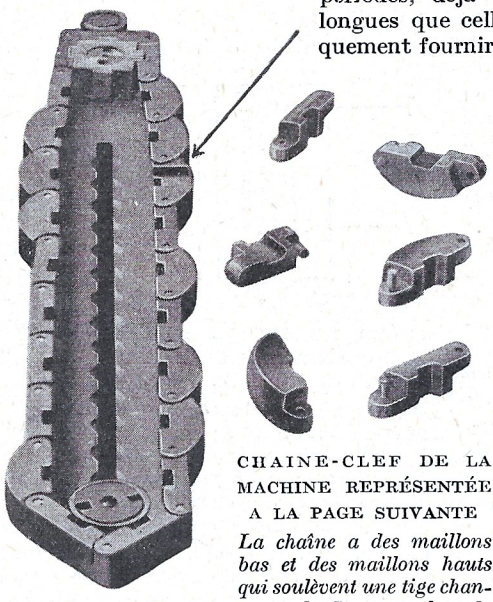
en passant par un dispositif qui permet à l'appareil de tourner sans gêner les connexions électriques, aboutissent à des aimants faisant mouvoir les leviers portant les caractères imprimeurs de la machine à écrire. Dans une position initiale du disque mobile, et pour un dispositif donné de plots, supposons qu'en frappant la touche A, nous fassions imprimer *a*, en frappant B, *b*, etc... Faisons tourner d'une lettre le disque mobile. En frappant A, nous imprimons *b*, en frappant B, *c*, etc... C'est donc bien le système à cadrans que nous avions considéré. Le mouvement du disque mobile est réglé par un équipage d'engrenages qui le fait tourner, après qu'on a imprimé chaque lettre, d'un angle correspondant, soit à une, soit à deux, soit à x lettres. La loi de ce mouvement peut être très compliquée, et les organes mécaniques la reproduiront sans erreurs, tandis qu'avec un cadran mû à la main, les erreurs pouvant être fréquentes.



CHAINE-CLEF DE LA MACHINE REPRÉSENTÉE A LA PAGE SUIVANTE

La chaîne a des maillons bas et des maillons hauts qui soulèvent une tige changeant le sens du mouvement de l'organe dont la fonction est d'assurer la correspondance du texte clair au texte chiffré.

En appliquant le même principe, on a employé des disques mobiles portant des plots sur les deux faces, mais les connexions entre les plots de la face antérieure et ceux de la face postérieure sont réalisées de telle manière que les séries des plots de ces deux faces constituent des alphabets différents. Un plot d'une face correspond, par exemple, avec celui qui se trouve à deux lettres plus loin, son voisin correspond à celui qui se trouve à six lettres. Il y aurait donc, même sans rotation, substitution des lettres ; avec la rotation, la substitution change constamment et le chiffrement se complique.

La période de tels systèmes peut facilement être augmentée. Au lieu de ne mettre qu'un disque mobile, on peut en juxtaposer plusieurs : l'action du premier sera modifiée par le second de la même manière que si l'on avait fait deux chiffrements successifs. Si le premier substituait à la lettre du clair celle qui la suit à deux rangs, par exemple, et que le deuxième substitue à la lettre qu'il reçoit du mécanisme celle qui suit cette dernière à trois rangs, il n'importera pas au résultat que l'opération qui décale la lettre du clair de 2 + 3 soit faite d'abord avec une impression intermédiaire de cette lettre + 2, comme on l'aurait fait avec un cadran à main ordinaire, puis avec un nouveau chiffrement ajoutant 3 à ce décalage, ou que toute l'opération du décalage de 5 se fasse instantanément à travers la machine.

Un autre équipage d'engrenages réglera le mouvement du deuxième disque. Les deux périodes, déjà individuellement plus longues que celles que pouvait pratiquement fournir le cadran à main, se multiplient l'une par l'autre. On peut mettre autant de disques que l'on veut. Au lieu de laisser les connexions dans un ordre régulier tel que les lettres, quand tous les disques sont à une position initiale, se succèdent dans l'ordre de l'alphabet, on peut croiser ces connexions de manière que le disque qui reçoit un A donne un *m* et donne pour B, non pas *n* mais *k*, par exemple. (Lorsque les listes de substitution sont brouillées, le décryptement est plus difficile). On arrive ainsi à des périodes et à des mélanges qui semblent rendre les cryptogrammes pratiquement intraduisibles.

Nous avons décrit ici le principe sur lequel ont été basés un certain nombre de types de machines. Elles impriment le texte cryptographié, et, en général et comme vérification, impriment aussi le texte clair sur une autre bande de papier, par le fonctionnement de la première partie de l'appareil comme machine à écrire simple. De telles machines donnent des cryptogrammes que l'on peut théoriquement considérer comme indéchiffrables, mais à la condition que les correspondants soient maîtres d'éléments, tenus par eux secrets, qui empêchent tout possesseur d'une machine de même type de traduire leur correspondance.

Il faut donc que tous les appareils sor-