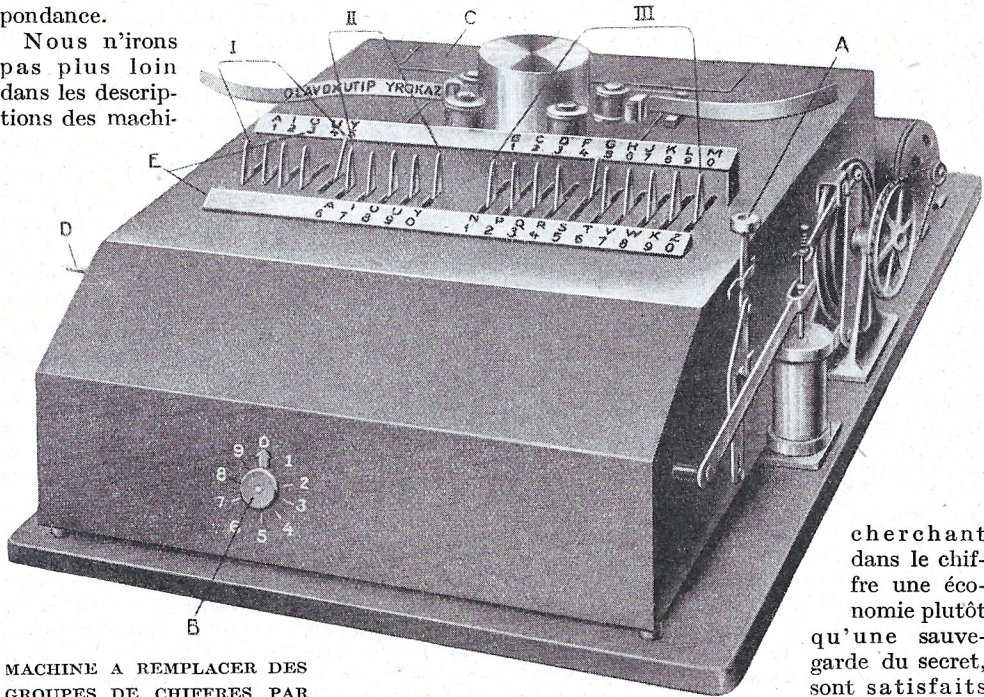


rêt. Or, il est des machines qui, par leur construction, restreignent tellement les possibilités théoriques, qu'un petit nombre d'essais, avec des éléments favorables dont disposent souvent les services de décryptement (tels que des hypothèses précises sur le contenu d'un télégramme) permet de retrouver la forme des conventions entre expéditeur et destinataire et de traduire toute la correspondance.

Nous n'irons pas plus loin dans les descriptions des machi-

ou trop coûteux. Les premiers n'assurent pas le secret. Les autres, lorsque les correspondants sont nombreux, exigent une dépense de premier établissement trop élevée.

En attendant l'apparition de machines faciles à transporter, à utiliser et d'un prix raisonnable, il est à croire que les anciens systèmes resteront pratiqués par la plupart des correspondants, aussi bien par ceux qui,



MACHINE A REMPLACER DES GROUPES DE CHIFFRES PAR

DES GROUPES DE LETTRES PRONONÇABLES, EN CHANGEANT LA CORRESPONDANCE DES LETTRES ET DES CHIFFRES

I, II, III, groupes de leviers à pousser suivant les chiffres du clair (ou, au déchiffrement, suivant les lettres du cryptogramme) ; E, indication des chiffres ou lettres ; A, touche donnant l'impression sur la bande C que l'on voit se dérouler en haut, à gauche ; D, repère donnant la position primitive de la clef.

cherchant dans le chiffre une économie plutôt qu'une sauvegarde du secret, sont satisfaits des codes où un groupe remplace une série de mots, et ne vont point augmenter leurs dépenses par l'achat de machines

nes. Il en est qui ont pour objet de transformer les groupes numériques donnés par les codes en groupes de lettres prononçables (économie de 50 % sur la taxe), tout en modifiant la correspondance des lettres et des chiffres d'un caractère à l'autre, ce qui assure le secret en même temps qu'une très importante économie. Une machine de ce genre est construite par les adaptateurs de la chaîne-clef que nous avons citée plus haut.

Les machines à cryptographier sont fort rares en France. Il semble, d'après les catalogues des firmes qui les construisent, qu'il en existe un certain nombre à l'étranger. Les types actuels sont, semble-t-il, ou trop simples

coûteuses, que par ceux qui, tenant à garder secrètes leurs affaires, ont des communications assez réduites pour pouvoir se contenter de systèmes classiques ou soigneusement étudiés. Cependant, les grandes administrations, faisant un emploi considérable du chiffre, ne devront pas rester indifférentes aux machines, qui peuvent, comme nous l'avons dit, remédier à certains des défauts de la T.S.F. en rendant facile et sûr l'usage de la cryptographie, et les services de décryptement trouveront, dans l'analyse des cryptogrammes chiffrés avec des machines, les éléments d'études intéressantes.

LIEUTENANT-COLONEL GIVIERGE.