Criptografia Histórica

Introdução à Criptografia Símetrica por Exemplos Históricos

Enno Nagel

Minicurso no IFAL – Maceió, 24 Novembro 2018

Criptografia Outrora

A criptografia estuda a transformação de um

texto inteligível

$$\Downarrow$$

texto *in*inteligível

tal que só uma informação adicional secreta, a *chave*, permite desfazê-la.

Substituição (do Alfabeto por traslado)

Este método foi usado por César (63 - 14 a.C.).

- Escolhemos uma *chave*

  δ = uma distância entre letras em ordem alfabética

  = um número entre 0 e 25

- trasladamos por δ cada letra do alfabeto (latino e cujas letras são arranjadas em um anel).

Por exemplo, se $\delta = 3$, então

$$\mathrm{A} \mapsto \mathrm{D}, \mathrm{B} \mapsto \mathrm{E}, \mathrm{C} \mapsto \mathrm{F}, \ldots, \mathrm{W} \mapsto \mathrm{Z}, \mathrm{X} \mapsto \mathrm{A}, \ldots, \mathrm{Z} \mapsto \mathrm{C}.$$

e, por exemplo, para $\delta = 3$,

$$\mathrm{CARA} \mapsto \mathrm{FDUD}$$

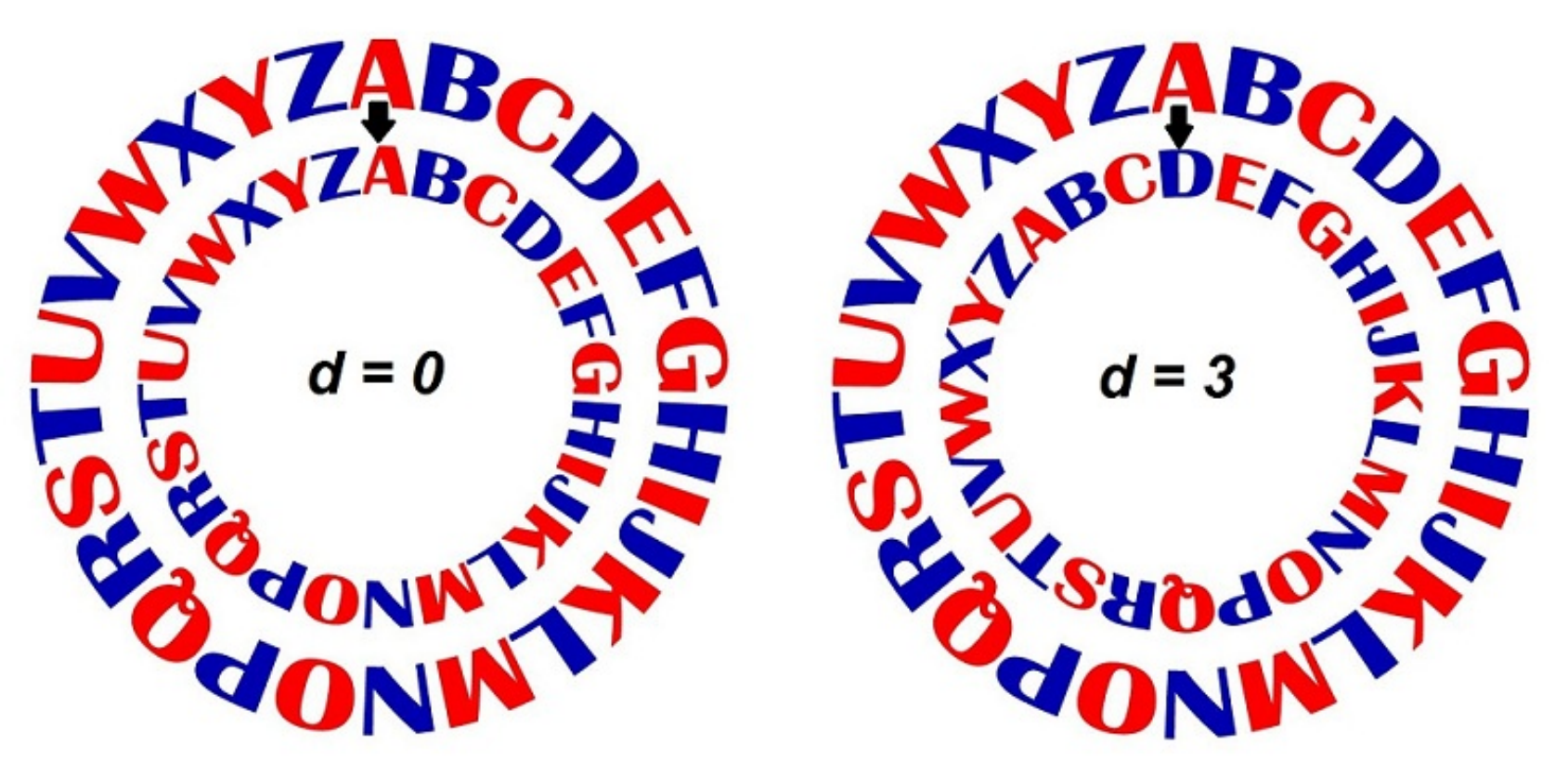


Figura 1: César como duas rodas deslocadas

- Na **cifração** traslada-se cada letra no sentido **horário**, e
- na **decifração** no sentido **anti-horário**.

Pela circularidade, d no sentido anti-horário = $26 - d$ no sentido horário. **Questão:** Com qual d cifração = decifração?

Substituição (do Alfabeto por permutação das letras)

Em vez de

- substituirmos cada letra por um traslado pela mesma distância δ,
- substituímos cada letra por uma letra arbitrária; isto é, permutamos as letras. Por exemplo,

A	B	...	Y	Z
↓	↓	...	↓	↓
E	Z	...	G	A

Por exemplo,

$$\mathrm{ABA} \mapsto \mathrm{EZE}.$$

Há $26 \cdot 25 \cdots 1 = 26! > 10^{26}$ chaves = permutações.

Transposição (das letras do Texto Claro)

A *cítala* ou o *bastão de Licurgo* (= legislador de Esparta) é um bastão com o qual os espartanos cifravam como segue:

- enrolar o bastão com um pano estreito,
- escrever neste pano no sentido da borda maior, e
- desenrolar o pano do bastão.

As letras assim transpostas no pano unicamente podiam ser decifradas por um bastão com

- a mesma circunferência (e o mesmo comprimento),

pela mesma maneira como o texto foi cifrado:

- enrolar o bastão com um pano,
- ler este pano no sentido da borda maior.

A chave é o número dado pelo **número das letras que cabem nesta circunferência**.

Exemplo da Cítala

Por exemplo, se o bastão tem uma circunferência de 2 letras (e um comprimento de 3 letras), as duas linhas

l u a
m e l

tornam-se as três linhas

l m
u e
a l

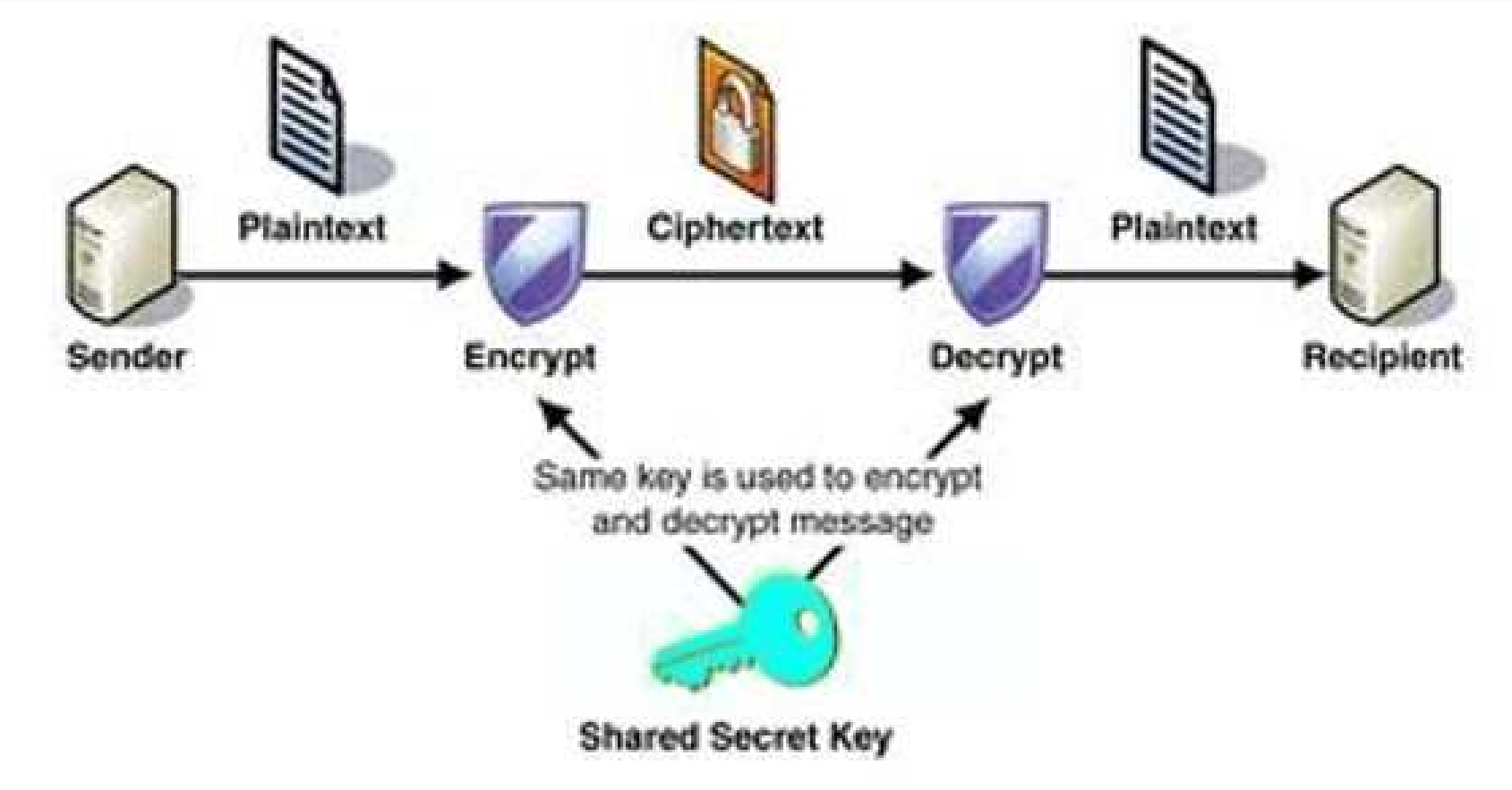
que são concatenadas (para não revelarem nem a circunferência, nem o comprimento) à linha

L M U E A L

Criptografia Simétrica

A criptografia é **simétrica** se

chave para cifrar = chave para decifrar.



A criptografia simétrica já era usada pelos egípcios 2000 anos antes de Cristo, e todos os exemplos históricos são simétricos.

Qualidades Desejáveis de um Algoritmo Criptográfico

O *princípio de Kerckhoff* postula que o

- algoritmo seja **público**.

Enquanto o conhecimento da chave compromete uma única cifração, o conhecimento do algoritmo compromete todas as;

$\Longrightarrow$

Um algoritmo público garante a dificuldade da decifração depender só da segurança da *chave*, mas não da do *algoritmo*. Quanto mais usado, tanto mais provável que o algoritmo será conhecido. Para ele ser útil, necessita ser seguro sendo público.

As *metas de Shannon* da

- *Confusão* respectivamente
- *Difusão*

desejam **minimizar** a **relação** entre o texto cifrado e

- a **chave** respectivamente
- o **texto claro**

Idealmente, quando uma letra do texto claro respectivamente da chave muda, cada letra do texto cifrado muda com uma probabilidade de *50%*.

$\Longrightarrow$

Uma boa confusão ou difusão evita ataques estatísticas sobre

- ou muitas *chaves* cifrando o mesmo texto claro,
- ou muitos *textos claros* cifrados pela mesma chave.

Qualidades Desejáveis nos Exemplos Históricos

Aplicamos os critérios aos exemplos históricos das *Substituições do Alfabeto*

- por traslado,

$$\mathrm{A} \mapsto \mathrm{D}, \mathrm{B} \mapsto \mathrm{E}, \mathrm{C} \mapsto \mathrm{F}, ..., \mathrm{W} \mapsto \mathrm{Z}, \mathrm{X} \mapsto \mathrm{A}, ..., \mathrm{Z} \mapsto \mathrm{C}.$$

- por permutação

A	B	...	Y	Z
↓	↓	...	↓	↓
E	Z	...	G	A

- a *Transposição do Texto* (claro) pela cítala, que torna linhas em colunas.

Falhas do Cesar

A *Substituição do Alfabeto* por traslado usada por César

$$\mathrm{A} \mapsto \mathrm{D}, \mathrm{B} \mapsto \mathrm{E}, \mathrm{C} \mapsto \mathrm{F}, \ldots, \mathrm{W} \mapsto \mathrm{Z}, \mathrm{X} \mapsto \mathrm{A}, \ldots, \mathrm{Z} \mapsto \mathrm{C}.$$

viola todas as qualidades desejáveis, principalmente o *princípio de Kerckhoff*, que o algoritmo seja público:

Uma vez o método for conhecido, considerando a pequena quantidade de *25* chaves, o texto cifrado cede em pouco tempo a um **ataque de força bruta** que prova cada chave.

Falhas da Substituição do Alfabeto

A *Substituição do Alfabeto* por permutação

A	B	…	Y	Z
↓	↓	…	↓	↓
E	Z	…	G	A

tem $26 \cdot 25 \cdots 1 = 26! > 10^{26}$ chaves,

$\Longrightarrow$ ataque de força bruta computacionalmente inviável.

Mas viola os *princípios de difusão e confusão*. Se a chave (= permutação do alfabeto) permuta a letra α pela letra β, então há

- má *confusão* porque a troca de β na chave implica unicamente a troca da letra β no texto cifrado,
- má *difusão* porque a troca de α no texto claro implica unicamente a troca da letra β no texto cifrado.

Ataque pela Frequência Estatística

Com efeito, permite ataques estatísticas sobre a frequência de

- letras,
- bigramas (= pares de letras) e
- trigramas (= triplos de letras).

em português. Por exemplo,

- a letra mais frequente em português é “a”
- o bigrama mais frequente em português é “de”
- o trigrama mais frequente em português é “que”

$\Longrightarrow$ se há suficientemente texto, associando

- a letra mais frequente do *texto cifrado* à letra mais frequente *em português* (= “a”),
- o bigrama mais frequente do *texto cifrado* ao bigrama mais frequente *em português* (= “de”), …

Exemplo do Ataque

Sera cifrado por uma permutação o texto:

GUP WPV KPX GSQVEP P WVXMG

As três letras mais comuns do português são, nesta ordem, AEO.

Obtemos

E*A *AO *A* E**O*A A *O**E.

Supomos que $E * A = ELA$ e $*AO = NAO$. Em particular, W corresponde a N. Logo

ELA NAO *A* E**O*A A NO**E.

Em seguida, as três letras mais comuns são SRI.

Experimentado com elas, estamos levados ao chute

ELA NAO VAI EMBORA A NOITE.

Exemplo do Ataque

Sera cifrado por uma permutação o texto:

GUP WPV KPX GSQVEP P WVXMG

As três letras mais comuns do português são, nesta ordem, AEO.

Obtemos

E*A *AO *A* E**O*A A *O**E.

Supomos que $E * A = ELA$ e $*AO = NAO$. Em particular, W corresponde a N. Logo

ELA NAO *A* E**O*A A NO**E.

Em seguida, as três letras mais comuns são SRI.

Experimentado com elas, estamos levados ao chute

ELA NAO VAI EMBORA A NOITE.

Exemplo do Ataque

Sera cifrado por uma permutação o texto:

GUP WPV KPX GSQVEP P WVXMG

As três letras mais comuns do português são, nesta ordem, AEO.

Obtemos

E*A *AO *A* E**O*A A *O**E.

Supomos que $\mathrm{E} * \mathrm{A} = \mathrm{ELA}$ e $*\mathrm{AO} = \mathrm{NAO}$. Em particular, W corresponde a N. Logo

ELA NAO *A* E**O*A A NO**E.

Em seguida, as três letras mais comuns são SRI.

Experimentado com elas, estamos levados ao chute

ELA NAO VAI EMBORA A NOITE.

Exemplo do Ataque

Sera cifrado por uma permutação o texto:

GUP WPV KPX GSQVEP P WVXMG

As três letras mais comuns do português são, nesta ordem, AEO.

Obtemos

E*A *AO *A* E**O*A A *O**E.

Supomos que $\mathrm{E} * \mathrm{A} = \mathrm{ELA}$ e $*\mathrm{AO} = \mathrm{NAO}$. Em particular, W corresponde a N. Logo

ELA NAO *A* E**O*A A NO**E.

Em seguida, as três letras mais comuns são SRI.

Experimentado com elas, estamos levados ao chute

ELA NAO VAI EMBORA A NOITE.

Falhas da Cítala

A cítala viola

- o *princípio de Kerckhoff*, que o algoritmo seja público.

Com efeito, o valor máximo da circunferência é $< n/2$ onde n = o número das letras do texto cifrado. Por isso, um ataque de força bruta, é viável.

Ela tem

- má *difusão* porque a substituição de uma letra α no texto claro implica unicamente a substituição da mesma letra α no texto cifrado.

Com efeito, o algoritmo permite ataques estatísticas sobre a frequência de

- bigramas (= pares de letras)
- trigramas (= triplos de letras), e assim por diante.

Exemplo do Ataque

Por exemplo, propício seria a escolha da circunferência como o número n que maximiza a frequência do bigrama “de” entre as cadeias de letras nas posições $1, 1+n, 1+2n$, ...,
$2, 2+n, 2+2n$, ...

Por exemplo, olhamos

ADABESACA.

Observamos que d e e são distanciados por três letras.
Arriscamos o chute que

$$\text{circunferência} = 3 \text{ letras},$$

Obtemos à decifração

ABA DE CASA.

Exemplo do Ataque

Por exemplo, propício seria a escolha da circunferência como o número n que maximiza a frequência do bigrama “de” entre as cadeias de letras nas posições $1, 1+n, 1+2n, \ldots,$
$2, 2+n, 2+2n, \ldots.$

Por exemplo, olhamos

ADABESACA.

Observamos que d e e são distanciados por três letras.
Arriscamos o chute que

$$\text{circunferência} = 3 \text{ letras},$$

Obtemos à decifração

ABA DE CASA.

Exemplo do Ataque

Por exemplo, propício seria a escolha da circunferência como o número n que maximiza a frequência do bigrama “de” entre as cadeias de letras nas posições $1, 1+n, 1+2n, \ldots,$
$2, 2+n, 2+2n, \ldots.$

Por exemplo, olhamos

ADABESACA.

Observamos que d e e são distanciados por três letras.
Arriscamos o chute que

$$\text{circunferência} = 3 \text{ letras},$$

Obtemos à decifração

ABA DE CASA.

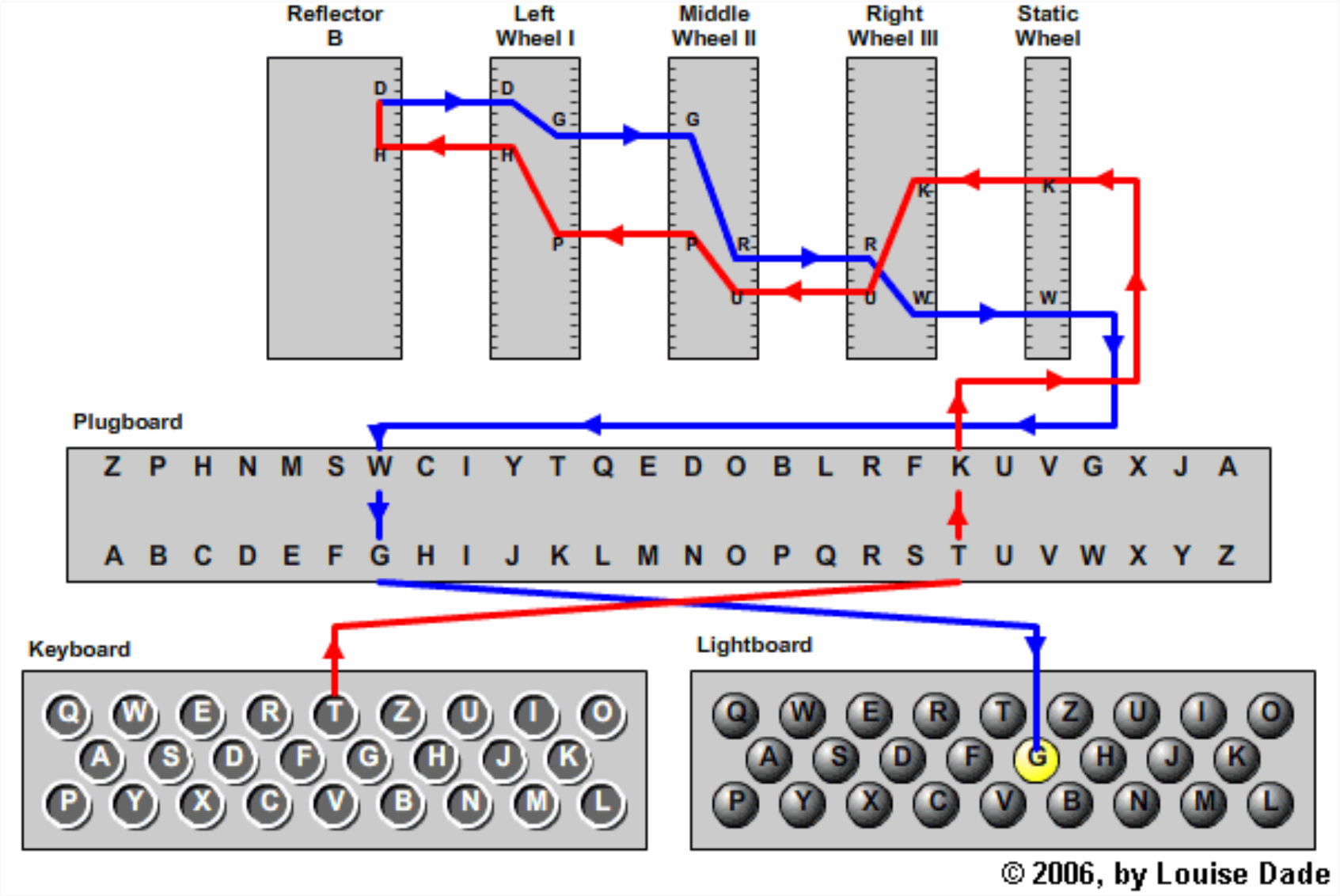


Figura 3: O percurso da corrente nos cabos da Enigma ao teclar uma letra

Construção

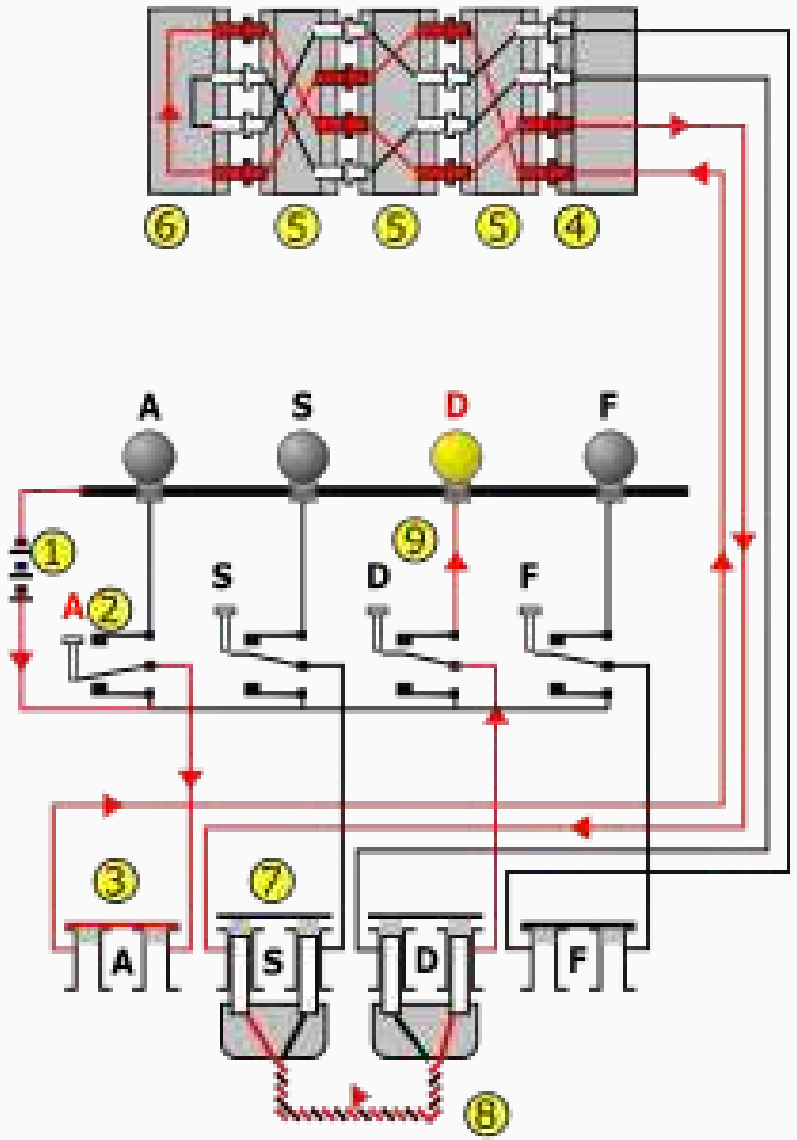


Figura 4: O esquema elétrico

O esquema elétrico, constituído por:

- Bateria (1),
- Teclado (2),
- O painel de ligações (3, 7) com cabo (8),
- o jogo dos cilindros (5) com o da entrada (4) e o de retorno (6), e
- o painel das lampadas (9)

Ao teclar uma letra, a corrente entra

1. pelo painel de ligações,
2. no cilindro da entrada,
3. no jogo dos cilindros,
4. no cilindro de retorno, e
5. percorre todo o caminho outra vez, no sentido inverso,

para finalmente ascender a lampada da letra cifrada.

Ao **teclar** uma letra, o rotor direito (= o rotor *rapido*) **avança** uma posição. O diagrama mostra o percurso da letra $\mathbf{A}$ nos cilindros

- ao *primeiro*, e
- ao *segundo* teclar.

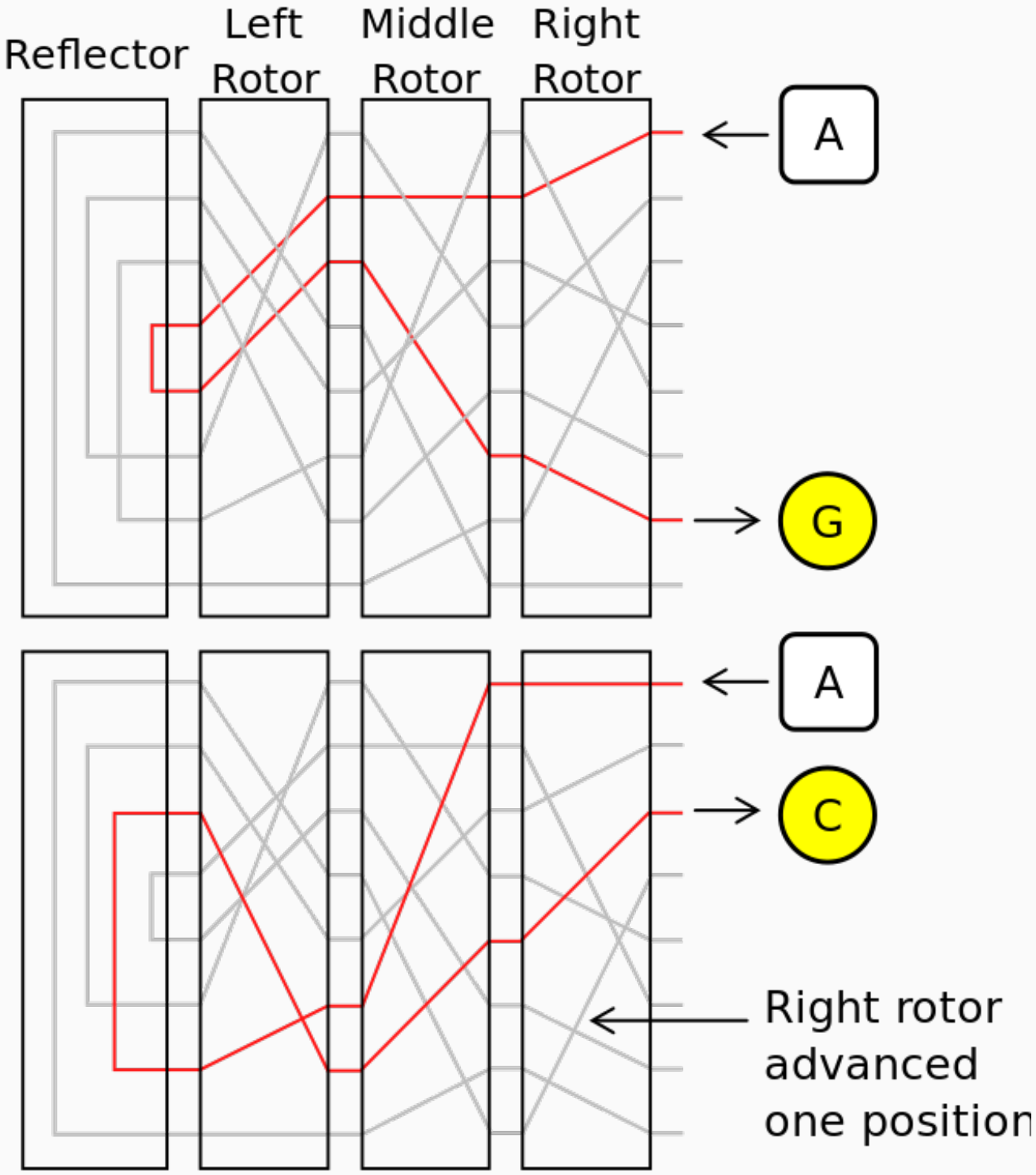
Em posições inicialmente determinadas pela posição do anel do rotor rápido e do rotor no meio, também

- primeiro o rotor no meio (o rotor *médio*) e
- depois o à esquerda (o rotor *lento*)

avança. Após o primeiro avanço (do rotor médio ou lento),

- o rotor médio avança após 26 avanços do rotor rápido, e
- o rotor lento avança após 26 avanços do rotor médio.

Isto é, os rotores comportam-se como os de um taxímetro ou **conta-quilômetros**, com a diferença que os da Enigma têm $26 = \#\{\text{letras do alfabeto}\}$ dígitos (e o conta-quilômetros 10).


Reflector
Left Rotor
Middle Rotor
Right Rotor
A
G
A
C
Right rotor advanced one position

Cada *cilindro* permuta o alfabeto inteiro por um cabeamento interno. Este cabeamento é fixo, e não pode ser mudado pelo usuário. Por dentro, há uma verdadeira salada de cabos:

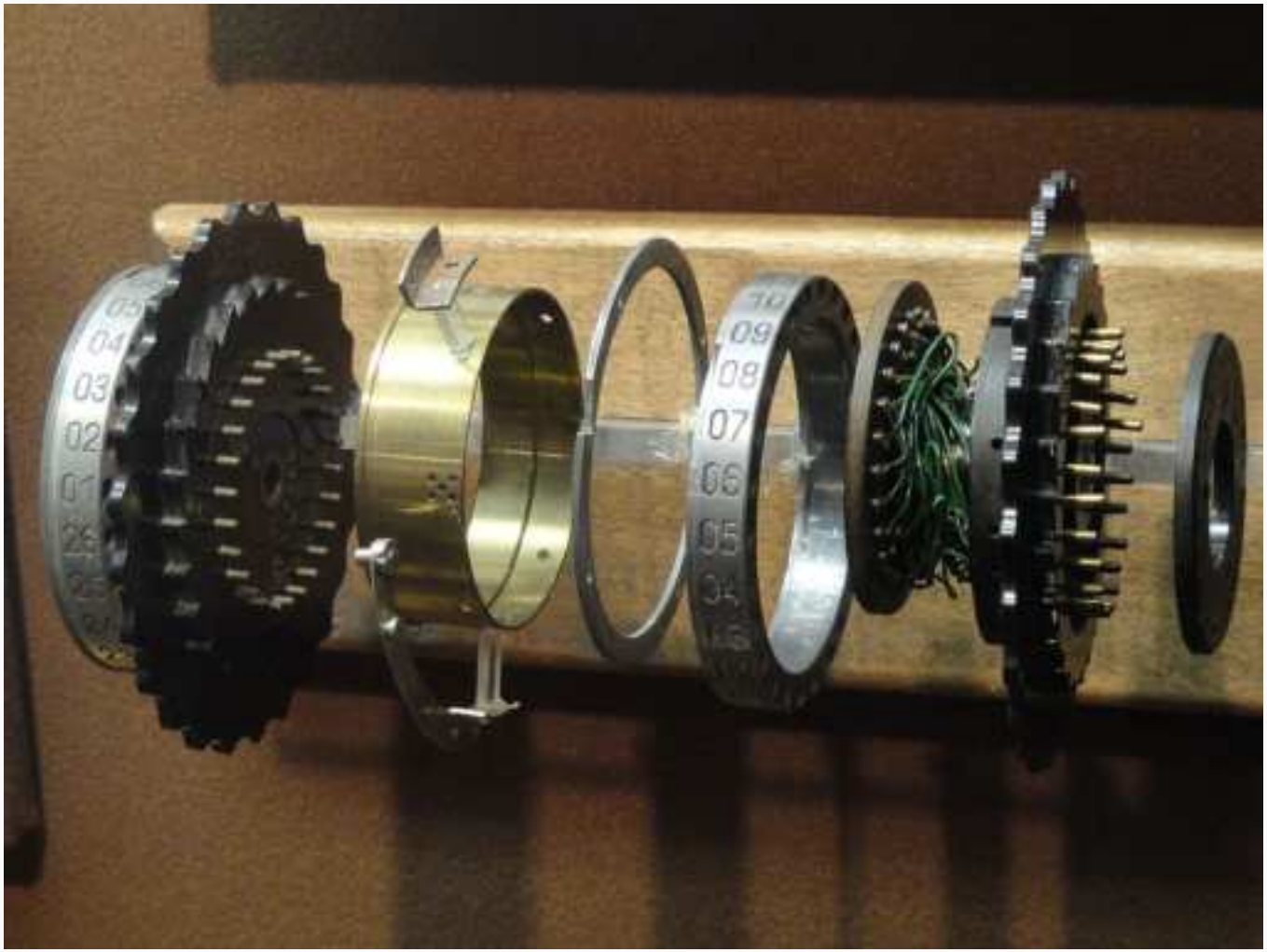


Figura 6: Os cilindros

O cilindro de entrada = Identidade

O cilindro de entrada igualmente permuta o alfabeto, mas

- só existia na **versão comercial** da Enigma.
- na **versão militar**, não fazia nada, isto é, a substituição é a identidade.

Isto foi intuído por *Marian Rejweski*, criptógrafo polonês (pelo vício dos alemães na ordem) antes da Segunda Guerra Mundial. Assim conseguiu inferir o cabeamento dos cilindros da Enigma, enquanto os franceses e britânicos não fizeram progresso.

Figura 7: Marian Rejweski

Cilindro de Retorno

Figura 8: Cilindro de Retorno

O **cilindro de retorno** garante que a substituição seja auto-inversa, isto é, *cifração* = *decifração*.

$\Longrightarrow$ para evitar um curto-circuito, a Enigma **nunca** cifrou uma letra a **si mesma**! Um defeito criptográfico considerável.

O *painel de ligações* troca umas pares de letras, na prática, dez. Por exemplo, na foto, A e J, e S e O.

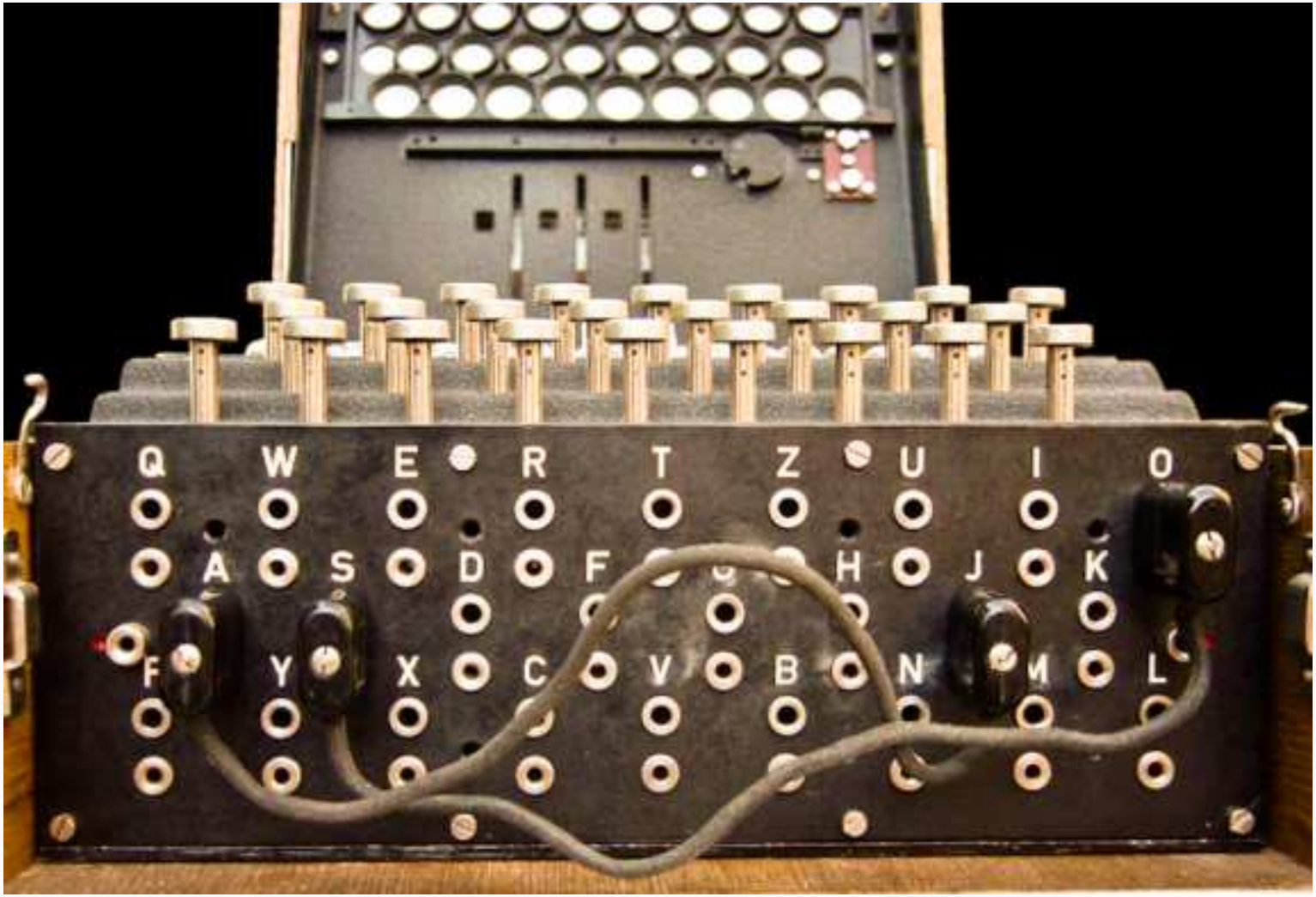


Figura 9: O painel de ligações

A substituição M (= Maquina) da Enigma é a concatenação

$$\mathrm{M} = \mathrm{PEC_R}(c_\mathrm{R})\mathrm{C_M}(c_\mathrm{M})\mathrm{C_L}(c_\mathrm{L})\mathrm{RC_L}(c_\mathrm{L})^{-1}\mathrm{C_M}(c_\mathrm{M})^{-1}\mathrm{C_R}(c_\mathrm{R})^{-1}\mathrm{E}^{-1}\mathrm{P}^{-1}$$

onde

- P é a substituição pelo Painel de ligações
- E é a substituição pelo cilindro de Entrada
- R é a substituição pelo cilindro de Retorno.
- $\mathrm{C_R}(c_\mathrm{R})$, $\mathrm{C_M}(c_\mathrm{M})$ e $\mathrm{C_L}(c_\mathrm{L})$ são as substituições pelo Cilindro Rápido, Médio e Lento na posição c_R, c_M e c_L, onde

  $$\mathrm{C_{R/M/L}}(c_\mathrm{R/M/L}) = \mathrm{T}^{c_\mathrm{R/M/L}}\mathrm{C_{R/M/L}}\mathrm{T}^{-c_\mathrm{R/M/L}}$$

  com
  - $c_\mathrm{R/M/L} = r_\mathrm{R/M/L} - a_\mathrm{R/M/L}$ onde
    - $r_\mathrm{R/M/L}$ = posição do Rotor, e
    - $a_\mathrm{R/M/L}$ = posição do Anel;
  - T = a traslação = a substituição que traslada cada letra do alfabeto à sua vizinha, isto é $\mathrm{A} \mapsto \mathrm{B}$, $\mathrm{B} \mapsto \mathrm{C}$, …, $\mathrm{Z} \mapsto \mathrm{A}$, e
  - $\mathrm{C_{R/M/L}}$ = a substituição do cilindro.

Periodicidade e Frequência de Letras

Como a cada letra teclada o rotor rápido avança uma posição,

- isto é $r_{\mathrm{R}} \rightsquigarrow r_{\mathrm{R}} + 1$, e
- logo $c_{\mathrm{R}} = r_{\mathrm{R}} - a_{\mathrm{R}} \rightsquigarrow c_{\mathrm{R}} + 1$,
- segue que $\mathrm{C}_{\mathrm{R}}(c_{\mathrm{R}} + 1) = \mathrm{T}^{c_{\mathrm{R}}} \mathrm{C}_{\mathrm{R}}(c_{\mathrm{R}}) \mathrm{T}^{-c_{\mathrm{R}}}$ muda, e
- por isso toda a substituição M muda!

$\Longrightarrow$ a mesma substituição só se aplica após uma rotação completa de cada cilindro, isto é, após cerca de 17.000 tecladas,

$\Longrightarrow$ a decifração pela frequência das letras (por exemplo, da língua alemã) se aplica se e somente se

$$\#\{ \text{ letras do texto } \} = \text{ múltiplo de } 17.000$$

Por ordem, as mensagens alemãs tinham < 250 letras.

Chaves

Para a `Engima I`, há quatro fatores:

- Posição do **Anel**: Determina a qual ponto o cilindro seguinte inicilamente avança uma posição, isto é, quando a rodada inicial se completa. Depois, uma rodada se completa a cada 26 letras. Há 26 posições (1 – 26) do anel para o rotor rápido e no meio (enquanto a posição do anel do rotor lento não importa, porque não implica um avanço de um cilindro em seguida), resultando em $26 \cdot 26 = 676$ possibilidades.
- Posição do **Rotor**: Determina em qual ponto a corrente inicialmente entra. Para cada um dos 3 rotores, há 26 possíveis posições (A – Z), resultando em $26 \cdot 26 \cdot 26 = 17.576$ posições. Por causa do mecanismo do escalonamento, $26 \cdot 26 = 676$ posições entre elas são criptograficamente redundantes, sobrando $17.576 - 676 = 16.900$ possibilidades.

...

- Ordem e Escolha dos **Cilindros:** Foram escolhidos 3 entre 5 cilindros (o lento, no meio e o rápido) em qualquer ordem, resultando em $5 \cdot 4 \cdot 3 = 60$ possibilidades.
- Conexões do **Painel**: Há até 13 cabos com dois conectores para conectar as 26 letras do alfabeto.
    1. Para o *primeiro* cabo, há 26 possibilidades para a letra do conector entrante e 25 possibilidades para a letra do conector sainte. Como não importa a ordem dos 2 conectores, sobram $[26 \cdot 25]/2$ possibilidades.
    2. Semelhantemente, para o *segundo* cabo, há 24 possibilidades para a letra do conector entrante e 23 possibilidades para a letra do conector sainte. Como não importa a ordem dos 2 conectores, sobram $[24 \cdot 23]/2$ possibilidades.
    3. ...

    Em geral, para o cabo n, há $n(n-1)/2$ possibilidades.

...

Como a ordem em que os 13 pares de letras foram conectadas pelos cabos não importa, divide-se por $13 \cdot 12 \cdots 2 \cdot 1 = 13!$.

Ao total, obtemos

$$26 \cdot 25 \cdot 24 \cdot 23 \cdots 2 \cdot 1 / (2 \cdots 2) \cdot (13 \cdot 12 \cdots 1)$$

possibilidades. Durante a guerra, a partir de Agosto 1939, foram conectados 10 pares de letras, dando

$$26 \cdot 25 \cdot 24 \cdot 23 \cdots 8 \cdot 7 / (2 \cdots 2) \cdot (10 \cdot 9 \cdots 1) = 150.738.274.937.250$$

possibilidades.

Número de Chaves da Enigma

Resumimos que há

- 60 possibilidades para os **cilindros**,
- 676 possibilidades para as posições dos **anéis**,
- 16.900 possibilidades para as posições dos **rotores**, e
- 150.738.274.937.250 possibilidades para os **conectores** do painel de ligações,

o que dá ao total

$$60 \cdot 676 \cdot 16.900 \cdot 150.738.274.937.250 \sim 10^{23} \sim 80 \text{ bit}$$

possibilidades. (Por exemplo, o DES (= Data Encryption Standard) utiliza uma chave de 56 bits.)

Simplificações

Observamos que as mensagens enviadas tiveram, por ordem, um comprimento máximo de 250 letras. Por isso, na prática,

- a posição do anel do cilindro no meio quase não importava, porque só avançou a um múltiplo (= 13 em média) de 26. Isto é, este avanço raramente ocorreu.
- a posição do anel do cilindro rápido importava mais, mas não tanto, porque em média valia 13 > o comprimento da maioria das palavras alemães.

Por isso, criptograficamente importam

- as 60 possibilidades para os cilindros,
- as 16.900 possibilidades para as posições dos cilindros, e
- as $150.738.274.937.250$ possibilidades para os pares de letras conectados pelos cabos,

A Bomba de Turing

A *bomba de Turing* (o nome deriva-se do som de uma bomba-relógio que a primeira tal máquina, a bomba criptográfica polonesa, emitia) ajudou a reduzir estas possibilidades, sobretudo as do maior fator, as das ligações do painel. Assim, sobraram ainda

$$60 \cdot 17.576 = 1.054.560$$

possibilidades. Considerando a força de trabalho de 4200 pessoas (das quais 80% mulheres) em Bletchley Park, o centro criptográfico inglês, neste ponto, um **ataque de força bruta** é viável: provar exaustivamente todas as possibilidades sobrantes.

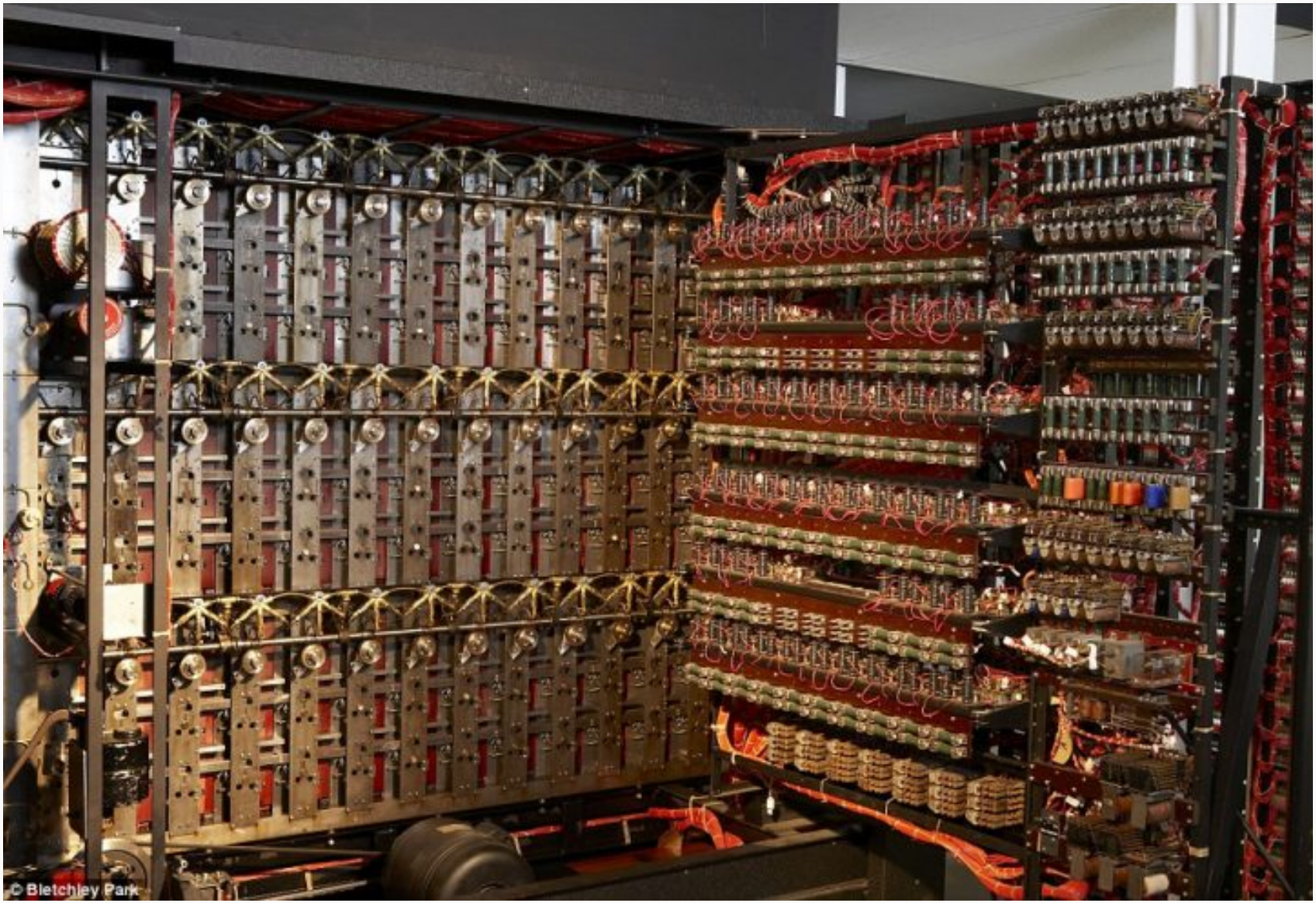


Figura 10: O interior da Bomba de Turing

O Crib

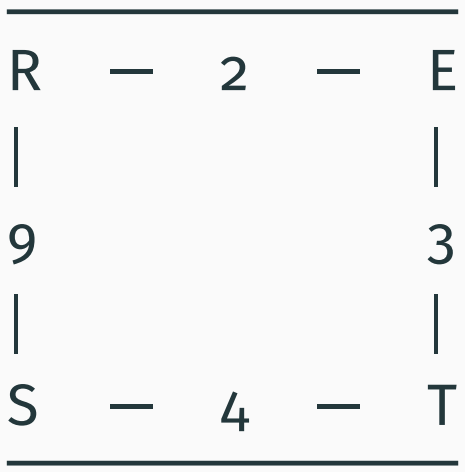
1. Intui o **crib**, uma palavra provável, por exemplo,
   - `OBERKOMMANODERWEHRMACHT`, (= comando supremo do exercito alemão)
   - `WETTERBERICHT` (= previsão do tempo)
   - `EINS` (= o número um)

   e compara com um trecho do texto cifrado. Para encontrar o trecho certo, toma em conta que a Enigma nunca cifrou uma letra a si mesma!

1	2	3	4	5	6	7	8	9	10	11	12	13
W	E	T	T	E	R	B	E	R	I	C	H	T
A	R	E	S	T	U	W	L	S	K	H	I	O

O menu

2. Cria o **menu**, um diagrama que associa as letras do texto claro às do texto cifrado; aqui obtemos o circuíto



Isto é, são trocados

- R e E na segunda posição,
- E e T na terceira posição,
- T e S na quarta posição, e
- S e R na nona posição.

O conector

3. Intui um **conector** do painel de ligações que troca uma das letras co circuito, por exemplo a troca entre R e Z.

Então, a *Bomba de Turing*, fixados

- uma **palavra provável**, aqui WETTERBERICHT,
- o texto cifrado, aqui ARESTUWLSKHIO, e
- um **conector** no painel de ligações, aqui entre R e Z

provou cada posição de cilindros para a sua compatibilidade com os circuitos do menu, da seguinte maneira:

Recordemo-nos de que a substituição de uma letra pela Enigma se descreve pela concatenação M das substituições seguintes

$$\mathrm{M} = \mathrm{P} \circ \mathrm{E} \circ \mathrm{C_R} \circ \mathrm{C_M} \circ \mathrm{C_L} \circ \mathrm{R} \circ \mathrm{C_L^{-1}} \mathrm{C_M^{-1}} \mathrm{C_R^{-1}} \circ \mathrm{E^{-1}} \circ \mathrm{P}$$

onde

- P é a substituição pelo painel de ligações
- E é a substituição pelo cilindro de entrada
- R é a substituição pelo cilindro de retorno.
- $\mathrm{C_R}$, $\mathrm{C_M}$ e $\mathrm{C_L}$ são as substituições pelo cilindro rápido, médio e lento.

Para facilitar,

- tomamos em conta que $\mathrm{E} = \mathrm{id}$ é a identidade, e
- abreviamos

$$\mathrm{C} := \mathrm{C_R} \circ \mathrm{C_M} \circ \mathrm{C_L} \circ \mathrm{R} \circ \mathrm{C_L^{-1}} \mathrm{C_M^{-1}} \mathrm{C_R^{-1}}$$

Isto é,

$$\mathrm{M} = \mathrm{P} \circ \mathrm{C} \circ \mathrm{P}$$

Para destacar a dependência da substituição C da posição p da letra no texto a cifrar (pelo avanço do cilindro rápido a cada letra teclada), denote

$$\mathrm{C}(p) = \text{ a substituição pelos cilindros na posição } p \text{ do texto.}$$

Aqui para $p = 2$, como $\mathrm{M}(\mathbf{R}) = \mathbf{E}$, obtemos

$$\mathbf{E} = \mathrm{P}(\mathrm{C}(2)(\mathrm{P}(\mathbf{R}))).$$

Temos

$$\mathbf{E} = \mathrm{P}(\mathrm{C}(2)(\mathrm{P}(\mathbf{R}))).$$

Como o painel de ligação troca as letras em pares, a substituição pelo painel de ligação é auto-inversa, isto é, $\mathrm{P} \circ \mathrm{P} = \text{identidade}$. Por isso, ao aplicarmos P a ambos lados desta equação,

$$\mathrm{P}(\mathbf{E}) = \mathrm{C}(2)(\mathrm{P}(\mathbf{R}));$$

Em seguida, da mesma maneira,

$$\mathrm{P}(\mathbf{T}) = \mathrm{C}(3)(\mathrm{P}(\mathbf{E})) = \mathrm{C}(3)\mathrm{C}(2)(\mathrm{P}(\mathbf{R}));$$

e assim por diante para as outras letras no circuito, até

$$\mathrm{P}(\mathbf{R}) = \mathrm{C}(9) \circ \mathrm{C}(4) \circ \mathrm{C}(3) \circ \mathrm{C}(2)(\mathrm{P}(\mathbf{R})),$$

fechando o circuito.

Utilidade da Bomba de Turing

Isto é, sob esta configuração dos cilindros, obtemos que a substituição $\mathrm{C} = \mathrm{C}(9)\mathrm{C}(4)\mathrm{C}(3)\mathrm{C}(2)$ deixa a letra $\mathrm{P}(\mathbf{R})$ invariante,

$$\mathrm{C}(\mathrm{P}(\mathbf{R})) = \mathrm{P}(\mathbf{R}).$$

Concluímos que cada tal circuito (obtido pelo texto claro e cifrado) exclui muitas configurações. A Bomba calculou as quais.

Alan Turing calculou quantas configurações de posições de cilindros são em média compatíveis para um *Crib* com dado número de circuitos e letras :

circuitos \ letras	8	9	10	11	12	13	14
3	2.2	1.1	0.42	0.14	0.04	<0.01	<0.01
2	58	28	11	3.8	1.2	0.30	0.06
1	1500	720	280	100	31	7.7	1.6

As equações acima implicam também, a partir de

- uma configuração válida e
- a troca de uma letra do circuito por um conector do painel de ligações,

todas as outras trocas das letras no circuito pelo painel de ligações:

Por exemplo, dado $\mathrm{P}(\mathbf{R})$, o valor $\mathrm{P}(\mathbf{E})$ define-se por

$$\mathrm{P}(\mathbf{E}) = \mathrm{C}(2)(\mathrm{P}(\mathbf{R}));$$

em seguida,

$$\mathrm{P}(\mathbf{T}) = \mathrm{C}(9)(\mathrm{P}(\mathbf{E})) = \mathrm{C}(9)\mathrm{C}(2)(\mathrm{P}(\mathbf{R}));$$

e assim por diante, obtendo as trocas de todas as letras do circuito: **R**, **E**, **T** e **S**.

Utilidade

Como a validade da chave era um **dia**, e a **mesma** entre todas as naves (e entre todas as aeronaves e entre todos os trens), logo que uma chave foi obtida, **todas as mensagens entre todas as naves** durante este dia podiam ser decifradas com ela.

Mudavam as posições dos rotores e conectores do painel cada dia, e a escolha e ordem dos cilindros cada mês.

Destacamos a **importância do `crib`**, da palavra típica alemã, neste método. Os aliados até provocaram pelas suas manobras certas mensagens para aplicar este método. Caso contrário, não conseguiram por exemplo decifrar a comunicação entre os condutores de trem por desconhecimento do jargão (= gírias profissionais) entre eles.

Anotações

Estão **disponíveis**

- os **eslaides** desta palestra e
- um **manuscrito** sobre criptografia que aprofunda o que aprendemos

online em `konfekt.bitbucket.io/talks/criptografia`

1. Exemplos: Históricos
2. Criptografia Simétrica
3. Exemplo: `Enigma`