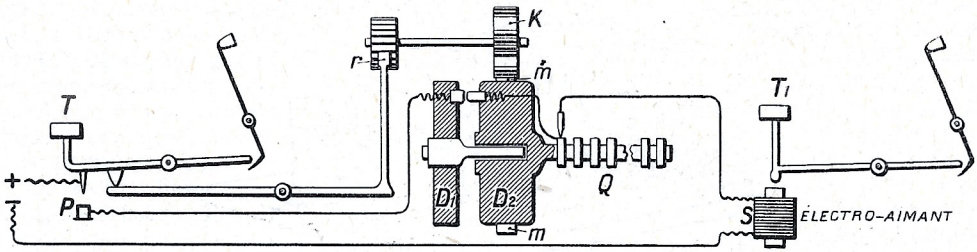
lité propre : A reste A, B reste B, mais l'ordre des lettres dans le texte est mélangé de telle sorte que la physionomie de la phrase ne soit plus reconnaissable. Le mot PARISIEN, par exemple, sera écrit IIAENSRP. La clef du système est la convention qui permet de replacer les lettres dans l'ordre. Cet ordre est souvent indiqué par une clef littérale, mot ou phrase convenue entre les correspondants et dont on numérote les lettres suivant l'ordre de l'alphabet pour indiquer l'ordre de relèvement des colonnes.

De tels systèmes peuvent être combinés à l'infini. Il suffit d'un procédé simple pour fixer l'ordre de *relèvement* des lettres.

Dans les systèmes de *substitution*, les ces *substitutions simples à représentation unique* dans les romans, le *Scarabée d'or*, d'Edgar Poe, les *Hommes dansants*, de Conan Doyle, etc... La traduction, qui est généralement assez facile, est basée sur ce que, dans la plupart des langues, la lettre qui se présente le plus souvent est l'E. On admet donc que le caractère le plus fréquent représente l'E du clair. Partant de cette hypothèse, on s'appuie sur certaines remarques faites dans chaque langue sur les alliances de lettres qui se produisent le plus souvent pour deviner aisément d'autres lettres.

On peut avoir plusieurs caractères ou plusieurs groupes de chiffres pour représenter une même lettre du clair. Ainsi, A



COUPE SCHÉMATIQUE D'UNE MACHINE A CHIFFRER

T, *touche d'une machine à écrire sur laquelle on frappe le clair ;* P, *plot recevant à ce moment le courant de la pile ;* D_1, *disque fixe portant des plots disposés en cercle, chacun d'eux laissant paser le courant dans un des plots du disque mobile* D_2 *;* Q, *série de bagues reliées chacune à un plot de* D_2. *Le courant passe par la bague, un balai et un fil et actionne l'électro* S *agissant sur la touche* T_1 *qui fait imprimer la lettre du cryptogramme;* r, *roue à rochet avançant d'une dent quand on frappe* T *et entraînant* K, *roue à engrenage irrégulier, faisant tourner* D_2, *par l'intermédiaire de la denture* m, *suivant une loi donnée.*

caractères du texte clair sont remplacés par d'autres caractères, au besoin des dessins inventés, ou des lettres d'un alphabet étranger, ou des groupes de lettres ou de chiffres. On peut se contenter d'un tableau de remplacement ou substitution d'après lesquels une lettre du clair est remplacée par un seul caractère du cryptogramme, toujours le même, et où un caractère du cryptogramme représente toujours la même lettre du texte, comme ci-après :

A	B	C	D	E	F	G	H	I	J
b	*e*	*k*	*p*	*i*	*t*	*c*	*u*	*l*	*d*
K	L	M	N	O	P	Q	R		
r	*f*	*a*	*m*	*g*	*q*	*v*	*w*		
S	T	U	V	W	X	Y	Z		
x	*s*	*z*	*n*	*h*	*o*	*y*	*j*		

On écrira, par exemple, le mot ATTAQUE : *bssbvzi*, l'A du clair étant remplacé par *b* du cryptogramme, T du clair par *s* du cryptogramme, etc... Et alors *s* du cryptogramme représentera toujours un T du clair, *b*, un A, etc... On trouvera de nombreux exemples de peut être remplacé par 14 ou par 22 ou par 38 ; B, par 16 ou 18 ou 96. Mais si 14, 22 ou 38 représentent toujours A, etc..., la substitution qui est dite *simple à représentations multiples*, bien que beaucoup plus compliquée qu'une substitution à *représentation unique*, constitue un système encore souvent résolu par les cryptologues entraînés.

Il existe d'autres systèmes, ceux qu'on appelle des *substitutions à double clef*, où un caractère donné du cryptogramme ne représente pas toujours la même lettre du clair et où, par suite, on ne peut pas s'appuyer sur les fréquences pour décrypter. Formons, par exemple, plusieurs tableaux ou listes de substitution simple, l'une, que nous appellerons la liste ou alphabet B, où A clair sera représenté, comme ci-dessous, par *b* du cryptogramme, B, par *c*, C, par *d*, etc...

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

une autre, que nous appellerons la liste ou alphabet C, où A du clair sera remplacé par *c*