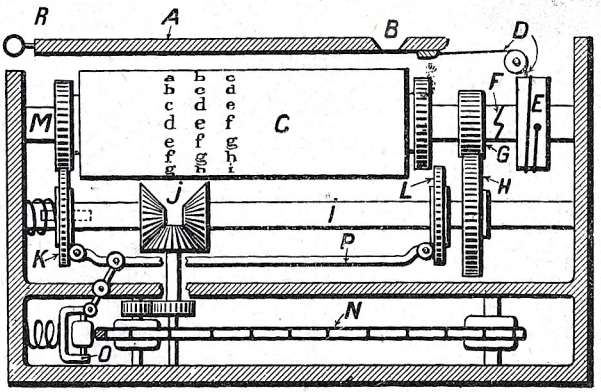
face d'un repère *R*. En même temps, par l'intermédiaire d'un fil de traction, on fait mouvoir un cylindre portant des alphabets et se déplaçant devant la fenêtre *B* où apparaît la lettre du cryptogramme. Une chaîne-clef à maillons épais ou minces a pour effet de modifier, suivant la convention qu'elle rend concrète, le sens des mouvements de la bande et, par suite, la lettre correspondant à une lettre du clair.

Il est à remarquer qu'un grand nombre de machines ne donnent pas des cryptogrammes aussi compliqués que ceux dont nous venons d'examiner la formation.

Certaines d'entre elles se contentent même de donner une substitution simple, le déclenchement de la touche *A* donnant, par exemple, toujours un *m* : en changeant les touches au moyen d'étiquettes, on obtiendrait ce résultat avec une machine à écrire ordinaire. D'autres donnent une substitution double à période courte en employant un procédé, analogue à celui qui imprime les majuscules dans certaines machines : les leviers portent plusieurs lettres et un système à came élève ou abaisse le papier par rapport à cette série de lettres, si bien que l'attaque d'une touche fait imprimer l'une ou l'autre d'entre elles. Mais ces appareils n'assurent pas la sécurité qu'on est en droit d'exiger.

Toutefois on peut assurer qu'il existe certains types de machines à cryptographier, qui, mis dans les mains d'un dactylographe attentif (les erreurs de frappe de touches peuvent, avec certains appareils, avoir de graves conséquences) sont parfaitement aptes à donner toute sécurité pour la pratique de la correspondance secrète.

Nous ne suivrons pas les inventeurs lorsqu'ils prétendent baser l'excellence de leur machine sur le nombre de combinaisons que l'on peut obtenir en modifiant les pièces de leur appareil. Il est des éléments du mécanisme que le constructeur peut bien modifier, mais que les correspondants ne manieront qu'avec répugnance. Si, par exemple, il faut démonter l'appareil pour changer les connexions des plots dans les disques, on admettra que, dans la pratique, cette opération ne se fera que fort rarement une fois la machine sortie de l'usine, et qu'un groupe de correspondants nous donnera constamment des cryptogrammes faits avec les mêmes disques, et ne différant que par la position initiale de ceux-ci. Pourtant, les fabricants énoncent, dans leurs prospectus, un chiffre avec beaucoup de zéros correspondant au nombre de combinaisons possibles des lettres commandées par les connexions des plots et au total des modifications du nombre de dents des roues d'engrenages. Ces nombres « astronomiques » ne signifient pas grand'chose, à notre avis. Ce qui est important, c'est la facilité offerte aux correspondants d'employer des clefs nombreuses, c'est-à-dire de changer facilement les éléments de départ et la période. Ceci fait, comme les télégrammes de mille lettres sont bien rares, il nous est à peu près indifférent que le constructeur nous annonce que la même série de lettres du clair ne sera représentée par la même série de lettres du cryptogramme qu'au bout de *n* trillons caractères ou au bout de T quintillions. Si l'on peut découvrir le moyen de retrouver les conventions que les correspondants doivent établir entre eux, et qui doivent être simples si l'on veut mettre la machine dans les mains d'une personne non cryptologue, les considérations théoriques sur le nombre des combinaisons possibles à réaliser en changeant les pièces de la machine sont sans inté-



MACHINE A CRYPTOGRAPHIER A MAIN

A, *règle portant les lettres du clair, et par le fil* D, *enroulé sur le tambour* E, *faisant tourner (seulement dans un sens, grâce au rochet* F) *la roue* G *entraînant la roue* H *et l'axe* I *qui transmet le mouvement à la chaîne-clef* N. *Les maillons minces ou épais poussent le galet* O *et, par l'intermédiaire du levier* P *mettent en prise la roue* K *ou la roue* L *qui peuvent glisser sur les deux parties de l'axe* I *(tournant en sens contraire) et engrener (l'une ou l'autre), avec une des roues dentées fixées au cylindre des lettres* C *fou sur l'axe* M. C *a des mouvements alternatifs qui amènent les lettres du cryptogramme sous la fenêtre* B.