciphertexts*, Cryptologia 41(5):1-27, Janvier 2017.

[9] Paul Paillole, *Notre espion chez Hitler*, Robert Laffont, 290 pages 1985, Eds. Nouvelle édition de 340 pages chez Nouveau Monde Eds en 2013.

[10] Alan Turing, *Mathematical Theory of ENIGMA Machine*, Livre connu en tant que *Prof's book*.
`https://archive.org/download/TuringMathTheoryEnigma/Turing%20-%20Math%20Theory%20Enigma.pdf`.

[11] Dermot Turing, David Kenyon, *The Bombe Breakthrough*, livre-guide de couleur bleu, vendu par Bletchley Park trust, 96 pages, ISBN 978-1-84165-821-6, 2018.

[12] Dermot Turing, *Enigma. Ou comment les Alliés ont réussi à casser le code nazi*, 406 pages, Nouveau Monde Eds, Septembre 2019.

[13] Adi Shamir, *On the security of DES*, Crypto'85, LNCS 218, Springer, p. 280-281, 1985.