L'Enigma, la màquina de xifrar quasi perfecta
Dissabtes de les Matemàtiques

Rosa Camps
Departament de Matemàtiques
Universitat Autònoma de Barcelona

18 de març de 2023

Índex

De Juli Cèsar a la màquina Enigma

La màquina Enigma

Introducció

text en clar

canal insegur

text en clar

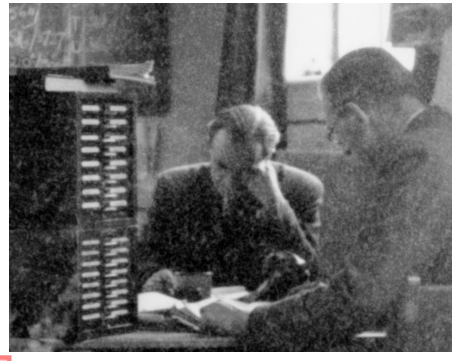
Introducció

text en clar

xifratge

missatge xifrat

canal insegur



missatge xifrat

desxifratge

text en clar

Introducció

text en clar

xifratge

missatge xifrat

canal insegur

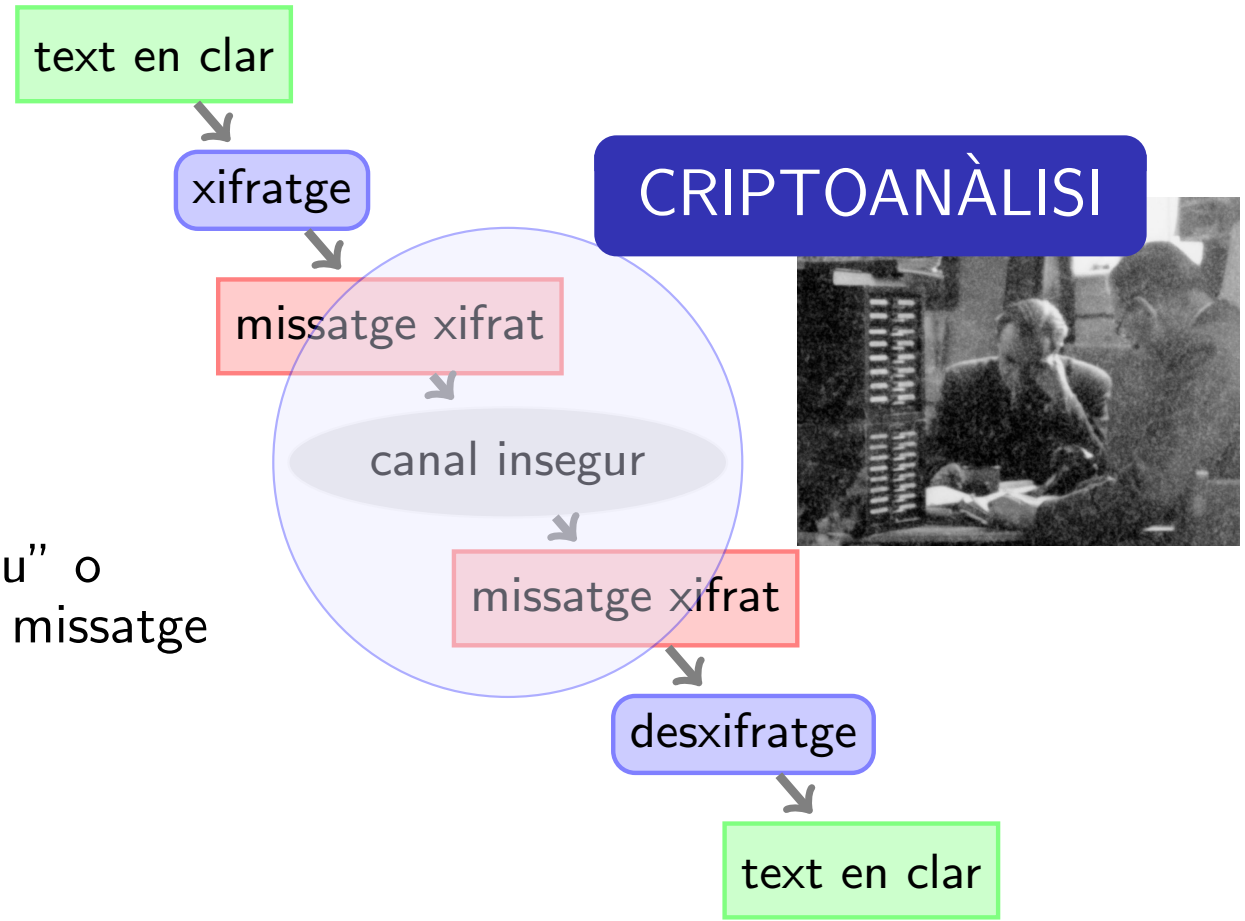
missatge xifrat

desxifratge

text en clar

CRIPTOSISTEMA

Introducció



"trencar la clau" o
"craquejar" el missatge

Mètodes de substitució

Criptosistema de Cèsar o de desplaçament

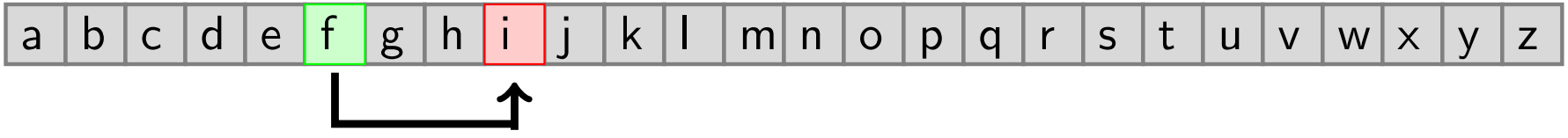
Substitueix cada lletra per la lletra que hi ha tres posicions més endavant a l'alfabet.
(Suetoni, Vides dels dotze Cèsars)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Mètodes de substitució

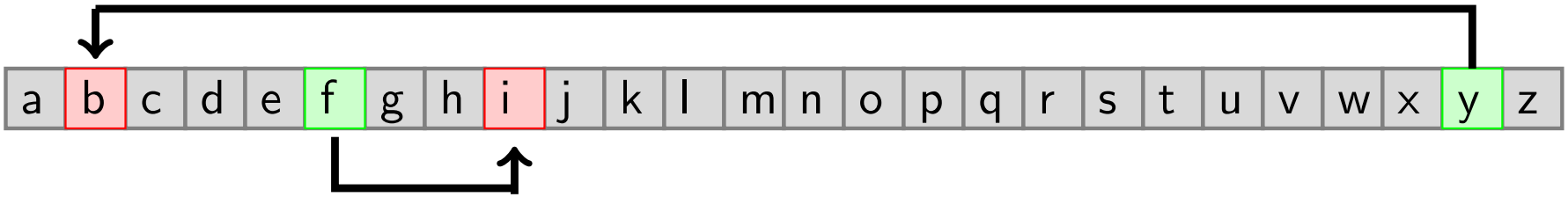
Criptosistema de Cèsar o de desplaçament

Substitueix cada lletra per la lletra que hi ha tres posicions més endavant a l'alfabet.
(Suetoni, Vides dels dotze Cèsars)



Criptosistema de Cèsar o de desplaçament

Substitueix cada lletra per la lletra que hi ha tres posicions més endavant a l'alfabet.
(Suetoni, Vides dels dotze Cèsars)



Mètodes de substitució (Cèsar)

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Mètodes de substitució (Cèsar)

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

veni vidi vici

Mètodes de substitució (Cèsar)

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

veni vidi vici 

Mètodes de substitució (Cèsar)

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Mètodes de substitució (continuació)

Mètode Kama–Sutra (s. IV a.c.)

Les 64 arts que una dona ha de dominar:
els escacs, l'enquadernació, la jardineria, . . . i la criptografia!

Mètodes de substitució (continuació)

Mètode Kama–Sutra (s. IV a.c.)

a	b	d	e	f	j	k	l	m	o	r	y	z
t	c	i	h	u	s	q	n	x	w	g	p	v

- s'aparellen les 26 lletres de l'alfabet (13 parelles)
- per xifrar se substitueix cada lletra per la seva parella
- per desxifrar es fa el mateix

Mètodes de substitució (continuació)

Mètode Kama–Sutra (s. IV a.c.)

a	b	d	e	f	j	k	l	m	o	r	y	z
t	c	i	h	u	s	q	n	x	w	g	p	v

- s'aparellen les 26 lletres de l'alfabet (13 parelles)
- per xifrar se substitueix cada lletra per la seva parella
- per desxifrar es fa el mateix

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	t	c	b	i	h	u	r	e	d	s	q	n	x	l	w	y	k	g	j	a	f	z	o	m	p	v

a mitjanit al jardi
dels tarongers

Mètodes de substitució (continuació)

Mètode Kama–Sutra (s. IV a.c.)

a	b	d	e	f	j	k	l	m	o	r	y	z
t	c	i	h	u	s	q	n	x	w	g	p	v

- s'aparellen les 26 lletres de l'alfabet (13 parelles)
- per xifrar se substitueix cada lletra per la seva parella
- per desxifrar es fa el mateix

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	t	c	b	i	h	u	r	e	d	s	q	n	x	l	w	y	k	g	j	a	f	z	o	m	p	v

a mitjanit al jardi dels tarongers →

Mètodes de substitució (continuació)

Mètode Kama–Sutra (s. IV a.c.)

a	b	d	e	f	j	k	l	m	o	r	y	z
t	c	i	h	u	s	q	n	x	w	g	p	v

- s'aparellen les 26 lletres de l'alfabet (13 parelles)
- per xifrar se substitueix cada lletra per la seva parella
- per desxifrar es fa el mateix

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	t	c	b	i	h	u	r	e	d	s	q	n	x	l	w	y	k	g	j	a	f	z	o	m	p	v

a mitjanit al jardi dels tarongers → t xdastlda tn stgid ihnj atgwlrhgj

Mètodes de substitució (continuació)

Substitució arbitrària

- S'utilitza un alfabet xifrat qualsevol per fer la substitució
- per desxifrar es llegeix al revés la taula (de baix cap a dalt)

Mètodes de substitució (continuació)

Substitució arbitrària

- S'utilitza un alfabet xifrat qualsevol per fer la substitució
- per desxifrar es llegeix al revés la taula (de baix cap a dalt)

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	h	e	v	m	d	l	s	k	i	g	n	b	t	y	r	j	p	u	f	w	z	q	x	a	o	c

Mètodes de substitució (continuació)

Substitució arbitrària

- S'utilitza un alfabet xifrat qualsevol per fer la substitució
- per desxifrar es llegeix al revés la taula (de baix cap a dalt)

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	h	e	v	m	d	l	s	k	i	g	n	b	t	y	r	j	p	u	f	w	z	q	x	a	o	c

també es pot utilitzar una clau per generar l'alfabet xifrat

clau:
VIATGE AL CENTRE DE LA TERRA

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Mètodes de substitució (continuació)

Substitució arbitrària

- S'utilitza un alfabet xifrat qualsevol per fer la substitució
- per desxifrar es llegeix al revés la taula (de baix cap a dalt)

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	h	e	v	m	d	l	s	k	i	g	n	b	t	y	r	j	p	u	f	w	z	q	x	a	o	c

també es pot utilitzar una clau per generar l'alfabet xifrat

clau:
VIATGE AL CENTRE DE LA TERRA

alfabet en clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
alfabet xifrat	v	i	a	t	g	e	l	c	n	r	d	b	f	h	j	k	j	m	o	p	s	u	w	x	y	z

Atac per força bruta

Provar totes les possibles claus fins obtenir un missatge amb sentit.

- Factible si el nombre de claus és petit. Cèsar: 25 claus.

Atac per força bruta

Provar totes les possibles claus fins obtenir un missatge amb sentit.

- Factible si el nombre de claus és petit. Cèsar: 25 claus.
- Impossible en substitució arbitrària:
  $26! - 1 = 403\,291\,461\,126\,605\,635\,584\,000\,000 \approx 4x10^{26}$.

Atac per força bruta

Provar totes les possibles claus fins obtenir un missatge amb sentit.

- Factible si el nombre de claus és petit. Cèsar: 25 claus.
- Impossible en substitució arbitrària:
  $26! - 1 = 403\,291\,461\,126\,605\,635\,584\,000\,000 \approx 4x10^{26}$.
- Impossible també en Kama–Sutra:
  $\frac{26!}{13!\,2^{13}} = 25 \times 23 \times .. \times 3 = 7905853580625 \approx 7.9x10^{12}$.

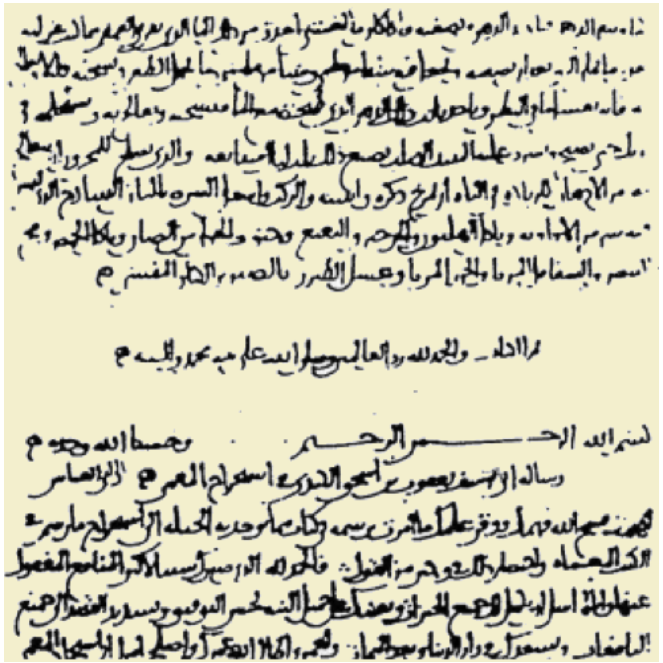
Atac per força bruta

Provar totes les possibles claus fins obtenir un missatge amb sentit.

- Factible si el nombre de claus és petit. Cèsar: 25 claus.
- Impossible en substitució arbitrària:
  $26! - 1 = 403\,291\,461\,126\,605\,635\,584\,000\,000 \approx 4x10^{26}$.
- Impossible també en Kama–Sutra:
  $\frac{26!}{13!\,2^{13}} = 25 \times 23 \times .. \times 3 = 7905853580625 \approx 7.9x10^{12}$.

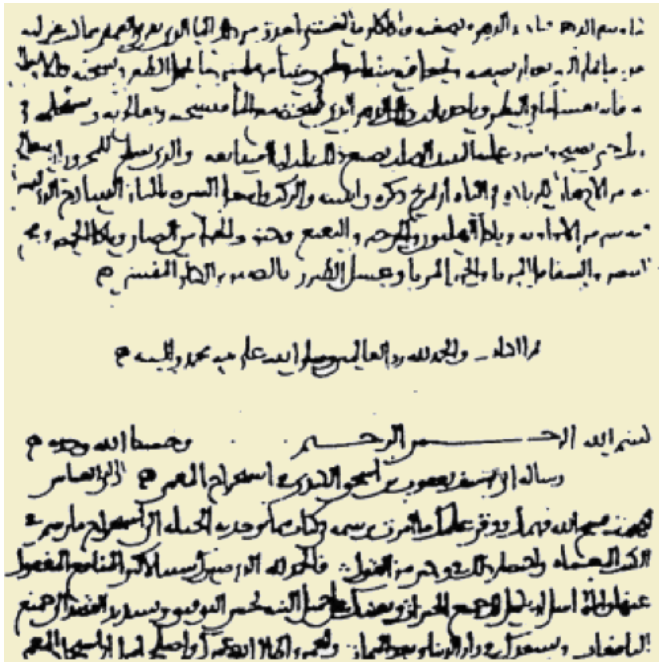
Cal tenir en compte que la informació caduca.

Naixement de la criptoanàlisi (Bagdad, s IX)



Al Kindi (s. IX)
"Sobre el desxiframent de missatges criptogràfics"

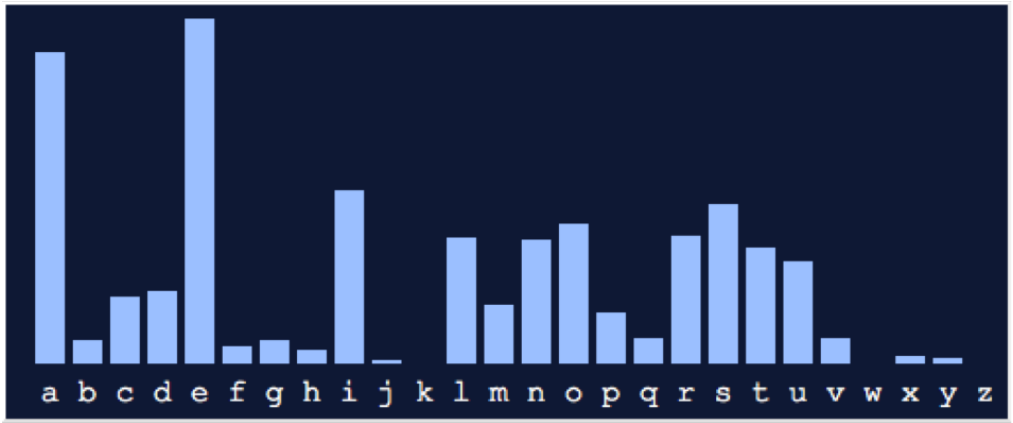
Naixement de la criptoanàlisi (Bagdad, s IX)



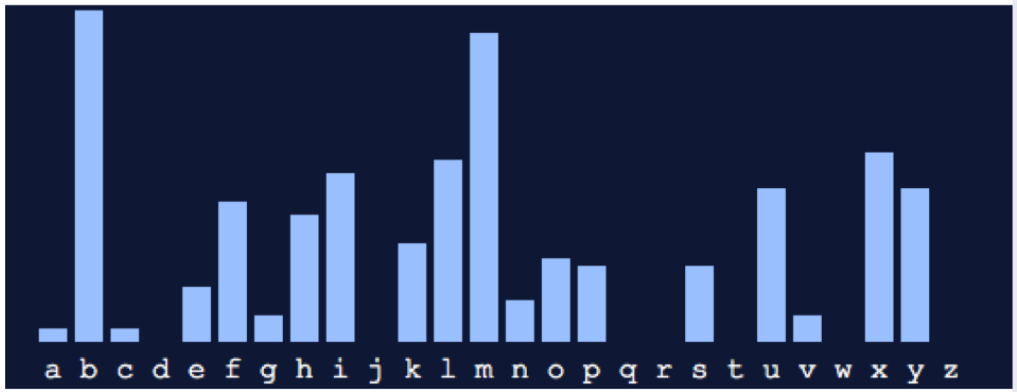
Al Kindi (s. IX)
"Sobre el desxiframent de missatges criptogràfics"

Mètode d'anàlisi de freqüències

Naixement de la criptoanàlisi (Bagdad, s IX)



Freqüències de les lletres en català

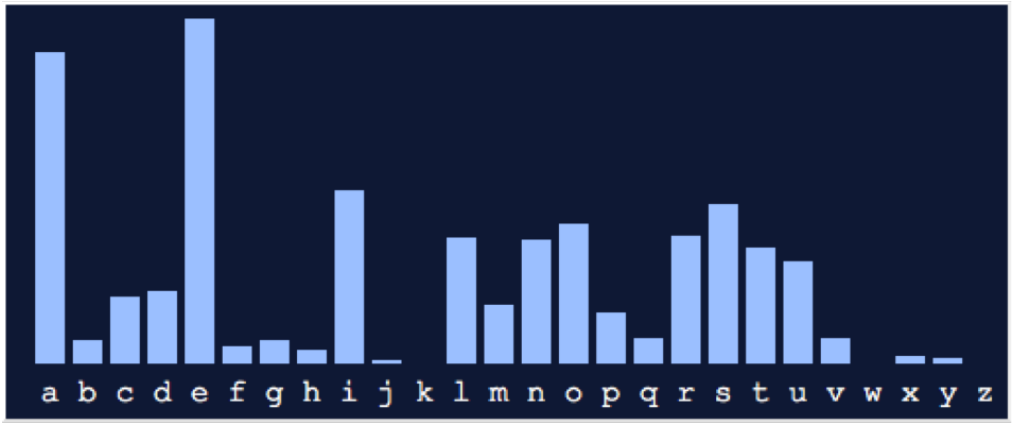


Freqüències de les lletres en el missatge xifrat

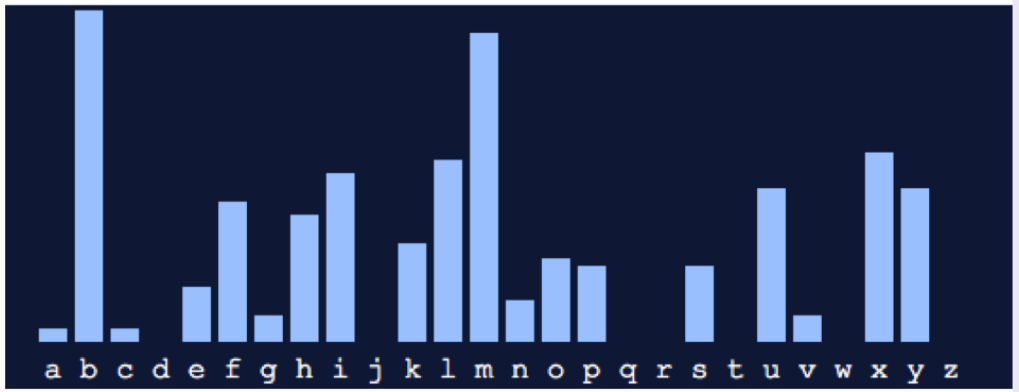
Mètode d'anàlisi de freqüències

- Comparació de freqüències de les lletres en el llenguatge del missatge en clar i en el text xifrat.

Naixement de la criptoanàlisi (Bagdad, s IX)



Freqüències de les lletres en català

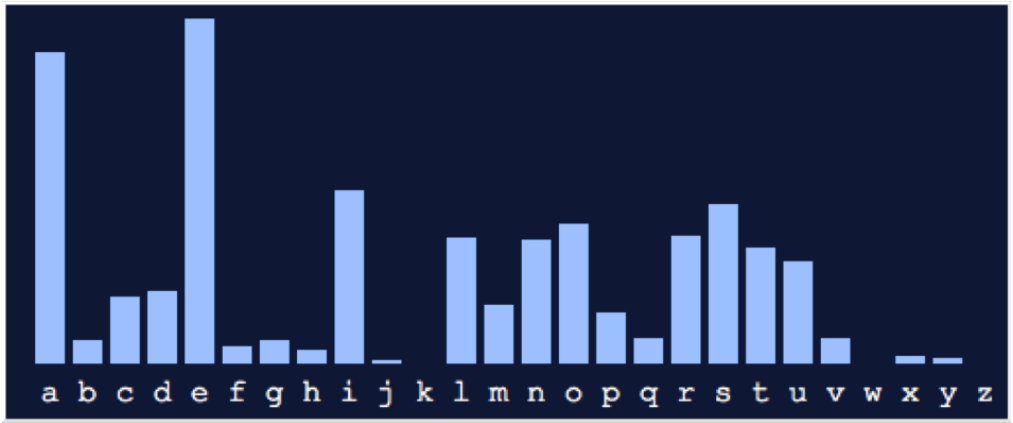


Freqüències de les lletres en el missatge xifrat

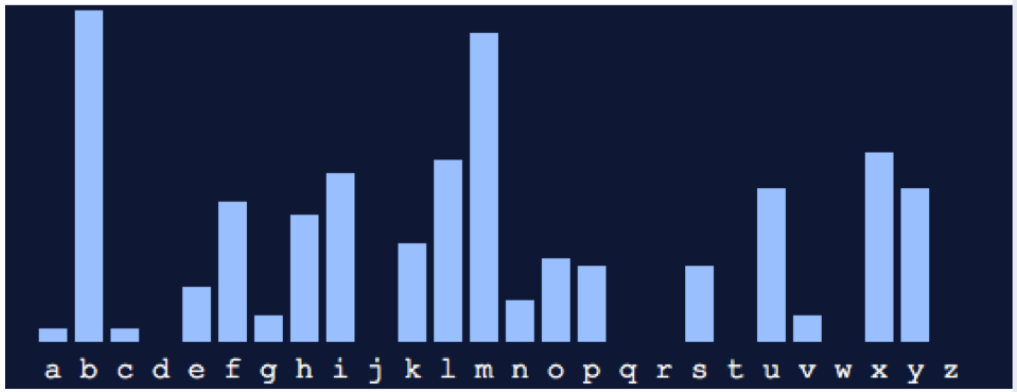
Mètode d'anàlisi de freqüències

- Comparació de freqüències de les lletres en el llenguatge del missatge en clar i en el text xifrat.
- Estudi de síl·labes.

Naixement de la criptoanàlisi (Bagdad, s IX)



Freqüències de les lletres en català

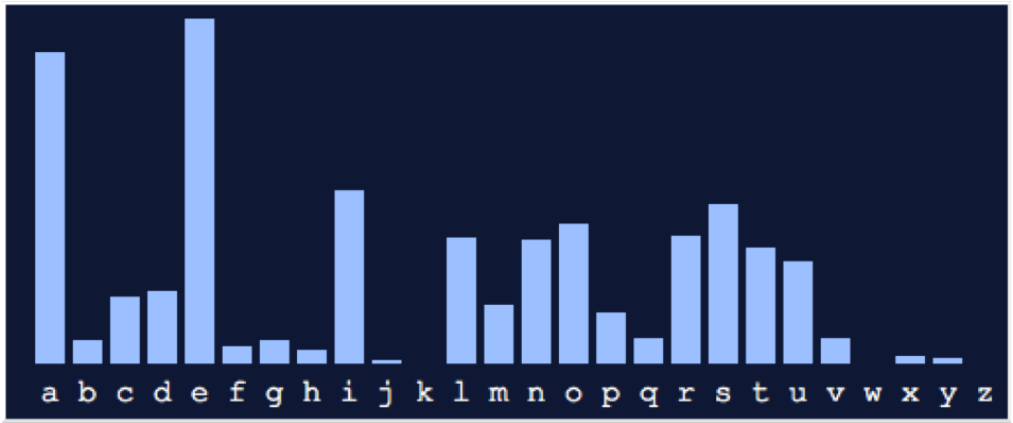


Freqüències de les lletres en el missatge xifrat

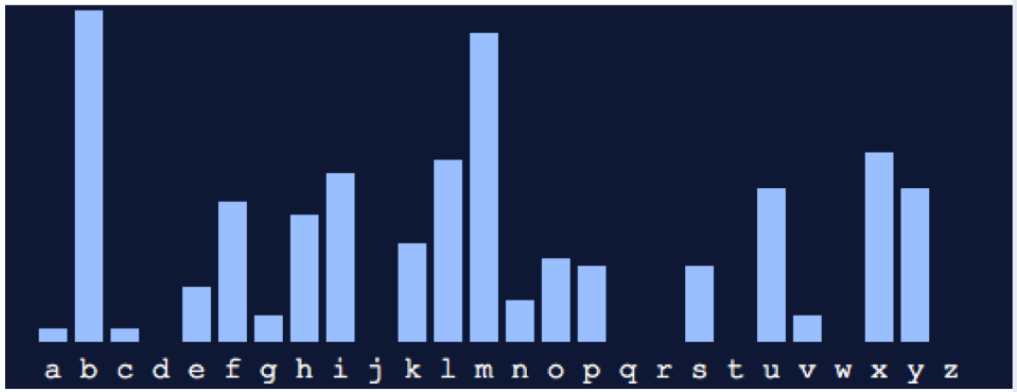
Mètode d'anàlisi de freqüències

- Comparació de freqüències de les lletres en el llenguatge del missatge en clar i en el text xifrat.
- Estudi de síl·labes.
- Propietats d'aparellament de les lletres.

Naixement de la criptoanàlisi (Bagdad, s IX)



Freqüències de les lletres en català

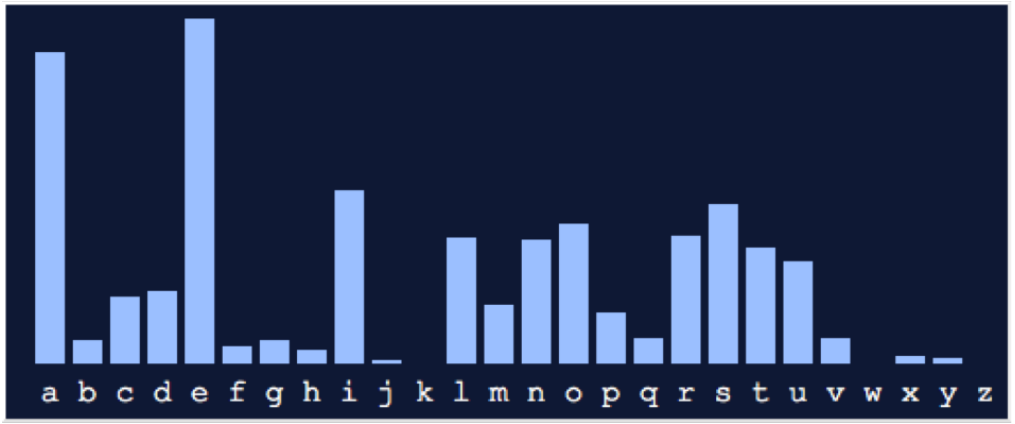


Freqüències de les lletres en el missatge xifrat

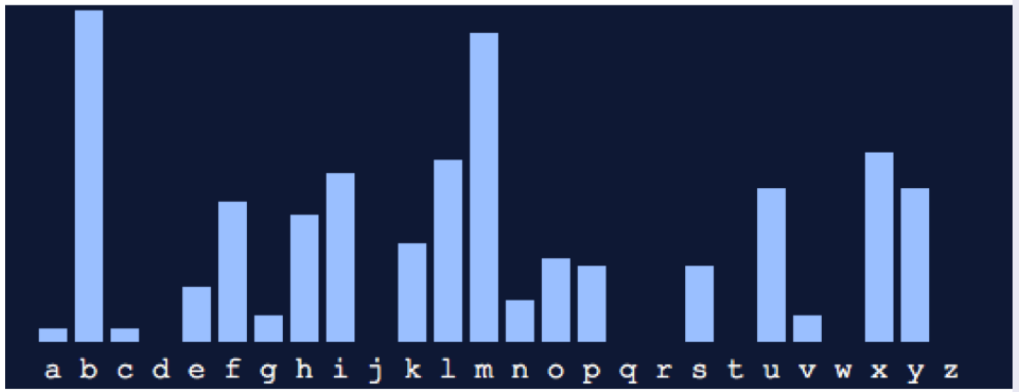
Mètode d'anàlisi de freqüències

- Comparació de freqüències de les lletres en el llenguatge del missatge en clar i en el text xifrat.
- Estudi de síl·labes.
- Propietats d'aparellament de les lletres.
- Paraules freqüents.

Naixement de la criptoanàlisi (Bagdad, s IX)



Freqüències de les lletres en català



Freqüències de les lletres en el missatge xifrat

Mètode d'anàlisi de freqüències

- Comparació de freqüències de les lletres en el llenguatge del missatge en clar i en el text xifrat.
- Estudi de síl·labes.
- Propietats d'aparellament de les lletres.
- Paraules freqüents.
- Lletres dobles.

- Un bon criptosistema ha d'amagar les propietats estadístiques del text en clar.

Primera lliçó

- Un bon criptosistema ha d'amagar les propietats estadístiques del text en clar.
- El text xifrat hauria de semblar aleatori.

- Un bon criptosistema ha d'amagar les propietats estadístiques del text en clar.
- El text xifrat hauria de semblar aleatori.
- Si bé un conjunt de claus gran és sufucient per protegir-se de l'atac per força bruta, no és garantia de seguretat davant d'altres atacs.

Com contrarestar l'anàlisi de freqüències?

- Substituir parelles de lletres.

Com contrarestar l'anàlisi de freqüències?

- Substituir parelles de lletres.
- Codificar paraules senceres freqüents.

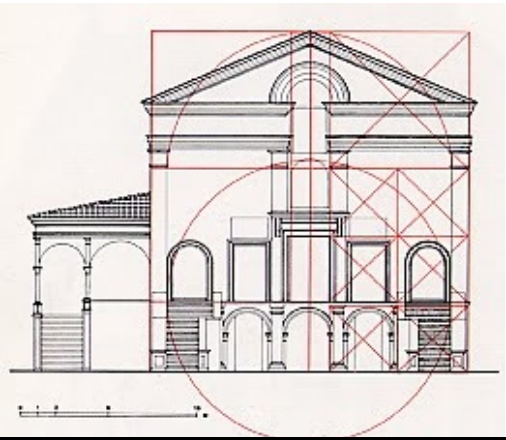
Com contrarestar l'anàlisi de freqüències?

- Substituir parelles de lletres.
- Codificar paraules senceres freqüents.
- Substituir les lletres més freqüents per més d'un símbol.

Una idea genial i senzilla

Leon Battista Alberti (1404 - 1472)

pintor, poeta, arquitecte i teòric de l'art, músic i criptògraf ("De componendis xifris")



Una idea genial i senzilla

Leon Battista Alberti (1404 - 1472)

Canviar d'alfabet xifrat per fer la substitució durant el xifratge d'un sol missatge

Una idea genial i senzilla

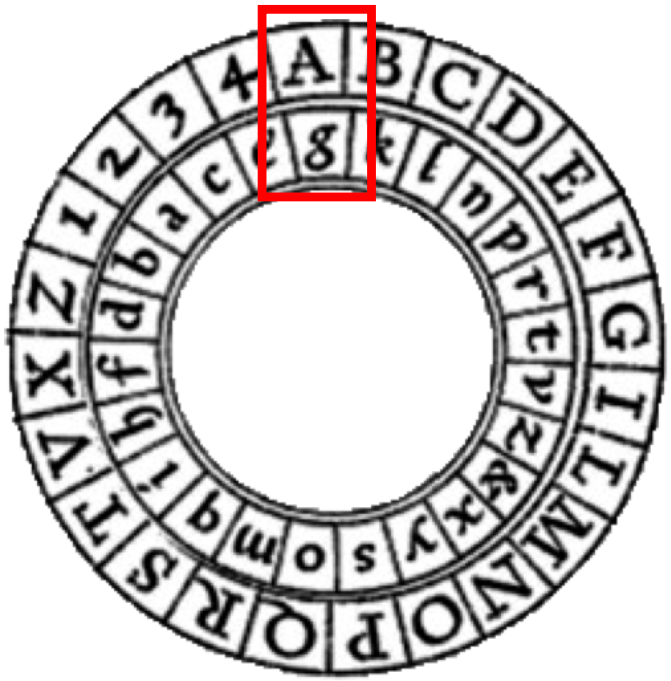
Leon Battista Alberti (1404 - 1472)

Canviar d'alfabet xifrat per fer la substitució durant el xifratge d'un sol missatge

Una idea genial i senzilla

Leon Battista Alberti (1404 - 1472)

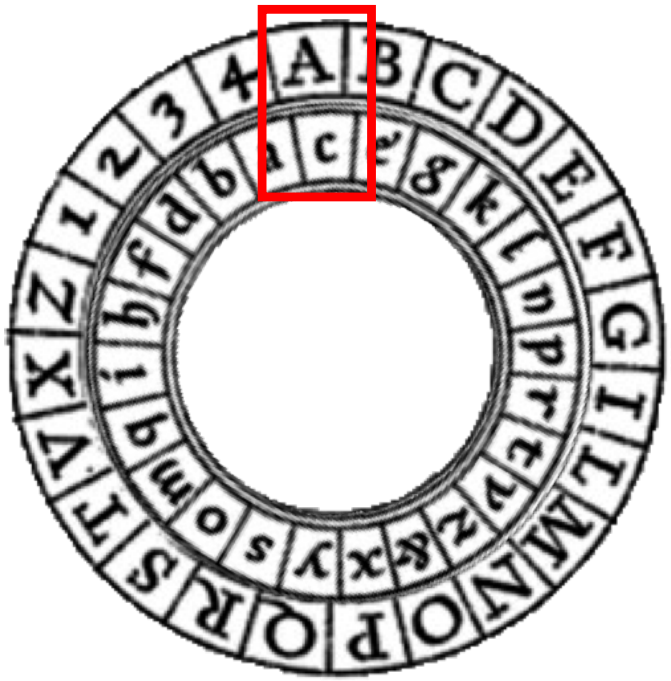
Canviar d'alfabet xifrat per fer la substitució durant el xifratge d'un sol missatge



Una idea genial i senzilla

Leon Battista Alberti (1404 - 1472)

Canviar d'alfabet xifrat per fer la substitució durant el xifratge d'un sol missatge



El xifratge de Vigenère (1523)

El xifratge de Vigenère (1523)

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

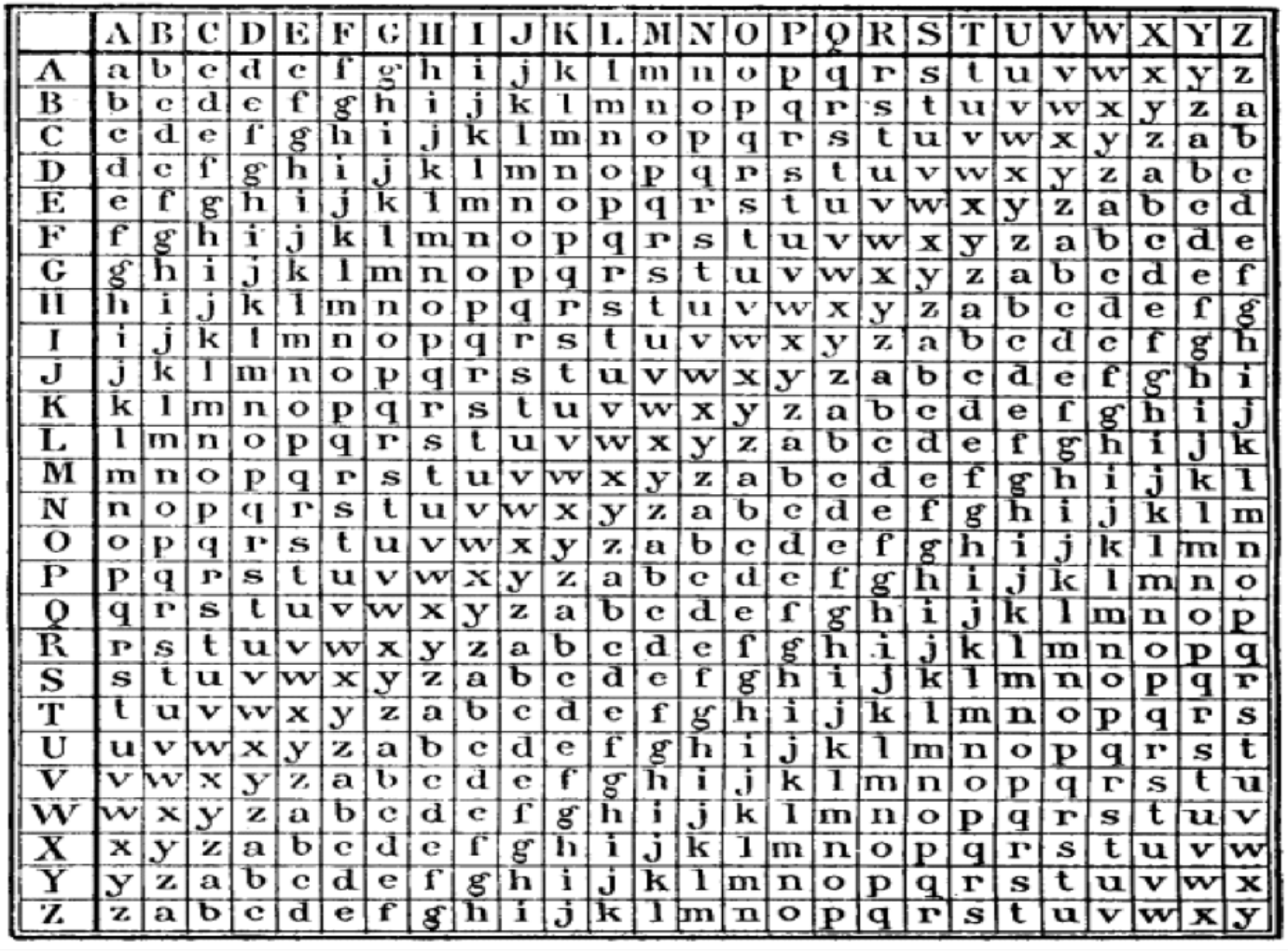
El xifratge de Vigenère (1523)

tria uns quants dels alfabets xifrats de la taula

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

El xifratge de Vigenère (1523)

tria uns quants dels alfabets xifrats de la taula



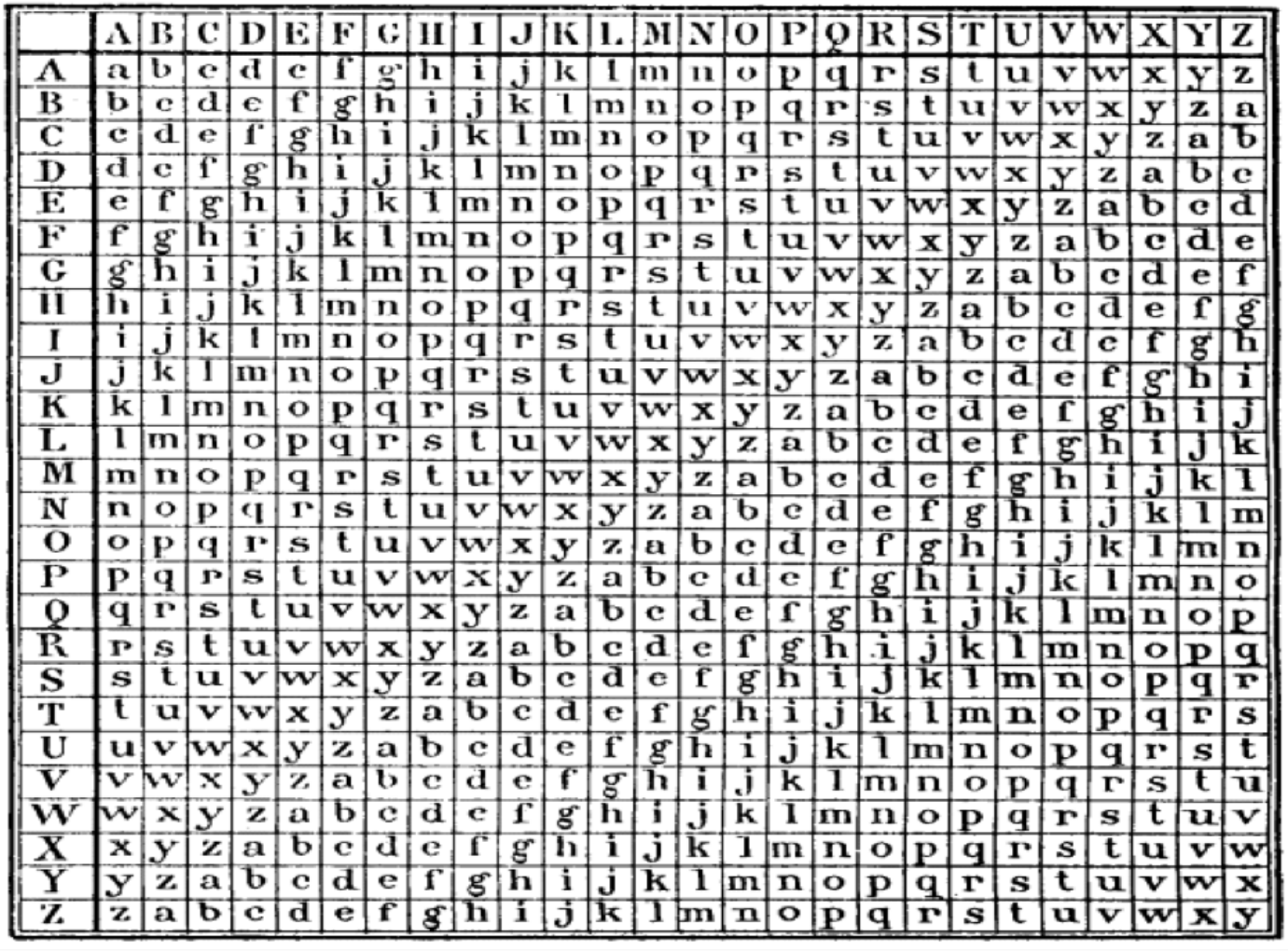
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t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

El xifratge de Vigenère (1523)

tria uns quants dels alfabets xifrats de la taula

clau: TREN

la clau en determina l'ordre d'ús



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

El xifratge de Vigenère (1523)

tria uns quants dels alfabets xifrats de la taula

clau: TREN

la clau en determina l'ordre d'ús

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

El xifratge de Vigenère (1523)

tria uns quants dels alfabets xifrats de la taula

clau: TREN

la clau en determina l'ordre d'ús

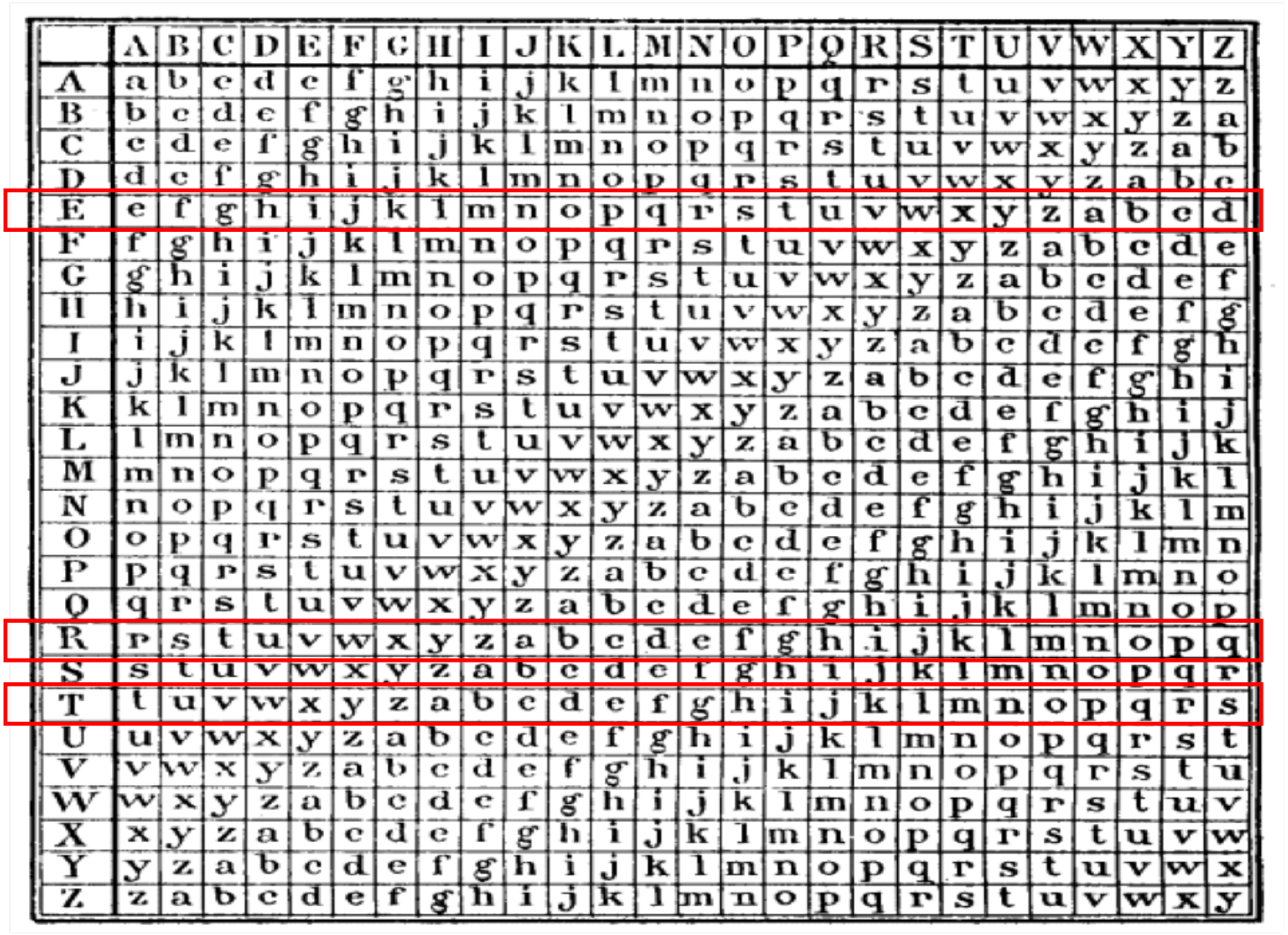
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t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

El xifratge de Vigenère (1523)

tria uns quants dels alfabets xifrats de la taula

clau: TREN

la clau en determina l'ordre d'ús



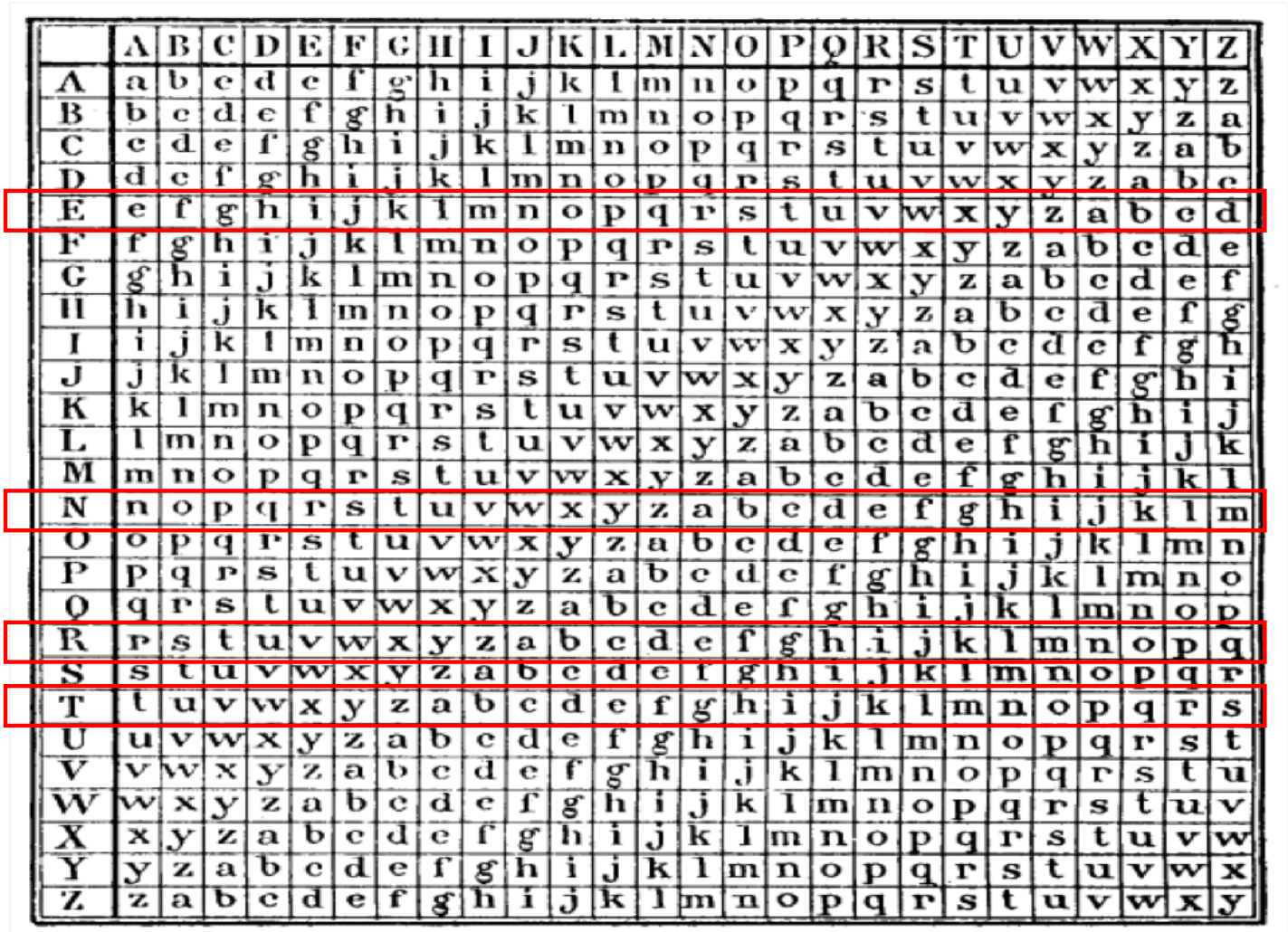
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t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

El xifratge de Vigenère (1523)

tria uns quants dels alfabets xifrats de la taula

clau: TREN

la clau en determina l'ordre d'ús



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

El xifratge de Vigenère (1523)

clau: TREN

a.clar

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

El xifratge de Vigenère (1523)

clau: TREN

a.clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

El xifratge de Vigenère (1523)

clau: TREN

a.clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q

El xifratge de Vigenère (1523)

clau: TREN

a.clar

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d

El xifratge de Vigenère (1523)

clau: TREN

a.clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
4 alfabets xifrats	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m

El xifratge de Vigenère (1523)

clau: TREN

a.clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
4 alfabets xifrats	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m

m.clar	e	l		m	i	s	s	a	t	g	e	r		e	s		u	n		t	r	a	i	d	o	r
clau	t	r		e	n	t	r	e	n	t	r	e		n	t		r	e		n	t	r	e	n	t	r
m.xifrat	x	c		q	v	l	j	e	g	z	v	v		r	l		l	r		g	k	r	m	q	h	i

El xifratge de Vigenère (1523)

clau: TREN

a.clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q			u	v	w	x	y	z
4 alfabets xifrats	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i					n	o	p	q	r	s
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f					k	l	m	n	o	p	q
	e	f	g	h	i	j	k	l	m	n	o	p	q						v	w	x	y	z	a	b	c	d
	n	o	p	q	r	s	t	u	v	w	x						d	e	f	g	h	i	j	k	l	m

m.clar	e	l		m	i	s	s							e	s		u	n		t	r	a	i	d	o	r
clau	t	r		e	n	t						r	e		n	t		r	e		n	t	r	e	n	t	r
m.xifrat	x	c		q	v	l	j			z	v	v		r	l		l	r		g	k	r	m	q	h	i

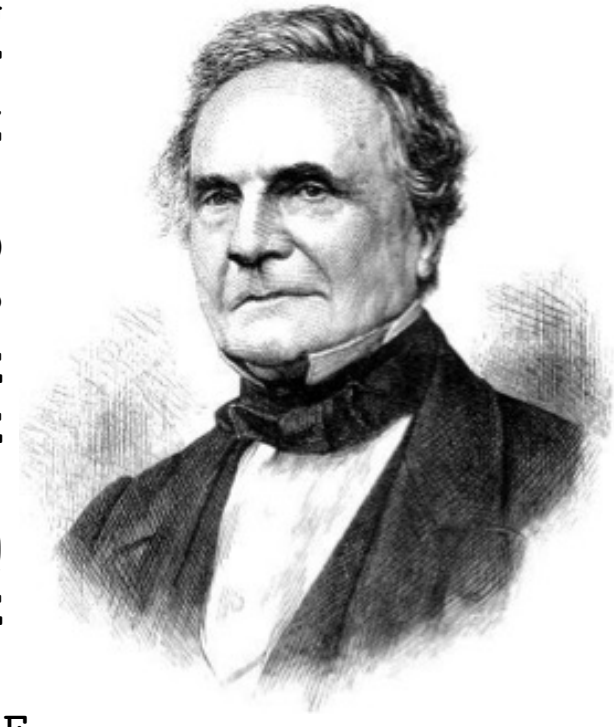
"La xifra indesxifrable"

Trencant Vigenère (Charles Babbage 1855)

TSQMSOEWGEWAXOEIJIAPRHIODRNYQEEEHEWRQAVPOEERRPDCUIGEW
EZIAEHXOOIEFIACPEPBDOFYETQFEEQIMGVWSEGGCIUSAHNHHLMG
HTHRRWPMHDQZGIURQBLIOSMFGMFLQGFIJUQBGWTUQDRVWAZMRRF
OZXHRWAYSAXDLQGCIUSABRWHLEBBQVDQZRWTUMZFESADSVBHNMZ
QSFUYSAXQUYSESWRQGNHMUZHRPSRUARVGIBCFMWVMQBRVIEHVV
HNYWYGDTAFMIOLUIEIVDQCEMWRQGZMOVGWGGHNFSFHRTLSYPLUD
SFHHPXOGEGIBCFMWAPSFIONAJRQERQRRQLLHIVXFEZHFHLNAIRP
VESCAIVVMFREOIFNNVHLPSFIPBDSQIPIXJHMWCQBGWYIZHVGRNE
WFXLAQBZMONAIPIQTQGYPLUDSFHHODWZMODAGPIQTQGIYLTMBGE
YUUHYPLUDSFHHPXOGEWAYPRNRIQGBFWIZUHHHSMGNRWLXIVWDC
MBIMGEBZNXDPQFSEFIXWGEUEXHEEQSBCEXGEXHEIVODWIEOODOQ
IVEZHEIWZQAVPGOXOEWWOFSYUXETSZIQCUCAEWEEHNIPBMZNXGE
YOAIUAESTYUAQBBPOEERRJHRDCNQETMDRWGERSEVRLMSKGDVM
QVSHSFOZIVOYSACVEZJBPWAPOQISEPFRWLLQGBPOEEFRTRSQBFSE
RQFBGDSAZVHDIQGGEQCAPRVWEEDRVDLFFRWHLBOCIUNGARVRUP
SFGUIGZNYEIOOPMREJOPXDDQZNIACMJNGLOBSEUXEZCUMKASWPES
DUTVGXLFOGIQTDCOEULMGRKRNMLVJUAPSOIDLQAVPYUUHPIQTEJVR
WXUTEEGAGGNRWCAANXHXFQYEXLMRRGOADOPMRDQWAHHPQBQIQ
CUOASUDMARVLCMBNIAPXWPEHLOCAXLNSIGHHLFFRWRRXOCVLMQF
NBLFDODYHCABGIOAGPVGDCUCQIOTDSFSUEZQNVDNAVNIVTMHQIVX
UTEEGA

Trencant Vigenère (Charles Babbage 1855)

TSQMSOEWGEWAXOEIJIAPRHIODRNYQEEEHEWRQAVPOEERRPDCUIGEW
EZIAEHXOOIEFIACPEPBDOFYETQFEEQIMGVWSEGGCIUSAHNHHLMG
HTHRRWPMHDQZGIURQBLIOSMFGMFLQGFIJUQBGWTUQDRVWAZMRRF
OZXHRWAYSAXDLQGCIUSABRWHLEBBQVDQZRWTUMZFESADSVBHNMZ
QSFUYSAXQUYSESWRQGNHMUZHRPSRUARVGIBCFMWVMQBRVIEHVV
HNYWYGDTAFMIOLUIEIVDQCEMWRQGZMOVGWGGHNFSFHRTLSYPLUD
SFHHPXOGEGIBCFMWAPSFIONAJRQERQRRQLLHIVXFEZHFHLNAIRP
VESCAIVVMFREOIFNNVHLPSFIPBDSQIPIXJHMWCQBGWYIZHVGRNE
WFXLAQBZMONAIPIQTQGYPLUDSFHHODWZMODAGPIQTQGIYLTMBGE
YUUHYPLUDSFHHPXOGEWAYPRNRIQGBFWIZUHHHSMGNRWLXIVWDC
MBIMGEBZNXDPQFSEFIXWGEUEXHEEQSBCEXGEXHEIVODWIEOODOQ
IVEZHEIWZQAVPGOXOEWWOFSYUXETSZIQCUCAEWEEHNIPBMZNXGE
YOAIUAESTYUAQBBPOEERRJHRDCNQETMDRWGERSEVRLMSKGDVM
QVSHSFOZIVOYSACVEZJBPWAPOQISEPFRWLLQGBPOEEFRTRSQBFSE
RQFBGDSAZVHDIQGGEQCAPRVWEEDRVDLFFRWHLBOCIUNGARVRUP
SFGUIGZNYEIOOPMREJOPXDDQZNIACMJNGLOBSEUXEZCUMKASWPES
DUTVGXLFOGIQTDCOEULMGRKRNMLVJUAPSOIDLQAVPYUUHPIQTEJVR
WXUTEEGAGGNRWCAANXHXFQYEXLMRRGOADOPMRDQWAHHPQBQIQ
CUOASUDMARVLCMBNIAPXWPEHLOCAXLNSIGHHLFFRWRRXOCVLMQF
NBLFDODYHCABGIOAGPVGDCUCQIOTDSFSUEZQNVDNAVNIVTMHQIVX
UTEEGA



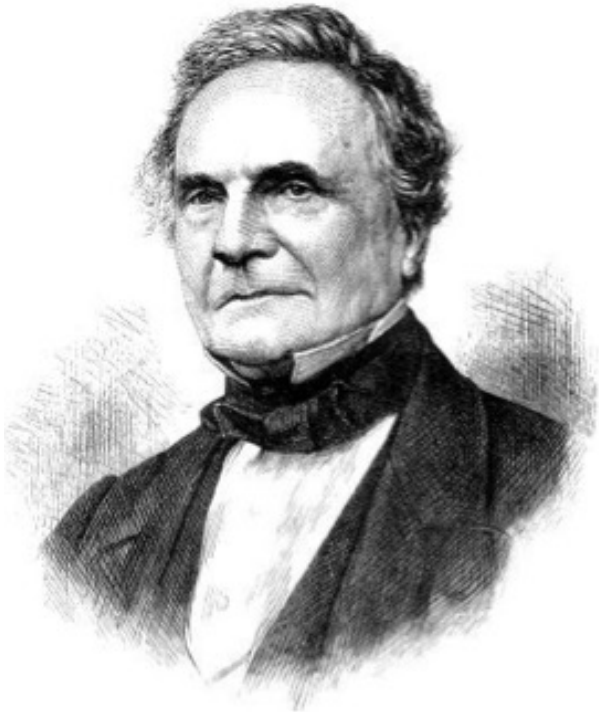
Trencant Vigenère (Charles Babbage 1855)

TSQMSOEWGEWAXOEIJIAPRHIODRNYQEEEHEWRQAVPOEERRPDCUIGEW
EZIAEHXOOIEFIACPEPBDOFYETQFEEQIMGVWSEGGCIUSAHNHHLMG
HTHRRWPMHDQZGIURQBLIOSMFGMFLQGFIJUQBGWTUQDRVWAZMRRF
OZXHRWAYSAXDLQGCIUSABRWHLEBBQVDQZRWTUMZFESADSVBHNMZ
QSFUYSAXQUYSESWRQGNHMUZHRPSRUARVGIBCFMWVMQBRVIEHVV
HNYWYGDTAFMIOLUIEIVDQCEMWRQGZMOVGWGGHNFSFHRTLSYPLUD
SFHHPXOGEGIBCFMWAPSFIONAJRQERQRRQLLHIVXFEZHFHLNAIRP
VESCAIVVMFREOIFNNVHLPSFIPBDSQIPIXJHMWCQBGWYIZHVGRNE
WFXLAQBZMONAIPIQTQGYPLUDSFHHODWZMODAGPIQTQGIYLTMBGE
YUUHYPLUDSFHHPXOGEWAYPRNRIQGBFWIZUHHHSMGNRWLXIVWDC
MBIMGEBZNXDPQFSEFIXWGEUEXHEEQSBCEXGEXHEIVODWIEOODOQ
IVEZHEIWZQAVPGOXOEWWOF
YOAIUAESTYUAQBBPOEERRJ
QVSHSFOZI
RQFBGDSAZ
SFGUIGZNY
DUTVGXLFO
WXUTEEGAG
CUOASUDMARVLCMBNIAPXWPEHLOCAXLNSIGHHLFFRWRRXOCVLMQF
NBLFDODYHCABGIOAGPVGDCUCQIOTDSFSUEZQNVDNAVNIVTMHQIVX
UTEEGA

L'anàlisi de freqüències és inútil

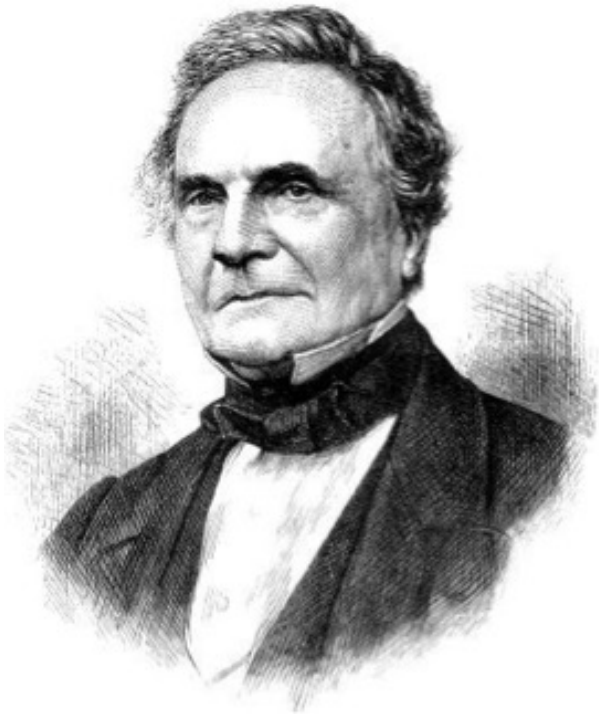
Trencant Vigenère (Charles Babbage 1855)

TSQMSOEWGEWAXOEIJIAPRHIODRNYQEEEHEWRQAVPOEERRPDCUIGEW
EZIAEHXOOIEFIACPEPBDOFYETQFEEQIMGVWSEGGCIUSAHNHHLMG
HTHRRWPMHDQZGIURQBLIOSMFGMFLQGFIJUQBGWTUQDRVWAZMRRF
OZXHRWAYSAXDLQGCIUSABRWHLEBBQVDQZRWTUMZFESADSVBHNMZ
QSFUYSAXQUYSESWRQGNHMUZHRPSRUARVGIBCFMWVMQBRVIEHVV
HNYWYGDTAFMIOLUIEIVDQCEMWRQGZMOVGWGGHNFSFHRTLSYPLUD
SFHHPXOGEGIBCFMWAPSFIONAJRQERQRRQLLHIVXFEZHFHLNAIRP
VESCAIVVMFREOIFNNVHLPSFIPBDSQIPIXJHMWCQBGWYIZHVGRNE
WFXLAQBZMONAIPIQTQGYPLUDSFHHODWZMODAGPIQTQGIYLTMBGE
YUUHYPLUDSFHHPXOGEWAYPRNRIQGBFWIZUHHHSMGNRWLXIVWDC
MBIMGEBZNXDPQFSEFIXWGEUEXHEEQSBCEXGEXHEIVODWIEOODOQ
IVEZHEIWZQAVPGOXOEWWOFSYUXETSZIQCUCAEWEEHNIPBMZNXGE
YOAIUAESTYUAQBBPOEERRJHRDCNQETMDRWGERSEVRLMSKGDVM
QVSHSFOZIVOYSACVEZJBPWAPOQISEPFRWLLQGBPOEEFRTRSQBFSE
RQFBGDSAZVHDIQGGEQCAPRVWEEDRVDLFFRWHLBOCIUNGARVRUP
SFGUIGZNYEIOOPMREJOPXDDQZNIACMJNGLOBSEUXEZCUMKASWPES
DUTVGXLFOGIQTDCOEULMGRKRNMLVJUAPSOIDLQAVPYUUHPIQTEJVR
WXUTEEGAGGNRWCAANXHXFQYEXLMRRGOADOPMRDQWAHHPQBQIQ
CUOASUDMARVLCMBNIAPXWPEHLOCAXLNSIGHHLFFRWRRXOCVLMQF
NBLFDODYHCABGIOAGPVGDCUCQIOTDSFSUEZQNVDNAVNIVTMHQIVX
UTEEGA



Trencant Vigenère (Charles Babbage 1855)

TSQMSOEWGEWAXOEIJIAPRHIODRNYQEEEHEWRQAVPOEERRPDCUIGEW
EZIAEHXOOIEFIACPEPBDOFYETQFEEQIMGVWSEGGCIUSAHNHHLMG
HTHRRWPMHDQZGIURQBLIOSMFGMFLQGFIJUQBGWTUQDRVWAZMRRF
OZXHRWAYSAXDLQGCIUSABRWHLEBBQVDQZRWTUMZFESADSVBHNMZ
QSFUYSAXQUYSESWRQGNHMUZHRPSRUARVGIBCFMWVMQBRVIEHVV
HNYWYGDTAFMIOLUIEIVDQCEMWRQGZMOVGWGGHNFSFHRTLSYPLUD
SFHHPXOGEGIBCFMWAPSFIONAJRQERQRRQLLHIVXFEZHFHLNAIRP
VESCAIVVMFREOIFNNVHLPSFIPBDSQIPIXJHMWCQBGWYIZHVGRNE
WFXLAQBZMONAIPIQTQGYPLUDSFHHODWZMODAGPIQTQGIYLTMBGE
YUUHYPLUDSFHHPXOGEWAYPRNRIQGBFWIZUHHHSMGNRWLXIVWDC
MBIMGEBZNXDPQFSEFIXWGEUEXHEEQSBCEXGEXHEIVODWIEOODOQ
IVEZHEIWZQAVPGOXOEWWOFSYUXETSZIQCUCAEWEEHNIPBMZNXGE
YOAIUAESTYUAQBBPOEERRJHRDCNQETMDRWGERSEVRLMSKGDVM
QVSHSFOZIVOYSACVEZJBPWAPOQISEPFRWLLQGBPOEEFRTRSQBFSE
RQFBGDSAZVHDIQGGEQCAPRVWEEDRVDLFFRWHLBOCIUNGARVRUP
SFGUIGZNYEIOOPMREJOPXDDQZNIACMJNGLOBSEUXEZCUMKASWPES
DUTVGXLFOGIQTDCOEULMGRKRNMLVJUAPSOIDLQAVPYUUHPIQTEJVR
WXUTEEGAGGNRWCAANXHXFQYEXLMRRGOADOPMRDQWAHHPQBQIQ
CUOASUDMARVLCMBNIAPXWPEHLOCAXLNSIGHHLFFRWRRXOCVLMQF
NBLFDODYHCABGIOAGPVGDCUCQIOTDSFSUEZQNVDNAVNIVTMHQIVX
UTEEGA



Trencant Vigenère (Charles Babbage s.XIX)

No pot ser per casualitat.

m.clar	..	l	s	a	r	t	i	c	l	e	s	s	e	g	u	e	n	t	s	q	u	e	p	e	r
clau	..	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e
m.xifrat	..	o	s	m	f	g	m	f	l	q	g	f	i	j	u	q	b	g	w	t	u	q	d	r	v

m.clar	t	a	n	y	e	n	c	o	n	j	u	n	t	a	m	e	n	t	a	l	e	s	p	e	..
clau	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e	..
m.xifrat	w	a	z	m	r	r	f	o	z	x	h	r	w	a	y	s	a	x	d	l	q	g	c	i	..

m.clar	..	..	s	n	o	m	s	d	e	l	e	s	q	u	..	..									
clau	..	..	m	o	n	e	d	a	m	o	n	e	d	a	..	..									
m.xifrat	..	..	e	b	b	q	v	d	q	z	r	w	t	u	..	..									

Trencant Vigenère (Charles Babbage s.XIX)

No pot ser per casualitat.

m.clar	..	l	s	a	r	t	i	c	l	e	s	s	e	g	u	e	n	t	s	q	u	e	p	e	r
clau	..	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e
m.xifrat	..	o	s	m	f	g	m	f	l	q	g	f	i	j	u	q	b	g	w	t	u	q	d	r	v

m.clar	t	a	n	y	e	n	c	o	n	j	u	n	t	a	m	e	n	t	a	l	e	s	p	e	..
clau	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e	..
m.xifrat	w	a	z	m	r	r	f	o	z	x	h	r	w	a	y	s	a	x	d	l	q	g	c	i	..

m.clar	..	..	s	n	o	m	s	d	e	l	e	s	q	u	..	..									
clau	..	..	m	o	n	e	d	a	m	o	n	e	d	a	..	..									
m.xifrat	..	..	e	b	b	q	v	d	q	z	r	w	t	u	..	..									

Trencant Vigenère (Charles Babbage s.XIX)

No pot ser per casualitat.

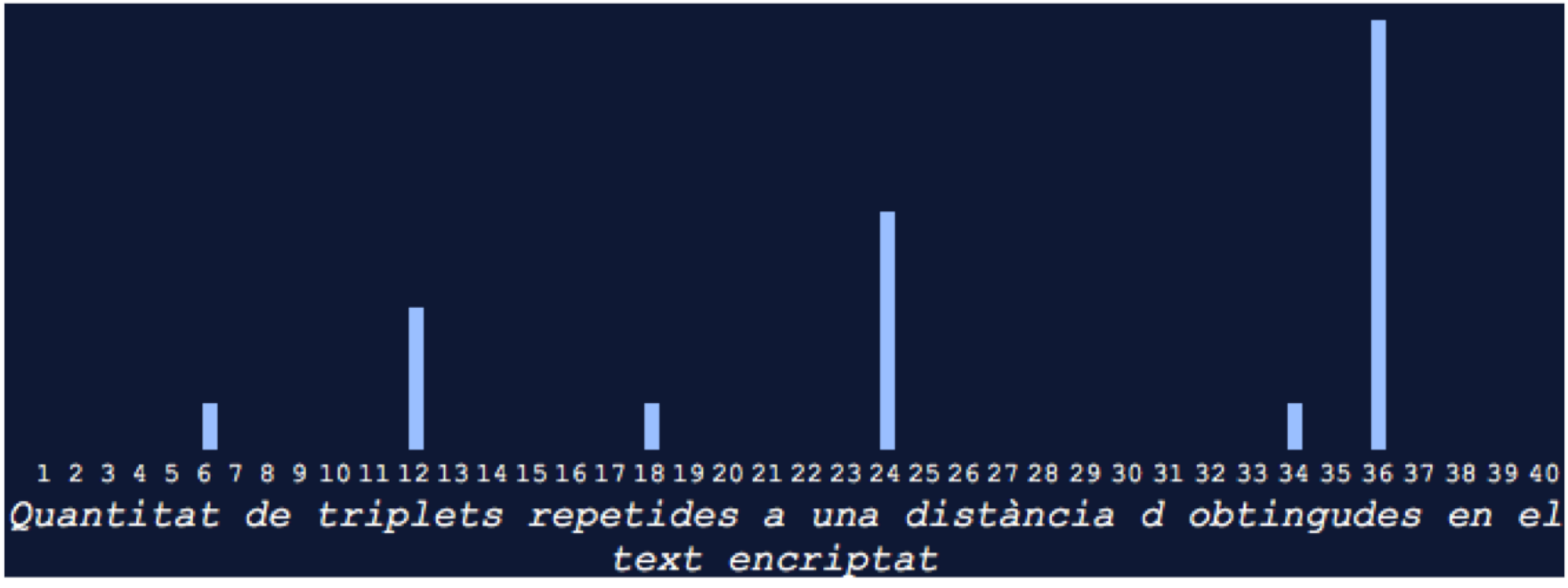
m.clar	..	l	s	a	r	t	i	c	l	e	s	s	e	g	u	e	n	t	s	q	u	e	p	e	r
clau	..	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e
m.xifrat	..	o	s	m	f	g	m	f	l	q	g	f	i	j	u	q	b	g	w	t	u	q	d	r	v

m.clar	t	a	n	y	e	n	c	o	n	j	u	n	t	a	m	e	n	t	a	l	e	s	p	e	..
clau	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e	d	a	m	o	n	e	..
m.xifrat	w	a	z	m	r	r	f	o	z	x	h	r	w	a	y	s	a	x	d	l	q	g	c	i	..

m.clar	..	..	s	n	o	m	s	d	e	l	e	s	q	u	..	..								
clau	..	..	m	o	n	e	d	a	m	o	n	e	d	a	..	..								
m.xifrat	..	..	e	b	b	q	v	d	q	z	r	w	t	u	..	..								

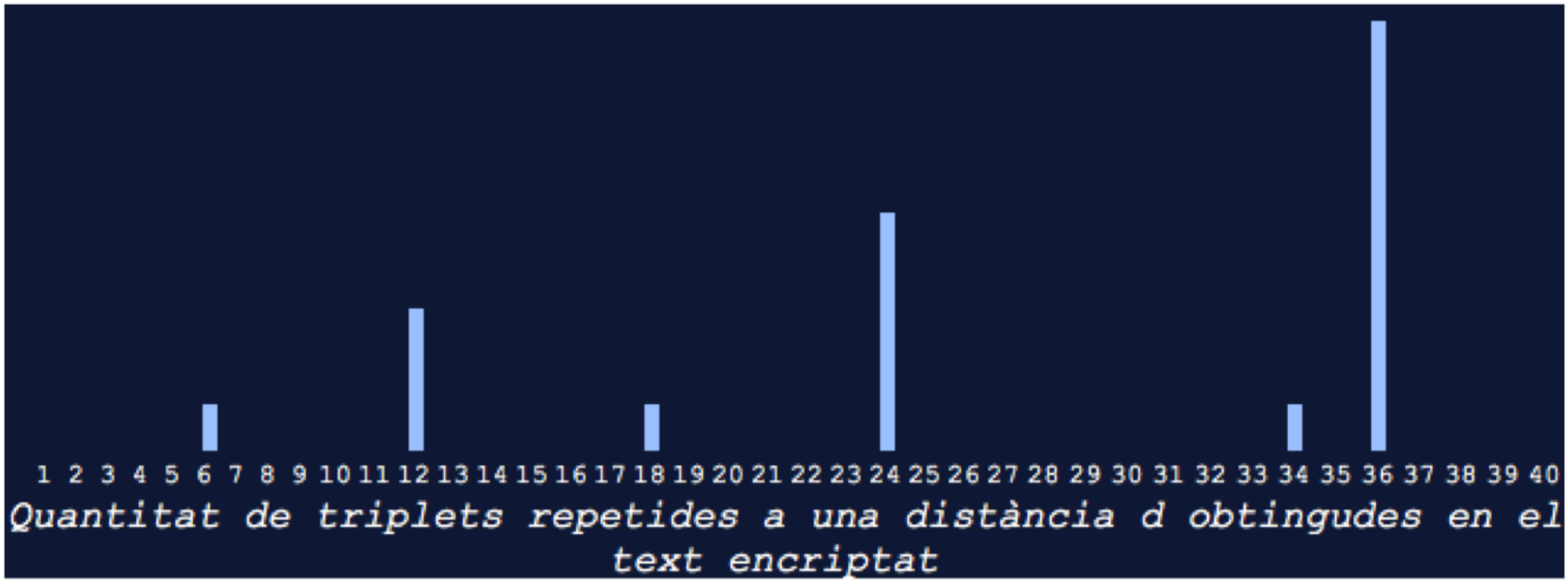
Mètode per trencar Vigenère (Charles Babbage s.XIX)

Calculem totes les distàncies entre les síl·labes repetides. Aquestes distàncies són: 6, 12, 18, 24, 34, 36. Això suggereix que la clau té longitud 6.



Mètode per trencar Vigenère (Charles Babbage s.XIX)

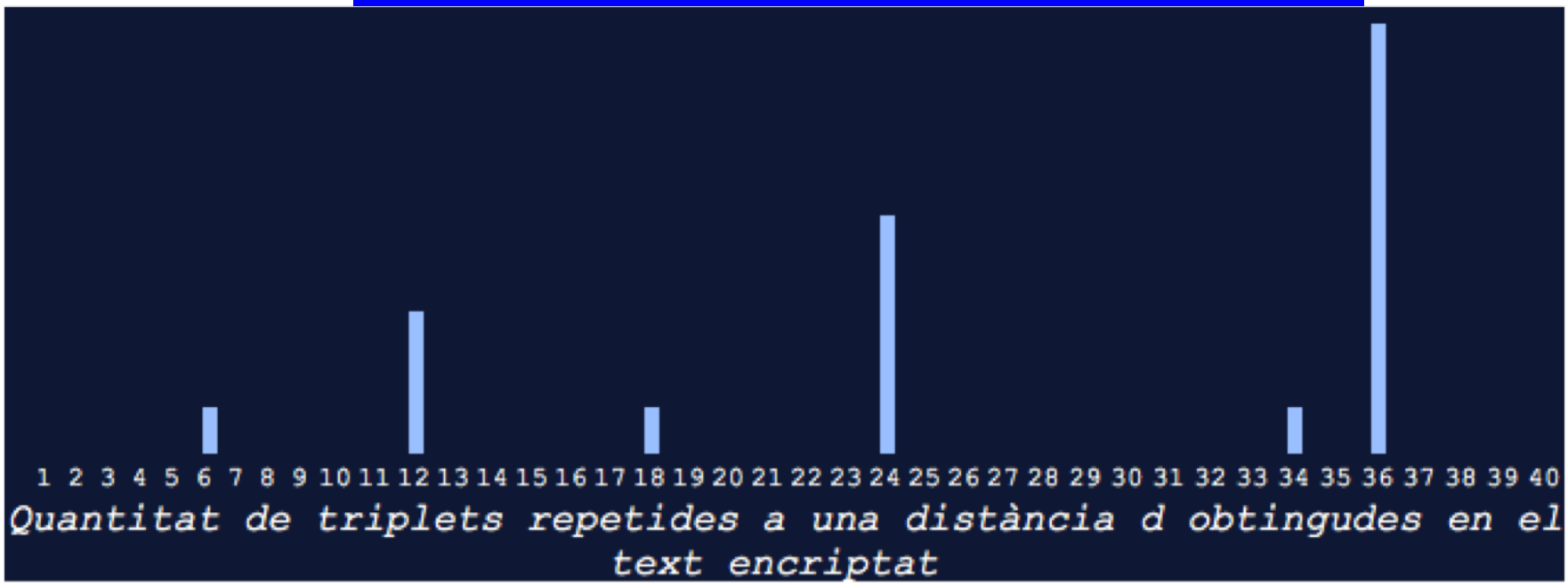
Calculem totes les distàncies entre les síl·labes repetides. Aquestes distàncies són: 6, 12, 18, 24, 34, 36. Això suggereix que la clau té longitud 6.



Mètode per trencar Vigenère (Charles Babbage s.XIX)

Calculem totes les distàncies entre les síl·labes repetides. Aquestes distàncies són: 6, 12, 18, 24, 34, 36. Això suggereix que la clau té longitud 6.

Conjecturem que la longitud de la clau és 6



Mètode per trencar Vigenère

Dividim el missatge en sis "missatges"

```
tsqmsoewgewaxoeijiaprhiodrnyqeeehewrqavpoeerrpdcuigewezіaehxo
oiefiacpepbdofyetqfeeqimgvwseggciusahnhhlmghthrrwpmhdqzgiurq
bliosmfgmflqgfijuqbgwtuqdrvwazmrrfozxhrwaysaxdlqgciusabrwhle
bbqvdqzrwtumzfesadsvbhnmzqsfuysaxquyseswrqgnhmuzhrpsruarvgib
cfmwvmqbrviehvvhnywygdtafmioluieivdqcemwrqgzmovgwgghnfsfhrtl
sypludsfhhpxogegibcfmwapsfionajrqerqrrqllhivxfezhfhlnairpves
caivvmfreoifnnvhlpsfipbdsqipixjhmwcqbgwyizhvgrnewfxlaqbzmona
ipiqtqgypludsfhhodwzmodagpiqtqgiyltmbgeyuuhypludsfhhpxogeway
prnriqgbfwizuhhhsmgnrwlxivwdcmbimgebznxdpqfsefixwgeuexheeqsb
cexgexheivodwieoodoqivezheiwzqavpgoxoewwofsyuxetsziqcucaewee
hnipbmznxgeyoaiuaestyuaqbbpoeerrjhrdcnqetmdrwgersevrlmskgdvm
qvshsfozivoysacvezjbpwapoqisepfrwllqgbpoeefrtrsqbfserqfbgdsa
zvhdiqggeqcaprvweedrvdlffrwhlbociungarvrupsfguigznyeioopmrej
opxddqzniacmjnglobseuxezcumkaswpesdutvgxlfogiqtdcoeulmgrkrnm
lvjuapsoidlqavpyuuhpiqtejvrwxuteegaggnrwcaanxhxfqyexlmrrgoad
opmrdqwahhpqbqiqcuoasudmarvlcmbniapxwpehlocaxlnsighhlffrwrrx
ocvlmqfnblfdodyhcabgioagpvgdcucqiotdsfsuezqnvdnavnivtmhqivxu
                        teega
```

Mètode per trencar Vigenère

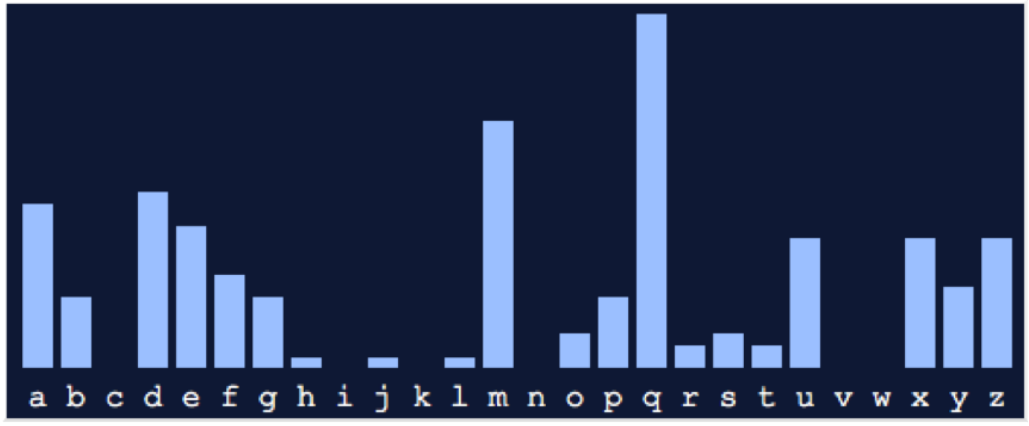
Dividim el missatge en sis "missatges"

primer	segon	tercer	quart	cinquè	sisè
texadeqeuzoadq	swoprearіiocof	qgernhvrgaipfe	mgihyeppeeep	swjiywodwhfpe	oaioerecexibti
mgamrqqmqqqz	gghgwzbfgbdmxs	vcnhpglgfgrrh	yewihtmiigiwv	qwuhhhuofjtvfw	eslrdrsluuaoals
zyqaeqmdmyyq	gbbzzszssghacq	acrbrfvqaenrrf	rrxiwqrebsxsh	duhvtshsqwms	lduanuururivin
zubmeyauqqgfld	hwficgwsssocsj	bvymeezgf	pvmbvgiimmgh	gwvhdivwohrlhg	tldrvntupianrl
xbpaqhzasmfpd	rihicfnssjbhwb	yfgffrrvfrarnf	pfemiqqxhpirvi	wielflvvohpiwyr	enevilbicinan
xqzeqaqddaqm	igswggbhsopgug	qhgvfzpyfzpigyf	imwgxmiyhmi	loqlhoilylhwrwh	tuodttuu
udxyqzmxmbqx	ibzfwhchwohao	grbhnvinsgeee	yephenbhrwmx	wwgdfuqgvovig	paiislcepieseo
xbxddzqxftuemy	sschzosbrcdss	iqeveyzannatbr	eeexeeiipwuiei	wxqwpguupheg	oezooecebeaa
eqedmrmmfyzpp	qosjofgfbfzgp	nrekvzabqrbrfb	niypjqwvgszcp	rdhvvwiloreddq	ertelvsoeaelesr
qeqqaqaefbgpgo	dfoaszoozjscw	vgrrrcrfnppnne	iwptsghgvvwivg	wdwuruerdalxm	sicellnuiiedcoe
jqmbzsufdmmpqu	tocglsahjtgaq	upvgorvovpvenny	ymxngumegie	sxqurudyqrgw	adltlnalutxac
eugafmdqqummx	rowboabwcifof	rpaqarnpagrc	kjopirerxegma	hxorhquvahlhrl	xladpcdcplnl
osfxqdagudzamu	obpcsqvht	ndgvqfnnqe	isviexhwvnyig	lhogoudvvg	rmfcactentxa
			isviie		

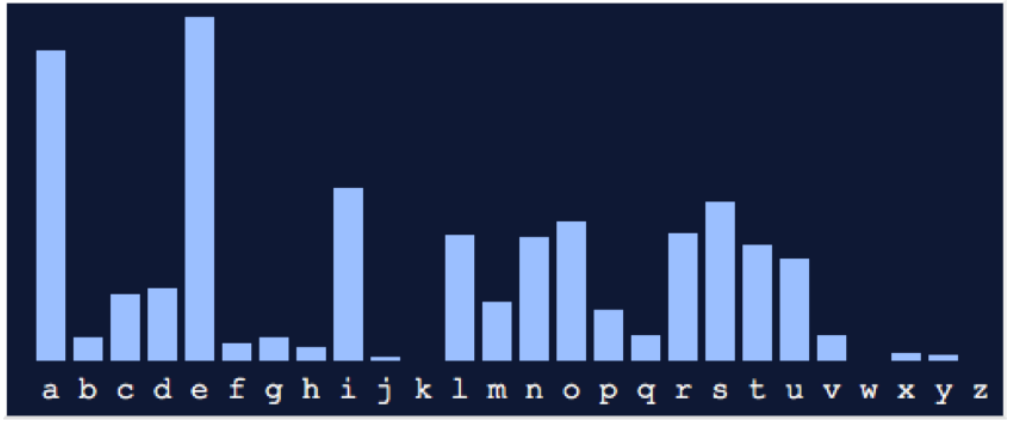
Mètode per trencar Vigenère.

Anàlisi de freqüències del primer "missatge"

```
texadeqeuzoadqmgamrq
qmqqqzzyqaeqmdmyyq
zubmeyauqqgfldxbpaq
hzasmfpdxqzeqaqddaq
mudxyqzmxmbqxxbxd
dzqxftuemyeqedmrmm
fyzppqeqqaqaefbgpgojq
mbzsufdmmpqueugafmd
qqummxosfxqdagudzamu
```



freqüències del primer "missatge" xifrat

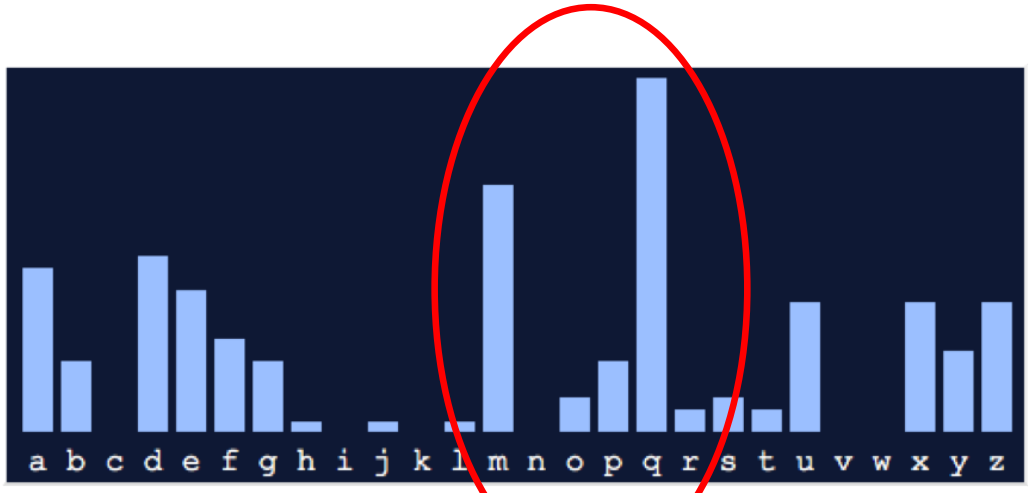


freqüències lletres en català

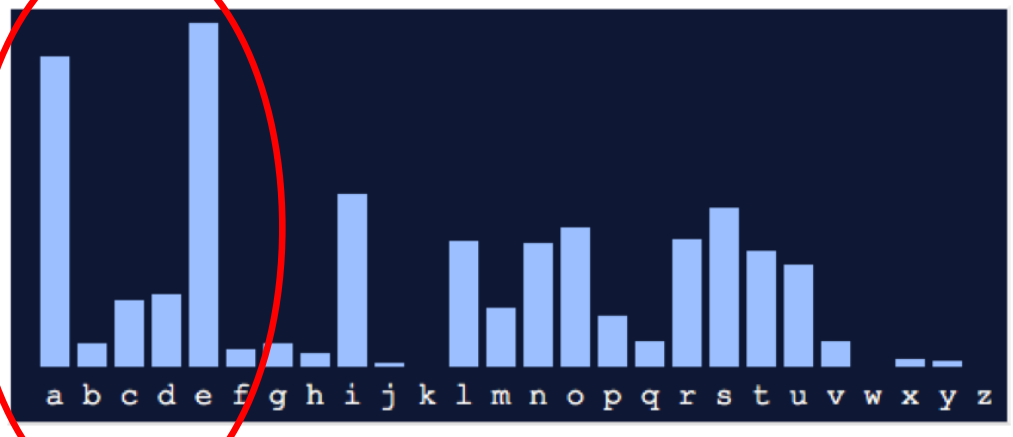
Mètode per trencar Vigenère.

Anàlisi de freqüències del primer "missatge"

```
texadeqeuzoadqmgamrq
qmqqqzzyqaeqmdmyyq
zubmeyauqqgfldxbpaq
hzasmfpdxqzeqaqddaq
mudxyqzmxmbqxxbxd
dzqxftuemyeqedmrmm
fyzppqeqqaqaefbgpgojq
mbzsufdmmpqueugafmd
qqummxosfxqdagudzamu
```



freqüències del primer "missatge" xifrat



freqüències lletres en català

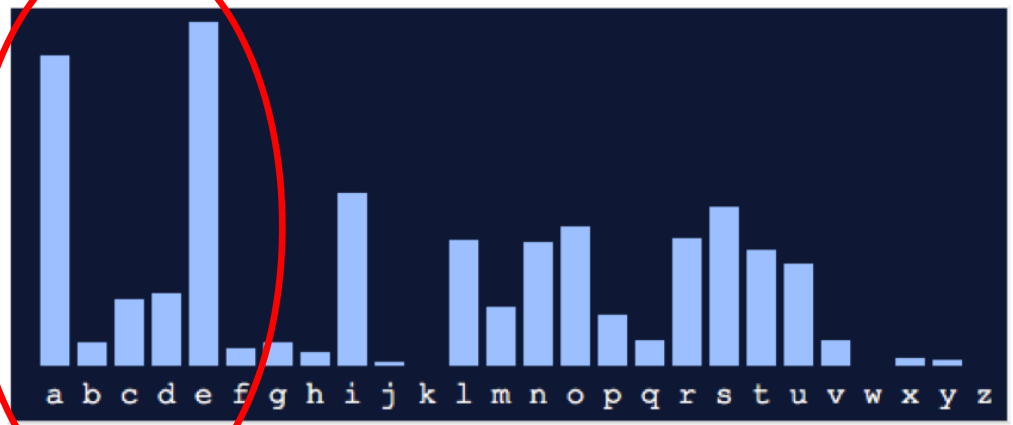
Mètode per trencar Vigenère.

Anàlisi de freqüències del primer "missatge"

```
texadeqeuzoadqmgamrq
qmqqqzzyqaeqmdmyyq
zubmeyauqqgfldxbpaq
hzasmfpdxqzeqaqddaq
mudxyqzmxmbqxxbxd
dzqxftuemyeqedmrmm
fyzppqeqqaqaefbgpgojq
mbzsufdmmpqueugafmd
qqummxosfxqdagudzamu
```

a $\rightarrow$ m
la primera lletra de la clau és M

freqüències del primer "missatge" xifrat

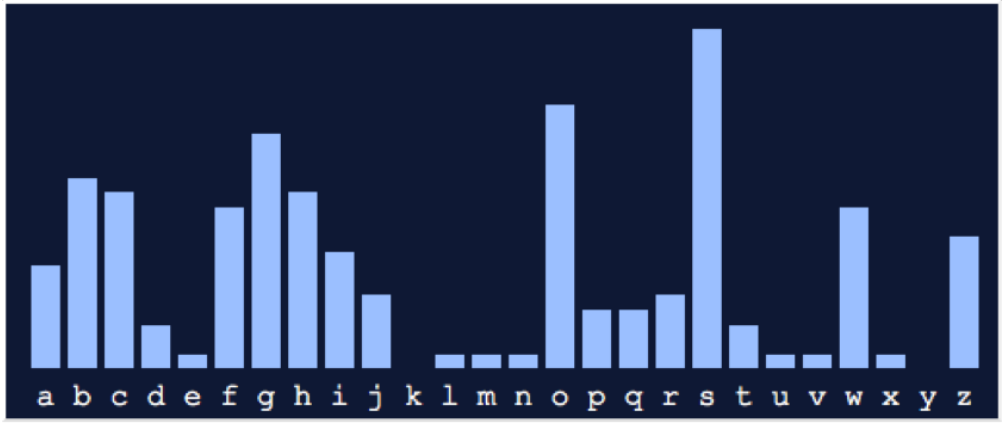


freqüències lletres en català

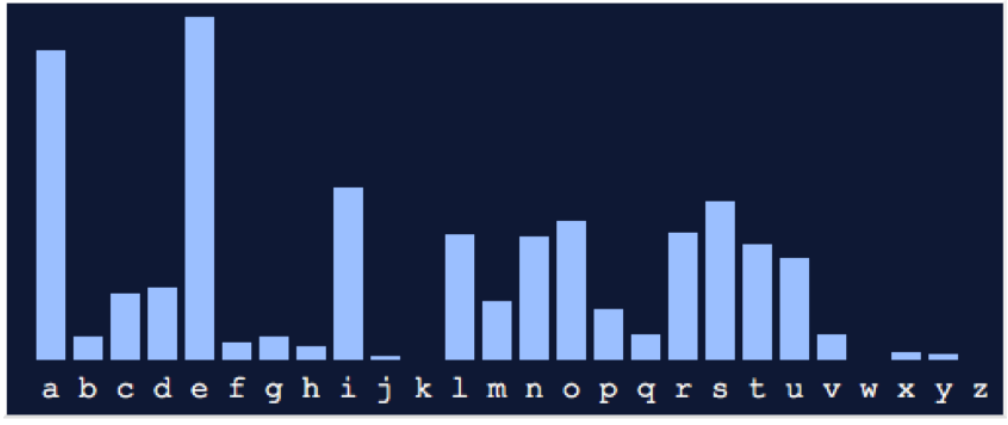
Mètode per trencar Vigenère.

Anàlisi de freqüències del segon "missatge"

```
swopreariiocofgghgwz
bfgbdmxsgbbzzszssg
hacqhwficgwsssocsjri
hicfnssjbhwbigswggb
hsopgugibzfwhchwoh
aosschzosbrcdssqosj
ofgfbfzgpdfoaszoozjsc
wtocglsahjtgaqrowb
oabwcifofobpcsqvht
```



freqüències del segon "missatge" xifrat

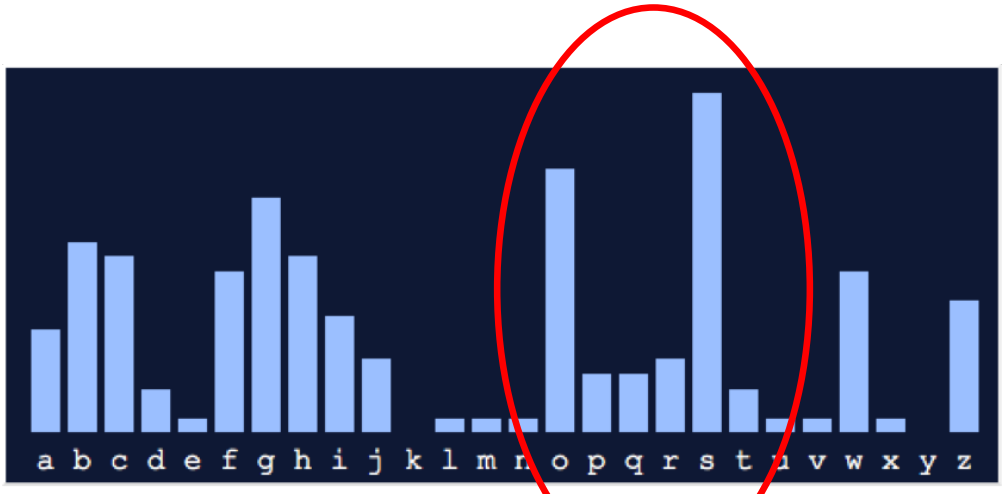


freqüències lletres en català

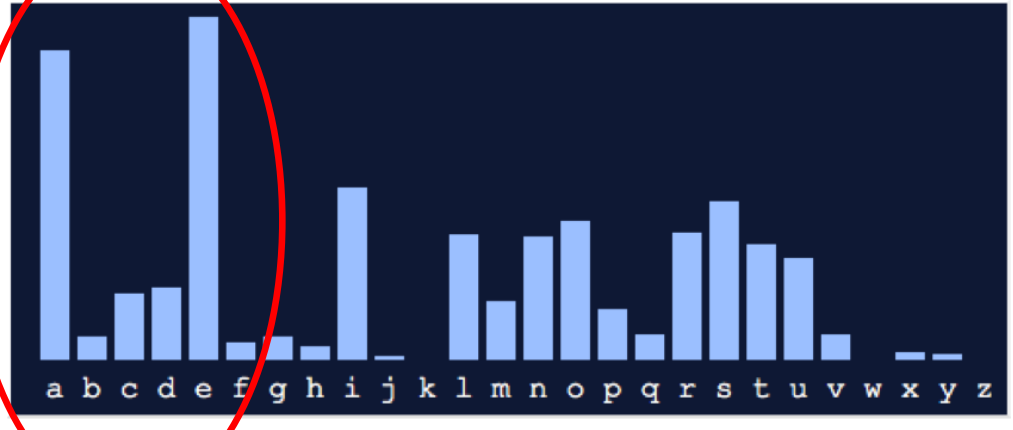
Mètode per trencar Vigenère.

Anàlisi de freqüències del segon "missatge"

```
swoprearіiocofgghgwz
bfgbdmxsgbbzzszssg
hacqhwficgwsssocsjri
hicfnssjbhwbigswggb
hsopgugibzfwhchwoh
aosschzosbrcdssqosj
ofgfbfzgpdfoaszoozjsc
wtocglsahjtgaqrowb
oabwcifofobpcsqvht
```



freqüències del segon "missatge" xifrat



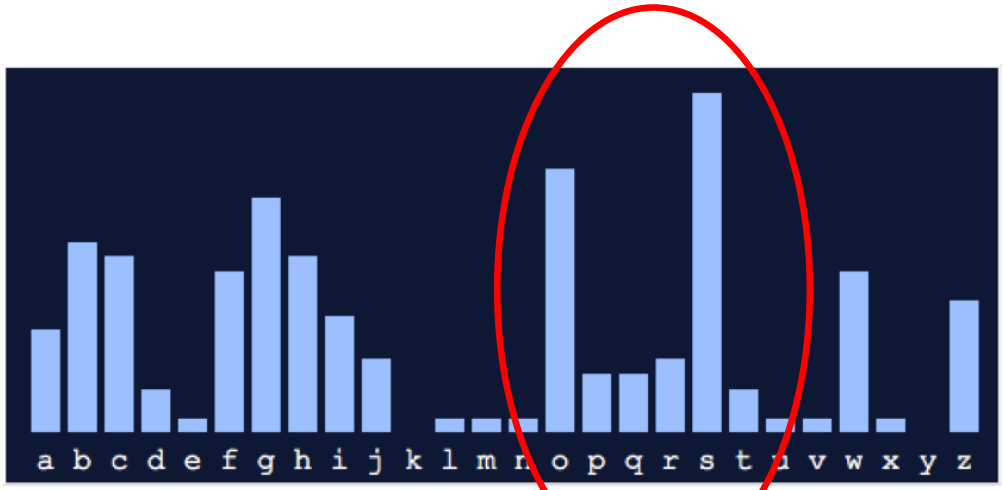
freqüències lletres en català

Mètode per trencar Vigenère.

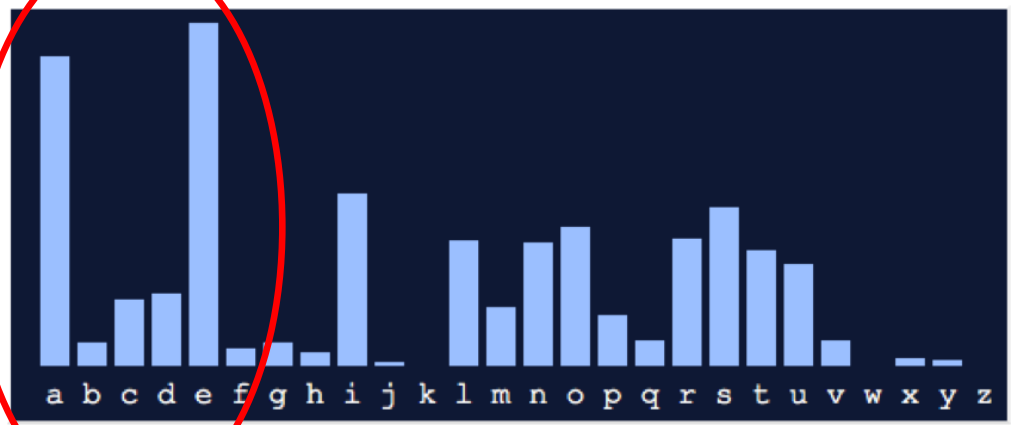
Anàlisi de freqüències del segon "missatge"

```
swoprearіiocofgghgwz
bfgbdmxsgbbzzszssg
hacqhwficgwsssocsjri
hicfnssjbhwbigswggb
hsopgugibzfwhchwoh
aosschzosbrcdssqosj
ofgfbfzgpdfoaszoozjsc
wtocglsahjtgaqrowb
oabwcifofobpcsqvht
```

a $\rightarrow$ o
la segona lletra de la clau és O



freqüències del segon "missatge" xifrat



freqüències lletres en català

Mètode per trencar Vigenère

Repetim el procediment amb els sis "missatges" i per fi ... trobem la clau:

clau: MONEDA

L'Enigma!

Arthur Scherbius

- 1918: registra la patent (criptosistema electromecànic)
- 1919: l'ofereix a l'exèrcit alemany, que la rebutja
- 1926: l'armada alemanya adopta Enigma després de demanar modificacions (més lleugera, rotors específics, connexions extres, simetria)
- 1928: la resta de cossos militars alemanys l'adopten. Milers d'Enigma venudes.

L'Enigma!

Arthur Scherbius

- 1918: registra la patent (criptosistema electromecànic)
- 1919: l'ofereix a l'exèrcit alemany, que la rebutja
- 1926: l'armada alemanya adopta Enigma després de demanar modificacions (més lleugera, rotors específics, connexions extres, simetria)
- 1928: la resta de cossos militars alemanys l'adopten. Milers d'Enigma venudes.

La màquina Enigma. Una màquina d'escriure amb llumetes

- En pitjar una tecla s'encén la lletra xifrada corresponent en un tauler lluminós

La màquina Enigma. Una màquina d'escriure amb llumetes

- En pitjar una tecla s'encén la lletra xifrada corresponent en un tauler lluminós
- Per a la lletra següent s'utilitza un altre alfabet xifrat.

La màquina Enigma. Una màquina d'escriure amb llumetes

- En pitjar una tecla s'encén la lletra xifrada corresponent en un tauler lluminós
- Per a la lletra següent s'utilitza un altre alfabet xifrat.

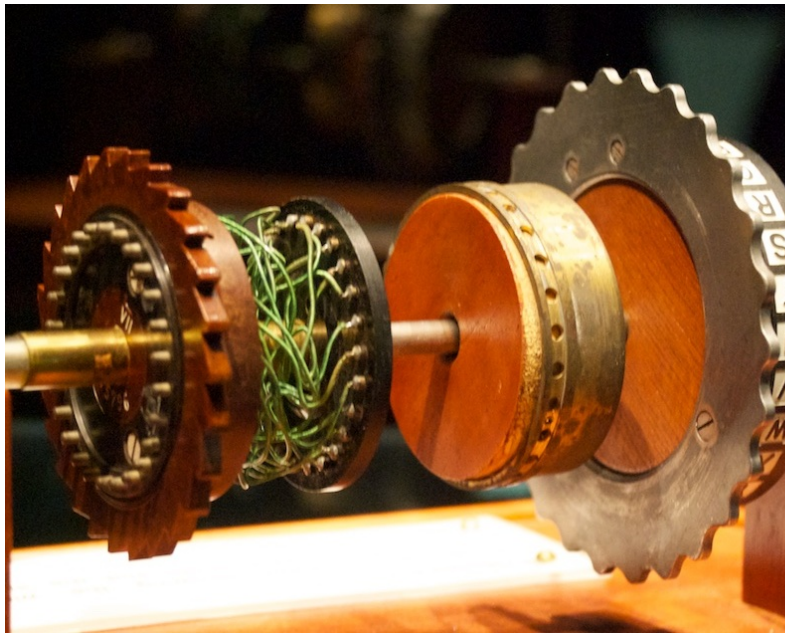
  $\rightarrow$ Si pitgem dos cops la mateixa lletra, probablement se xifrarà com dues lletres diferents.

L'Enigma: els rotors

L'Enigma: els rotors

Un rotor és un disc d'Alberti elèctric

- a una cara hi té l'alfabet en clar
- a l'altra l'alfabet xifrat
- el rotor xifra quan hi circula un impuls elèctric
- proporciona 26 alfabets al girar.



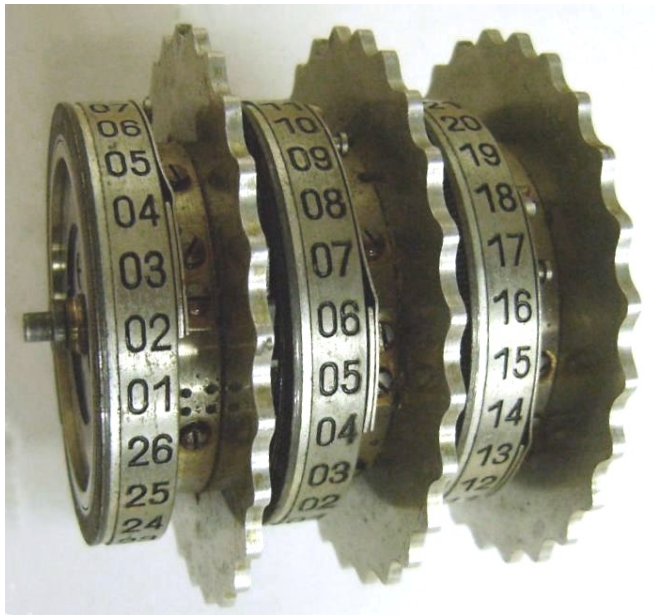
L'Enigma: els rotors

Un rotor és un disc d'Alberti elèctric

- a una cara hi té l'alfabet en clar
- a l'altra l'alfabet xifrat
- el rotor xifra quan hi circula un impuls elèctric
- proporciona 26 alfabets al girar.

Tres rotors enllaçats:

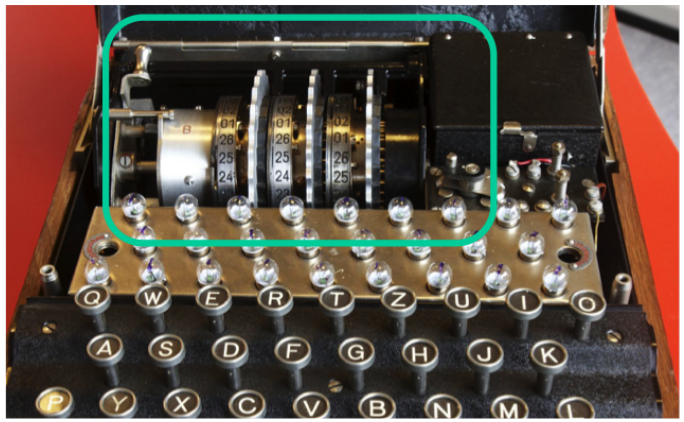
- disposarem de $26 \times 26 \times 26$ alfabets.



Parts mòbils de l'Enigma

Els rotors, selecció i ordenació

- 5 rotors disponibles,
- se'n trien 3,
- es posen en un ordre determinat.



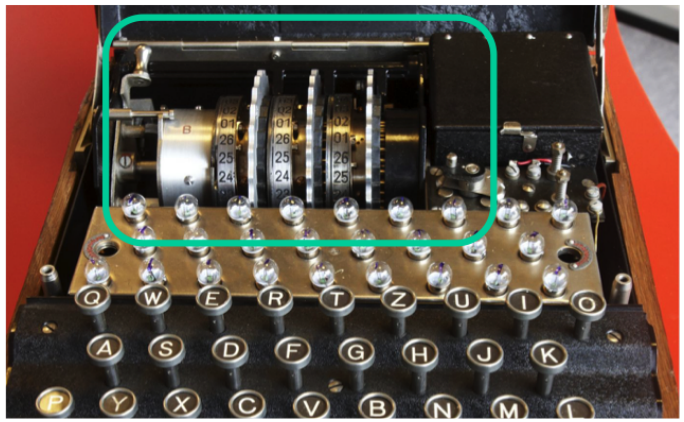
Parts mòbils de l'Enigma

Els rotors, selecció i ordenació

- 5 rotors disponibles,
- se'n trien 3,
- es posen en un ordre determinat.

Els rotors, posició inicial

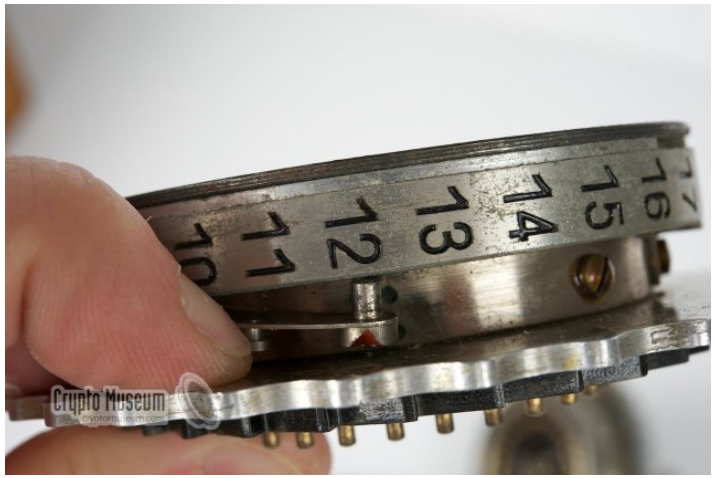
cada rotor es pot girar dins la màquina a una de les 26 posicions.



Parts mòbils de l'Enigma

Els anells dels rotors

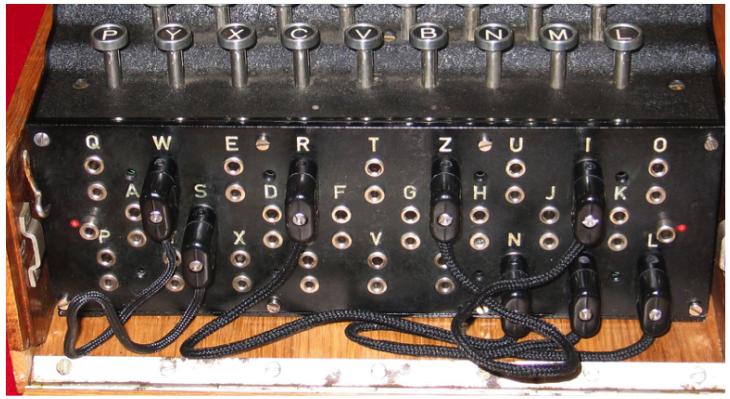
- anell extern del rotor que pot girar respecte el cablejat
- fixació en 26 posicions.
- osca que fa girar el rotor de l'esquerra.



Parts mòbils de l'Enigma

El tauler de connexions o claviller

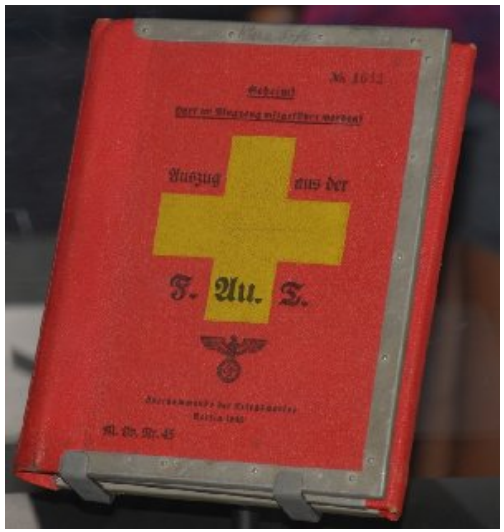
- permet connectar parelles de lletres
- es connecten entre 6 i 10 parelles



Parts mòbils de l'Enigma

Les claus d'Enigma

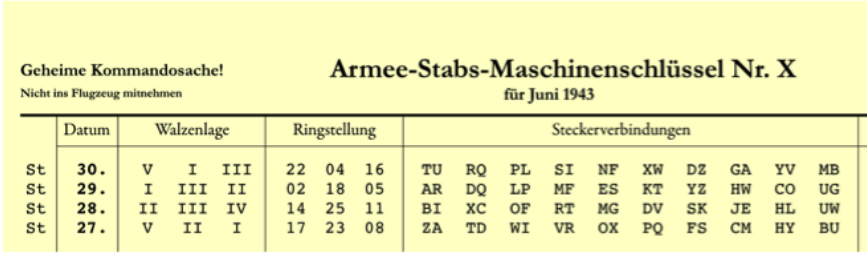
- Selecció ordenada dels rotors.
- Posició inicial de cada rotor (canviava en cada missatge).
- Configuració de l'anell.
- Connexions del claviller.



Parts mòbils de l'Enigma

Les claus d'Enigma

- Selecció ordenada dels rotors.
- Posició inicial de cada rotor (canviava en cada missatge).
- Configuració de l'anell.
- Connexions del claviller.



Geheime Kommandosache!
Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. X
für Juni 1943

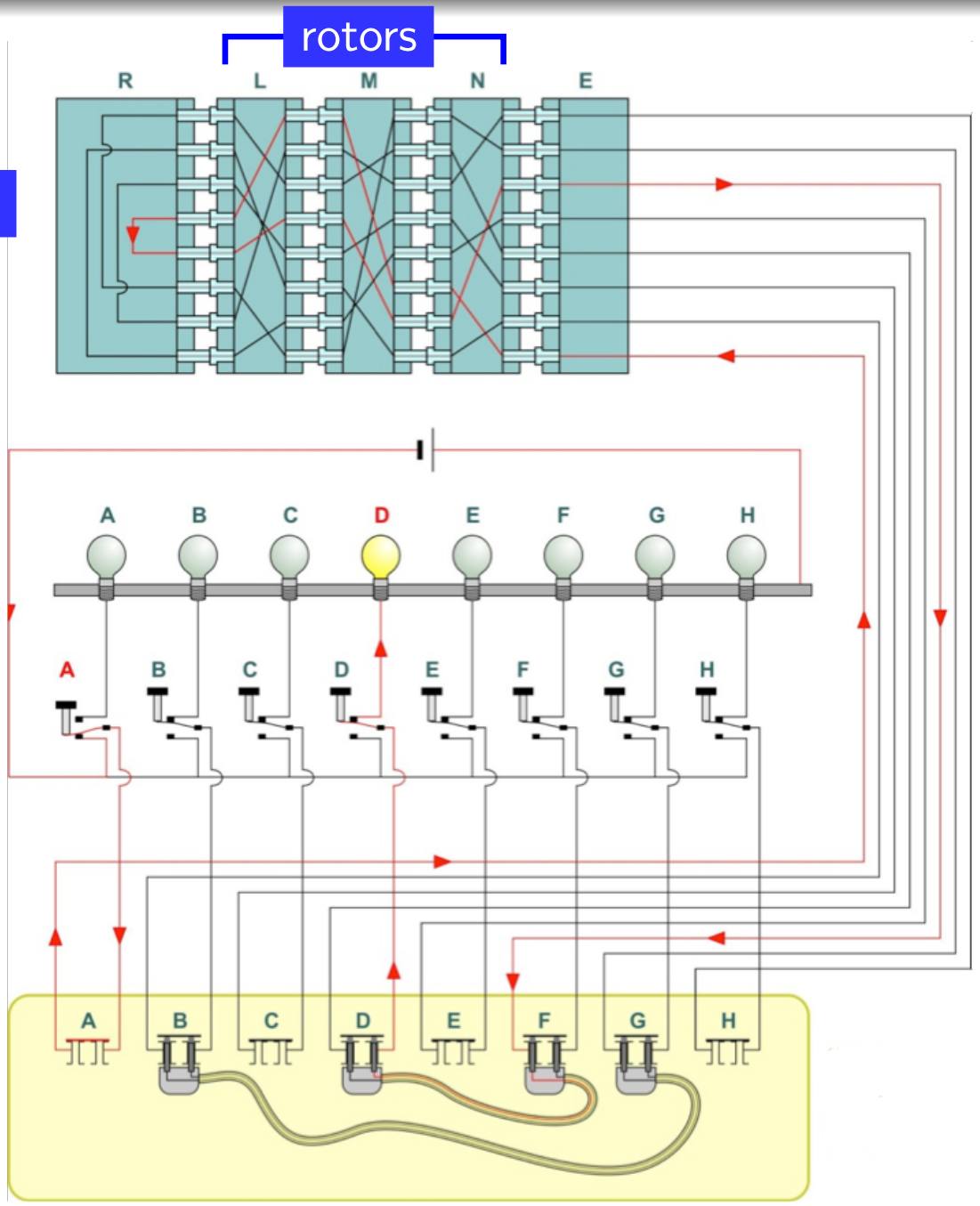
	Datum	Walzenlage	Ringstellung	Steckerverbindungen
St	30.	V I III	22 04 16	TU RQ PL SI NF XW DZ GA YV MB
St	29.	I III II	02 18 05	AR DQ LP MF ES KT YZ HW CO UG
St	28.	II III IV	14 25 11	BI XC OF RT MG DV SK JE HL UW
St	27.	V II I	17 23 08	ZA TD WI VR OX PQ FS CM HY BU

Quantes claus té Enigma?

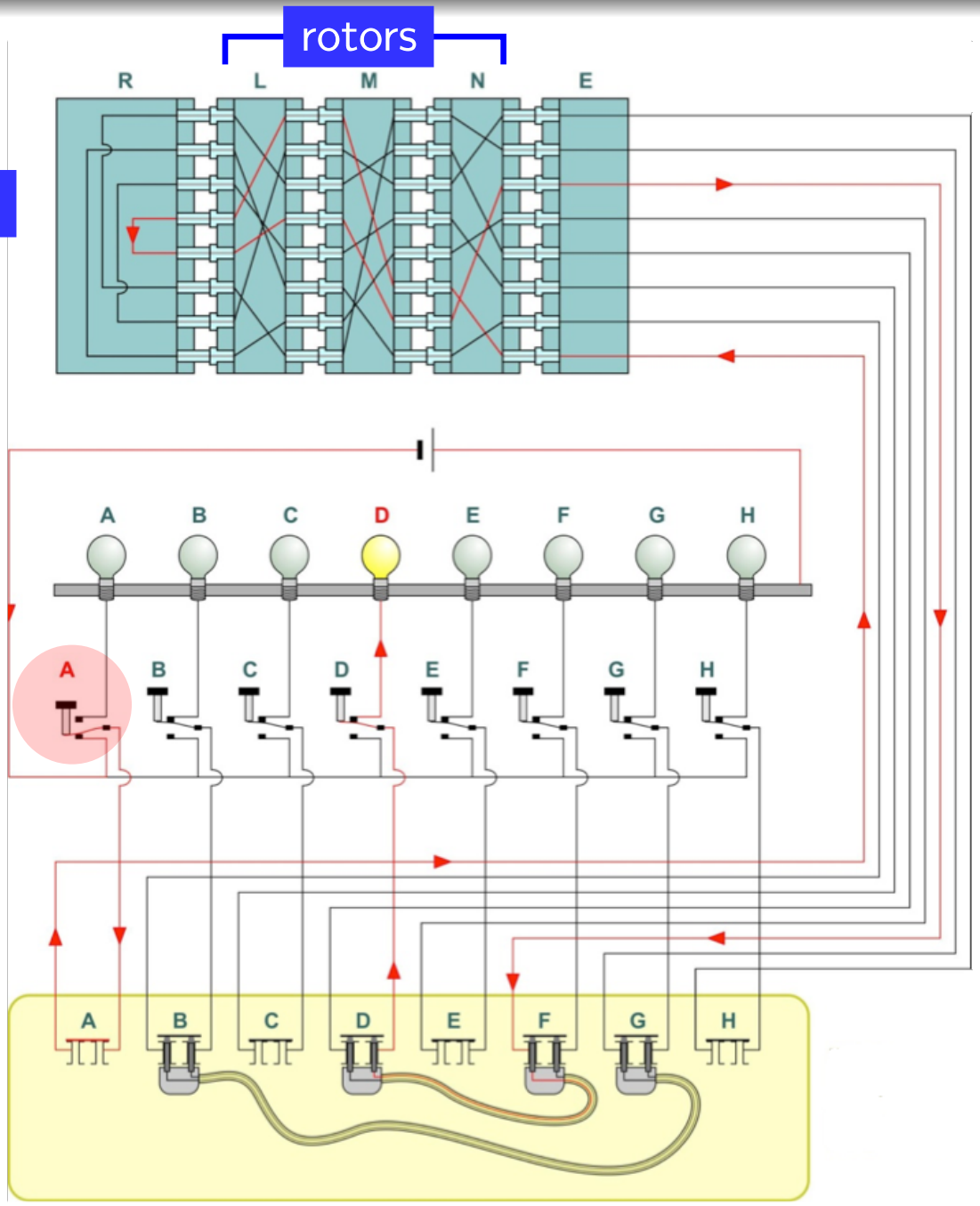
- Selecció ordenada dels rotors:
$$5 \times 4 \times 3 = 60$$
- Posició inicial dels rotors (es podien girar en una de les 26 posicions, normalment marcades amb números):
$$26 \times 26 \times 26$$
- Configuració dels anells:
$$26 \times 26$$
- Connexions del claviller (10 parelles de lletres entre les 26):
$$\frac{26 \times 25 \times \cdots \times 7}{2^{10} \times 10!} = 150\,738\,274\,937\,250 \approx 1.5 \times 10^{14}$$

Nombre total de claus possibles: 1.07×10^{23}.

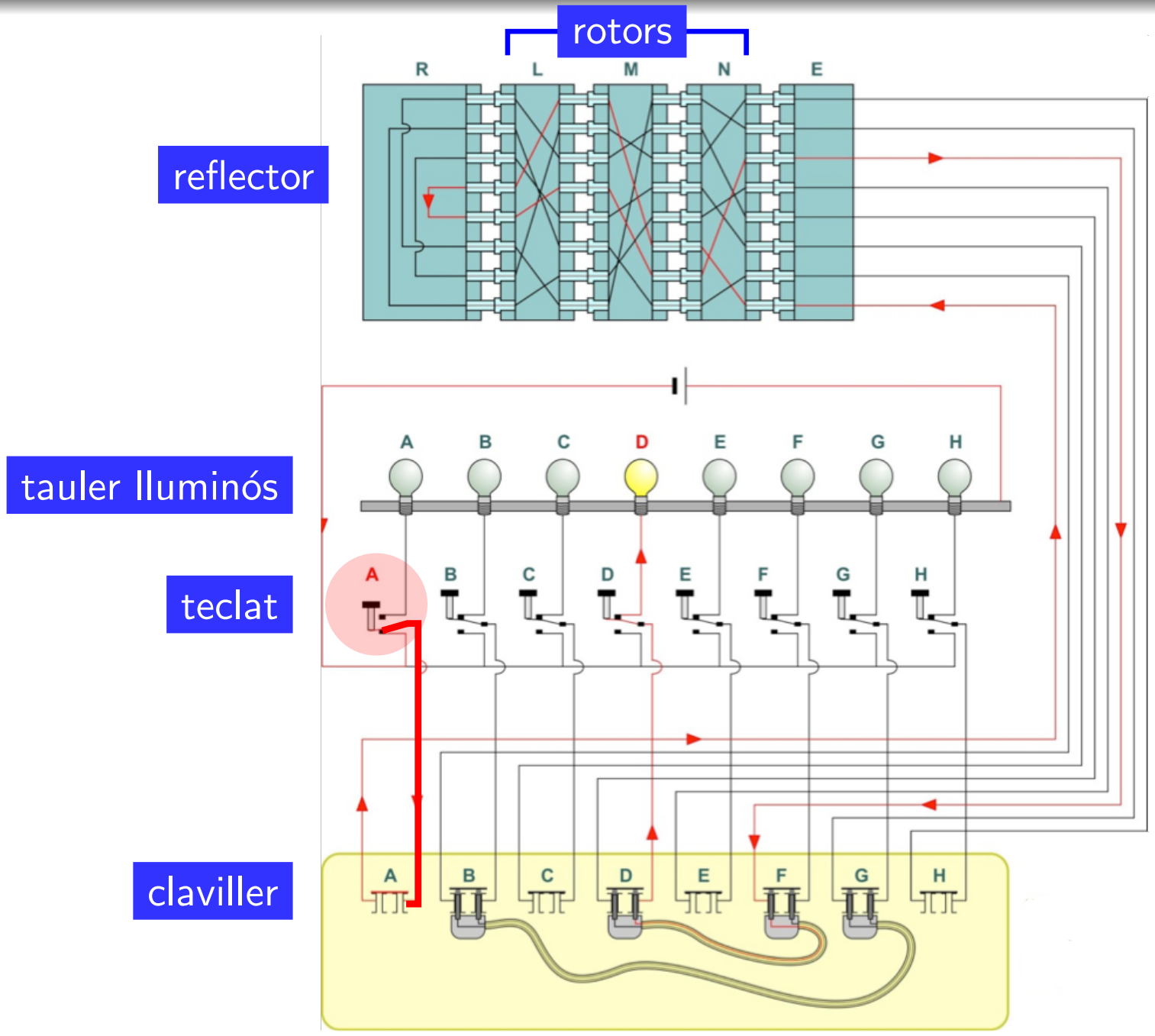
El circuït encriptador d'Enigma



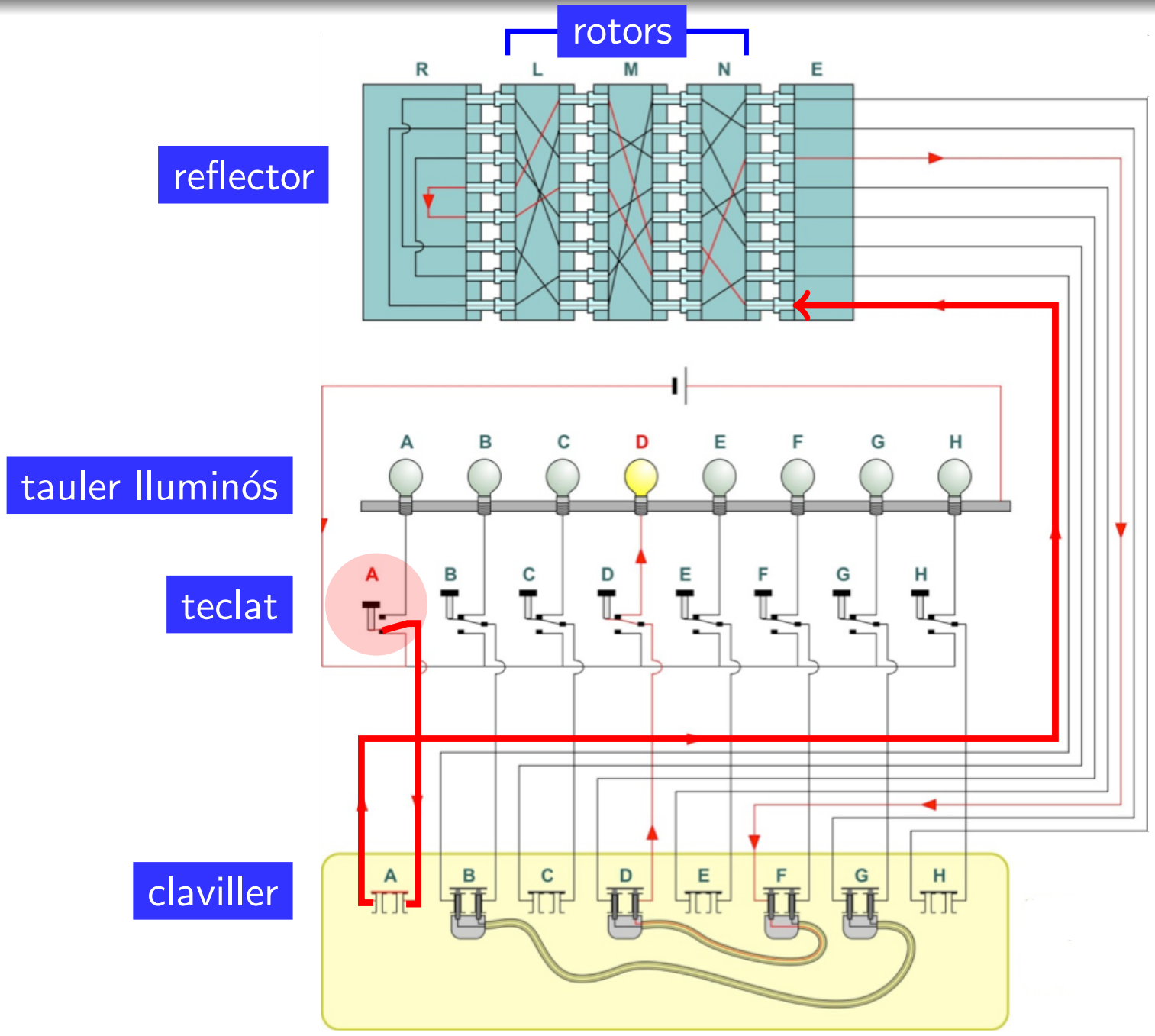
El circuït encriptador d'Enigma



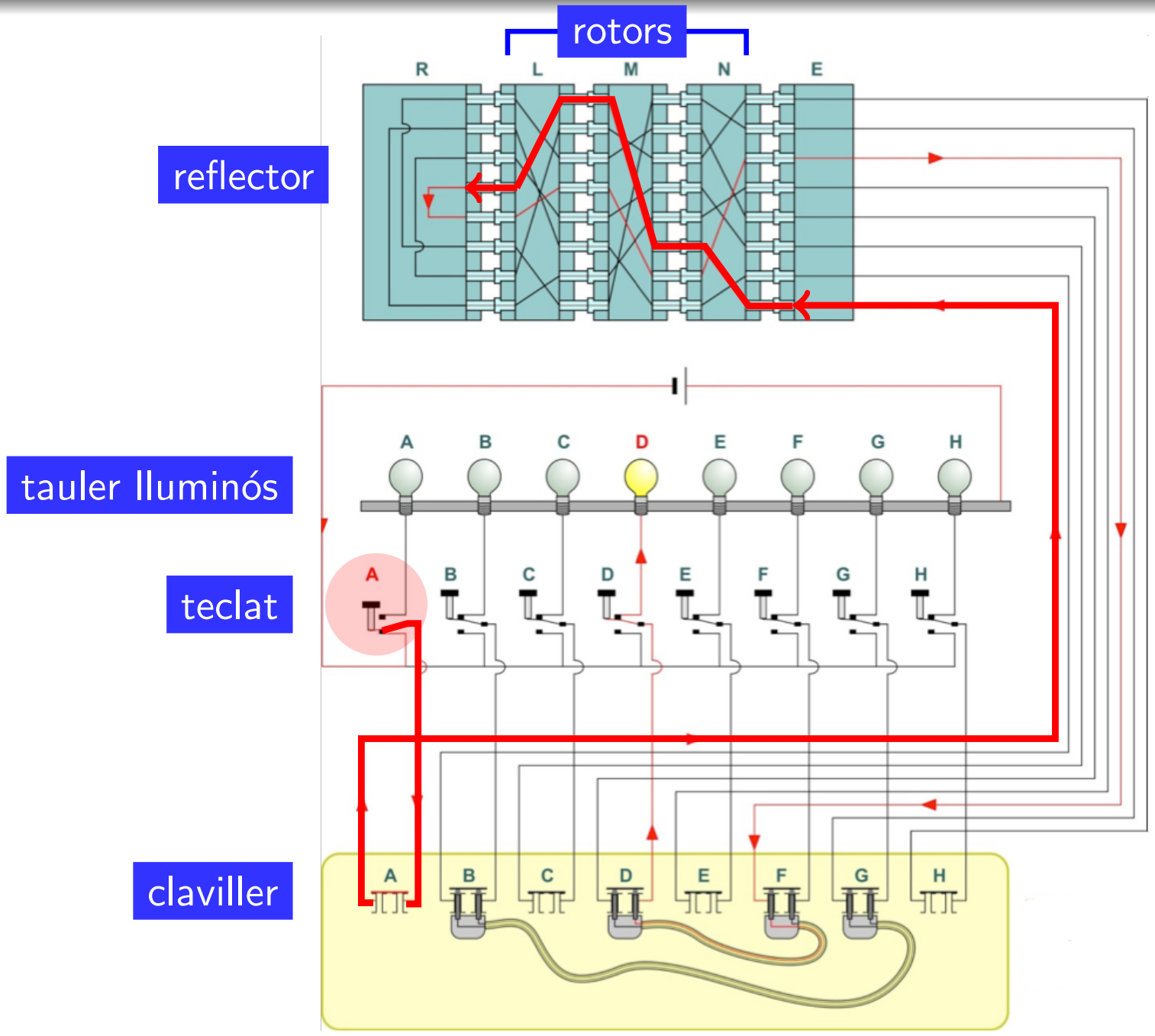
El circuït encriptador d'Enigma



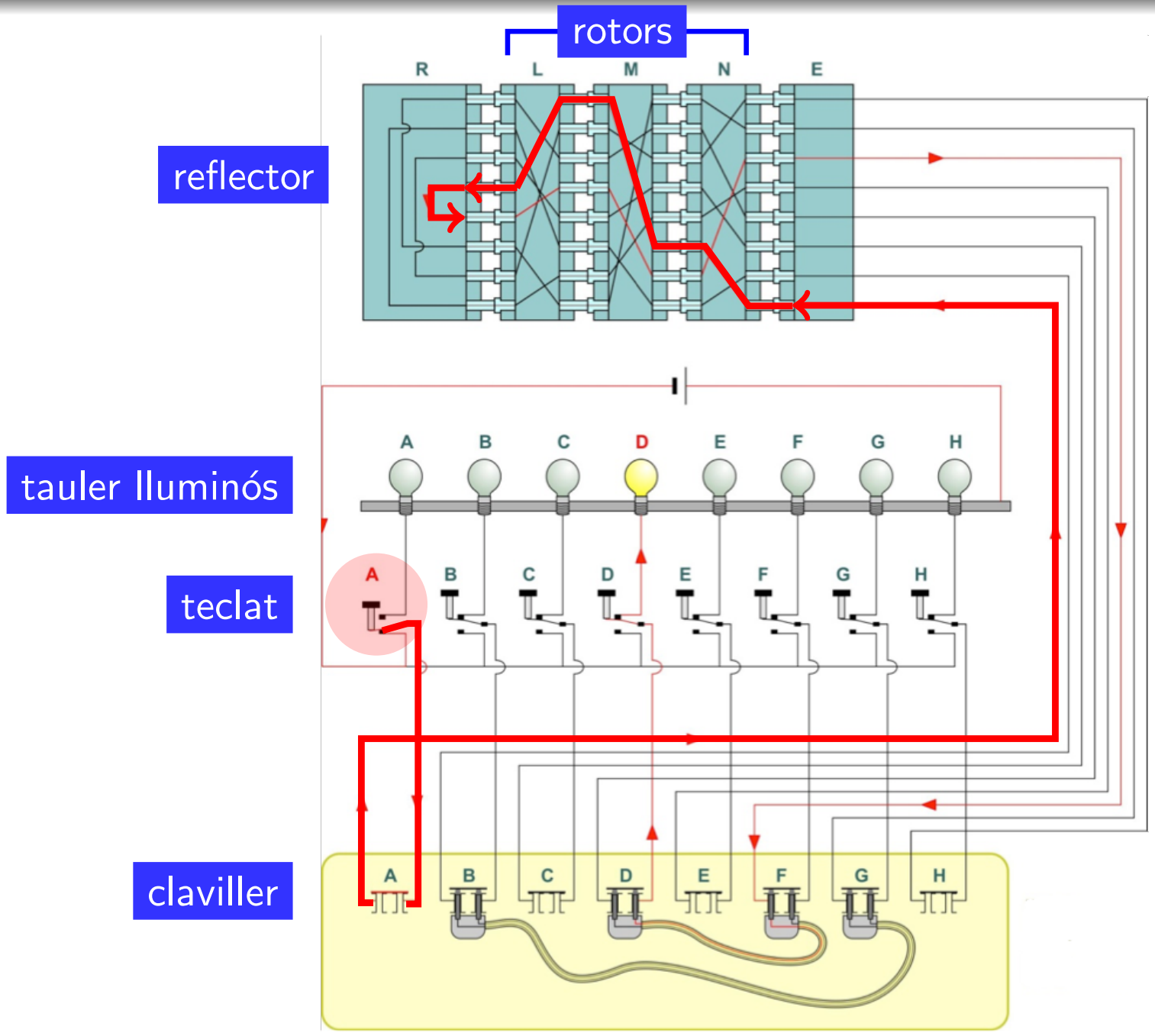
El circuït encriptador d'Enigma



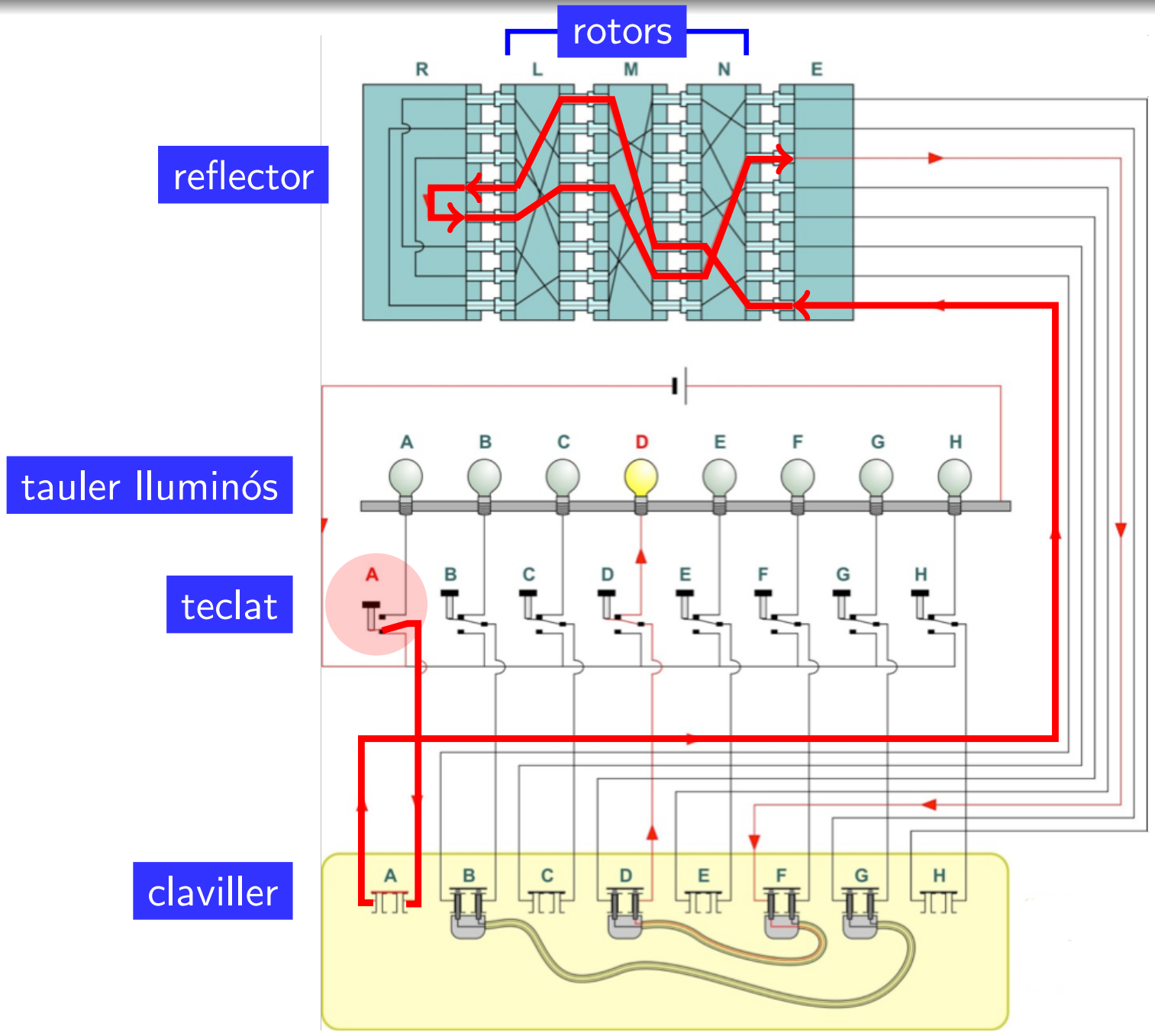
El circuït encriptador d'Enigma



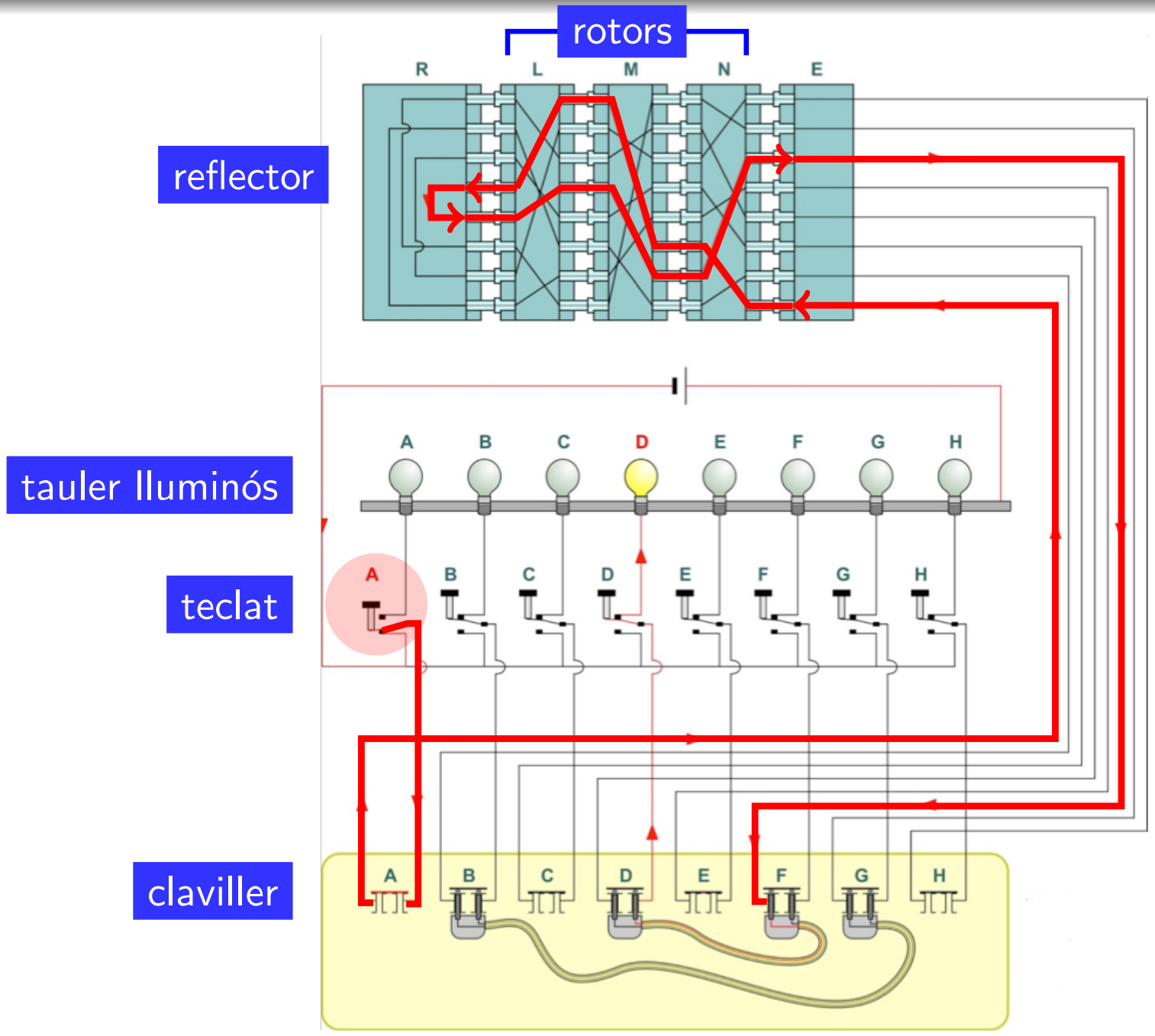
El circuït encriptador d'Enigma



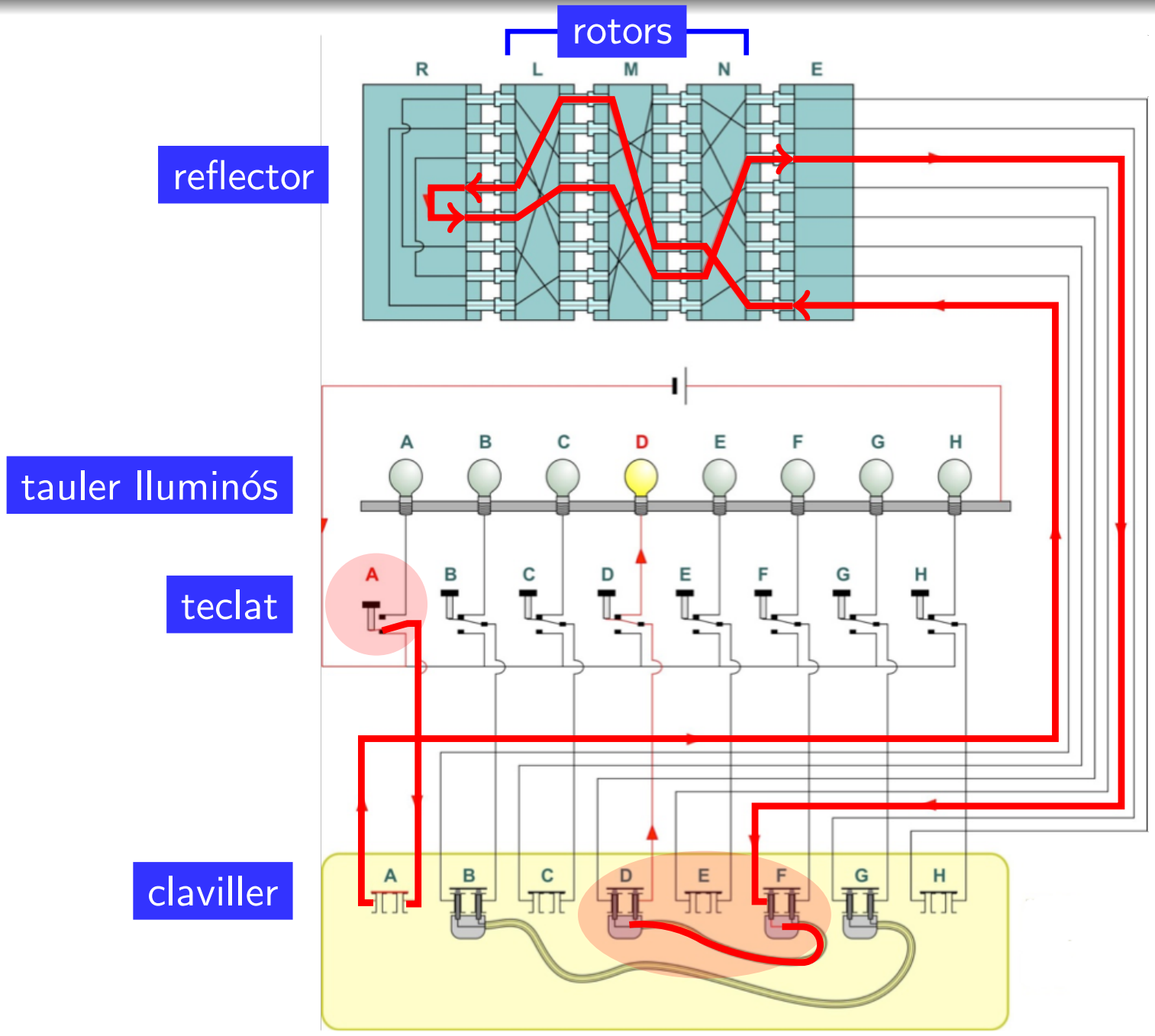
El circuït encriptador d'Enigma



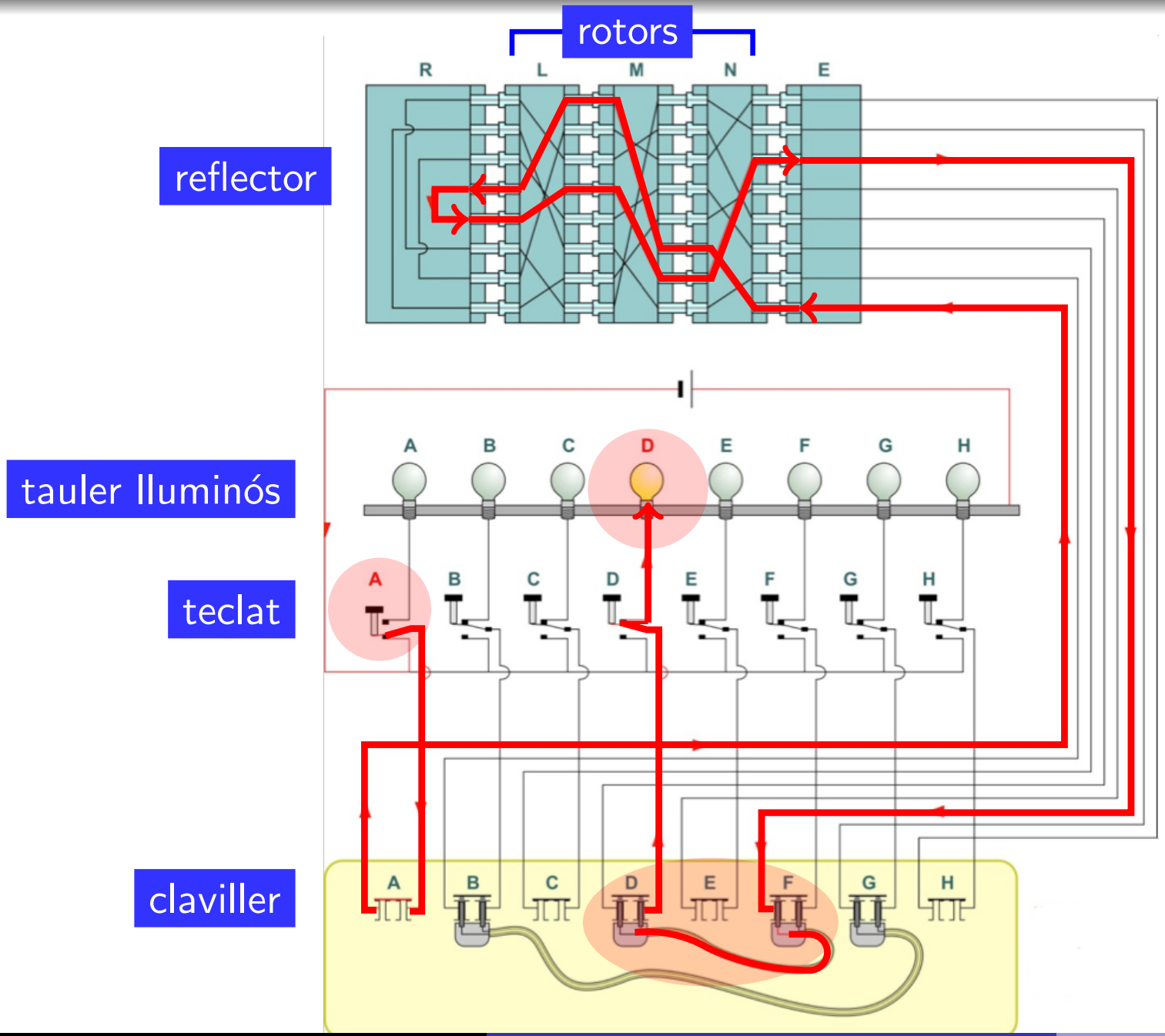
El circuït encriptador d'Enigma



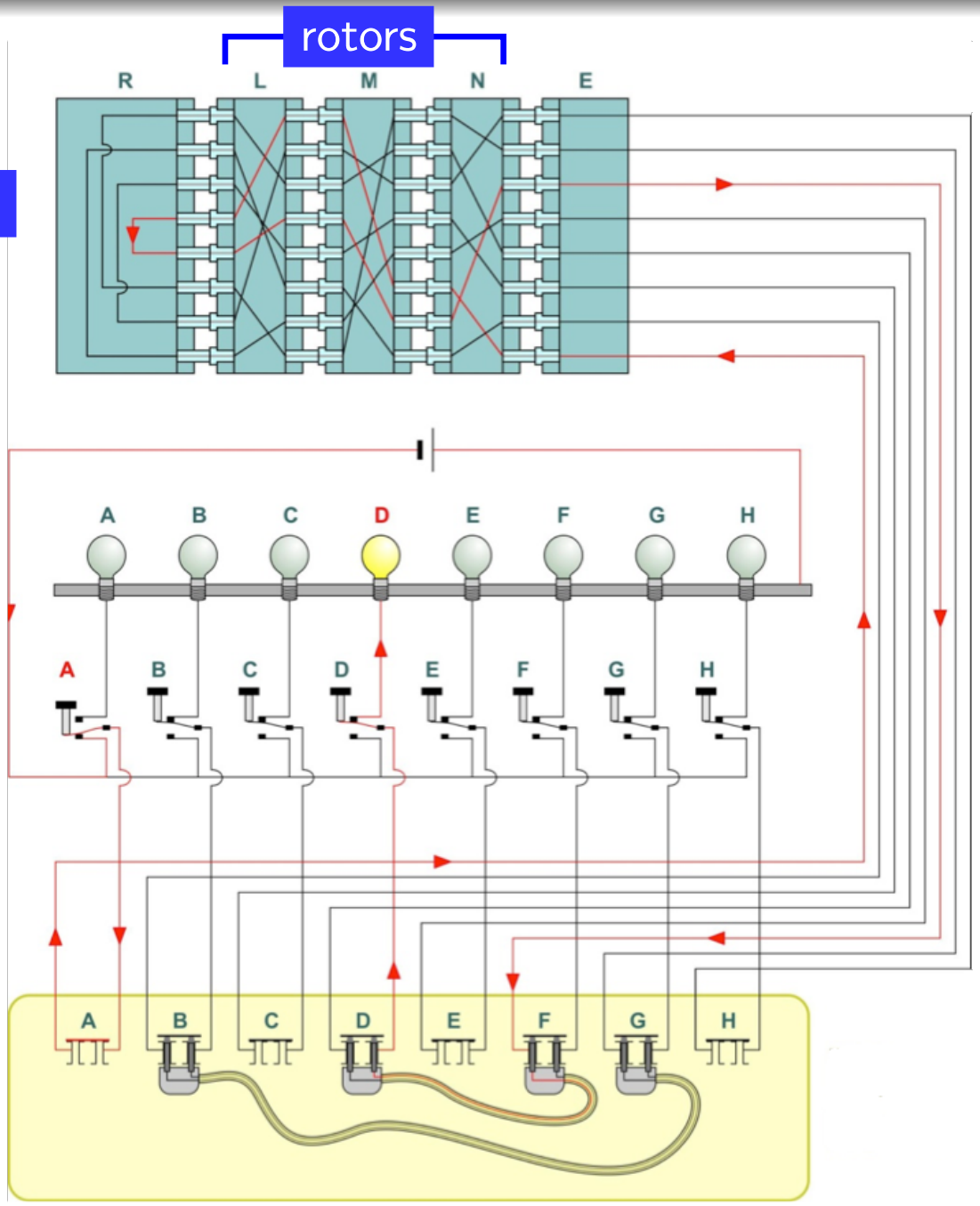
El circuït encriptador d'Enigma



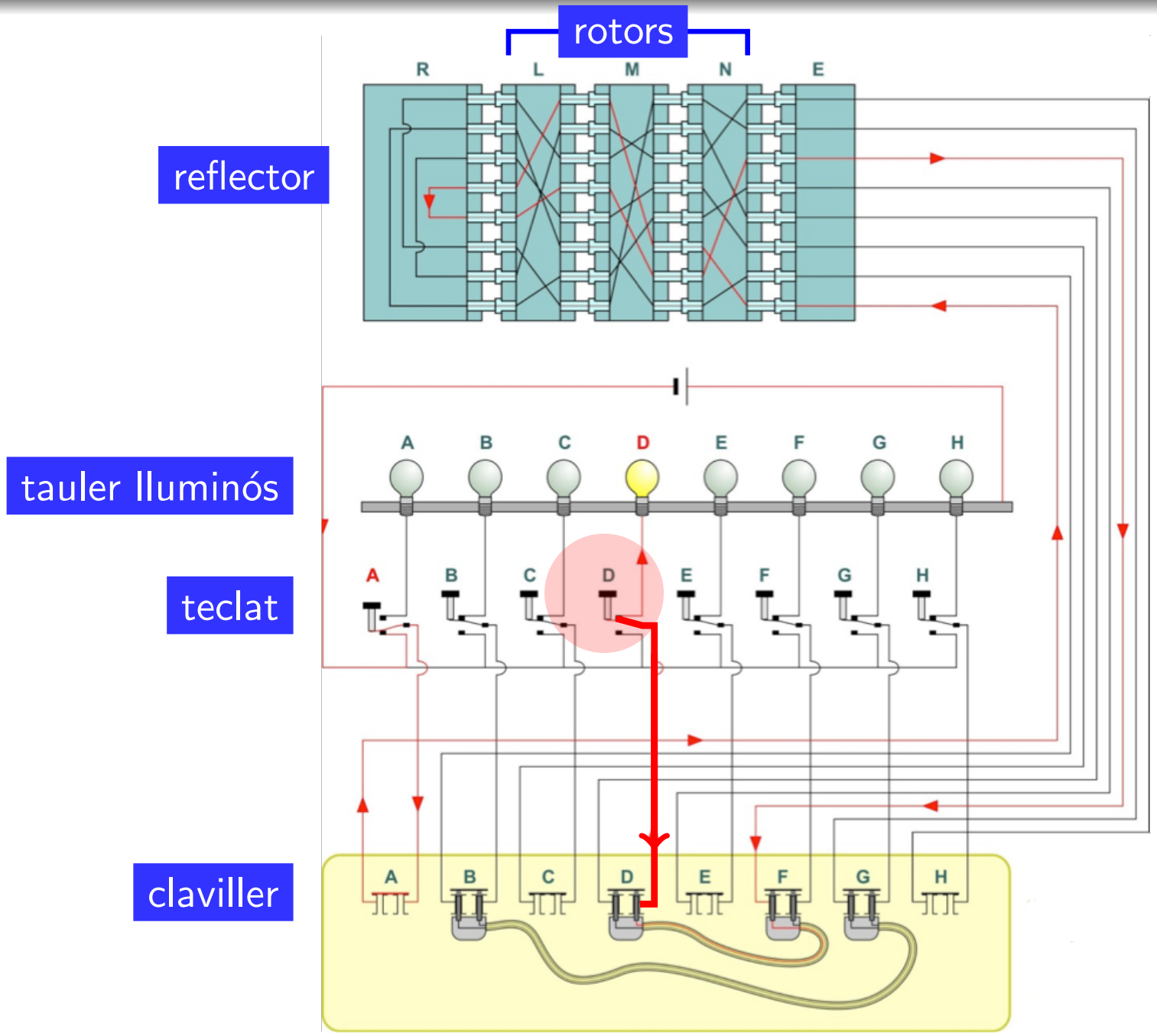
El circuït encriptador d'Enigma



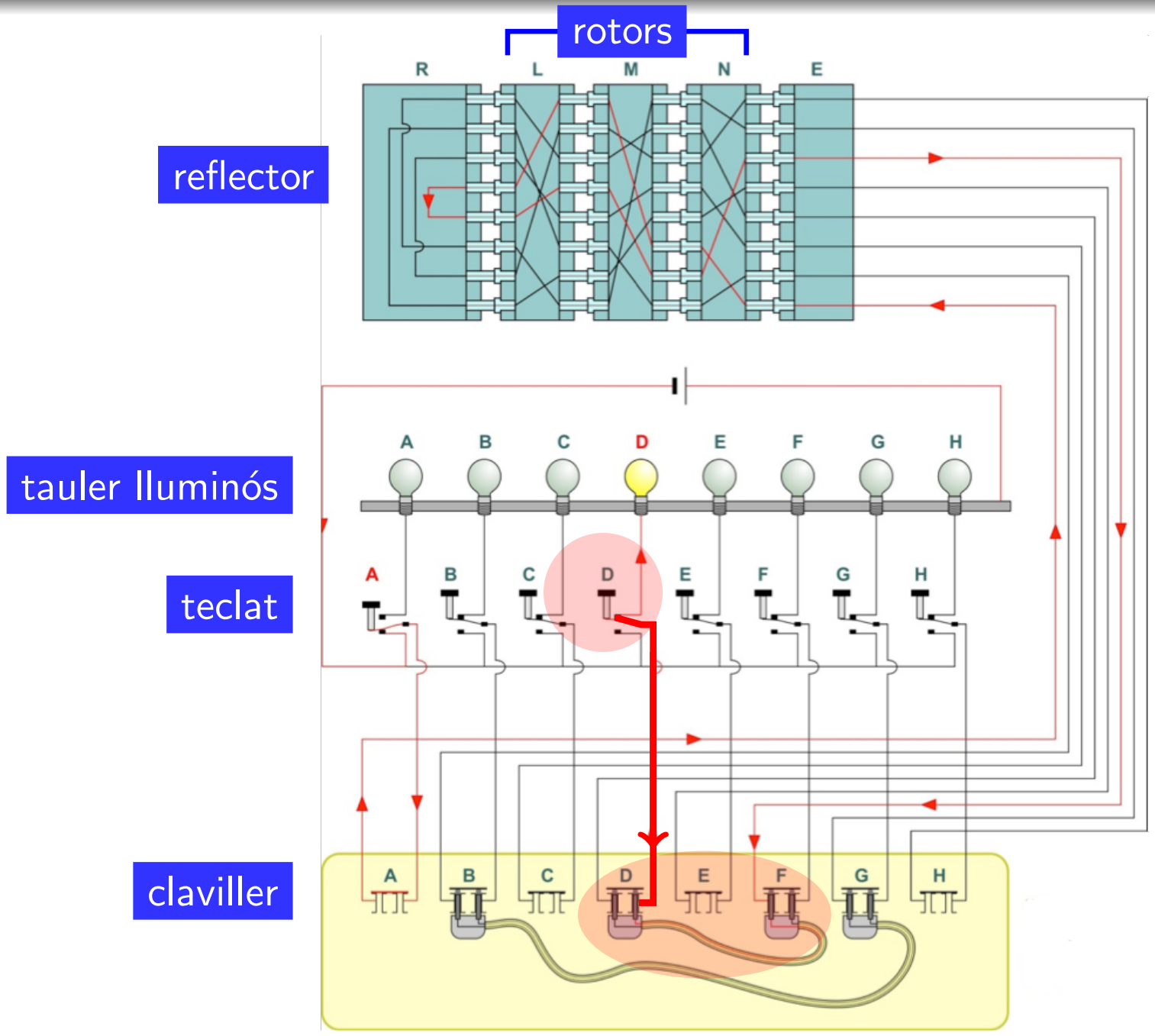
El circuït encriptador d'Enigma



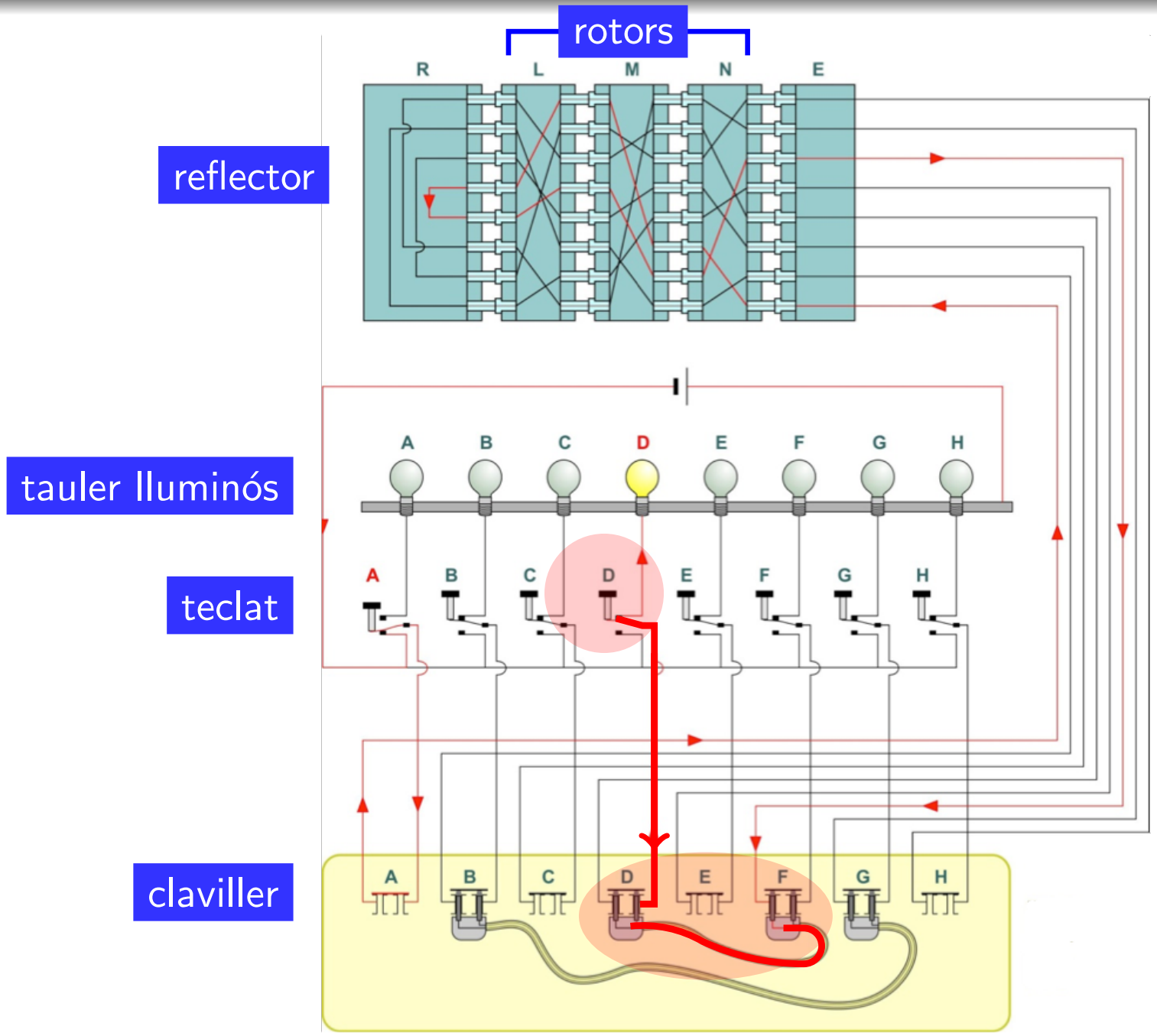
El circuït encriptador d'Enigma



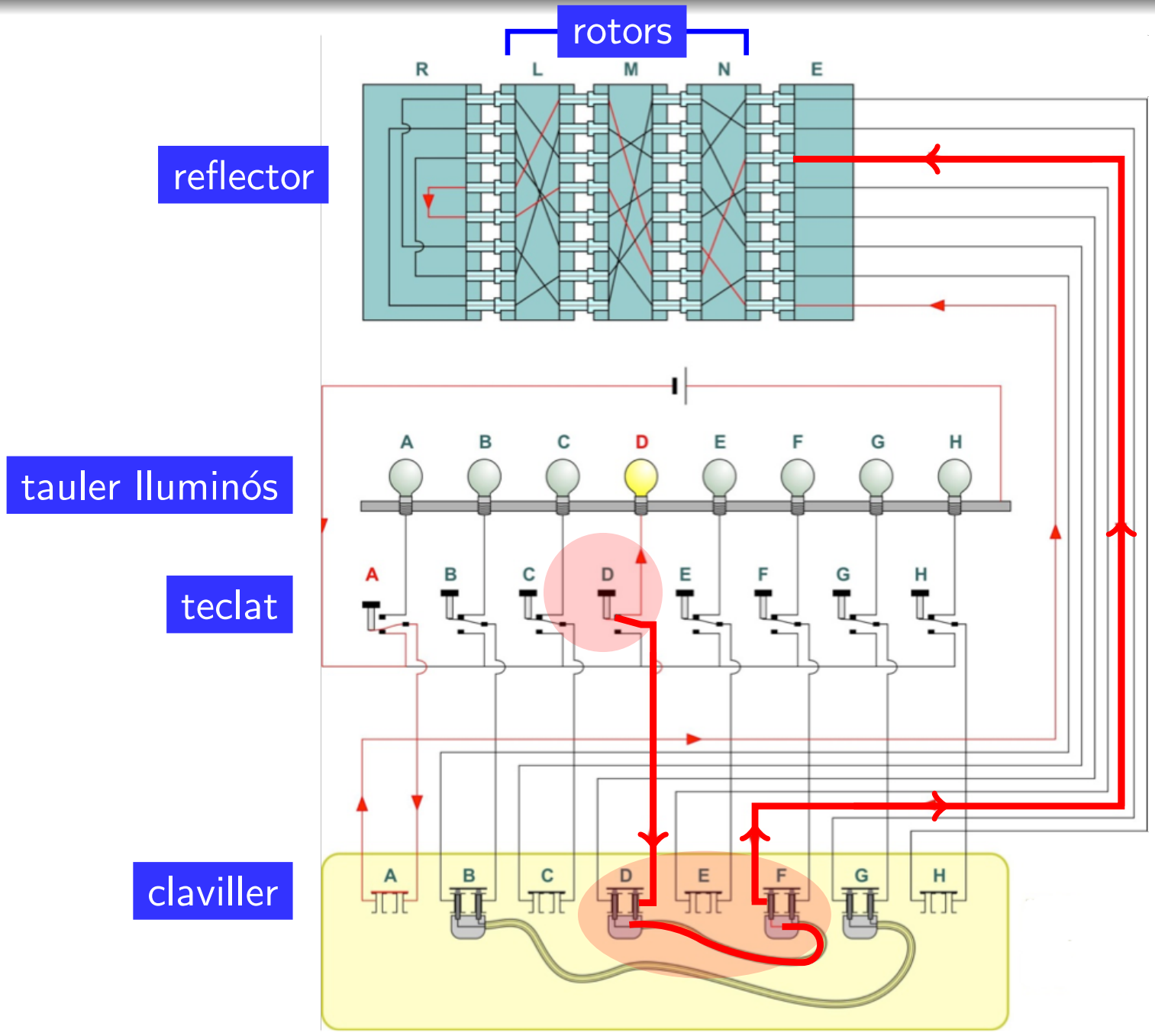
El circuït encriptador d'Enigma



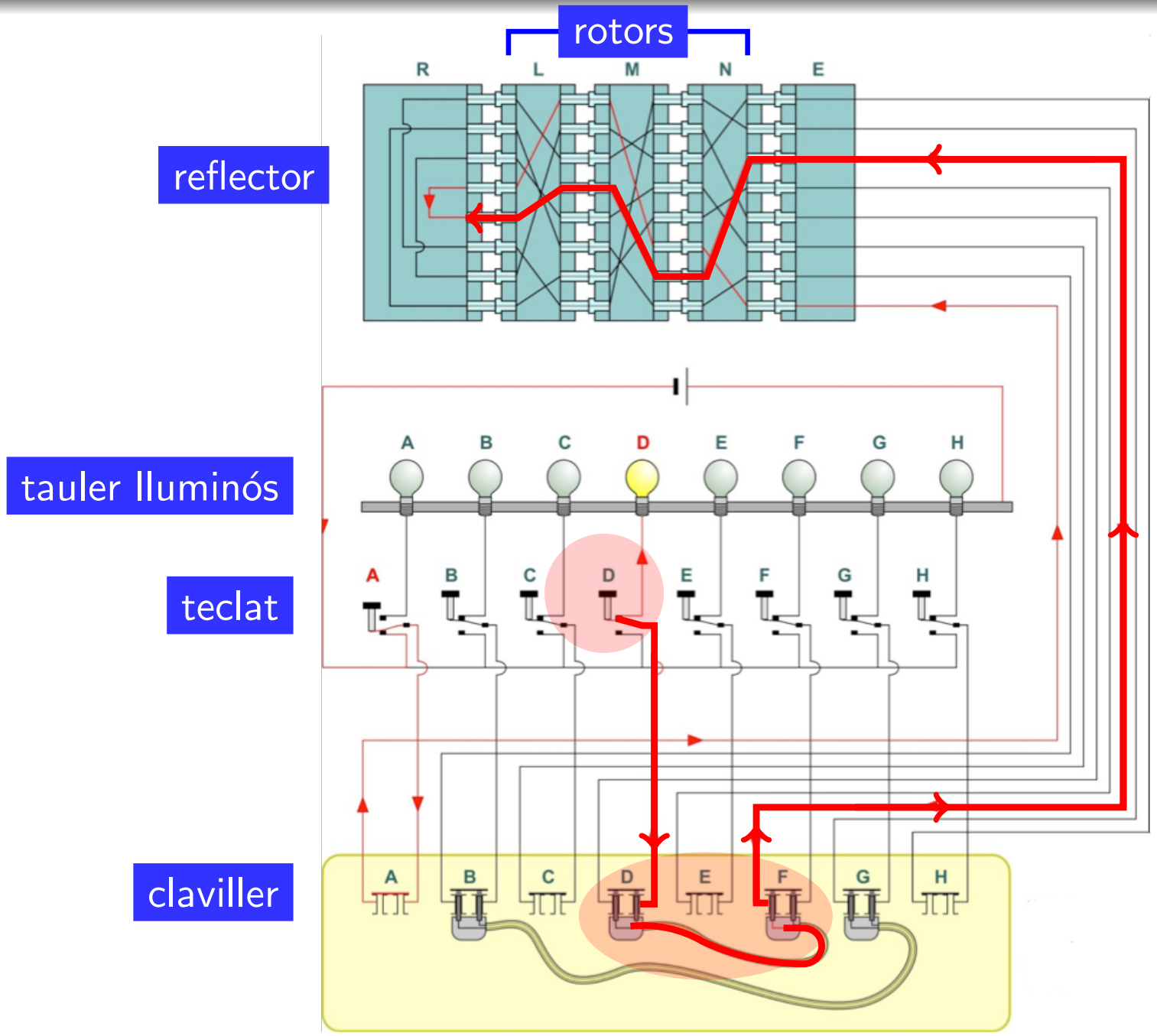
El circuït encriptador d'Enigma



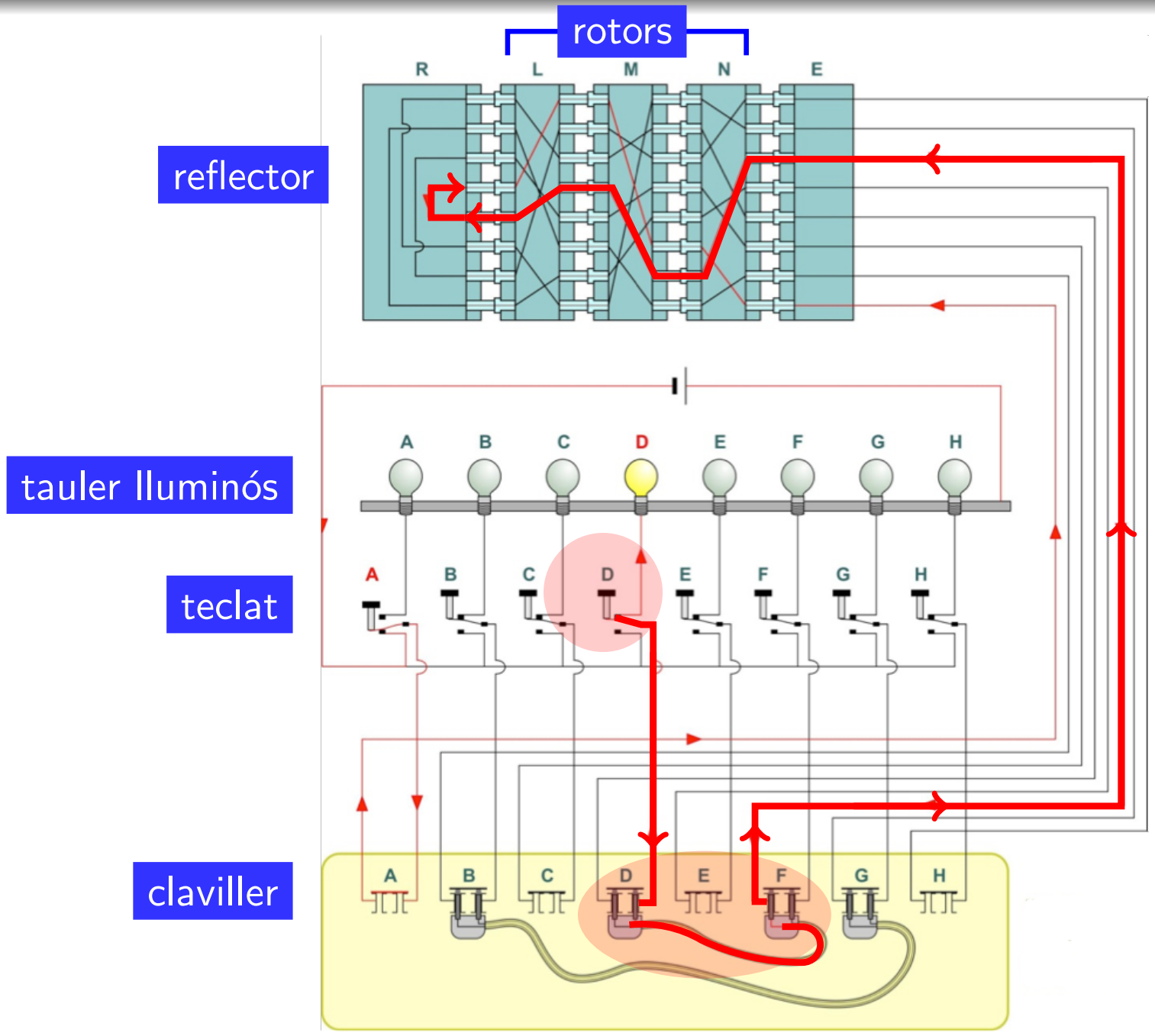
El circuït encriptador d'Enigma



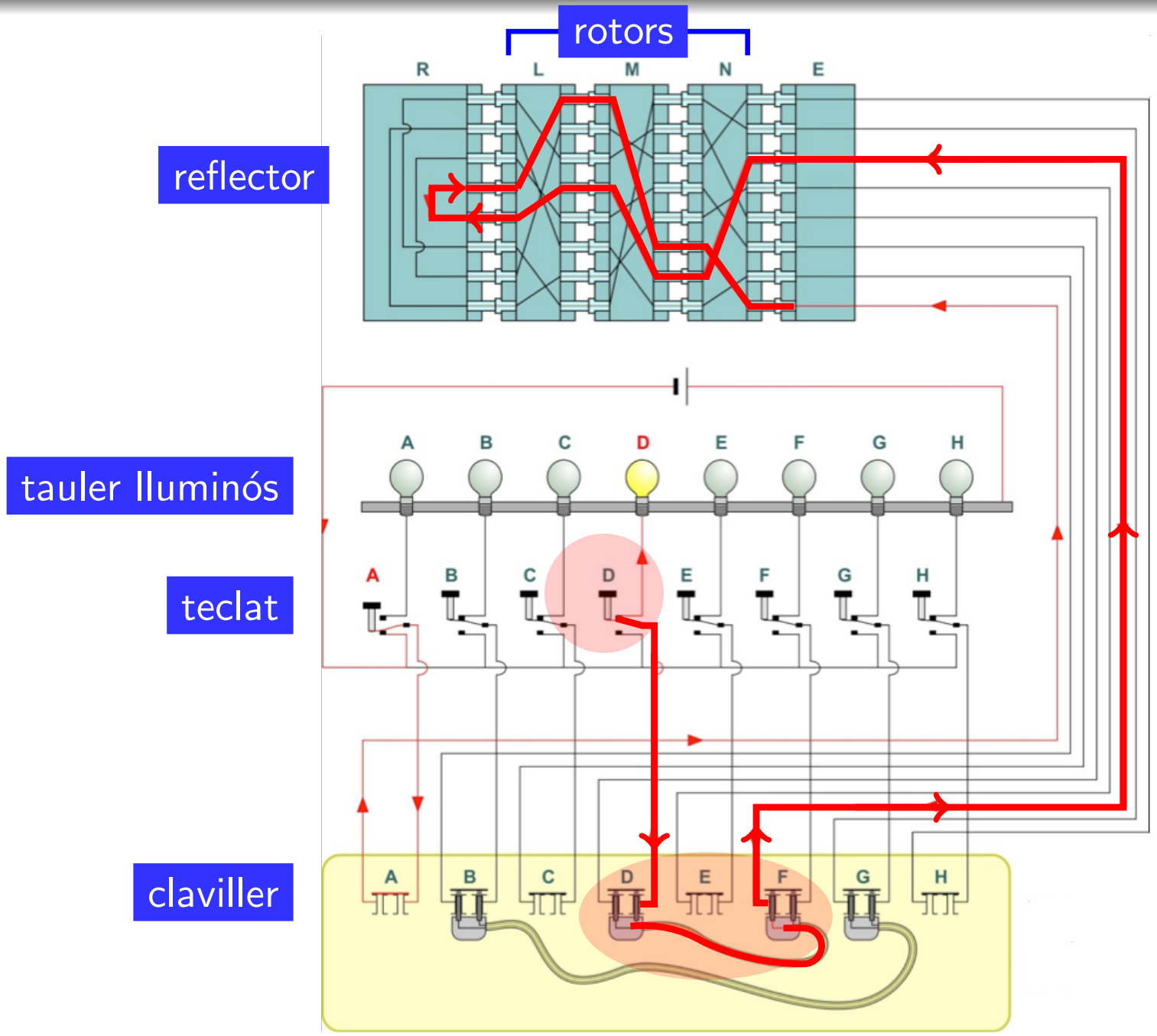
El circuït encriptador d'Enigma



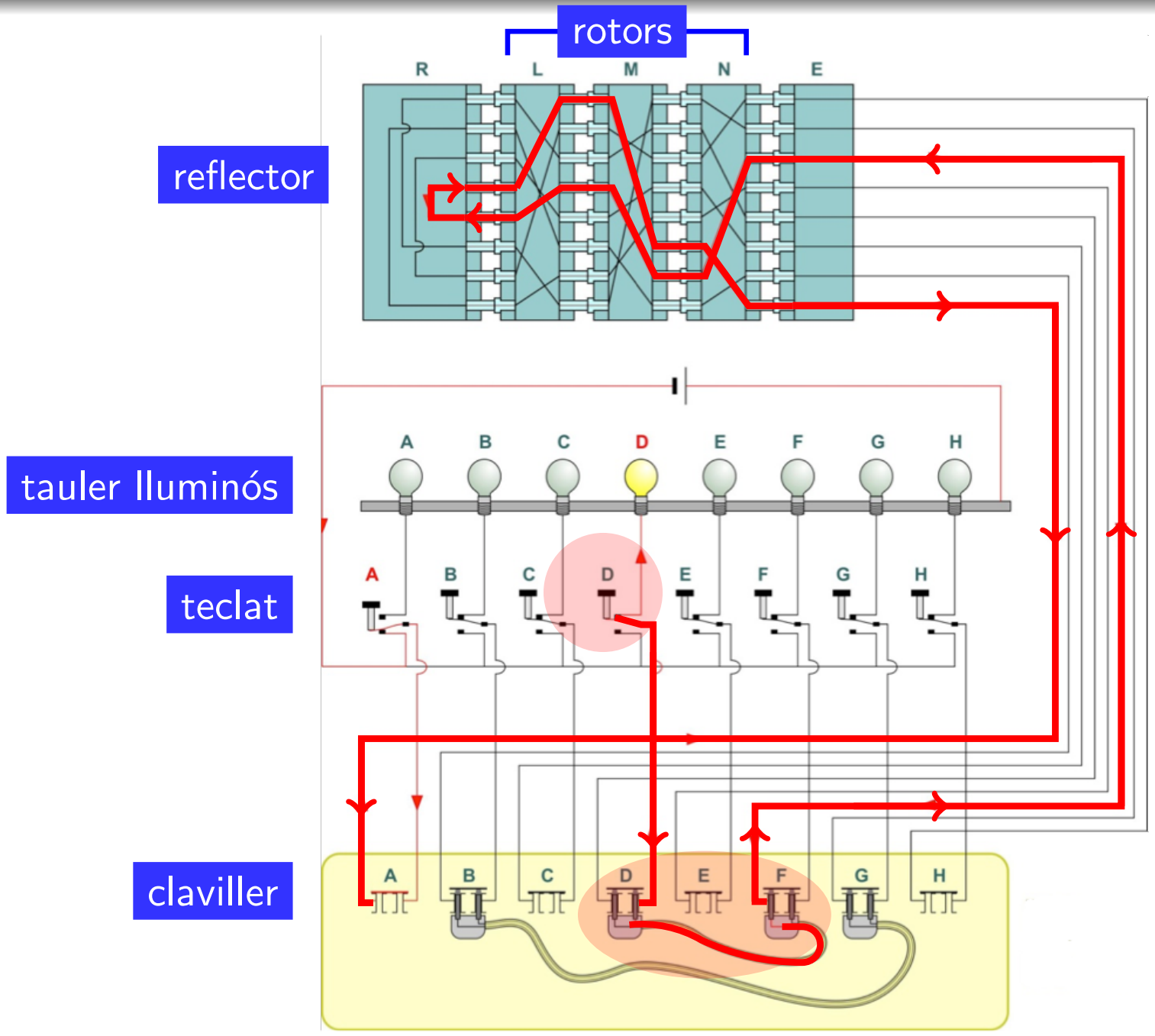
El circuït encriptador d'Enigma



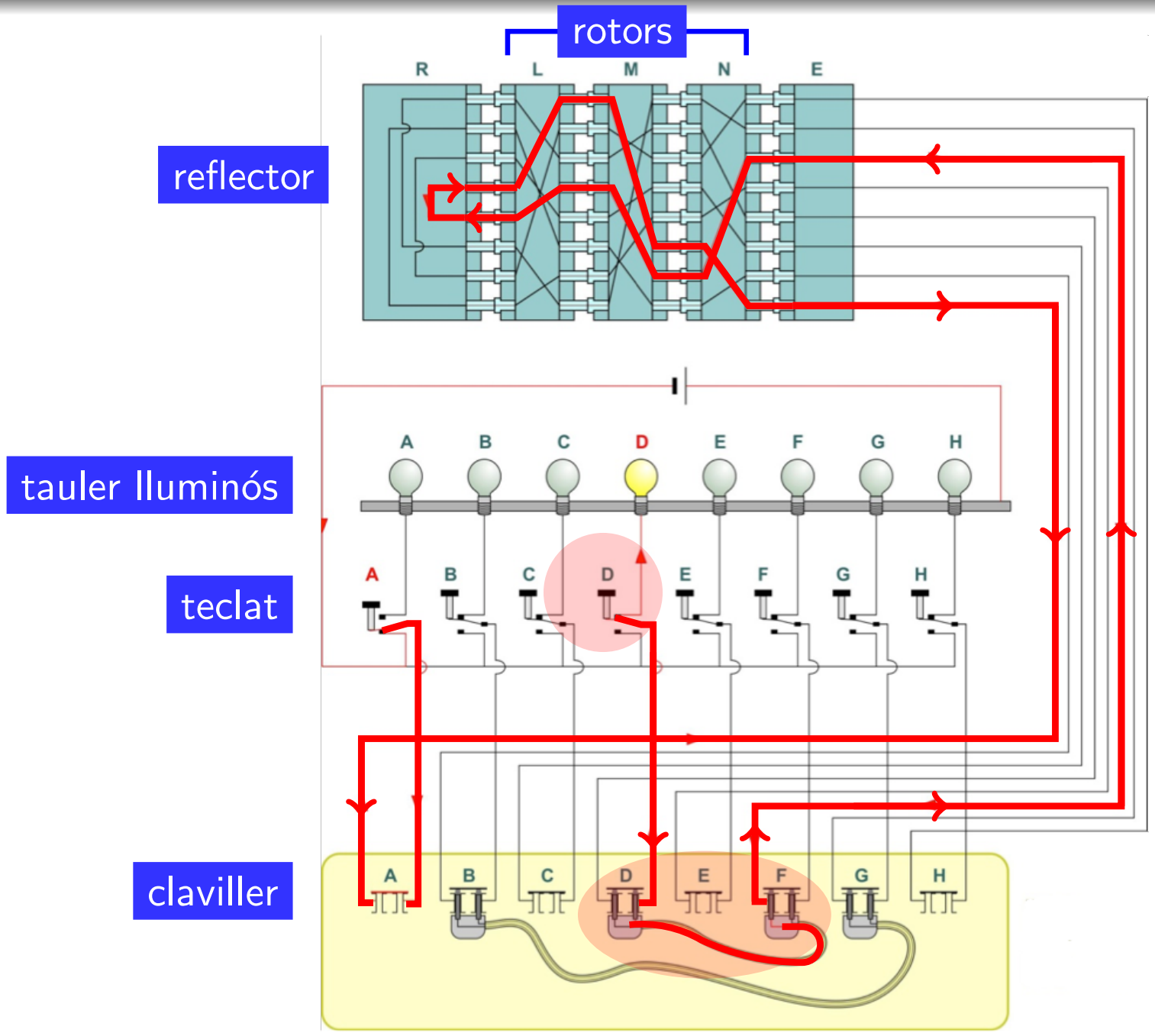
El circuït encriptador d'Enigma



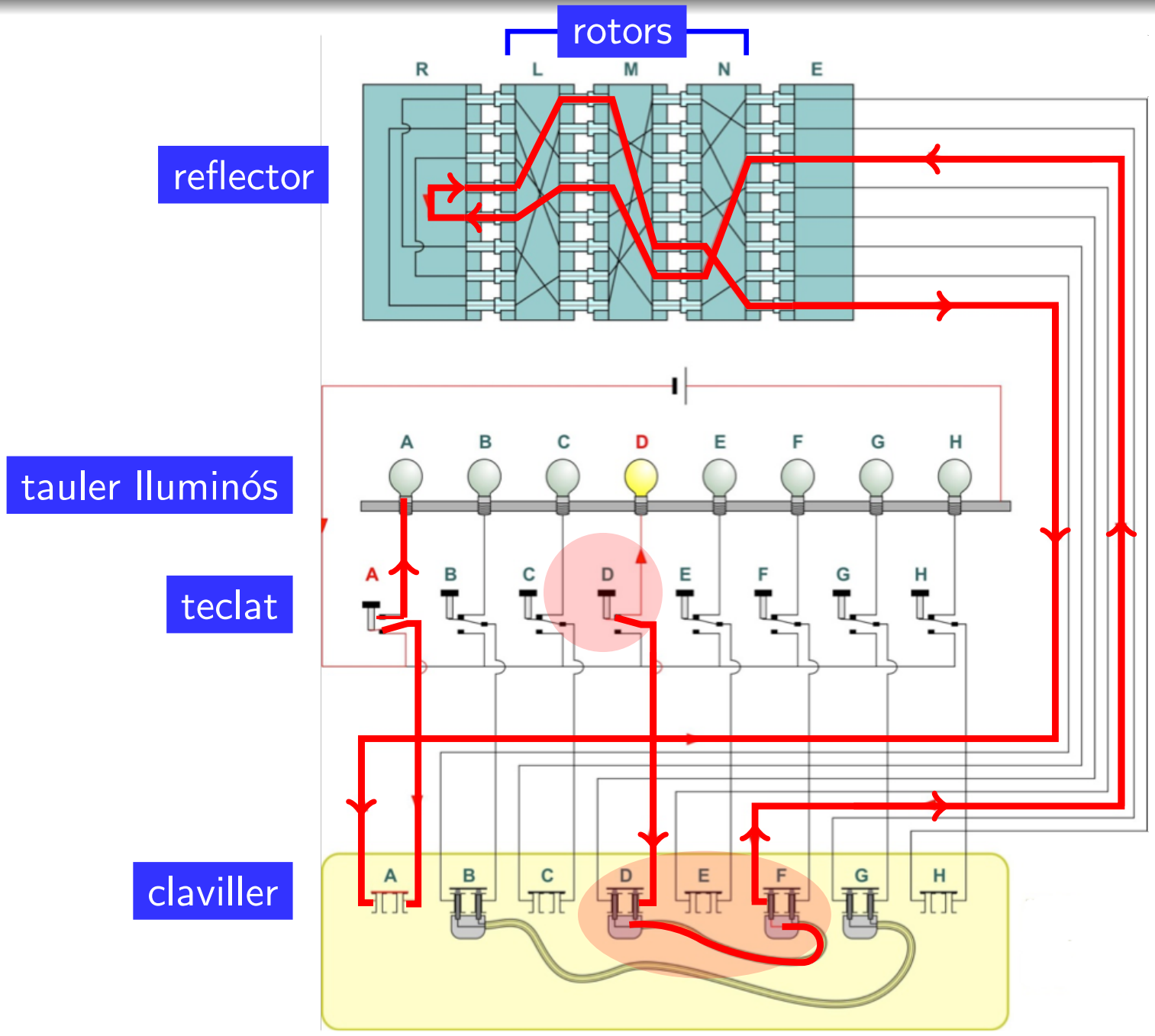
El circuït encriptador d'Enigma



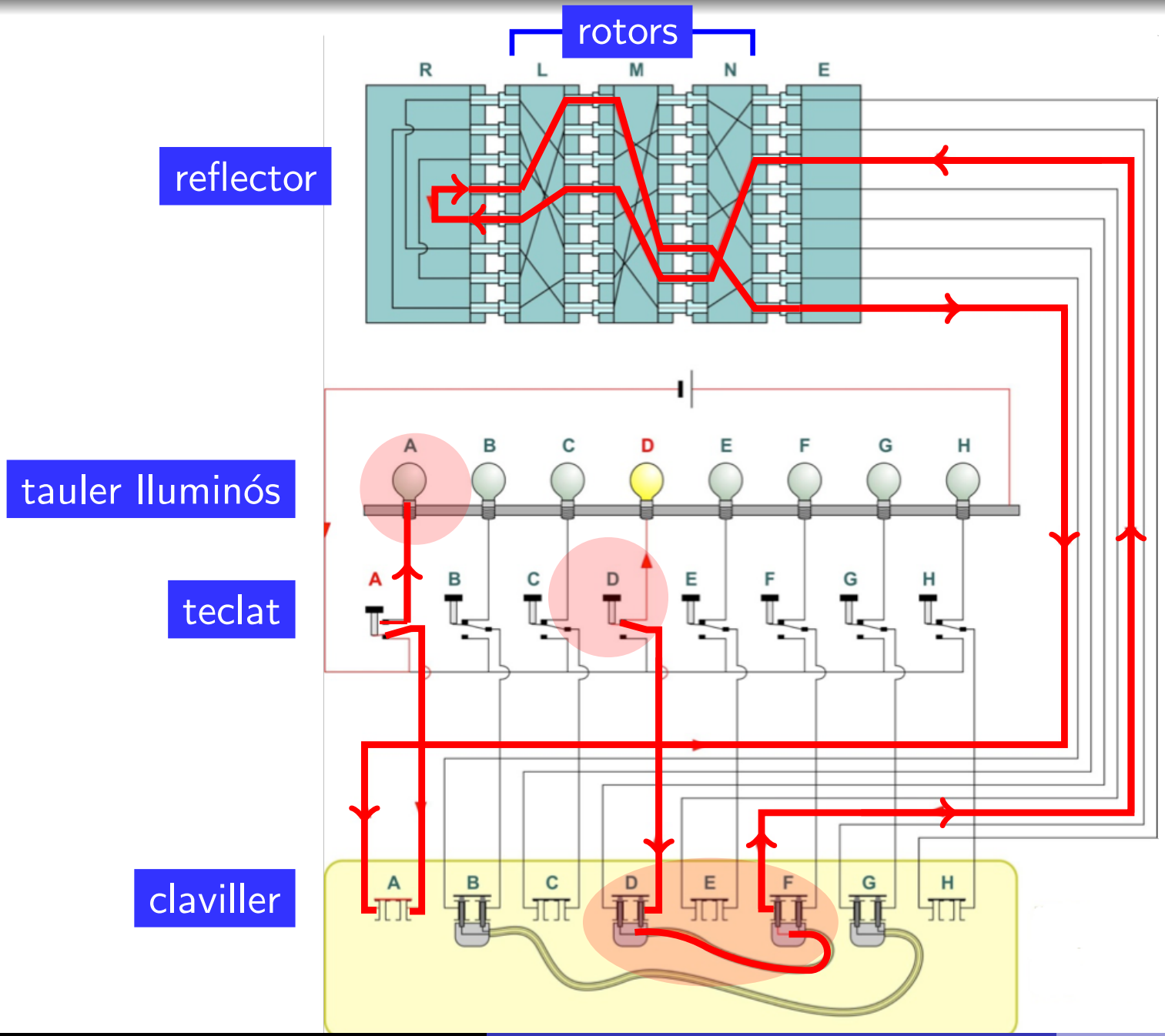
El circuït encriptador d'Enigma



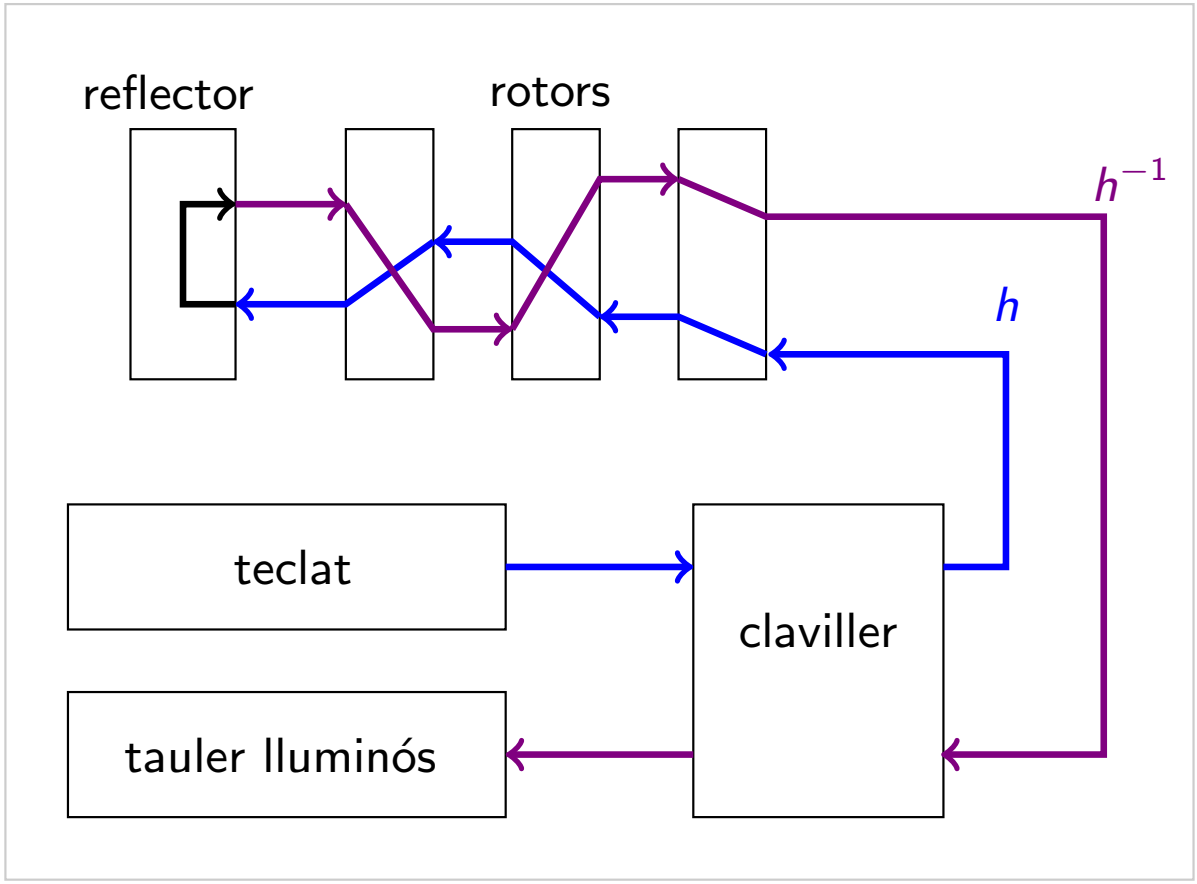
El circuït encriptador d'Enigma



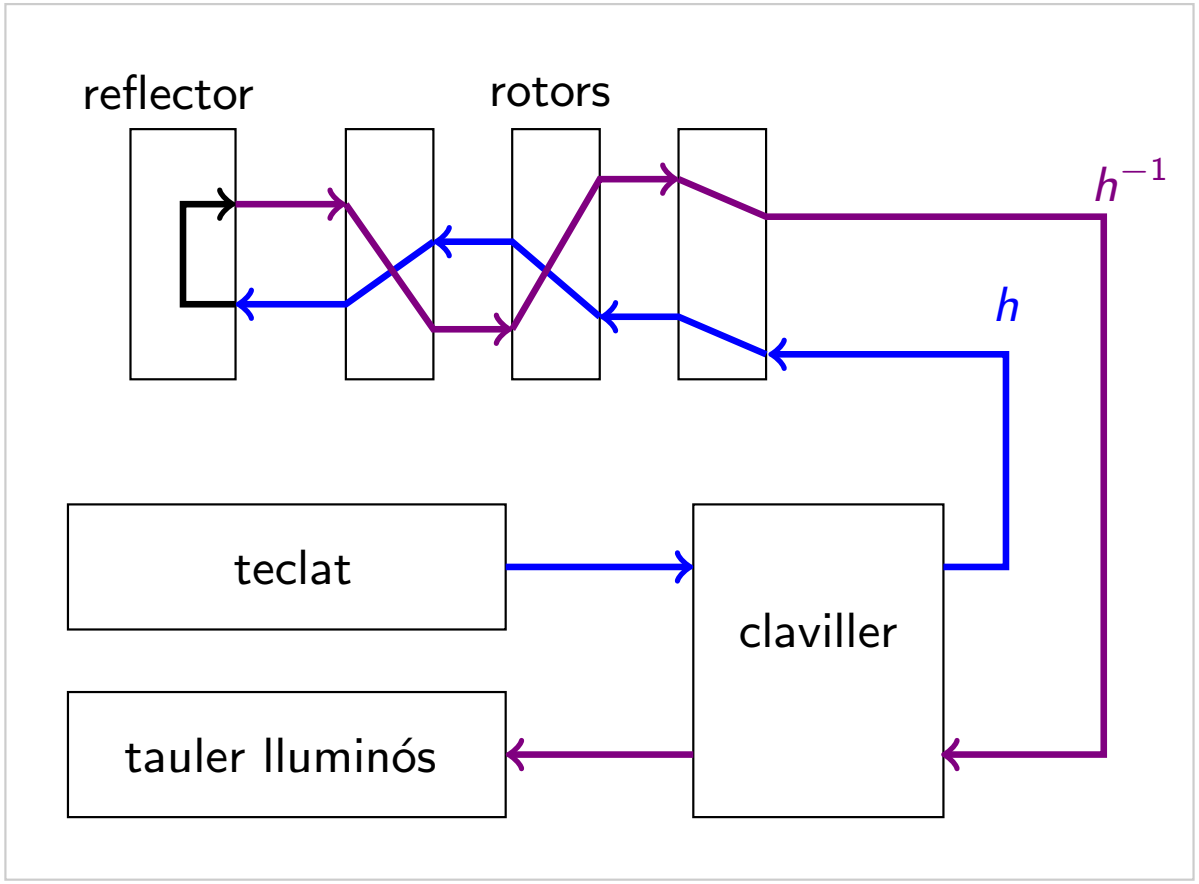
El circuït encriptador d'Enigma



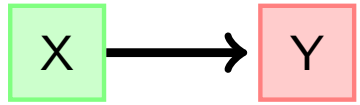
Propietat 1: simetria



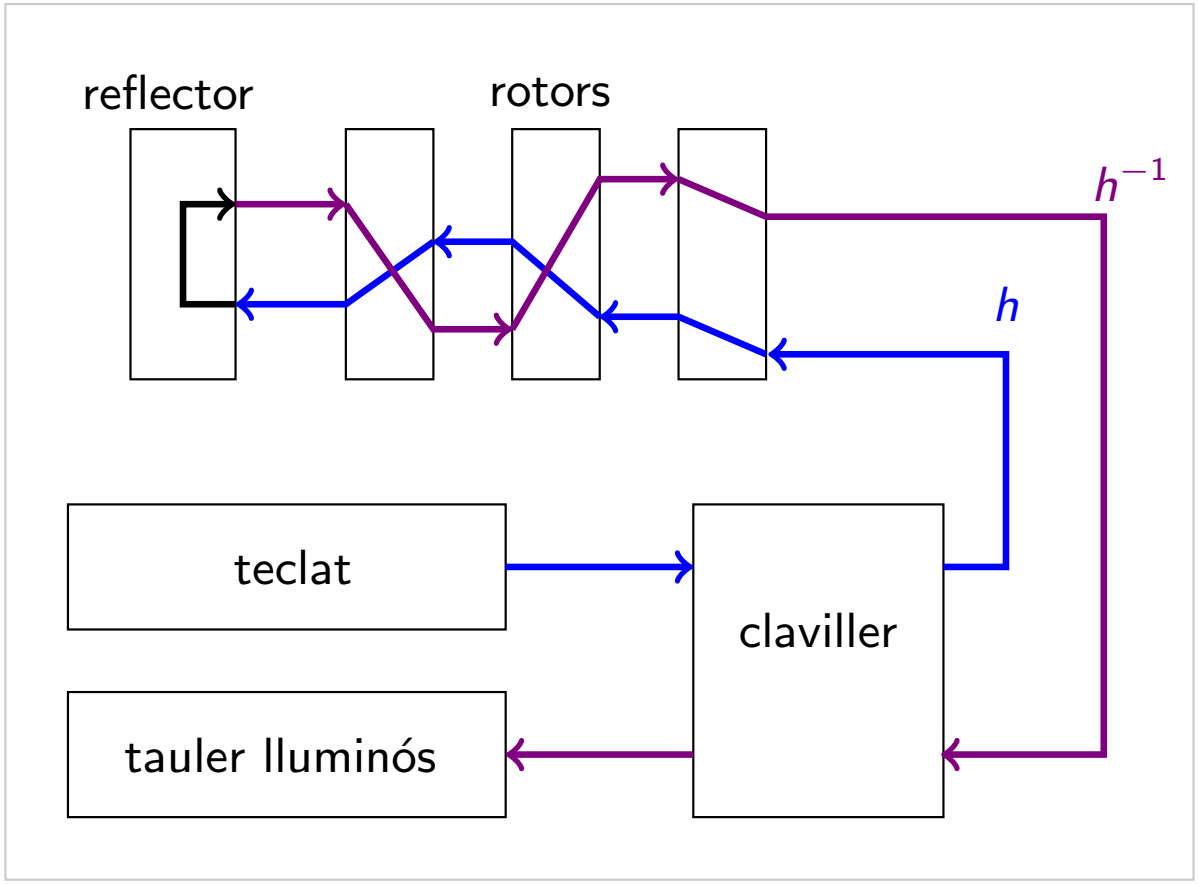
Propietat 1: simetria



xifratge

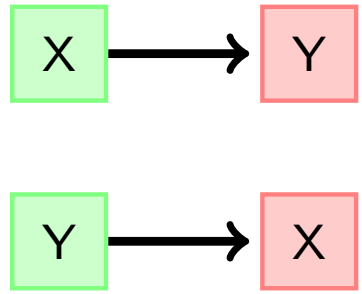


Propietat 1: simetria

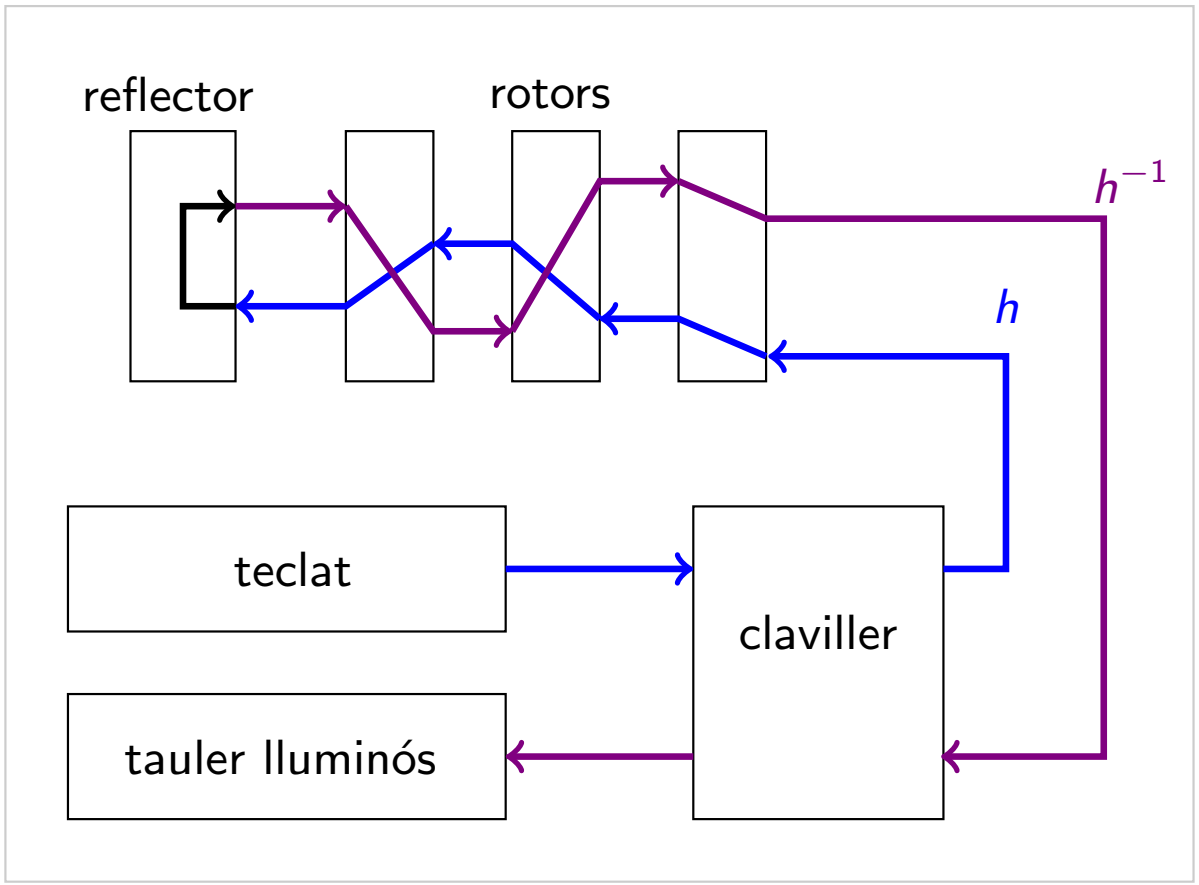


xifratge

i desxifratge!

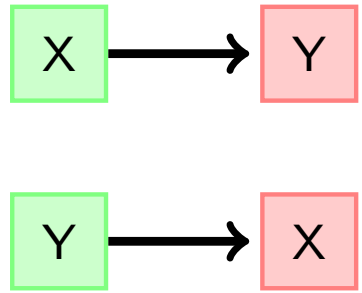


Propietat 1: simetria



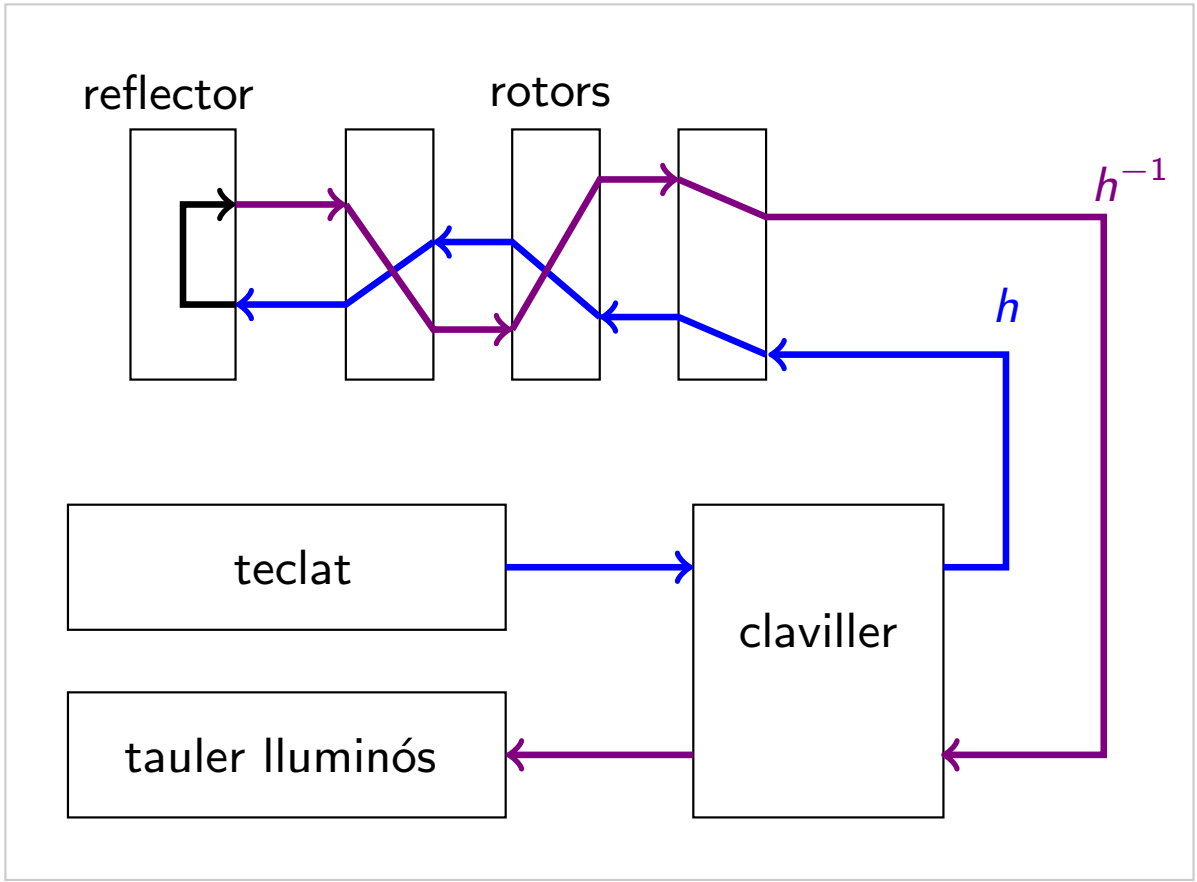
xifratge

i desxifratge!

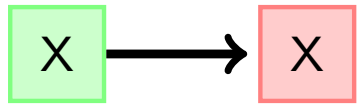


per desxifrar es configura la màquina igual que per xifrar

Propietat 2: cap lletra se xifra com ella mateixa



és impossible que

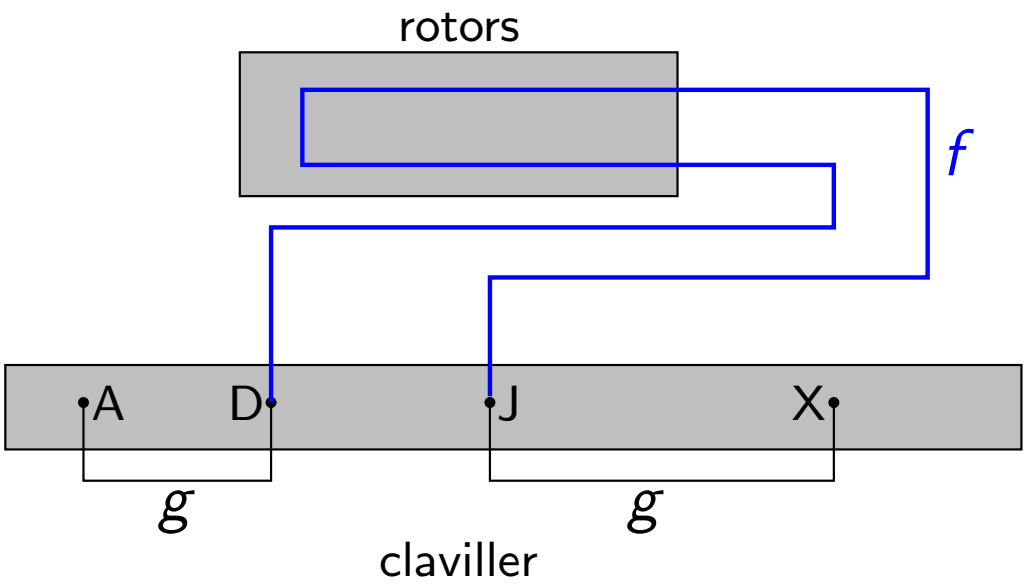


Estructura del xifratge d'una lletra

Descomposició:

g funció del claviller

f funció de recórrer els rotors i tornar.

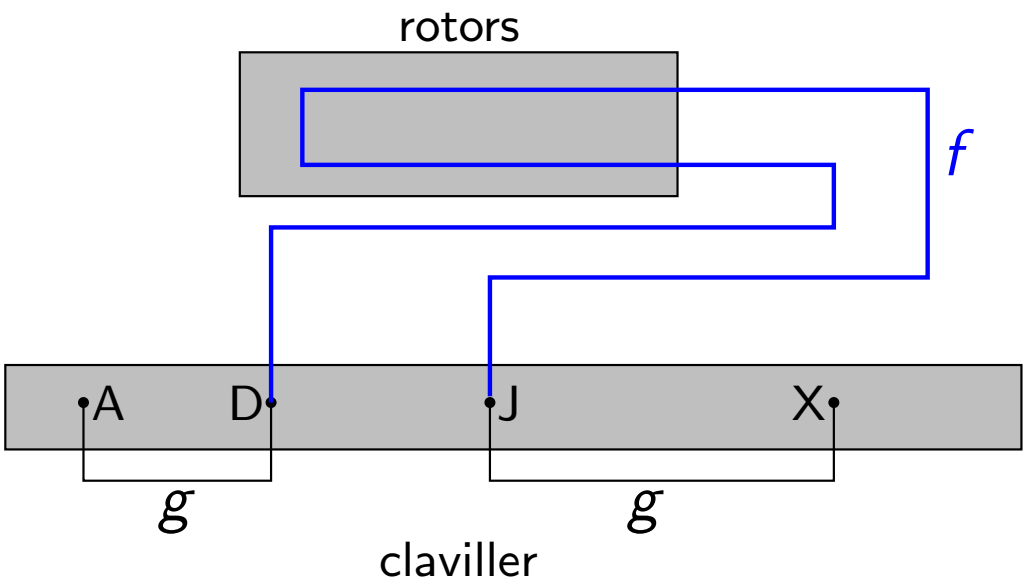


Estructura del xifratge d'una lletra

Descomposició:

g funció del claviller

f funció de recórrer els rotors i tornar.



Propietats

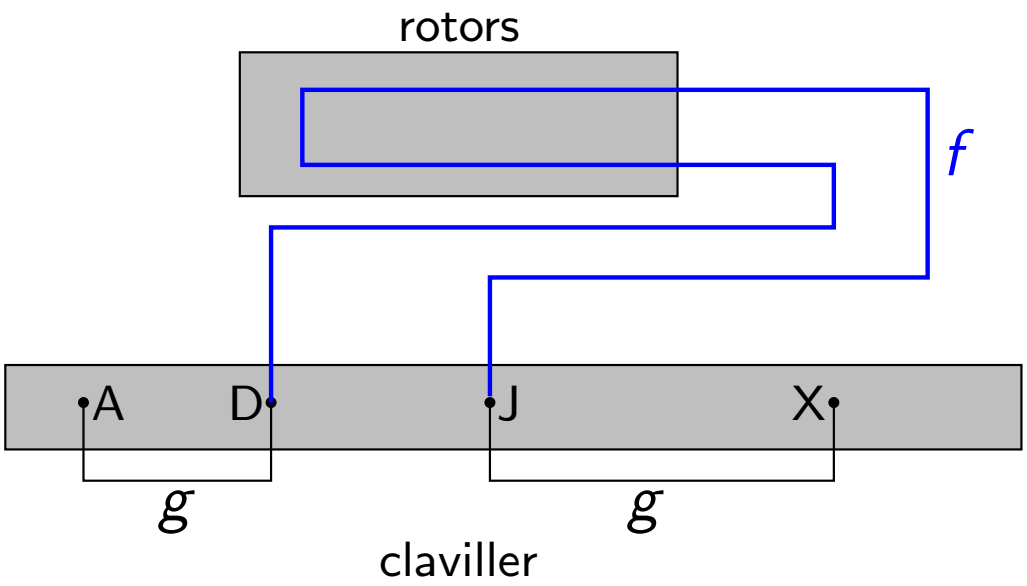
- $f = f^{-1}$

Estructura del xifratge d'una lletra

Descomposició:

g funció del claviller

f funció de recórrer els rotors i tornar.



Propietats

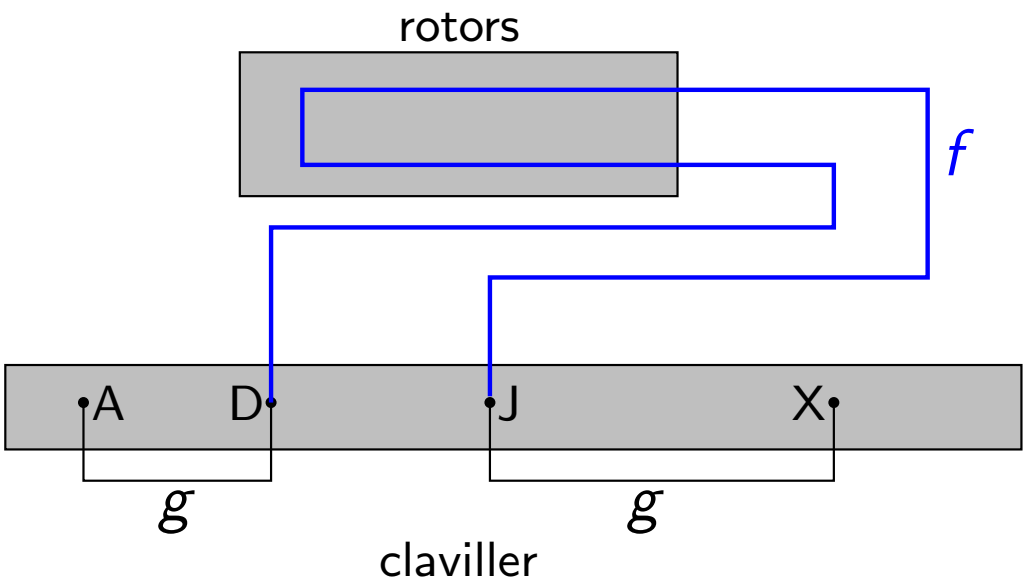
- $f = f^{-1}$
- $g = g^{-1}$

Estructura del xifratge d'una lletra

Descomposició:

g funció del claviller

f funció de recórrer els rotors i tornar.



Propietats

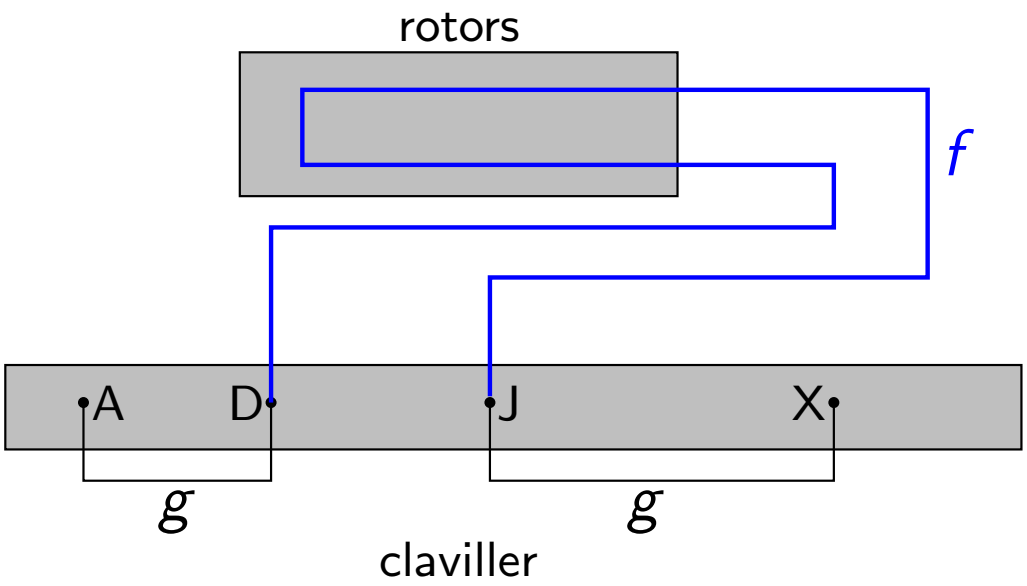
- $f = f^{-1}$
- $g = g^{-1}$
- funció de xifratge/desxifratge: $g \circ f \circ g$.

Estructura del xifratge d'una lletra

Descomposició:

g funció del claviller

f funció de recórrer els rotors i tornar.



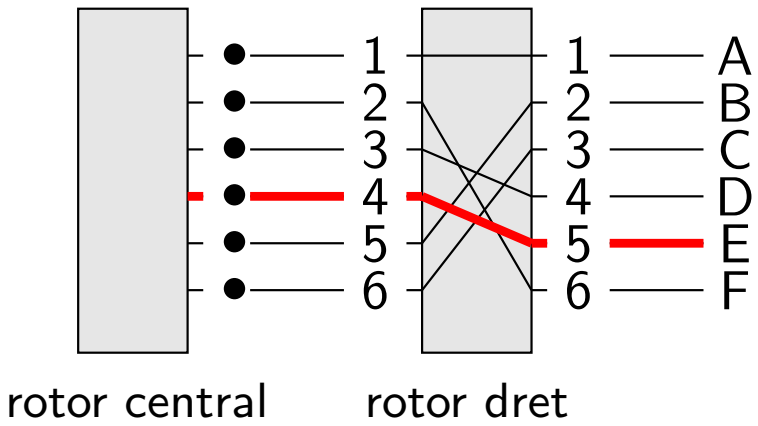
Propietats

- $f = f^{-1}$
- $g = g^{-1}$
- funció de xifratge/desxifratge: $g \circ f \circ g$.
- cap lletra se xifra com ella mateixa.

Canvi en el circuït encriptador en pitjar una tecla

Abans de xifrar una lletra el rotor dret gira un pas

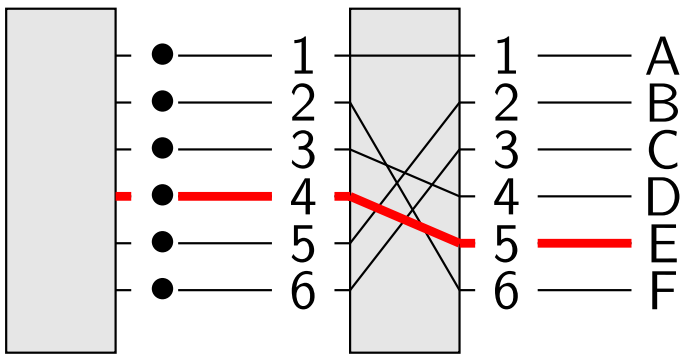
xifratge primera lletra



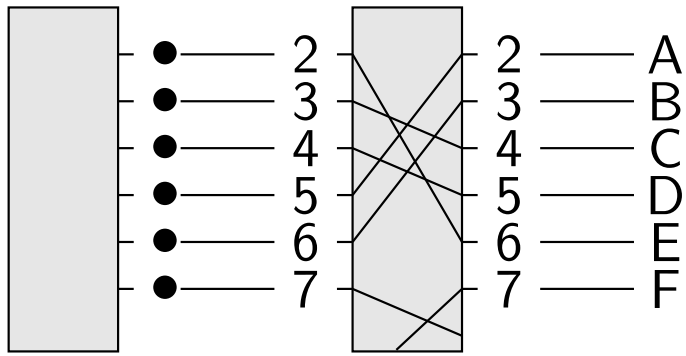
Canvi en el circuït encriptador en pitjar una tecla

Abans de xifrar una lletra el rotor dret gira un pas

xifratge primera lletra



xifratge segona lletra



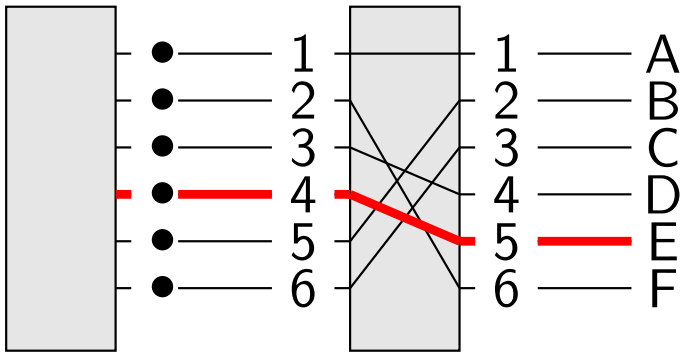
no s'ha mogut

ha avançat un pas

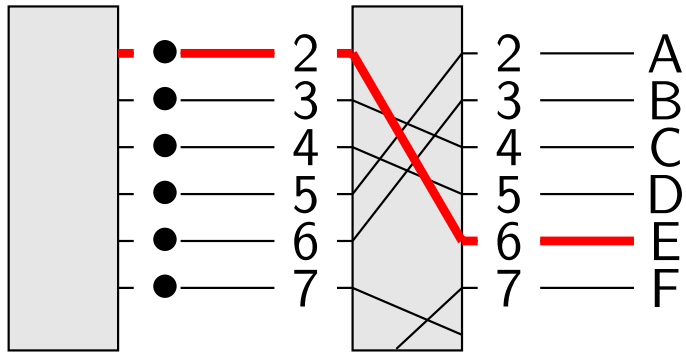
Canvi en el circuït encriptador en pitjar una tecla

Abans de xifrar una lletra el rotor dret gira un pas

xifratge primera lletra



xifratge segona lletra

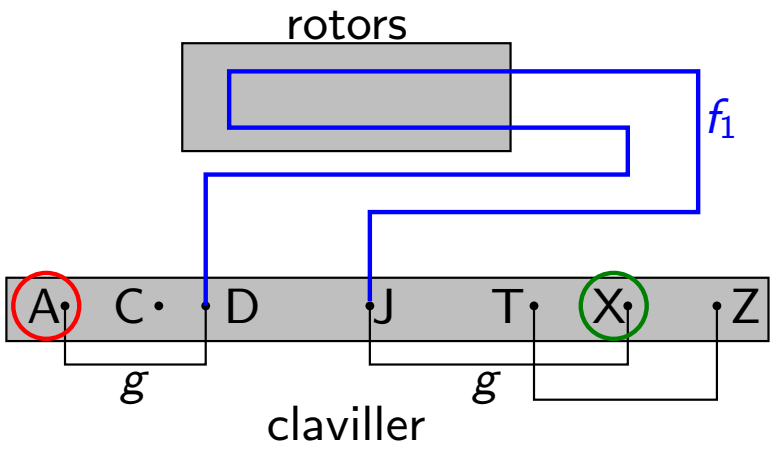


Xiframent d'una paraula

Xifrem A T A C

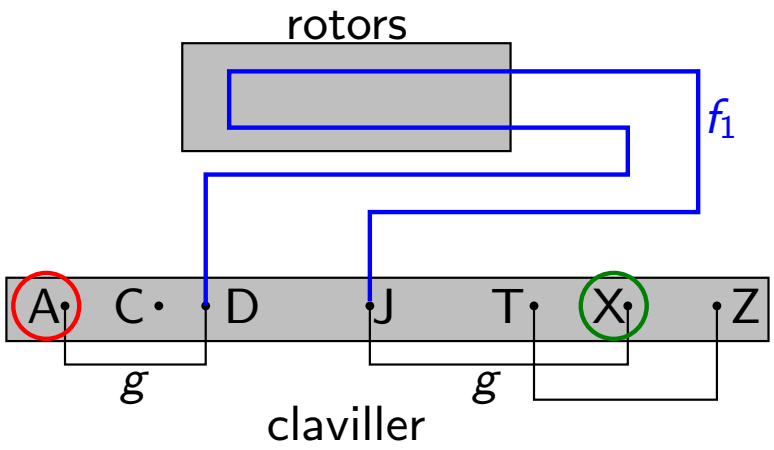
Xiframent d'una paraula

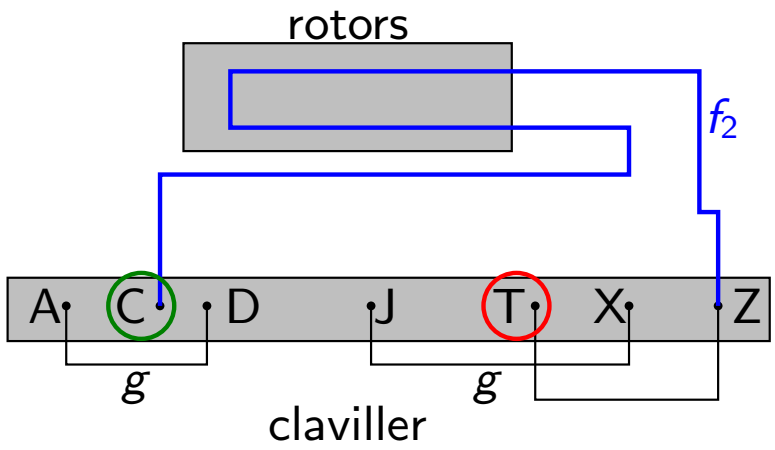
Xifrem A T A C $\longrightarrow$ X _ _ _



Xiframent d'una paraula

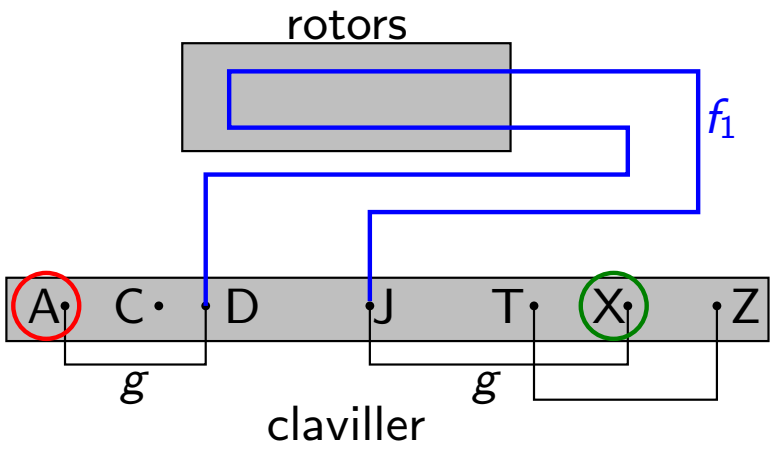
Xifrem A T A C $\longrightarrow$ X C _ _

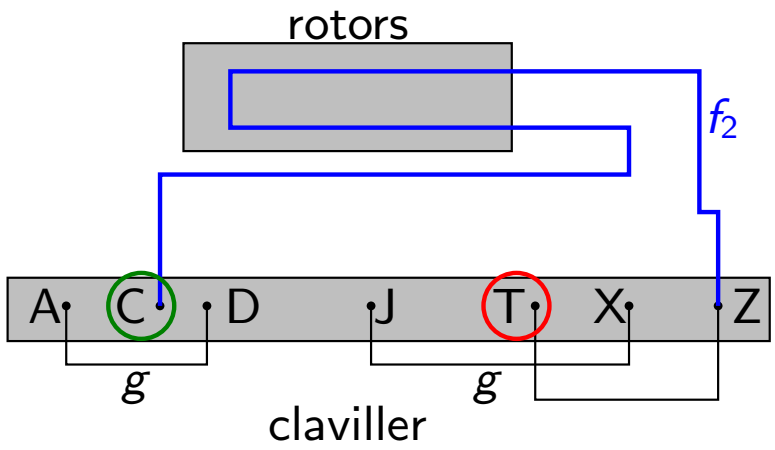


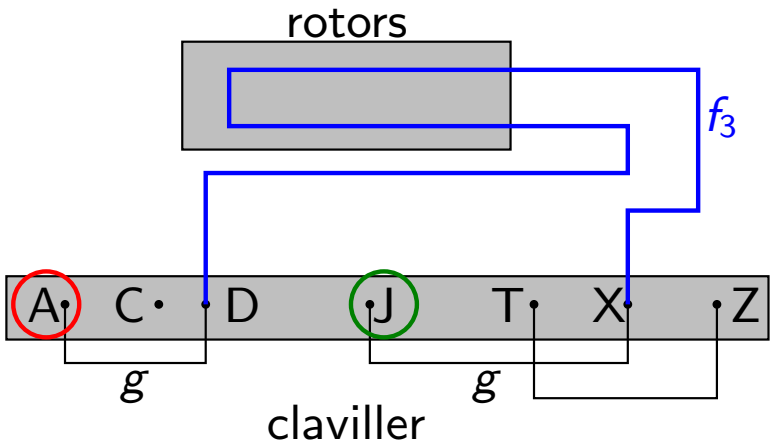


Xiframent d'una paraula

Xifrem A T A C $\longrightarrow$ X C J _

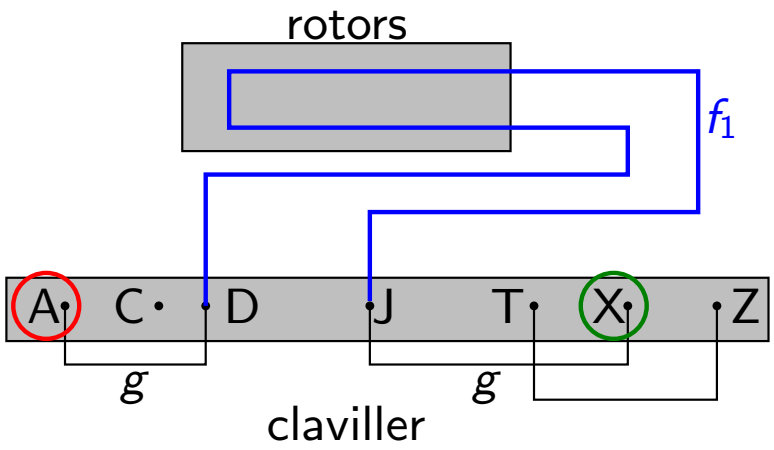


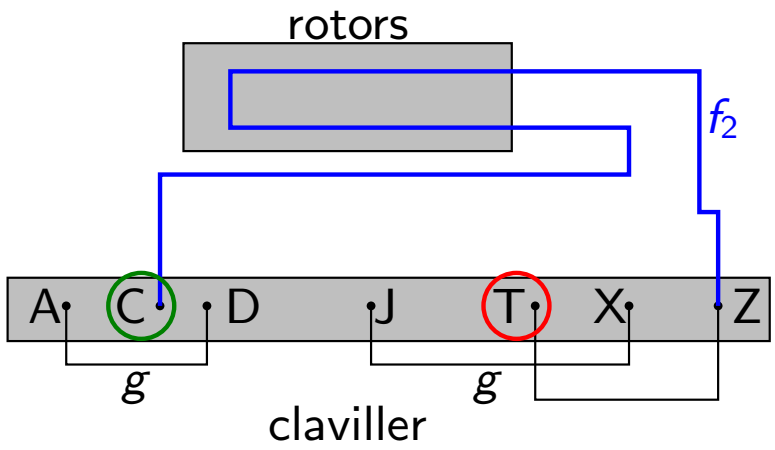


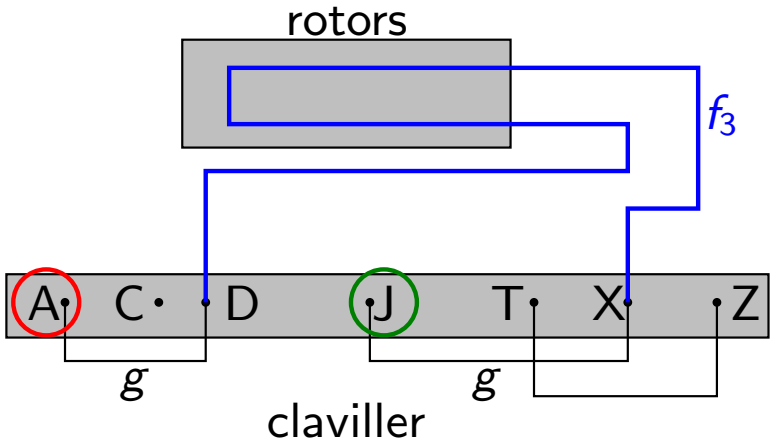


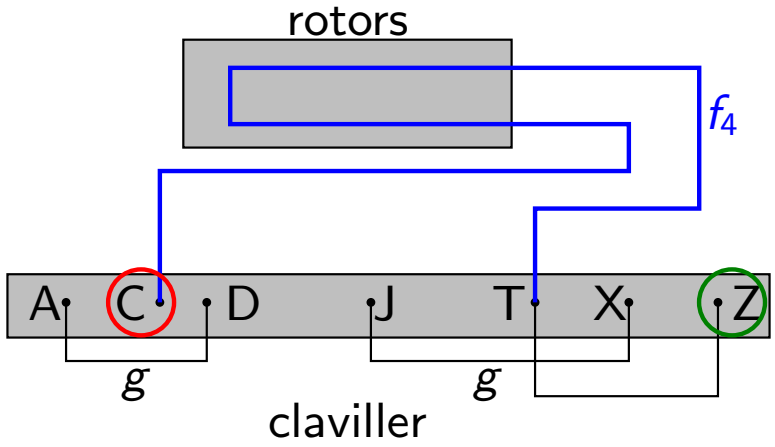
Xiframent d'una paraula

Xifrem A T A C $\longrightarrow$ X C J Z









Primer desxiframent de l'Enigma (Polònia, 1930–1939)

Marian Rejewski

Henryk Zygalski

Primer desxiframent de l'Enigma (Polònia, 1930–1939)

Marian Rejewski

Disseny de prototips de la màquina Enigma, deduint el cablejat.

Henryk Zygalski

Primer desxiframent de l'Enigma (Polònia, 1930–1939)

Marian Rejewski

Disseny de prototips de la màquina Enigma, deduint el cablejat.

Diversos mètodes per trobar la clau d'un missatge.

Henryk Zygalski

Primer desxiframent de l'Enigma (Polònia, 1930–1939)

Marian Rejewski

Disseny de prototips de la màquina Enigma, deduint el cablejat.

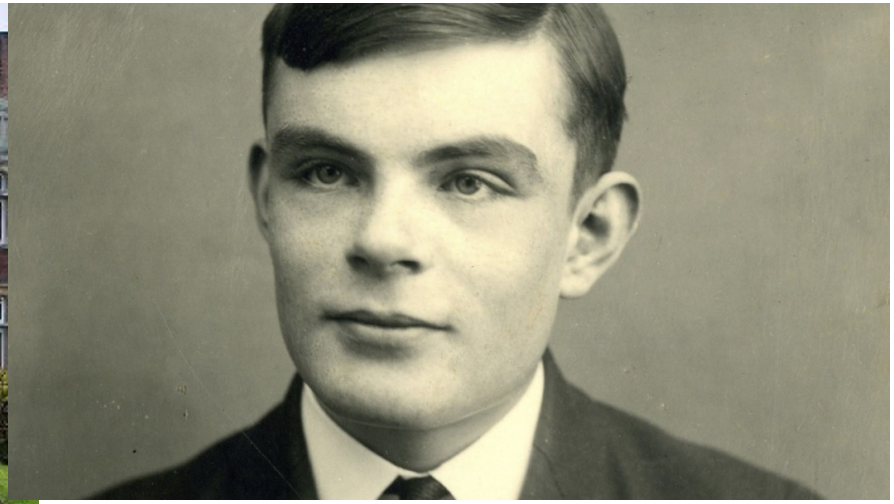
Diversos mètodes per trobar la clau d'un missatge.

Construcció de la primera bomba

Henryk Zygalski

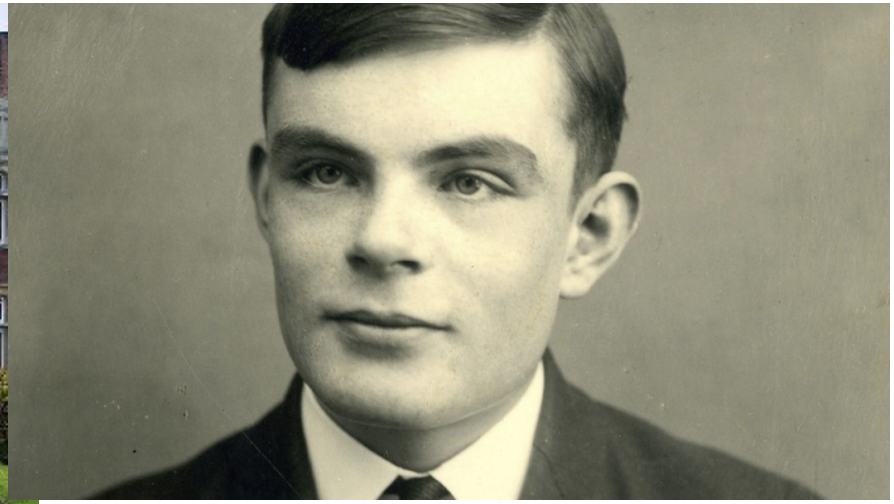
Bletchley Park. Projecte ULTRA

Bletchley Park. Projecte ULTRA



Alan Turing

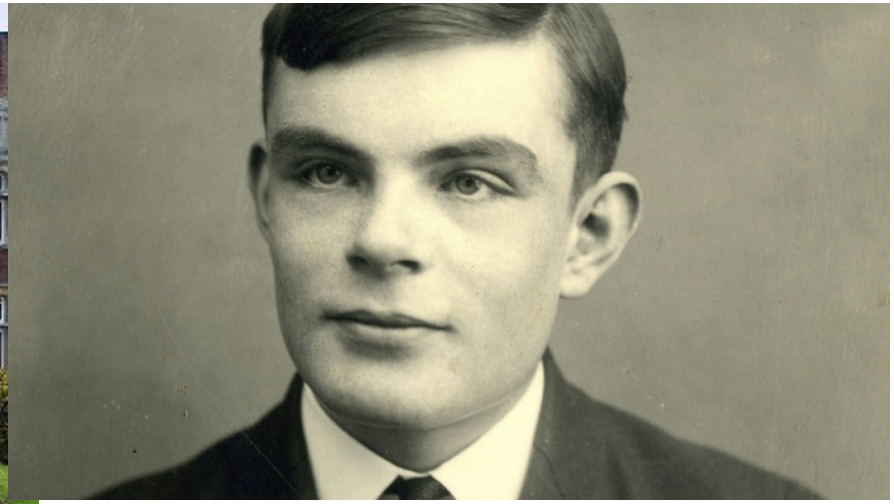
Bletchley Park. Projecte ULTRA



Alan Turing

Gordon Welchman

Bletchley Park. Projecte ULTRA



Alan Turing

Harold Keen

Gordon Welchman

Procediment de xifratge Enigma des de 1939

Per xifrar un missatge

- Configurar la màquina segons la **clau del dia** (ordre dels rotors, configuració dels anells, 10 connexions).
- Triar **la clau del missatge**, per exemple ABC.
- Triar **l'indicador**, per exemple GDN
- Girar els rotors a posició GND. Xifrar dos cops ABC, per exemple WQRCCA.
- Girar els rotors a la posició ABC i continuar xifrant el missatge.

Per desxifrar el missatge

- Configurar la màquina segons la **clau del dia**
- Girar els rotors segons **l'indicador** GDN (apareix en clar al preàmbul)
- Desxifrar les 6 primeres lletres del missatge xifrat.
- S'obté ABCABC.
- Girar els rotors a la posició ABC i continuar desxifrant el missatge.

Les "cribs" o paraules probables

paraula probable: és una paraula en clar que suposem que apareix en el missatge que hem de desxifrar.

Les "cribs" o paraules probables

paraula probable: és una paraula en clar que suposem que apareix en el missatge que hem de desxifrar.

Conjectura basada en:

- frases molt usades com ara "Sense novetats",
- l'experiència (butlletins meteorològics, avisos d'atacs),
- missatges ja trencats que els alemanys tornaven a xifrar amb una nova clau,
- espionatge o captures de submarins.

Les "cribs" o paraules probables

paraula probable: és una paraula en clar que suposem que apareix en el missatge que hem de desxifrar.

Conjectura basada en:

- frases molt usades com ara "Sense novetats",
- l'experiència (butlletins meteorològics, avisos d'atacs),
- missatges ja trencats que els alemanys tornaven a xifrar amb una nova clau,
- espionatge o captures de submarins.

alineament

missatge xifrat	S	A	E	T	J	W	P	X
paraula probable	W	E	T	T	E	R		

Les "cribs" o paraules probables

paraula probable: és una paraula en clar que suposem que apareix en el missatge que hem de desxifrar.

Conjectura basada en:

- frases molt usades com ara "Sense novetats",
- l'experiència (butlletins meteorològics, avisos d'atacs),
- missatges ja trencats que els alemanys tornaven a xifrar amb una nova clau,
- espionatge o captures de submarins.

alineament

missatge xifrat	S	A	E	T	J	W	P	X
paraula probable	W	E	T	T	E	R		

missatge xifrat	S	A	E	T	J	W	P	X
paraula probable		W	E	T	T	E	R	

Les "cribs" o paraules probables

paraula probable: és una paraula en clar que suposem que apareix en el missatge que hem de desxifrar.

Conjectura basada en:

- frases molt usades com ara "Sense novetats",
- l'experiència (butlletins meteorològics, avisos d'atacs),
- missatges ja trencats que els alemanys tornaven a xifrar amb una nova clau,
- espionatge o captures de submarins.

alineament

missatge xifrat	S	A	E	T	J	W	P	X
paraula probable	W	E	T	T	E	R		

missatge xifrat	S	A	E	T	J	W	P	X
paraula probable		W	E	T	T	E	R	

missatge xifrat	S	A	E	T	J	W	P	X
paraula probable			W	E	T	T	E	R

Informació que dona un alineament correcte

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
R	W	I	V	T	Y	R	E	S	X	B	F	O	G	J	Y	G	Q	B	A	I	S	E
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A

Informació que dona un alineament correcte

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
R	W	I	V	T	Y	R	E	S	X	B	F	O	G	J	Y	G	Q	B	A	I	S	E
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A

Desconeixem la configuració de la màquina amb què s'ha xifrat el missatge,

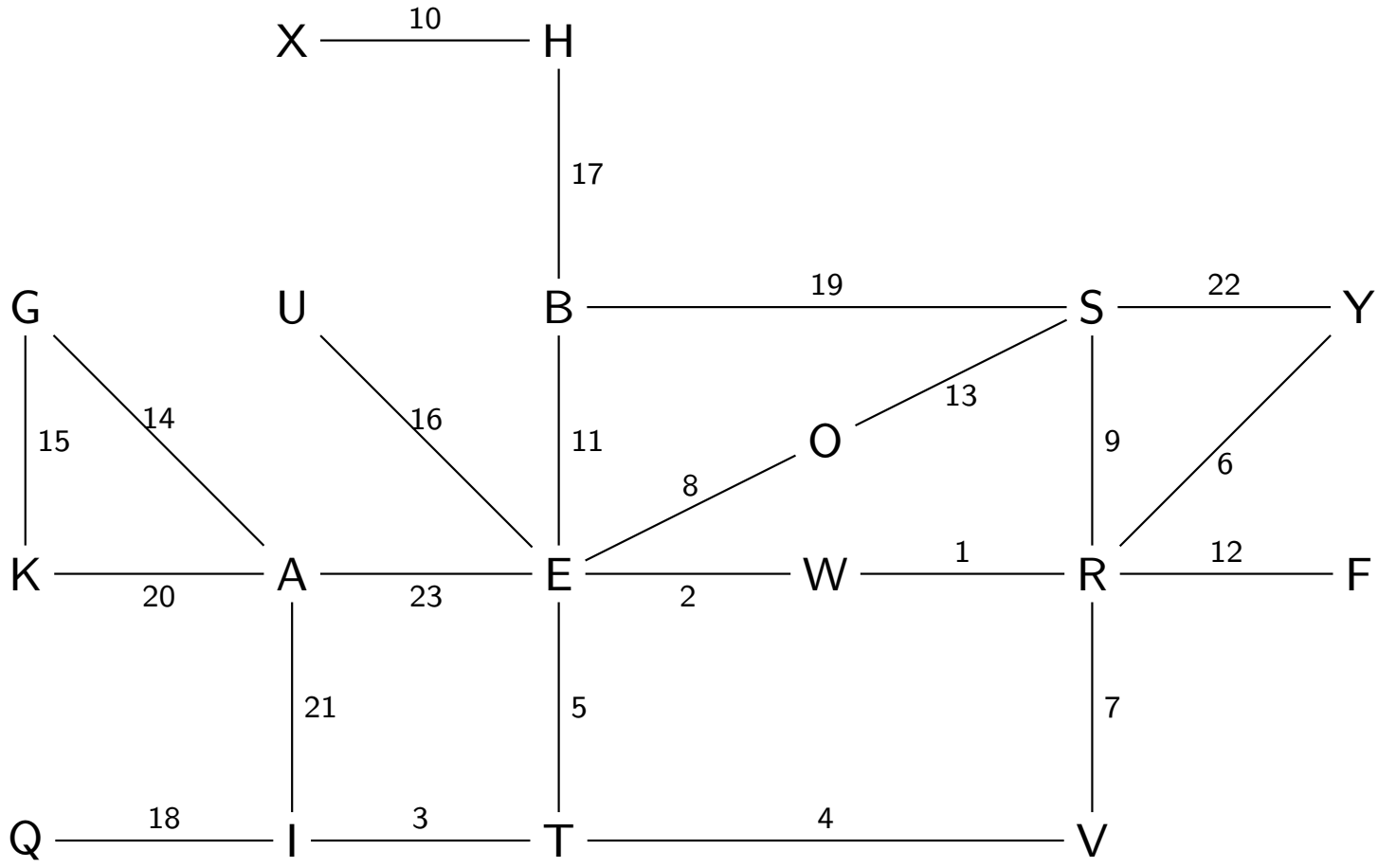
Informació que dona un alineament correcte

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
R	W	I	V	T	Y	R	E	S	X	B	F	O	G	J	Y	G	Q	B	A	I	S	E
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A

Desconeixem la configuració de la màquina amb què s'ha xifrat el missatge,
però sí que les seves lletres s'han xifrat en configuracions consecutives.

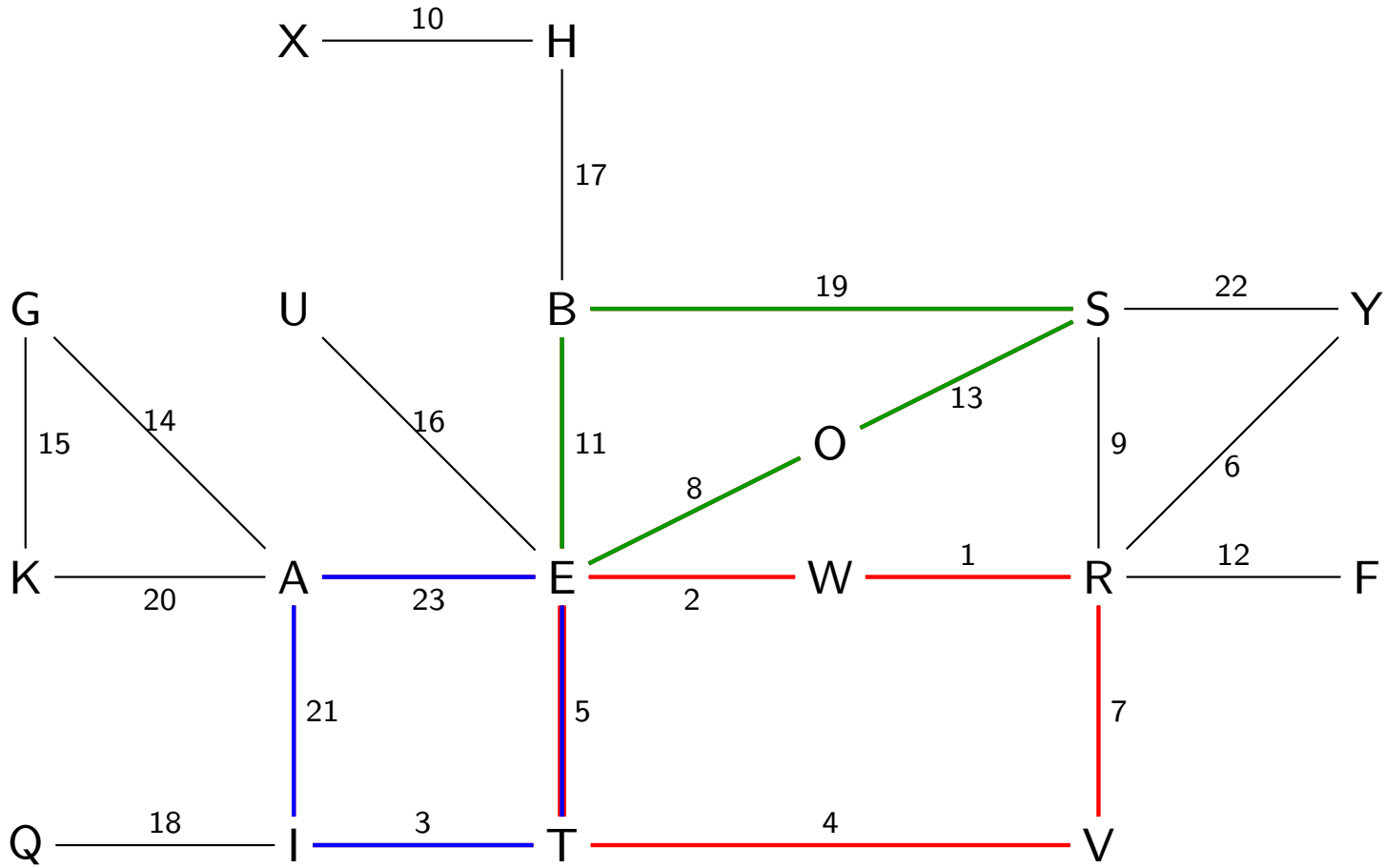
Cicles a partir d'un alineament correcte

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
R	W	I	V	T	Y	R	E	S	X	B	F	O	G	J	Y	G	Q	B	A	I	S	E
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A

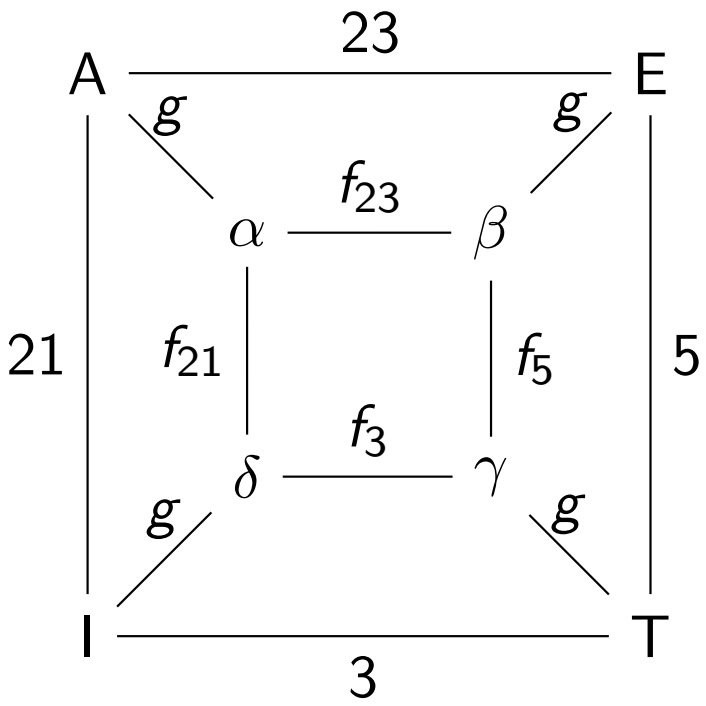


Cicles a partir d'un alineament correcte

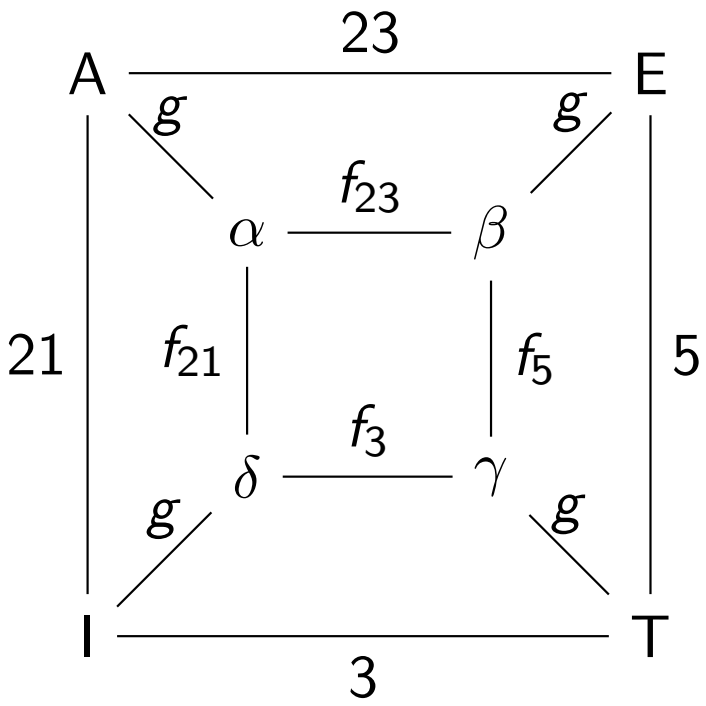
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
R	W	I	V	T	Y	R	E	S	X	B	F	O	G	J	Y	G	Q	B	A	I	S	E
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A



Anàlisi d'un cicle

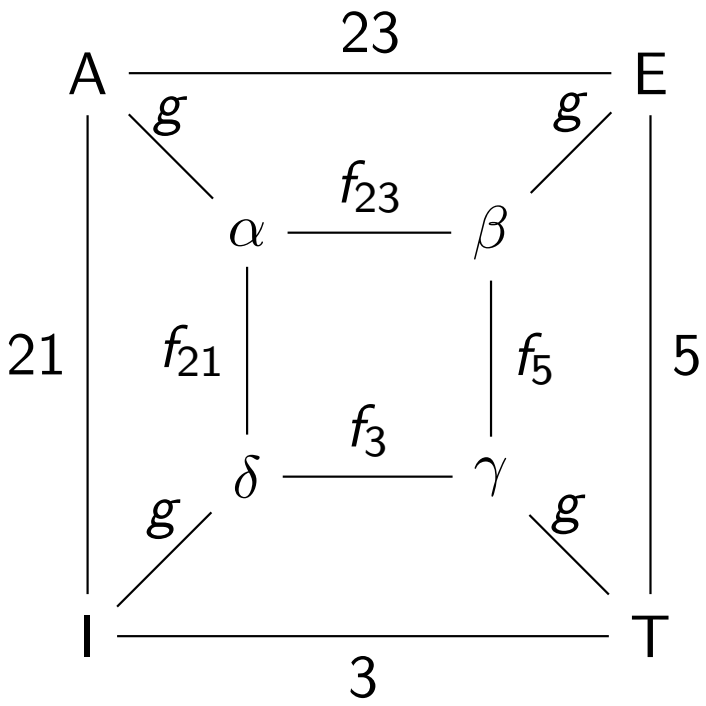


Anàlisi d'un cicle



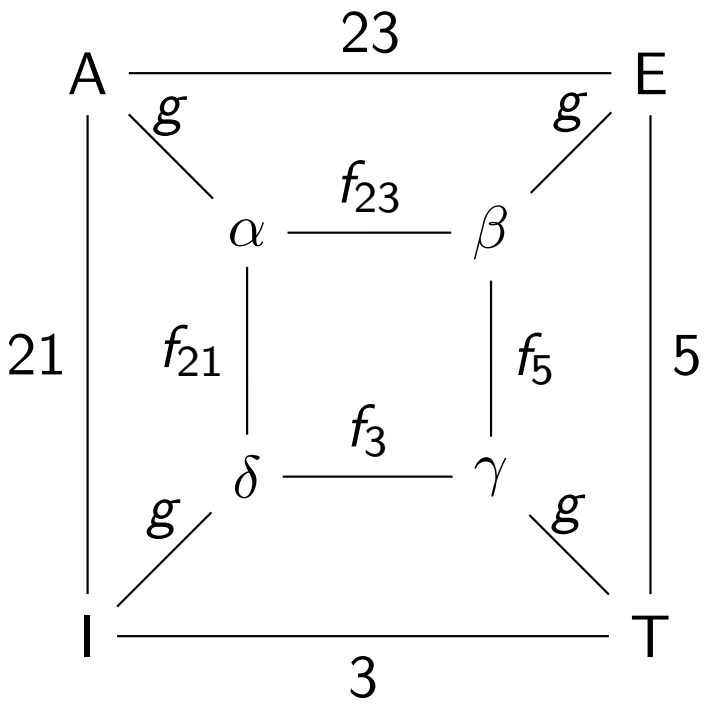
- desconeixem β, γ, δ i α (connectades en el claviller amb E, T, I, A)

Anàlisi d'un cicle



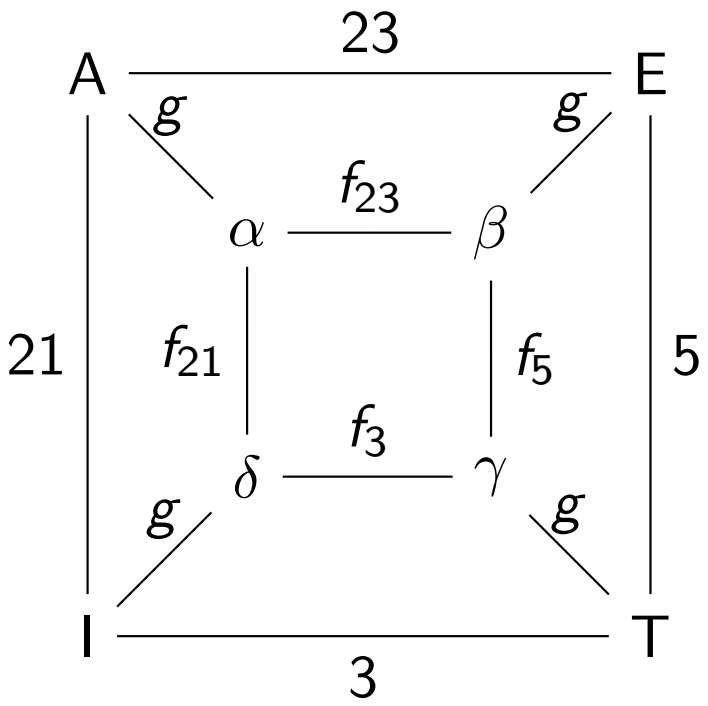
- desconeixem β, γ, δ i α (connectades en el claviller amb E, T, I, A)
- desconeixem f_5, f_3, f_{21}, f_{23} (les funcions de xifratge dels rotors en posicions 5, 3, 21, 23)

Anàlisi d'un cicle



- desconeixem β, γ, δ i α
- desconeixem f_5, f_3, f_{21}, f_{23}
- si trobem β i la posició dels rotors que dona f_5, haurem resolt el problema!

Anàlisi d'un cicle

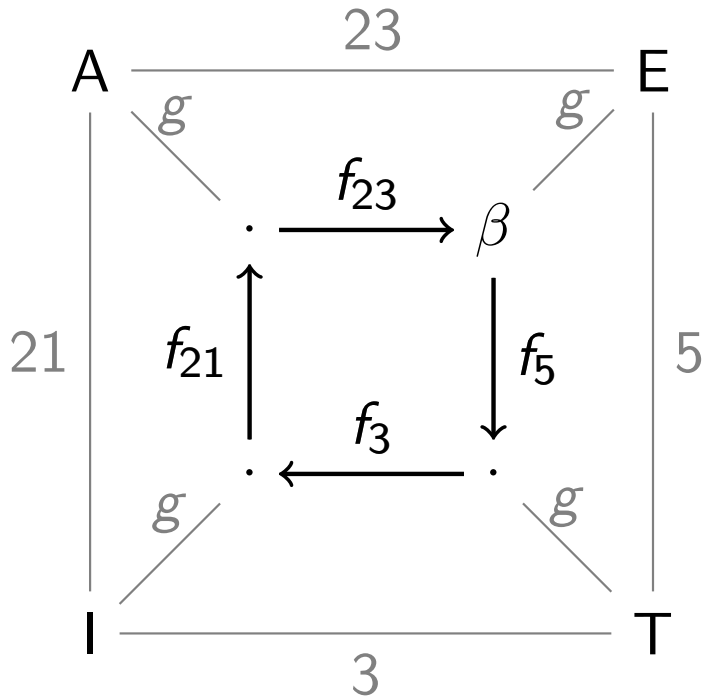


- desconeixem β, γ, δ i α
- desconeixem f_5, f_3, f_{21}, f_{23}
- si trobem β i la posició dels rotors que dona f_5, haurem resolt el problema! (suposant que el rotor del mig no ha girat durant el cicle)

Descartar hipòtesis falses

Idea:

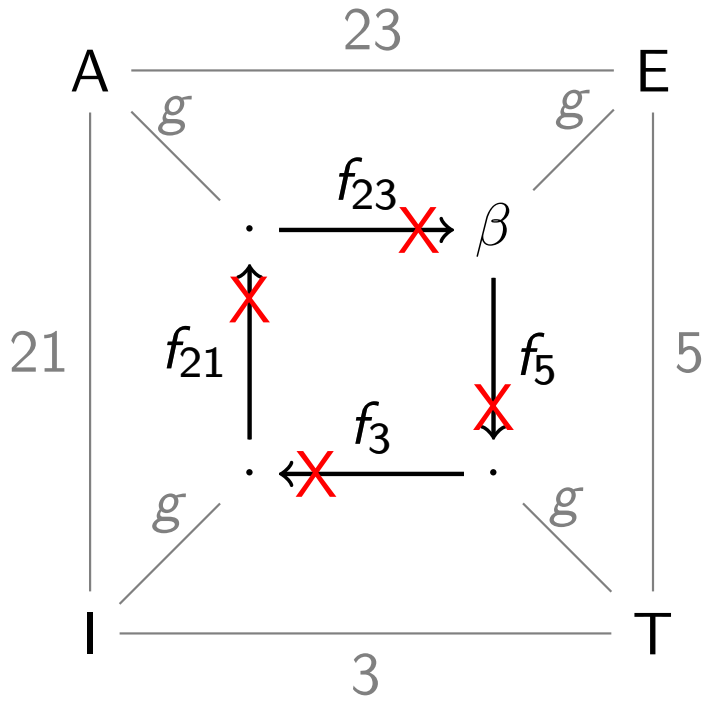
Si les funcions f_5, f_3, f_{21}, f_{23} són correctes, només per a una única lletra β de l'alfabet es tancarà el cicle



Descartar hipòtesis falses

Idea:

Si les funcions f_5, f_3, f_{21}, f_{23} són incorrectes, no es tancarà el cicle per cap lletra β de l'alfabet



Descartar hipòtesis falses

Idea:

Podria ser que per casualitat una elecció incorrecta de f_5, f_3, f_{21}, f_{23} i β tanqués el cicle. Aquest fals positiu es produeix amb probabilitat $\frac{1}{26}$.

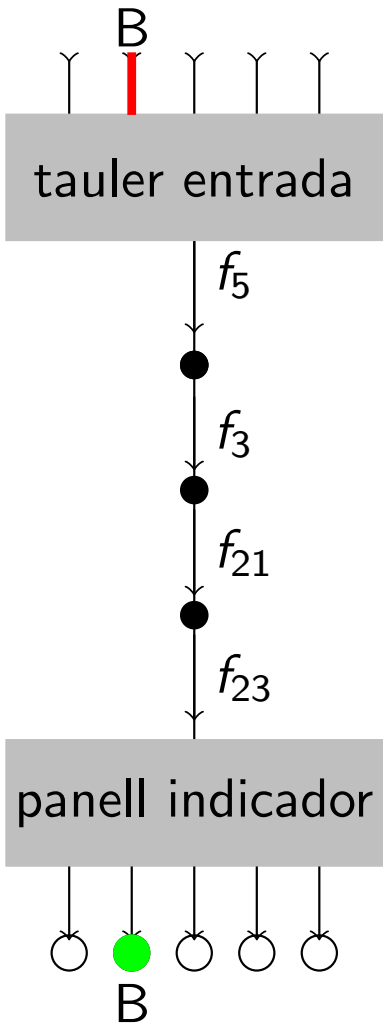
Descartar hipòtesis falses

Idea:

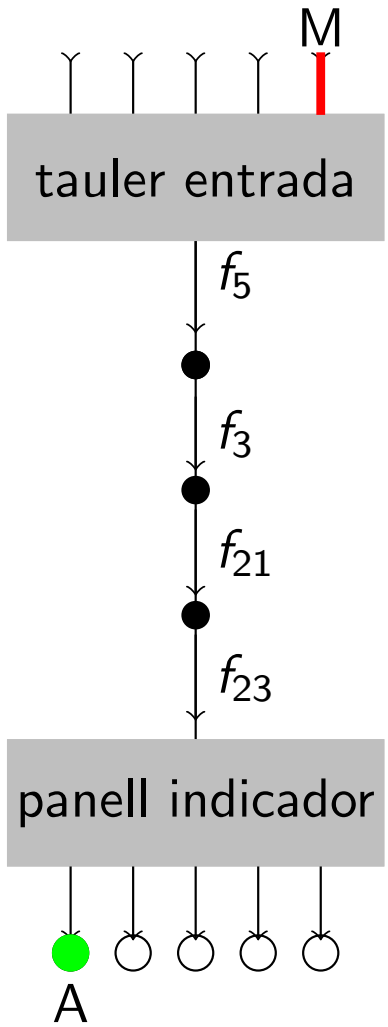
Podria ser que per casualitat una elecció incorrecta de f_5, f_3, f_{21}, f_{23} i β tanqués el cicle. Aquest fals positiu es produeix amb probabilitat $\frac{1}{26}$.

Però si provem alhora tres cicles la probabilitat d'un fals positiu es redueix al $\frac{1}{26} \times \frac{1}{26} \times \frac{1}{26} = 5.6 \times 10^{-5}$

Comprovació electrònica

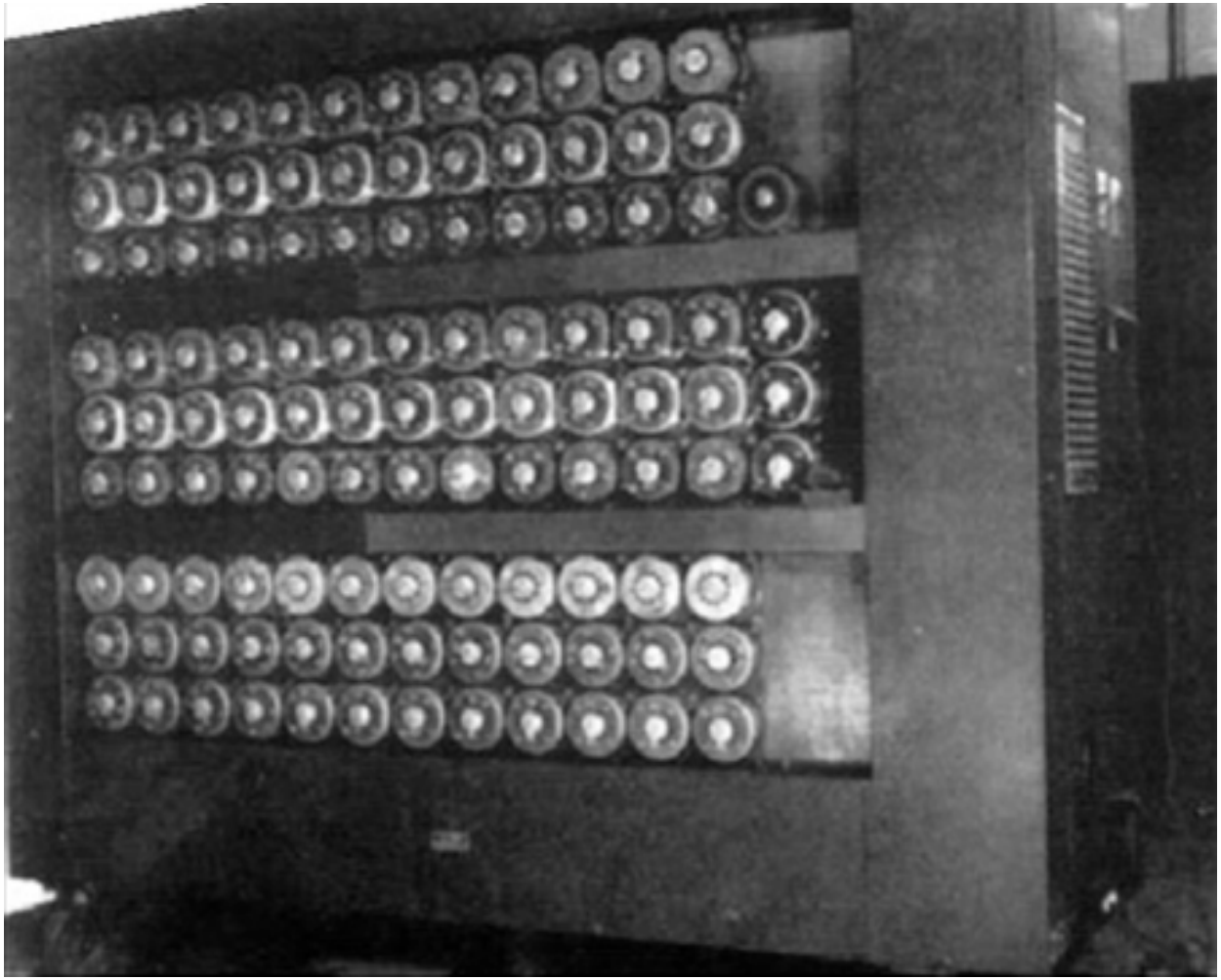


rotors i connexió correcta



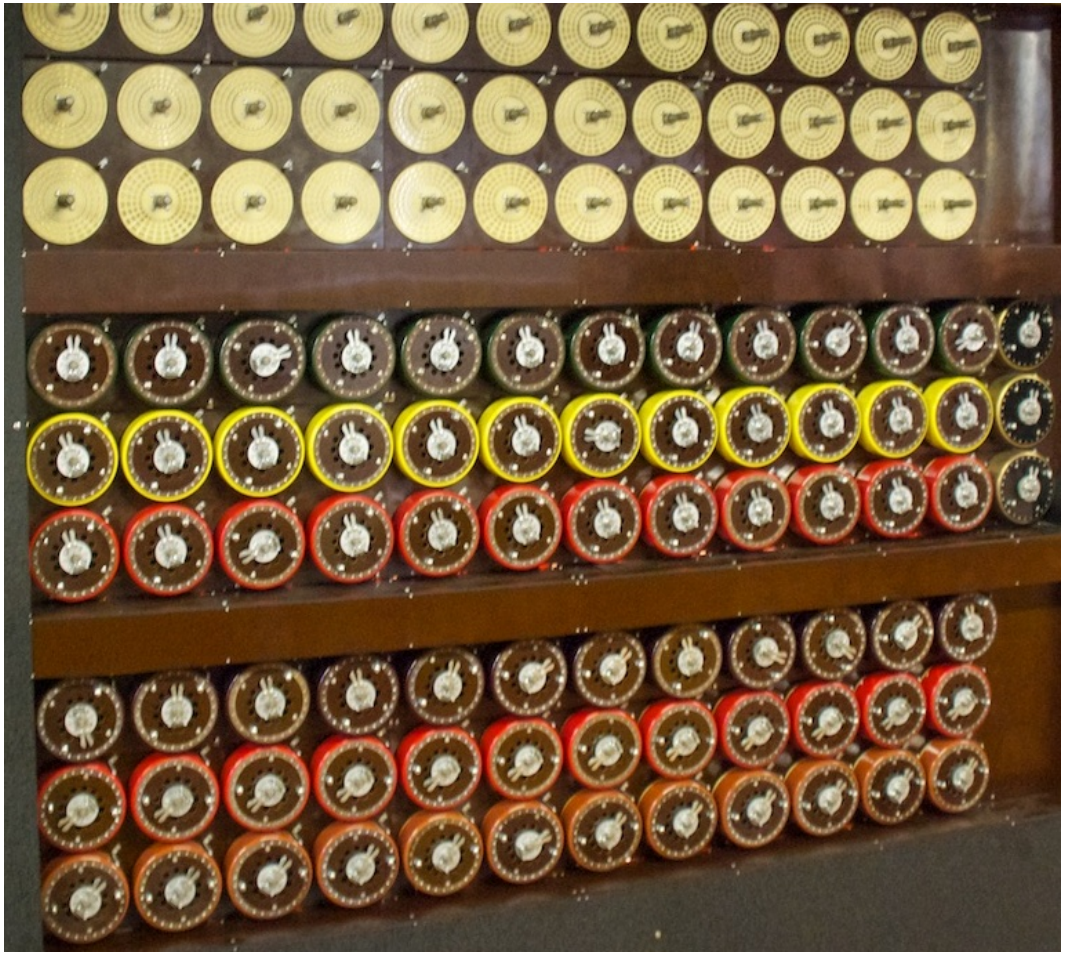
rotors i/o connexió incorrecta

La bomba de Turing, Welchman i Keen



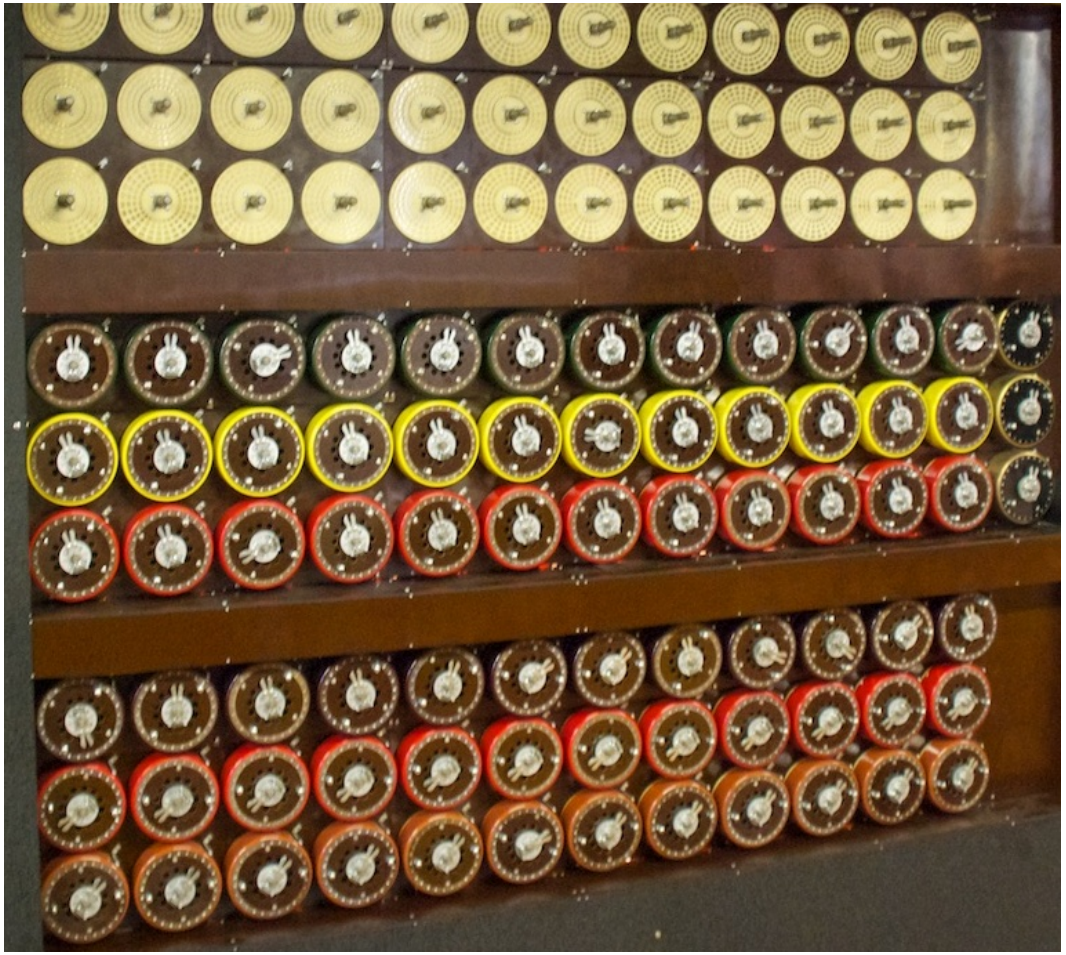
Bomba de tres rotors original

La bomba de Turing, Welchman i Keen

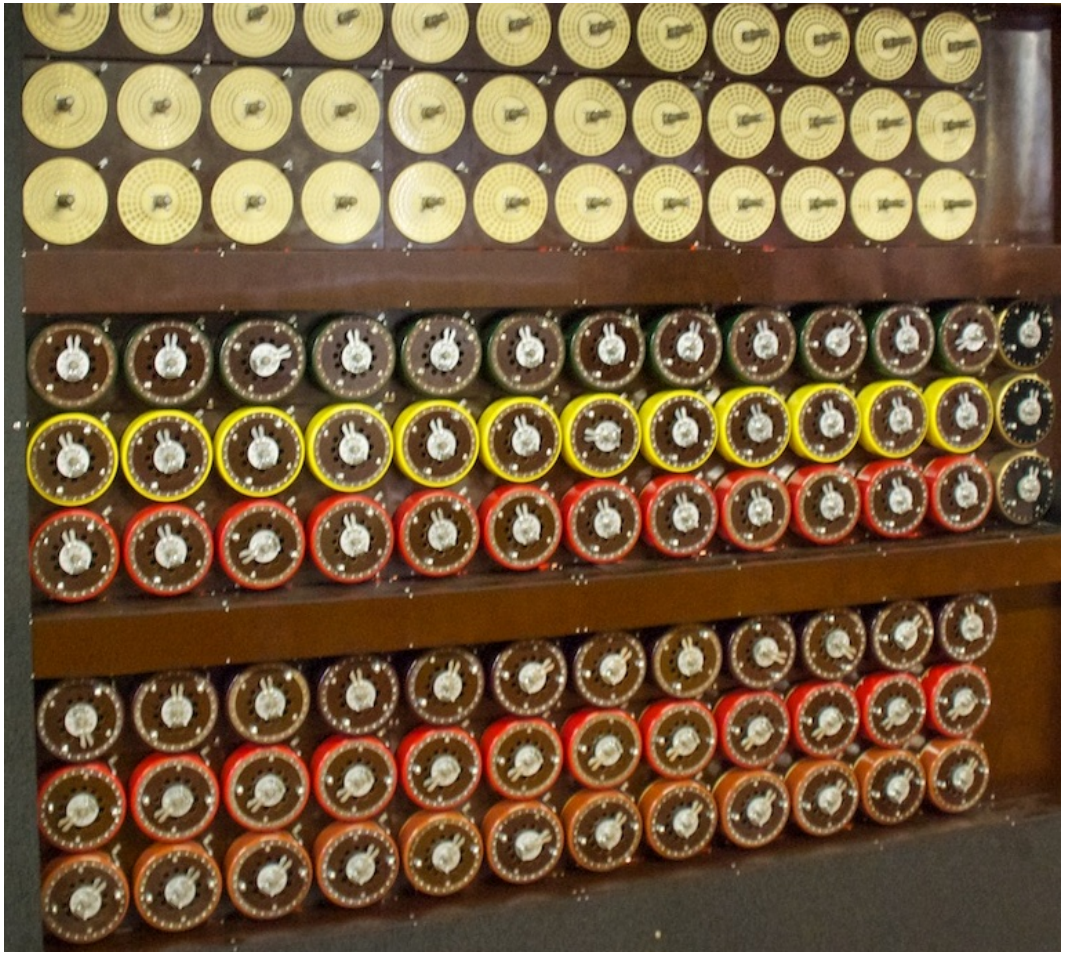


Bomba de tres rotors reconstruïda

La bomba de Turing, Welchman i Keen

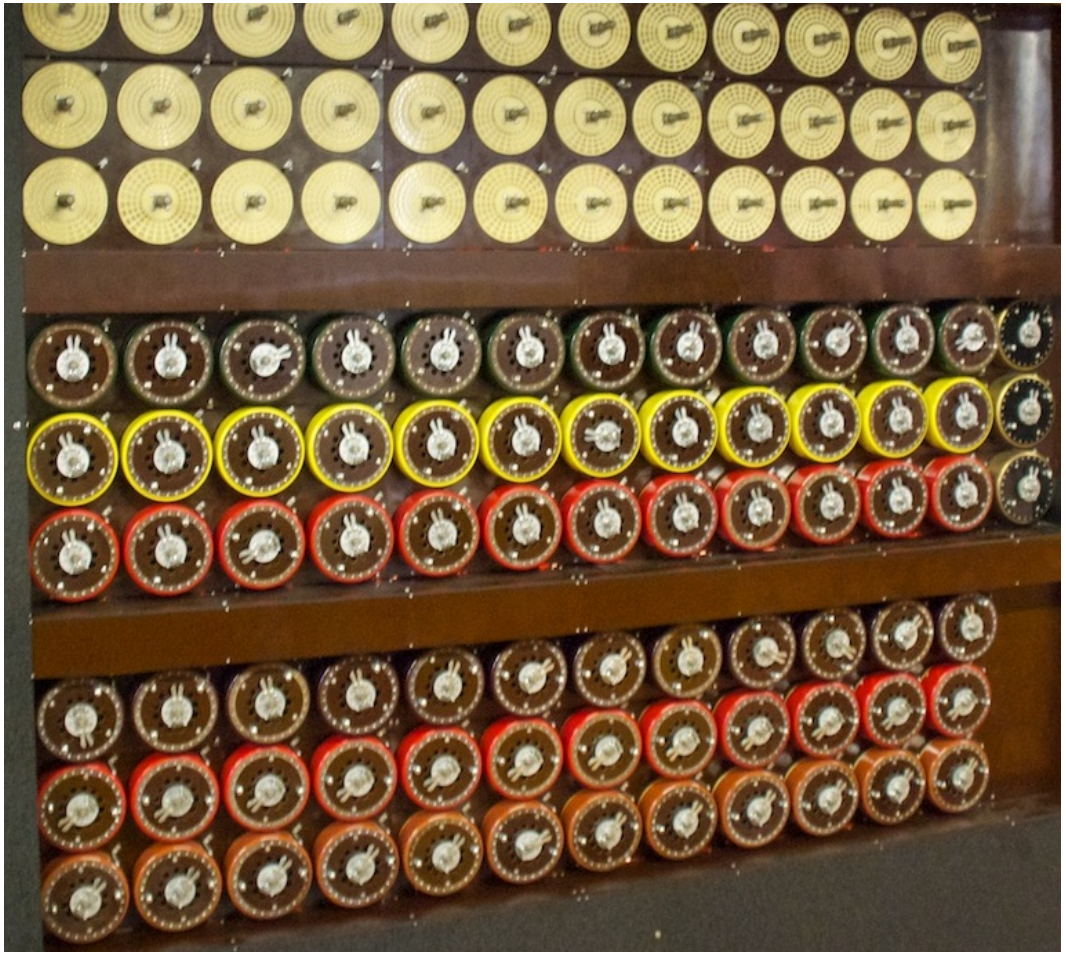


La bomba de Turing, Welchman i Keen



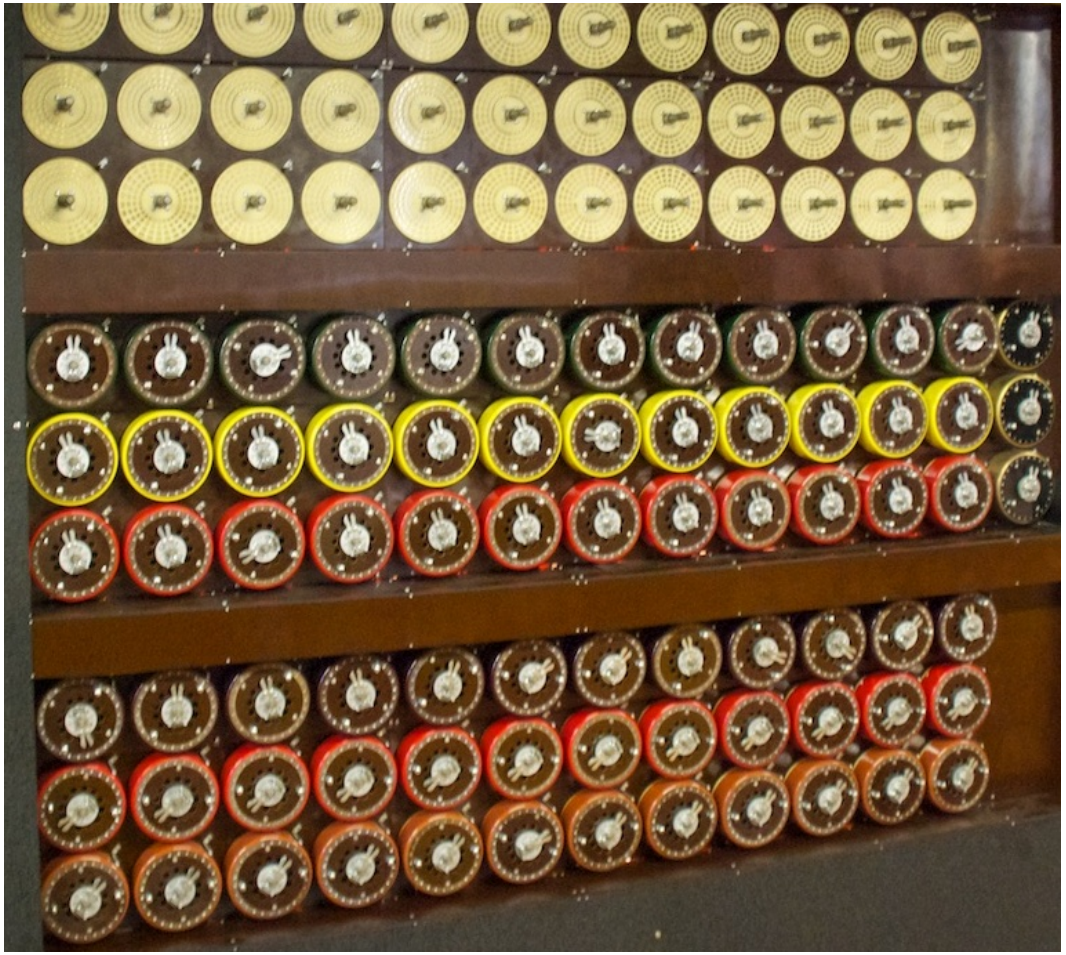
- 3 discs simulen una màquina Enigma.

La bomba de Turing, Welchman i Keen



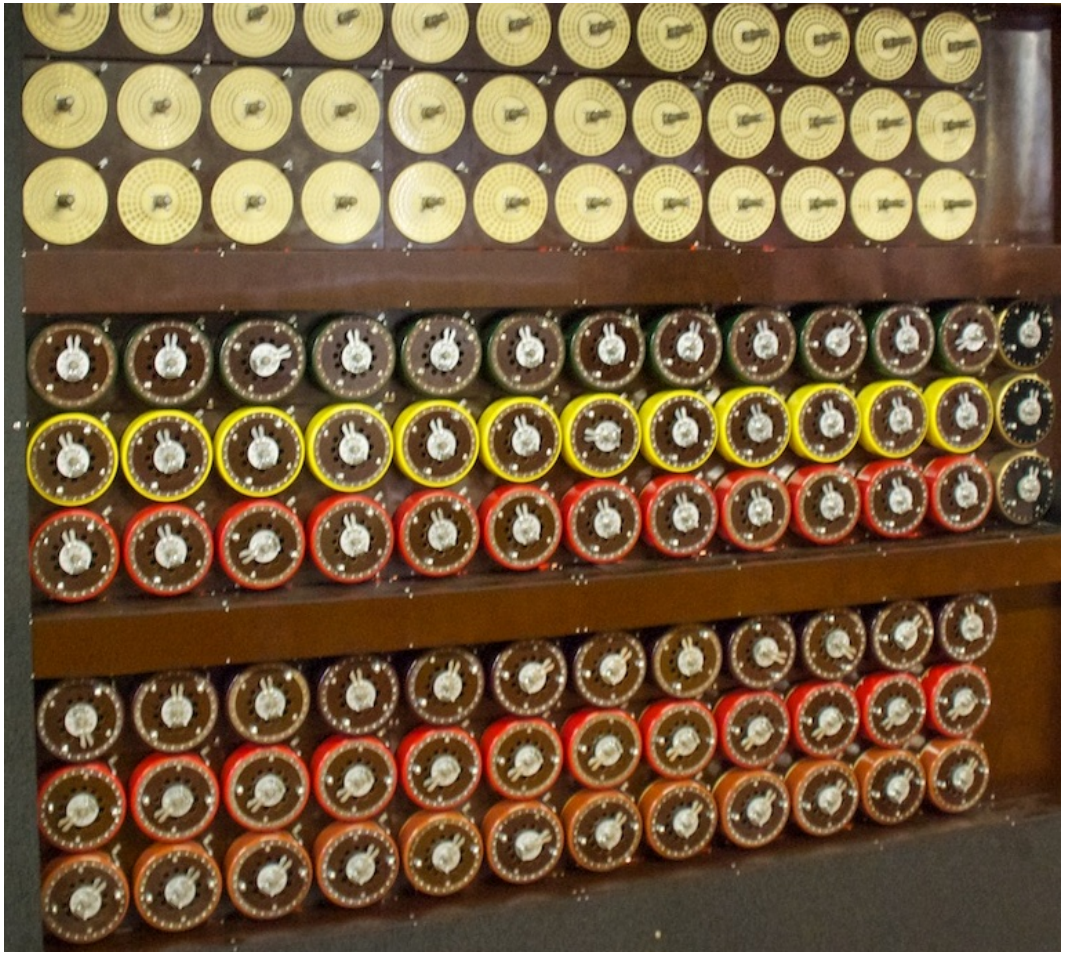
- 3 discs simulen una màquina Enigma.
- 3 files simulen 12 màquines en la posició relativa donada pels cicles

La bomba de Turing, Welchman i Keen



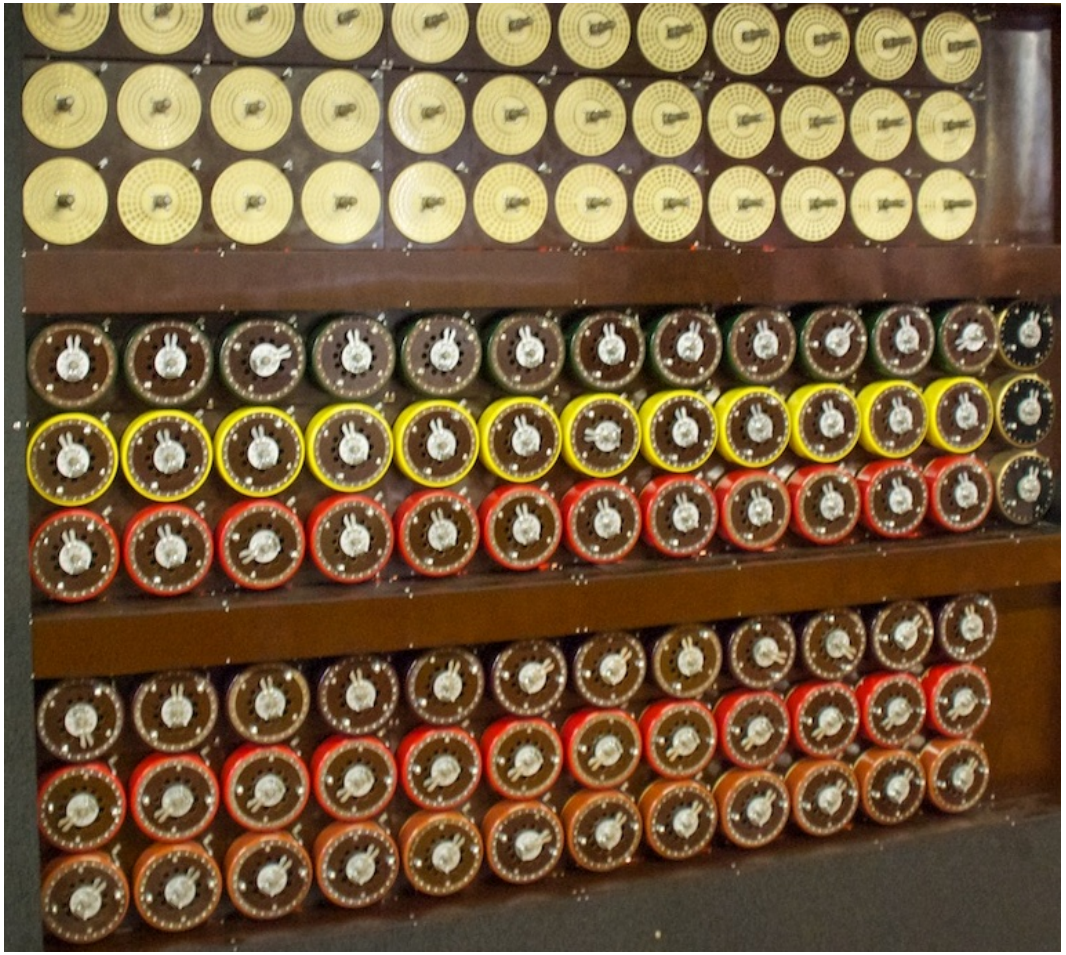
- 3 discs simulen una màquina Enigma.
- 3 files simulen 12 màquines en la posició relativa donada pels cicles
- giren mantenint posició relativa

La bomba de Turing, Welchman i Keen



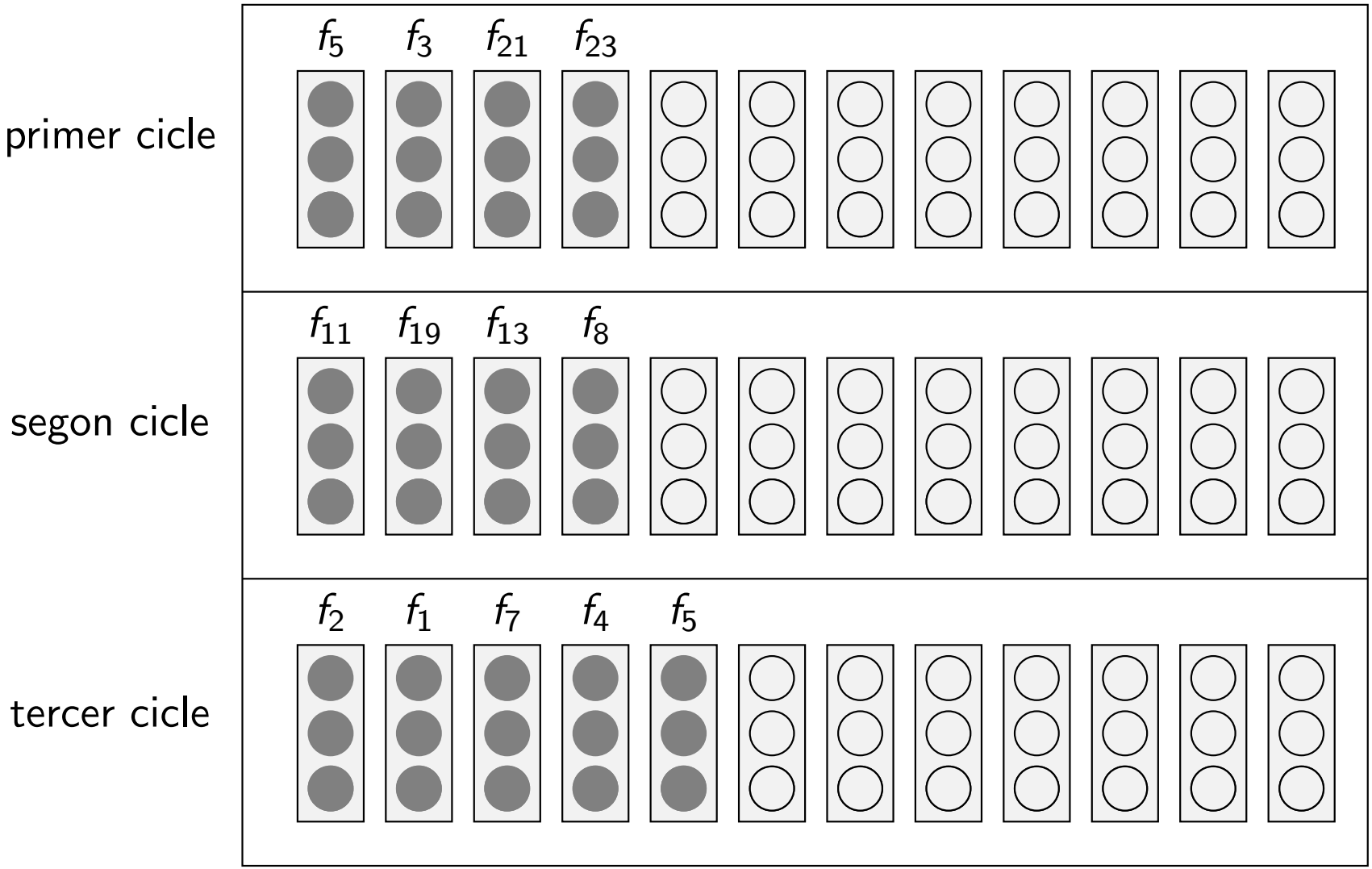
- 3 discs simulen una màquina Enigma.
- 3 files simulen 12 màquines en la posició relativa donada pels cicles
- giren mantenint posició relativa
- 100 voltes per minut (del disc més ràpid)

La bomba de Turing, Welchman i Keen



- 3 discs simulen una màquina Enigma.
- 3 files simulen 12 màquines en la posició relativa donada pels cicles
- giren mantenint posició relativa
- 100 voltes per minut (del disc més ràpid)
- s'aturen quan es detecten els cicles

La bomba preparada fer el test amb tres cicles



Finalment...

- L'Enigma Naval va anar canviant els protocols (quart rotor, indicador del missatge xifrat amb digrames, llibres de codis,...)

Finalment...

- L'Enigma Naval va anar canviant els protocols (quart rotor, indicador del missatge xifrat amb digrames, llibres de codis,...)
- A Bletchley Park van passar mesos sense poder desxifrar missatges dels submarins alemanys.

Finalment...

- L'Enigma Naval va anar canviant els protocols (quart rotor, indicador del missatge xifrat amb digrames, llibres de codis,...)
- A Bletchley Park van passar mesos sense poder desxifrar missatges dels submarins alemanys.
- Només captures de material criptogràfic permetien avançar.

Finalment...

- L'Enigma Naval va anar canviant els protocols (quart rotor, indicador del missatge xifrat amb digrames, llibres de codis,...)
- A Bletchley Park van passar mesos sense poder desxifrar missatges dels submarins alemanys.
- Només captures de material criptogràfic permetien avançar.
- Es calcula que la guerra es va escurçar en dos anys gràcies al seu esforç.

Finalment...

- L'Enigma Naval va anar canviant els protocols (quart rotor, indicador del missatge xifrat amb digrames, llibres de codis,...)
- A Bletchley Park van passar mesos sense poder desxifrar missatges dels submarins alemanys.
- Només captures de material criptogràfic permetien avançar.
- Es calcula que la guerra es va escurçar en dos anys gràcies al seu esforç.
- El desxiframent de l'Engima va ser secret durant la guerra i fins els anys 70.

Finalment...

- L'Enigma Naval va anar canviant els protocols (quart rotor, indicador del missatge xifrat amb digrames, llibres de codis,...)
- A Bletchley Park van passar mesos sense poder desxifrar missatges dels submarins alemanys.
- Només captures de material criptogràfic permetien avançar.
- Es calcula que la guerra es va escurçar en dos anys gràcies al seu esforç.
- El desxiframent de l'Engima va ser secret durant la guerra i fins els anys 70.
- Per trencar Lorenz, el criptosistema utilitzat en les comunicacions entre l'alt comandament a Berlin i els comandaments militars en la zona ocupada, es va construir Collosus, considerat el primer ordinador.