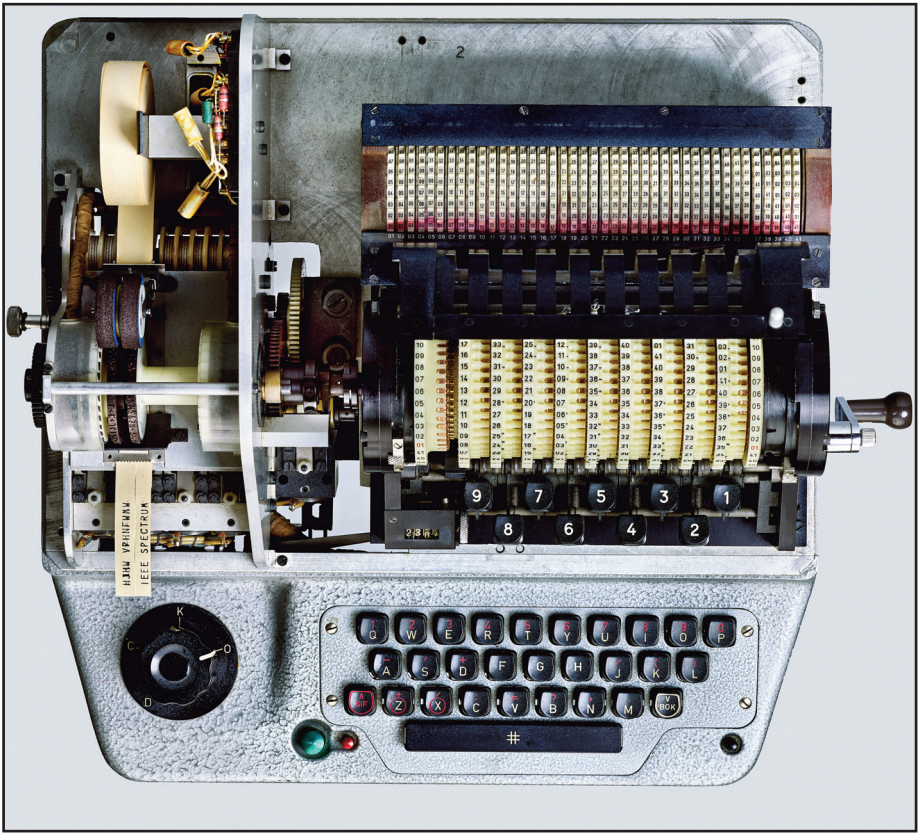
La dernière machine à rotor[1]

Au crépuscule du chiffrement électromécanique une machine exceptionnelle a été impliquée dans un grand scandale d'espionnage

Jon D. Paul



La machine à chiffrer HX-63 était un système électromécanique à rotor conçu et fabriqué par Crypto AG. La machine utilisait neuf rotors [au milieu à droite] pour chiffrer les messages. Une imprimante sur bande de papier [deux lignes] est située sur la partie gauche.

[1] © [2021] IEEE. Traduit et publié avec la permission de l'IEEE. L'article original est paru sous le titre « *The Last Rotor Machine* » dans la revue Spectrum de septembre 2021 (pages 32 à 39 et 52) : https://spectrum.ieee.org/the-scandalous-history-of-the-last-rotor-cipher-machine.

Vidéo en anglais : https://youtu.be/NSqbub5Bo3I

Photographies de la HX-63 : Peter Adams. Illustrations : source Jon D. Paul, dessins Chris Philpot.

Durant mon enfance, à New York, j'ai toujours rêvé d'être un espion. Mais lorsqu'en janvier 1968 j'ai obtenu mon diplôme universitaire, la guerre froide et la guerre du Vietnam faisaient rage, et l'espionnage semblait un choix risqué. Je suis finalement devenu ingénieur en électronique, travaillant sur des analyseurs de spectre en temps réel dans une entreprise de défense.

En 1976, lors d'une visite à Varsovie d'un musée de l'armée polonaise, je suis tombé en arrêt devant une Enigma, la célèbre machine à chiffrer allemande de la Seconde Guerre mondiale. J'étais fasciné. Quelques années plus tard, j'ai eu la chance de visiter, en Suisse près de Zug, l'immense siège de la société Crypto AG (CAG), et de m'y lier d'amitié avec un cryptologue de haut niveau. Cet ami m'a remis un document interne sur l'histoire de la société écrit par son fondateur, Boris Hagelin. Il y était question d'une machine à chiffrer de 1963, la HX-63.

Comme l'Enigma, la HX-63 était une machine de chiffrement électromécanique du type « machine à rotors ». C'était la seule machine à rotors électromécanique jamais construite par CAG, et elle se révéla beaucoup plus perfectionnée et sécurisée que les célèbres Enigma. En fait, c'était sans doute la machine à rotors la plus sûre jamais construite. J'avais envie de mettre la main sur l'une d'elles, mais je doutais de pouvoir le faire un jour.

Faisons un saut en 2010. Je me trouve dans un sombre troisième sous-sol d'une base de télécommunication militaire française. Accompagné de généraux deux étoiles et d'officiers des transmissions, j'entre dans une pièce sécurisée remplie d'anciennes radios militaires et de machines à chiffrer. Et voilà ! Je suis stupéfait de voir une Crypto AG HX-63, ignorée depuis des décennies et reléguée sur une étagère poussiéreuse et peu éclairée.

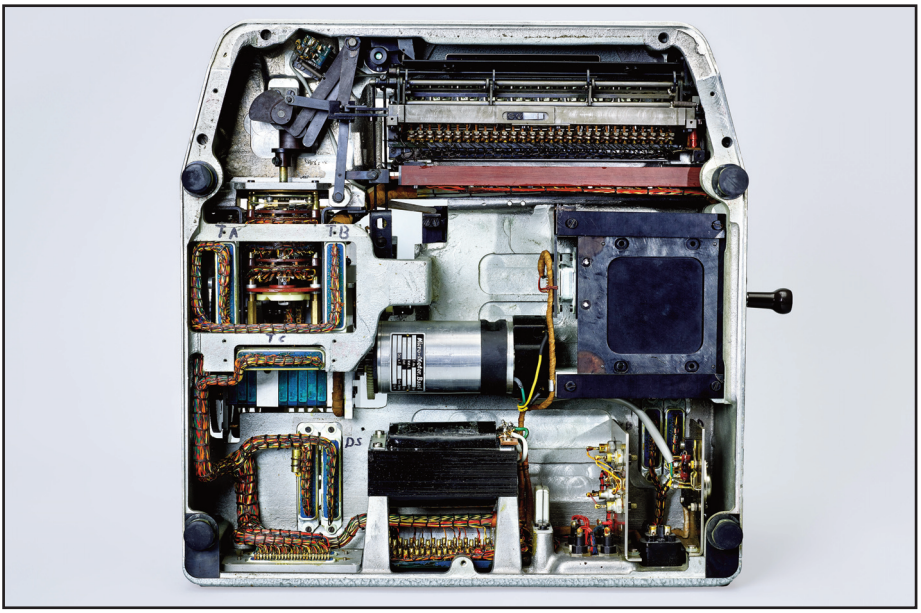
J'extrais avec précaution la machine de 16 kg. Sur le côté droit se trouve une manivelle permettant à la machine de fonctionner en l'absence d'alimentation électrique. La faisant tourner avec précaution, tout en frappant sur le clavier, voilà que les neuf rotors se mettent en mouvement et les roues d'impression en relief frappent doucement une bande de papier.

Je décide sur-le-champ de faire tout ce qui sera en mon pouvoir pour trouver une HX- 63 que je pourrai remettre en état de marche.

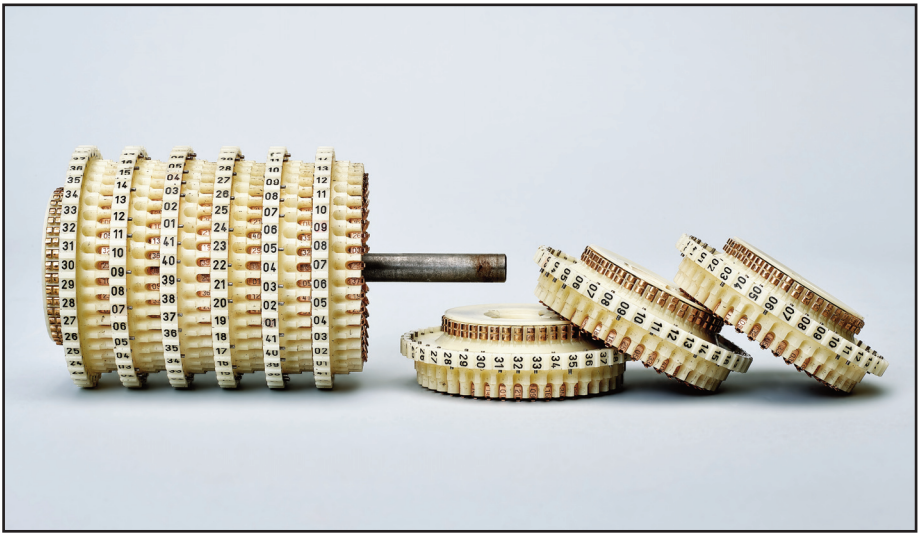
Si vous ne connaissez pas du tout la HX-63, ne soyez pas étonnés. La plupart des cryptologues professionnels n'en ont jamais entendu parler. Et pourtant, elle était si sécurisée que son invention a alarmé William Friedman, l'un des plus grands cryptanalystes de tous les temps et, au début des années 1950, le premier cryptologue en chef de la NSA (l'agence de sécurité nationale américaine). Friedman avait suivi les évolutions des machines de chiffrement de CAG. Grâce à un brevet Hagelin de 1957 (nous y reviendrons plus tard), il comprend que la nouvelle machine de CAG est, au minimum, plus sûre que la propre machine de chiffrement de la NSA, la KL-7 alors considérée comme incassable. Pendant la guerre froide, de 1952 à 1968, la NSA a construit des milliers de KL-7, qui ont été utilisées par toutes les agences militaires, diplomatiques et de renseignement des États-Unis[2].

---

[2] Précision de la rédaction du bulletin de l'ARCSI : la KL7 a également été utilisée par les forces de tous les pays de l'OTAN.



Au centre de la base en aluminium moulé de la machine à chiffrer HX-63 se trouve un moteur à engrenages à courant continu de précision fabriqué en Suisse. On peut également voir l'alimentation électrique [en bas à droite] et le commutateur de fonction [à gauche], qui était utilisé pour sélectionner le mode de fonctionnement - par exemple, le cryptage ou le décryptage.

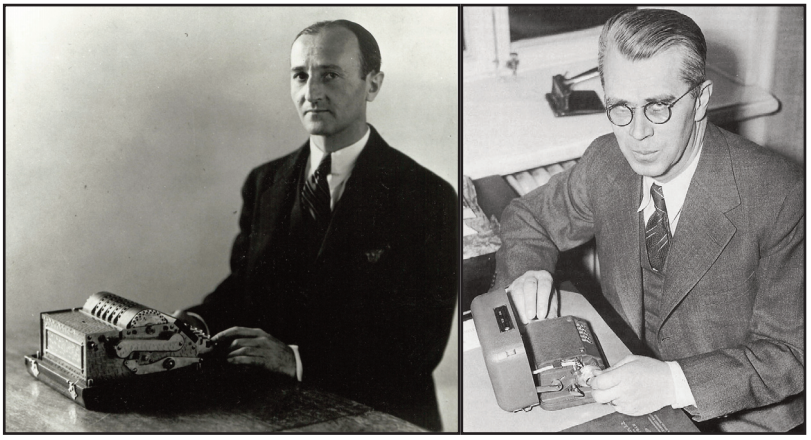


Le HX-63 disposait de 12 rotors différents, dont neuf étaient utilisés à tout moment. Le courant circule dans l'un des 41 contacts plaqués or situés sur le plus petit côté du rotor, dans un conducteur à l'intérieur du rotor, puis dans un contact plaqué or de l'autre côté, avant de passer au rotor suivant. Le mouvement de chaque rotor était déterminé par des ergots, qui sont uniquement visibles sur le rotor horizontal.

Les raisons de l'inquiétude de Friedman sont assez faciles à comprendre. La HX-63 avait environ 10 600 combinaisons de clés possibles ; ce qui équivaut à une clé binaire de 2000 bits. À titre de comparaison, l'AES (Advanced Encryptions Standard), utilisé aujourd'hui pour protéger les informations sensibles dans les administrations, les banques et de nombreux autres secteurs, utilise une clé de 128 ou 256 bits.

Tout aussi inquiétant, CAG était une société suisse privée, vendant à n'importe quel gouvernement, entreprise ou individu. À la NSA, le travail de Friedman était de s'assurer que le gouvernement américain gardait un accès aux communications sensibles et chiffrées de tous les gouvernements amis et ennemis du monde entier. Mais les échanges chiffrés par la HX-63 étaient lui échappaient.

Friedman et Hagelin étaient de bons amis. Pendant la Seconde Guerre mondiale, Friedman avait contribué à faire d'Hagelin un homme très riche en suggérant des modifications à l'une de ses machines, ce qui permit à l'armée américaine d'obtenir une licence pour les brevets d'Hagelin. La machine ainsi créée, la M-209-B, est devenue une bête de somme pendant la guerre, avec quelque 140 000 unités mises en service. Au cours des années 1950, la relation étroite entre Friedman et Hagelin a conduit à une série d'accords de type « *Gentleman's Agreement* » entre les services de renseignement américains et la société suisse : en résumé, Hagelin acceptait de ne pas vendre ses machines les plus sécurisées aux pays spécifiés par les services de renseignements américains, ceux-ci ayant également obtenu un accès secret aux machines, aux plans, au registre des ventes et à d'autres données de CAG.



William F. Friedman [à gauche] a dominé la cryptologie américaine pendant plus de 40 ans et a été le premier cryptologue en chef de l'Agence de sécurité nationale américaine. Son ami Boris Hagelin [à droite], un brillant inventeur et entrepreneur suédois, a fondé Crypto AG en 1952 à Zug, en Suisse, et en a fait la plus grande entreprise de machines de chiffrement au monde.

Mais en 1963, CAG commence à commercialiser la HX-63, et Friedman devient encore plus inquiet. Il convainc Hagelin de ne pas fabriquer le nouvel appareil, alors que la conception de la machine avait demandé plus de dix ans et que seule une quinzaine d'exemplaires avait été fabriquée pour l'armée française. Cependant, 1963 est une année intéressante pour la cryptographie. Les machines à chiffrer arrivaient à la croisée des chemins ; il était clair alors que l'avenir appartenait au chif-

frement électronique. Même une machine exceptionnelle comme la HX-63 serait bientôt obsolète.

C'était un défi pour CAG, qui avait une expertise limitée en électronique. C'est peut-être en partie pour cette raison qu'en 1966, les services de renseignements américains ont fait passer leurs relations avec CAG à un niveau supérieur. Cette année-là, la NSA a livré à son partenaire suisse un système de chiffrement électronique qui est devenu la base d'une machine de CAG appelée H-460. Introduite quatre ans plus tard, la machine comportait une faille. Cependant en 1970, de plus grands changements sont en cours chez CAG : la CIA et le Service fédéral de renseignement allemand acquièrent secrètement CAG pour 5,75 millions de dollars (La même année, Bo, le fils d'Hagelin, qui s'était opposé à la transaction, décède dans un accident de voiture près de Washington, D.C.).

Bien que la H-460 comportât une faille, elle a été remplacée par une machine appelée H-4605, dont plusieurs milliers ont été vendus. Le H-4605 a été conçu avec l'aide de la NSA. Pour générer des nombres aléatoires, elle utilise plusieurs registres à décalage basés sur la technologie alors émergente de l'électronique CMOS. Ces nombres n'étaient pas de vrais nombres aléatoires, mais plutôt des nombres pseudo-aléatoires, qui sont générés par un algorithme mathématique à partir d'une « graine » initiale.

Cet algorithme mathématique a été créé par la NSA, qui pouvait donc déchiffrer tous les messages chiffrés par la machine. Dans le langage courant, les machines comportaient une porte dérobée. Mais c'est le début d'une nouvelle ère pour CAG. À partir de ce moment-là, ses machines électroniques, notamment la série HC-500, ont été secrètement conçues par la NSA, parfois avec l'aide de partenaires commerciaux tels que Motorola. Cet accord américano-suisse porte le nom de code Rubicon. L'installation de portes dérobées dans toutes les machines de CAG va se poursuivre jusqu'en 2018, date à laquelle la société est liquidée.

Tout cela, nous est connu grâce à des fuites provenant d'employés de CAG avant 2018, ainsi qu'à une enquête ultérieure du *Washington Post* et de deux entreprises de communication européennes, ZDF (*Zweites Deutsches Fernsehen*) en Allemagne et SRF (*Schweizer Radio und Fernsehen*) en Suisse. L'article du Post, en particulier, publié le 11 février 2020, a déclenché des tempêtes de feu dans les milieux de la cryptologie, de la sécurité de l'information et du renseignement. Les révélations ont gravement porté atteinte à la réputation de discrétion et de fiabilité de la Suisse, déclenché des litiges civils et pénaux et provoqué des retombées politiques qui se poursuivent aujourd'hui encore. Elles ont conduit, en mai 2021, à la démission du chef du renseignement suisse Jean-Philippe Gaudin qui s'était brouillé avec le ministre de la Défense sur la façon dont les révélations avaient été gérées. En fait, il existe un parallèle intéressant avec notre époque, où les portes dérobées sont de plus en plus courantes et où le FBI et d'autres agences américaines de renseignement et d'application de la loi se battent sporadiquement avec les fabricants de smartphones pour accéder aux données chiffrées qui y sont stockées.

Avant même ces révélations, j'étais profondément fasciné par la HX-63, la dernière des grandes machines à rotors. J'eus donc du mal à croire à ma chance en 2020 lorsque, après des années de négociations, j'ai pris possession d'une HX-63 pour mes recherches pour l'ARCSI. Cette unité, différente de celle que j'avais vue dix ans auparavant, était restée intacte depuis 1963. J'ai immédiatement commencé à planifier la restauration de cette machine à forte résonance historique.

Depuis quelques milliers d'années, les gens utilisent des codes et le chiffrement pour protéger les informations sensibles. Les premiers chiffres étaient basés sur des calculs manuels et des tables. En 1467, fut inventé un dispositif mécanique connu sous le nom de roue chiffrante d'Alberti. Puis, juste après la Première Guerre mondiale, une immense avancée s'est produite, l'une des plus grandes de l'histoire de la cryptographie : Edward Hebern aux États-Unis, Hugo Koch aux Pays Bas et Arthur Scherbius en Allemagne font breveter, à quelques mois d'intervalle, des machines électromécaniques utilisant des rotors pour chiffrer les messages. C'est ainsi que commence l'ère des machines à rotors. La machine de Scherbius, la célèbre Enigma, fut utilisée par l'armée allemande durant les années 1930 jusqu'à la fin de la Seconde Guerre mondiale.

Pour comprendre le fonctionnement d'une machine à rotors, il faut d'abord se rappeler l'objectif fondamental de la cryptographie : remplacer chacune des lettres d'un message, appelé texte clair, par d'autres afin de produire un message incompréhensible, appelé texte chiffré. Il ne suffit pas de réaliser la même substitution à chaque fois - remplacer chaque « F » par un « Q », par exemple, et chaque « K » par un « H ». Une telle substitution à représentation unique serait facilement décryptable en raison des distributions bien connues de la fréquence des différentes lettres dans chaque langue.

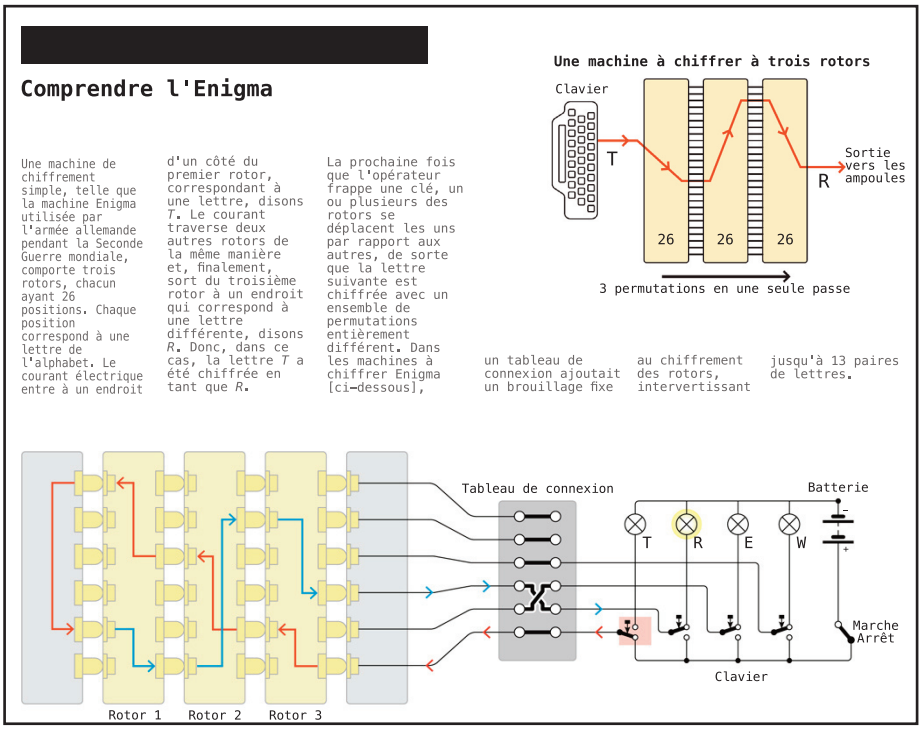
Une machine à rotors contourne ce problème en utilisant, vous l'avez deviné, des rotors. Imaginez un disque dont le diamètre est à peu près celui d'un palet de hockey (environ 76 mm), mais beaucoup plus fin. Des deux côtés du disque, sur le bord, espacés régulièrement, se trouvent 26 contacts métalliques, chaque contact correspondant à une lettre de l'alphabet. À l'intérieur du disque, des fils relient un contact situé sur une face à un autre contact situé sur l'autre face. Ce disque fait partie d'un appareil de type machine à écrire. Lorsqu'un utilisateur frappe une touche du clavier, par exemple un « W », une connexion électrique est établie vers la position « W » d'un côté du rotor. Le courant traverse le rotor et ressort à une autre position, supposons « L » dans notre exemple. Cependant, après cette frappe, le rotor tourne d'une ou de plusieurs positions. Ainsi, la prochaine fois que l'utilisateur appuiera sur la touche « W », la lettre ne sera pas chiffrée par un « L », mais par une autre lettre.

Bien que plus complexe qu'une simple substitution, la cryptanalyse d'une machine à un rotor aussi simple serait un jeu d'enfant pour un cryptanalyste entraîné. Les machines à rotor utilisaient donc plusieurs rotors. Les différentes versions de l'Enigma, par exemple, avaient trois ou quatre rotors. Lors de son fonctionnement, chaque rotor se déplace à des intervalles variables par rapport aux autres : la frappe d'une touche pouvait déplacer un, deux ou tous les rotors. Les opérateurs compliquaient encore le système de chiffrement en choisissant les rotors à insérer dans leur machine, chaque rotor étant câblé différemment. Les machines Enigma disposaient également d'un tableau de connexion, qui intervertissait des paires de lettres spécifiques, tant à l'entrée du clavier qu'à la sortie des lampes.

L'ère des machines à rotors s'est finalement terminée vers 1970, avec l'avènement du chiffrement électronique et logiciel, il y a eu pourtant une machine à rotor soviétique appelée Fialka qui a été déployée jusque dans les années 1980.

La HX-63 a repoussé les limites de la cryptographie. Pour commencer, elle possède

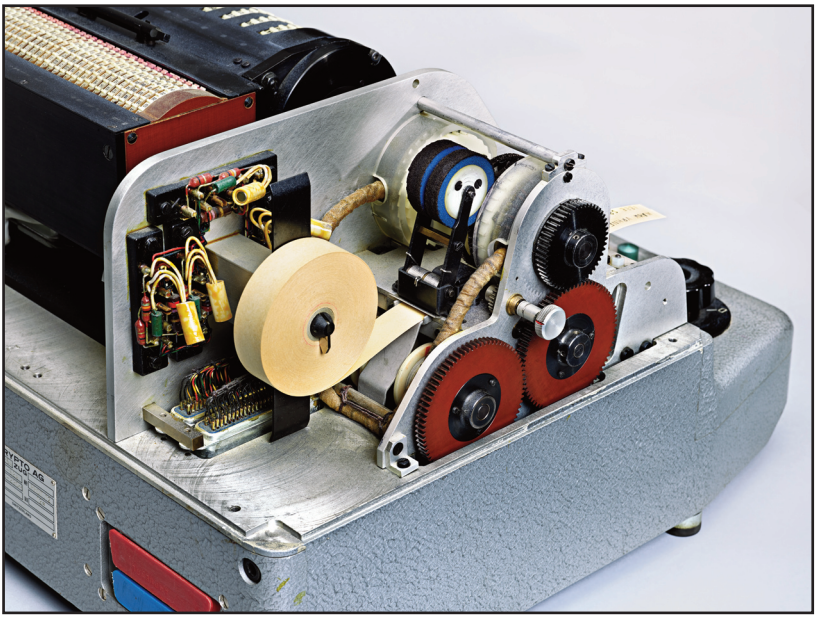
un ensemble de neuf rotors amovibles. Il y a également un « modificateur », composé de 41 commutateurs rotatifs, chacun disposant de 41 positions, qui, comme le tableau de connexion de l'Enigma, ajoute au chiffrement une autre couche, un brouillage invariable. L'unité que j'ai acquise est dotée d'une base en aluminium moulé, d'une alimentation électrique, d'un moteur, d'un clavier mécanique et d'une imprimante sur bande conçue pour afficher à la fois le texte saisi et le texte chiffré ou déchiffré. Un commutateur situé sur la base permet de passer de l'un à l'autre des quatre modes suivants : arrêt, test, chiffrement et déchiffrement.



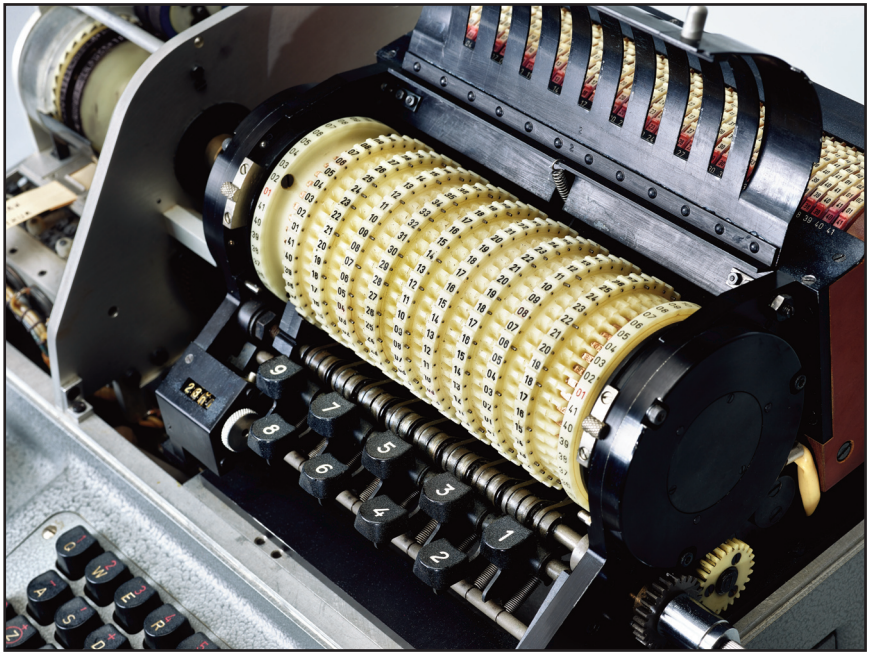
En mode chiffrement, l'opérateur tape le texte clair et le message chiffré est imprimé sur la bande de papier. Chaque lettre du texte clair saisie sur le clavier est brouillée selon les nombreuses permutations du banc de rotors et du modificateur pour donner la lettre du texte chiffré. En mode déchiffrement, le processus est inversé.

L'utilisateur saisi le message chiffré, et le message original ainsi que le message déchiffré sont imprimés, caractère par caractère et côte à côte, sur la bande de papier.

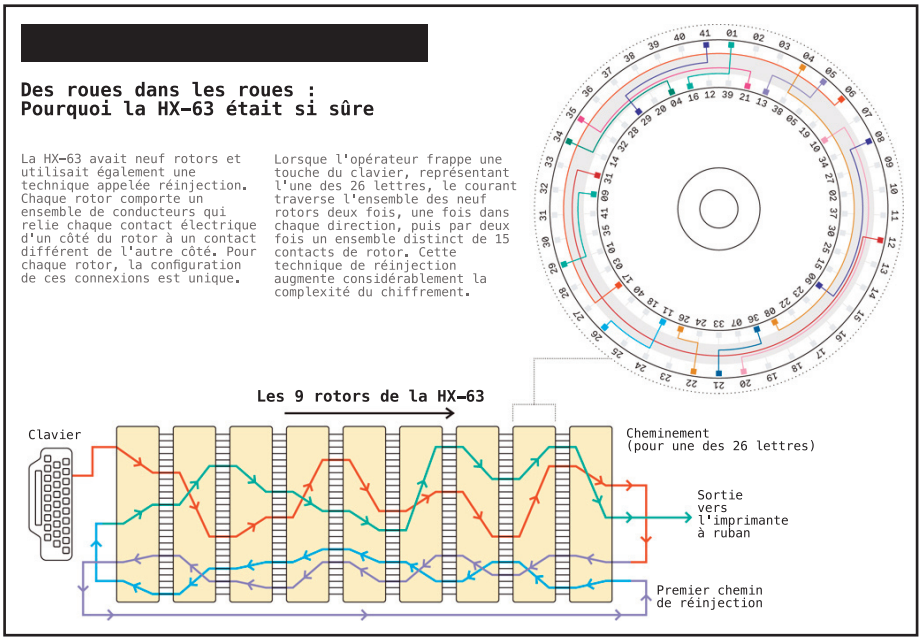
Pour commencer à chiffrer un message, il faut sélectionner neuf rotors (parmi douze) et mettre en place les ergots des rotors qui déterminent le mouvement pas à pas des rotors les uns par rapport aux autres. Ensuite, vous placez les rotors dans la machine dans un ordre spécifique, de droite à gauche, et vous placez chaque rotor dans une position de départ spécifique. Enfin, vous positionnez chacun des 41



Lors du chiffrement ou du déchiffrement d'un message, le HX-63 imprimait à la fois le message original et le message chiffré sur une bande de papier. Les roues bleues sont constituées d'une mousse absorbante qui absorbe l'encre et l'applique sur les roues d'impression gaufrées.



Sous les neuf rotors du HX-63 se trouvent neuf touches qui permettent de déverrouiller chaque rotor afin de définir la position initiale du rotor avant de traiter un message. Cette position initiale était un élément important de la clé cryptographique.



interrupteurs du modificateur dans la position prescrite. Pour déchiffrer le message, les mêmes rotors et réglages, ainsi que ceux du modificateur, doivent être recopiés dans la machine de réception. L'ensemble de ces positions, câblages et réglages des rotors et du modificateur constitue la clé.

La HX-63 comprend, en plus de la manivelle, une batterie au nickel-cadmium pour faire fonctionner l'ensemble en l'absence d'alimentation secteur.

Une alimentation linéaire de 12 volts continus fait fonctionner le moteur, l'imprimante et charge la batterie. Le moteur de précision de 12 volts fonctionne en permanence, entraînant les rotors et l'arbre de l'imprimante par l'intermédiaire d'un engrenage et d'un embrayage. L'appui sur une touche du clavier libère le mécanisme, de sorte que l'engrenage fait effectuer un cycle à la machine, faisant tourner l'arbre, qui fait progresser les rotors et imprime un caractère.

L'imprimante comporte deux roues en relief de l'alphabet, qui tournent à chaque frappe et sont arrêtées à la lettre voulue par quatre solénoïdes et un mécanisme à cliquet. Alimentés par les sorties des rotors et du clavier, des encodeurs mécaniques à arbre détectent la position des roues de l'imprimante et arrêtent la rotation à la lettre voulue. Chaque roue possède son propre encodeur. Une roue imprime l'entrée sur la moitié gauche de la bande de papier, l'autre imprime la sortie sur le côté droit de la bande. Après l'arrêt d'une roue, une came libère un marteau d'impression, qui frappe la bande de papier contre la lettre en relief. À la dernière étape, le moteur fait avancer la bande de papier, de sorte que le cycle se termine et que la machine est prête pour la lettre suivante.

Lorsque j'ai commencé à restaurer la HX-63, j'ai rapidement réalisé l'ampleur du défi. Les engrenages en plastique et les pièces en caoutchouc s'étaient détériorés,

au point que le stress mécanique dû au fonctionnement du moteur pouvait facilement les détruire. Les pièces de rechange n'existant pas, j'ai dû les fabriquer moi-même.

Après avoir nettoyé et lubrifié la machine, j'ai frappé sur quelques touches du clavier. J'ai été ravi de voir que les neuf rotors de chiffrement tournaient et que la machine imprimait quelques caractères sur la bande de papier. Mais l'impression était parfois vide et déformée. J'ai remplacé la batterie nickel-cadmium corrodée et recâblé le transformateur de l'alimentation, puis j'ai appliqué progressivement le courant alternatif. À mon grand étonnement, le moteur, les rotors et l'imprimante ont fonctionné le temps de quelques frappes. Mais soudain, il y eut un fracas d'engrenages grinçants, et des morceaux de plastique brisés ont volé hors de la machine. L'impression s'est arrêtée, et les battements de mon cœur ont failli en faire autant.

J'ai décidé de désassembler la HX-63 par modules : Le banc de rotors a été enlevé, puis l'imprimante. La base contient le clavier, l'alimentation électrique et les commandes. Au fond de l'imprimante se trouvent quatre amortisseurs qui positionnent les leviers qui arrêtent les roues à la lettre indiquée. Ces amortisseurs s'étaient désintégrés. De même, les disques en mousse qui encrent les roues se décomposaient, et des morceaux gluants obstruaient les roues.

J'ai fait des trouvailles heureuses et inattendues. Pour reconstruire les pièces brisées de l'imprimante, j'avais besoin d'un tube en caoutchouc dense. J'ai découvert qu'un tuyau d'aspirateur en néoprène, largement disponible, convenait parfaitement. À l'aide d'une perceuse à colonne et d'une tige d'acier servant de mandrin, j'ai découpé le tuyau en sections précises de 10 millimètres. Mais l'espace situé au fond de l'imprimante, où les amortisseurs sont censés se trouver, était bloqué par de nombreux arbres et leviers, qu'il semblait trop risqué de retirer et de remplacer. J'ai donc utilisé des pinces à long bec à angle droit et des outils dentaires pour positionner les nouveaux amortisseurs sous le mécanisme. Après des heures de chirurgie habile, j'ai réussi à installer les amortisseurs.

Les roues d'encrage étaient faites d'une mousse poreuse inhabituelle. J'ai testé de nombreux matériaux de remplacement, pour finalement opter pour un cylindre de mousse bleue dense. Hélas, sa surface lisse à cellules fermées n'absorbait pas l'encre. J'ai donc abrasé la surface avec du papier de verre rugueux pour ouvrir les cellules de la mousse.

Après quelques autres bricolages de ce type, j'ai dû faire face à un autre problème : un bourrage de ruban de papier. J'avais chargé un nouveau rouleau, mais je n'avais pas compris que celui-ci avait un noyau légèrement plus petit. Le ruban a grippé, s'est déchiré et s'est coincé sous les roues de l'alphabet, profondément enfoui et inaccessible. Je suis resté bouche bée, mais j'ai ensuite fait une merveilleuse découverte. La HX-63 était livrée avec de fines bandes en acier inoxydable aux bords dentelés, conçues spécialement pour extraire le ruban de papier coincé. J'ai fini par éliminer le bourrage, et la restauration était terminée.

L'une des raisons pour lesquelles la HX-63 était si diaboliquement sûre était une technique appelée réinjection, qui augmentait sa sécurité de manière exponentielle. Les rotors ont généralement une position pour chaque lettre de l'alphabet qu'ils sont censés chiffrer. Ainsi, un rotor typique pour l'anglais aurait 26

positions. Mais les rotors de la HX- 63 ont 41 positions. Cela s'explique par le fait que la réinjection (également appelée réentrée) utilise des circuits supplémentaires en plus de ceux destinés aux lettres de l'alphabet. Dans le HX-63, il y avait 15 chemins supplémentaires.

Voici comment la réinjection fonctionnait dans la HX-63. En mode de chiffrement, le courant circule dans un sens à travers tous les rotors, chacun introduisant une permutation. Après être sorti du dernier rotor, le courant repasse par le dernier rotor pour parcourir les rotors dans le sens opposé. Cependant, lorsqu'il retraverse les rotors, il suit un chemin différent, à travers les 15 chemins de circuit supplémentaires réservés à cet effet. Le chemin exact dépend non seulement du câblage des rotors, mais aussi de la position des 41 modificateurs. Le nombre total de configurations de circuits possibles est donc de 26 ! x 15 ! ce qui équivaut à environ 5,2 x 10 381. Et chacune des connexions internes des neuf rotors peut être recâblée de 26 ! façons différentes. En outre, l'incrémentation des rotors est contrôlée par une série de 41 broches mécaniques. Si l'on met tout cela ensemble, le nombre total de combinaisons de clés est d'environ 10 600.

Un chiffrement aussi complexe était non seulement incassable dans les années 1960, mais il serait extrêmement difficile à casser même aujourd'hui. La réinjection a été utilisée pour la première fois sur la machine à rotor KL-7 de la NSA. La technique a été inventée pendant la Seconde Guerre mondiale par Albert W. Small, du *Signal Intelligence Service* de l'armée américaine. Elle a fait l'objet d'un brevet secret que Small a déposé en 1944 et qui a finalement été accordé en 1961 (numéro 2984700).

Entre-temps, en 1953, Hagelin a déposé une demande de brevet américain pour la technique qu'il comptait utiliser dans ce qui est devenu la HX-63. De manière peut-être surprenante, étant donné que la technique faisait déjà l'objet d'une demande de brevet de la part de Small, Hagelin se voit accorder son brevet en 1957 (numéro 2802047).

Friedman, pour sa part, avait toujours été alarmé par l'utilisation de la réinjection par Hagelin, car cette technique avait été utilisée dans toute une série de machines à chiffrer américaines d'importance vitale. En plus d'être utilisée dans la KL-7, la réinjection était également une caractéristique de ses successeurs, y compris la KL-47.

L'utilisation de la réinjection dans les machines CAG était une grande menace pour la capacité de la NSA à écouter à volonté les messages gouvernementaux et militaires. Finalement, comme déjà dit, Hagelin a accepté d'arrêter le développement et la fabrication de la HX-63. La série de réunions entre Friedman et Hagelin qui a abouti à l'abandon de la HX-63 a été mentionnée dans le livre de Ronald Clark, *The Man Who Broke PURPLE* (1977), et a été détaillée en 2014 par la divulgation par la NSA des documents de William F. Friedman.

La révélation des accords secrets entre Crypto AG et les services de renseignement américains a peut-être provoqué un scandale amer, mais vu sous un autre angle, Rubicon était certainement l'une des opérations d'espionnage les plus réussies de l'histoire - et un précurseur des portes dérobées actuelles. De nos jours, les agences de renseignement ne sont pas les seules à exploiter les portes dérobées et à écouter les messages et les transactions dites « sécurisés ». La fonction « télémétrie » de Windows 10 surveille en permanence l'activité et les données d'un utilisateur. Les

Macs d'Apple ne sont pas non plus en sécurité. Des logiciels malveillants permettant aux attaquants de prendre le contrôle d'un Mac ont circulé de temps à autre, un exemple notable étant *Backdoor. MAC.Eleanor* vers 2016. Et fin 2020, la société de cybersécurité FireEye a révélé qu'un malware avait ouvert une porte dérobée dans la plateforme SolarWinds Orion, utilisée dans les serveurs des chaînes d'approvisionnement et des gouvernements. Le malware, appelé SUNBURST, était le premier d'une série d'attaques de malware sur Orion. L'étendue des dégâts est encore inconnue.

La machine HX-63 que j'ai restaurée fonctionne aujourd'hui aussi bien qu'en 1963. Je ne me suis pas encore lassé du son du moteur semblable à celui d'un télétype ni du claquement du clavier. Bien que je n'aie jamais réalisé mon rêve d'adolescent de devenir un agent secret, je suis ravi de cette petite lueur d'antan de ce monde glamour.

Et il y a même un post-scriptum. J'ai récemment découvert que mon contact chez Crypto AG, que j'appellerai « C », était également agent de sécurité des services de renseignement suisses. Ainsi, pendant des décennies, alors qu'il travaillait aux plus hauts niveaux de Crypto AG, « C » était une voie de communication indirecte avec la CIA et les services de renseignement suisses, il avait même un nom de code à la CIA. Ironie de l'histoire, mon vieil ami suisse savait tout depuis le début !

Après une carrière d'ingénieur électricien et d'inventeur, l'auteur Jon D. Paul effectue aujourd'hui des recherches, écrit et donne des conférences sur l'histoire de la technologie numérique, en particulier la cryptographie. Dans les années 1970, il a commencé à collectionner des instruments électroniques anciens, tels que les oscilloscopes Tektronix et les analyseurs de spectre Hewlett-Packard que l'on voit ici.