# DE NOUVEAUX APPAREILS CRYPTOGRAPHIQUES POUR LE SECRET DES MESSAGES

Par Charles BRACHET

*La cryptographie est aussi vieille que le monde : de tout temps, les hommes ont employé, pour assurer le secret de certains messages, particulièrement en matière militaire et diplomatique, des signes ou des alphabets conventionnels, plus ou moins compliqués, ou même des « grilles » qui laissent apparaître les seules lettres intéressant le destinataire. De nombreuses méthodes ont ainsi successivement vu le jour, dont l'efficacité n'était cependant jamais certaine, l'ingéniosité des « décrypteurs » se jouant, la plupart du temps, des complications nouvelles imaginées pour rendre plus impénétrables à l'adversaire les messages transmis. Les progrès de la technique n'ont pas manqué — là encore — de bouleverser l'art cryptographique. Des machines ingénieuses ont été construites, qui permettent de brouiller automatiquement les messages frappés en clair et, inversement, de « décrypter » les communications conventionnelles reçues. Enfin, les perfectionnements apportés au* bélinographe *(1) ont permis, en adaptant convenablement cet appareil transmetteur d'images, d'apporter une solution nouvelle et décisive au problème de la cryptographie. Désormais, le secret des communications est rigoureusement assuré entre deux postes même très éloignés, soit par fil, soit par sans-fil, le déchiffrement des messages secrets s'effectuant automatiquement comme leur transmission.*

De récentes affaires d'espionnage ont attiré de nouveau l'attention sur les moyens de correspondance qu'utilisent entre eux les agents de cette peu recommandable industrie. D'autre part, les messages radiotélégraphiés se multiplient ; il n'est même pas d'autre mode de correspondre entre un passager de paquebot et le continent où il laisse ses affaires courantes. S'il lui faut donner ou recevoir une communication de grande importance qui exige une discrétion absolue, l'homme d'affaires doit recourir aux mêmes méthodes de secret que les espions dans leurs messages écrits. Et sans même parler du temps de guerre, pour recevoir les renseignements de son département aussi bien que pour donner ses instructions à ses agents disséminés dans le monde entier, tout ministre des Affaires étrangères, des Colonies, de la Marine, de la Guerre, doit avoir à sa disposition une et même plusieurs de ces méthodes dont l'ensemble constitue aujourd'hui une véritable science : la *cryptographie*.

Comme *La Science et la Vie* l'expliquait il y a onze ans (2) par la plume de l'un des spécialistes français les plus qualifiés, le lieutenant-colonel Givierge, si le soin de résoudre le problème ardu que représente la lecture d'un message secret d'origine inconnue revient aux « cryptologues », le soin d'écrire ces messages est depuis longtemps confié à des machines complexes (1). Ces « machines à écrire » frappent le texte chiffré suivant une clé arbitraire, sans que le dactylographe ait à se préoccuper d'autre chose que de « taper » suivant l'alphabet classique. S'il tape, inversement, le message secret, la machine restitue le texte en « clair ». Quels progrès ont été réalisés dans ces machines, à l'heure actuelle ?

D'autre part, le télégraphe, avec ou sans fil, permet de transmettre des autographes, des documents originaux, des photographies. L'inventeur et l'initiateur de ce mode de transmission, M. Edouard Belin, se devait de garantir également ces messages contre une capture indiscrète. C'est ce qu'il vient de réaliser, complétant ainsi de la plus heu-

(1) Voir *La Science et la Vie*, n° 91, page 13.
(2) Voir *La Science et la Vie*, n° 69, page 223.

(1) Nous laissons volontairement de côté la méthode de correspondance au moyen de codes ou dictionnaires secrets dont les pages, les lignes, les mots, repérés par des nombres, fournissent le moyen d'écrire une suite des chiffres qui tirent leur sens de ces coordonnées. Il suffit que les correspondants possèdent chacun un exemplaire du code secret. Dailleurs la méthode de brouillage cryptographique est ordinairement superposée au chiffrage qui concerne les codes. Ultime précaution contre le vol éventuel de ces documents de base.

reuse manière, l'application des machines à la cryptographie.

Tels sont les remarquables progrès que nous allons exposer.

## Comment la cryptographie est devenue une « science »

Il n'y a plus de secrets en cryptographie ; il n'y a que des problèmes et, par conséquent, des méthodes grâce auxquelles les problèmes sont : 1° posés ; 2° résolus. Ceci étant toujours plus difficile que cela (1).

Autrefois, les méthodes n'étaient que des trucs que l'on pouvait, par conséquent, garder secrets. Le plus simple et le plus enfantin de ces trucs consiste à établir un alphabet à *signes* conventionnels, dont le sens n'est connu que des deux correspondants. Mais les statisticiens ont vite fait de démêler l'ordre de fréquence des « lettres » figurées dans le texte chiffré. La fréquence de chaque lettre, surtout si c'est une voyelle, suffit à l'identifier. Le mystère est ainsi percé, de proche en proche. Il ne sert donc pas à grand'chose aujourd'hui de brouiller simplement un alphabet.

Par contre, on peut convenir d'un *décalage* entre la lettre écrite dans le texte chiffré et la lettre correspondante du texte en clair.

Et puis convenir, en second lieu, que ce décalage *variera périodiquement*, et d'une manière arbitraire, d'une lettre à l'autre du texte. La « période » choisie étant, par exempie, de 5 lettres, il reste à convenir des 5 « décalages » qui devront jouer successivement. Un *mot-clé* suffit à noter cette convention. Convenons que ce sera le mot TEMPS ; le chiffreur n'aura plus qu'à écrire en décalant chacune des 5 premières lettres du message relativement à l'alphabet classique de 26 lettres, comme sont décalées, relativement à ce même alphabet, chacune des lettes du mot TEMPS, c'est-à-dire : la première de 19 rangs, comme T ; la seconde de 4 rangs, comme E ; la troisième de 12 rangs, comme M ; la quatrième de 15 rangs, comme P ; la cinquième de 18 rangs, comme S. Après quoi, la « période » recommence pour les 6e, 7e, 8e, 9e et 10e lettres, etc... (L'alphabet est supposé écrit en circuit fermé, A succédant à Z, chaque lettre formant ainsi le maillon d'une chaîne sans fin.) Dans ces conditions, la phrase :

A T T A Q — U E Z D E — M A I N
1 2 3 4 5 1 2 3 4 5 1 2 3 4

s'écrira, en texte chiffré :

T X F P I — N I L S W — F E U Q

L'opération inverse de substitution des lettres chiffrées par les lettres correspondantes du texte en clair est aisée pour qui connaît la convention exposée ainsi que le mot-clé.

La méthode de chiffrement que nous venons d'indiquer dérive de la méthode inventée par Vigenère, au XVIIe siècle. Celle-ci a d'ailleurs été synthétisée dans un tableau *carré* dont nous nous contentons de donner l'amorce à la page 100.

Si nous donnons comme « mot-clé » : D E F I et si nous voulons chiffrer le mot : E N N E M I, nous n'avons qu'à prendre, dans le tableau de Vigenère, la lettre qui, dans la colonne D, correspond à la ligne E (soit *h*) ; puis celle qui, dans la colonne E, correspond à la ligne N (soit *r*) ; celle qui, dans la colonne F, correspond au second N du mot chiffré (soit *s*) ; et, dans la colonne I, celle qui correspond à la ligne E (soit *m*). Puis, nous continuons à lire le mot E N N E — M I en recommençant le cycle du « mot-clé » (D E F I), dont chaque lettre indique la colonne où puiser la lettre chiffrée. Nous trouvons ainsi pour l'ensemble du mot : E N N E M I = *h r s m p m*.

Nous arrêterons au tableau de Vigenère cet exposé de cryptographie élémentaire. Il se borne à la méthode dite « de substitution ». Nous n'entrerons pas dans les complications que l'on peut faire subir au système en y introduisant des « bigrammes », des « trigrammes », plus généralement des « polygrammes », c'est-à-dire des « groupes » de lettres chiffrées qui correspondent chacun à une seule lettre du texte clair. Qu'il nous suffise de montrer comment le tableau de Vigenère peut donner lieu, immédiatement, à la construction d'une machine à cryptographier.

## Du tableau de Vigenère à la machine rotative élémentaire

Imaginons, en effet, que chaque colonne du tableau soit enroulée sur le tambour d'une roue et que toutes les roues ainsi constituées soient juxtaposées suivant un même axe. Il est évident que si les vingt-six roues présentent, dans leurs positions initiales, la suite des lettres de l'alphabet, *suivant une même génératrice*, il suffira de faire tourner

(1) Remarque intéressante : les mathématiciens savent toujours poser un problème par équations différentielles. Par contre, l'intégration de ces équations n'est réalisable qu'exceptionnellement. Le même jeu semble s'être établi entre les « cryptographes » qui posent l'énigme et les « cryptologues », qui tâchent à la résoudre. Ajoutons que la cryptographie par signes alphabétiques discrets relève de combinaisons arithmétiques par *nombres entiers*, et, que M. Belin, en introduisant le brouillage des images, transpose le problème sur le plan *géométrique*.

les roues qui correspondent aux lettres du « mot-clé », et de les faire tourner d'un angle proportionnel au rang qu'occupent les « lettres à chiffrer » sur les « lignes » du tableau de Vigenère, pour que les « lettres-chiffres » recherchées apparaissent successivement sur la ligne repère, aux lieu et place des lettres du mot-clé. On peut, en effet, toujours remplacer un tableau à double entrée par un système de roues parallèles dont *les tambours correspondent aux colonnes* du tableau, tandis que *leurs déplacements angulaires correspondent aux lignes.*

Mais, en l'espèce, il n'est pas besoin de conserver vingt-six roues : il suffit d'en garder juste autant que l'on veut donner de lettres au mot-clé : cinq, par exemple.

On disposera seulement à l'origine les cinq roues de telle manière qu'elles forment les cinq lettres convenues sur la ligne génératrice de départ. (C'est ainsi que se forme le mot-clé sur les cadenas à secret, également munis de roues-alphabets.)

Quant aux déplacements angulaires destinés à figurer les lignes, c'est une roue à cliquet qui les assurera. ou encore un engrenage exactement denté dans ce but.

Mais il serait puéril de construire une machine simplement pour remplacer un tableau. Les roues d'engrenage (dont chaque dent représente une case du tableau) « matérialisent » les « périodes » des substitutions alphabétiques, dans l'opération cryptographique. Mais nous allons voir combien la rotation mécanique des alphabets, conjuguée avec des commandes électriques, peut accentuer la complication et, par conséquent, le secret du cryptogramme que l'on demande à la machine de fournir.

LETTRES DESTINÉES A FORMER LA CLÉ

| LETTRES A CHIFFRER | A | B | C | D | E | F | G | H | I | ... |
|---|---|---|---|---|---|---|---|---|---|---|
| A | a | b | c | d | e | f | g | h | i | ... |
| B | b | c | d | e | f | g | h | i | j | ... |
| C | c | d | e | f | g | h | i | j | k | ... |
| D | d | e | f | g | h | i | j | k | l | ... |
| E | e | f | g | h | i | j | k | l | m | ... |
| F | f | g | h | i | j | k | l | m | n | ... |
| G | g | h | i | j | k | l | m | n | o | ... |
| H | h | i | j | k | l | m | n | o | p | ... |
| I | i | j | k | l | m | n | o | p | q | ... |
| J | j | k | l | m | n | o | p | q | r | ... |
| K | k | l | m | n | o | p | q | r | s | ... |
| L | l | m | n | o | p | q | r | s | t | ... |
| M | m | n | o | p | q | r | s | t | u | ... |
| N | n | o | p | q | r | s | t | u | v | ... |
| O | o | p | q | r | s | t | u | v | x | ... |
| : | : | : | : | : | : | : | : | : | : | : |

LE TABLEAU DE VIGENÈRE (XVII[e] SIÈCLE)

*Le mot choisi comme « clé » étant, par exemple,* D E F I, *et le mot à chiffrer étant* E N N E M I, *nous cryptographierons celui-ci en substituant à chacune de ses lettres (lues comme en-tête d'une « ligne » du tableau) le caractère qui lui correspond dans les colonnes* D, E, F, I *prises* à tour de rôle *dans l'ordre du mot-clé jusqu'à épuisement du texte à chiffrer. Par cette méthode, en se référant au tableau ci-dessus,* E N N E M I *devient ici :* h r s m p m.

## Les machines cryptographiques procèdent par « substitution » de lettres

Longtemps, la méthode Vigenère fut considérée comme offrant le minimum de chances aux « cryptologues » : nous appellerons ainsi les spécialistes dont l'art est de deviner les méthodes, les clés et de lire ainsi des textes de provenance inconnue. Les cryptologues émérites sont extrêmement rares. Au contraire, les *déchiffreurs* (ou « décrypteurs ») sont des praticiens aussi avertis et aussi intelligents que possible,

mais sans vocation spéciale : ils reconstituent simplement les textes chiffrés d'après des conventions connues d'eux. Leur travail est *mécanique* comme celui des chiffreurs. Il résulte de là que toute machine *à chiffrer* pourra et devra être « réversible », c'est-à-dire également apte *à déchiffrer* les textes établis par elle ou ses sœurs de même modèle.

Qui dit « machine » dit « répétition », c'est-à-dire « périodes ». C'est pourquoi, seule, la méthode de Vigenère ou ses dérivées complexes, peuvent se « mécaniser ».

Nous donnons, ci-joint, un modèle de machine des plus modernes basé sur ces principes. L'image montre nettement les quatre roues-alphabets qui sont l'âme du système. On amène les quatre roues sur une position *d'origine du mouvement* déterminée par quatre lettres placées côte à côte : c'est la « clé ».

Les quatre roues-alphabets sont entraînées ensemble par une roue à rochet que commande le clavier de la machine.

Suivons l'action de ces roues : sous chaque

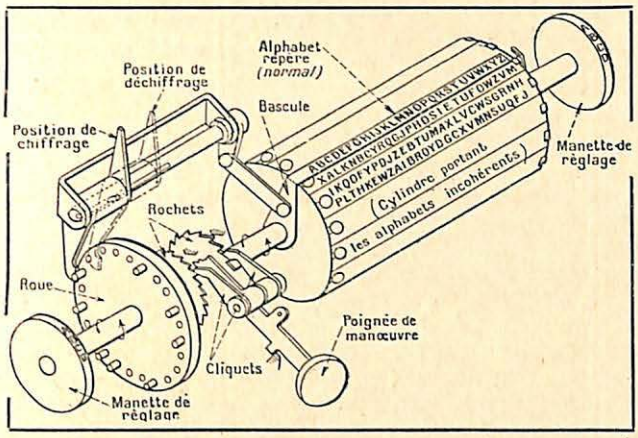


FIG. 1. — LE CRYPTOGRAPHE A ALPHABET INCOHÉRENT

*La méthode cryptographique consiste ici à placer sur un cylindre une série de réglettes longitudinales (suivant les génératrices). Chacune de ces réglettes comporte toutes les lettres de l'alphabet disposées d'une manière incohérente. Aucune de ces réglettes ne se répète. Chacune d'elles est marquée d'un numéro connu des seuls correspondants, ce qui permet à chacun d'eux de disposer les alphabets incohérents dans le même ordre, sur leurs cylindres respectifs. Ceci posé, voici comment se fait le chiffrage : sur la roue visible à gauche sont disposés des ergots dont chacun correspond à une réglette du cylindre. Le correspondant chiffreur choisit* arbitrairement *un certain nombre d'ergots (numérotés comme les réglettes), qu'il pousse de manière à les faire émerger à gauche de la roue. Puis, agissant sur la poignée de manœuvre, il actionne la roue à rochets indiquée sur la figure. Cette roue dentée entraîne celle des ergots, en poussant la « bascule » de l'appareil. Celle-ci (par une connexion mécanique facile à suivre sur le schéma) fait avancer une* réglette mobile *au-dessus du cylindre. Cette réglette mobile porte* l'alphabet dans son ordre naturel ; *à chacun de ses arrêts successifs, le chiffreur lit* sur l'alphabet incohérent *le caractère correspondant à la lettre* du texte en clair ; *il note ce caractère. Et ainsi, de proche en proche, il construit son* texte chiffré. *A la réception du texte chiffré ainsi obtenu, le* « déchiffreur », *qui connaît les réglettes à alphabet incohérent dont il doit garnir son cylindre, connaît également la disposition des ergots sur la roue. Il opère de la manière suivante : il met l'onglet d'entraînement de la bascule dans la position de déchiffrage. Puis, agissant à son tour sur la poignée de manœuvre, il obtient un déplacement de la réglette-repère comportant l'alphabet naturel. Cette réglette, venant se juxtaposer sur l'alphabet incohérent, permet l'opération inverse qui consiste à traduire les lettres de l'alphabet-repère dans les caractères correspondants du cylindre. Comme les ergots sont « en position inverse » sur leur roue, durant cette opération de déchiffrage (en raison du déplacement préalable de l'onglet), c'est là que réside le secret de la réussite. La manette située à l'extrême droite de la figure sert au réglage qui fixe une même origine à la rotation du cylindre dans les deux cas du chiffrage et du déchiffrage.*

lettre, elles portent, à leur périphérie, un ergot transversal et mobile qui joue le rôle de dent d'engrenage. Voici donc des roues d'engrenage dont on peut modifier à volonté le nombre de dents en éclipsant telle série d'ergots conventionnellement choisis. Au chiffre de la « clé » se superpose donc un nouveau chiffre relatif à chacune des roues-clefs.

Les ergots de chaque roue ainsi disposés entraînent, de manière fort irrégulière (par un engrenage intermédiaire), *deux* collecteurs électriques comportant chacun cinq jeux de bagues et de balais de contact. L'ajustage des deux collecteurs et des quatre roues-clefs ajoute donc deux facteurs à la clé proprement dite. Ces facteurs se traduisent, de cette façon, par deux lettres supplémentaires.

Ce n'est pas tout. Nous comprenons déjà que l'impression définitive des lettres brouillées se fera par la commande électromécanique des collecteurs électriques à dix contacts. Quelle que soit cette commande, nous voyons tout de suite qu'il est possible de

modifier arbitrairement les *dix* connexions électriques, au lieu de les laisser fonctionner dans l'ordre de construction purement « mécanique ». Cette modification n'exige que des fiches analogues à celles des standards téléphoniques : le « modificateur » de la machine comporte donc dix fiches de ce genre, identifiées chacune par une lettre de l'alphabet. L'ordre de disposition de ces fiches apporte un nouveau coefficient de brouillage : les dix fiches peuvent donner lieu à 14.040 combinaisons. Tant et si bien que *l'ordre d'imprimer*, finalement transmis par les collecteurs, est tellement brouillé qu'il faudrait taper 15.600.900 lettres sur le clavier de la machine avant de voir apparaître une série semblable à celle-là — c'est-à-dire qui, toute réserve faite sur le texte, comporte les mêmes correspondances entre la lettre en clair (tapée) et la lettre chiffrée (imprimée). Autrement dit, le « cryptologue » ignorant de la clé de six lettres et qui voudrait la retrouver par statistique (ou toute autre méthode), devrait travailler sur des séries de lettres couvrant chacune 10.000 pages dactylographiées. Tâche surhumaine !

Le destinataire du message chiffré, qui, connaissant les conventions, peut placer *sa* machine dans les mêmes conditions de fonctionnement que *celle* du chiffreur expéditeur, n'a qu'à taper le message chiffré pour voir apparaître, imprimé, le message en clair. Les deux opérations inverses de *chiffrage* et de *déchiffrage* se font, au gré de l'opérateur, en tournant préalablement une manette à deux positions : C et D.

Nous passons volontairement sous silence la partie imprimant de la machine : elle est constituée par l'un des nombreux systèmes télégraphiques imprimants. On pourrait, d'ailleurs, fort bien concevoir, si le message était télégraphique, que celui-ci soit tapé à Paris en clair et reçu chiffré à Toulouse. Et réciproquement...

Le fonctionnement du « télégraphe » imprimant exige, naturellement, comme dans le Baudot, ou tout appareil similaire, qu'un moteur électrique assure une rotation continue aux organes de déclenchement.

La machine que nous venons de prendre en exemple comporte donc deux clés superposées : l'une de deux lettres (ajustage des collecteurs), l'autre de quatre lettres (disposition des roues à ergots). En plus, intervient la clé du « modificateur » électrique. On conçoit que les services utilisant cet appareil peuvent convenir de changements périodiques (quotidiens par exemple) de l'une ou de l'autre clé ou de toutes ensemble.

## La machine à alphabets incohérents, procédé par « transposition »

Une simplification technique de la machine à cryptographier, qui n'enlève rien à sa puissance de combinaison, sera celle-ci :

Au lieu de « combiner » les substitutions de lettres en « périodes » dans le temps (par rotations mécaniques), on peut les combiner dans l'espace. Pour cela, on écrit sur des réglettes, aussi nombreuses qu'on le désire, autant d'alphabets incohérents. Les vingt-six lettres de l'alphabet peuvent donner lieu à un nombre de combinaisons vraiment astronomique, qui s'écrit $26^{26}$. Le choix est donc pratiquement infini pour fabriquer des alphabets incohérents. Supposons qu'on se borne à fabriquer trois mille réglettes portant chacune une combinaison différente de l'alphabet. Appliquons quelques-unes seulement de ces réglettes sur un cylindre tournant, qui comportera une *réglette-repère* sur laquelle est inscrit l'alphabet dans son ordre normal. Nous avons ainsi constitué un tableau dans lequel on peut noter mécaniquement (par rotation du cylindre et par indication du rang alphabétique normal) n'importe quel caractère perdu dans l'imbroglio du système.

La transmission par message des deux « coordonnées » (angle de rotation et case alphabétique) permet aux correspondants de retrouver les lettres du texte transmis. La convention devra seulement porter sur les réglettes *choisies* parmi les trois mille dont on est censé disposer. Ces réglettes à alphabets incohérents sont, d'ailleurs, arbitrairement numérotées par les correspondants eux-mêmes. Les chances de décrypter un message transmis dans ces conditions sont nulles pour qui n'a pas *d'abord surpris la convention des correspondants.*

Et, ici, nous touchons au défaut inévitable relatif aux machines à cryptographier, comme d'ailleurs au système de correspondance par codes-dictionnaires qui, eux aussi, peuvent être volés. La frontière de l'espionnage sera toujours le contre-espionnage.

Le procédé mécanique des alphabets incohérents relève de la méthode cryptographique générale dite de « transposition ». Elle remplace, nous venons de le voir, le brouillage systématique. à périodes successives, par le brouillage systématique en extension, sur un ensemble de caractères étalés en un tableau préparé d'avance. La méthode de substitutions est essentiellement « arithmétique ». La méthode de trans-

position est « géométrique ». L'une de ses formes les plus anciennes consiste dans le dessin de « grilles » à cases opaques et transparentes conventionnellement disposées, qui, appliquées à un texte conventionnel n'ayant pas de sens particulier, permettent de lire, à travers les seules cases claires, la suite des lettres choisies pour fournir le sens voulu. Dans ce cas, ce sont les grilles qui font l'objet de la correspondance.

D'ailleurs, tous les procédés peuvent se combiner entre eux. Exemple : les correspondants peuvent se servir de grilles pour se transmettre seulement des « mots-clés ». Autre exemple : on peut se transmettre un chiffrage relatif à un code, après l'avoir lui-même traité par « substitution » ou par « transposition ». Tout cela rend le mystère de plus en plus impénétrable, mais n'élimine pas le cas toujours plausible de trahison.

Voici, par contre, une machine véritablement merveilleuse parce qu'elle élimine radicalement ce risque. Cette machine fonctionne également par « transposition ». Seulement, elle traite non plus des caractères (lettres ou chiffres), mais les traits d'un dessin ou d'un autographe, les nuances d'un document photographique.

## Le cryptographe Belin

Le problème auquel s'est attaché M. Edouard Belin, l'inventeur bien connu du « bélinographe », est d'adapter cet appareil transmetteur d'images aux usages militaires et diplomatiques pour la transmission directe, *sans intermédiaire*, entre les intéressés, des documents les plus variés : plans, photographies et autographes.

Ce dernier cas résout évidemment, *ipso facto*, le problème cryptographique.

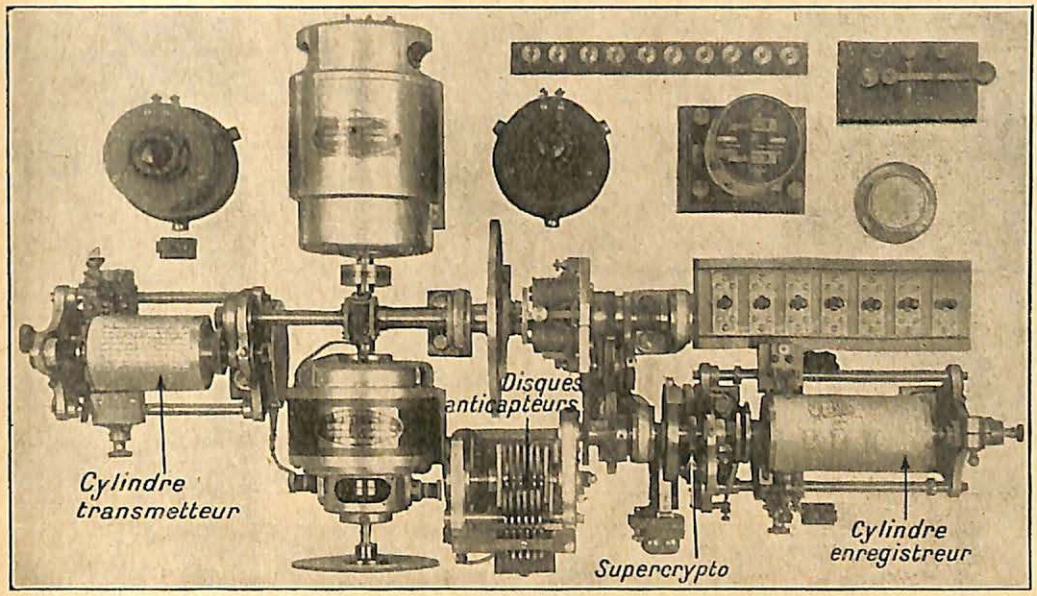


FIG. 2. — VUE EN PLAN DU CRYPTOGRAPHE « BELIN »

*Le cylindre transmetteur et le récepteur figurent simultanément sur cette image. Le dispositif cryptographique réside dans le brouillage des rotations de ces cylindres sans que leur synchronisme soit rompu. Il se compose d'un premier dispositif : les* disques anticapteurs *(voir détail sur figure ci-après) et le* supercrypto *composé d'un système d'engrenages très spécial, également détaillé dans la figure suivante.*

Le document à transmettre est placé sur le bélinographe, appareil aujourd'hui classique en matière de télégraphie avec ou sans fil. Mais, en l'espèce, l'appareil est réglé, comme nous allons l'expliquer, sur un jeu particulier de combinaisons.

La réception s'effectue sur un appareil semblable et réglé naturellement sur *le même jeu* de combinaison, car, s'il n'y avait pas la nécessité d'une clé, il n'y aurait pas secret.

Voici donc la nouveauté : même si, par suite d'une indiscrétion, les combinaisons conventionnelles étaient connues d'un tiers, celui-ci ne pourrait s'en servir pour capter le message téléphotographique. En effet, les deux appareils correspondants, accordés ensemble, sont soumis à l'obligation rigou-

reuse d'être mis en route *simultanément*.

Le principe fondamental est le suivant : étant donné qu'un document téléphotographié exige, pour être nettement lisible, une très grande précision de synchronisme entre le cylindre transmetteur et le cylindre récepteur (1), il s'agit de rompre ce synchronisme *suivant un rythme précis* qui soit le même dans les deux postes. C'est la fonction que remplit le nouvel organe adapté par M. Belin à son appareil primitif.

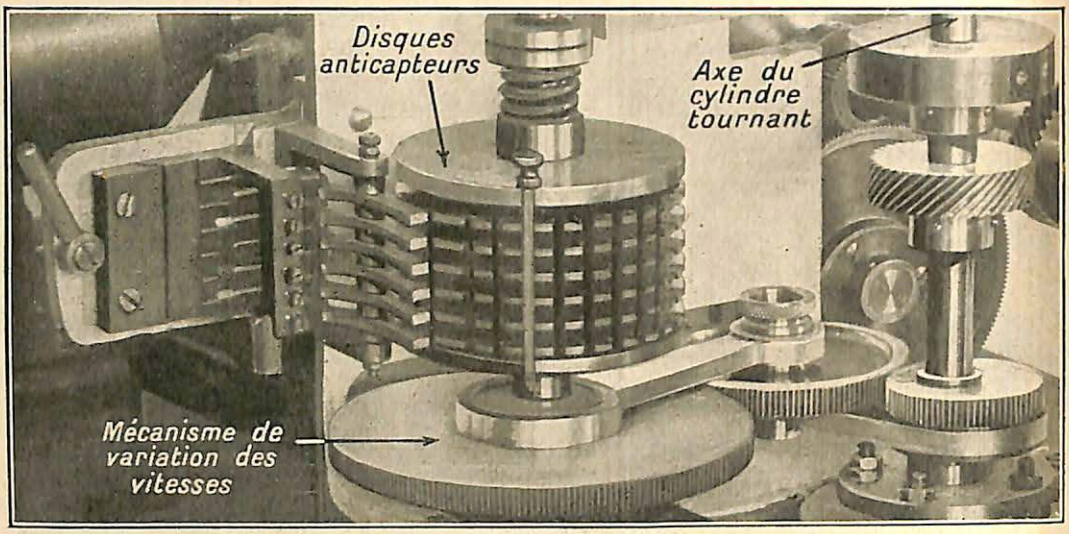


FIG. 3. — DÉTAILS DU DISPOSITIF DE BROUILLAGE DU CRYPTOGRAPHE « BELIN »

*On aperçoit ici les disques anticapteurs, qui actionnent des contacteurs destinés à donner des « tops » parasites irréguliers qui déroutent un récepteur non averti de la « clé » de ces disques pour la détermination du véritable « top » servant d'origine à la rotation. Les vitesses de rotation varient, d'ailleurs, d'une manière continue, grâce au jeu d'engrenages horizontaux visibles à droite du système anticapteur. Ces engrenages, qui commandent la rotation du cylindre enregistreur, se composent de trois roues dentées en nombres « premiers », dont l'une est excentrée et dont la troisième tourne en « satellite ». Dans ces conditions, la rotation du cylindre varie d'une manière absolument imprévisible de qui ne possède pas* les mêmes engrenages *et la « clé » de leur position relative. Aucun synchronisme n'est réalisable sans ces renseignements.*

Le crypto-télégraphe, inventé par l'auteur, atteint ce but en arrêtant les cylindres (transmetteur et récepteur) après chaque tour, tout en laissant subsister, entre deux tours successifs, des écarts de temps variables. Ces écarts sont caractérisés par l'un des deux nombres qui constituent la combinaison. Il est bien évident qu'un observateur espion n'a aucune raison de donner un tel régime de marche à son appareil. Il s'ensuit que les divers points constitutifs d'une lettre vont exactement se placer les uns à côté des autres chez le véritable destinataire (jouissant du rythme secret), tandis que ces mêmes points se jettent au hasard sur la feuille de l'appareil auquel ils ne sont pas destinés. Cette feuille prend bientôt l'aspect que lui donnerait un enfant l'aspergeant d'encre avec un pinceau (voir fig. 4, page 105.)

On objectera que l'observateur espion pourrait, avec beaucoup d'attention, saisir à l'oreille les « tops » par lesquels se transmettent les temps d'arrêts rythmés des cylindres. Ceci est prévu. Des tops parasites sont lancés par un organe accessoire durant le temps d'arrêt des cylindres. Le vrai destinataire ne les enregistre donc pas, tandis que l'appareil espion les subit pêle-mêle.

Cet effet est assuré, dans l'appareillage cryptographique Belin, par le jeu des « disques anticapteurs », qui, par leurs dentelures irrégulières, commandent (à la manière de cames) les leviers des contacts électriques — ceux-ci assurant les écarts de temps variables entre deux tours consécutifs des cylindres.

La figure de la page 103 montre l'emplacement de ces disques sur le dispositif général. La figure de la page 104 montre ces disques en détail. Sur cette même figure,

(1) Nous supposons connu du lecteur le principe général des appareils téléphotographiques et, notamment, du bélinographe décrit dans *La Science et la Vie*, n° 156, page 451.

juste au-dessous des disques, on aperçoit un système d'engrenages dont nous devons maintenant signaler la fonction, non moins capitale.

### Variation continue des vitesses des cylindres d'après une seconde « clé »

Une objection pouvait encore être faite au système précédent.

Imaginez que l'observateur espion capte le bélinogramme sur un long ruban de papier. Les « points » du dessin transmis s'y inscrivent fatalement en « périodes » qui correspondent chacune à un tour de cylindre.

Quel que soit le rythme des arrêts intermédiaires, il est « possible », bien que très malaisé, de découper dans le ruban des « tranches », qui, juxtaposées (à la manière des lignes réglées de façon *très serrée* d'une feuille de papier) pourront donner l'image recherchée. Opération très difficile, mais non pas rigoureusement impossible.

Pour parer à cette objection, M. Belin a imaginé de superposer un second brouillage au brouillage précédent. Il y parvient par le dispositif d'engrenage dont nous venons de parler, qu'il dénomme « supercrypto » et dont voici le principe : les *deux axes* du cylindre transmetteur et du cylindre récepteur (réunis ici sur la même machine) se commandent par deux roues dentées *d'inégal diamètre*, qui, au lieu d'être en prise directe, sont reliées par une troisième roue « satellite ». Suivant les positions initiales relatives des trois roues (dont les *nombres de dents* respectifs sont d'ailleurs premiers entre eux afin d'éviter toute répétition périodique simple), *les origines des rotations des deux cylindres se trouvent changées.* Et, une fois le mouvement amorcé, un tel engrenage assure une variation perpétuelle et imprévue des vitesses de rotation. Imprévisible tout au moins de qui ne possède pas la clé du dispositif, c'est-à-dire la position initiale des trois roues dentées.

Grâce au « supercrypto », la réception sur ruban donnerait, pour deux rangs successifs de points tirés d'une même image, *des longueurs inégales* et *variables dans leur inégalité*, puisque, désormais, chaque tour de cylindre qui fournit une tranche d'image, la fournit à une vitesse différente. Seul, un appareil récepteur dont le « supercrypto » est accordé à celui du transmetteur, peut rétablir le synchronisme.

Ainsi, l'appareil « cryptographe univer-

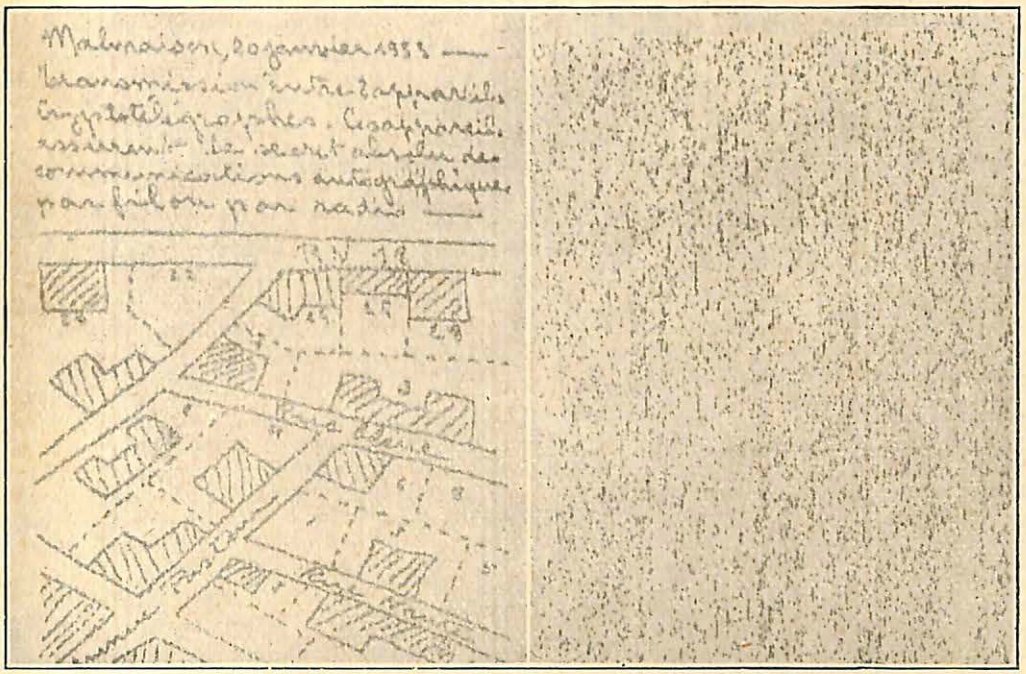

FIG. 4. — EXEMPLE D'UNE TRANSMISSION BROUILLÉE SUR CRYPTOGRAPHE « BELIN »
*A gauche, un texte en clair et un plan, tels qu'ils sont transmis. A droite, la réception illisible de l'observateur espion privé des « clés » nécessaires pour établir le synchronisme de la transmission et de la réception.*

sel » Belin résout absolument le problème des transmissions secrètes — que ces transmissions s'effectuent entre deux postes éloignés (par fil ou sans fil) ou qu'elles s'effectuent entre deux cylindres juxtaposés sur la même machine — le transmetteur étant affecté au « chiffrage », le récepteur au « déchiffrage », ou inversement. Dans ce cas, l'appareil est devenu un cryptographe de bureau, tout comme les machines alphabétiques.

### Conclusions pratiques

Nous nous abstiendrons de critiquer les différentes méthodes de cryptographie mécanique exposées ici. Nous remarquerons seulement que chacune d'elles a sa justification, suivant les cas spécifiques. Entre postes de commandement importants et distants l'un de l'autre, le système Belin a un rôle capital à jouer. Mais le document écrit, à porter par messager secret ou à télégraphier sur les lignes pubiiques, conserve son utilité : les machines en assurent le chiffrage et le déchiffrage ultra-rapide.

Et, par-dessus tout, les méthodes manuelles, dont la complexité peut encore dépasser celle des machines, ne devront pas être délaissées. Une machine se détraque. Les services nationaux doivent toujours posséder une excellente équipe de cryptographes manuels... et de « cryptologues » exercés à percer l'énigme, souvent grâce à leur instinct plutôt qu'à des règles fixes.

CHARLES BRACHET.

## 1934 MARQUE UN NOUVEL ESSOR DE LA CONSTRUCTION AUTOMOBILE AMÉRICAINE

Nous avons eu déjà l'occasion (1) de signaler la reprise marquée que connaissait la construction automobile américaine depuis le début de l'année 1934. Cette impression se trouve aujourd'hui entièrement confirmée par les chiffres et les documents officiels tout récents. Déjà, en 1933 — avant même que fussent appliquées les mesures exceptionnelles prises par le président Roosevelt — cette puissante industrie avait réussi à augmenter sensiblement ses ventes. Un seul chiffre permettra de mesurer l'ampleur de cette reprise : en 1932, la production américaine avait été de 1.431.494 véhicules ; en 1933, cette production a atteint 2.025.025 voitures ou camions (40% en plus). Les perspectives de 1934 apparaissent, d'ores et déjà, comme encore plus satisfaisantes : pour les quatre premiers mois de cette année, la production est en hausse, sur la période correspondante de 1933, de 94 % pour les voitures de tourisme et de 161 % pour les véhicules industriels ! Pour cette dernière catégorie de véhicules, le niveau des ventes a déjà regagné celui du début de 1930 et certains spécialistes estiment que ce niveau sera atteint également en fin de cette année pour les voitures de tourisme (3.500.000 autos).

Les exportations sont, au surplus, en sensible progrès : leur accroissement a porté, en 1933, sur plus de 23.000 voitures et de 19.000 camions, par rapport à 1932, sous forme de véhicules complets ou de pièces détachées.

Ce remarquable regain d'activité dans l'une des branches les plus importantes de l'industrie américaine est incontestablement imputable à cette massive « injection d'argent frais », que les nouveaux organismes de crédit instaurés après la fermeture générale des banques ont pratiquée dans l'économie américaine : le fait est particulièrement frappant pour les achats d'automobiles dans la région agricole de l'Ouest, dont le pouvoir d'achat s'est trouvé brusquement reconstitué. La diminution des ressources des classes moyennes américaines se traduit cependant par la faveur spéciale dont jouissent les voitures à très bas prix. Aussi, les constructeurs américains ont-ils dû, sous l'aiguillon de la concurrence très vive qui s'exerce outre-Atlantique, faire de sérieux efforts vers la réduction des prix de vente, bien que, cependant, la promulgation des codes ait déterminé une augmentation de 15% dans les prix de revient. La production américaine porte aujourd'hui, à raison de 80%, sur des voitures d'un prix de gros inférieur à 500 dollars (7.585 francs).

Certaines marques, telles que « Willys-Overland », ont mis en vente, au début de cette année, une 4 cylindres, au prix de 395 dollars (6.000 francs), et « Beacan », à 350 dollars (5.300 francs).

Ces prix étonnants — du moins pour le public français — laissent évidemment à ces constructeurs une marge bénéficiaire. Ils traduisent la parfaite organisation et les judicieuses conceptions commerciales de l'industrie américaine. Nul doute que cette modicité des prix ne soit le facteur déterminant de la reprise constatée dans cette industrie qui a su rapidement s'adapter à des conditions économiques entièrement nouvelles. Ce succès est, au surplus, l'œuvre d'un cadre de techniciens hors de pair, comme le résultat de programmes de production faits à longue échéance et sainement conçus au point de vue financier (judicieux amortissement réparti sur de longues séries).

(1) Voir *La Science et la Vie*, n° 202, page 332.