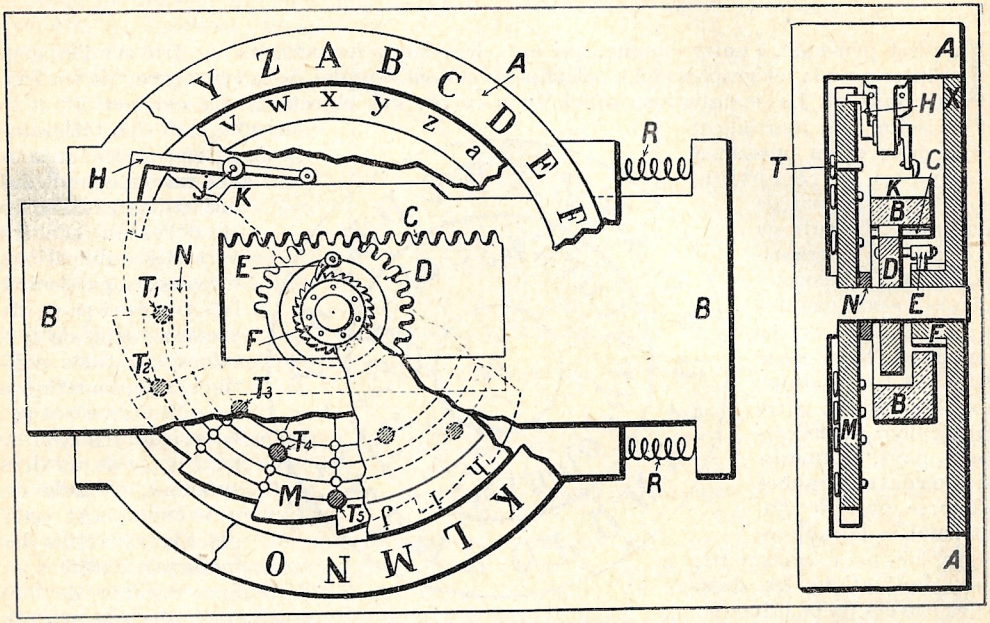
les machines à cryptographier, dont plusieurs types intéressants et vraiment ingénieux ont été brevetés depuis quelques années.

Avant d'expliquer comment ces machines fonctionnent et quels sont leurs avantages, nous croyons utile d'exposer brièvement quelques principes de cryptographie.

Le public est surtout habitué à l'emploi des codes ou dictionnaires chiffrés. Ce sont des répertoires où figurent, en face des mots de la langue ou de phrases usuelles, des groupes de lettres ou de chiffres. L'emploi de ces dictionnaires est souvent commandé par une simple raison d'économie : un groupe de cinq chiffres, en effet, est taxé pour un mot. Il est donc plus économique de faire transmettre le groupe 21419 que la phrase : « Nous regrettons l'erreur commise dans... », que ce groupe représente dans le code Veslot, et qui comprend six mots. Bien plus, comme l'administration ne taxe que comme un mot un groupe de dix lettres, quand ces lettres forment un ensemble à peu près prononçable, les codes renferment souvent des groupes de lettres au lieu de groupes de chiffres, et le même code Veslot nous permet d'envoyer à un correspondant, par le seul groupe, taxé pour un mot, *liraxconeæ*, la phrase : « En me référant à ma dernière lettre, j'ai encore à ajouter que je vous remercie de la complaisance que vous avez montrée dans cette affaire ». Mais le grand nombre de codes vendus dans le commerce assure déjà un certain secret aux correspondants, à cause de l'incertitude qui peut régner sur le document employé pour chiffrer, et certaines firmes ont, d'ailleurs, des dictionnaires établis pour elles seules, dont elles confient des exemplaires à des personnes sûres, et qui ne sont pas à la disposition des tiers.



CADRAN AUTOMATIQUE POUR CHIFFRER, VU EN PLAN ET EN COUPE

A, *bâti de l'appareil portant un alphabet circulaire et un axe central ;* B, *poussoir entraînant par la crémaillère* C *la roue dentée* D, *qui, elle-même, à l'aide du cliquet* E, *fait tourner (en sens direct seulement) la roue* F *solidaire du cadran mobile* X ; *(le poussoir* B, *ramené par les ressorts* R, *ne fait pas tourner* E *dans son trajet de retour) ;* N, *butée fixée à* B, *et limitant son mouvement vers la gauche, et par conséquent la rotation de* D, *de* F *et de* X ; T_1 T_2 *etc., chevilles fixées à volonté dans les trous d'une roue* M *et arrêtant la butée* N. *La roue* M *avance d'un angle constant après chaque effort sur* B, *grâce au cliquet* H *basculant autour de l'axe* j, *quand il est mû par la portée* K *de* B.

En dehors des dictionnaires, il existe des procédés de cryptographie, parfois désignés sous le nom de *systèmes alphabétiques*, où les cryptologues travaillent directement sur les lettres ou les syllabes de la phrase en clair. Les procédés employés dans cet ordre d'idées peuvent rentrer dans deux grandes catégories : *transposition* et *substitution*.

Dans les systèmes de transposition, les lettres du texte conservent leur personna-