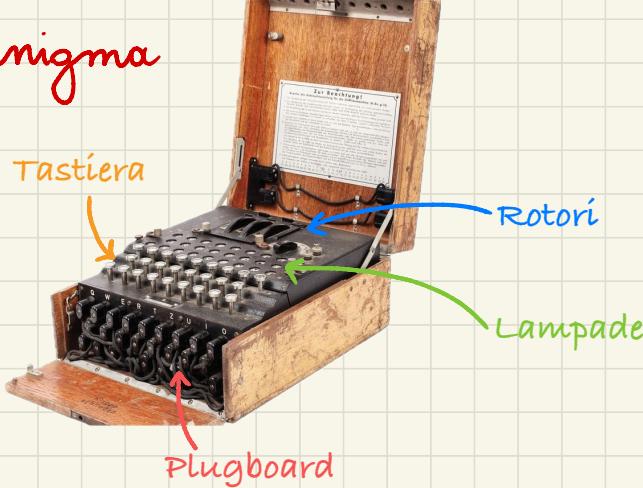
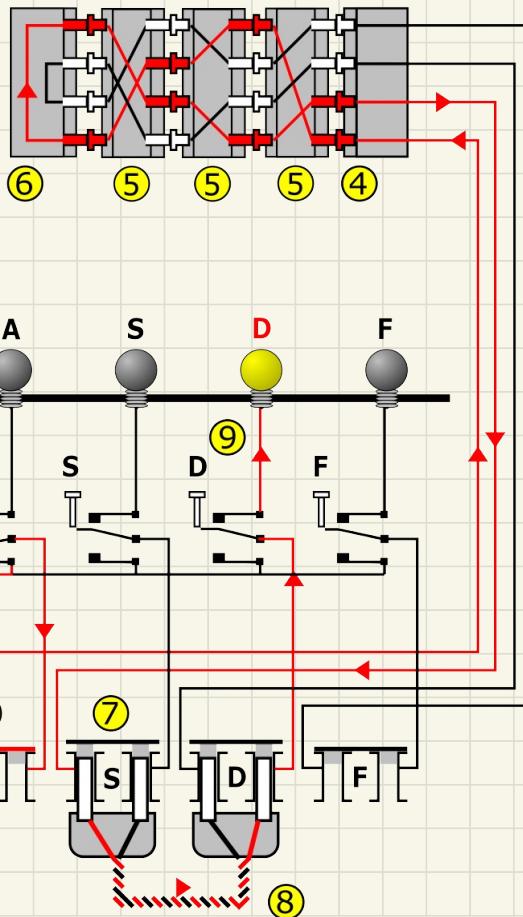


Enigma

Tastiera



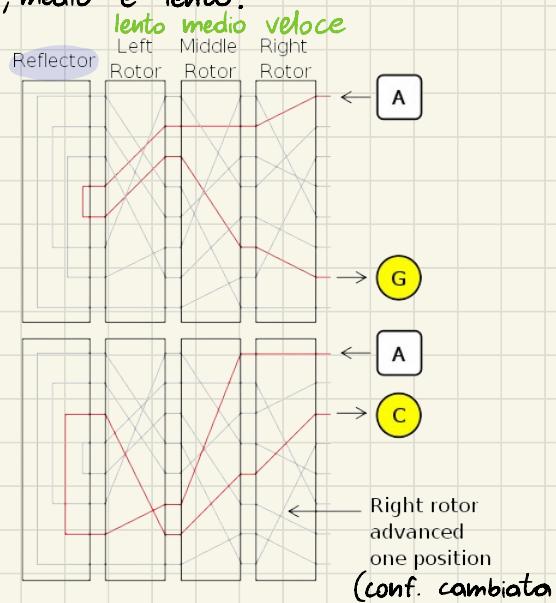
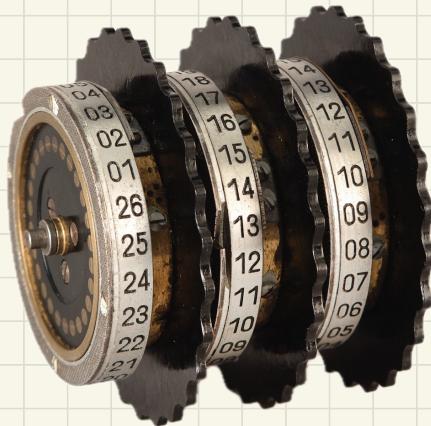
Non cifrerò mai una lettera con se stessa



Rotori

3 dischi con 26 contatti per lato, ogni contatto è collegato internamente con uno dall' altro lato.

I tre dischi sono in ordine: veloce, medio e lento.



Alla fine c'è un disco detto **reflector** con 26 pin solo da un lato, collegati internamente da 13 cavi per formare delle coppie. (veloce)

Dopo ogni pressione il rotore destro gira di 1 posizione, quando finisce un giro gira anche il medio, stesso meccanismo per il lento.

Quindi se premi 3 volte lo stesso tasto probabilmente ottieni 3 lettere diverse (non per forza).

Calcolo num. conf.

Le configurazioni di partenza venivano prese da un libro mensile, i settaggi venivano usati per 24h

Rotori

Ci sono $26^3 = 17576$ posizioni dei rotori possibili, ma siccome posso cambiare l'ordine dei rotori ho $3! = 6$ combinazioni di rotori.

quindi abbiamo $26^3 \cdot 3! = 105456$ possibili configurazioni di rotori

In fasi più avanzate della guerra sono passati a 5 rotori

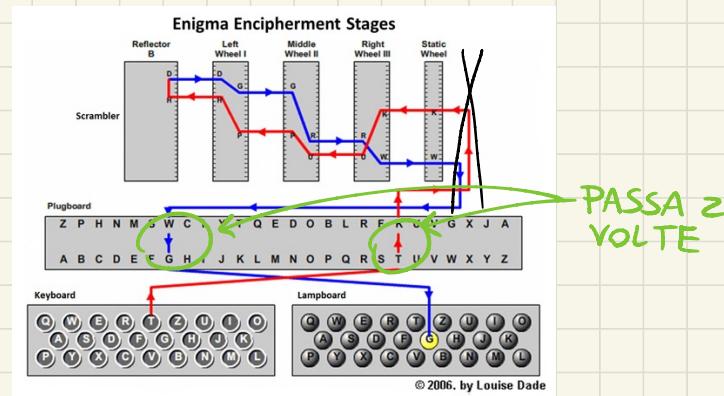
dunque $5! \cdot 26^5 = 585937.500$ possibili configurazioni dei rotori

Plugboard

bus a 26 fili tra tastiera e sezione rotori, dove avviene un'ulteriore permutazione.

Ogni macchina aveva un tot di fili a disposizione, inizialmente 6, successivamente 10.

Inoltre il segnale passa 2 volte dalla plugboard, quando premo il pulsante e quando il segnale torna dal blocco rotori.



Lavoro polacco anni 30

configurazione usata dai tedeschi:

- 3 rotori

- 6 cavi per plugboard

ogni giorno il libro ti indicava:

- permutazione dei rotori
- posizione iniziale dei rotori
- collegamenti della plugboard

All'inizio della comunicazione si invia una nuova posizione iniziale dei rotori che veniva ripetuta due volte. Il messaggio vero e proprio aveva stessa plugboard e permutazione dei rotori ma pos. iniziale diversa.

Notazione

$A = \{A, B, \dots, Z\} \quad S_A \rightarrow$ tutte le permutazioni di A

Utilizziamo la notazione ciclica.

es. $\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 1 & 2 & 4 \end{matrix} \Rightarrow (1 \ 3)(2 \ 5 \ 4)$ lunghezza z-3

implicito

- σ = permutazioni plugboard
- $s_0 \dots s_4$ = permutazioni dei 5 rotori
- τ = permutazione riflettore
- π^k = spostamento nell'alfabeto di k posizioni

σ e τ hanno solo cicli di lunghezza z, quindi $\tau^{-1} = \tau$ e $\sigma^{-1} = \sigma$

Se la posizione iniziale di un rotore è A allora la sua permutazione è s_i , se è invece ad es.

F allora la sua permutazione è $\pi^{-5}s_i\pi^5$.

Esempio

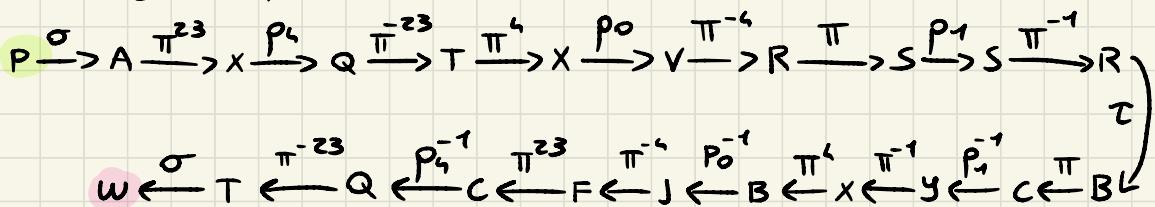
- $\rho_0 = (\text{BZ})(\text{CDKLHUP})(\text{ESZ})(\text{FIXVYOMW})(\text{GR})(\text{NT})$
- $\rho_1 = (\text{AELTPHQXRU})(\text{BKNW})(\text{CNOY})(\text{DFG})(\text{IV})(\text{JZ})$
- $\rho_2 = (\text{ABDHPEST})(\text{CFLVMZOYQIRWUKXSG})$
- $\rho_3 = (\text{ATV})(\text{BHKOXYDQMNF})(\text{CEULWZG})(\text{JRP})$
- $\rho_4 = (\text{AXQCNDTHSGEIOVLWMUJKRFPB})$
- $\tau = (\text{AY})(\text{BR})(\text{CU})(\text{DH})(\text{EQ})(\text{FS})(\text{GL})(\text{IP})(\text{JX})(\text{KN})(\text{MO})(\text{TZ})(\text{VW})$
- $\sigma = (\text{AP})(\text{CM})(\text{DE})(\text{GL})(\text{JZ})(\text{TW})$

Selezioniamo i rotori $\pi_0 - \pi_1 - \pi_2$ rispettivamente con posizione iniziale B-E-X. Ciò significa fare:

$$\underbrace{\sigma(\bar{\pi}^{23}\rho_4\pi^{23})(\bar{\pi}^4\rho_0\pi^4)(\bar{\pi}^4\rho_1\pi)}_{\text{scrittura compatta:}}\tau(\bar{\pi}^4\rho_2\pi)(\bar{\pi}^4\rho_3\pi)(\bar{\pi}^{23}\rho_5\pi^{23})\sigma$$

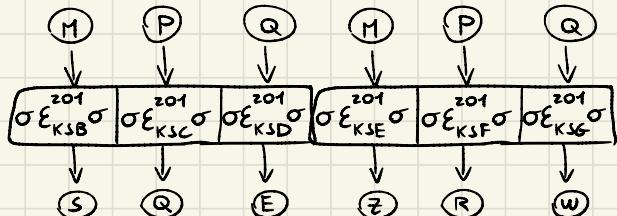
$\begin{matrix} 104 \\ \Sigma_{\text{BEX}} \end{matrix}$

diamogli in pasto un carattere



Debolezze metodo tedesco

All'inizio di ogni messaggio mandavano la nuova configurazione iniziale ripetuta 2 volte es.



dopo di che il resto del messaggio è cifrato partendo da $\sigma^{201} \circ^{201}$

ora troviamo che $\sigma^{201} \circ^{201} \sigma^{201} \circ^{201} \sigma^{201} (S) = Z \Rightarrow \sigma^{201} \circ^{201} \sigma^{201} \circ^{201} \sigma^{201} (S) = Z$
id

analogamente: $\sigma^{201} \circ^{201} \sigma^{201} \circ^{201} \sigma^{201} (Q) = R$ e $\sigma^{201} \circ^{201} \sigma^{201} \circ^{201} \sigma^{201} (E) = W$

se riceviamo abbastanza messaggi in un giorno possiamo fare le permutazioni complete

$\sigma^{201} \circ^{201} \sigma^{201} \circ^{201} \sigma^{201}$, $\sigma^{201} \circ^{201} \sigma^{201} \circ^{201} \sigma^{201} (Q)$, $\sigma^{201} \circ^{201} \sigma^{201} \circ^{201} \sigma^{201} (E)$

sfruttiamo la proprietà:

siano σ e τ due permutazioni in S_n , allora τ e $\sigma^{-1}\tau\sigma$ hanno la stessa lunghezza di cicli, in particolare se σ ha lunghezza=2 anche $\sigma\tau\sigma$ ha la stessa lunghezza

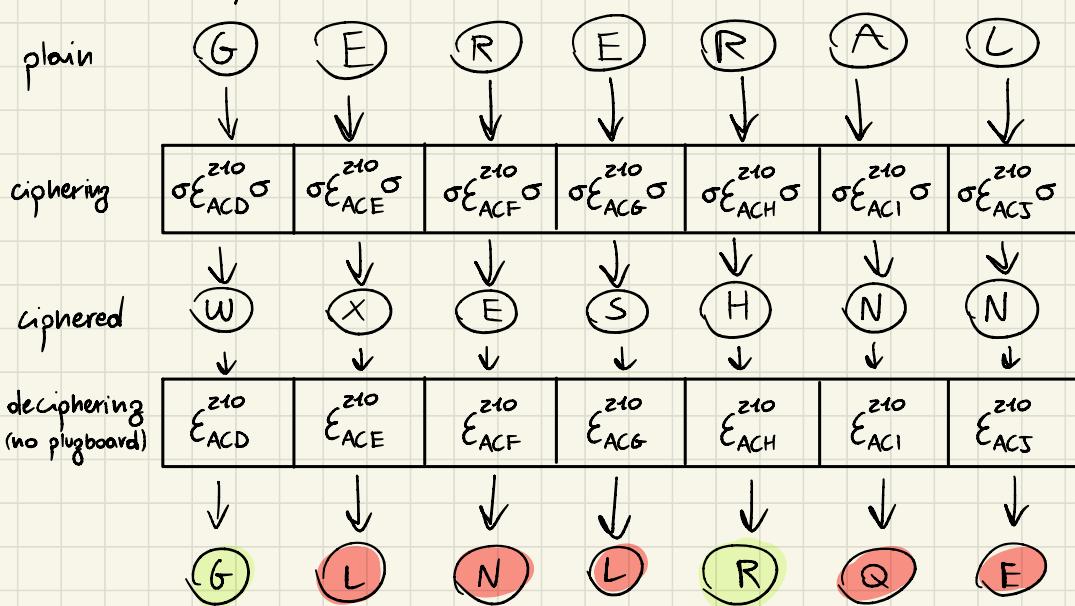
Adesso troviamo scomposizione ciclica (e quindi lunghezza) di

$$\begin{aligned} &\sigma^{201} \circ^{201} \sigma^{201} \circ^{201}, \\ &\sigma^{201} \circ^{201} \sigma^{201} \circ^{201} (Q), \\ &\sigma^{201} \circ^{201} \sigma^{201} \circ^{201} (E) \end{aligned}$$

trovare possibili partizioni / lunghezze di cicli

quante combinazioni di lunghezze di cicli possibili con permutazioni di lunghezza 26? (2436)
abbiamo 3 rotori quindi $2436^3 \approx 1.4 \cdot 10^{14}$ combinazioni possibili, inoltre il numero di possibili pos. iniziali è $6 \cdot 26^6 \approx 10^9$.

Ci sono quindi molte più lunghezze possibili che posizioni. Questo ispirò i polacchi a fare una lista delle possibili posizioni iniziali con le corrispondenti scomposizioni cicliche delle 3 permutazioni. Questa lista ha più di 100.000 righe ma ci sono ottime probabilità che, sapendo la scomposizione dei 3 cicli, puoi determinare in modo univoco la posizione iniziale. Questo metodo però non fornisce σ, quindi è ancora necessario trattare il linguaggio.



La probabilità che una lettera non sia collegata tramite plugboard è $\frac{14}{26}$, la probabilità che una lettera non venga cambiata due volte è quindi $(\frac{14}{26})^2 \approx \frac{1}{3}$

Quindi in $1/3$ dei casi la plugboard non la sto usando, da qui con conoscenza del linguaggio si può risalire a σ.

Questi sforzi polacchi vennero nullificati dall'introduzione dei 5 rotori

The Turing bomb

Weakness: very often used the same words

This method uses a "crib": a piece of code we know

for example

Nr	1	2	3	4	5	6	7	8	9	10	11	12	13
Tekst	K	E	I	N	E	Z	U	S	A	E	T	Z	E
Code	D	A	E	D	A	Q	O	Z	S	I	Q	M	M
Nr	14	15	16	17	18	19	20	21	22	23	24	25	
Tekst	Z	U	M	V	O	R	B	E	R	I	Q	T	
Code	K	B	I	L	G	M	P	W	H	A	I	V	

lets take rotor combination $z40$ and define rotor position $k \in \mathbb{N}_0$

so:
$$\left\{ \begin{array}{l} E_1 := E_{AAA}^{z40} \\ E_2 := E_{AAB}^{z40} \\ \vdots \\ E_{26^3} := E_{ZZZ}^{z40} \\ E_{26^3+1} := E_{AAA}^{z40} \end{array} \right.$$

if rotors are placed correctly there must exist $k \in \mathbb{N}$ so that:

$$\sigma E_{k+1} \sigma(K) = D$$

$$\sigma E_{k+2} \sigma(E) = A$$

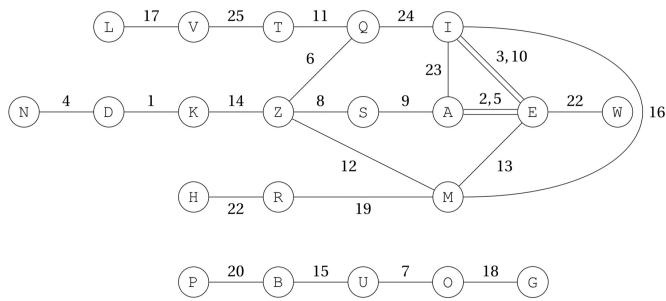
$$\sigma E_{k+3} \sigma(I) = E$$

⋮

now we have to find k without knowing σ

We can start the solution by building a graph where nodes are letters and the edges are connections between the plaintext letters and encrypted letters.

Also add the position in the crib to the edge



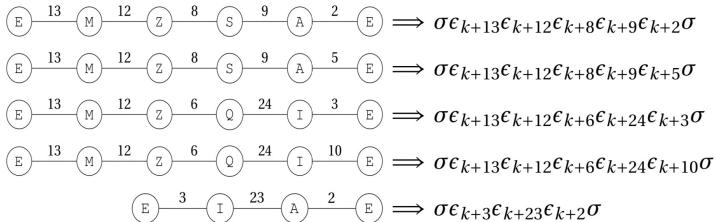
for a fixed k the edge i corresponds to the perm $\sigma \epsilon_{k+i} \sigma$

We can assign the composition of the permutations of the edges to each path
e.g.



corresponds to the permutation $\sigma \epsilon_{k+8} \sigma \epsilon_{k+6} \sigma = \sigma \epsilon_{k+6} \sigma \epsilon_{k+8} \sigma$

Now we look for a letter whose vertex lies in as many cycles as possible
In this example we take E



each cycle c therefore produces an equality of the form:

$$\sigma \epsilon_{k,c} \sigma(E) = E \implies \epsilon_{k,c} \sigma(E) = \sigma(E)$$

where $\epsilon_{k,c}$ is the composition of the ϵ_{k+i} 's of c .

if we now note $\text{Fix}(p)$ the fixed points of a permutation p

$$(\text{Fix}(p) = \{q \mid p(q) = q\})$$

then for every cycle trough c we find that $\sigma(E) \in \text{Fix}(\epsilon_{k,c})$ and therefore

$$\sigma(E) \in \bigcap_{\text{cycle } c \text{ for } E} \text{Fix}(\epsilon_{k,c})$$

if k is the correct position then the set is not empty.

The set probably is empty if k is wrong.

The more cycles I use the higher the probability that if it's empty then k is wrong

the permutations $E_{k,c}$ for every k can be easily be constructed pluggin in different enigma machines without plugboard.

The first turing bomb was that , it checked if there was any letter sent to itself trough all cycles , if so the machine stopped in that position k , and wrote it . There could be other k 's to be checked manually

disadvantages :

- Ⓐ σ must be known , we can immediately determine $\sigma(E)$ and all the other images
- Ⓑ Does not work if there are no (or few) cycles in the graph

The advanced Turing bomb

Here closed paths (cycles) are no longer necessary

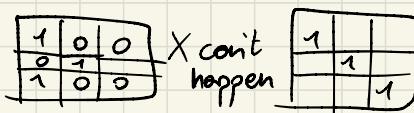
let's represent the permutations σ of the plugboard with all letters

	A	B	...	Z
A	$\sigma(A) = A$	$\sigma(A) = B$...	$\sigma(A) = Z$
B	$\sigma(B) = A$	$\sigma(B) = B$...	$\sigma(B) = Z$
:	:	:	..	:
Z	$\sigma(Z) = A$	$\sigma(Z) = B$...	$\sigma(Z) = Z$

each element is either true or false (1/0)

Since σ is a permutation of order 2 we will have only one 1 per row and one per column.

The matrix has to be symmetric



yes ✓

$$\sigma(L_1) = L_2 \iff \sigma(L_2) = L_1$$

now, suppose that in our crib-graph we have the edge:

$$(S) \xrightarrow{s} (Z) \implies \sigma(s) = \epsilon_{K+s} \sigma(z)$$

given that $\sigma(z) = p$ we can deduce that $\sigma(s) = \epsilon_{K+s}(p)$

in general: $(L_1) \xrightarrow{l} (L_2)$

$$\sigma(L_1) = L_3 \iff \sigma(L_2) = \epsilon_{K+l}(L_3) \quad \text{if the rotors are in position } K$$

$$\sigma(L_1) = \epsilon_{K+l} \sigma(L_2) \quad \text{alphabet}$$

We make a new graph with 26^2 vertices corresponding to $A \times A$ as the table above the graph's edges come from the equalities

• $\forall L_1, L_2 \in A$ we have the edge $(L_1, L_2) — (L_2, L_1)$

• for every $(L_1) \xrightarrow{l} (L_2)$ we add the edge $(L_1, L_3) — (L_2, \epsilon_{K+l}(L_3))$

so we make a changing graph Γ_K in which the edges move every time the rotor position K changes.

The first condition says that symmetrically placed vertices are connected via an edge.

The second says that if there is an edge $(L_1) \xrightarrow{l} (L_2)$ in the crib-graph then every vertex L_3 on row L_1 is connected to a vertex $\epsilon_{K+l}(L_3)$ on row L_2

The goal is to give each vertex a value either 1 or 0, if we have the right K we'll have the following situation:

- each row has one 1 and 25 zeros
- " " column "
- vertices that are connected have the same number

If we don't have the right K we would almost certainly fail.

If we do have the right K then there must be one or more solutions.

Graph-theoretically you can say that for the correct K there must be a connection component (or a union of them) that contains exactly 1 vertex for each row and column

The machine

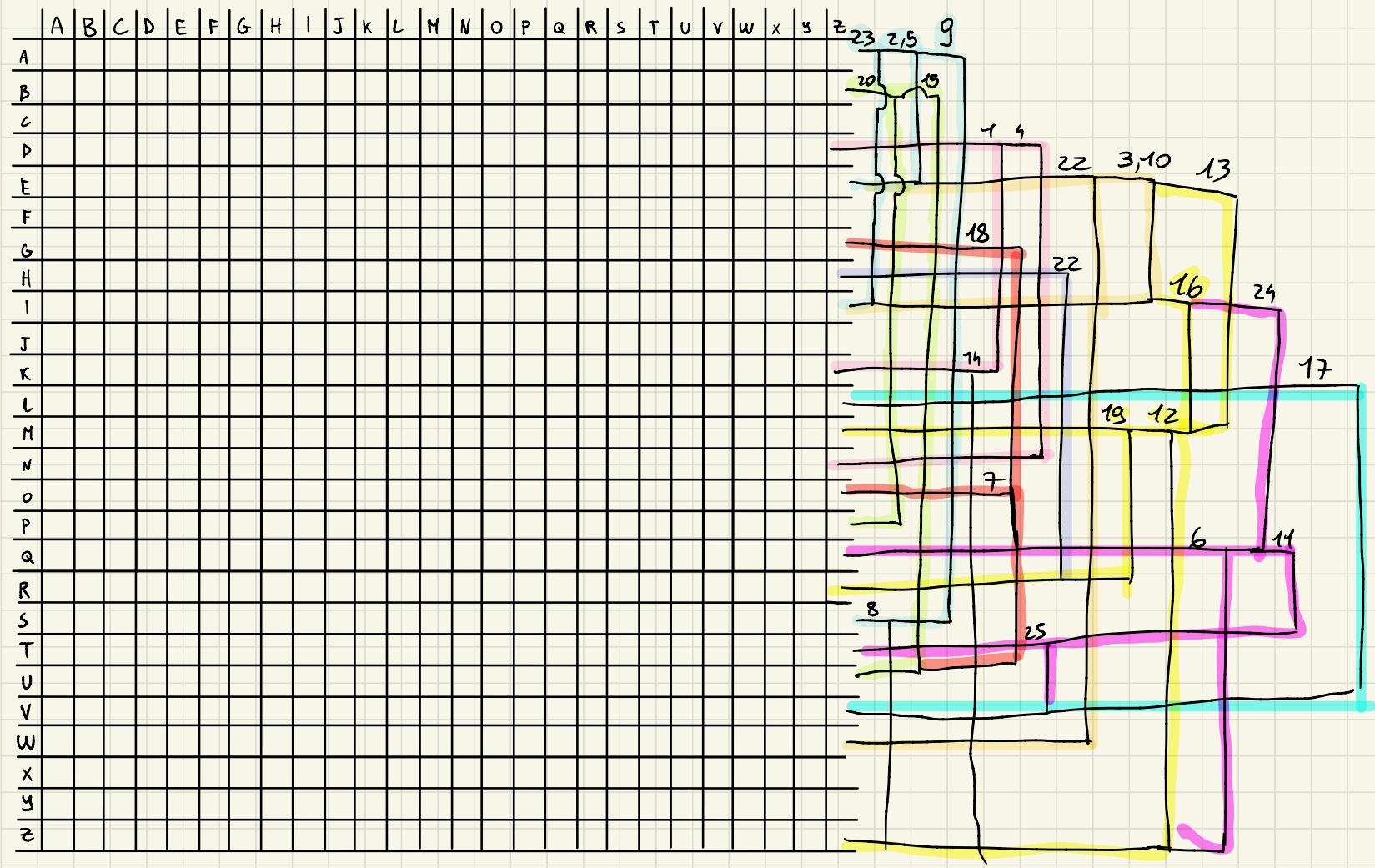
Choose the letter L_1 from crib-graph with the most edges

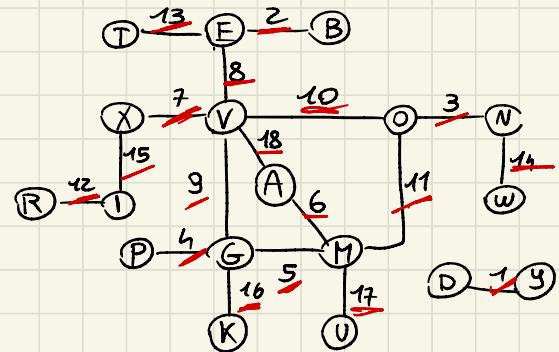
Convert the graph to electric circuit

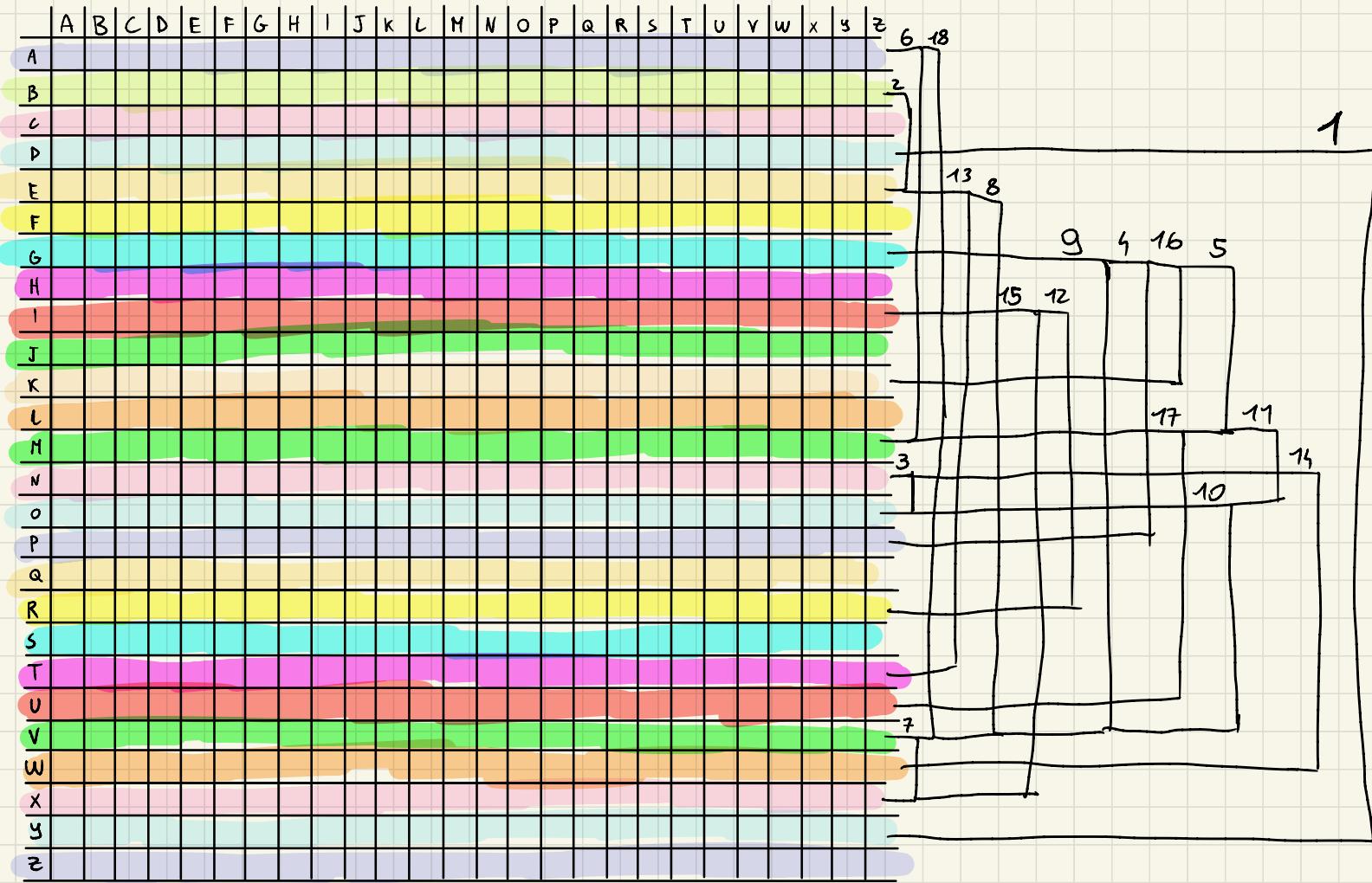
Apply tension to (L_1, L_2) in Γ_K , there will be potential to every vertex connected to (L_1, L_2)

if K was the right rotor position and (L_1, L_2) is a connection in the plugboard then on the horizontal line of L_1 (L_1, L_2) will be the only one with tension.

if it's not the right K almost all other vertex has potential except the plugboard position also almost all (L_1, L_i) would have tension.







Hello world

reflector

