Orígens de la criptografia: Antiga Grècia. s.VII a.C.

Orígens de la criptografia: Antiga Grècia. s.VII a.C.

Figure: Escítala

Orígens de la criptografia: Antiga Grècia. s.VII a.C.

Figure: Escítala

Xifrat per permutació dels símbols

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)

Figure: Mètode Cesar

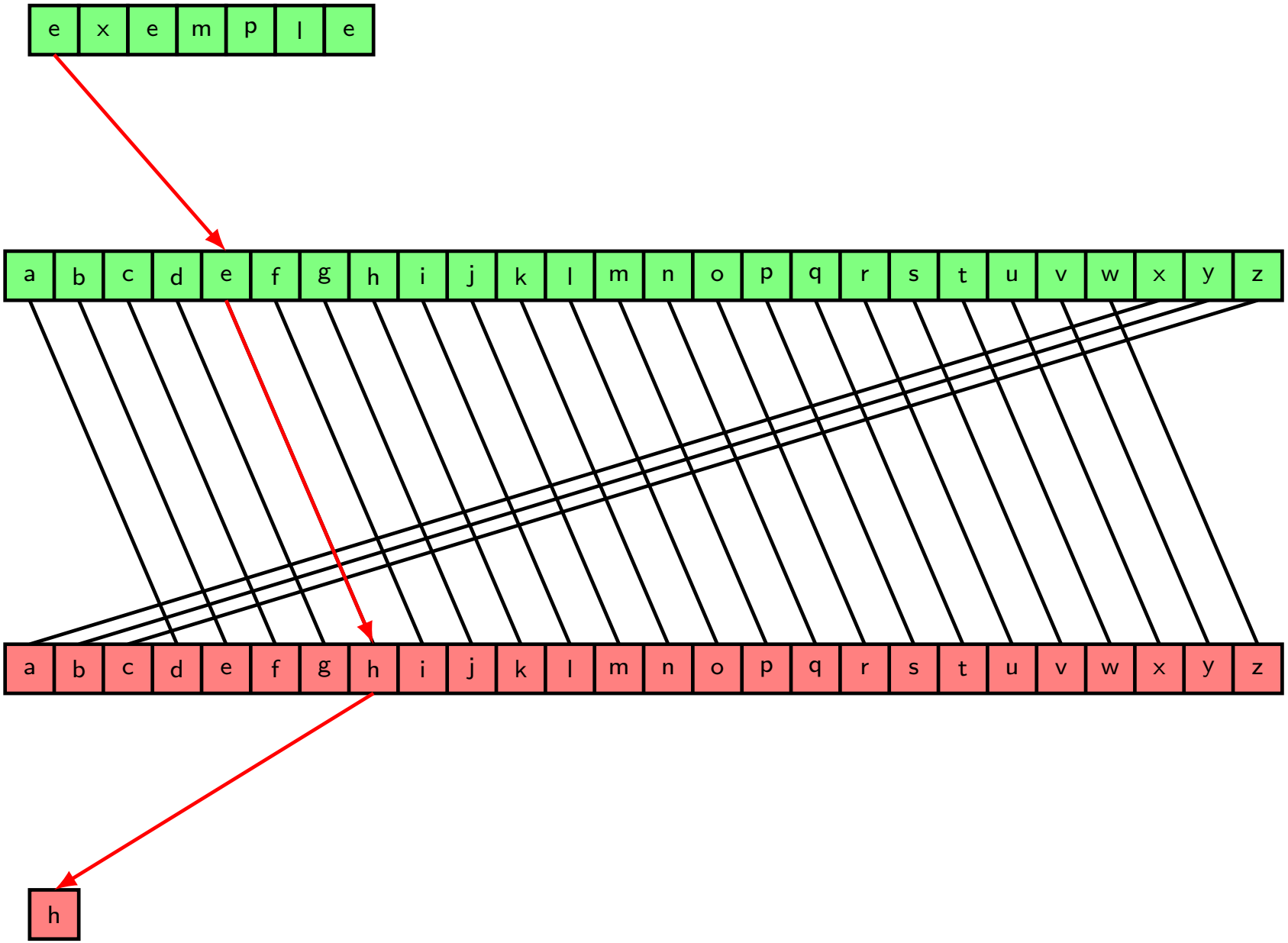
Orígens de la criptografia: Mètode de Cesar (s.I a.C.)

Figure: Mètode Cesar

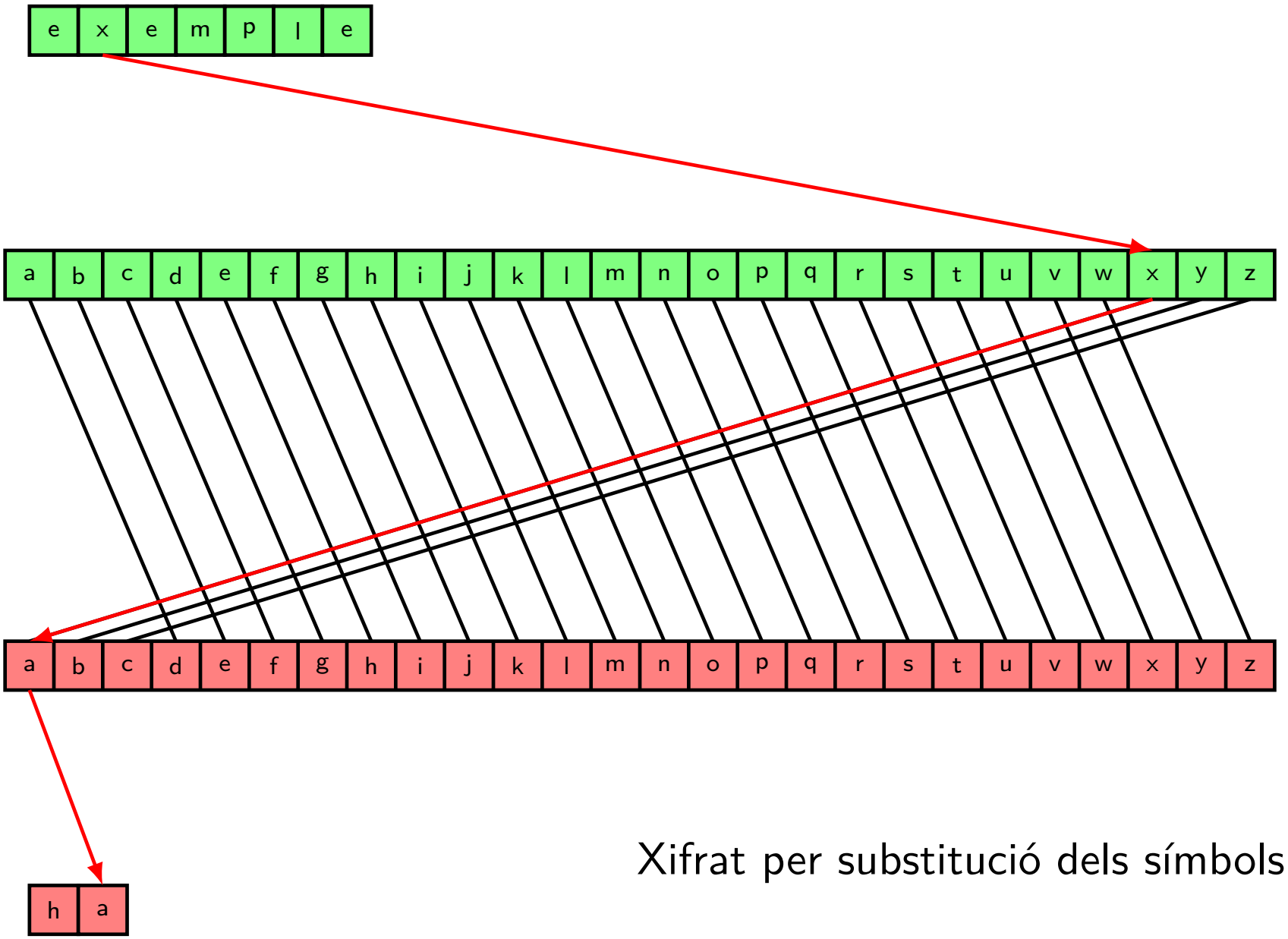
Xifrat per substitució dels símbols

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)

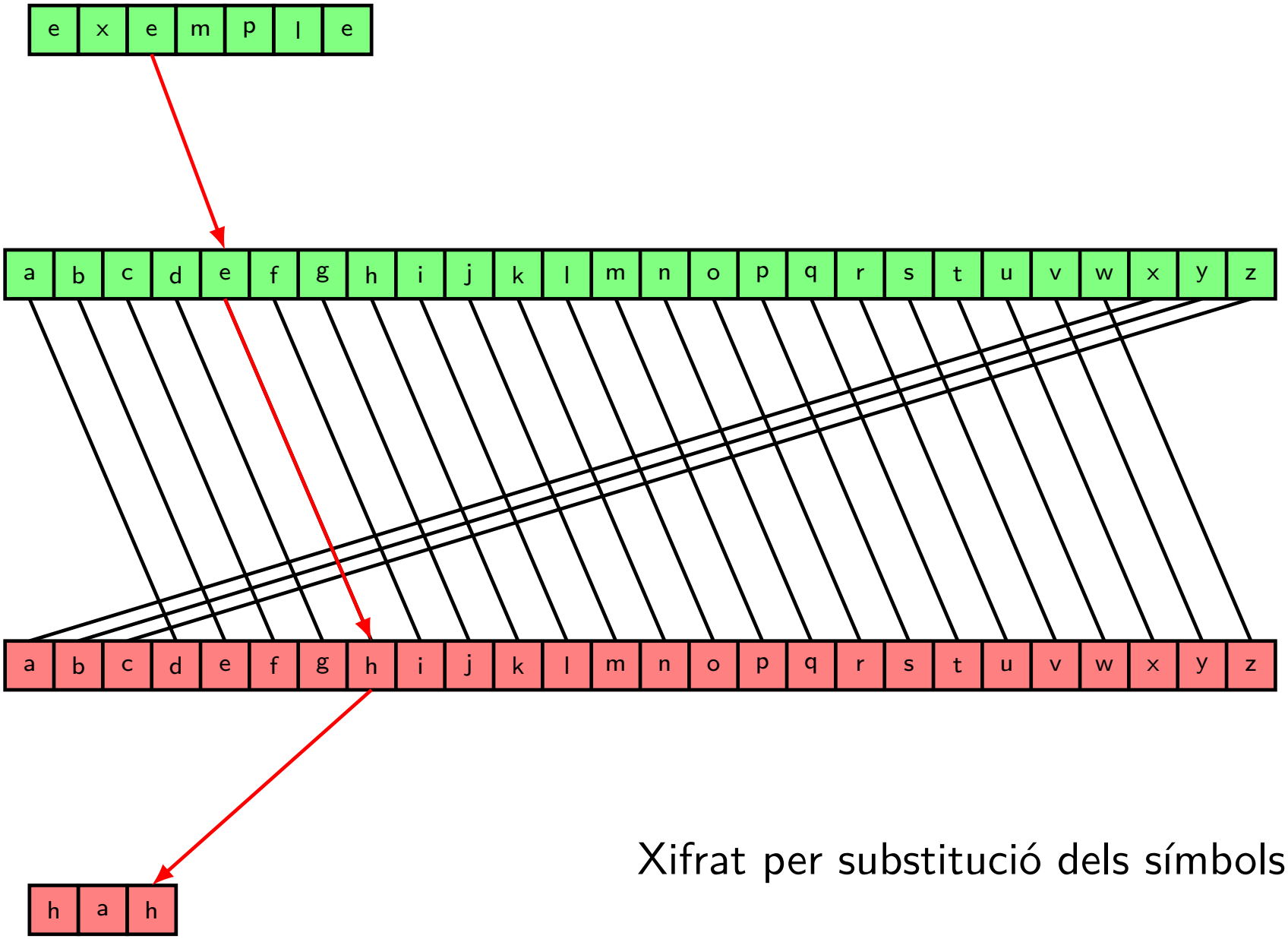


Orígens de la criptografia: Mètode de Cesar (s.I a.C.)



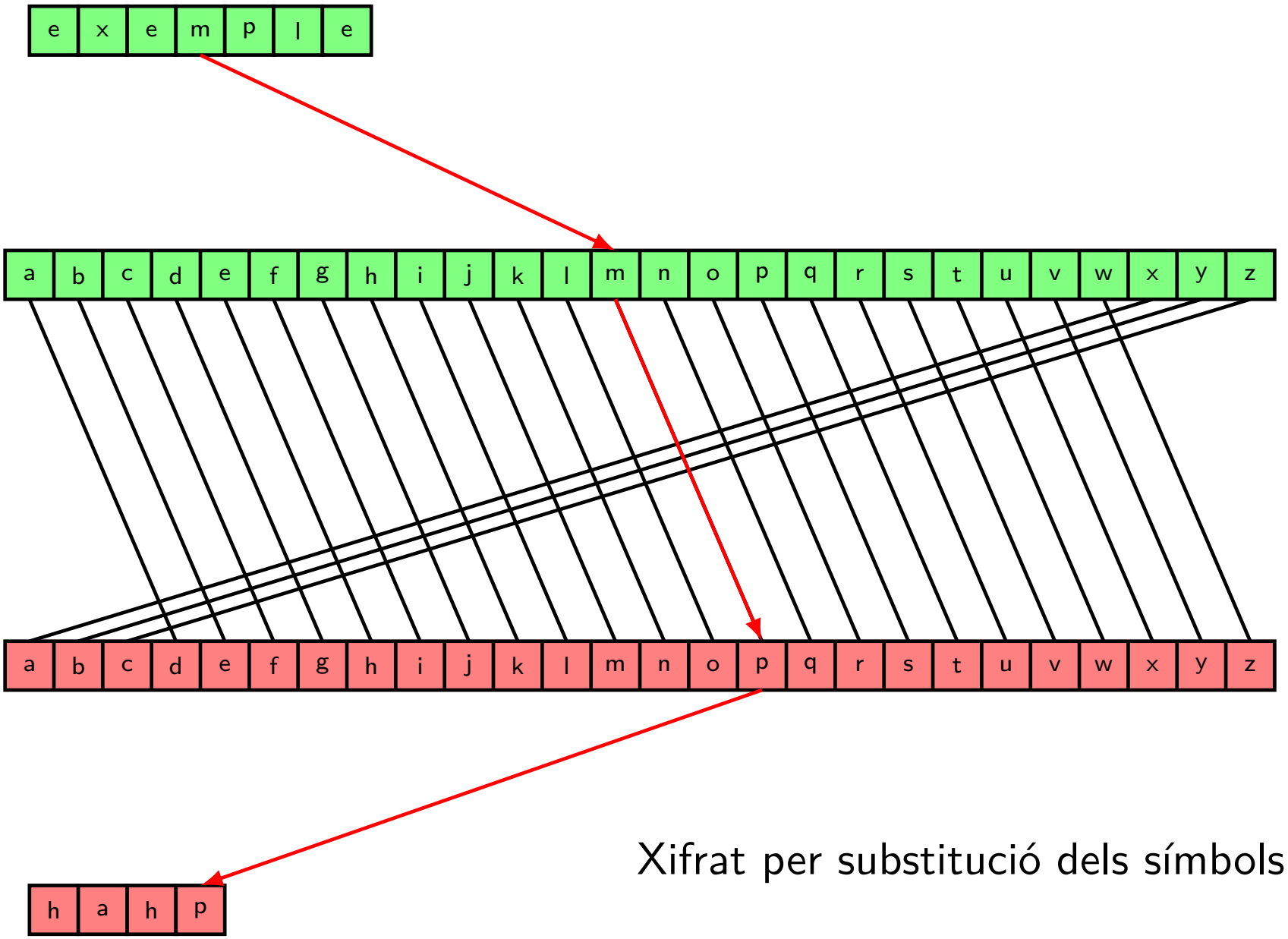
Xifrat per substitució dels símbols

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)



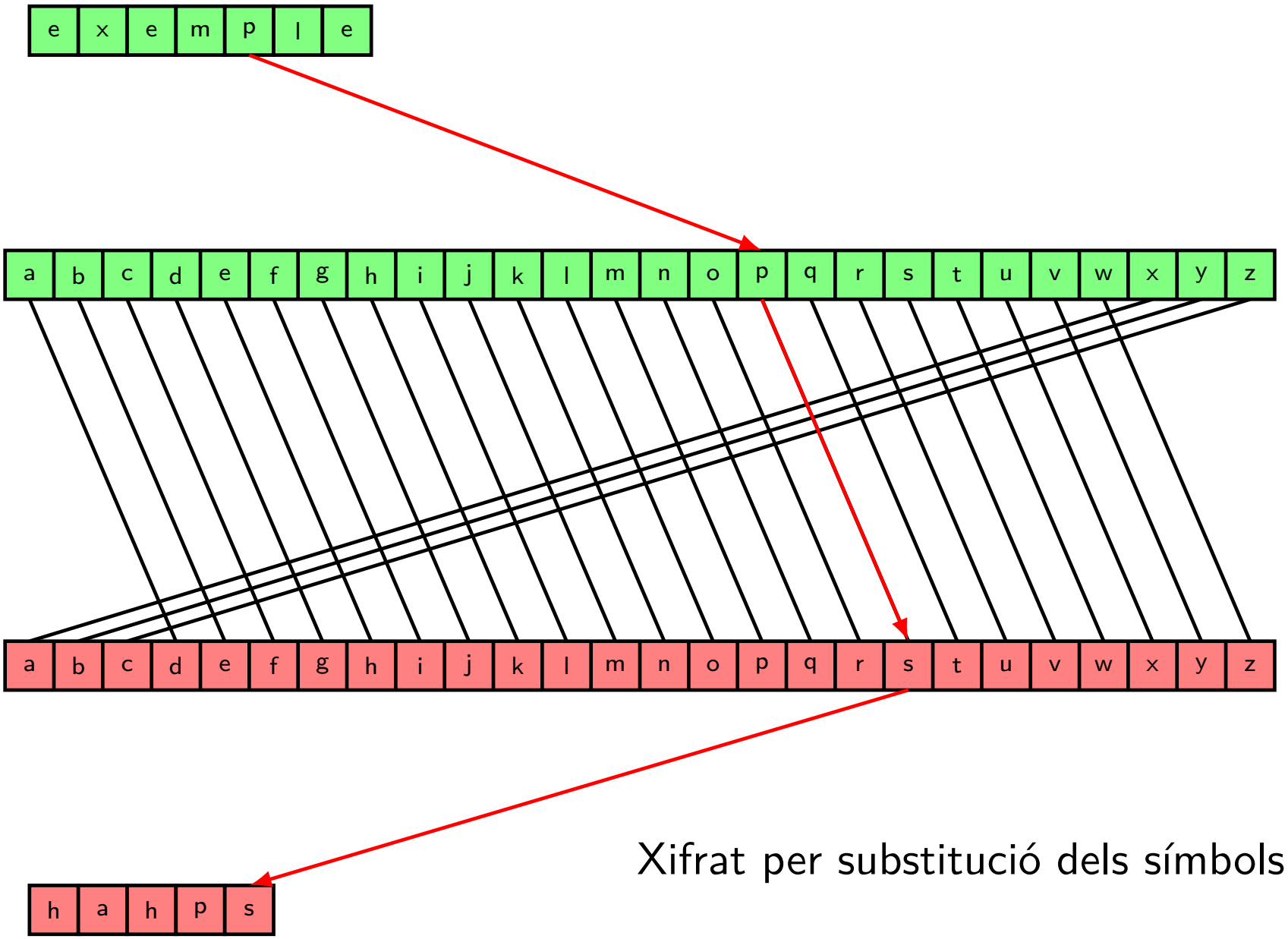
Xifrat per substitució dels símbols

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)



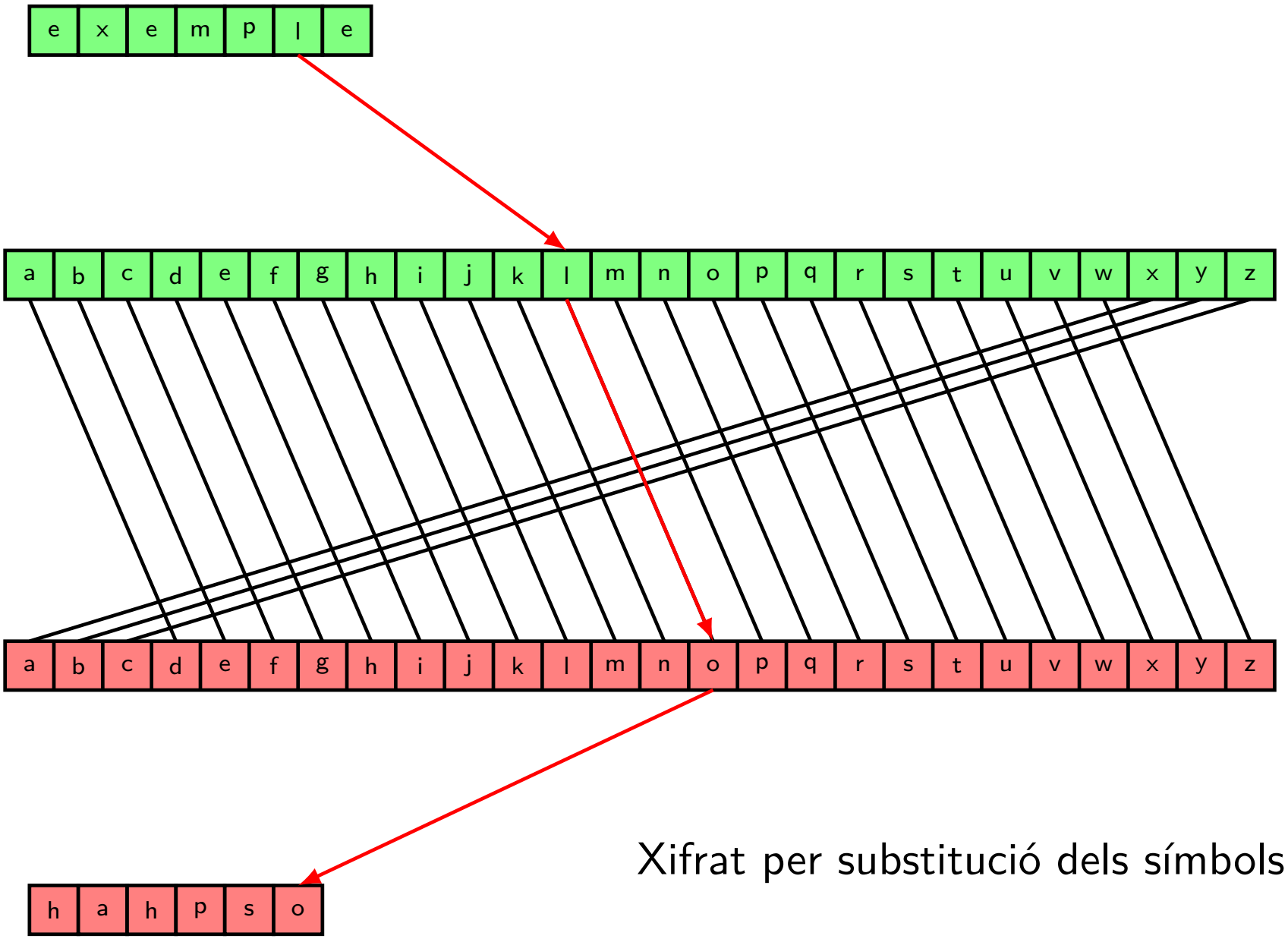
Xifrat per substitució dels símbols

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)



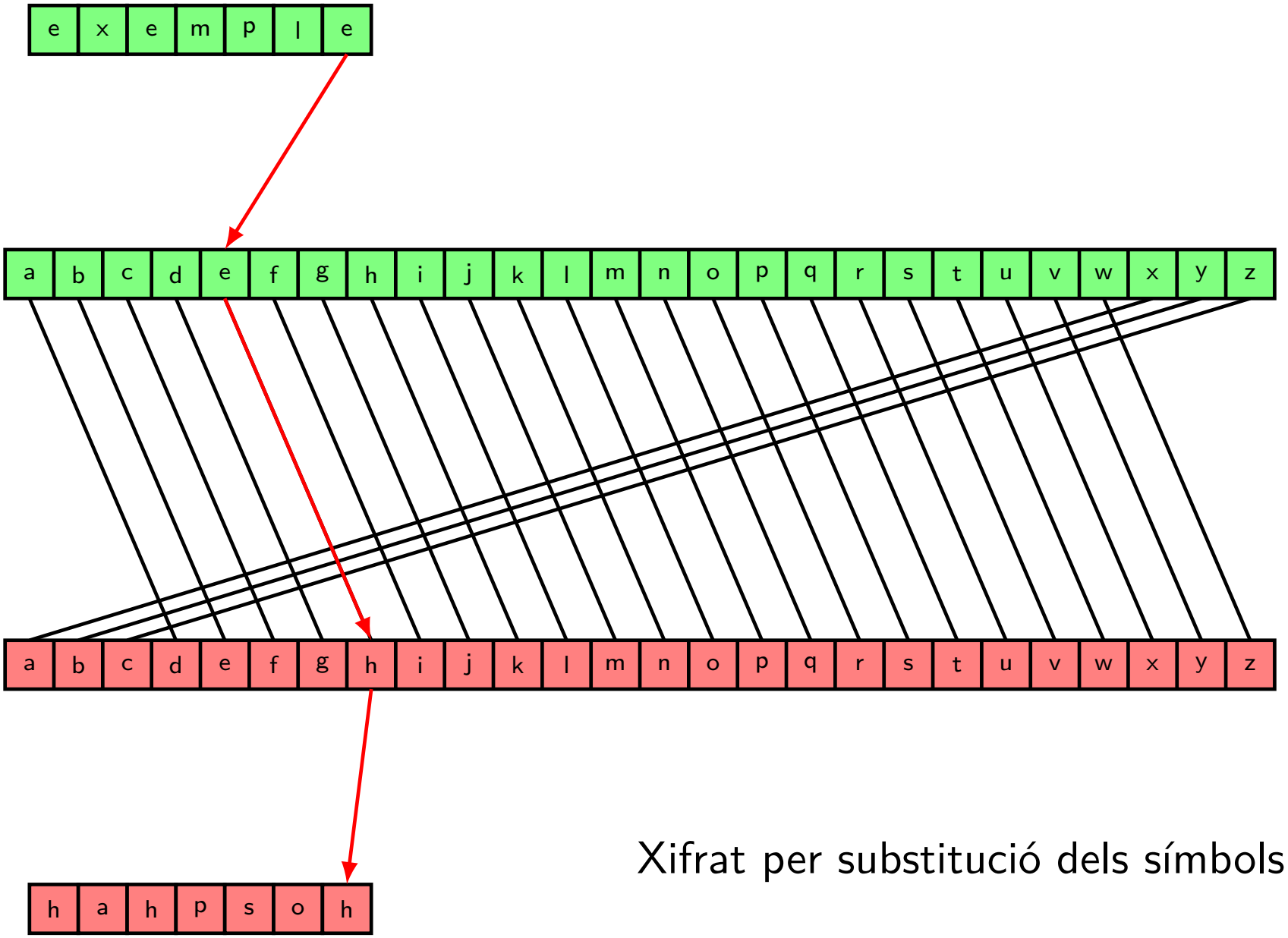
Xifrat per substitució dels símbols

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)



Xifrat per substitució dels símbols

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)

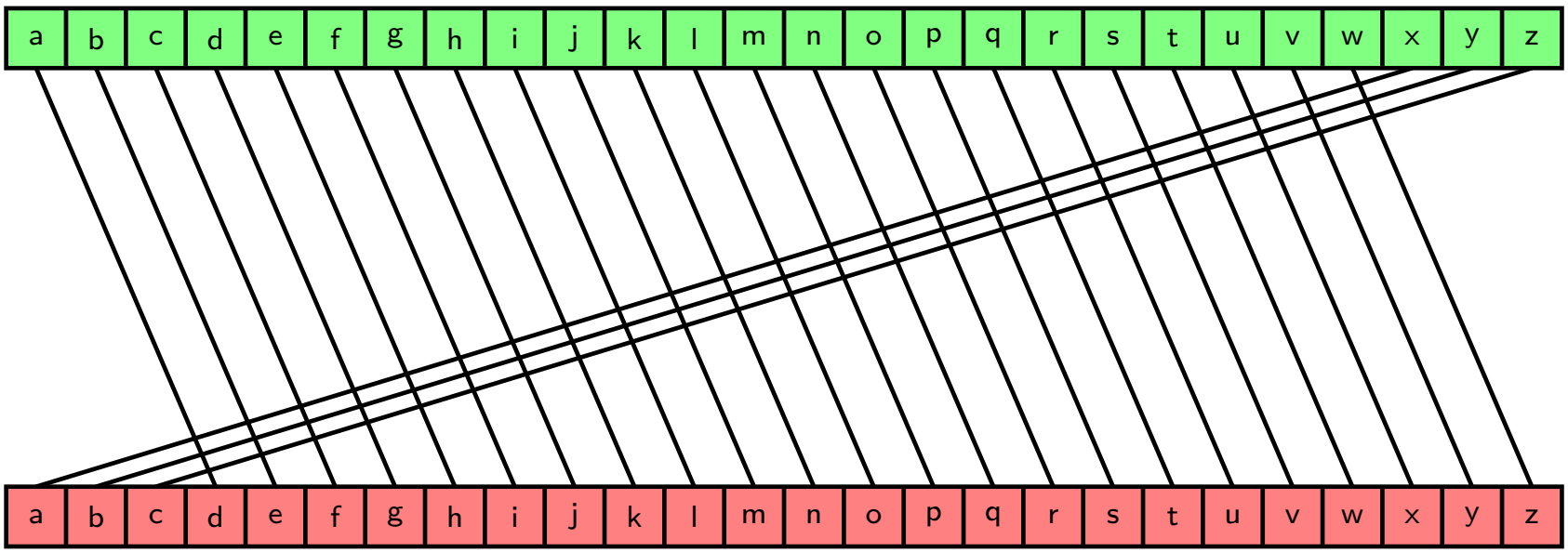


Xifrat per substitució dels símbols

Orígens de la criptografia: Mètode de Cesar (s.I a.C.)

e	x	e	m	p	l	e

$x \mapsto x + 3 \bmod n$ amb $x \in \{0, \ldots, n-1\}$



Xifrat per substitució dels símbols

h	a	h	p	s	o	h

Criptografia clàssica: Algunes consideracions

Criptografia clàssica: Algunes consideracions

- Mètodes clàssics:
  - permutacions.
  - substitucions.

Criptografia clàssica: Algunes consideracions

- Mètodes clàssics:
  - permutacions.
  - substitucions.
- Robustesa condicional

Criptografia clàssica: Algunes consideracions

- Mètodes clàssics:
  - permutacions.
  - substitucions.
- Robustesa condicional
- Robustesa d'un mètode de xifrat

Criptografia clàssica: Algunes consideracions

- Mètodes clàssics:
  - permutacions.
  - substitucions.
- Robustesa condicional
- Robustesa d'un mètode de xifrat
  - Basada en el secret del mètode.
  - Basada en el secret de la clau.

Mètodes de permutació. Exemple

Texte que es vol xifrar:
"AIXO ES UN SISTEMA CRIPTOGRAFIC BASAT EN PERMUTACIO DELS SIMBOLS"

Mètodes de permutació. Exemple

Texte que es vol xifrar:
"AIXO ES UN SISTEMA CRIPTOGRAFIC BASAT EN PERMUTACIO DELS SIMBOLS"

A	I	X	O	E	S	U	N	S	I	S
T	E	M	A	C	R	I	P	T	O	G
R	A	F	I	C	B	A	S	A	T	E
N	P	E	R	M	U	T	A	C	I	O
D	E	L	S	S	I	M	B	O	L	S

Mètodes de permutació. Exemple

Texte que es vol xifrar:
"AIXO ES UN SISTEMA CRIPTOGRAFIC BASAT EN PERMUTACIO DELS SIMBOLS"

A	I	X	O	E	S	U	N	S	I	S
T	E	M	A	C	R	I	P	T	O	G
R	A	F	I	C	B	A	S	A	T	E
N	P	E	R	M	U	T	A	C	I	O
D	E	L	S	S	I	M	B	O	L	S

Texte xifrat:
"ATRNDIEAPEXMFELOAIRSECCMS SRBUIUIATMNPSABSTACOIOTILSGEOS"

Mètodes de permutació. Exemple

Texte que es vol xifrar:
"AIXO ES UN SISTEMA CRIPTOGRAFIC BASAT EN PERMUTACIO DELS SIMBOLS"

A	I	X	O	E	S	U	N	S	I	S
T	E	M	A	C	R	I	P	T	O	G
R	A	F	I	C	B	A	S	A	T	E
N	P	E	R	M	U	T	A	C	I	O
D	E	L	S	S	I	M	B	O	L	S

Texte xifrat:
"ATRNDIEAPEXMFELOAIRSECCMS SRBUIUIATMNPSABSTACOIOTILSGEOS"

La clau és la llargada de la línia.

Mètodes de permutació. Exemple millorat

Texte que es vol xifrar:
"AIXO ES UN SISTEMA CRIPTOGRAFIC BASAT EN PERMUTACIO DELS SIMBOLS"

clau: "CITRONEUMAS"

Mètodes de permutació. Exemple millorat

Texte que es vol xifrar:
"AIXO ES UN SISTEMA CRIPTOGRAFIC BASAT EN PERMUTACIO DELS SIMBOLS"

clau: "CITRONEUMAS"

C I T R O N E U M A S

Mètodes de permutació. Exemple millorat

Texte que es vol xifrar:
"AIXO ES UN SISTEMA CRIPTOGRAFIC BASAT EN PERMUTACIO DELS SIMBOLS"

clau: "CITRONEUMAS"

C	I	T	R	O	N	E	U	M	A	S
2	4	10	8	7	6	3	11	5	1	9

Mètodes de permutació. Exemple millorat

Texte que es vol xifrar:
"AIXO ES UN SISTEMA CRIPTOGRAFIC BASAT EN PERMUTACIO DELS SIMBOLS"

clau: "CITRONEUMAS"

C	I	T	R	O	N	E	U	M	A	S
2	4	10	8	7	6	3	11	5	1	9
A	I	X	O	E	S	U	N	S	I	S
T	E	M	A	C	R	I	P	T	O	G
R	A	F	I	C	B	A	S	A	T	E
N	P	E	R	M	U	T	A	C	I	O
D	E	L	S	S	I	M	B	O	L	S

Mètodes de permutació. Exemple millorat

Texte que es vol xifrar:
"AIXO ES UN SISTEMA CRIPTOGRAFIC BASAT EN PERMUTACIO DELS SIMBOLS"

clau: "CITRONEUMAS"

C	I	T	R	O	N	E	U	M	A	S
2	4	10	8	7	6	3	11	5	1	9
A	I	X	O	E	S	U	N	S	I	S
T	E	M	A	C	R	I	P	T	O	G
R	A	F	I	C	B	A	S	A	T	E
N	P	E	R	M	U	T	A	C	I	O
D	E	L	S	S	I	M	B	O	L	S

Texte xifrat:
"IOTIL ATRND UIATM IEAPE STACO SRBUI ECCMS OAIRS SGEOS XMFEL NPSAB"

Mètodes de substitució: César amb clau

Mètodes de substitució: César amb clau

- Introducció de clau en el mètode de César: La clau es el desplaçament que es fa servir.

$$x \to x + k \mod n, \quad k \in \{1..n-1\}$$

Mètodes de substitució: César amb clau

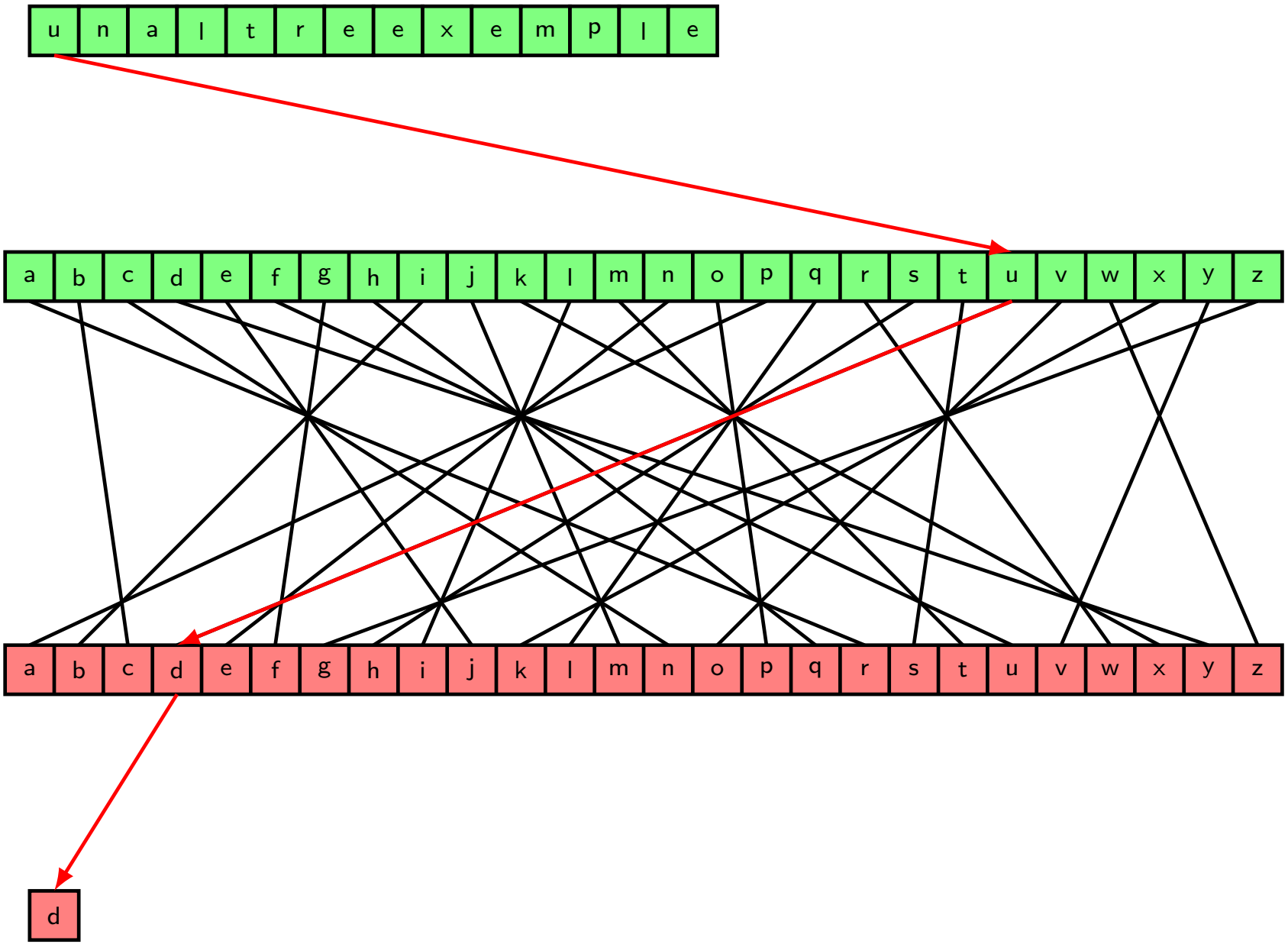
- Introducció de clau en el mètode de César: La clau es el desplaçament que es fa servir.

$$x \to x + k \mod n, \quad k \in \{1..n-1\}$$

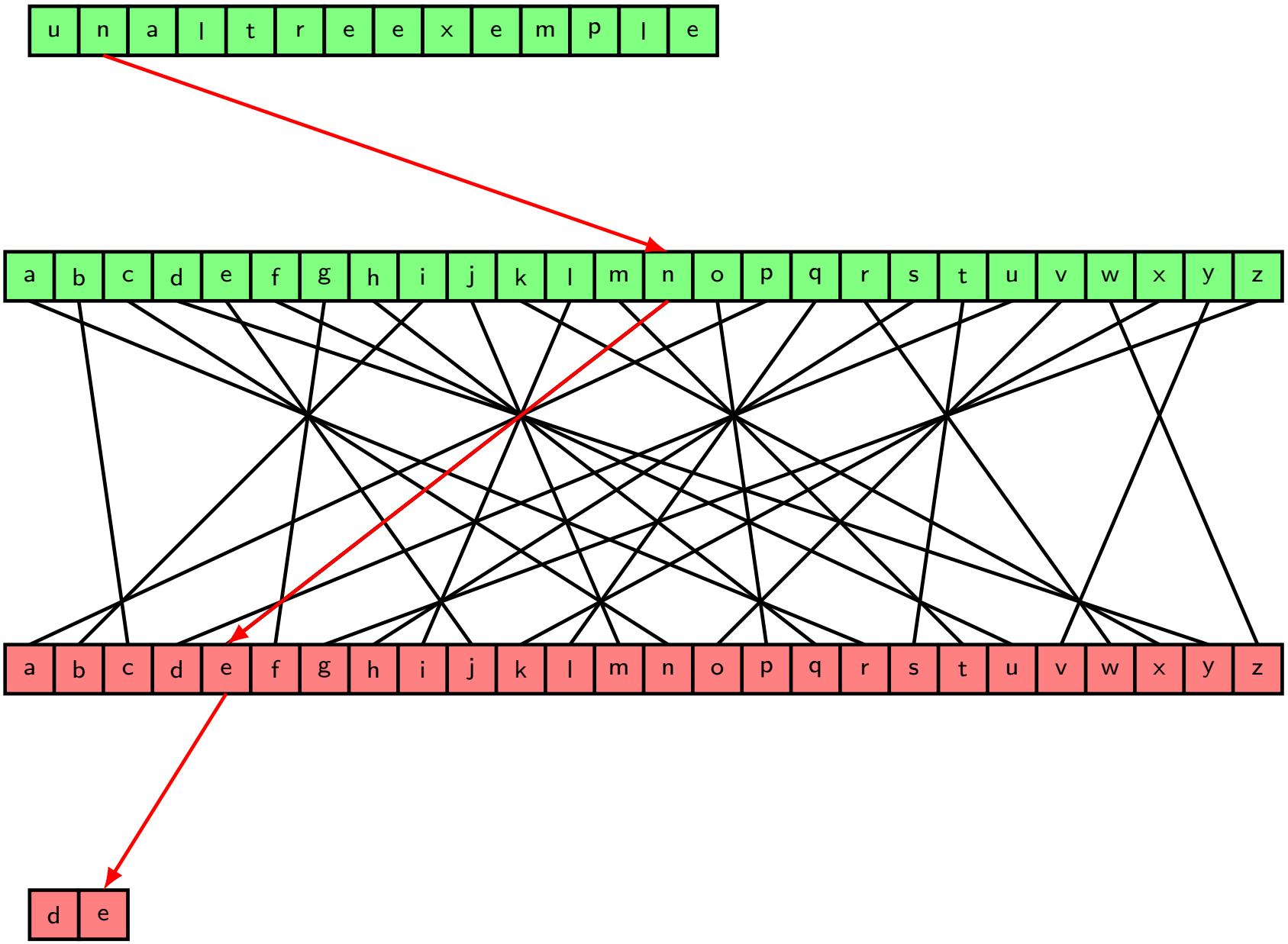
- No resisteix un atac per força bruta: Exploració de l'univers de claus.

Mètodes de substitució: Substitució monoalfabètica (I)

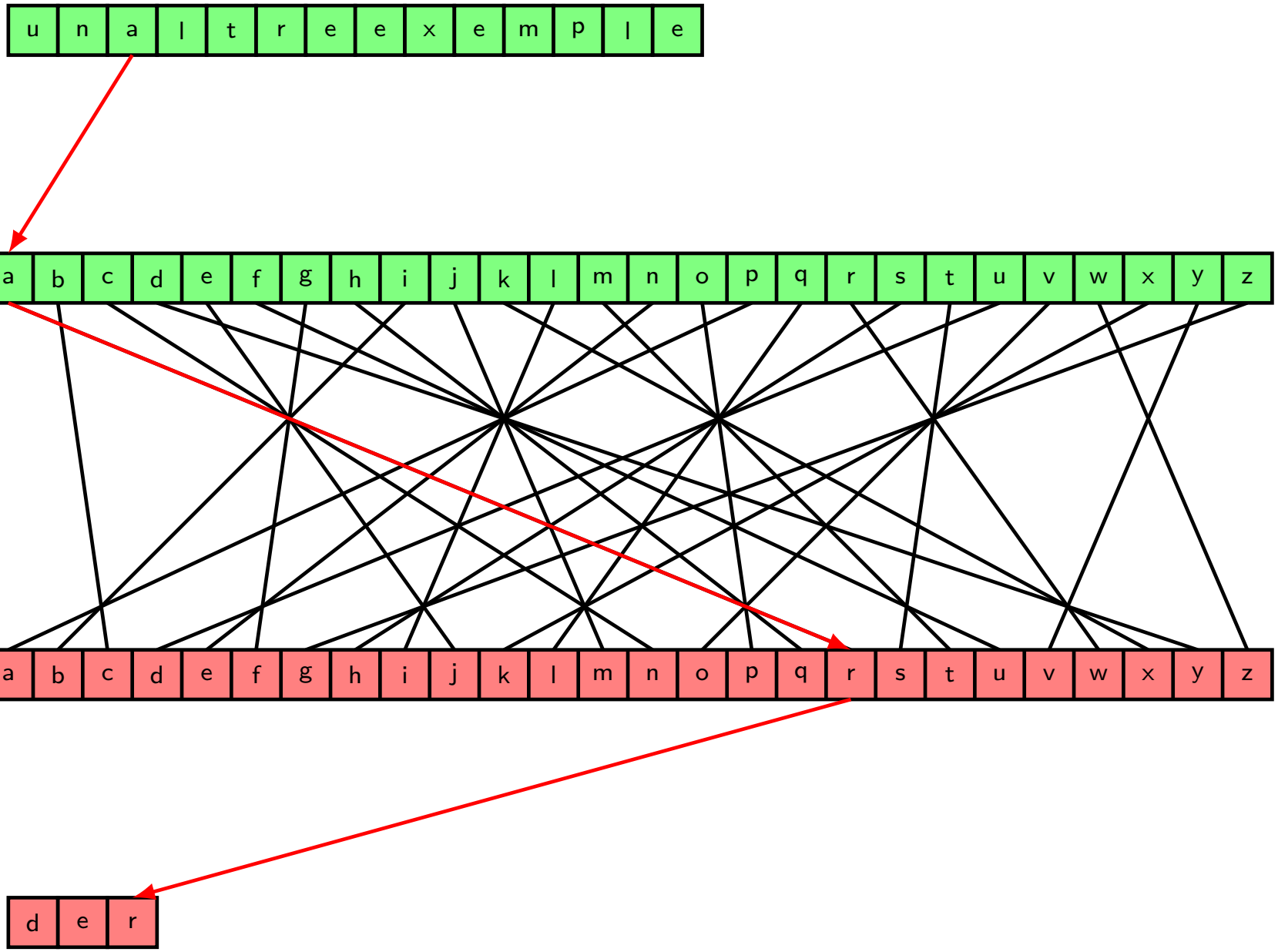
Mètodes de substitució: Substitució monoalfabètica (I)



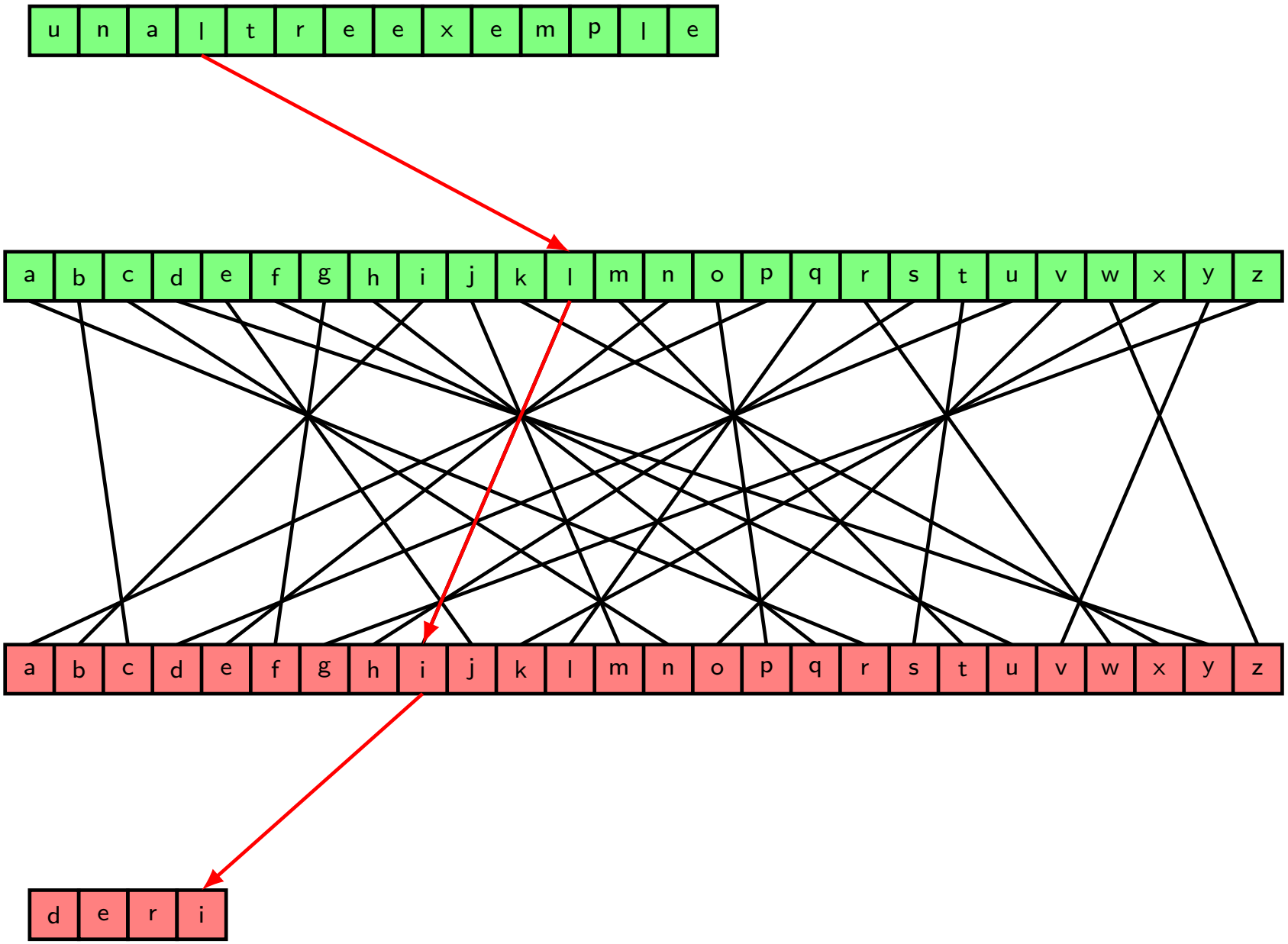
Mètodes de substitució: Substitució monoalfabètica (I)



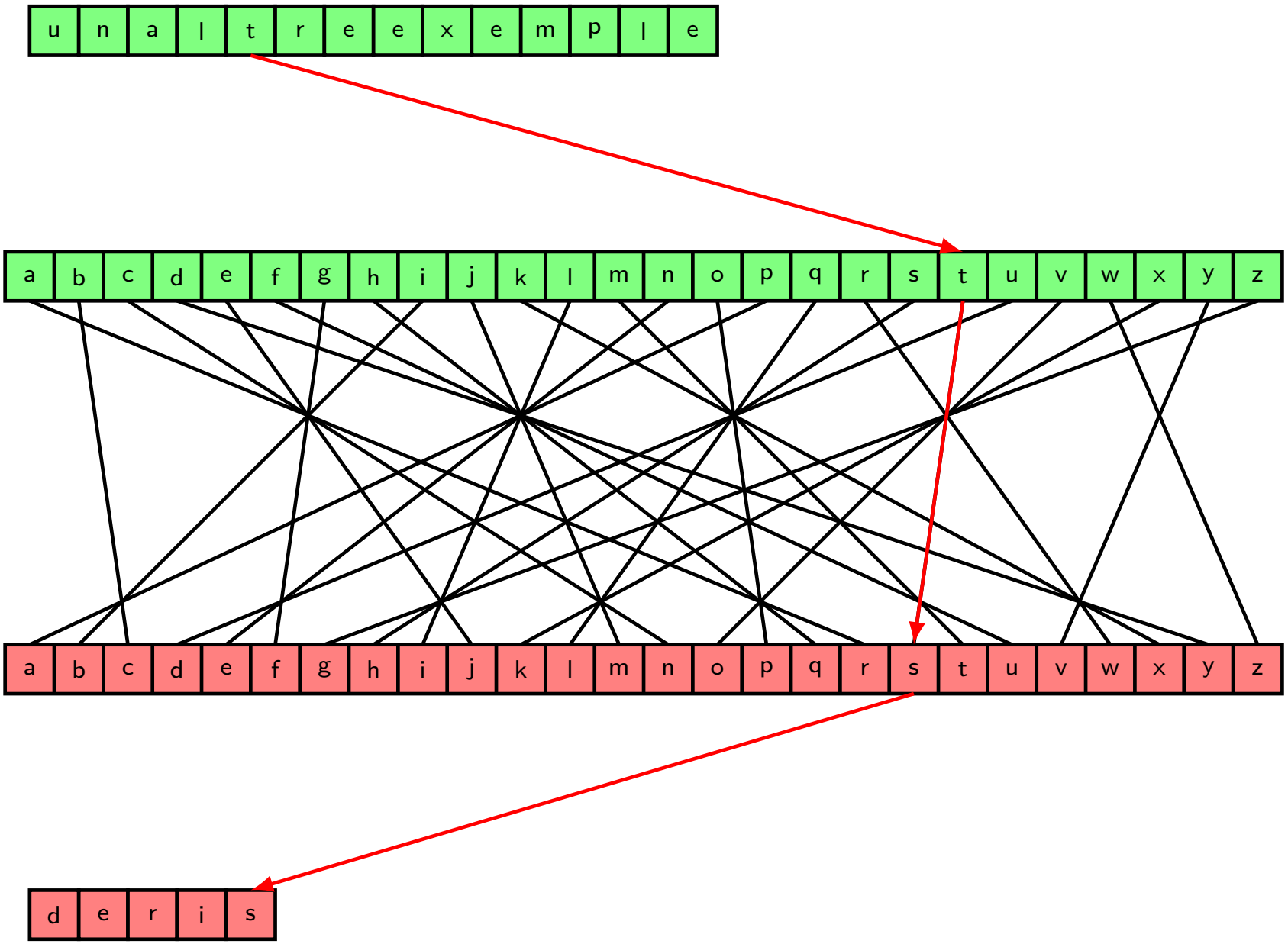
Mètodes de substitució: Substitució monoalfabètica (I)



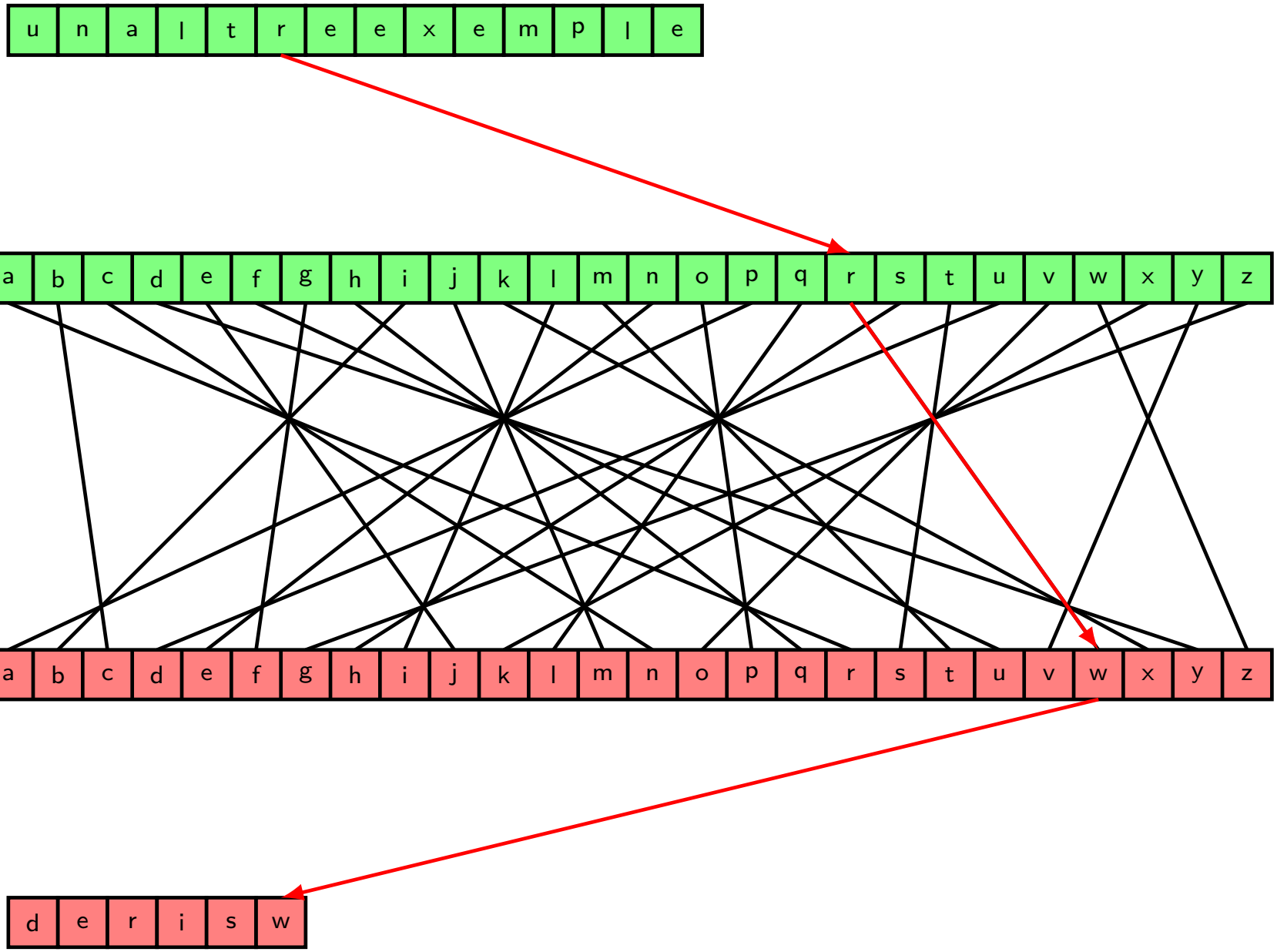
Mètodes de substitució: Substitució monoalfabètica (I)



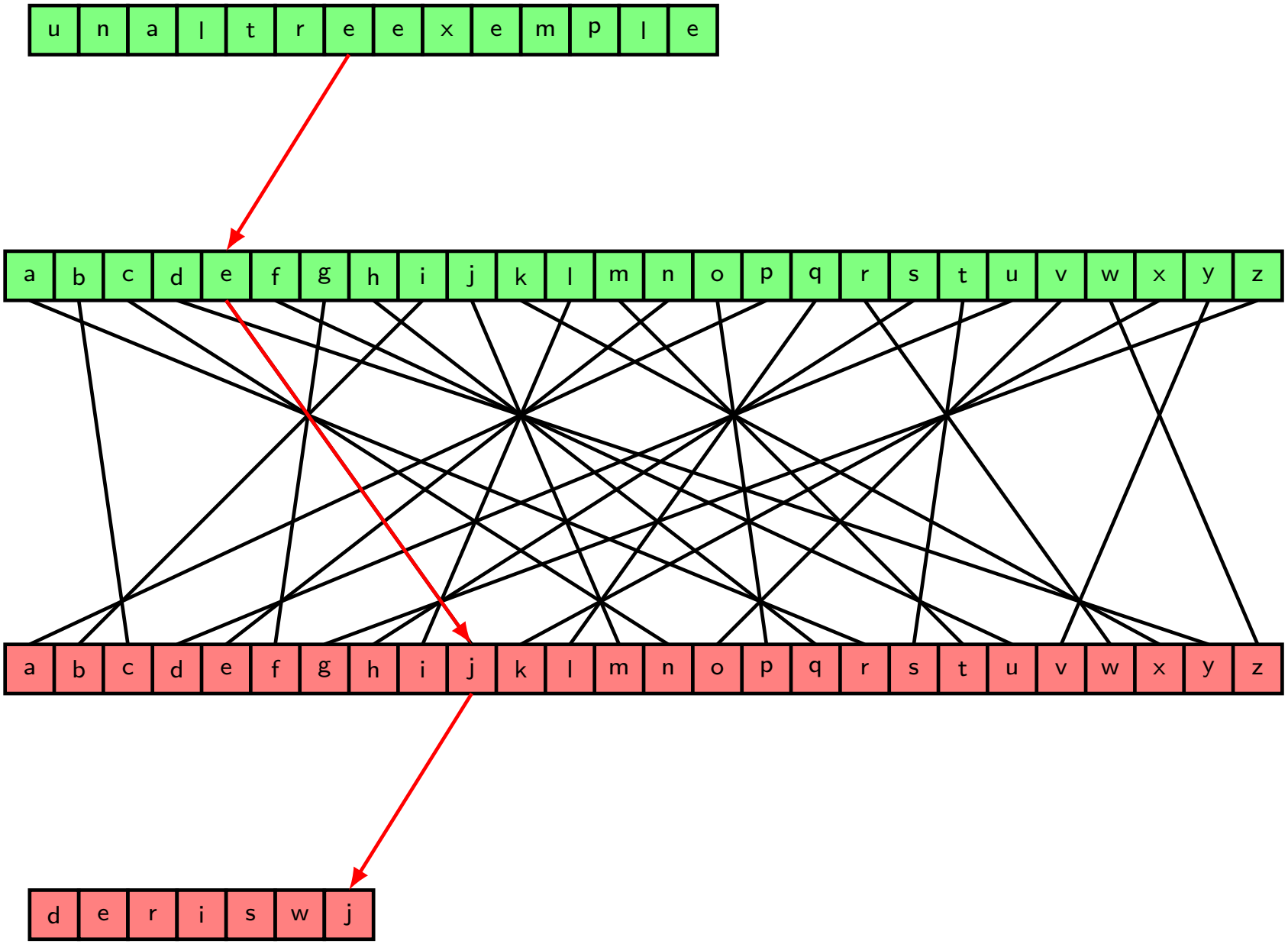
Mètodes de substitució: Substitució monoalfabètica (I)



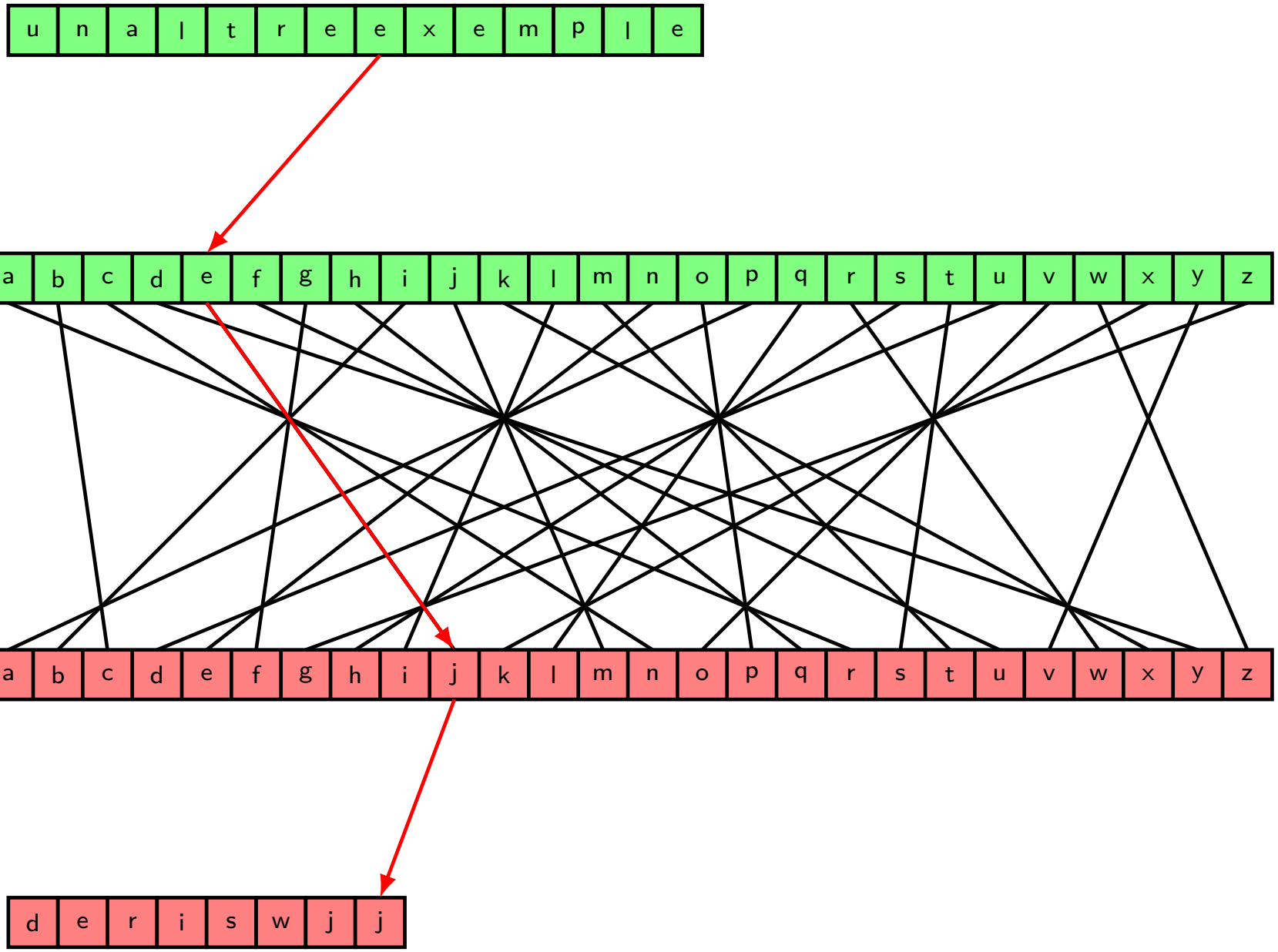
Mètodes de substitució: Substitució monoalfabètica (I)



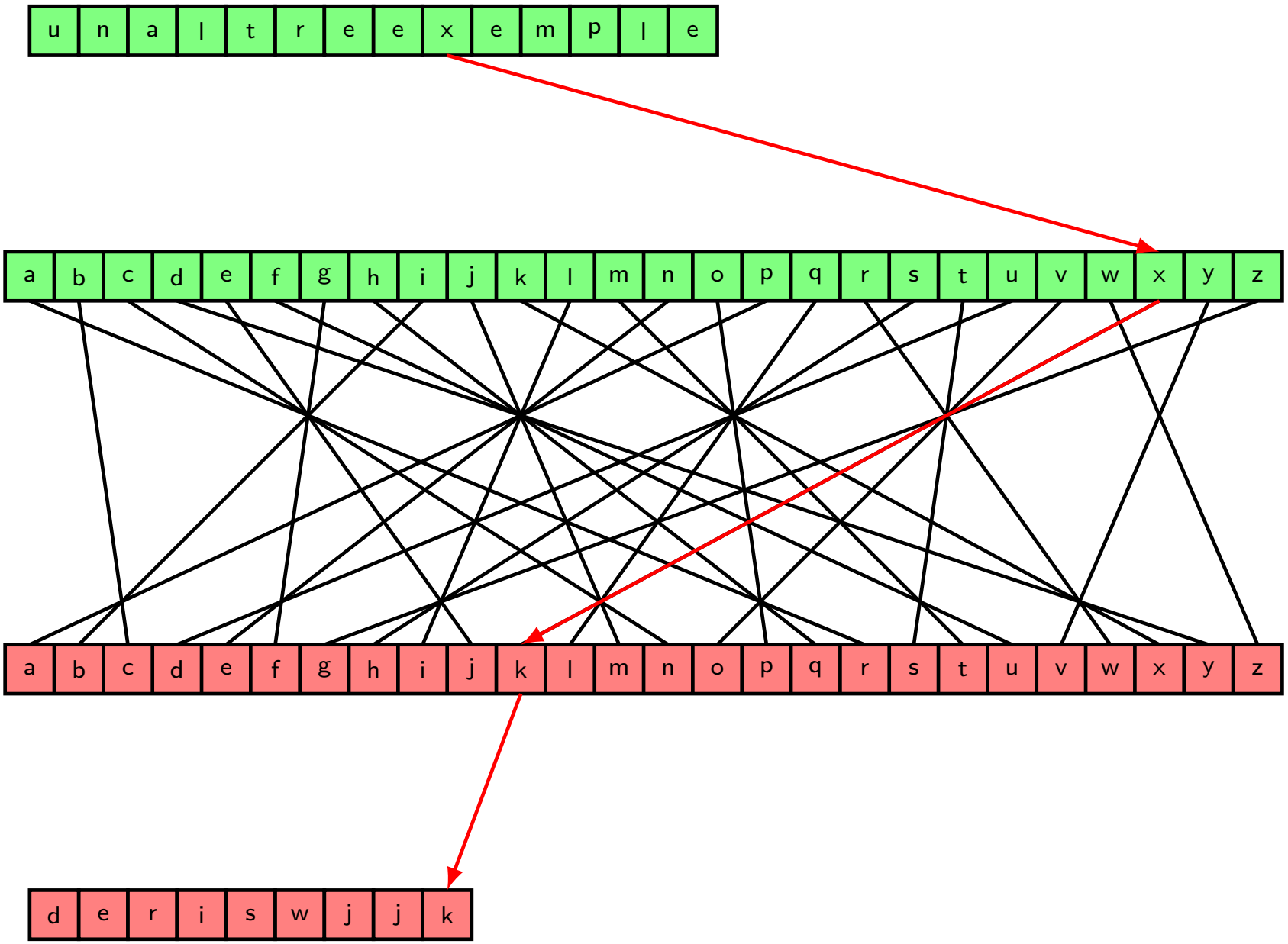
Mètodes de substitució: Substitució monoalfabètica (I)



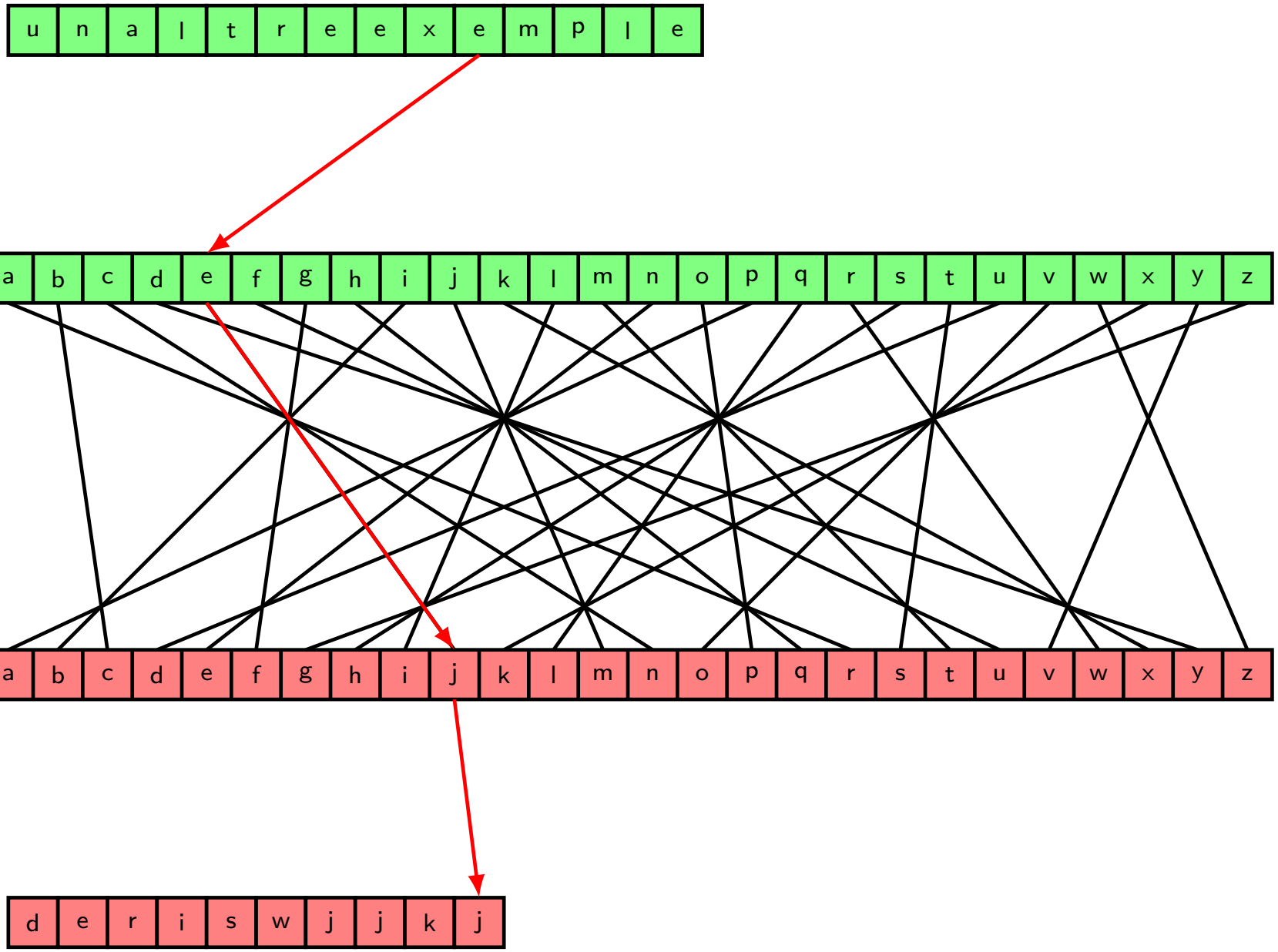
Mètodes de substitució: Substitució monoalfabètica (I)



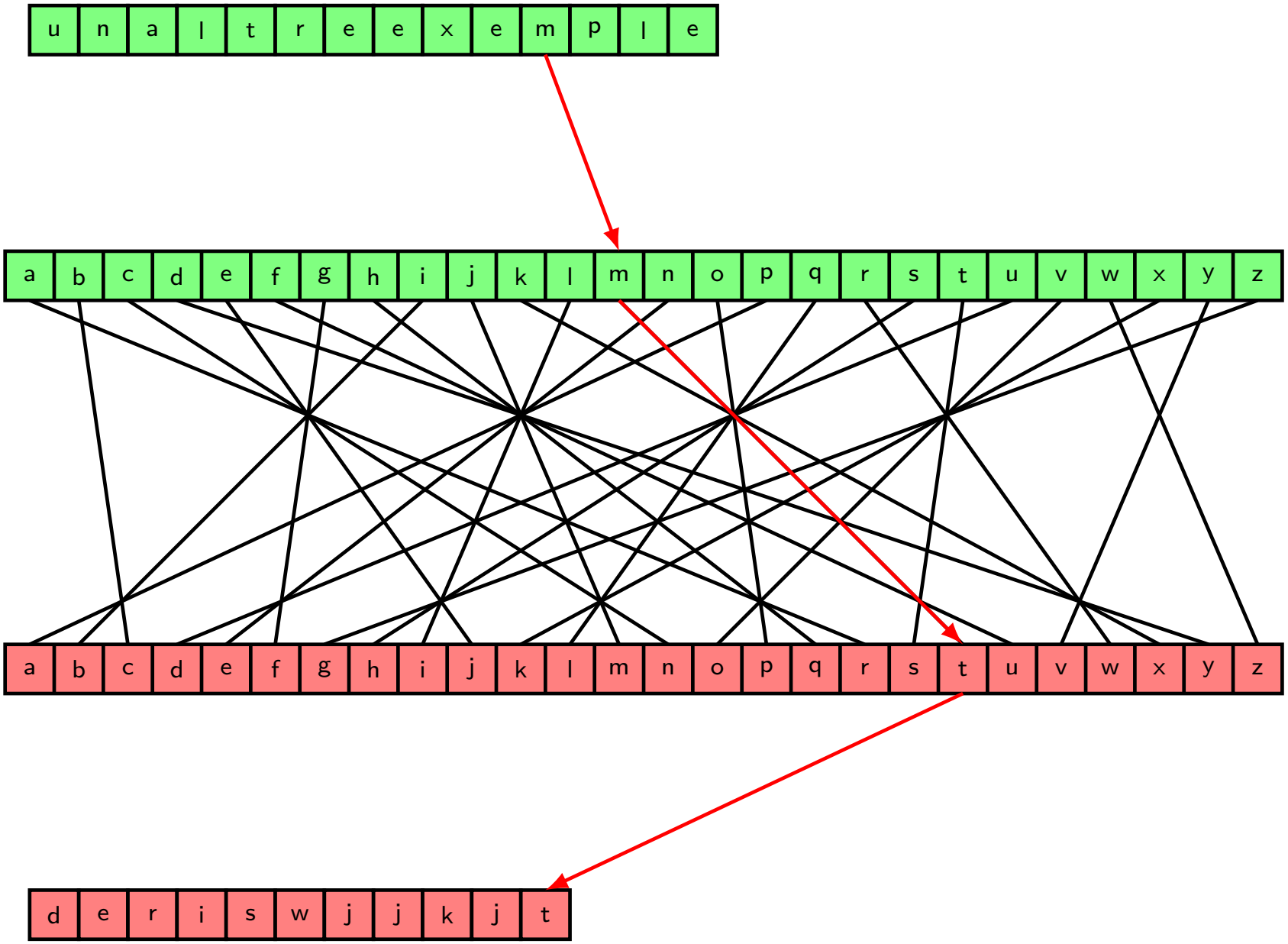
Mètodes de substitució: Substitució monoalfabètica (I)



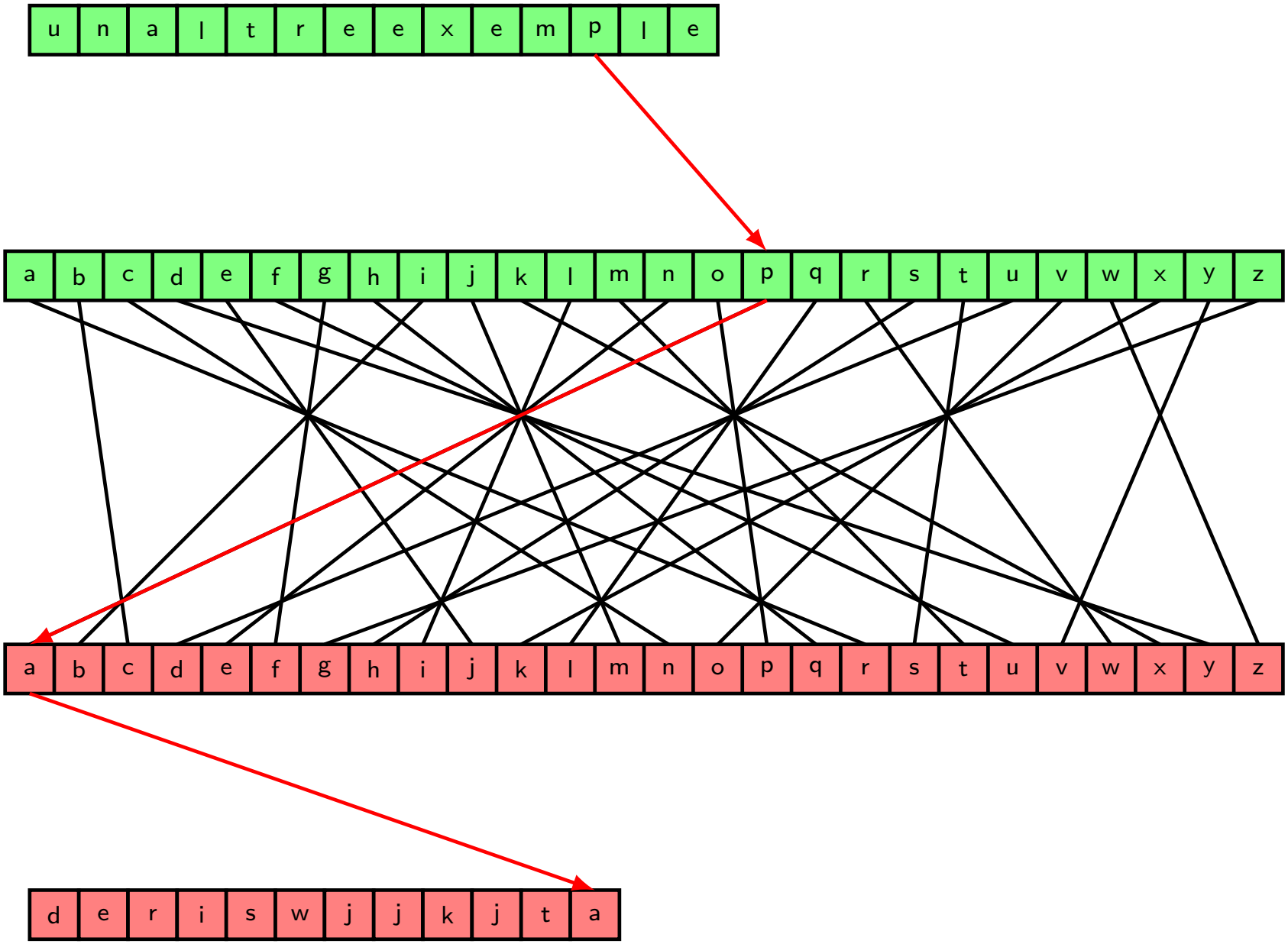
Mètodes de substitució: Substitució monoalfabètica (I)



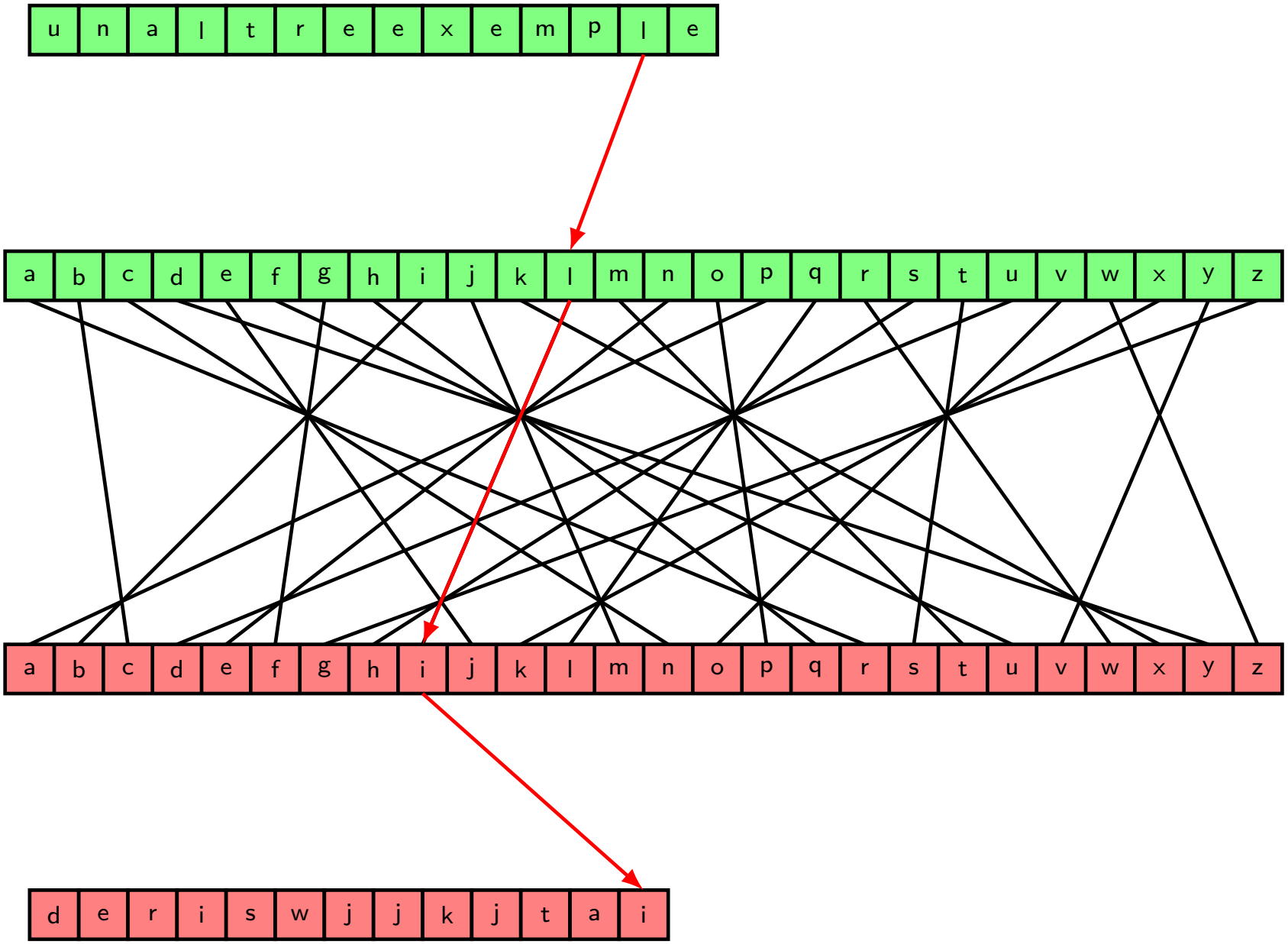
Mètodes de substitució: Substitució monoalfabètica (I)



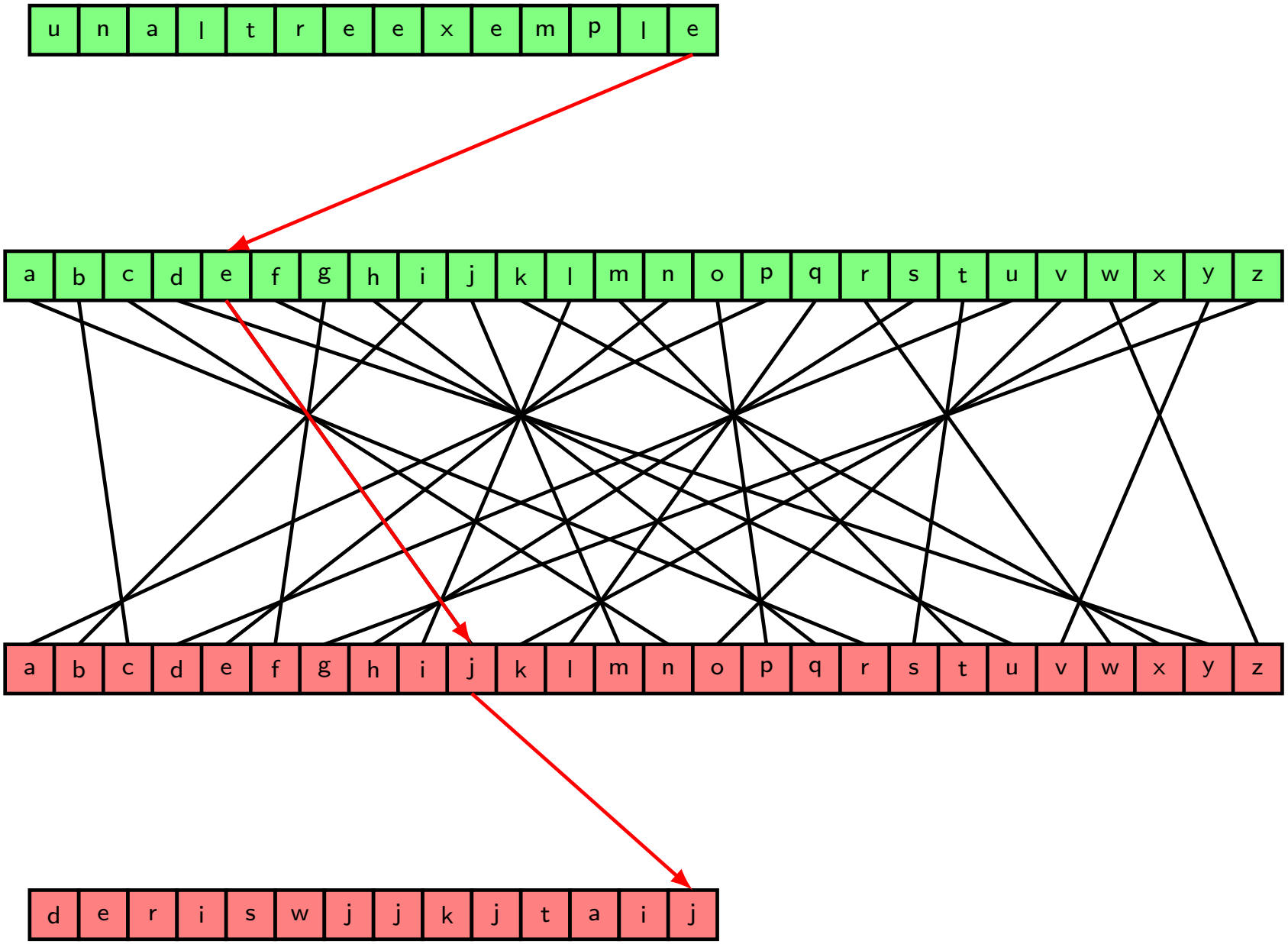
Mètodes de substitució: Substitució monoalfabètica (I)



Mètodes de substitució: Substitució monoalfabètica (I)



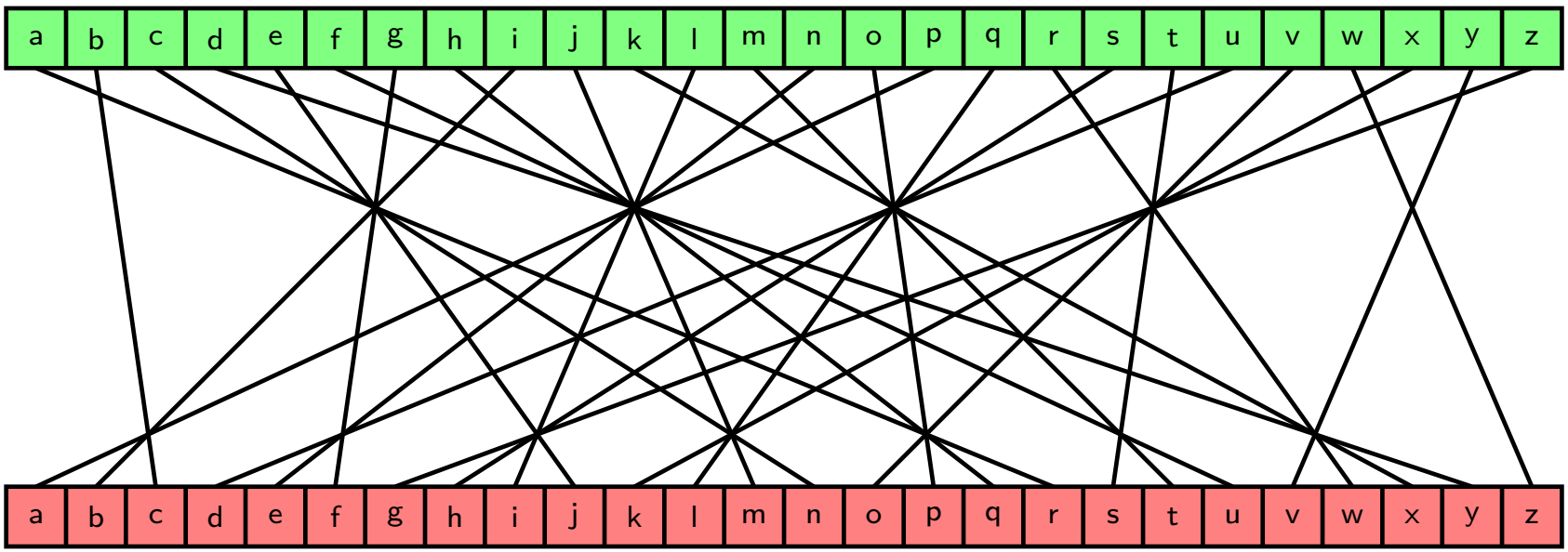
Mètodes de substitució: Substitució monoalfabètica (I)



Mètodes de substitució: Substitució monoalfabètica (I)

u	n	a	l	t	r	e	e	x	e	m	p	l	e

$x \mapsto \pi(x)$



d	e	r	i	s	w	j	j	k	j	t	a	i	j

Mètodes de substitució: Substitució monoalfabètica (III)

Mètodes de substitució: Substitució monoalfabètica (III)

- Conjunt de mètodes basats en fer una permutació de l'abecedari (Atbash, rot13, afí, franc-masó...)

Mètodes de substitució: Substitució monoalfabètica (III)

- Conjunt de mètodes basats en fer una permutació de l'abecedari (Atbash, rot13, afí, franc-masó...)
- L'univers de claus és ara $n!$. Robust vers un atac per força bruta.

Mètodes de substitució: Substitució monoalfabètica (III)

- Conjunt de mètodes basats en fer una permutació de l'abecedari (Atbash, rot13, afí, franc-masó...)
- L'univers de claus és ara $n!$. Robust vers un atac per força bruta.
- No resisteix atacs estadístics si el texte és prou llarg.

Atacs estadístics: Anàlisi freqüencial

Es basa en conèixer la freqüència d'aparició de cada lletra als diferents idiomes

Atacs estadístics: Anàlisi freqüencial

Es basa en conèixer la freqüència d'aparició de cada lletra als diferents idiomes

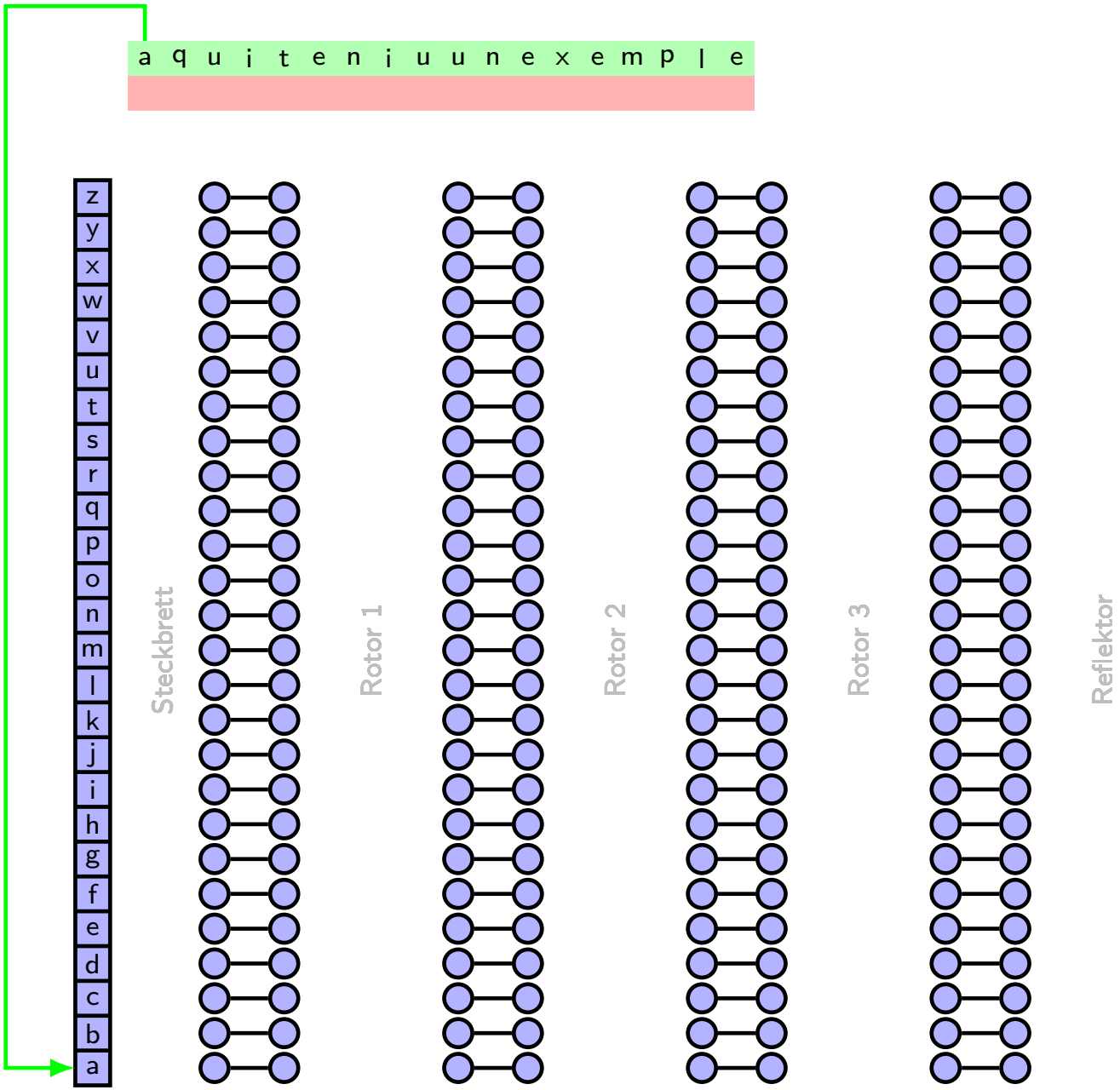
Letter	French [14]	German [15]	Spanish [16]	Portuguese [17]	Esperanto [18]	Italian[19]	Turkish[20]	Swedish[21]	Polish[22]	Dutch [23]	Danish[24]	Icelandic[25]	Finnish[26]	Czech
a	7.636%	6.516%	11.525%	14.634%	12.117%	11.745%	12.920%	9.383%	10.503%	7.486%	6.025%	10.110%	12.217%	8.421%
b	0.901%	1.886%	2.215%	1.043%	0.980%	0.927%	2.844%	1.535%	1.740%	1.584%	2.000%	1.043%	0.281%	0.822%
c	3.260%	2.732%	4.019%	3.882%	0.776%	4.501%	1.463%	1.486%	3.895%	1.242%	0.565%	0	0.281%	0.740%
d	3.669%	5.076%	5.510%	4.992%	3.044%	3.736%	5.206%	4.702%	3.725%	5.933%	5.858%	1.575%	1.043%	3.475%
e	14.715%	16.396%	12.681%	11.570%	8.995%	11.792%	9.912%	10.149%	7.352%	17.324%	15.453%	6.418%	7.968%	7.562%
f	1.066%	1.656%	0.692%	1.023%	1.037%	1.153%	0.461%	2.027%	0.143%	0.805%	2.406%	3.013%	0.194%	0.084%
g	0.866%	3.009%	1.768%	1.303%	1.171%	1.644%	1.253%	2.862%	1.731%	3.403%	4.077%	4.241%	0.392%	0.092%
h	0.737%	4.577%	0.703%	0.781%	0.384%	0.636%	1.212%	2.090%	1.015%	2.380%	1.621%	1.871%	1.851%	1.356%
i	7.529%	6.550%	6.247%	6.186%	10.012%	10.143%	9.600%*	5.817%	8.328%	6.499%	6.000%	7.578%	10.817%	6.073%
j	0.613%	0.268%	0.443%	0.397%	3.501%	0.011%	0.034%	0.614%	1.836%	1.461%	0.730%	1.144%	2.042%	1.433%
k	0.049%	1.417%	0.011%	0.015%	4.163%	0.009%	5.683%	3.140%	2.753%	2.248%	3.395%	3.314%	4.973%	2.894%
l	5.456%	3.437%	4.967%	2.779%	6.145%	6.510%	5.922%	5.275%	2.564%	3.568%	5.229%	4.532%	5.761%	3.802%
m	2.968%	2.534%	3.157%	4.738%	2.994%	2.512%	3.752%	3.471%	2.515%	2.213%	3.237%	4.041%	3.202%	2.446%
n	7.095%	9.776%	6.712%	4.046%	7.955%	6.883%	7.987%	8.542%	6.237%	10.032%	7.240%	7.711%	8.826%	6.468%
o	5.598%	2.594%	8.683%	9.735%	8.779%	9.832%	2.976%	4.482%	6.667%	6.063%	4.636%	2.166%	5.614%	6.695%
p	2.521%	0.670%	2.510%	2.523%	2.755%	3.056%	0.886%	1.839%	2.445%	1.370%	1.756%	0.789%	1.842%	1.906%
q	1.362%	0.018%	0.877%	1.204%	0	0.505%	0	0.020%	0	0.009%	0.007%	0	0.013%	0.001%
r	6.693%	7.003%	6.871%	6.530%	5.914%	6.367%	7.722%	8.431%	5.243%	6.411%	8.956%	8.581%	2.872%	4.799%
s	7.948%	7.273%	7.977%	6.805%	6.092%	4.981%	3.014%	6.590%	5.224%	5.733%	5.805%	5.630%	7.862%	5.212%
t	7.244%	6.154%	4.632%	4.736%	5.276%	5.623%	3.314%	7.691%	2.475%	6.923%	6.862%	4.953%	8.750%	5.727%
u	6.311%	4.166%	2.927%	3.634%	3.183%	3.011%	3.235%	1.919%	2.062%	2.192%	1.979%	4.562%	5.008%	2.160%
v	1.838%	0.846%	1.138%	1.575%	1.904%	2.097%	0.959%	2.415%	0.012%	1.854%	2.332%	2.437%	2.250%	5.344%
w	0.074%	1.921%	0.017%	0.037%	0	0.033%	0	0.142%	5.813%	1.821%	0.069%	0	0.094%	0.016%
x	0.427%	0.034%	0.215%	0.253%	0	0.003%	0	0.159%	0.004%	0.036%	0.028%	0.046%	0.031%	0.027%
y	0.128%	0.039%	1.008%	0.006%	0	0.020%	3.336%	0.708%	3.206%	0.035%	0.698%	0.900%	1.745%	1.043%
z	0.326%	1.134%	0.517%	0.470%	0.494%	1.181%	1.500%	0.070%	4.852%	1.374%	0.034%	0	0.051%	1.503%

Màquina Enigma. II guerra mundial.

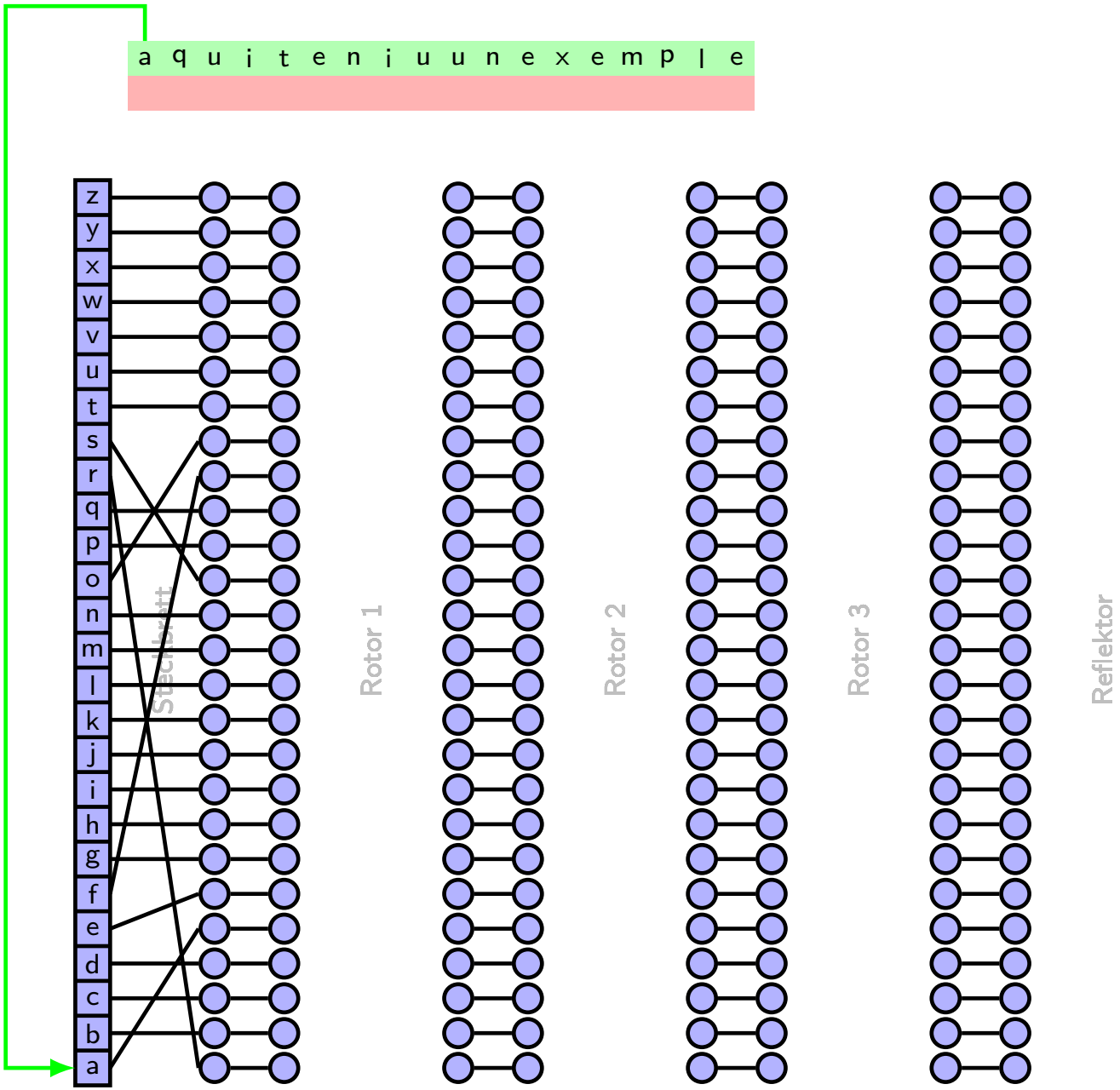
Figure: Màquina Enigma

Descifrando Enigma

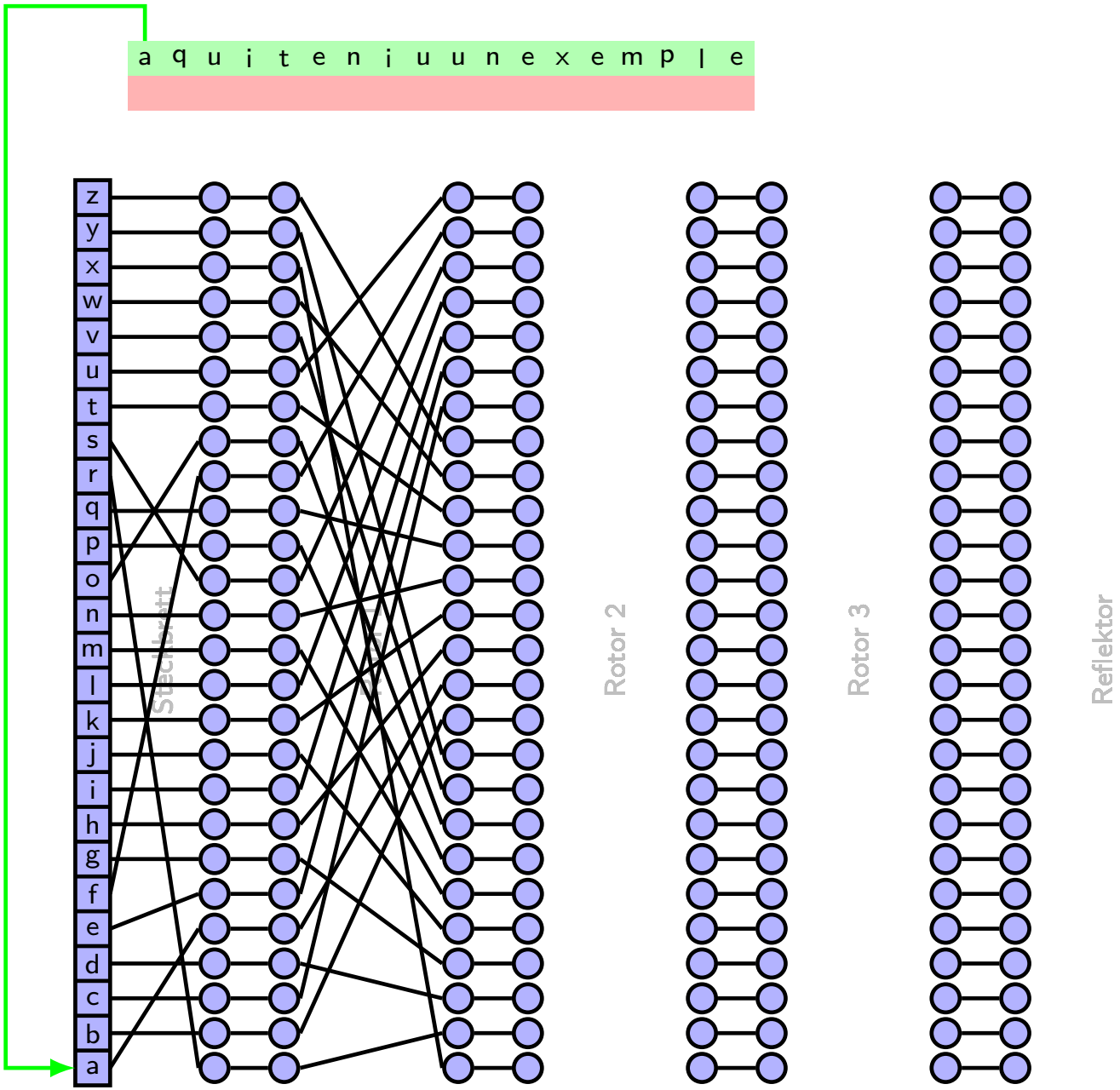
Funcionament de la màquina Enigma



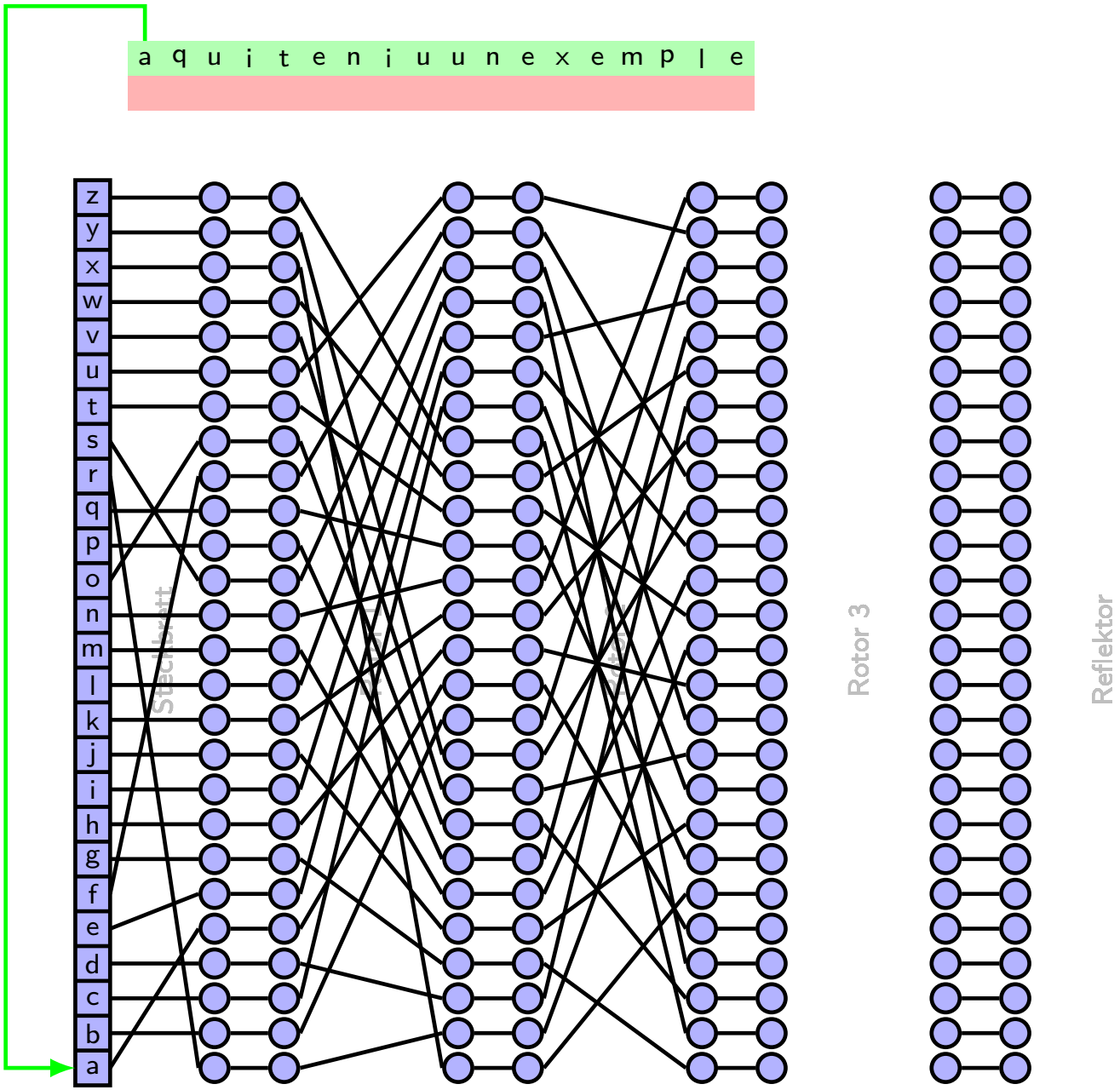
Funcionament de la màquina Enigma



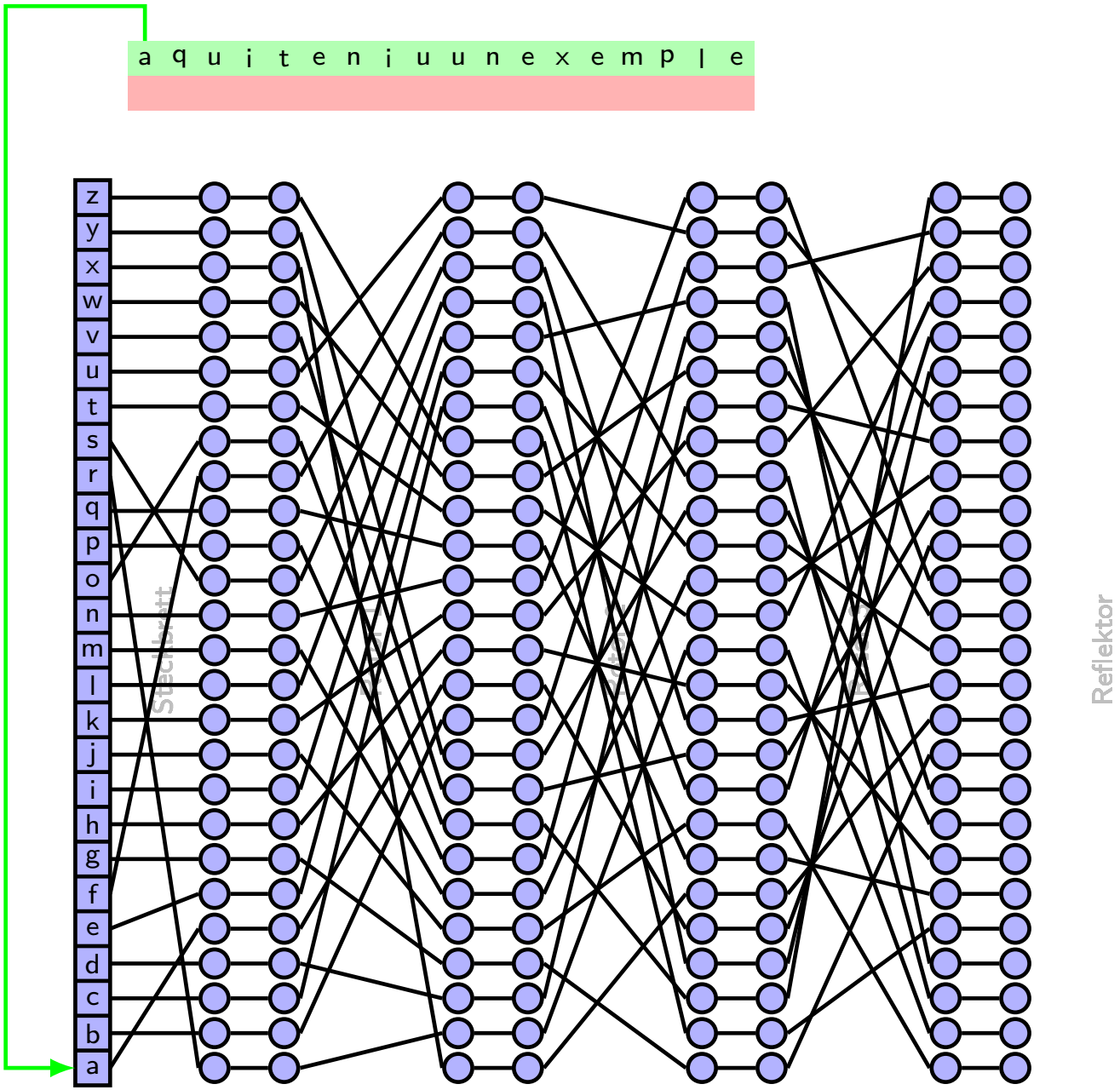
Funcionament de la màquina Enigma



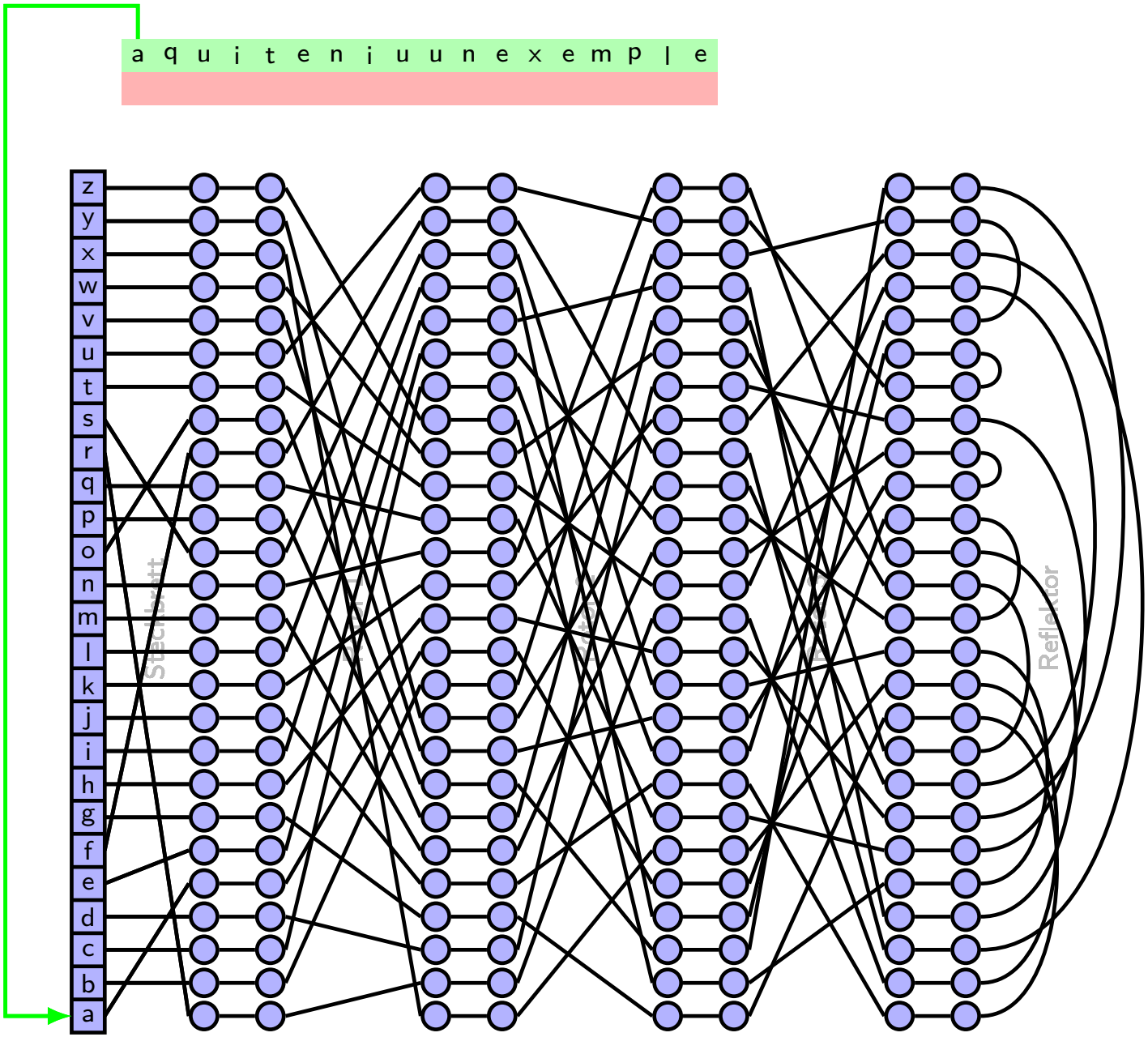
Funcionament de la màquina Enigma



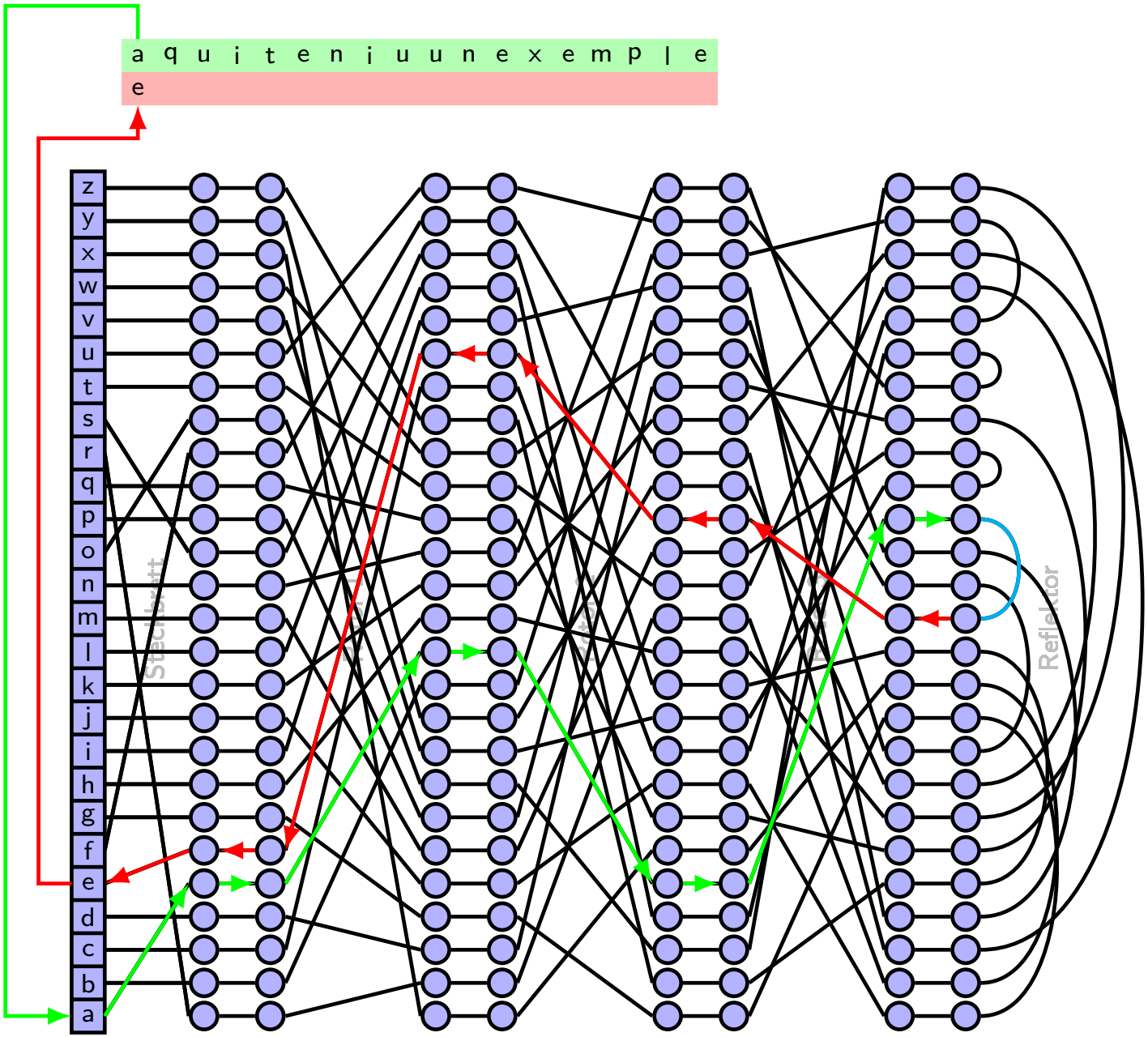
Funcionament de la màquina Enigma



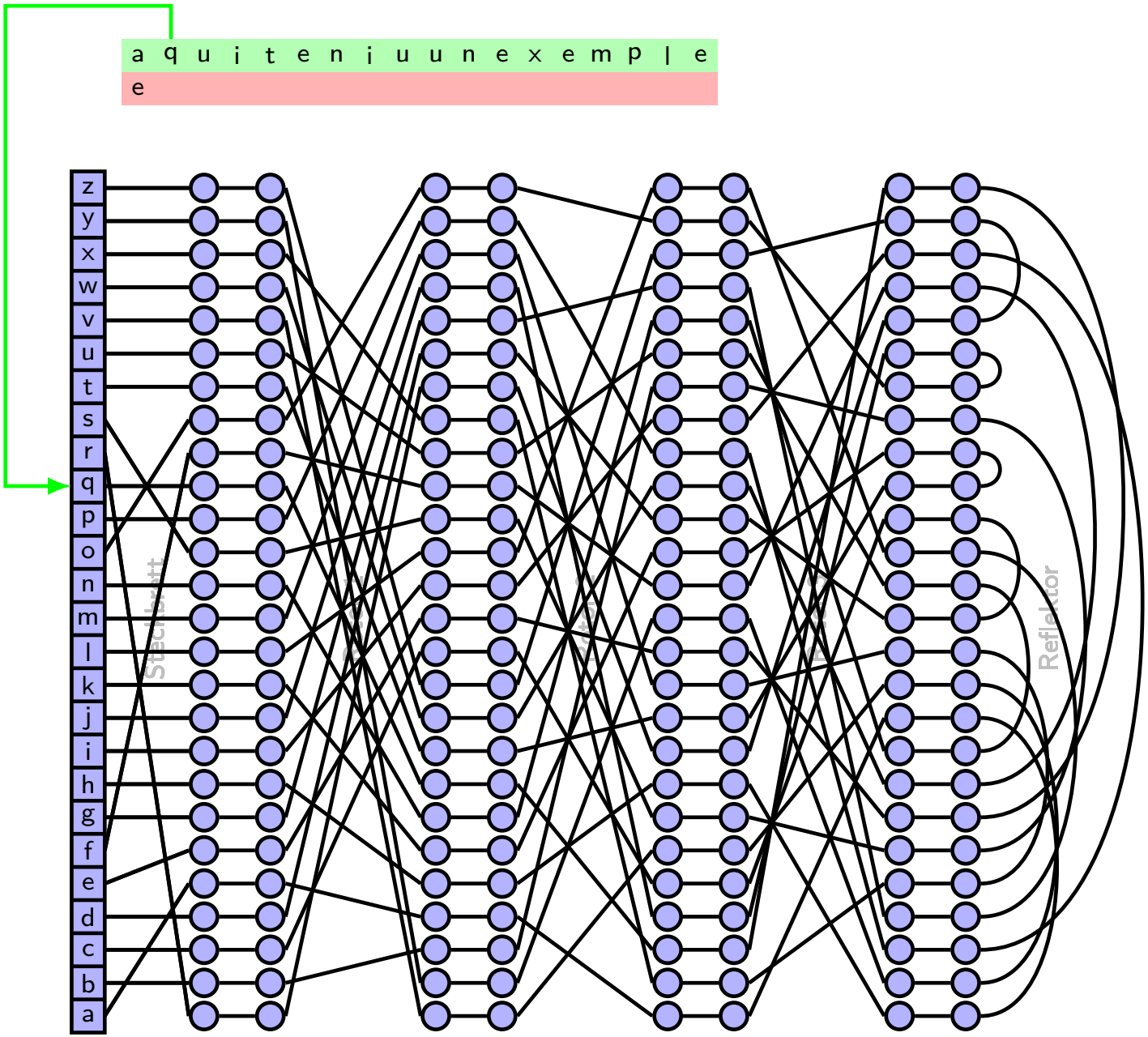
Funcionament de la màquina Enigma



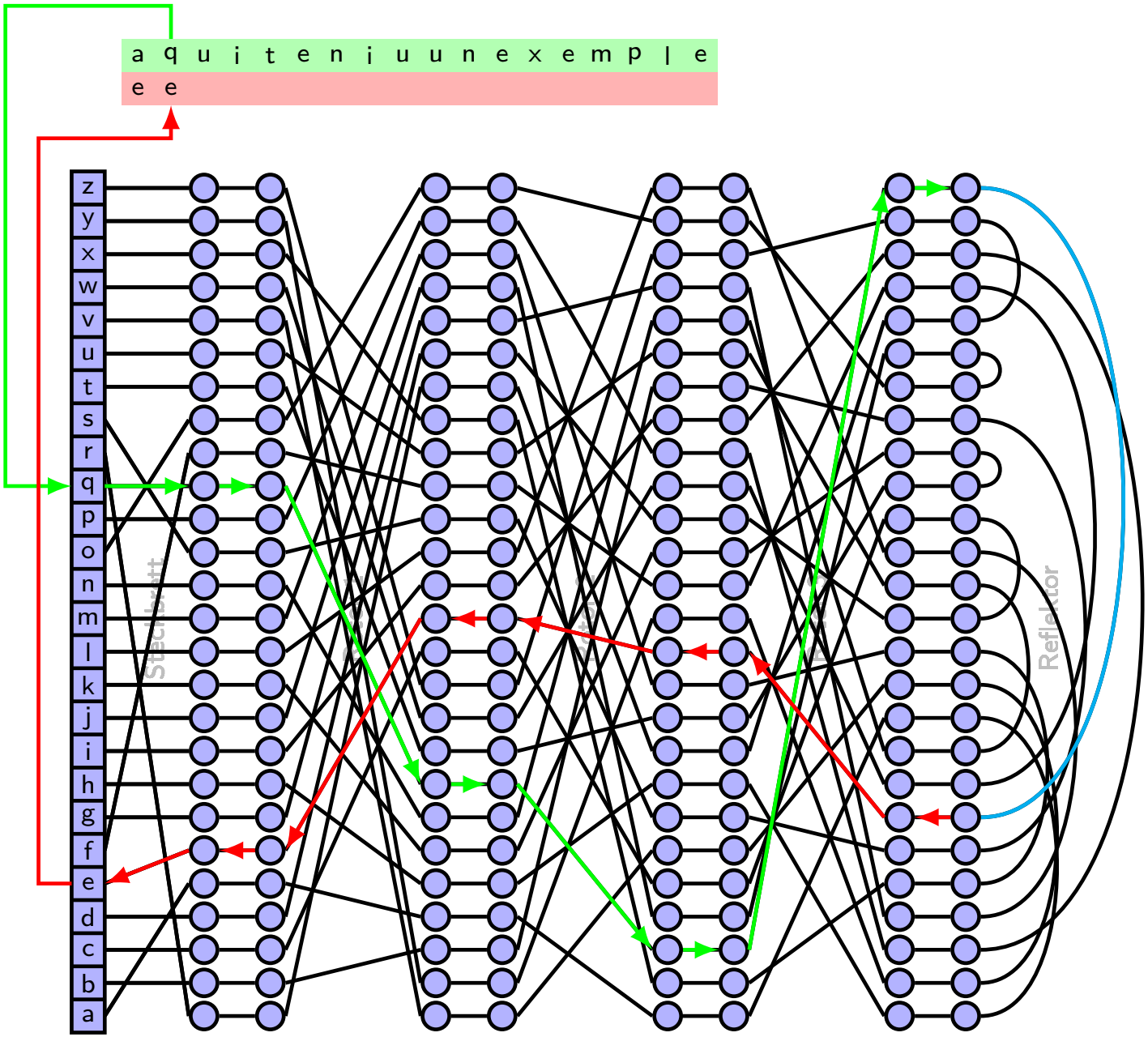
Funcionament de la màquina Enigma



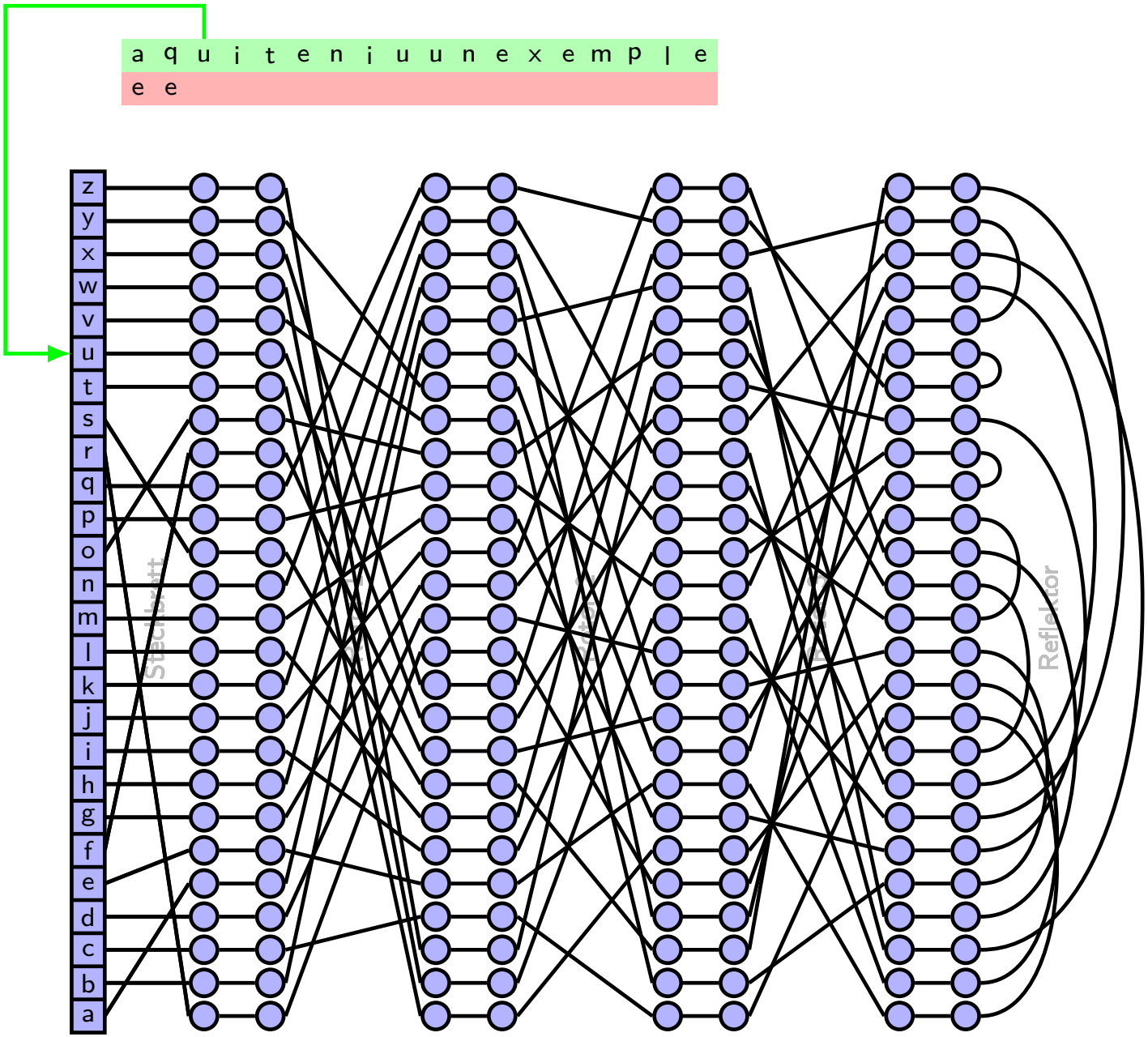
Funcionament de la màquina Enigma



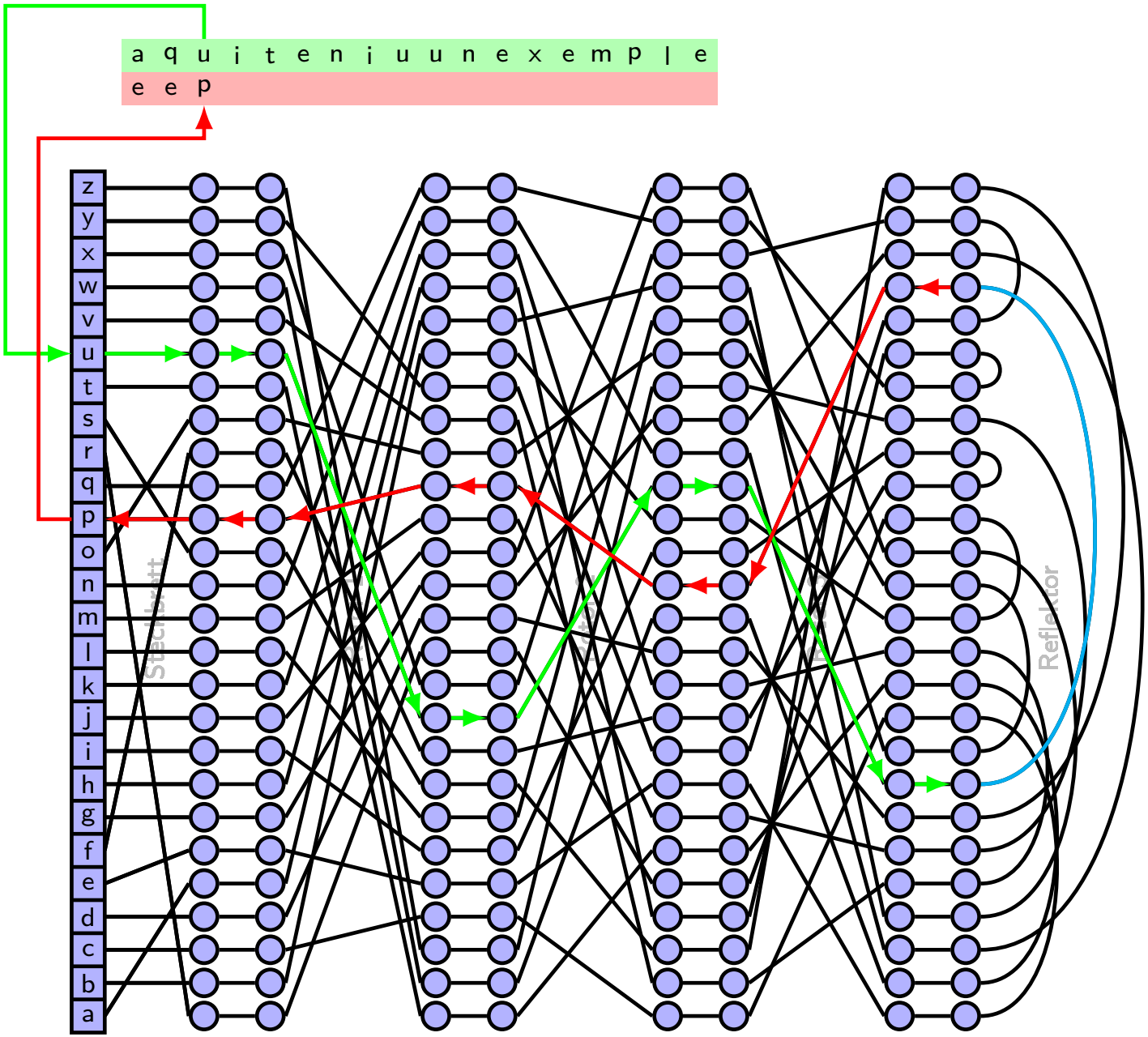
Funcionament de la màquina Enigma



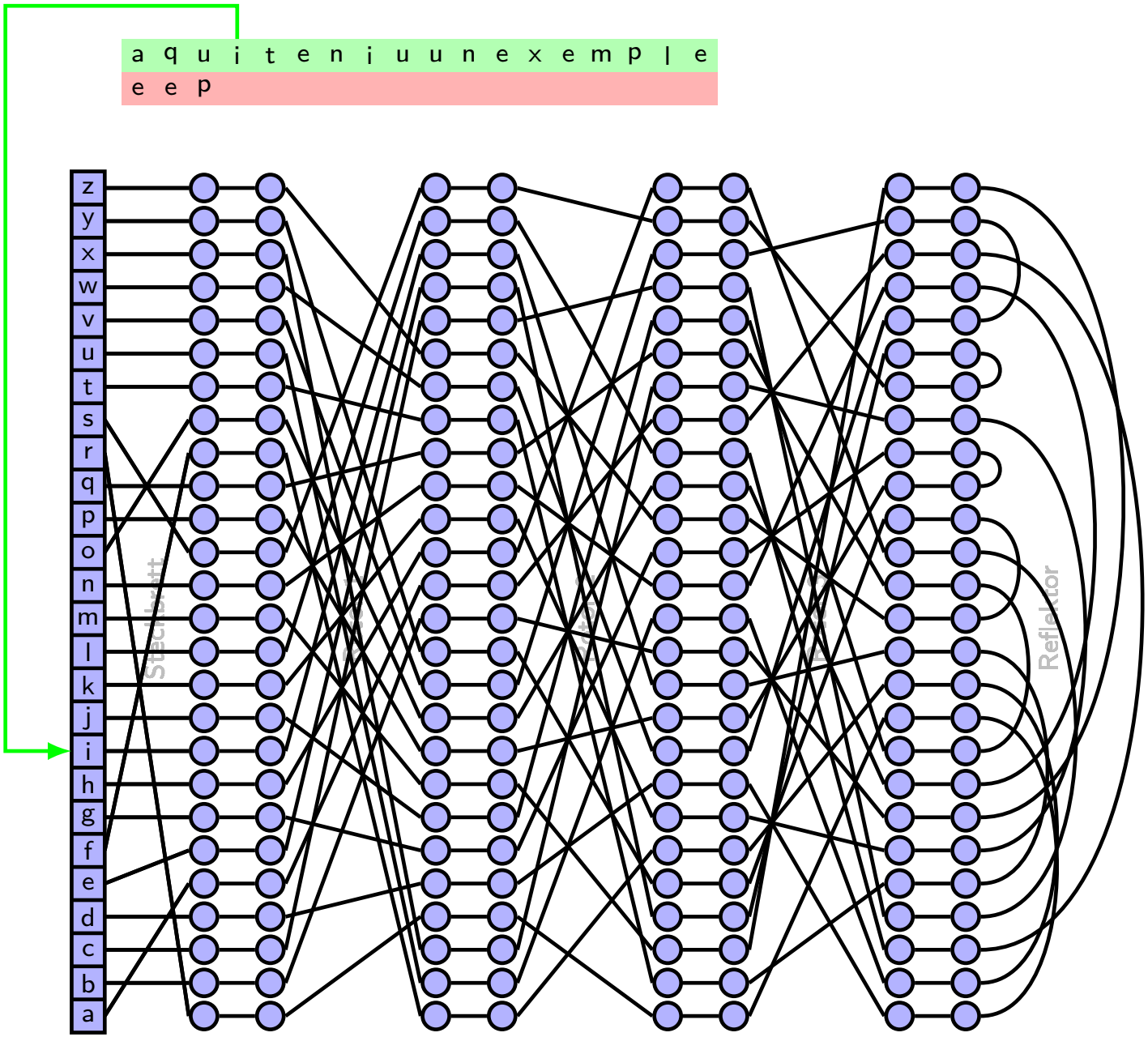
Funcionament de la màquina Enigma



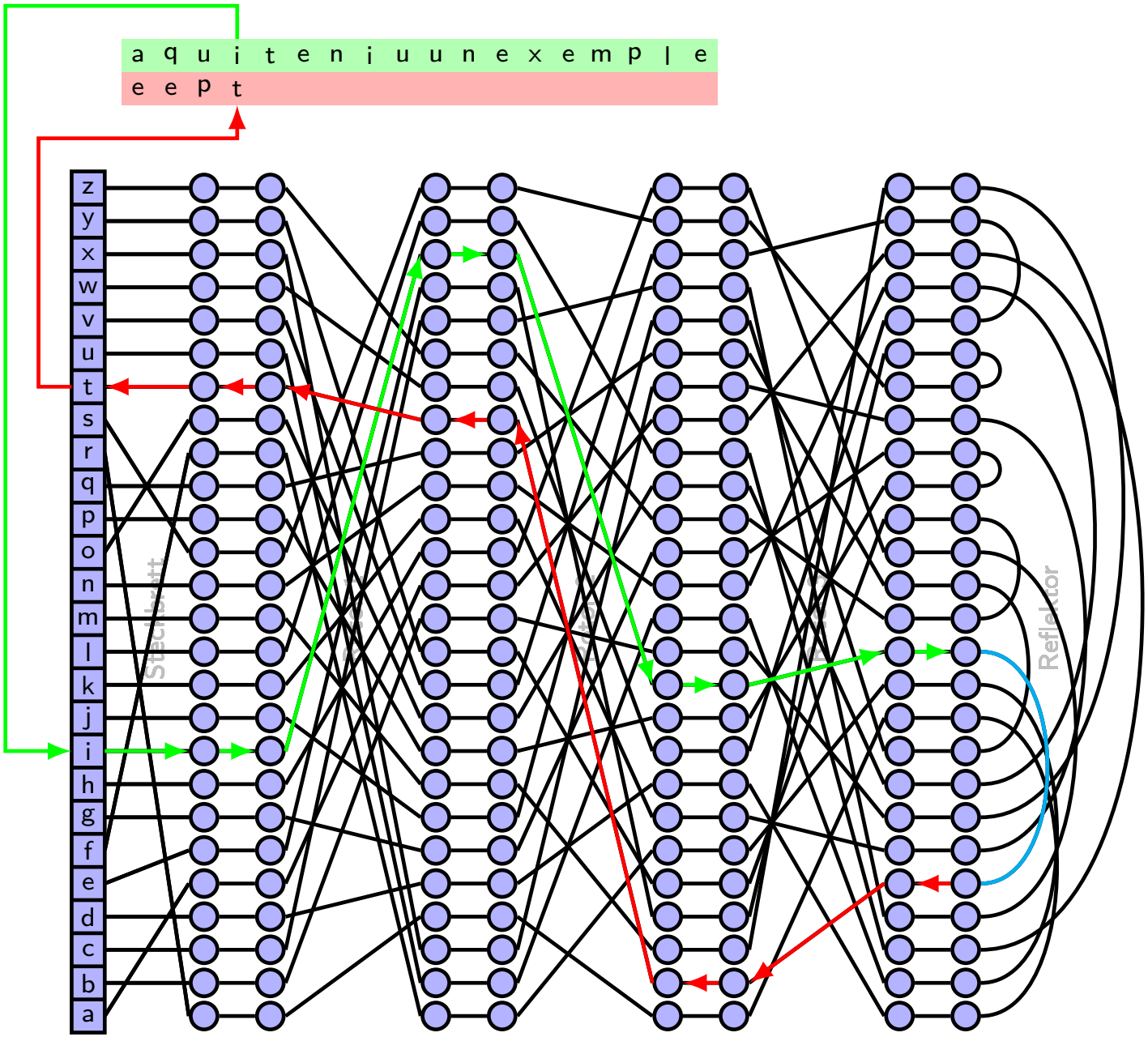
Funcionament de la màquina Enigma



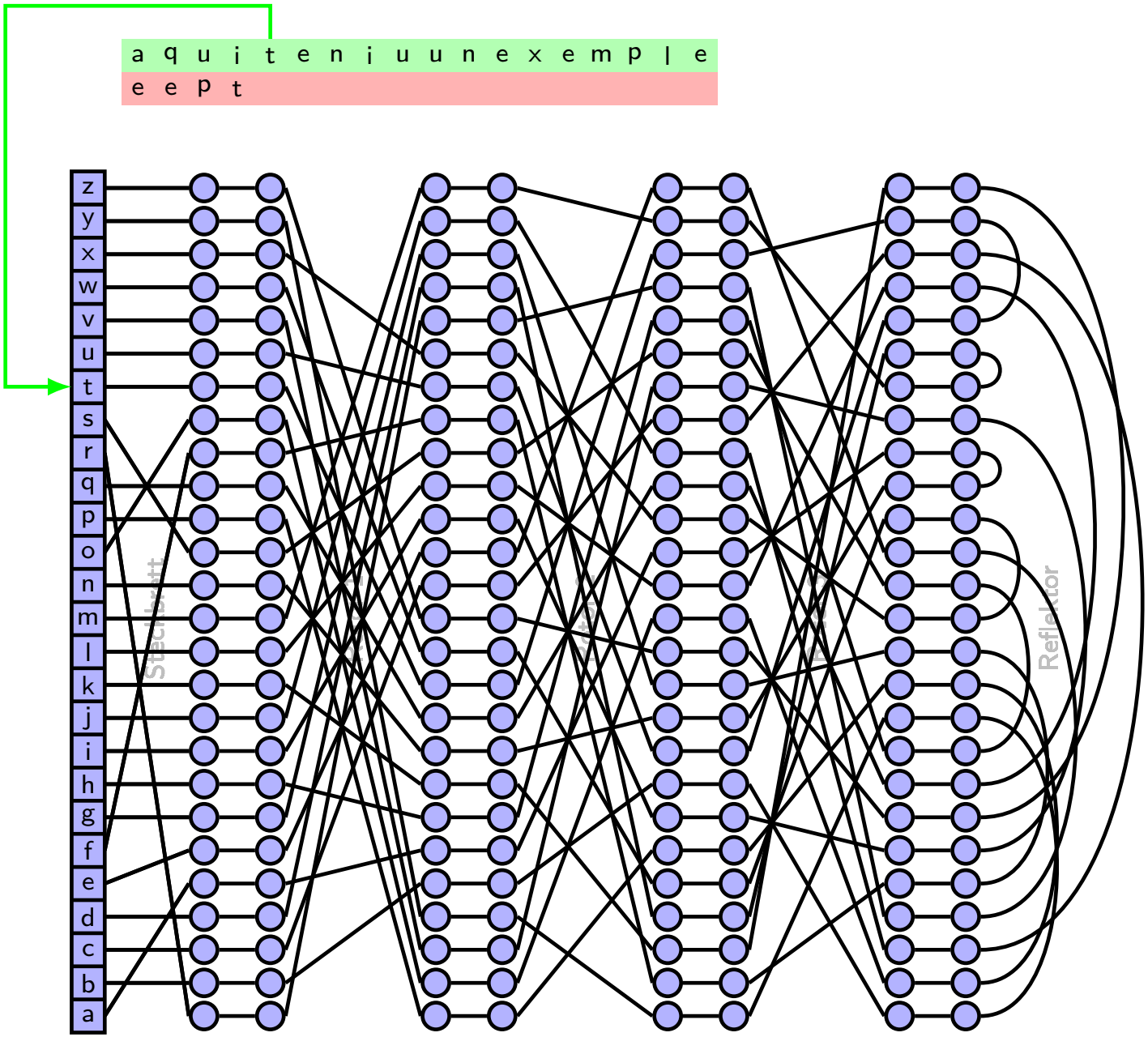
Funcionament de la màquina Enigma



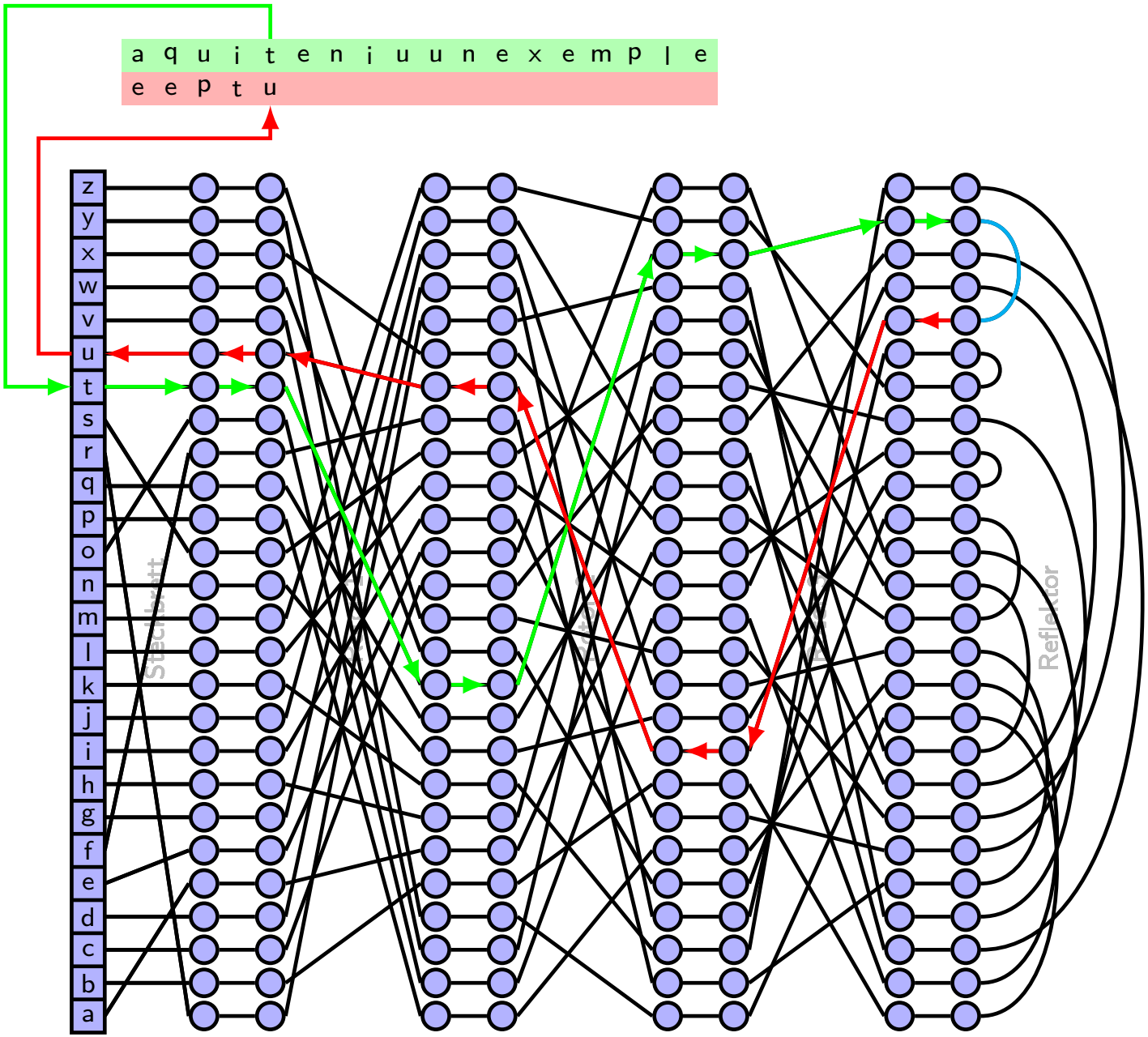
Funcionament de la màquina Enigma



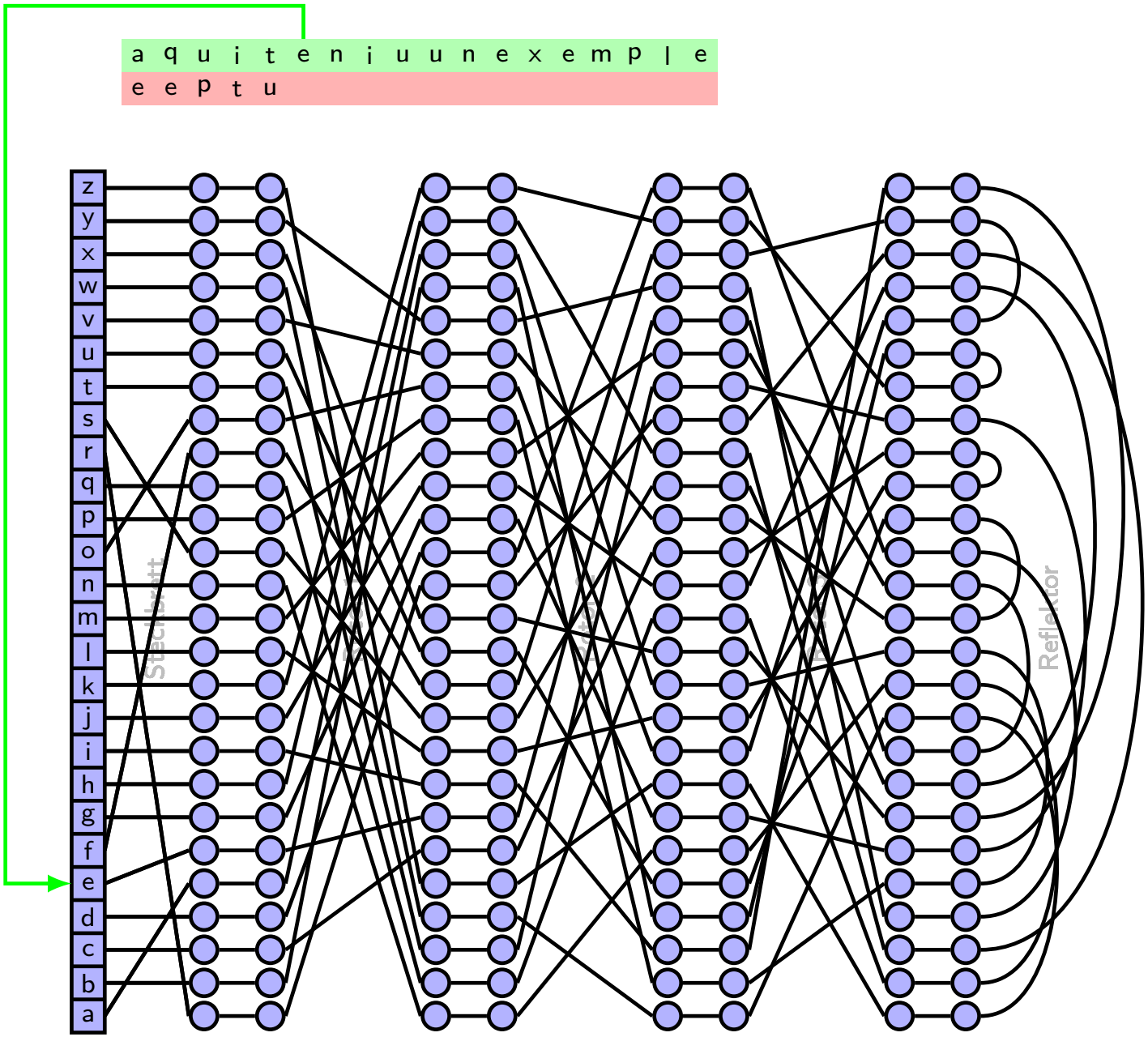
Funcionament de la màquina Enigma



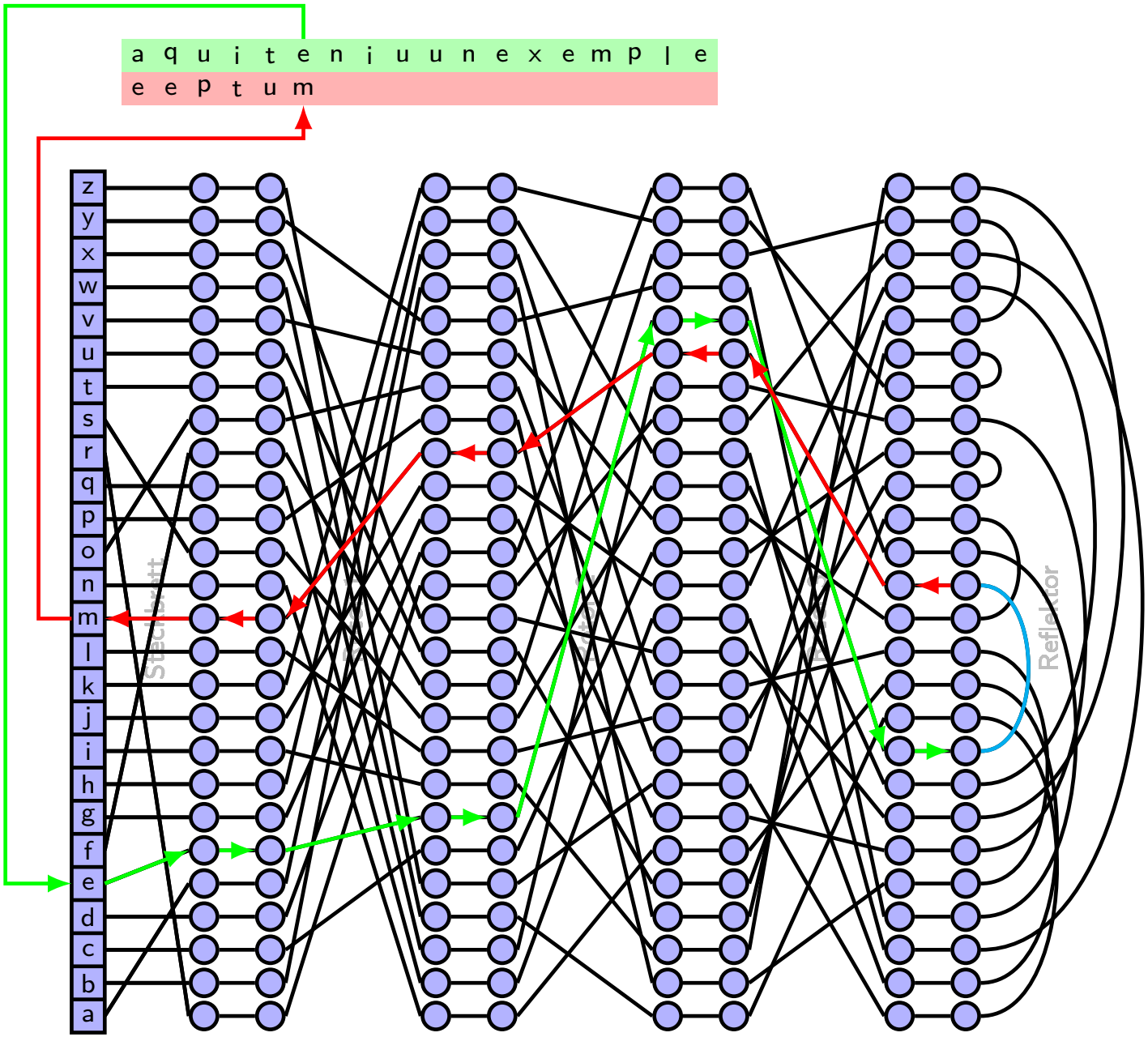
Funcionament de la màquina Enigma



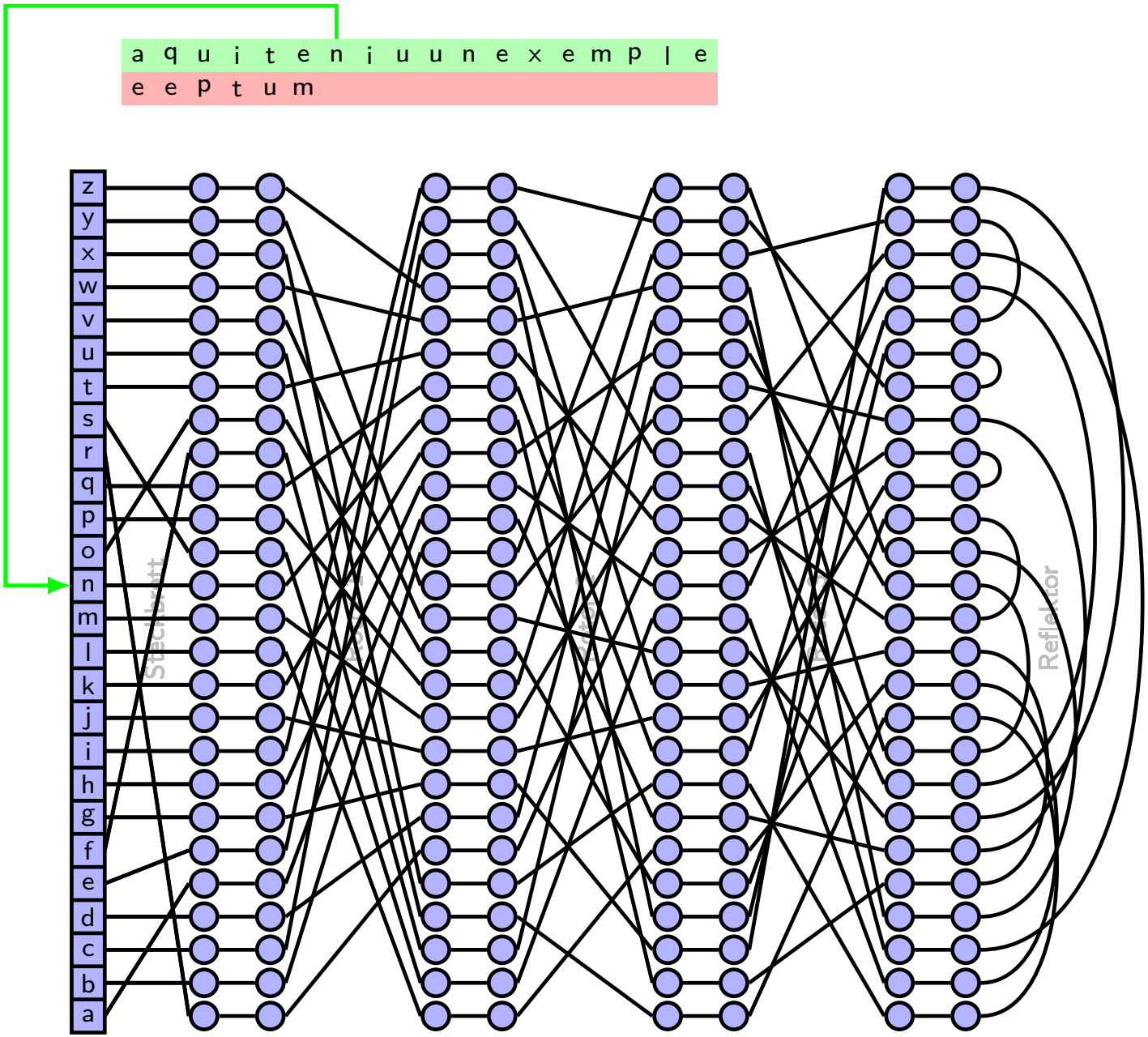
Funcionament de la màquina Enigma



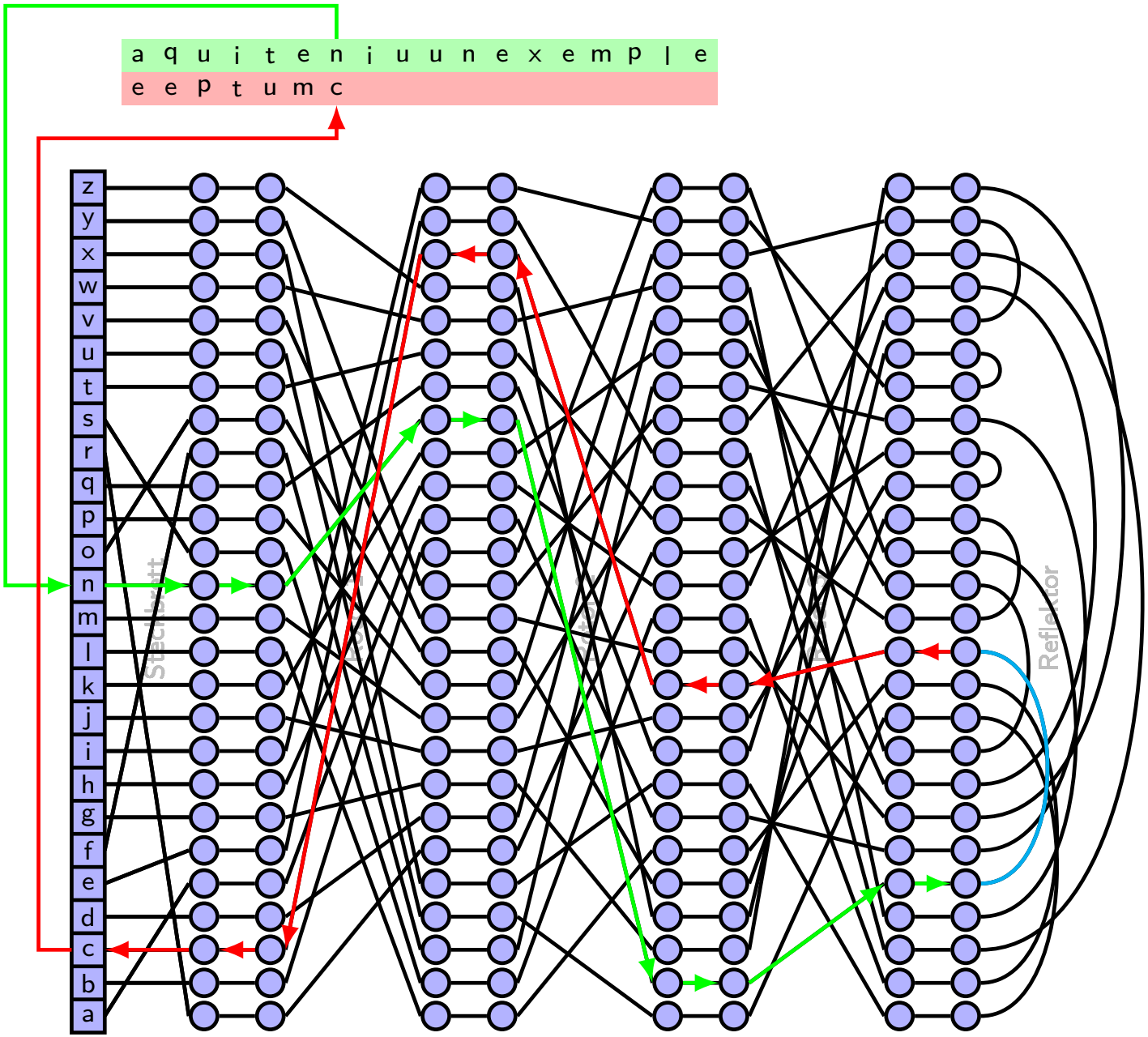
Funcionament de la màquina Enigma



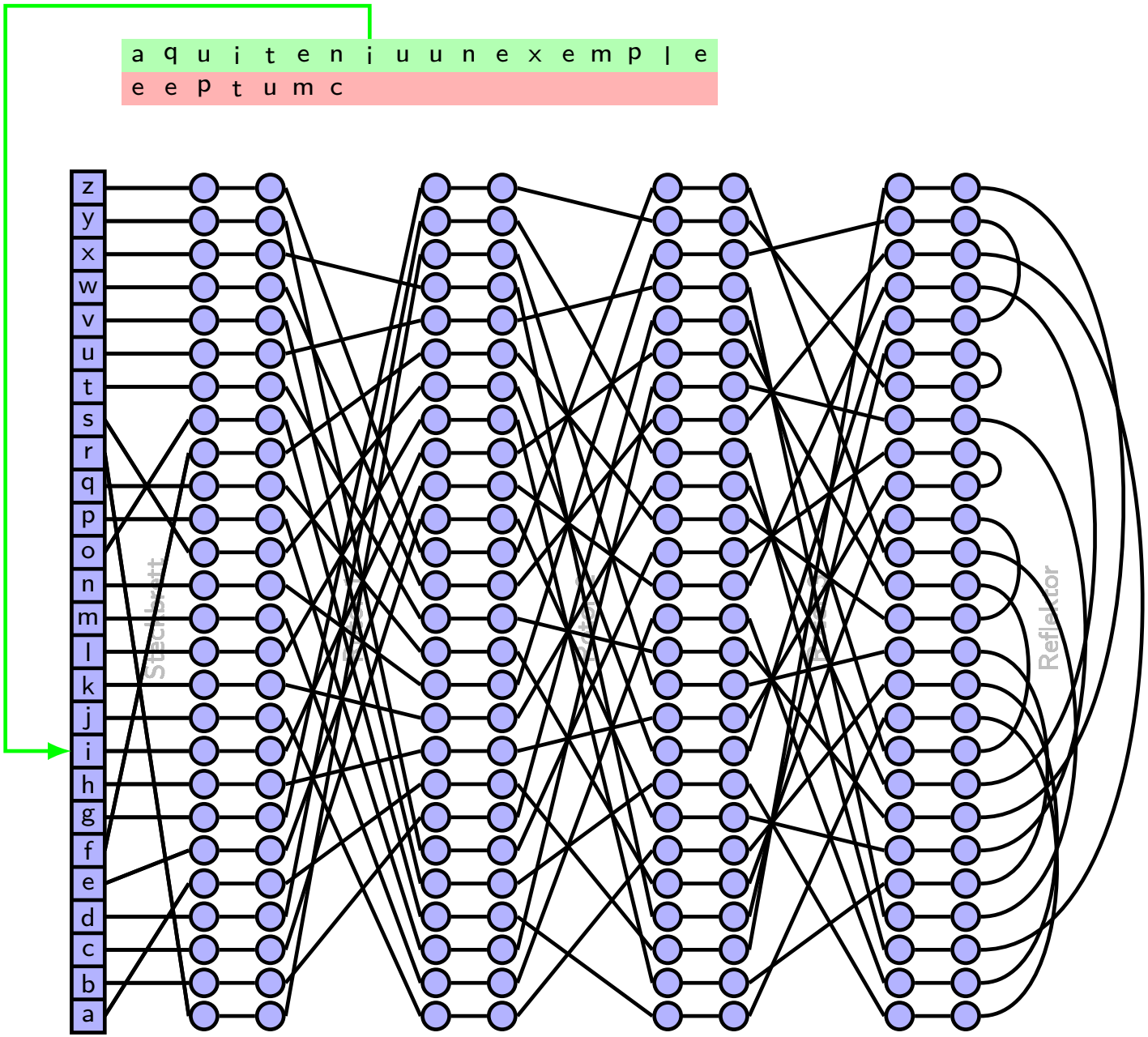
Funcionament de la màquina Enigma



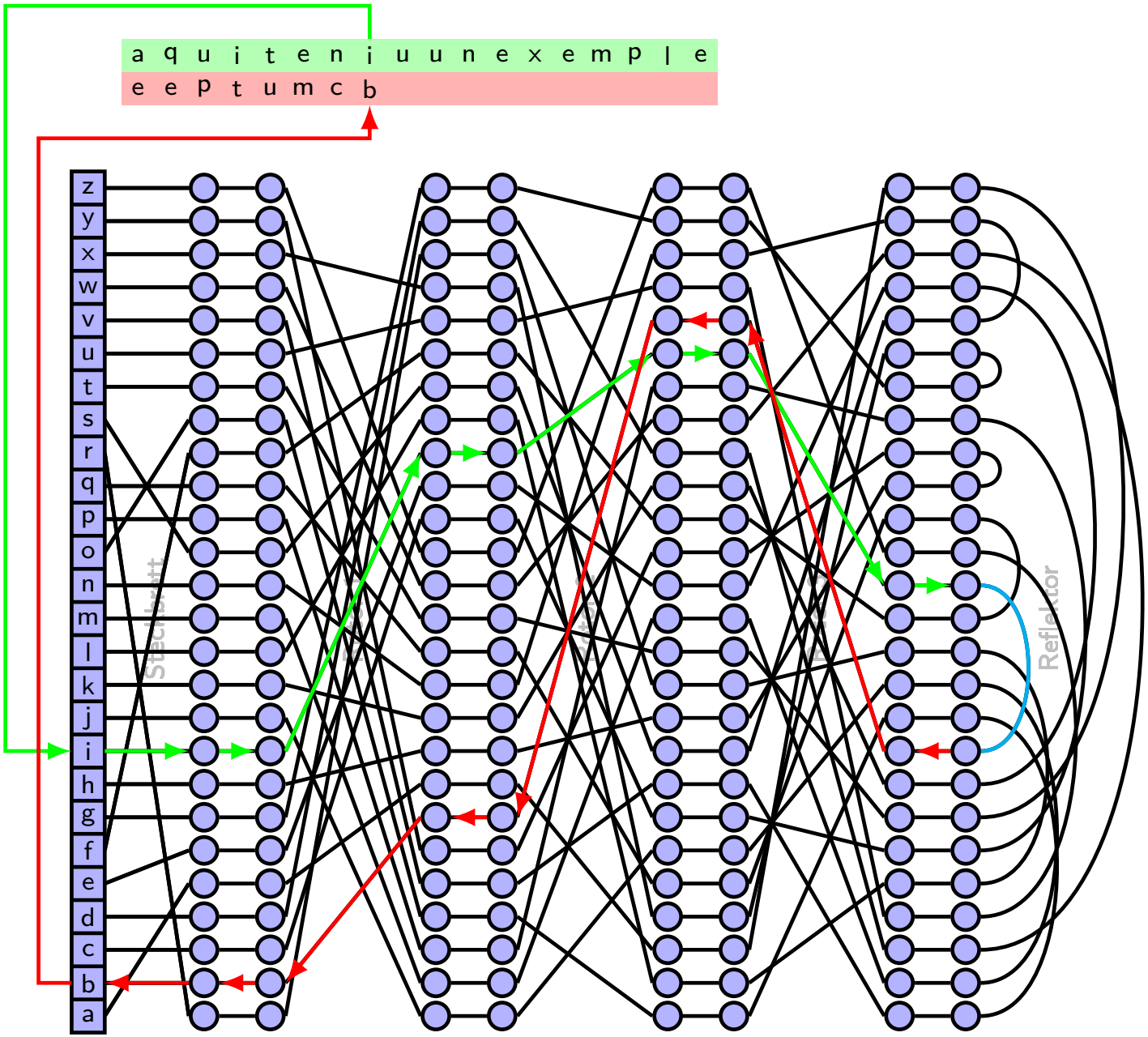
Funcionament de la màquina Enigma



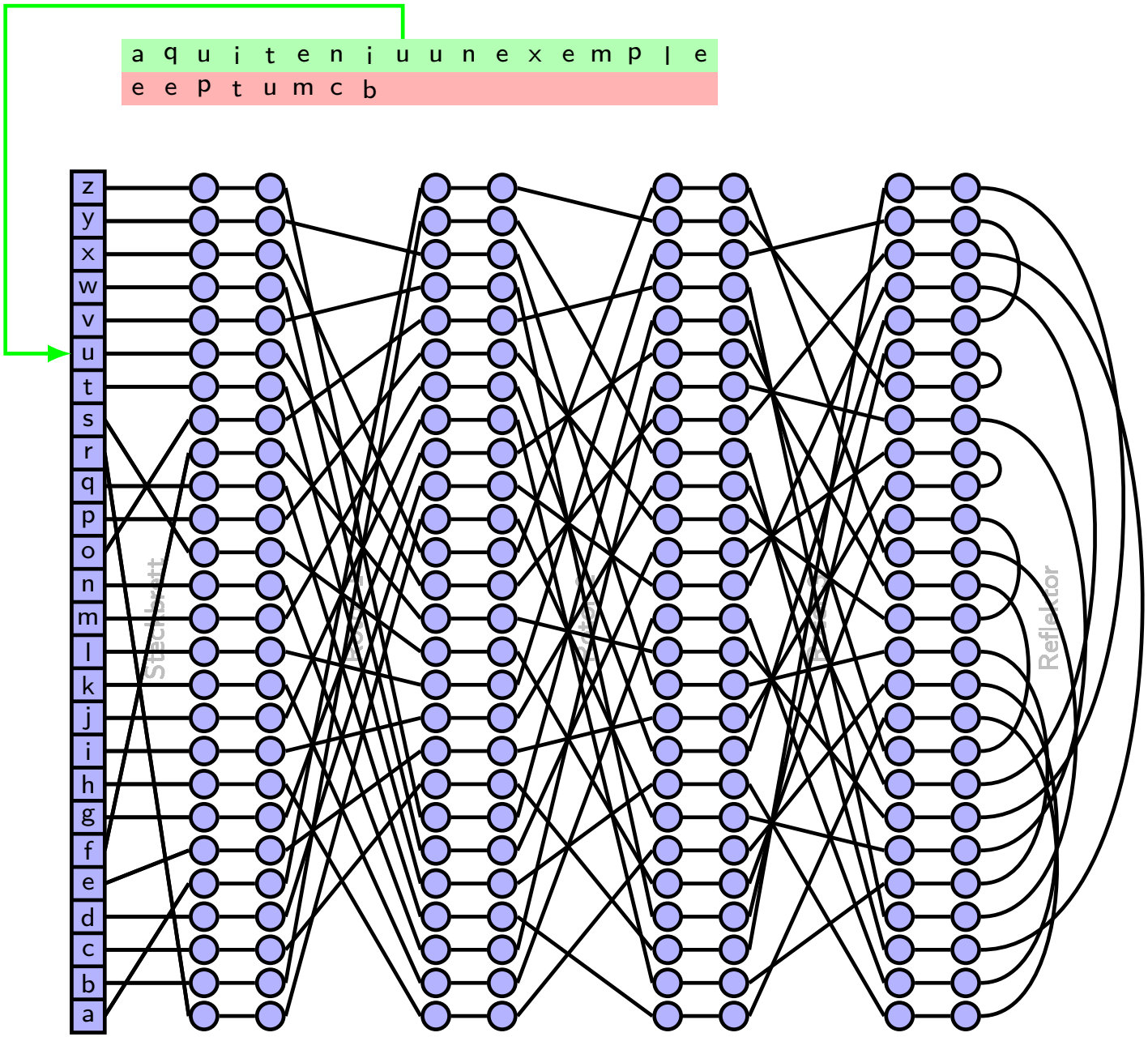
Funcionament de la màquina Enigma



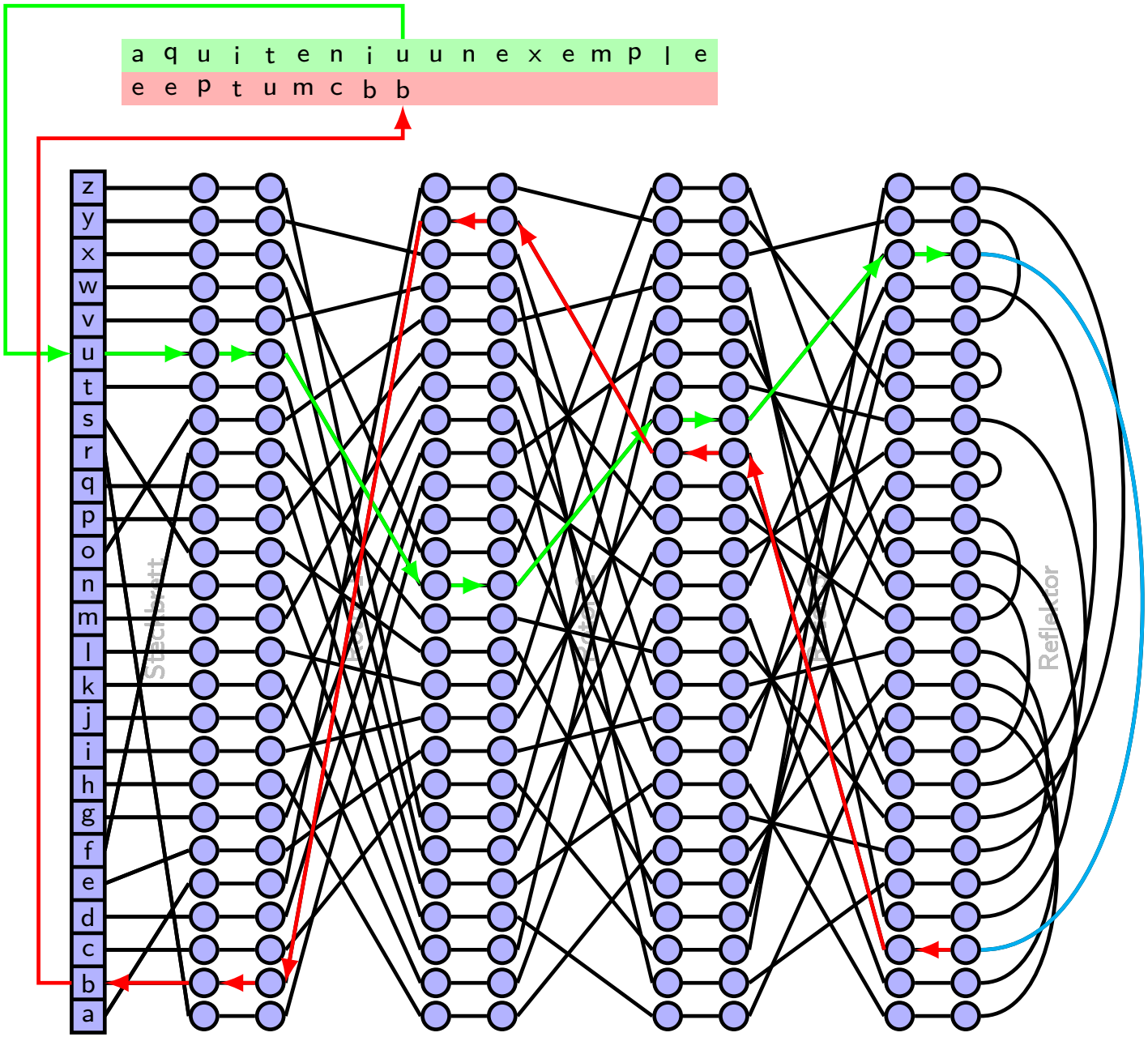
Funcionament de la màquina Enigma



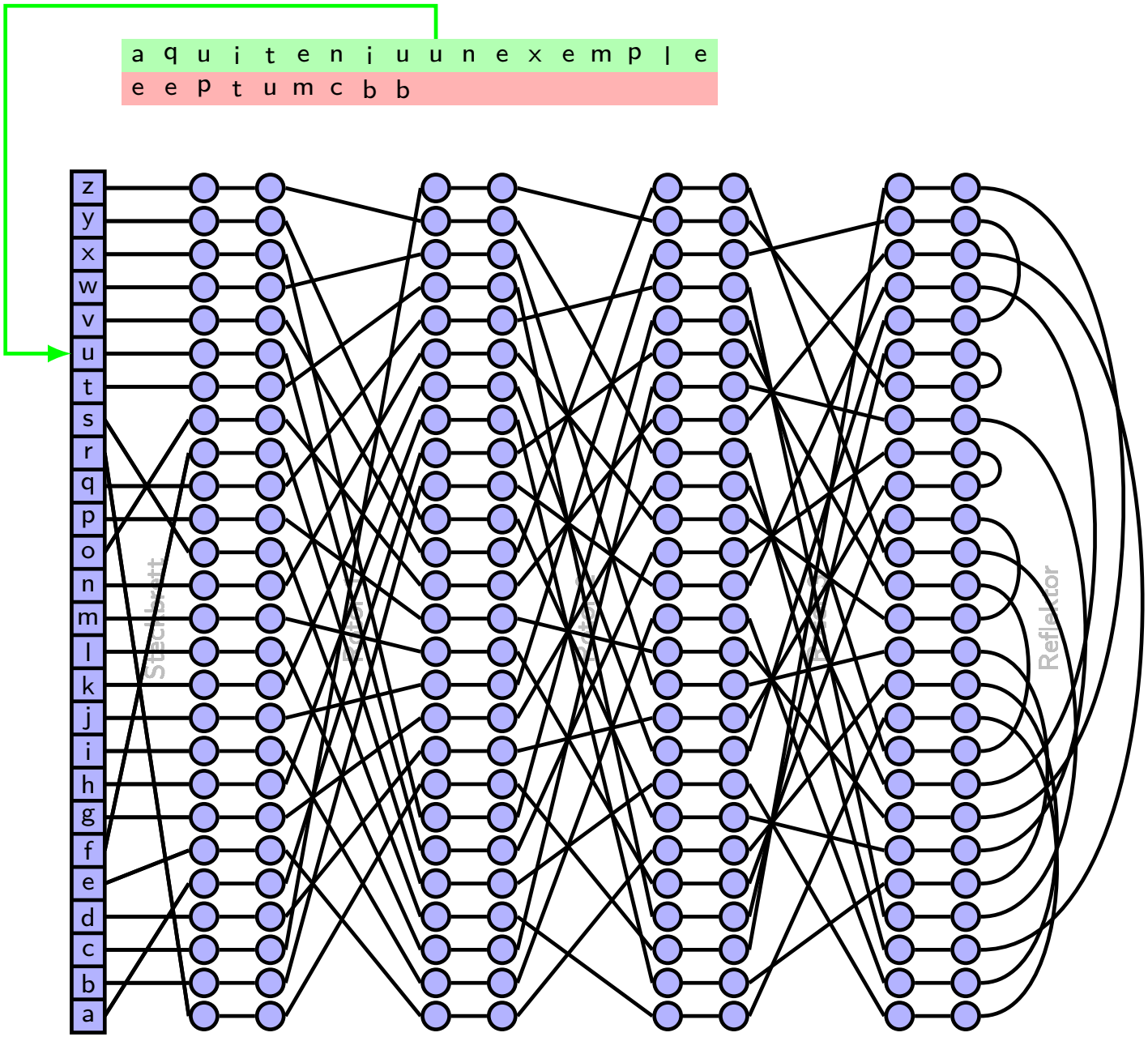
Funcionament de la màquina Enigma



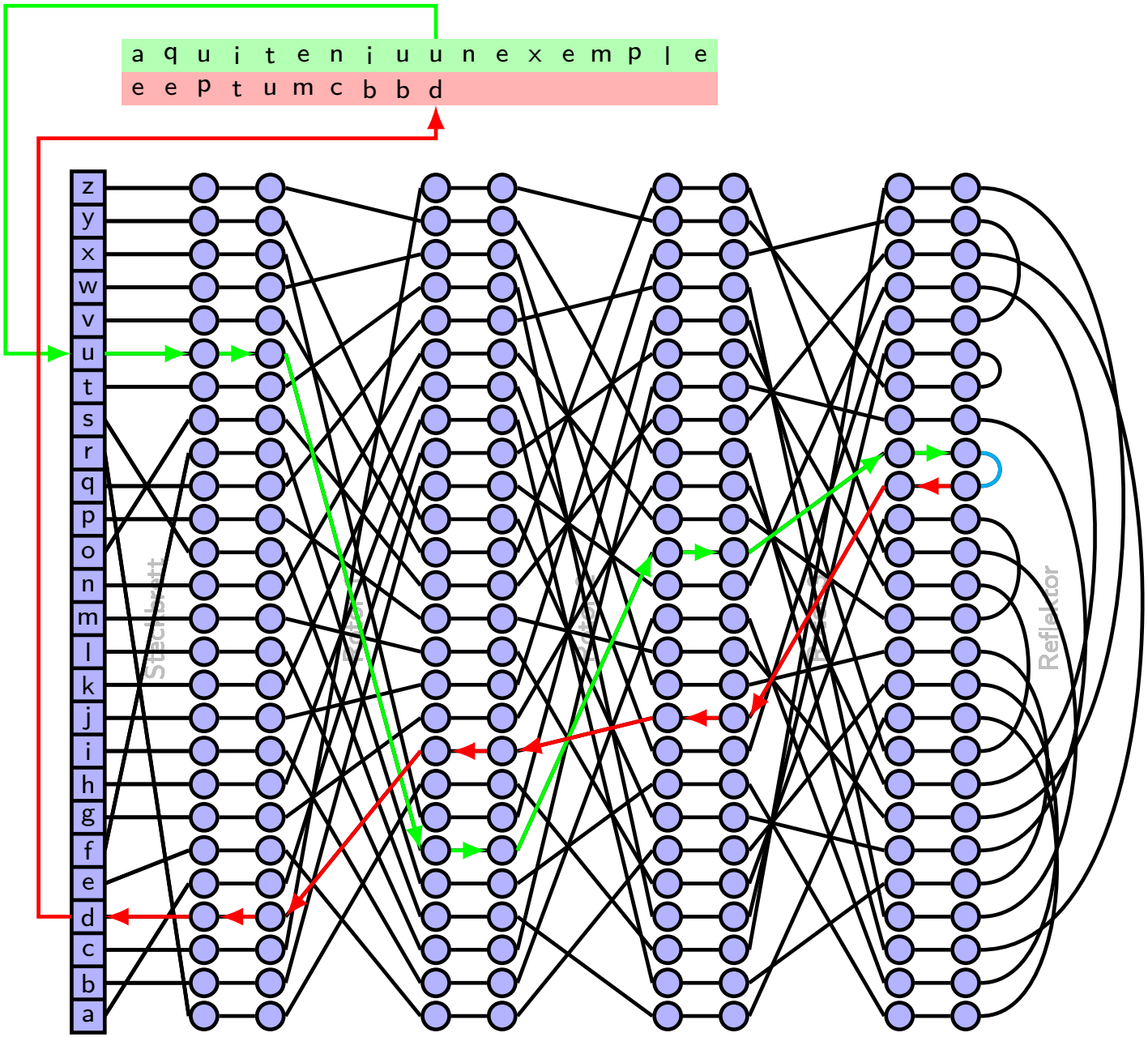
Funcionament de la màquina Enigma



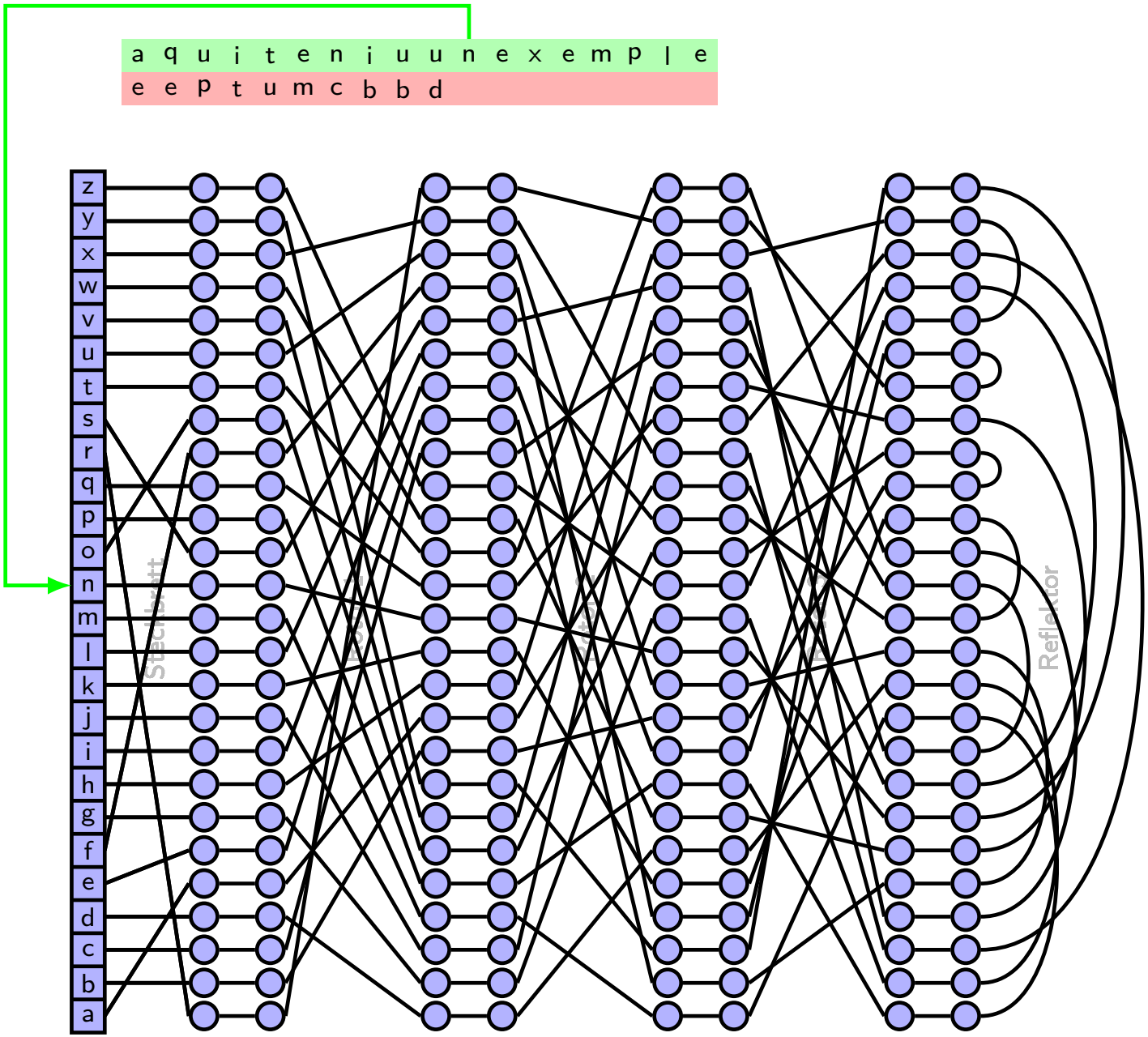
Funcionament de la màquina Enigma



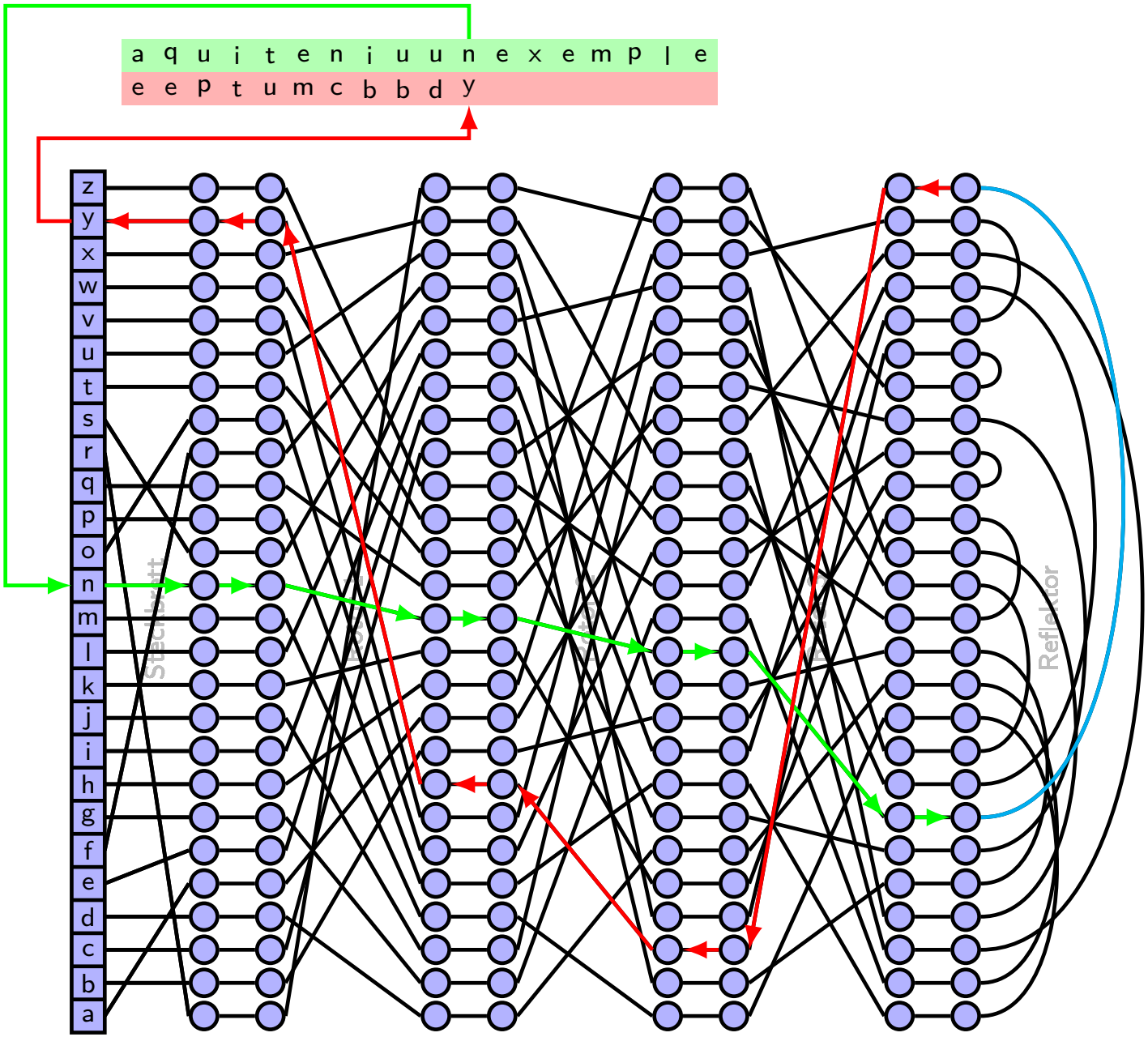
Funcionament de la màquina Enigma



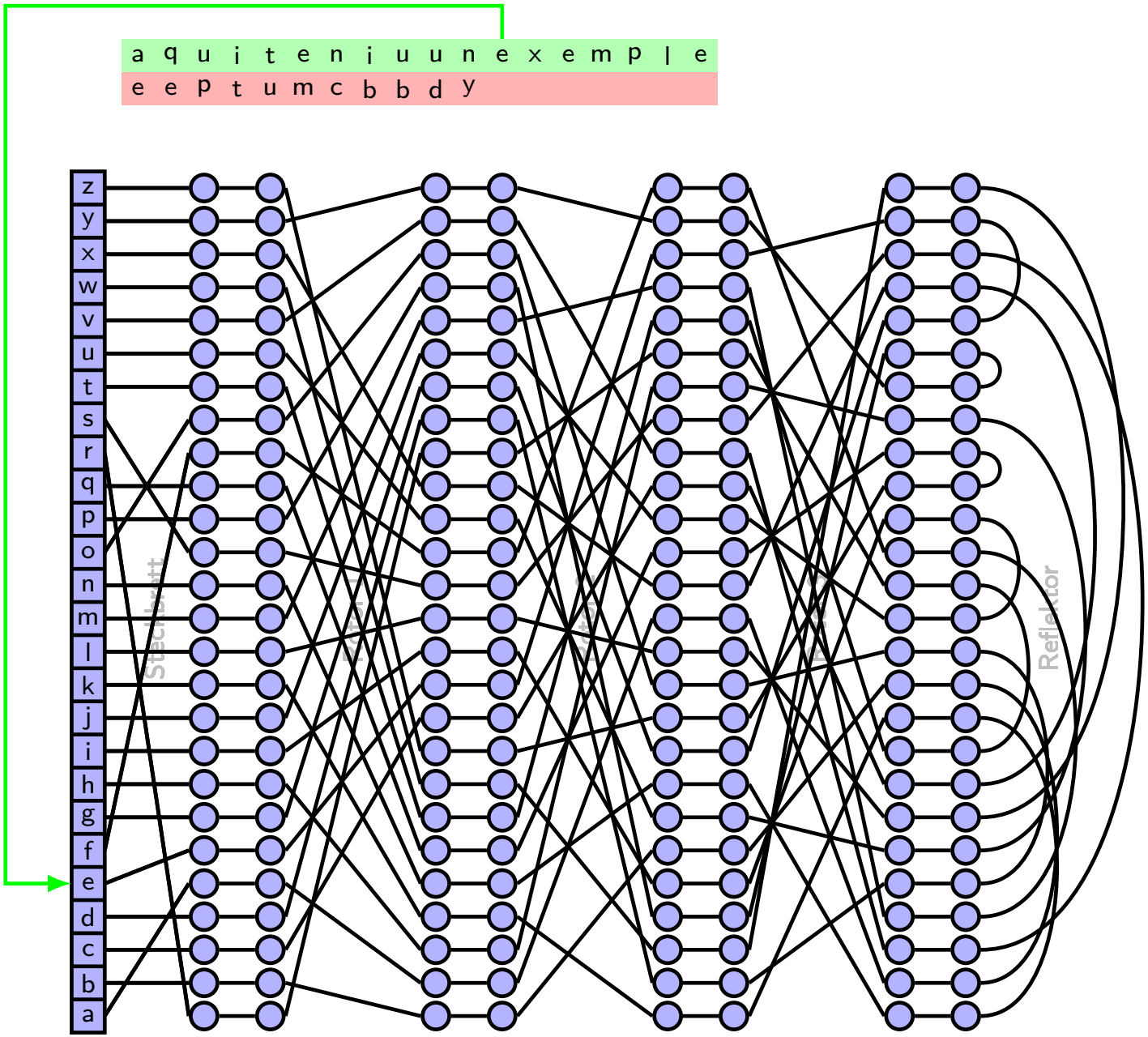
Funcionament de la màquina Enigma



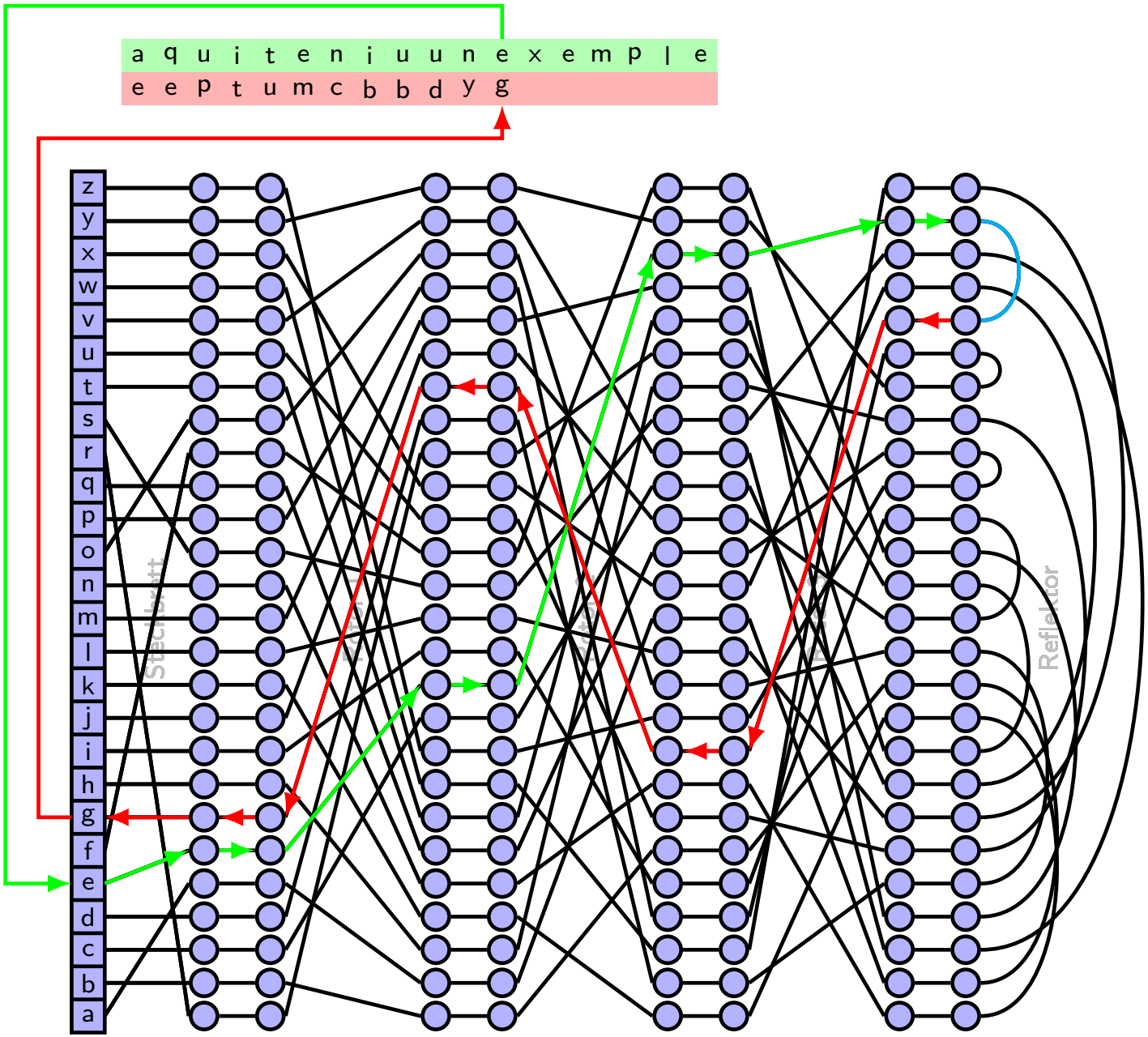
Funcionament de la màquina Enigma



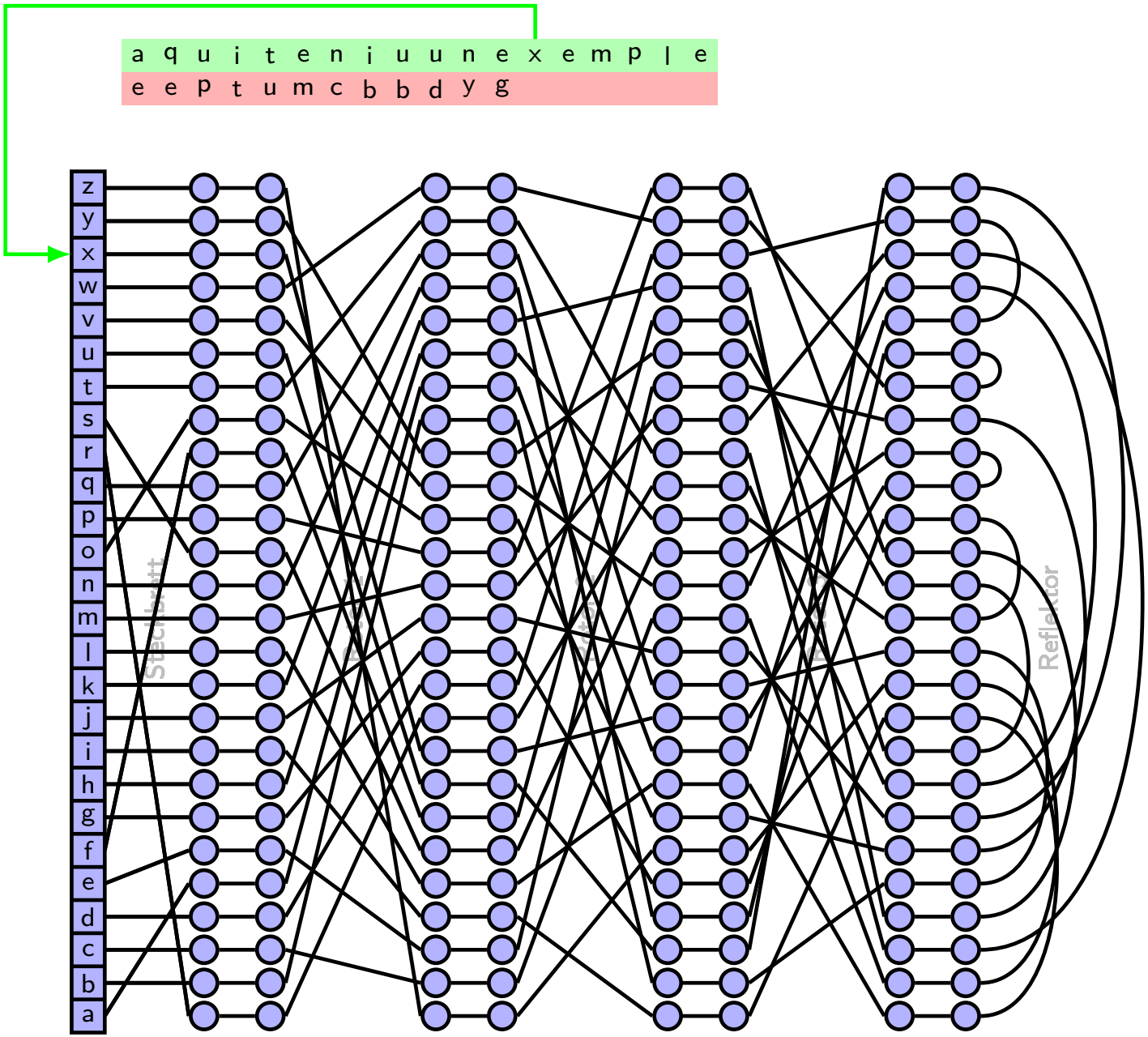
Funcionament de la màquina Enigma



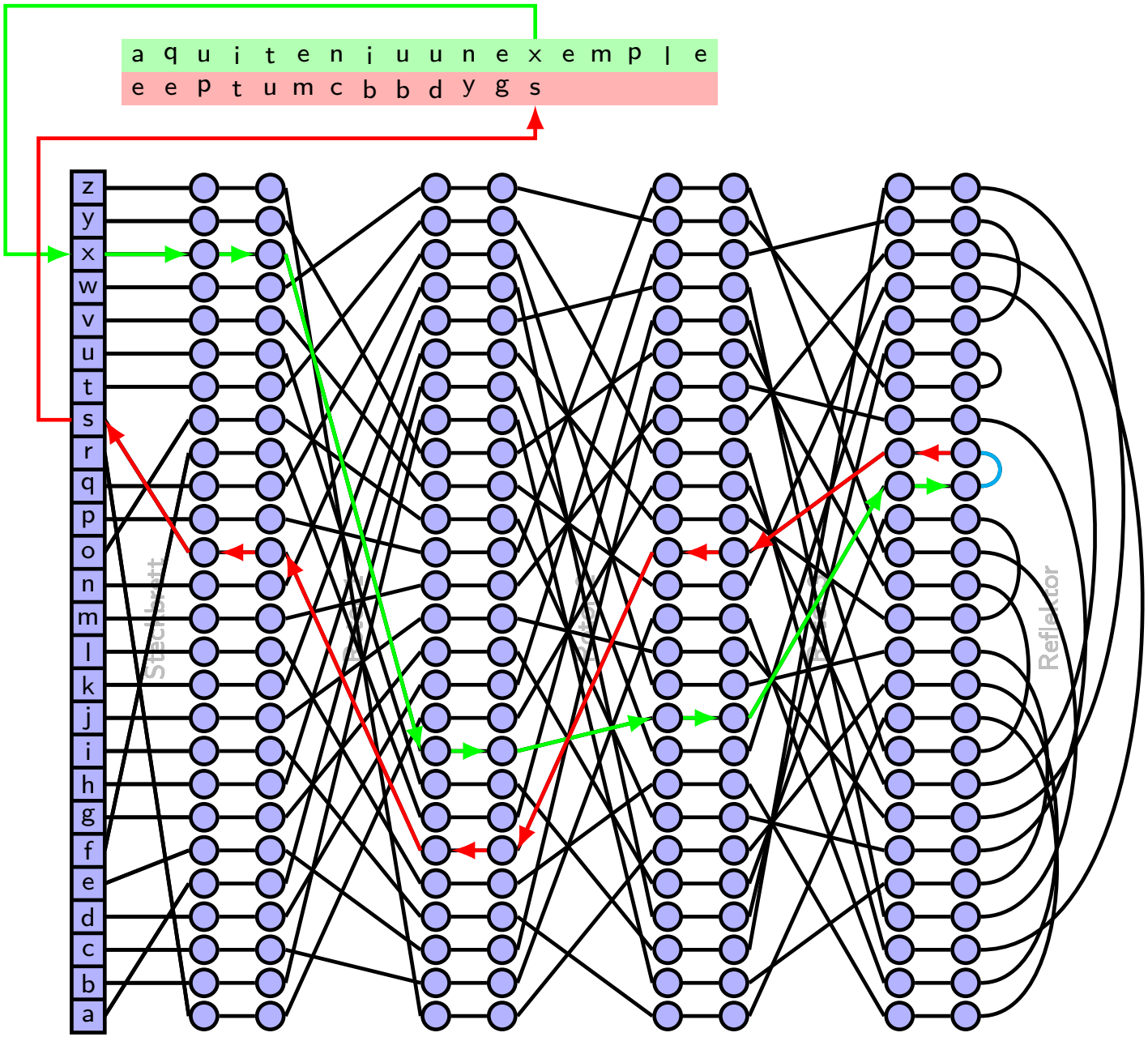
Funcionament de la màquina Enigma



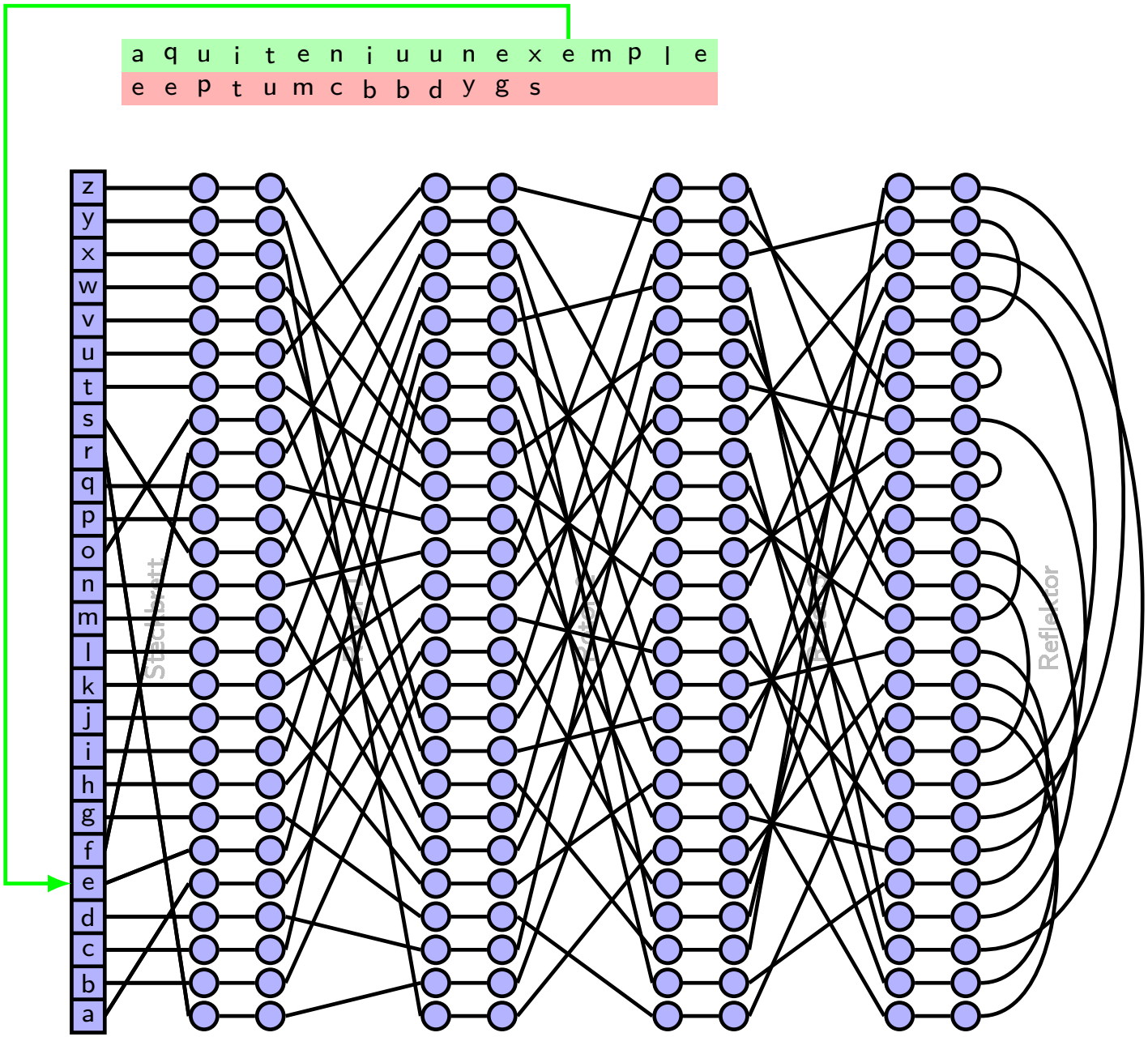
Funcionament de la màquina Enigma



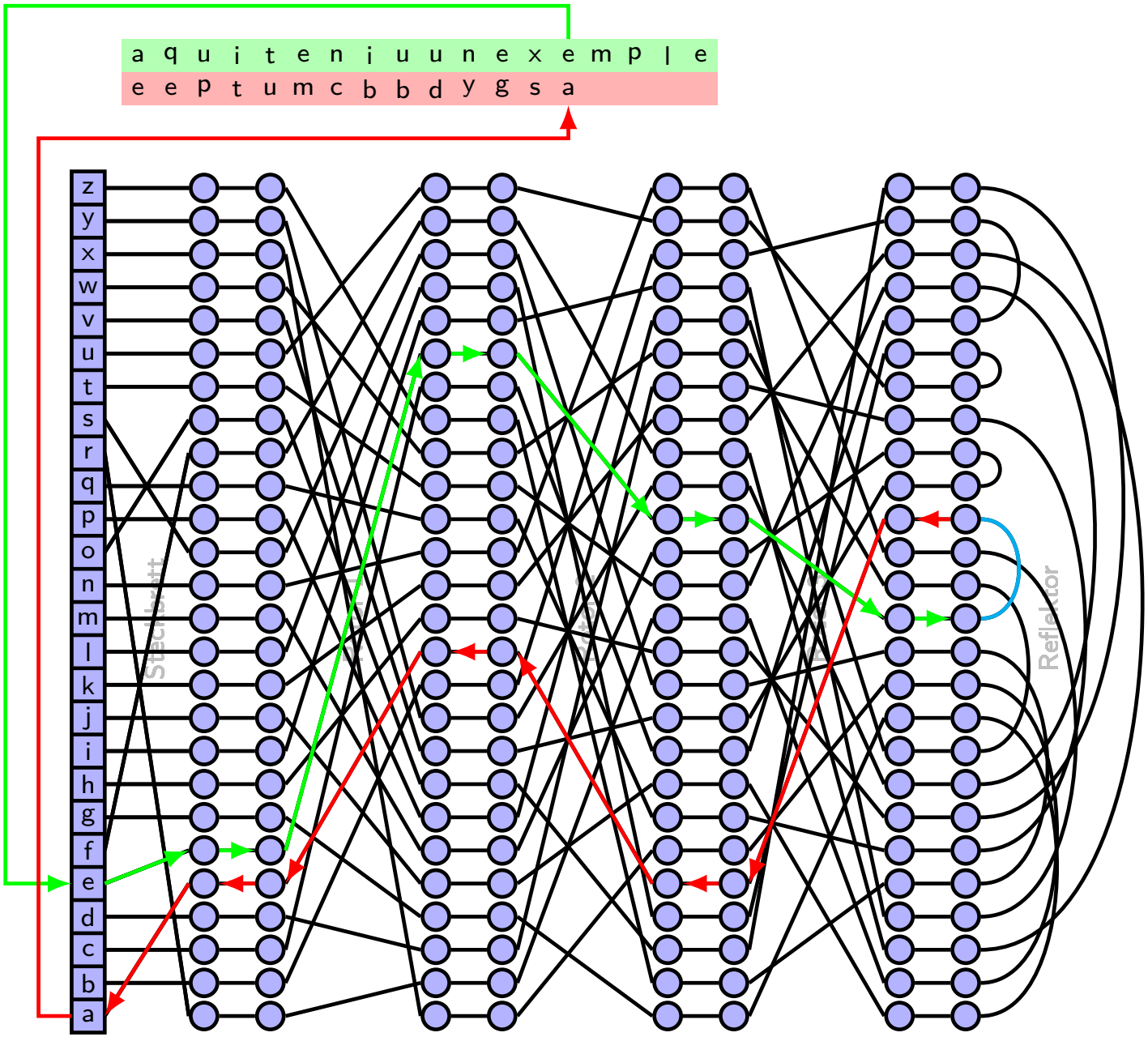
Funcionament de la màquina Enigma



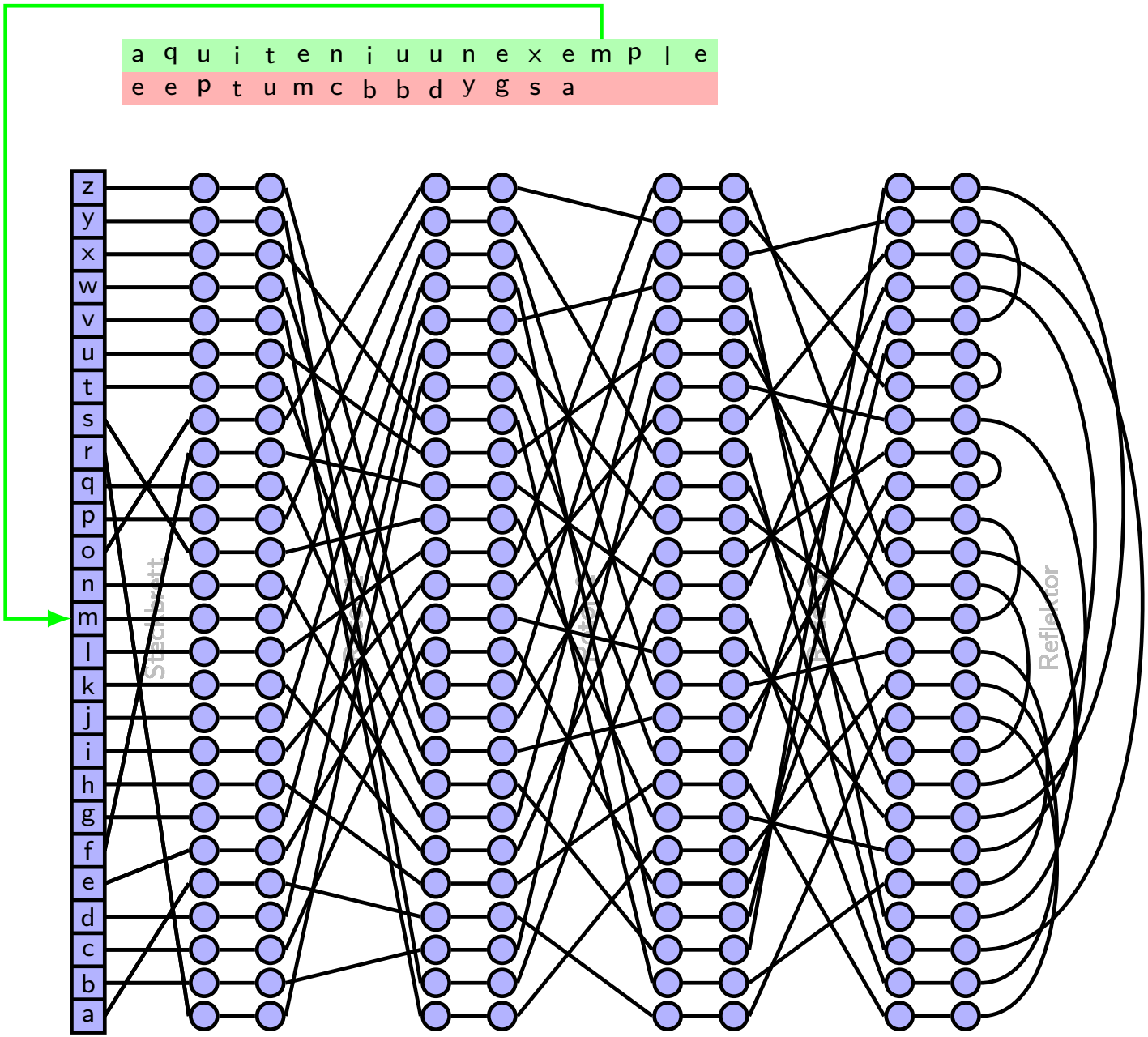
Funcionament de la màquina Enigma



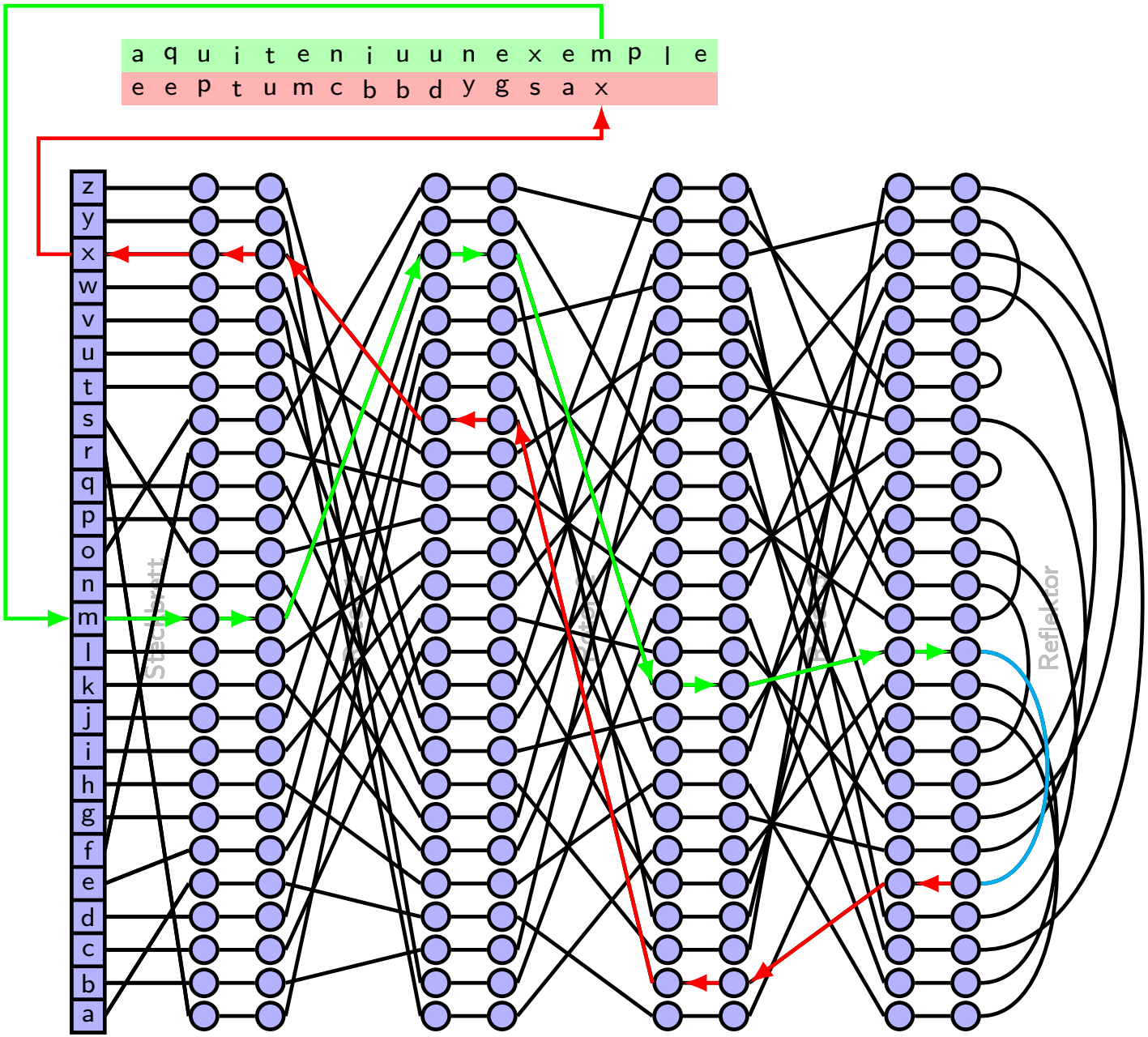
Funcionament de la màquina Enigma



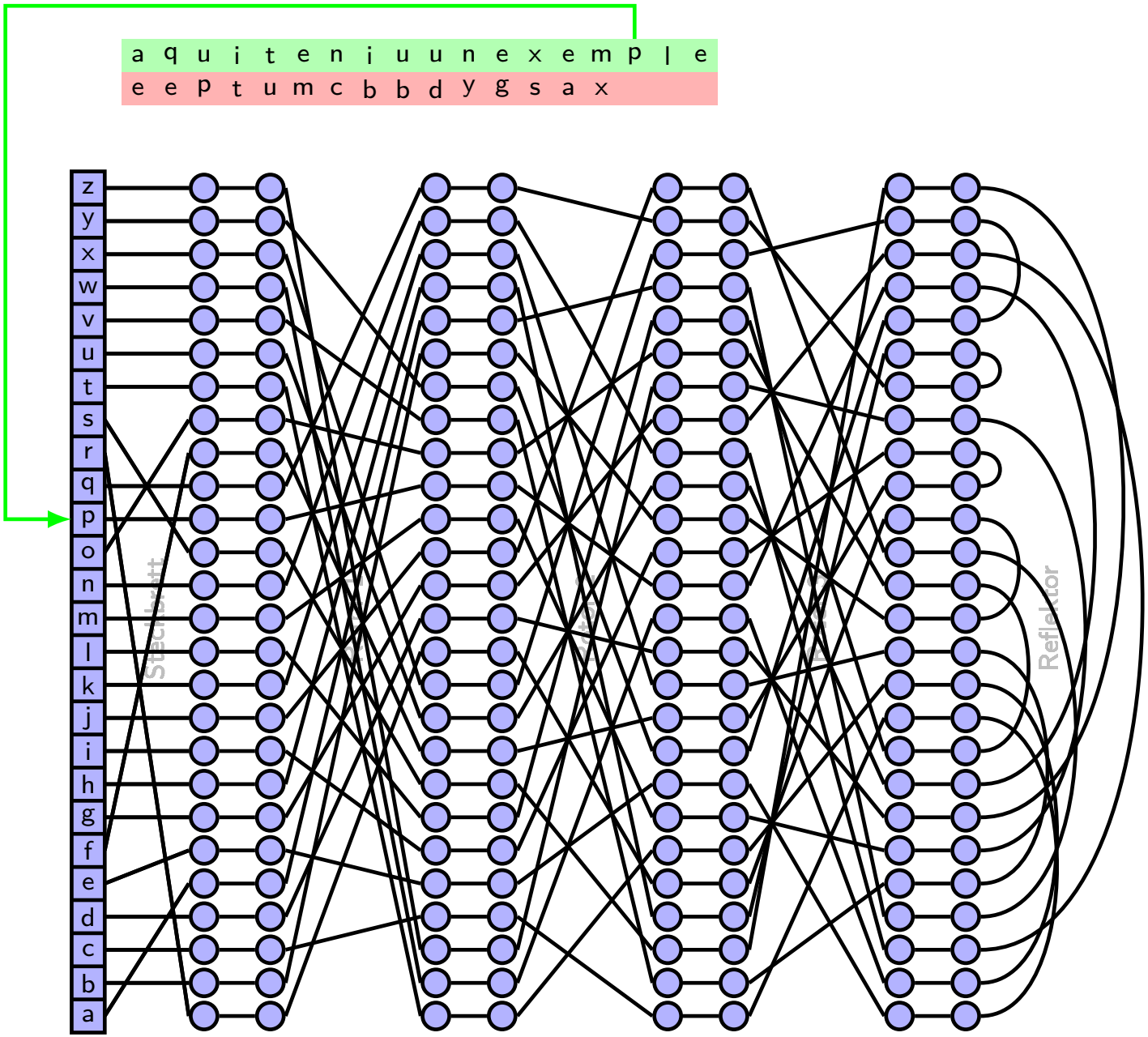
Funcionament de la màquina Enigma



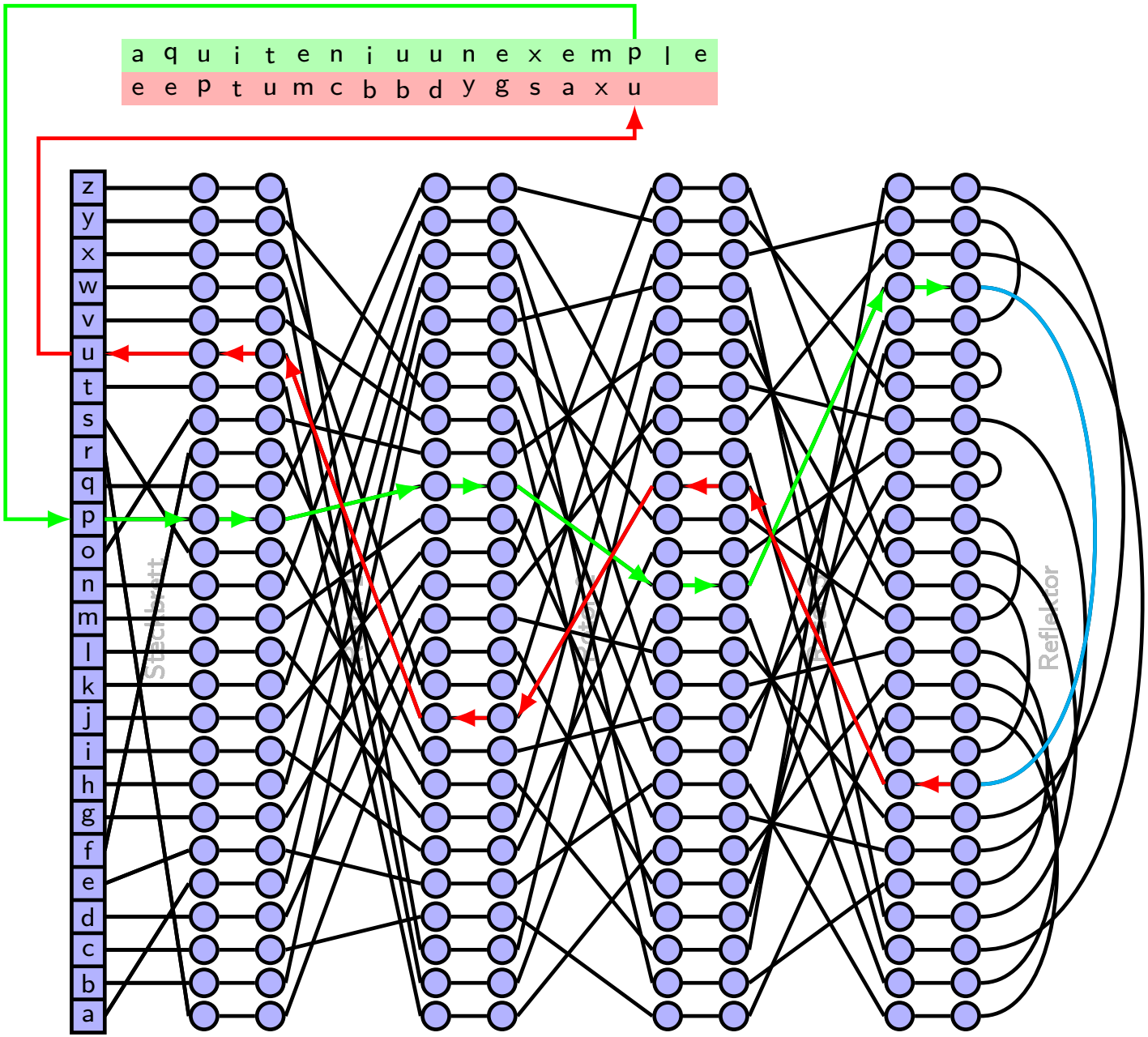
Funcionament de la màquina Enigma



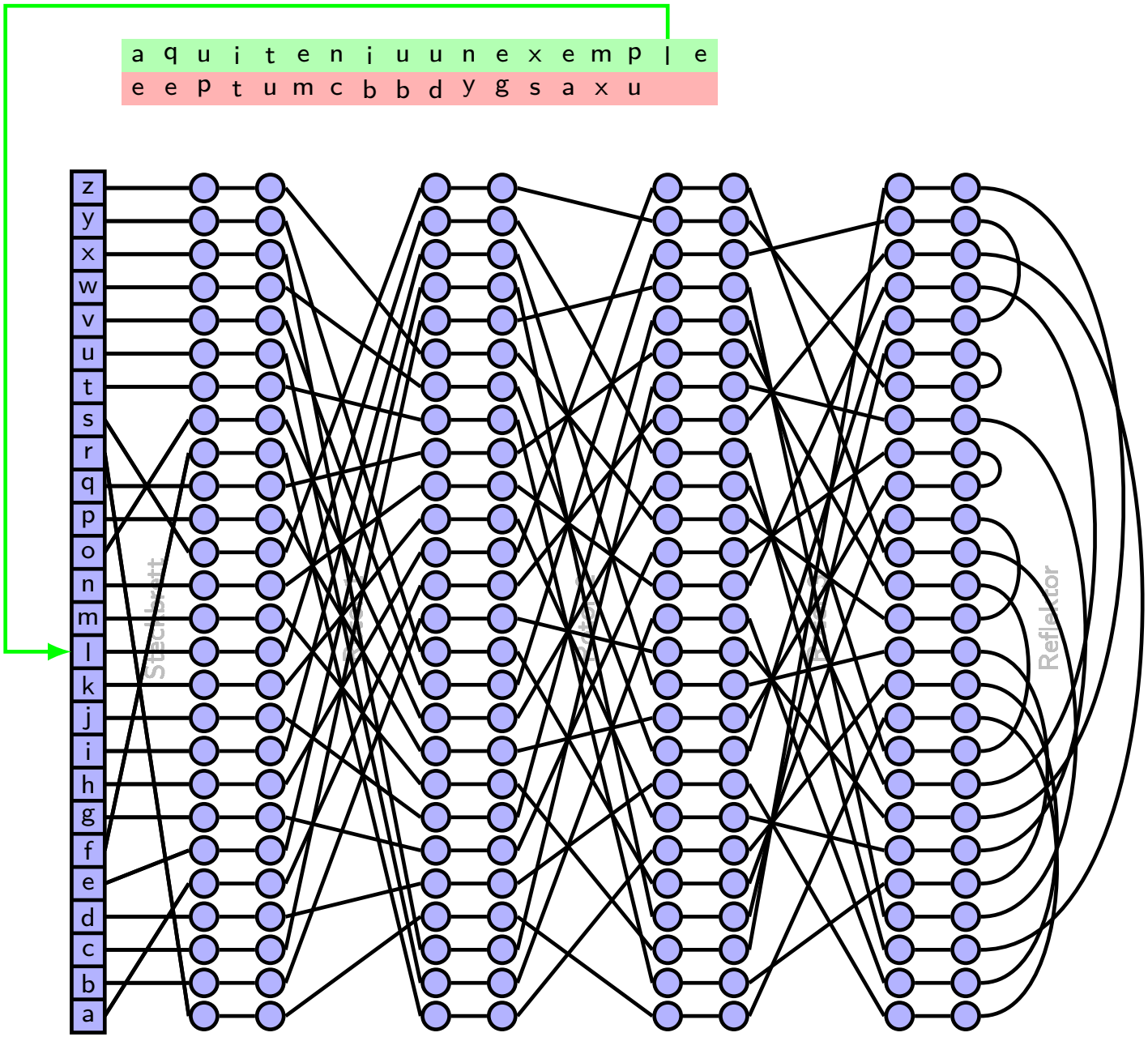
Funcionament de la màquina Enigma



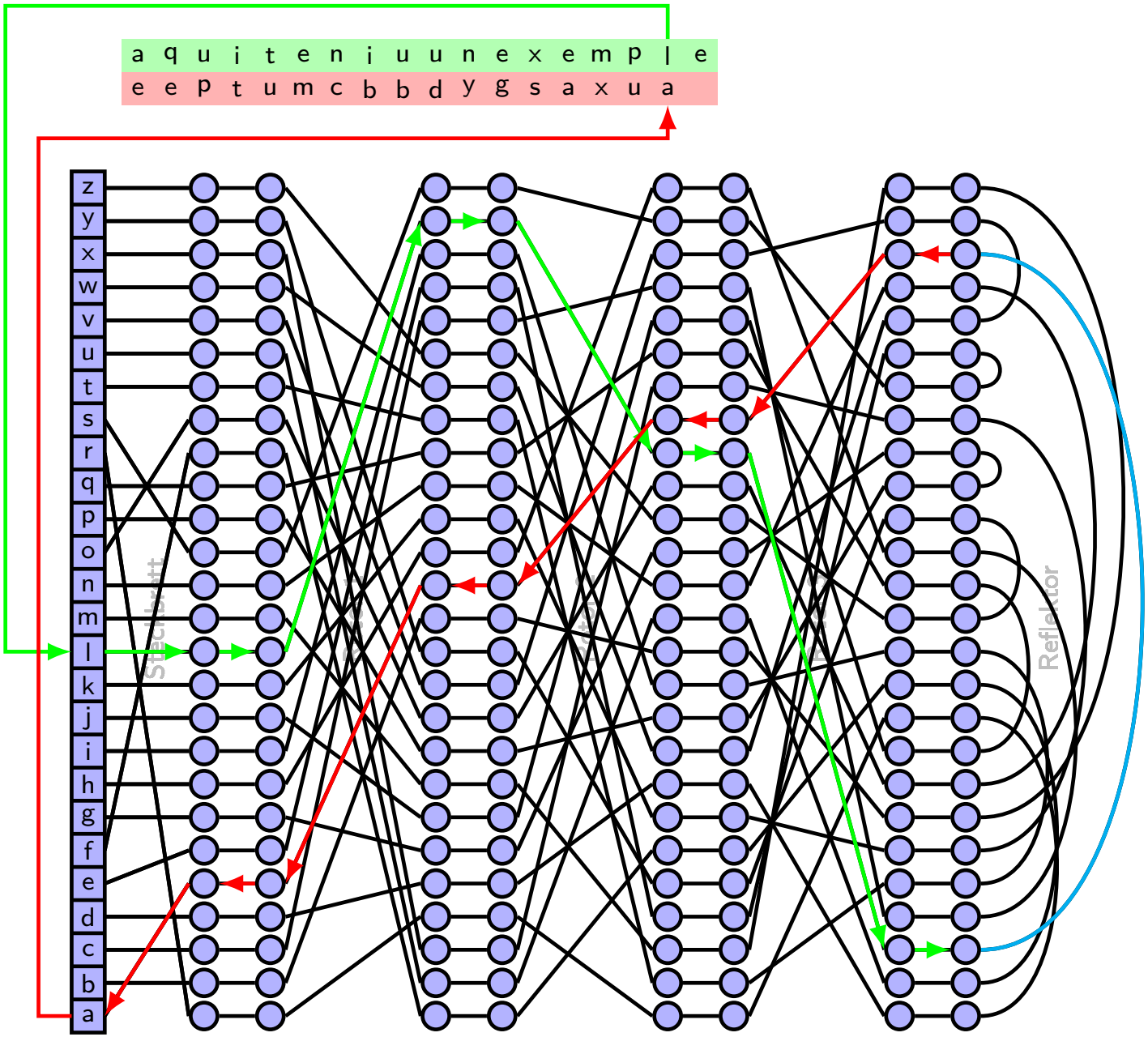
Funcionament de la màquina Enigma



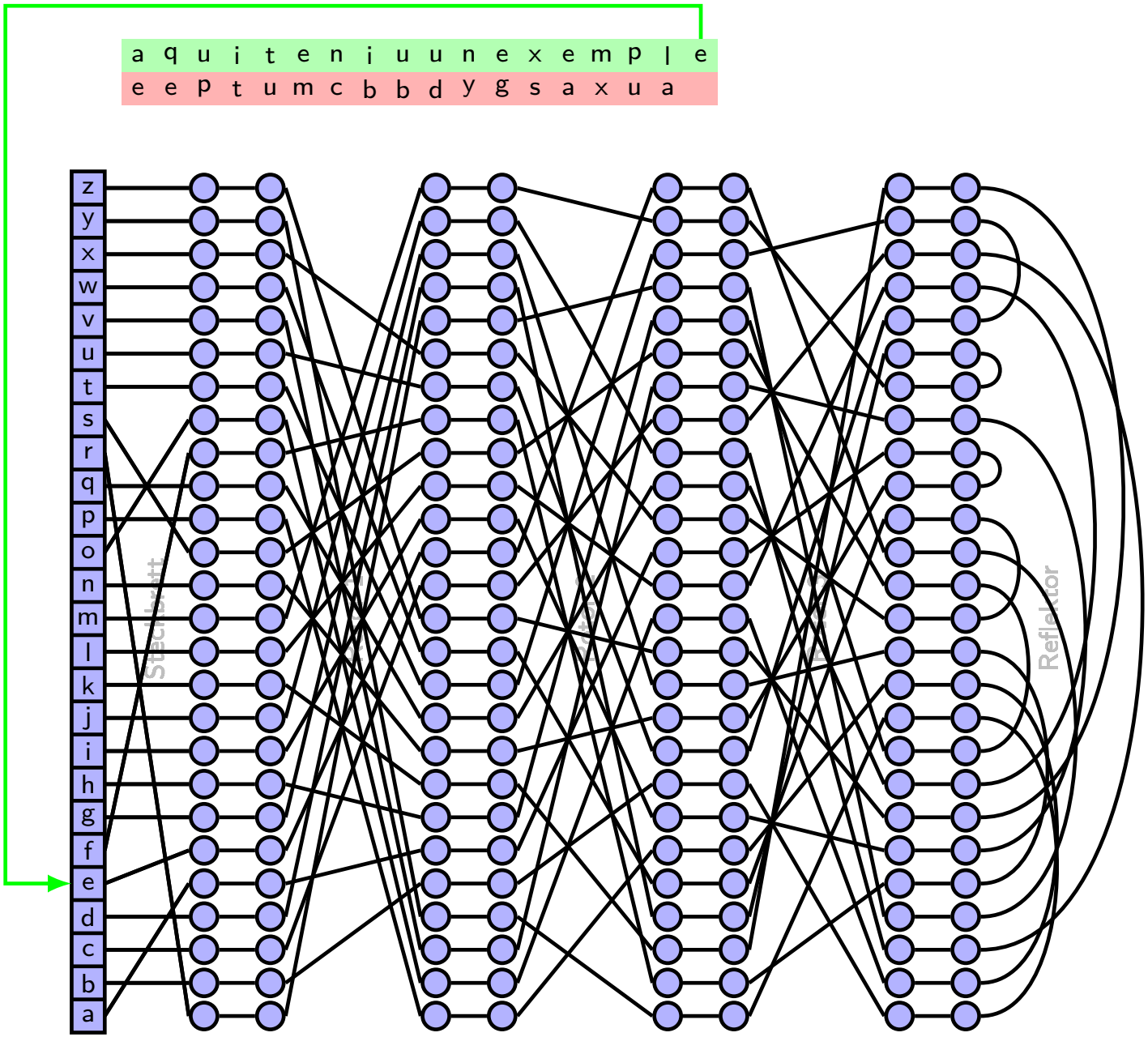
Funcionament de la màquina Enigma



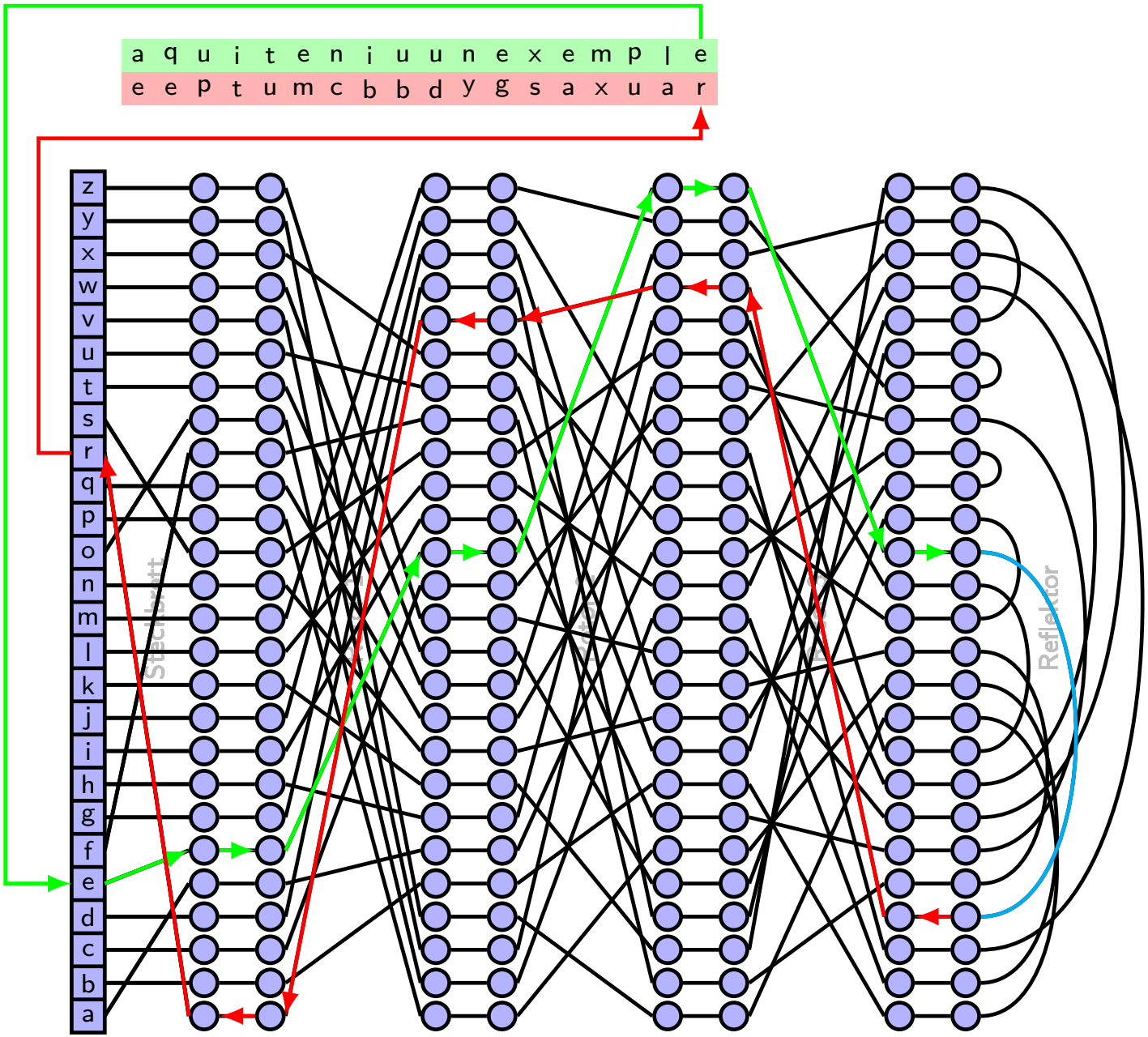
Funcionament de la màquina Enigma



Funcionament de la màquina Enigma



Funcionament de la màquina Enigma



Màquina Enigma feta amb un pot de Pringles

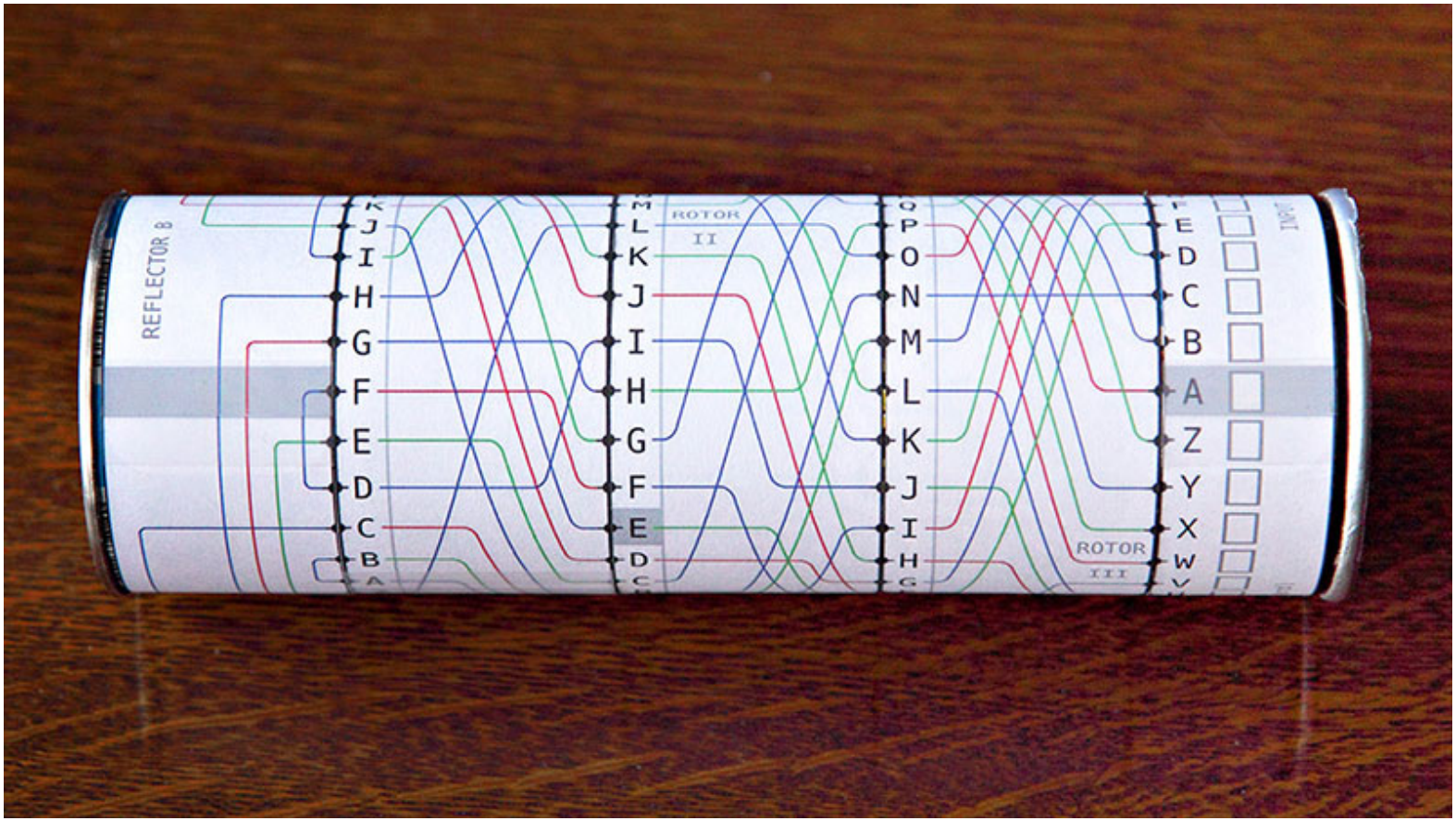


Figure: Màquina Enigma feta amb pot de Pringles

En tots els mètodes explicats...

En tots els mètodes explicats...

- La robustesa del secret depen del secret de la clau

criptografia moderna

En tots els mètodes explicats...

- La robustesa del secret depen del secret de la clau
- Dificultat de transmisió de claus

criptografia moderna

En tots els mètodes explicats...

- La robustesa del secret depen del secret de la clau
- Dificultat de transmisió de claus

No es poden solucionar aquest problemes?

Criptografia de clau pública

Criptografia de clau pública

- La criptografia de clau pública neix el 1.976

Criptografia de clau pública

- La criptografia de clau pública neix el 1.976
- Es basa en que la clau per xifrar és pública i és diferent de la clau per desxifrar.

Criptografia de clau pública

- La criptografia de clau pública neix el 1.976
- Es basa en que la clau per xifrar és pública i és diferent de la clau per desxifrar.
- Basat en funcions trampa: Molt senzilles en una direcció i molt complicades en l'altra direcció a no ser que es tingui informació addicional.

Criptografia de clau pública: Exemple senzill

Criptografia de clau pública: Exemple senzill

- La meva clau pública és el llistí de telèfons de Barcelona.

Criptografia de clau pública: Exemple senzill

- La meva clau pública és el llistí de telèfons de Barcelona.

Criptografia de clau pública: Exemple senzill

- La meva clau pública és el llistí de telèfons de Barcelona.

- Si algú em vol enviar un missatge substitueixi cada lletra que em vulgui enviar per el telèfon d'algú que el seu cognom comenci per aquella lletra

Criptografia de clau pública: Exemple senzill

- La meva clau pública és el llistí de telèfons de Barcelona.

- Si algú em vol enviar un missatge substitueixi cada lletra que em vulgui enviar per el telèfon d'algú que el seu cognom comenci per aquella lletra
- Xifrar és molt senzill....

Criptografia de clau pública: Exemple senzill

- La meva clau pública és el llistí de telèfons de Barcelona.

- Si algú em vol enviar un missatge substitueixi cada lletra que em vulgui enviar per el telèfon d'algú que el seu cognom comenci per aquella lletra
- Xifrar és molt senzill....
- Però desxifrar és de bojos!!!!

Criptografia de clau pública: Exemple senzill

- La meva clau pública és el llistí de telèfons de Barcelona.

- Si algú em vol enviar un missatge substitueixi cada lletra que em vulgui enviar per el telèfon d'algú que el seu cognom comenci per aquella lletra
- Xifrar és molt senzill....
- Però desxifrar és de bojos!!!!
- ...excepte per a mi, que tinc un llistí ordenat per nombres de telèfon (clau privada)

Complexitat computacional

Què vol dir que un problema és difícil?

Complexitat computacional

Què vol dir que un problema és difícil?

- La complexitat computacional estudia la "dificultat" dels problemes en termes del temps d'execució del millor algorisme possible que els pugui resoldre.

Complexitat computacional

Què vol dir que un problema és difícil?

- La complexitat computacional estudia la "dificultat" dels problemes en termes del temps d'execució del millor algorisme possible que els pugui resoldre.
- El temps d'execució d'un algorisme $t(n)$ és una funció creixent del volum de dades entrada n.

Complexitat computacional

Què vol dir que un problema és difícil?

- La complexitat computacional estudia la "dificultat" dels problemes en termes del temps d'execució del millor algorisme possible que els pugui resoldre.
- El temps d'execució d'un algorisme $t(n)$ és una funció creixent del volum de dades entrada n.
  Habitualment es tindrà que $\lim_{n\to\infty} t(n) = \infty$.

Complexitat computacional

Què vol dir que un problema és difícil?

- La complexitat computacional estudia la "dificultat" dels problemes en termes del temps d'execució del millor algorisme possible que els pugui resoldre.
- El temps d'execució d'un algorisme $t(n)$ és una funció creixent del volum de dades entrada n.
  Habitualment es tindrà que $\lim_{n\to\infty} t(n) = \infty$.
- Interesa coneixer com és aquest creixement.

Complexitat computacional

Què vol dir que un problema és difícil?

- La complexitat computacional estudia la "dificultat" dels problemes en termes del temps d'execució del millor algorisme possible que els pugui resoldre.
- El temps d'execució d'un algorisme $t(n)$ és una funció creixent del volum de dades entrada n.
  Habitualment es tindrà que $\lim_{n\to\infty} t(n) = \infty$.
- Interesa coneixer com és aquest creixement.
  No és el mateix $t(n) = \mathcal{O}(n^k)$ que $t(n) = \mathcal{O}(2^n)$

Complexitat computacional

Què vol dir que un problema és difícil?

- La complexitat computacional estudia la "dificultat" dels problemes en termes del temps d'execució del millor algorisme possible que els pugui resoldre.
- El temps d'execució d'un algorisme $t(n)$ és una funció creixent del volum de dades entrada n.
  Habitualment es tindrà que $\lim_{n\to\infty} t(n) = \infty$.
- Interesa coneixer com és aquest creixement.
  No és el mateix $t(n) = \mathcal{O}(n^k)$ que $t(n) = \mathcal{O}(2^n)$
- Els problemes es poden classificar en classes segons la seva complexitat computacional (P, NP, NP-hard,....)

Complexitat: Factorització de nombres enters

- L'algorisme més eficient que es coneix per factoritzar un nombre que és producte de dos primers:

$$\mathcal{O}\left(e^{\sqrt[3]{\frac{64}{9}b\log^2(b)}}\right)$$

Complexitat: Factorització de nombres enters

- L'algorisme més eficient que es coneix per factoritzar un nombre que és producte de dos primers:

$$\mathcal{O}\left(e^{\sqrt[3]{\frac{64}{9}b\log^2(b)}}\right)$$

on b és el nombre de bits necessaris per a codificar el nombre a factoritzar

Complexitat: Factorització de nombres enters

- L'algorisme més eficient que es coneix per factoritzar un nombre que és producte de dos primers:

$$\mathcal{O}\left(e^{\sqrt[3]{\frac{64}{9}b\log^2(b)}}\right)$$

  on b és el nombre de bits necessaris per a codificar el nombre a factoritzar

- Evidentment el temps d'execució deprendrà de l'eficiència de la implementació i de la potència de l'ordinador

Complexitat: Factorització de nombres enters

- L'algorisme més eficient que es coneix per factoritzar un nombre que és producte de dos primers:

$$\mathcal{O}\left(e^{\sqrt[3]{\frac{64}{9}b\log^2(b)}}\right)$$

  on b és el nombre de bits necessaris per a codificar el nombre a factoritzar

- Evidentment el temps d'execució deprendrà de l'eficiència de la implementació i de la potència de l'ordinador

- Suposem que volem factoritzar un nombre que es producte de dos primers de 500 xifres...

Complexitat: Factorització de nombres enters

- L'algorisme més eficient que es coneix per factoritzar un nombre que és producte de dos primers:

$$\mathcal{O}\left(e^{\sqrt[3]{\frac{64}{9}b\log^2(b)}}\right)$$

  on b és el nombre de bits necessaris per a codificar el nombre a factoritzar

- Evidentment el temps d'execució deprendrà de l'eficiència de la implementació i de la potència de l'ordinador

- Suposem que volem factoritzar un nombre que es producte de dos primers de 500 xifres...
- i fem servir l'ordinador més potent del mon

num.1 Top500.org (nov2024)

El Capitan

Site:	NNSA/LLNL (EEUU)
Manufacturer:	HPE
Cores:	11.039.616
Linpack Perf. (Rmax)	1,74 EFlop/s
Theor. Peak (Rpeak)	2,75 EFlop/s
Power:	29,6 MW (Producció elèctrica de La Baells 7.040 kW)

num.1 Top500.org (nov2024)

Figure: El Capitan: 1er al Top500.org (novembre 2024)

Factorització de nombres enters

- Nombre d'operacions necessàries: $t(b) = \left(e^{\sqrt[3]{\frac{64}{9} b \log^2(b)}}\right)$

  on $b = log_2(10^{1000})$

Factorització de nombres enters

- Nombre d'operacions necessàries: $t(b) = \left(e^{\sqrt[3]{\frac{64}{9} b \log^2(b)}} \right)$ on $b = log_2(10^{1000})$
- Prenem l'ordinador Frontier, operant a la seva capacitat màxima teòrica (1.74 EFlop/s $\approx 2 \times 10^{18}$ operacions per segon)

Factorització de nombres enters

- Nombre d'operacions necessàries: $t(b) = \left(e^{\sqrt[3]{\frac{64}{9} b \log^2(b)}} \right)$ on $b = log_2(10^{1000})$
- Prenem l'ordinador Frontier, operant a la seva capacitat màxima teòrica (1.74 EFlop/s $\approx 2 \times 10^{18}$ operacions per segon)
- El temps estimat de càlcul (en anys) per al producte de dos nombres primers de 500 xifres és de...

Factorització de nombres enters

- Nombre d'operacions necessàries: $t(b) = \left(e^{\sqrt[3]{\frac{64}{9} b \log^2(b)}} \right)$ on $b = log_2(10^{1000})$
- Prenem l'ordinador Frontier, operant a la seva capacitat màxima teòrica (1.74 EFlop/s $\approx 2 \times 10^{18}$ operacions per segon)
- El temps estimat de càlcul (en anys) per al producte de dos nombres primers de 500 xifres és de...

$$\frac{e^{\sqrt[3]{\frac{64}{9} \log_2(10^{1000}) \log^2(\log_2(10^{1000}))}}}{2 \times 10^{18} \times 3600 \times 24 \times 365}$$

Factorització de nombres enters

- Nombre d'operacions necessàries: $t(b) = \left(e^{\sqrt[3]{\frac{64}{9} b \log^2(b)}} \right)$ on $b = log_2(10^{1000})$
- Prenem l'ordinador Frontier, operant a la seva capacitat màxima teòrica (1.74 EFlop/s $\approx 2 \times 10^{18}$ operacions per segon)
- El temps estimat de càlcul (en anys) per al producte de dos nombres primers de 500 xifres és de...

$$\frac{e^{\sqrt[3]{\frac{64}{9} \log_2(10^{1000}) \log^2(\log_2(10^{1000}))}}}{2 \times 10^{18} \times 3600 \times 24 \times 365} \approx 2.6 \times 10^{38}$$

Factorització de nombres enters

- Nombre d'operacions necessàries: $t(b) = \left(e^{\sqrt[3]{\frac{64}{9} b \log^2(b)}} \right)$ on $b = log_2(10^{1000})$
- Prenem l'ordinador Frontier, operant a la seva capacitat màxima teòrica (1.74 EFlop/s $\approx 2 \times 10^{18}$ operacions per segon)
- El temps estimat de càlcul (en anys) per al producte de dos nombres primers de 500 xifres és de...

$$\frac{e^{\sqrt[3]{\frac{64}{9} \log_2(10^{1000}) \log^2(\log_2(10^{1000}))}}}{2 \times 10^{18} \times 3600 \times 24 \times 365} \approx 2.6 \times 10^{38}$$

- L'edat estimada de l'univers és de $1,3.10^{10}$ anys.....

Factorització de nombres enters

- Nombre d'operacions necessàries: $t(b) = \left(e^{\sqrt[3]{\frac{64}{9} b \log^2(b)}} \right)$ on $b = log_2(10^{1000})$
- Prenem l'ordinador Frontier, operant a la seva capacitat màxima teòrica (1.74 EFlop/s $\approx 2 \times 10^{18}$ operacions per segon)
- El temps estimat de càlcul (en anys) per al producte de dos nombres primers de 500 xifres és de...

$$\frac{e^{\sqrt[3]{\frac{64}{9} \log_2(10^{1000}) \log^2(\log_2(10^{1000}))}}}{2 \times 10^{18} \times 3600 \times 24 \times 365} \approx 2.6 \times 10^{38}$$

- L'edat estimada de l'univers és de $1,3.10^{10}$ anys.....
- El temps seria 2×10^{28} vegades l'edat de l'univers

Per fer-nos una idea...

- Com de gran és $2,6 \times 10^{38}$ anys?

Per fer-nos una idea...

- Com de gran és $2,6 \times 10^{38}$ anys?

- Suposem que posem un peresós a l'Equador i es posa a donar la volta al mon (5 km/dia)

Per fer-nos una idea...

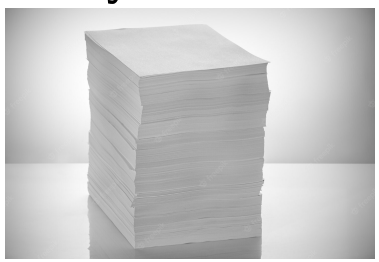
- Com de gran és $2,6 \times 10^{38}$ anys?

- Suposem que posem un peresós a l'Equador i es posa a donar la volta al mon (5 km/dia)
- Quan haurà fet una volta al mon, agafem dues gotes de l'oceà Atlàntic (0,1 ml)

Per fer-nos una idea...

- Com de gran és $2,6 \times 10^{38}$ anys?



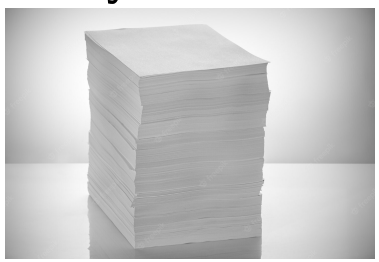


- Suposem que posem un peresós a l'Equador i es posa a donar la volta al mon (5 km/dia)
- Quan haurà fet una volta al mon, agafem dues gotes de l'oceà Atlàntic (0,1 ml)
- Quan haurem buidat l'oceà Atlàntic, posem un paper a terra, tornem a omplir l'oceà i tornem a començar a fer voltes al mon

Per fer-nos una idea...

- Com de gran és $2,6 \times 10^{38}$ anys?






- Suposem que posem un peresós a l'Equador i es posa a donar la volta al mon (5 km/dia)
- Quan haurà fet una volta al mon, agafem dues gotes de l'oceà Atlàntic (0,1 ml)
- Quan haurem buidat l'oceà Atlàntic, posem un paper a terra, tornem a omplir l'oceà i tornem a començar a fer voltes al mon
- Quan la pila de papers arribi a la lluna, l'ordinador encara no haurà acabat de calcular.