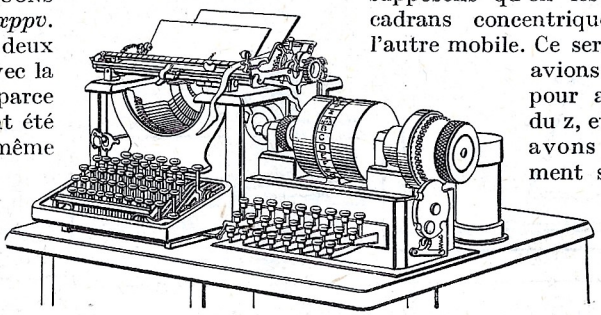
dans le cryptogramme, B, par *d*, C, par *e*, etc...

A B C D E F G H (clair)
c d e f g h i j (cryptogramme)

et ainsi de suite, suivant la même loi, chaque alphabet étant désigné par la lettre qui correspond à A du clair, et les autres lettres suivant dans l'ordre de l'alphabet.

Décidons de chiffrer la première lettre du clair avec l'alphabet B, la deuxième, avec l'alphabet C, la troisième, avec l'alphabet D, puis la quatrième avec l'alphabet B, la cinquième avec C, la sixième avec D, ainsi de suite, en employant pour cette opération trois listes de substitution simple.

Le mot ATTAQUONS sera chiffré *bvwbsxppv*. On voit que les deux A sont chiffrés avec la même lettre *b*, parce que tous deux sont été chiffrés avec le même alphabet de substitution, mais les deux T sont représentés par les lettres *v* et *w*, et *v* représente une fois T et une fois S.



MACHINE A CRYPTOGRAPHIER ANGLAISE, BREVETÉE PAR LA « PATENT DEVELOPING CY. »

Les touches d'une des machines à écrire, sur laquelle on frappe le clair, envoient seulement le courant électrique dans des électro-aimants faisant mouvoir les touches et, par suite, les caractères de l'autre machine. Un disque à plots modifie la correspondance entre la touche frappée et l'électro-aimant imprimeur.

Dans la cryptographie antérieure aux machines, on utilisait ordinairement ces systèmes en employant des clefs ou mots convenus qui indiquaient, par l'ordre des lettres, l'ordre dans lequel on employait les alphabets. De bonne heure, on chercha à simplifier ces chiffrements par l'emploi d'appareils relativement peu compliqués.

On utilisa d'abord la réglette de Saint-Cyr. Figurons-nous deux réglettes accolées. Sur l'une est écrit l'alphabet en clair dans son ordre ordinaire, sur l'autre, un alphabet où les lettres peuvent se trouver dans un ordre quelconque, mais pour nous faire comprendre et nous servir de ce que nous avons dit plus haut, nous prendrons, pour ce deuxième alphabet, la série *a b c d e f*...

Dans une position initiale, A de l'alphabet du clair étant en face de *a* de l'alphabet de la deuxième réglette, c'est-à-dire de l'alphabet du cryptogramme, B sera en face de *b*, C, de *c*, Z, de *z*. Poussons la deuxième règle d'une lettre à gauche, A sera en face de *b*, B, de *c*, etc... et nous aurons la même correspondance entre la lettre du clair, lue sur la première règle et la lettre du cryptogramme (celle qui lui correspond sur la deuxième règle) que dans l'alphabet de substitution *b* indiqué plus haut. (Voir la figure page 223).

En poussant encore la règle d'une lettre à gauche, on aura la substitution de l'alphabet *c*, etc... L'alphabet à prendre pour chiffrer, indiqué par la clef, sera obtenu en amenant la lettre de la clef, lue sur la deuxième règle, en face de l'A de la première règle. On chiffrera alors la lettre du clair correspondante en lisant cette lettre sur la première règle et en cherchant sur la deuxième règle la lettre qui lui correspond exactement.

Au lieu d'écrire les lettres sur deux règles, supposons qu'on les écrive sur deux cadrans concentriques, l'un fixe et l'autre mobile. Ce sera comme si nous avions courbé nos règles pour amener l'A à côté du z, et tout ce que nous avons dit précédemment s'applique encore.

Les méthodes de décryptement de tous ces systèmes reposent sur la recherche de la longueur de la clef. Si, en effet, la clef est de cinq lettres, on sait que les première, sixième et onzième lettres sont chiffrées avec un même alphabet de substitution simple, et dans chacun de ces alphabets, il y a des chances pour que le caractère le plus fréquent corresponde à E du clair. Il est donc d'un intérêt primordial de connaître la longueur de la clef, ou, autrement dit, le nombre de lettres après lequel les alphabets sont repris dans le même ordre, c'est-à-dire la période du cryptogramme. Or, on constate que, plus la période est longue, plus elle est difficile à déterminer. Avec des mots ou des phrases-clefs, les périodes ont ordinairement une longueur définie, mais, avec les cadrans, on peut obtenir mécaniquement des périodes extrêmement longues, et c'est cette possibilité que se sont efforcés d'appliquer beaucoup d'inventeurs de machines à chiffrer.

On conçoit, en effet, que l'on puisse commander le mouvement du cadran mobile par rapport au cadran fixe par un système d'engrenages. Si l'on déplace le cadran d'un angle égal après qu'on a chiffré chaque lettre, et que ce déplacement amène un décalage