d'une lettre, faisant succéder la disposition correspondante à l'alphabet C de notre exemple précédent à la disposition correspondant à l'alphabet B, puis faisant apparaître la disposition D, puis E, etc... on aura épuisé, au bout de vingt-six déplacements, toutes les dispositions correspondant à toutes les positions possibles de l'alphabet et on retombera sur la première position, qui sera suivie des autres dans le même ordre ; on aura une période de 26. Si l'on déplace le cadran mobile de deux lettres, passant de la disposition B à la disposition D, puis F, etc., on retombera sur la première au bout de treize déplacements : période de 13. Si on fait des déplacements inégaux, d'une lettre, deux lettres, trois lettres après le chiffrement de chaque caractère, on aura naturellement des périodes plus ou moins longues.

Le maniement du cadran à la main, lorsque la période des déplacements suit une loi compliquée, est malaisé et sujet à erreur, mais avec une machine, on peut augmenter sans danger la période. La figure page 224 représente un appareil de ce genre. Un poussoir entraîne le cadran mobile d'un nombre de lettres dépendant de l'enfoncement de ce poussoir (une, deux, trois lettres, etc...). Cet enfoncement est limité par la rencontre d'un taquet N avec une cheville T. Chaque fois qu'une lettre a été chiffrée, le mouvement du poussoir fait tourner un disque sur lequel des chevilles T_1, etc. sont plantées, au gré des correspondants, si bien que l'enfoncement du poussoir varie à chaque lettre.

Jusqu'à ces dernières années, on considérait comme suffisant pour la sécurité l'emploi de ces systèmes, dont certains sont déjà extrêmement difficiles à étudier, lorsqu'on n'a pas un grand nombre de cryptogrammes faits avec la même clef. Au cours de la guerre, à la suite sans doute de fuites, révélant l'activité des décrypteurs, on employa couramment des combinaisons de deux des systèmes que nous devons décrire. Ainsi, après avoir chiffré avec un dictionnaire, on fit subir à la série de nombres obtenus des substitutions ou des transpositions ayant pour but de masquer les groupes primitifs et de rendre inutile pour l'ennemi la possession d'un dictionnaire obtenu par trahison. On mélangea, par une transposition, les lettres d'un cryptogramme obtenu par une substitution. Ou encore, on chiffra une deuxième fois avec un cadran et une nouvelle combinaison de déplacements un texte chiffré une première fois avec le cadran que nous reproduisons à la page 223. Dans ce dernier cas, l'analyse des opérations montre que si la période du premier chiffrement est N, celle du deuxième n, le cryptogramme obtenu de la sorte présente une période de $N \times n$.

Ces chiffrements où l'on superpose deux procédés n'assurèrent encore pas une sécurité absolue, et, grâce aux conditions particulières où se produit le trafic des cryptogrammes par T. S. F. en temps de guerre, aux ressources de l'espionnage, à l'emploi, pour des chiffrements très nombreux et très rapides, d'un personnel mal instruit, à l'habileté et à l'entraînement enfin de cryptologues sélectionnés, certaines puissances possédèrent la traduction de correspondances chiffrées avec des systèmes de cette nature.

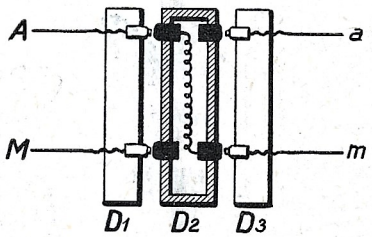

SCHÉMA DU DISQUE MOBILE A CONNEXIONS CROISÉES

Le courant venant de la touche frappée A *ne va pas par le fil* a *à l'électro-aimant qui imprime la lettre* a ; *un fil, à l'intérieur du disque* D_2, *le mène à un autre plot, qui est ici celui qui correspond à l'aimant imprimeur de* m.

Une bonne solution du problème de la sécurité des chiffrements réside dans l'accumulation des opérations successives allongeant les périodes de telle sorte qu'une même suite de lettres du clair ne soit jamais, dans un même cryptogramme ou dans des cryptogrammes successifs, chiffrée par la même suite de caractères (ce qui se produirait si, la première lettre de chaque suite étant chiffrée avec le même alphabet de substitution, les suivantes trouvaient les mêmes alphabets se succédant dans le même ordre). Or, ce qu'il est malaisé de demander à l'homme, la machine nous le fournit sans difficulté, comme nous allons le voir.

Le système à cadran, par exemple, sur lequel nous nous sommes étendus, a donné lieu à des brevets où il est réalisé de la manière suivante : aux vingt-six touches d'une machine à écrire sont reliés, par des fils électriques, vingt-six plots disposés en cercle, à intervalles égaux, sur un disque isolant, qui correspondent aux vingt-six lettres du cadran fixe dont nous avons parlé plus haut. Au contact de ce disque fixe se trouve un disque analogue mobile, avec vingt-six plots au contact des vingt-six plots précédents. Des fils partent de ces plots, et,