$G = \mathbb{Z}_{26}$ $\quad$ 0 ——— 25 $\quad$ A ——— Z $\quad$ $S(A) = \{f : A \to A : \text{biiettive}\}$.

CIFRARIO DI CESARE

stringa $\to$ elemento di G^n $\quad$ problema

1) ci sono poche chiavi

2) analisi frequenziale.

DATO UN KNOWN PLAINTEXT

$x \mapsto y$ $\qquad$ $y - x$ chiave. $\to$ $x + (y - x) = y$

Def: Sia $(G, \circ)$ un gruppo e $(M, +)$ un gruppo abeliano.

Si dice che M è un **G-modulo** se $\exists$

$* : G \times M \to M$ tale che

1) $\forall m \in M \quad Id_G * m = m$
2) $\forall \alpha, \beta \in G \quad (\alpha\beta) * m = \alpha * (\beta * m)$.
3) $\forall \alpha \in G : \forall m, n \in M : \alpha * (m + n) = (\alpha * m) + (\alpha * n)$

G-azione su M

prendiamo $G = A \qquad M = G^n$

$\forall \sigma \in G \qquad \sigma * m = \sigma(g_1 \text{ ——— } g_n) =$

$= (\sigma g_1 \; \sigma g_2 \text{ ——— } \sigma g_n)$

cifrario di Cesare

$A = \text{alfabeto} \qquad G = S(A) \qquad M = G^n$

$\forall \sigma \in G \qquad \sigma * m = (\sigma(m_1) \text{ ——— } \sigma(m_n))$

cifrario con permutazione arbitraria

$\to$ sostituzione monoalfabetica.

Sostituzione polialfabetica.

m

TESTO ABCD DI PROVA

CHIAV EDAU SA REGOLI

k

V E I I

caratteri diversi hanno la medesima codifica in posizioni differenti

$\mathcal{E}$ $K = M = A^n$

$\mathcal{E}(k, m) = k + m$

Esercizio: verificare che il cifrario con chiavi lunghe fanno quanto il messaggio è perfetto.

Supponiamo # chiave = h

messaggio = n ≥ h

Spazio delle chiavi $(\mathbb{Z}_{26}^h, +)$

$k = (k_0\ k_1 \ \_\_\_\_ \ k_{h-1})$

$M \subseteq \mathbb{Z}_{26}^n$ $\forall k \in K, \forall m \in M$

$k * m = (k_0 \ \_\_ \ k_{h-1}) * (m_0 \ \_\_ \ m_{h-1} m_h \ \_\_ \ m_{n-1}) =$

$= (k_0 + m_0 \quad k_1 + m_1 \ \_\_\_\_ \ k_{h-1} + m_{h-1} \ \_\_\_\_ \ k_{(n-1)\%h} + m_{n-1})$

MESSAGGIO DA CIFRARE

k = ABC

ABC ABC AB C A BC ABC AB

MFUSHI IP F

0 1 2 3 4 5 6 7 8 9 10 11

$c_i := m_i + k_{i\%h}$

Problemi

1) frequenza dei gruppi di caratteri.

2) "Sostanzialmente è un cifrario di cesare".

1) ragionare sulle frequenze di seq. di $1, 2, 3, \dots, n$ caratteri e vedere quando queste corrispondono alla frequenza "naturale" di una qualche lingua → k

2) risolvere k cifrari di Cesare in parallelo.

c'è un modo più veloce?

→ Si può ottimizzare la ricerca della lunghezza della chiave

→ INDICE DI COINCIDENZA

↳ definito come la probabilità che prendendo 2 caratteri a caso in un testo questi siano uguali.

IDEA → costruire uno "stream" lungo di caratteri

DATA UNA CHIAVE CORTA → costruire una sostituzione polialfabetica di "periodo lungo"

↓

tale che la stessa seq. di simboli da sostituire compaia "raramente"

$k_1 \rightarrow [\quad] \rightarrow [k_1 k_2 \dots k_N]$

con $N >> |k_1|$

Esempio

$G = (\mathbb{Z}_{26}, +)$ $\quad M = \mathbb{Z}_{26}^N$

chiave $\alpha \in G$

$$\alpha * (m_1\ m_1 \dots m_N) =$$

$$= (m_1 + \alpha\ \ m_{1+2+1} \dots m_{N+2+N})$$

Indice di coincidenza.

Testo di lunghezza = n

f_i = numero di occorrenze del carattere i

prob. che il primo carattere sia i → $\frac{f_i}{n}$ · prob. che il secondo carattere sia i → $\frac{(f_i - 1)}{n-1}$

$$p_i = \frac{f_i}{n} \cdot \frac{(f_i - 1)}{n-1}$$

$$k := \sum_i p_i = \frac{1}{n(n-1)} \sum f_i (f_i - 1)$$

N.B: Se testo casuale $\Rightarrow$ $p_i = \frac{1}{t}$ con t = # caratteri alfabeto $\forall i$

Macchine cifranti → disco cifrante di alberti

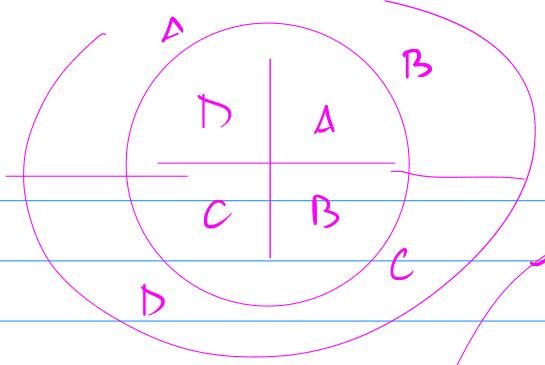
A) Sostituzione polialfabetica ottenuta da una permutazione che è funzione della chiave + me "rotazioni"

↓

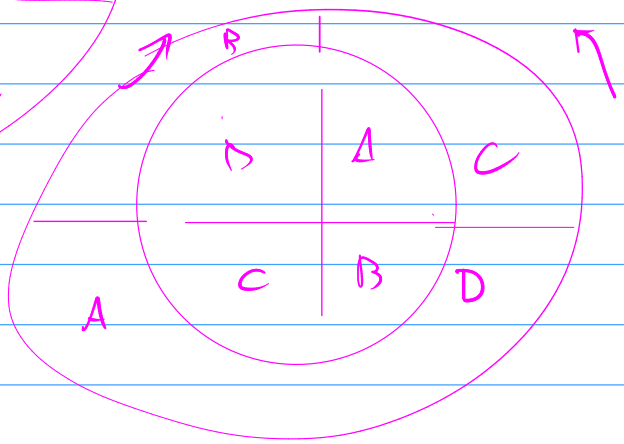
equivalente alla nozione di rotore

→ W.F. Friedman, "Military Cryptanalysis" Pt I, II

(guardare anche 3,4)

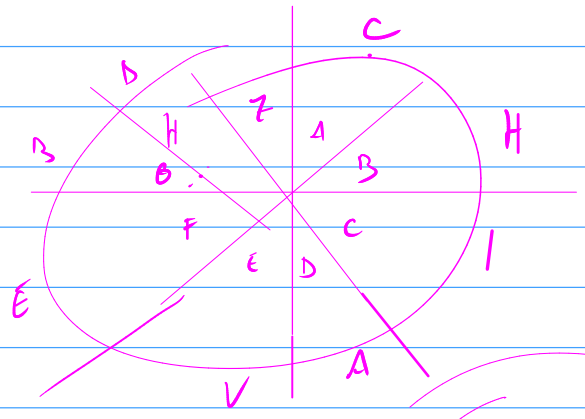


K = B



DISCO CIFRANTE DI ALBERTI

K = CHIAVE



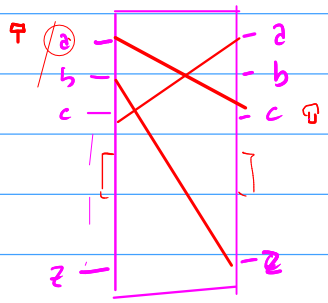
corrisponde una permutazione $\sigma \in S(\mathbb{Z}_{26})$

1 ↓ ↓

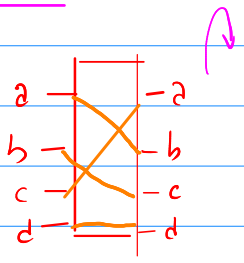
A W

MECCANIZZAZIONE DELLA CRITTOGRAFIA

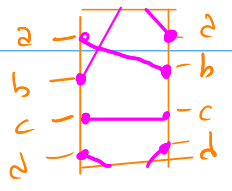
problema: come descrivere un rotore



ROTORE



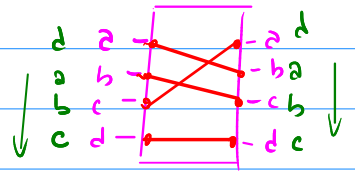
a → b
b → c
c → a
d → d



a → b
b → d
c → c
d → a

Come rappresentare questa azione di rotazione del rotore.

ROT. VERSO CALTO DEL ROTORE



$\equiv$

ROT. VERSO IL BASSO DELLE ETICHETTE ROTORE FISSATO

oss: Sia S_n = gruppo simmetrico su n elementi $(0\ 1\ 2 \dots n-1)$.

Un rotore ρ è un elemento $\rho \in S_n$

chiamiamo ϑ la biiezione $\begin{cases} \mathbb{Z}_n \to \mathbb{Z}_n \\ i \to i+1 \end{cases}$

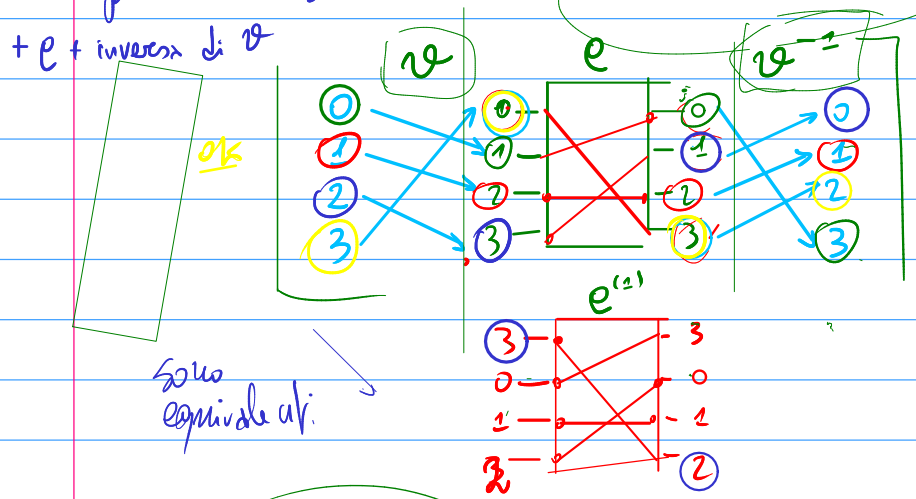
permutazione ciclica.

$$\begin{array}{l} 0 \to 1 \\ 1 \to 2 \\ \vdots \\ n-2 \to n-1 \\ n-1 \to 0 \end{array}$$

una rotazione di ρ di 1 posizione verso l'alto si scrive come

composizione di una permutazione ciclica ϑ + ρ + inversa di ϑ

$$\rho^{(1)} := \vartheta\, \rho\, \vartheta^{-1}$$



ρ	$\rho^{(1)}$
$0 \to 3$	$0 \to 3$
$1 \to 0$	$1 \to 1$
$2 \to 2$	$2 \to 0$
$3 \to 1$	$3 \to 2$

Solo equivale a:

$\vartheta : i \to i+1$

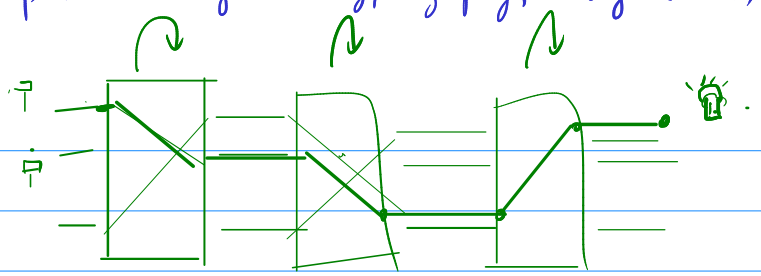
ρ: rotore

$$\rho^{(1)} = \vartheta\, \rho\, \vartheta^{-1}$$

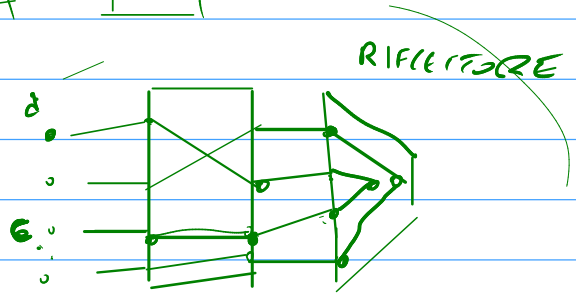
$$\boxed{\rho^{(i)} = \vartheta^{i}\, \rho\, \vartheta^{-i}}$$

$A \sim B \iff \exists\, M \in GL(n,k) : A = M^{-1} B M$

→ A. G. Konheim, "Computer security and cryptography", Wiley (2007)

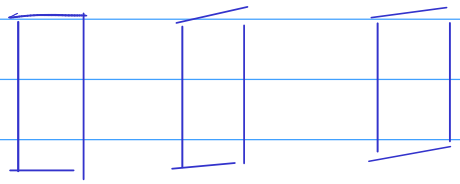


26^3

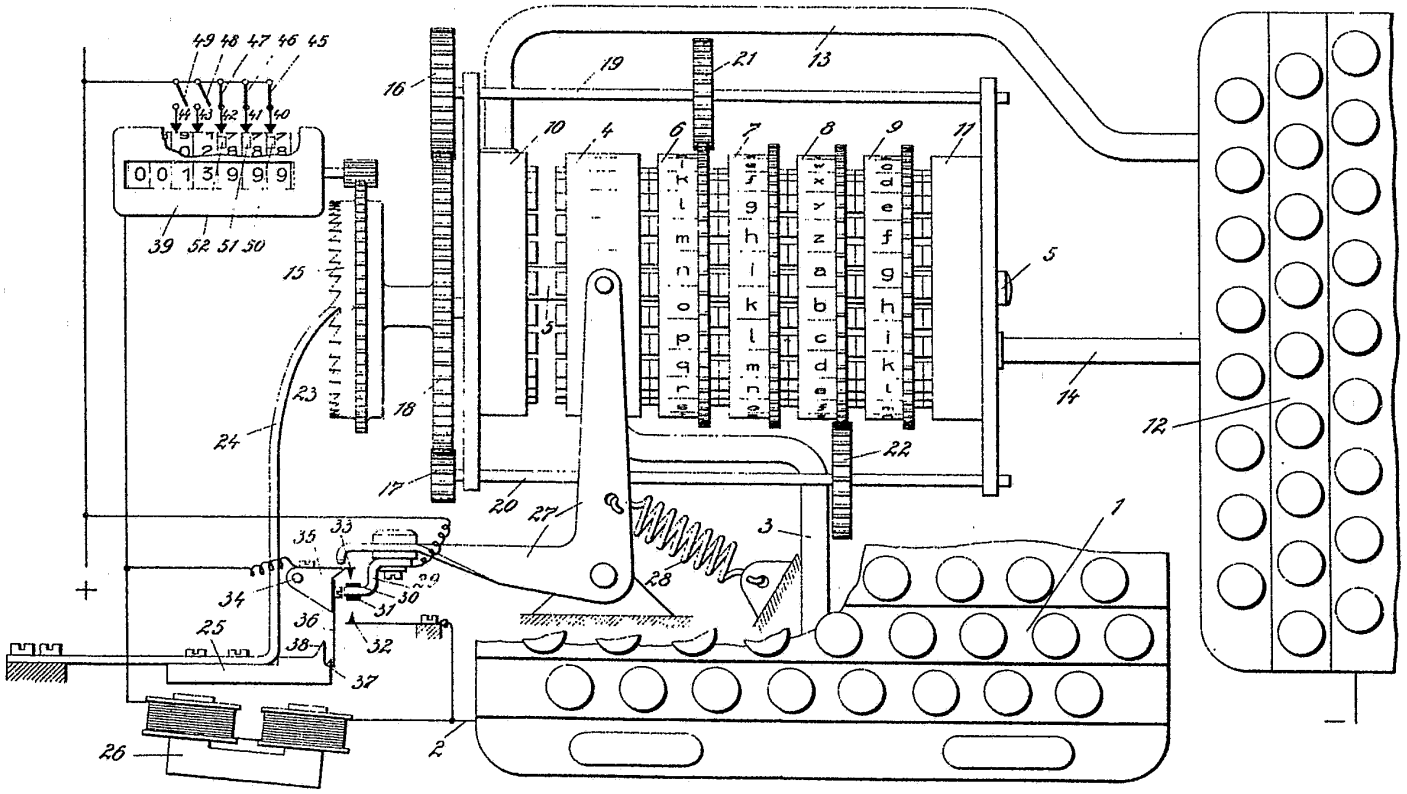


una macchina con un riflettore produce degli scambi nel resto in particolare 1) codifica e decodifica sono la medesima operazione
2) nessun carattere è codificato in se stesso.

→ Questo espone la cifratura ad attacchi di tipo known-plaintext (cribbing)



Zu der Patentschrift 383594
Kl. 42n Gr. 14



Zu der Patentschrift **452 194**
Kl. 42n Gr. 14

Blatt I.

Abb. 2.

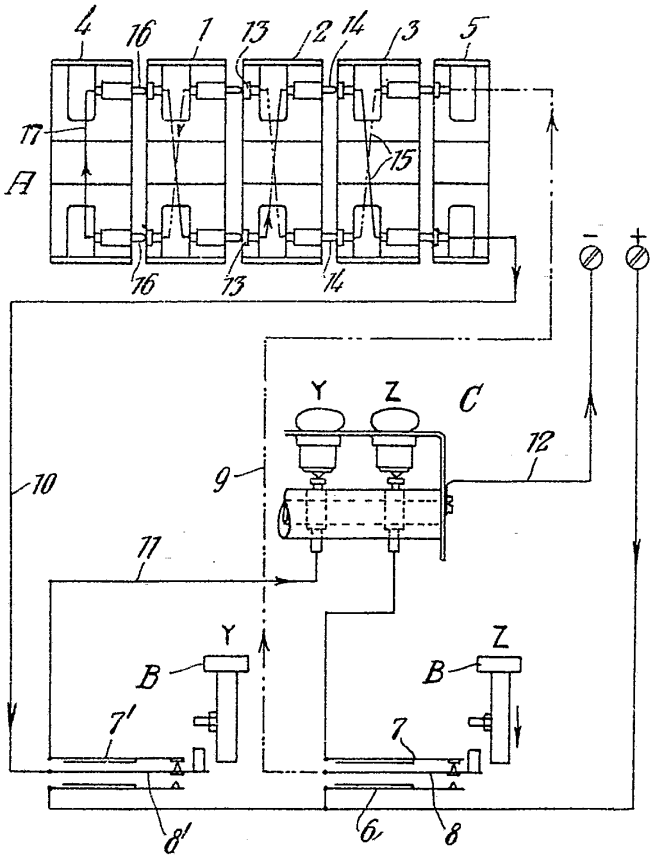


Abb. 3.

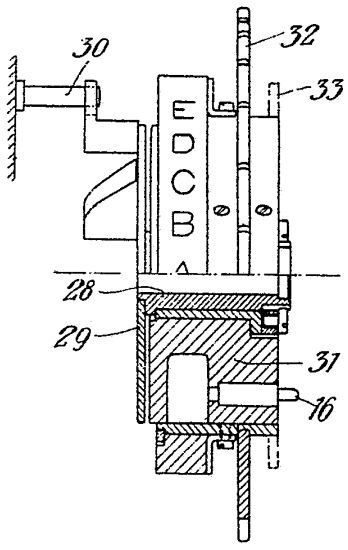


Fig. 3.

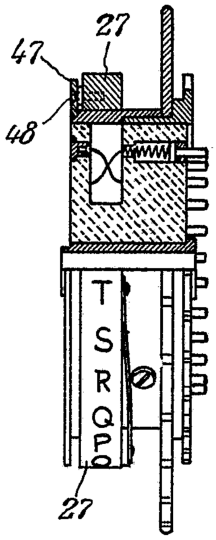


Fig. 2

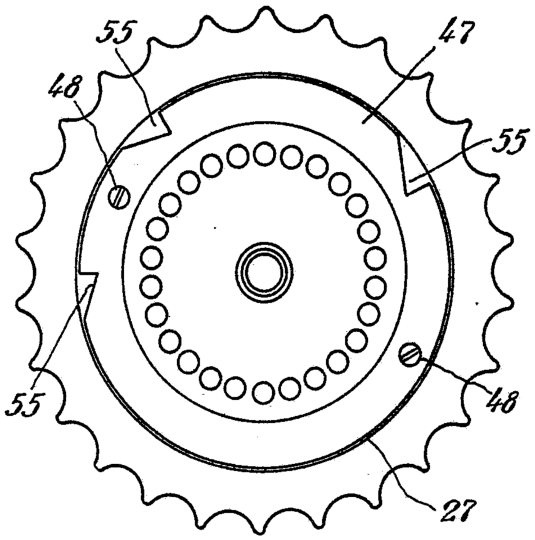
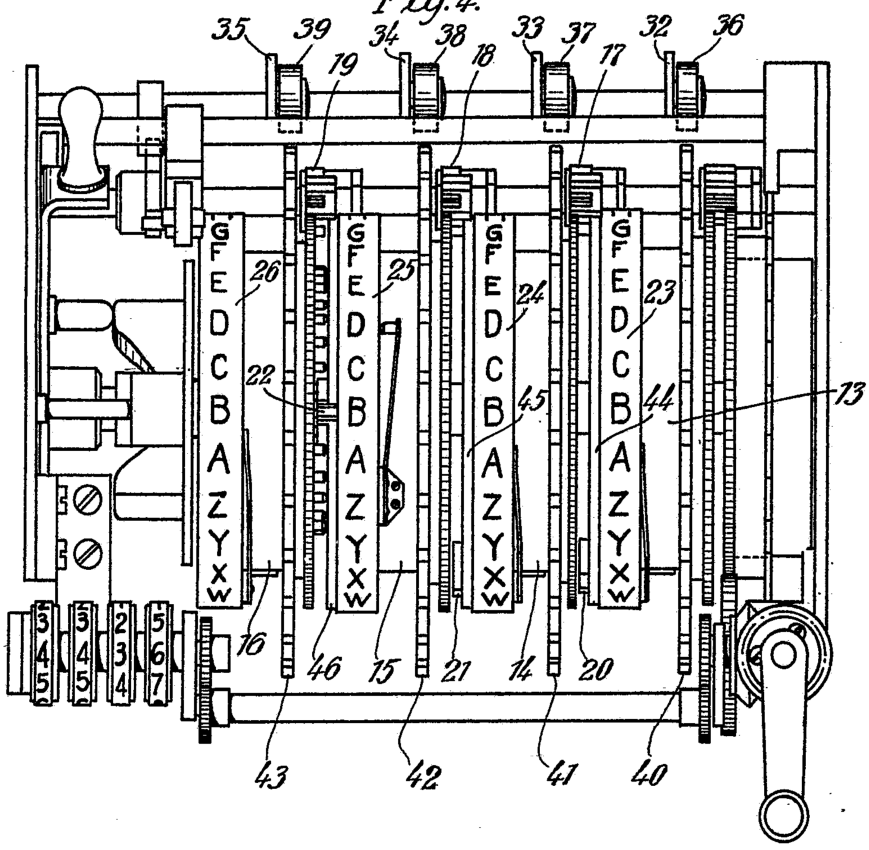


Fig. 4.


35
39
34
38
33
37
32
36
19
18
17
G F E D C B A Z Y X W
26
25
24
23
22
45
44
13
16
46
15
21
14
20
43
42
41
40
3 4 5
3 4 5
2 3 4
5 6 7

Zu der Patentschrift 579555
Kl. 42n Gr. 14

Fig. 3.

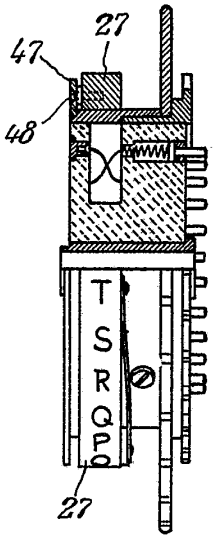


Fig. 2

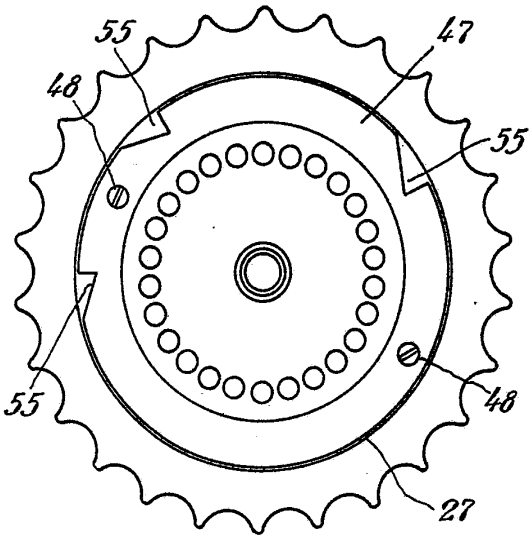
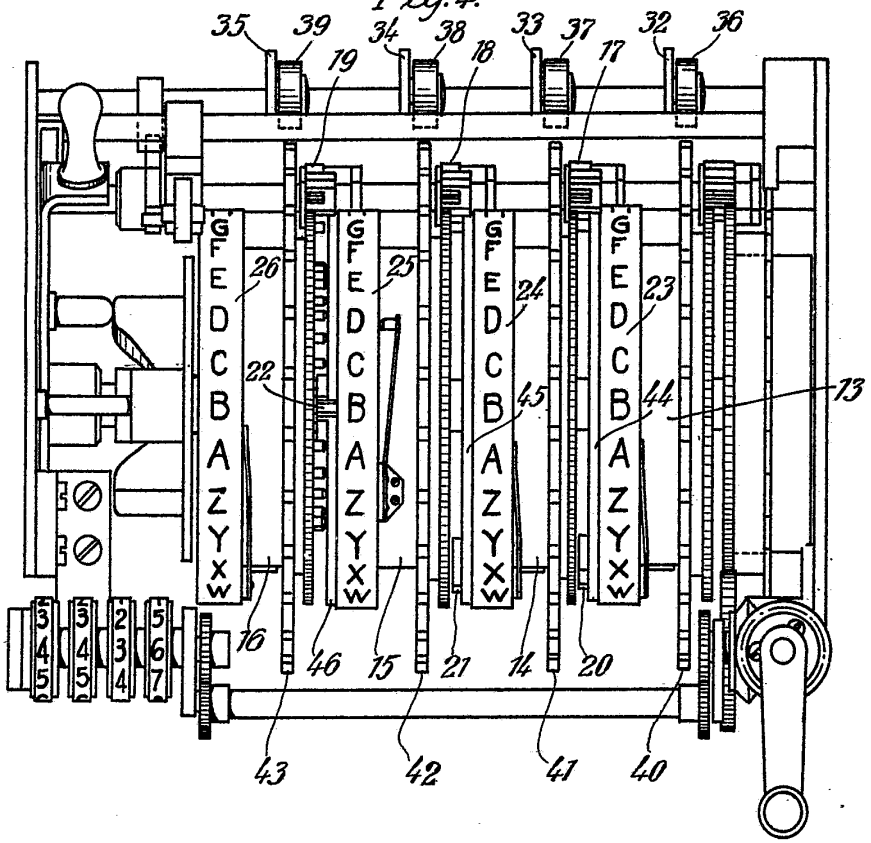
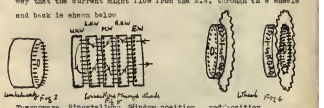


Fig. 4.



contact is connected to one and only one plate contact. On the wheels are rings or tyres carrying slabs of bete , and rotatable with respect to the rest of the wheel; more about this under 'turnovers'. When the machine is being used three of the wheels are put in between the U.K.W. and the R.W. in some prescribed order . The way that the current might flow from the R.W. through the wheels and back is shown below



Turnovers, Ringstellung, Window position , reflection.

From the point of view of the logistic designer, the position of the wheels is described by the letters on the tyres which show through the three (or 4 if the U.K.W. rotates) windows in the casing of the machine. This sequence of letters we call the 'window position'. When a key is depressed the window position changes, but does not change further when the key is allowed to rise. We will say that the position changes into the 'following' position. The position which follows a given one depends only on the order of the wheels and on the original window position. This is because the mechanism for changing the positions is carried on the tyres .

The turning mechanism consists of

Three pawls operated by the keys, one lying just to the right of the right hand wheel, one between the R.W.W and M.W. and one between the M.W. and the L.W.W.

86 catches fixed on each wheel on the right .

One (or conceivably more, here we will always assume it is only one) notch on each tyre to the left.

The effect of the right hand pall is to move the right hand R.W.W. forward one place every time a key is depressed. The middle pall