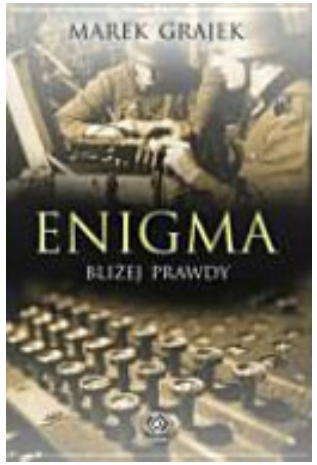
On weak rotors, latin squares, linear approximations and invariant differentials in Enigma



Nicolas T. Courtois
University College London, UK

Marek Grajek
Independent Crypto History Expert, Poland

youtube.com/watch?v=uuEcPvHJ9EM

Topics:

- a property which all ciphers ever made have…
  - except that nobody has yet studied it
  - they "imitate" a latin square!
  - are ciphers made with random permutations?
    - they never are: few rounds
    - they always are: many rounds

- history of Enigma and what nobody told you until today
  - mysteries about design of Enigma Rotors in 1929-1945
  - strong linear and differential properties of Enigma
  - the Zagreb Enigma A 16081 from 1943.

For 100 years encryption
[block ciphers, Enigma]
was about

Composing Permutations

non-commutative

PoQ ≠ QoP

UCL

Mystery Question

rotor III
(1929)

i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLMNOPQRSTUVWXYZ
0	BDFHJLCPRTXVZNYEIWGAKMUSQO
1	CEGIKBOQSWUYMXDHVFZJLTRPNA
2	DFHJANPRVTXLWCGUEYIKSQOMZB
3	EGIZMOQUSWKVBFTDXHJRPNLYAC
4	FHYLNPTRVJUAESCWGIQOMKXZBD
5	GXKMOSQUITZDRBVFHPNLJWYACE
6	WJLNRPTHSYCQAUEGOMKIVXZBDF
7	IKMQOSGRXBPZTDFNLJHUWYACEV
8	JLPNRFQWAOYSCEMKIGTVXZBDUH
9	KOMQEPVZNXRBDLJHFSUWYACTGI
10	NLPDOUYMWQACKIGERTVXZBSFHJ
11	KOCNTXLVPZBJHFDQSUWYAREGIM
12	NBMSWKUOYAIGECPRTVXZQDFHLJ
13	ALRVJTNXZHFDBOQSUWYPCEGKIM
14	KQUISMWYGECANPRTVXOBDFJHLZ
15	PTHRLVXFDBZMOQSUWNACEIGKYJ
16	SGQKUWECAYILNPRTVMZBDHFJXIO
17	FPJTVDBZXKMOQSULYACGEIWHNR
18	OISUCAYWJLNPRTKXZBFDHVGMQE
19	HRTBZXVIKMOQSJWYAECGUFLPDN
20	QSAYWUHJLNPRIVXZDBFTEKOCMG
21	RZXVTGIKMOQHUWYCAESDJNBLFP
22	YWUSFHJLNPGTVXBZDRCIMAKEOQ
23	VTREGIKMOFSUWAYCQBHLZJDNPX
24	SQDFHJLNERTVZXBPAGKYICMOWU
25	PCEGIKMDQSUYWAOZFJXHBLNVTR

Permuted Alphabets == Several Permutations P_i

Related art:

- Kryptos @CIA Langley HQ
- Cyrillic Projector [same author]

@Uni. Of North Carolina In Charlotte, US

Older Then You Think!

- Vigenère cipher = “le chiffre indéchiffrable” was known **earlier** and described by Bellaso in 1553 cf. *“La Cifra del Sig. Giovan Battista Belaso”*, book avail. at Museo Galileo, Florence, Italy.

Blaise de Vigenère
French diplomat
and cryptographer

Older Then You Think!

- Vigenère cipher [1553]
- Latin squares in maths:

August 15, 2014 SEOUL ICM 2014 03

SEOUL ICM 2014

The official newspaper of the 27th International Congress of Mathematicians 2014 Seoul

CHOI Seokjeong and traditional Asian mathematics

Confucian scholar's discovery predates the work of Euler

classified mathematical operations, problems and all nine chapters into four classes, represented by the four sasang symbols. Trying to understand mathematics and patterns with those four symbols, he produced a remarkable study of magic squares and related topics, in particular an orthogonal Latin square of order 9. This is an accomplishment predating Euler's work by more than 60 years. In 2007, CHOI was listed in the "Handbook of Combinatorial Designs"

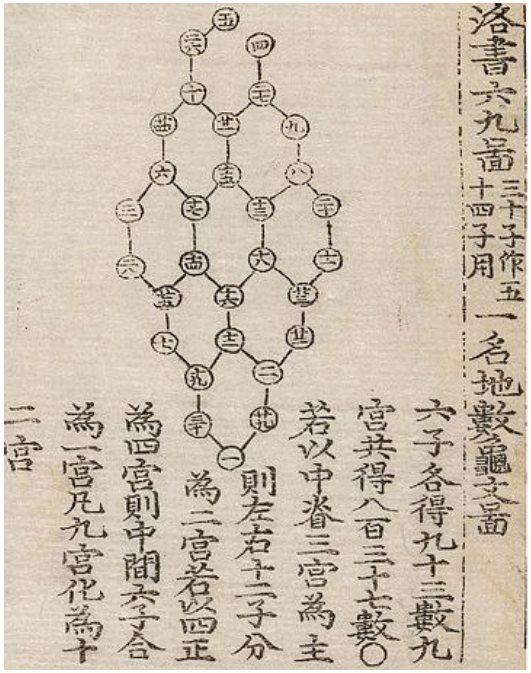
Older Then You Think!

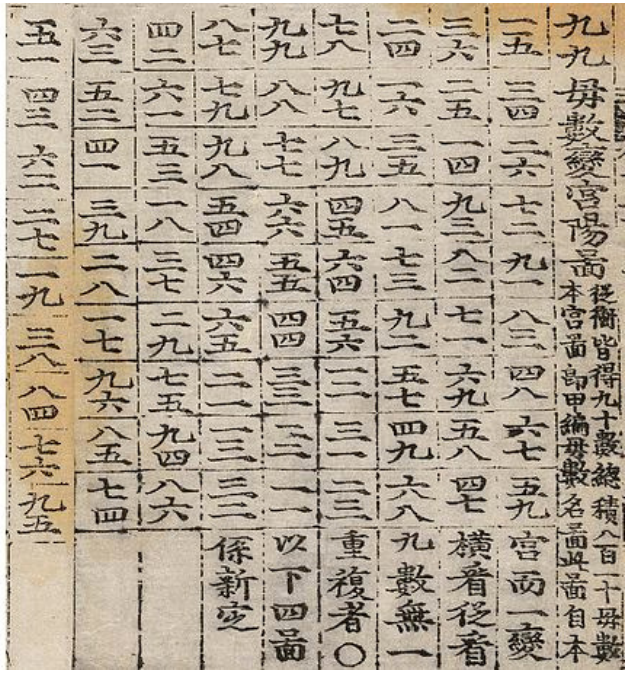
- Vigenère cipher [1553]
- Latin squares in maths:
  studied by Korean
  mathematician
  Seok-jeong Choi

  최석정

  published *Gusuryak*

  구수략



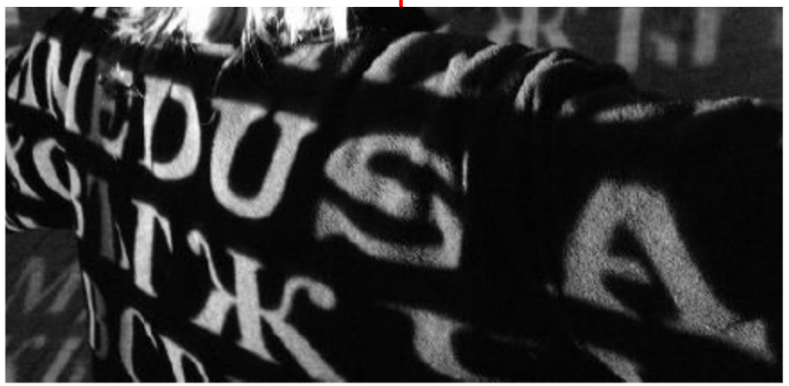


in year 1700, which is about latin squares,

predating Euler by 67 years!

Six Alphabets Only == Six Permutations P_i

- Vigenère cipher [1553]
- Latin squares [1700]

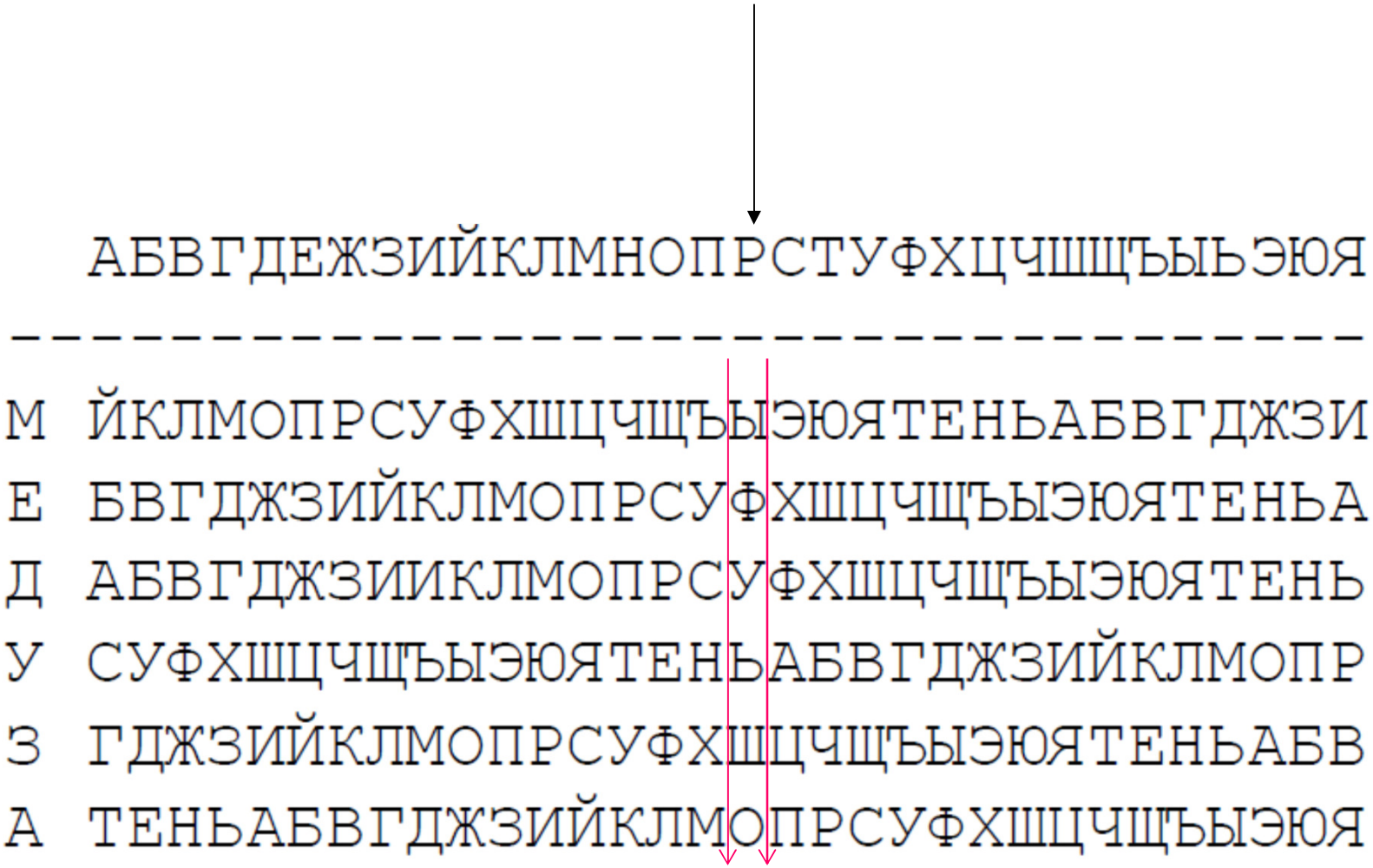


©Elonka Dunin

```
  АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
--------------------------------
М ЙКЛМОПРСУФХШЦЧЩЪЫЭЮЯТЕНЬАБВГДЖЗИ
Е БВГДЖЗИЙКЛМОПРСУФХШЦЧЩЪЫЭЮЯТЕНЬА
Д АБВГДЖЗИИКЛМОПРСУФХШЦЧЩЪЫЭЮЯТЕНЬ
У СУФХШЦЧЩЪЫЭЮЯТЕНЬАБВГДЖЗИЙКЛМОПР
З ГДЖЗИЙКЛМОПРСУФХШЦЧЩЪЫЭЮЯТЕНЬАБВ
А ТЕНЬАБВГДЖЗИЙКЛМОПРСУФХШЦЧЩЪЫЭЮЯ
```

Key Property – Latin-Square - Column Wise

Each letter appears ONCE in each column.



Enigma Rotors

Each letter appears ONCE in each column?

i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLM
0	BDFHJLCPRTXVZ
1	CEGIKBOQSWUYM
2	DFHJANPRVTXLW
3	EGIZMOQUSWKVB

Enigma Rotors

Each letter appears ONCE in each column?

IN FACT you NEVER get a complete Latin Square.

Very HARD to achieve

[and was NEVER achieved yet as far we know]

i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLM
0	BDFHJLCPRTXVZ
1	CEGIKBOQSWUYM
2	DFHJANPRVTXLW
3	EGIZMOQUSWKVB

Many Enigma Rotors **Approximate** This Property

"almost"

Each letter appears ONCE in each column.

Table 1. Collisions and entropy of one column for selected historical rotors.

rotor name	Nb.	code	dates	$ImS(R)$	$Ent(R)$
Army I	1	EKM	1930	17	3.95
Army II	2	AJD	1930	19	4.16
Army III	3	BDF	1930	20	4.21
Army IV-VIII	4-8		1938-39	23/24	≥ 4.47
Railway I-III	12-14		1941	23/24	≥ 4.47
Japan/Tirpitz	37-44		1944	23-25	≥ 4.47
Hungary G-111 I-III	12-14		193X	23/24	≥ 4.44
Swiss Airforce I-III	17-19		1938	16/17	≈ 3.85
Norway I	20	WTO	1945	13	3.46
Norway II	21	GJL	1945	16	3.80
Norway III	22	JWF	1945	15	3.66
Norway IV	23	ESO	1945	15	3.80
Norway V	24	HEJ	1945	15	3.80
Zagreb 16081 V	66	WMG	1935	25	4.62

*Enigma in Zagreb:

Zagreb Enigma

cryptocellar.org/pubs/EnigmaInSpain.pdf

- Enigma A 16081, used in 1943
- by German Military Attaché in Zagreb
- wheels and reflector bear Greek letter Δ
- found by TICOM in 1945

[US army archives, now in Berlin]

Wheel	Wheel Wiring	Notch	Window
	ABCDEFGHIJKLMNOPQRSTUVWXYZ		
I	CVFWJOBXANQTDZUMEYRPSKGILH	Y	Q
II	XJGURHZMYDLATWKSEPNCQFOIBV	M	E
III	SYIGXELDUKBVOAWTZHQNFCRMJP	D	V
IV	HKTZDSRFWPCQJIYXNVMUGELAOB	R	J
V	WMGRKEJUAZFTOXINDYBQVHLCPS	H	Z
UKW	DONAJUXTQELKSCBZIVMHFRYGWP		
ETW	ABCDEFGHIJKLMNOPQRSTUVWXYZ		

Figure 20. Wheel wiring for the Zagreb Delta machine A 16081.

Zagreb Enigma Rotors **Approximate** Extremely Well!

"almost"

Each letter appears ONCE in each column.

Table 1. Collisions and entropy of one column for selected historical rotors.

				$ImS(R)$
				17
				19
				20
				23/24
				23/24
				23-25
				23/24
				16/17
				13
				16
				15
				15
				15
Zagreb 16081 V	66	WMG	1935	25

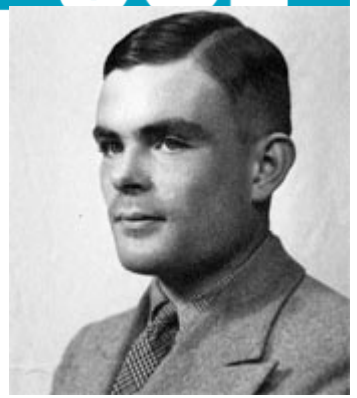
P(win)@lottery

Enigma

Rejewski

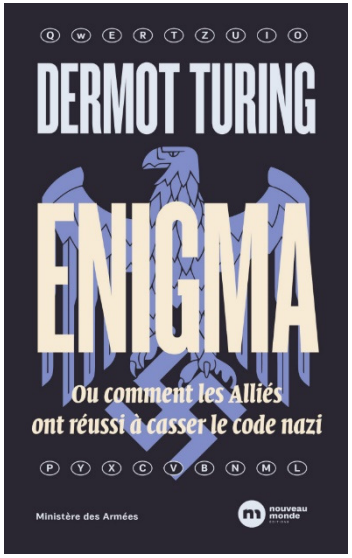
Zygalski

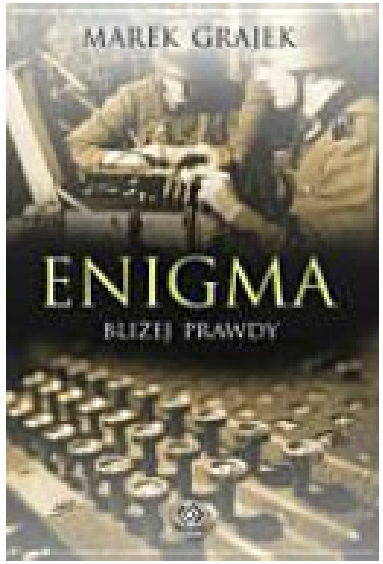
or How Some Mathematicians Won the WW2…



Turing

Welchman





Cryptanalysis

from Greek

- kryptós, "hidden“
- analýein, "to untie“

Term coined in 1920

by William F. Friedman.

- Born in Moldavia, emigrated to US in 1892.
- Chief cryptologist at National Security Agency in the 50s.

Encryption – **Permuted Alphabets**

A different permutations on 26 letters is used at each step

ciphertext

plaintext

-self-reciprocicity = involution pty
-no fixed points
-fast parts in outer layers

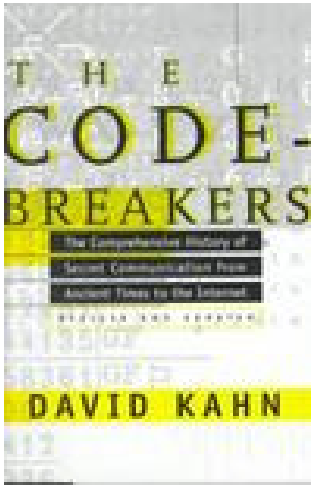
Marian Rejewski

December 1932:
reverse engineering of Enigma rotors

– “the greatest breakthrough in cryptanalysis in a thousand years” [David Kahn]

– cf. John Lawrence, "A Study of Rejewski's Equations", Cryptologia, 29 (3), July 2005, pp. 233–247. + other papers by the same author

$26! \approx 2^{88.4}$



This Paper

Also:

reverse engineering

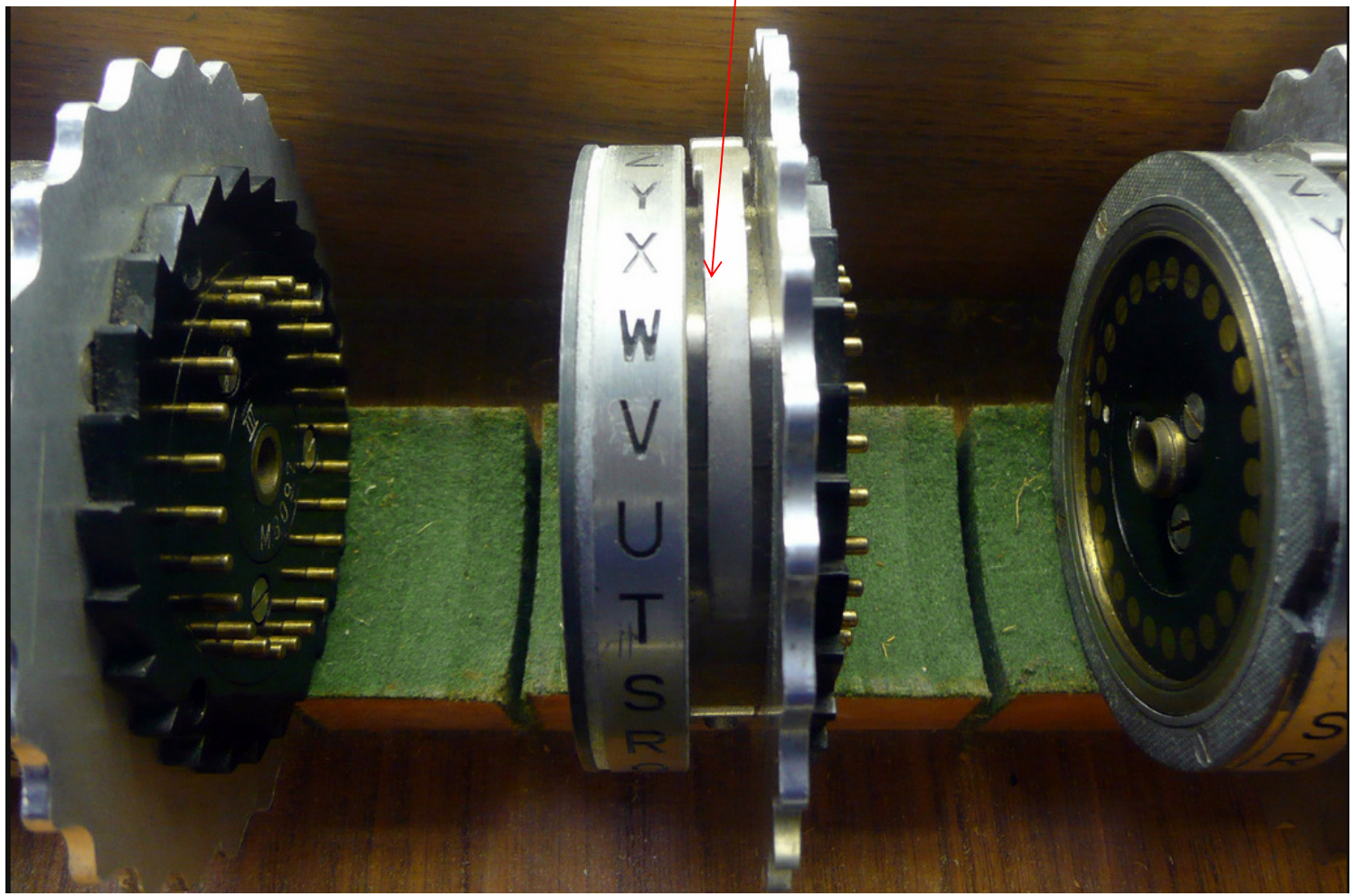
- inside just ONE of Enigma rotors
- hidden property
- not hard to detect

$26! \approx 2^{88.4}$

Rotors

26 relative settings

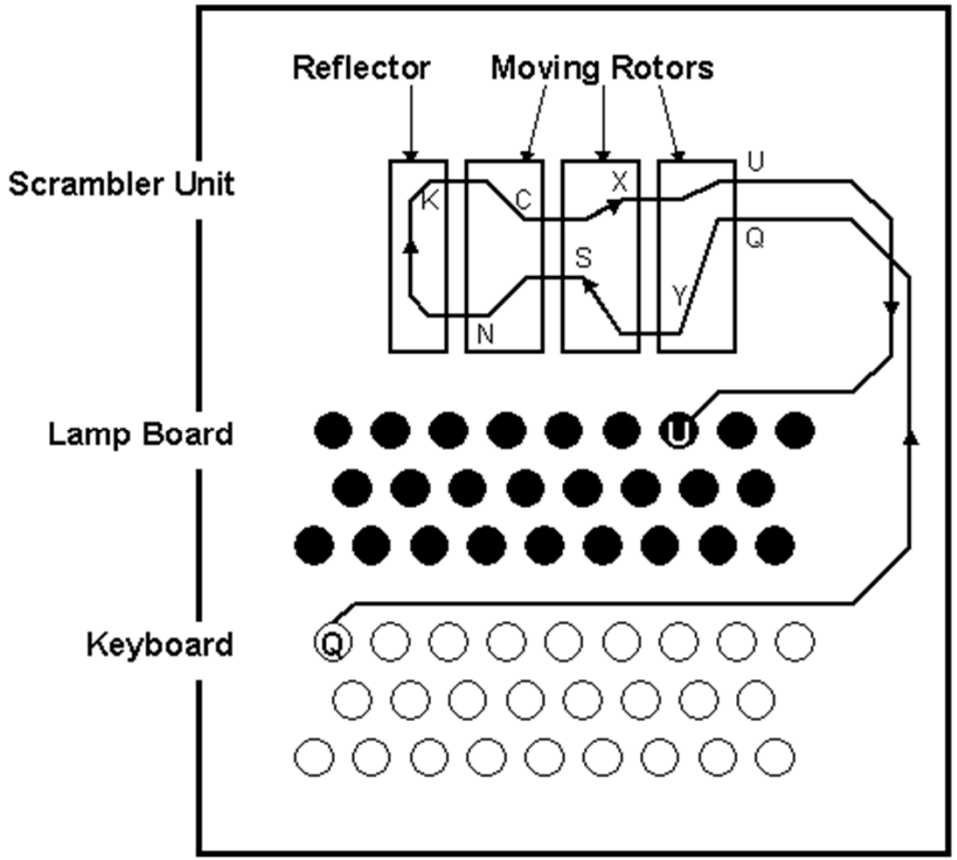
Difficult to obtain for the enemy…



Commercial Enigma [1920s]

insecure

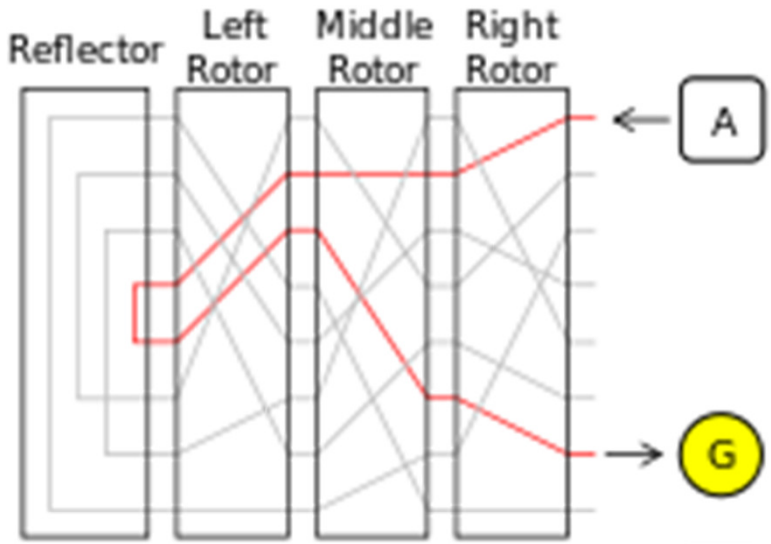
combines several permutations on 26 characters…



Rotor Stepping

Regular

odometer-like

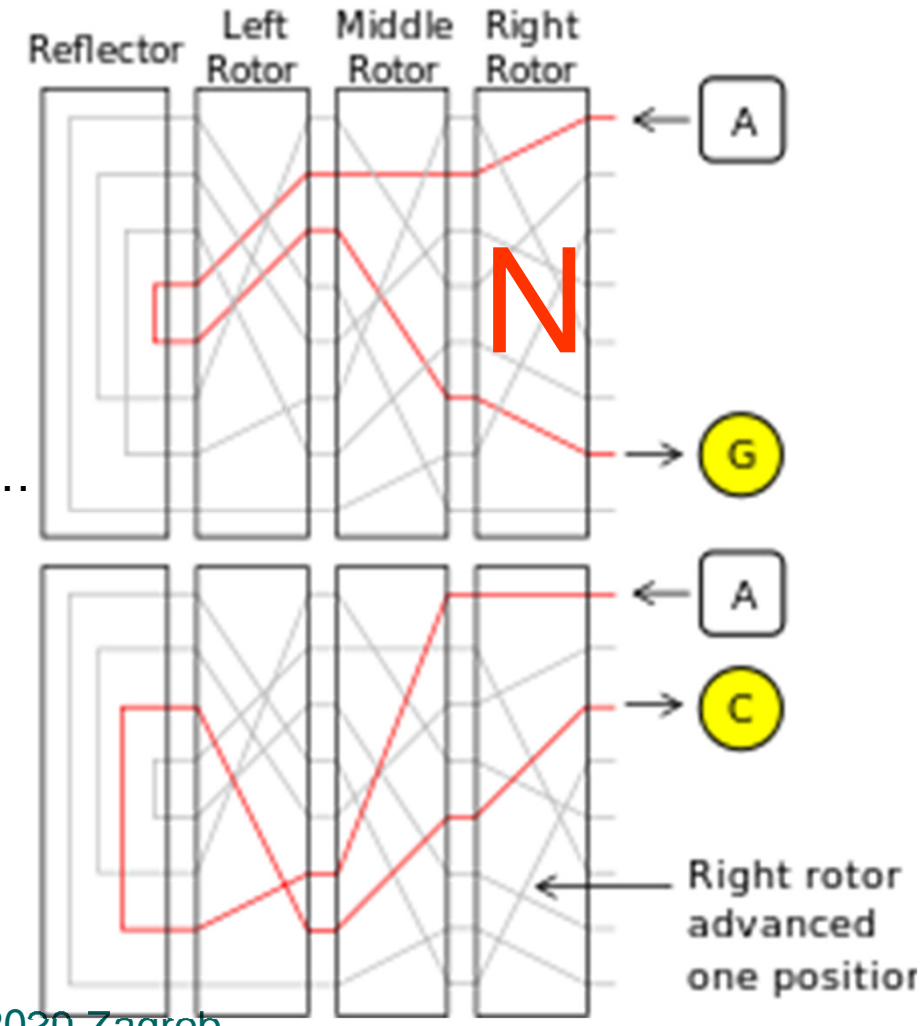


+1

Rotor Stepping

- Rotating a rotor:
- N becomes $C^{-1} \circ N \circ C$ (p)
- C is a circular shift a↦b…

- Proof:



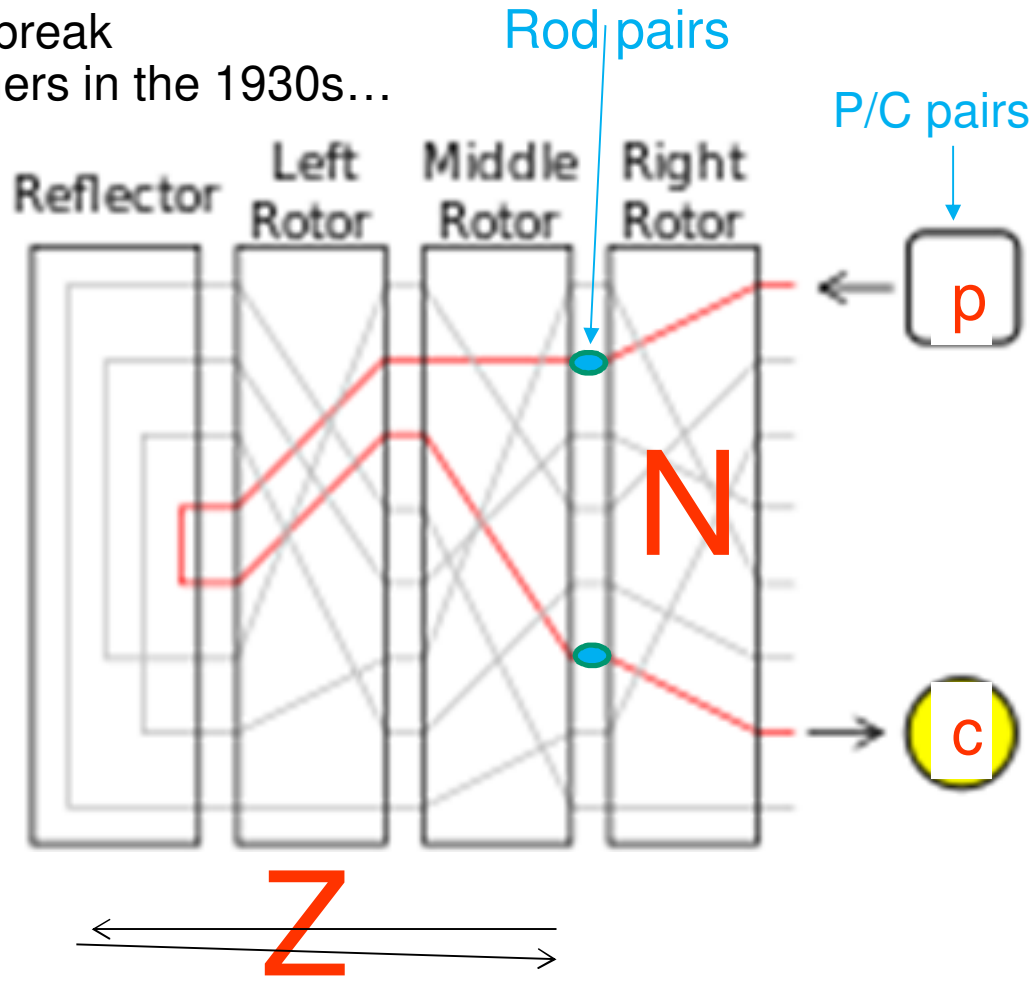
Bâtons/Rods Attack

Used by French/British/Germans to break Swiss/Spanish/Italian/British ciphers in the 1930s…

- assumes only first rotor moving
- rotor wiring known
- guess which rotor is at right
- guess starting position (26)
- guess SHORT crib [plaintext]
- t=0 $c=N^{-1} \circ Z \circ N\ (p)$
- t=0 $Z \circ N(p) = N(c)$
- Z is an involution

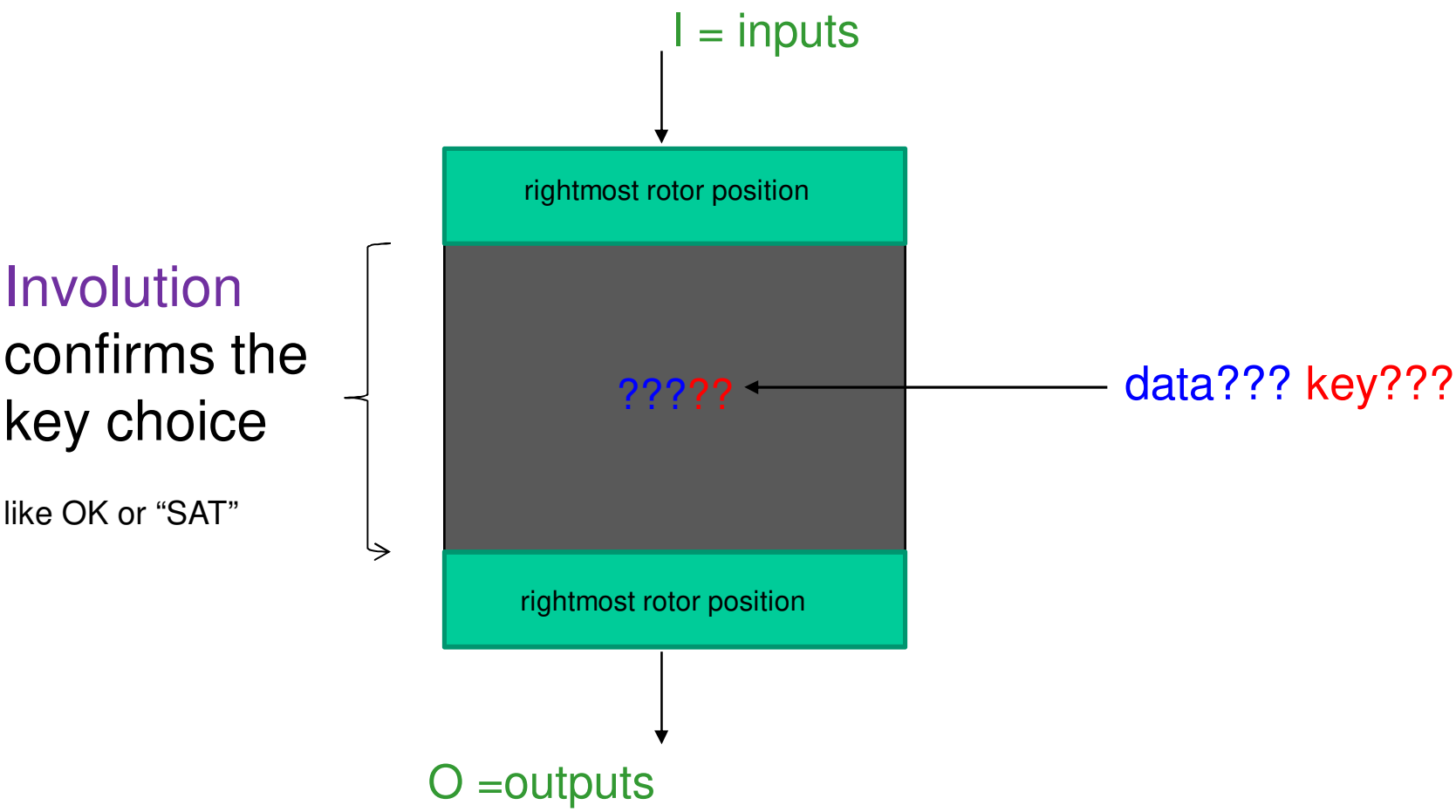
- Rotating a rotors:
- P becomes $C^{-1} \circ P \circ C\ (p)$
- C is a circular shift $a \mapsto b$…

- t=i $Z \circ C^{-i}NC^{i}\ (p) = C^{-i}NC^{i}\ (c)$



- everybody came up with this attack c. 1930 [Batey]
- worked until 1939 [cf. Spanish civil war]
- Germans: avoid the attack since 1929/30 with a **steckerboard**

Think Inside the Box



Key Size

About 2^{380} with rotors

$26! \approx 2^{88.4}$

Only 2^{76} when rotors are known.

Same 3 rotors used since 1920s…
until 1945!!! BIG MISTAKE.

Zygalski Netz Attack: until 1 May 1940

Based on "females":

Cycles of length 1.

AFKASF
female

T=1 $R_1 \circ S(x) = S(A)$

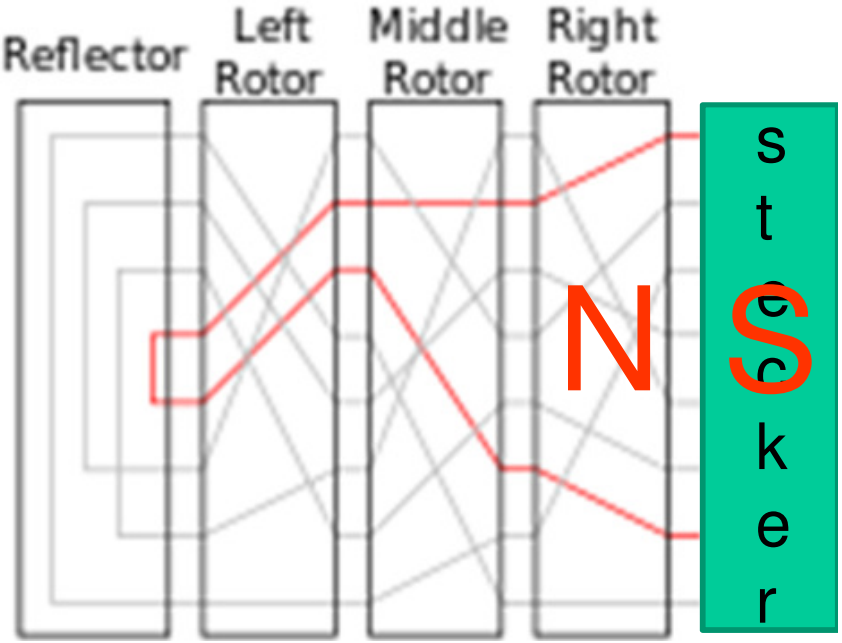
T=4 $R_4 \circ S(x) = S(A)$

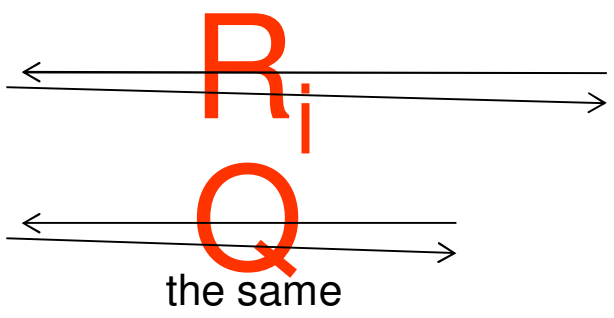
Same key, same input, same output… +3 steps

$S^{-1} \circ R_1 \circ R_4 \circ S \quad A \mapsto A$

$R_1 = N^{-1} \circ Q \circ N$

$R_4 = C^{-3}N^{-1}C^3 \circ Q \circ C^{-3}NC^3$





Conjugation

"Theorem Which Won World War 2",

[I. J. Good and Cipher A. Deavours, afterword to: Marian Rejewski, "How Polish Mathematicians Deciphered the Enigma", Annals of the History of Computing, 3 (3), July 1981, 229-232]

P and

Q^{-1} o P o Q

have the same cycle structure

$S^{-1} \circ R_1 \circ R_4 \circ S$ has a fixed point

<=>

$R_1 \circ R_4$ has a fixed point

Pty independent on stecker!

*Zygalski Attack: until 1 May 1940

fixed points for $R_1 \circ R_4$

Stacking them allowed to
determine the key uniquely…

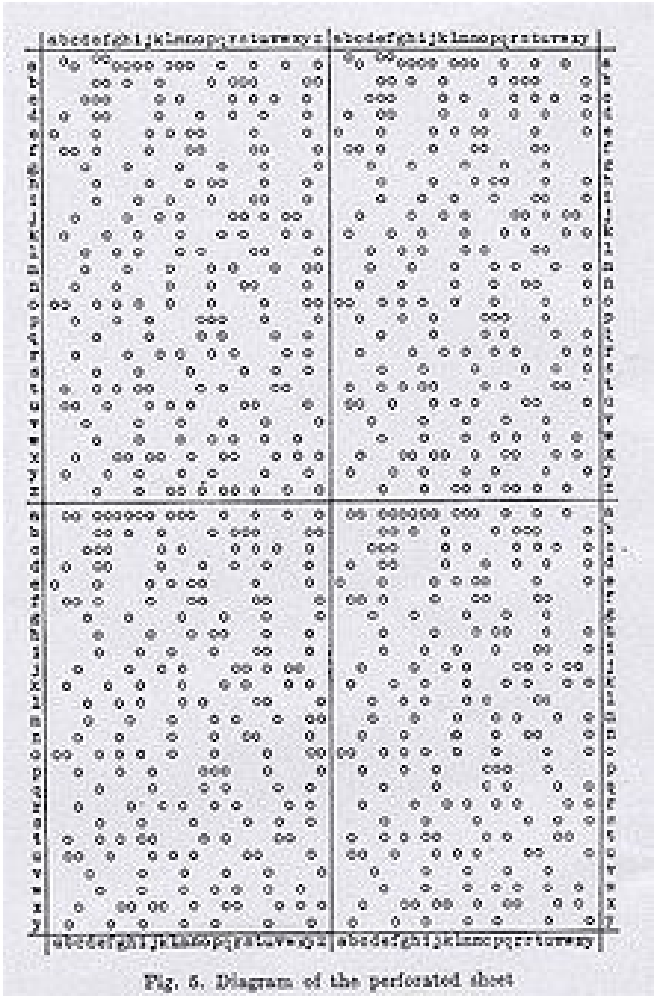
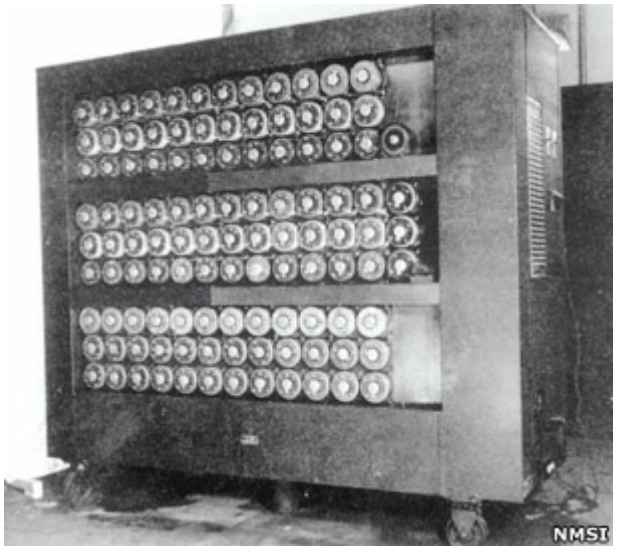


Fig. 6. Diagram of the perforated sheet

Turing-Welchman Bombe

Works with short cycles



guess/test all 26 possible S(E)

$R_7 \circ R_9 \circ R_{14} \circ S(E) = S(E)$

serial connection of several unsteckered Enigmas

IMPORTANT:
Bombes ASSUMED MIDDLE ROTOR not moving
(large proba for shorter cribs, if fails, repeat…)

Accept – Reject a guess for S(E)

Closed loop connection

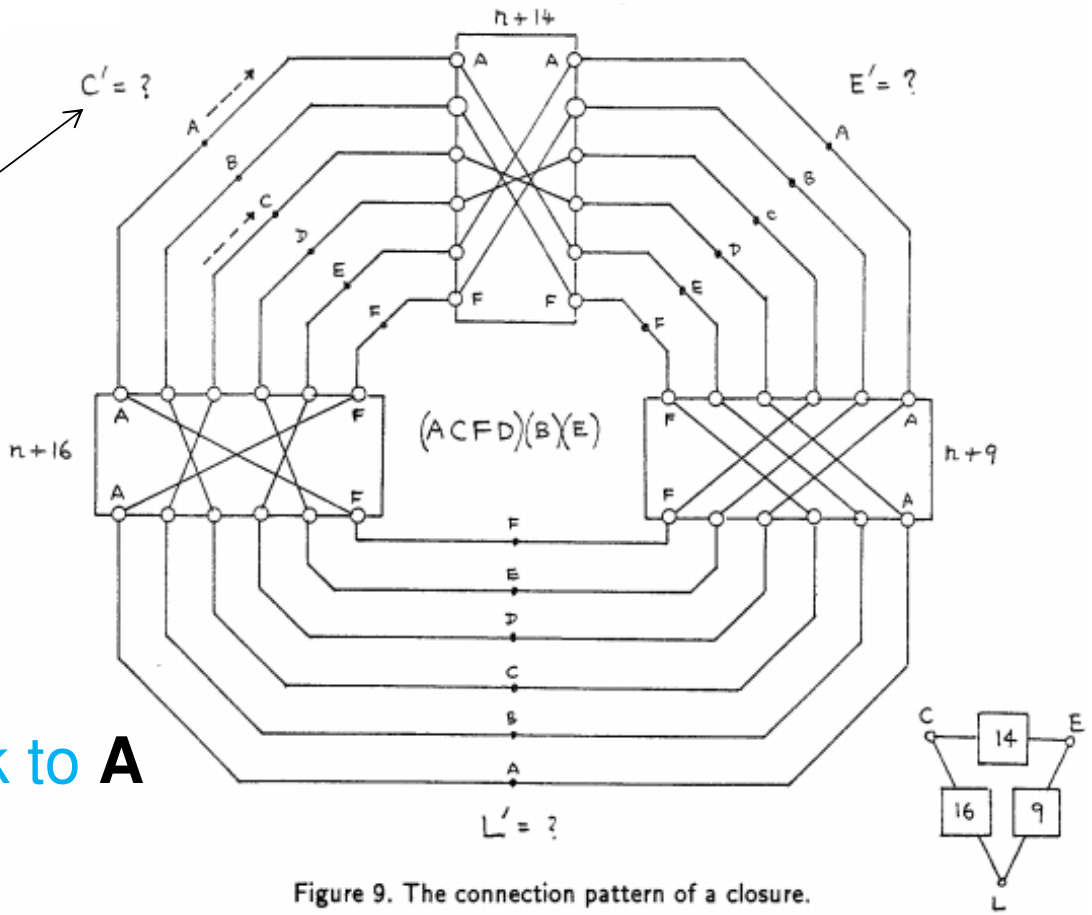


Figure 9. The connection pattern of a closure.

Correct S(E) is a fixed point!

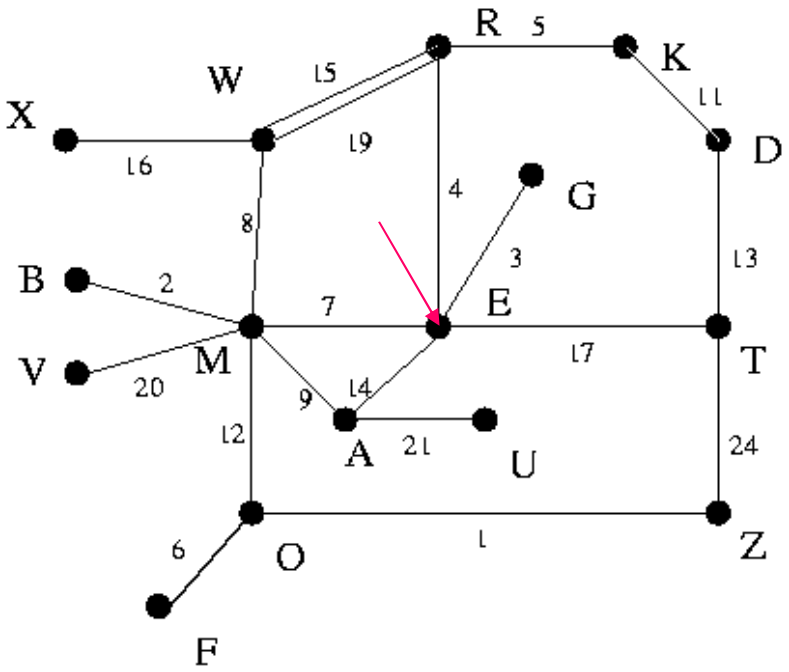
A correct
=>The current comes back to **A**

$R_7 \circ R_9 \circ R_{14} \circ S(E) = S(E)$

implemented by the bombe

Turing Attack = 1 cycle, 1 'central' letter [at place with several connections]

guess S(E)
=>test it



Fact:

Many attacks on Enigma CAN be improved SLIGHTLY if rotors have good linear approximations.

with A=0, B=1, etc.

Sth. wrong with Rotor III from 1929.

$$y = \rho^{-i} \circ R_{III} \circ \rho^{i}(j)$$

$$y \stackrel{?}{=} i + 2j + 1$$

$$\text{with } Pr = \frac{10}{26}$$

$$\text{with } Pr = \frac{10}{13} \quad \text{odd } y = \text{B,D,F,H,..}$$

i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLM
0	BDFHJLCPRTXVZ
1	CEGIKBOQSWUYM
2	DFHJANPRVTXLW
3	EGIZMOQUSWKVB

Full Table of Permuted Alphabets

red/blue

when

y=i+2j+1

j = input col.

y = out. letter

i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLMNOPQRSTUVWXYZ
0	BDFHJLCPRTXVZNYEIWGAKMUSQO
1	CEGIKBOQSWUYMXDHVFZJLTRPNA
2	DFHJANPRVTXLWCGUEYIKSQOMZB
3	EGIZMOQUSWKVBFTDXHJRPNLYAC
4	FHYLNPTRVJUAESCWGIQOMKXZBD
5	GXKMOSQUITZDRBVFHPNLJWYACE
6	WJLNRPTHSYCQAUEGOMKIVXZBDF
7	IKMQOSGRXBPZTDFNLJHUWYACEV
8	JLPNRFQWAOYSCEMKIGTVXZBDUH
9	KOMQEPVZNXRBDLJHFSUWYACTGI
10	NLPDOUYMWQACKIGERTVXZBSFHJ
11	KOCNTXLVPZBJHFDQSUWYAREGIM
12	NBMSWKUOYAIGECPRTVXZQDFHLJ
13	ALRVJTNXZHFDBOQSUWYPCEGKIM
14	KQUISMWYGECANPRTVXOBDFJHLZ
15	PTHRLVXFDBZMOQSUWNACEIGKYJ
16	SGQKUWECAYLNPRTVMZBDHFJXIO
17	FPJTVDBZXKMOQSULYACGEIWHNR
18	OISUCAYWJLNPRTKXZBFDHVGMQE
19	HRTBZXVIKMOQSJWYAECGUFLPDN
20	QSAYWUHJLNPRIVXZDBFTEKOCMG
21	RZXVTGIKMOQHUWYCAESDJNBLFP
22	YWUSFHJLNPGTVXBZDRCIMAKEOQ
23	VTREGIKMOFSUWAYCQBHLZJDNPX
24	SQDFHJLNERTVZXBPAGKYICMOWU
25	PCEGIKMDQSUYWAOZFJXHBLNVTR

Probabilities [0]

Can this happen by accident?

Theorem 5.10 (Rejewski). Let P and Q be two arbitrary permutations on n wires, then P and $Q^{-1} \circ P \circ Q$ have the same cycle structure.

This result is sometimes called "The Theorem Which Won World War 2", see [19, 23] or "The Main Theorem of Rotor Encryption"

```
{1: 1, 8: 1, 17: 1}
A=>B=>D=>H=>P=>E=>J=>T=>A
C=>F=>L=>V=>M=>Z=>O=>Y=>Q=>I=>R=>W=>U=>K=>X=>S=>G=>C
N=>N
```

Does it look normal?

Theorem 5.11 (Cycle Structure). A random permutation of length at least m contains on average $1/m$ cycles of length m, then 0 for larger sizes. The expected number of cycles of length at most m is about $\ln(m)$.

$ln(17) = 2.8$

Probabilities [1]

Can this happen by accident?

y=i+2j+1

$$\binom{26}{10}\frac{15!}{26!}\approx 2^{-25}$$

i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLM
0	BDFHJLCPRTXVZ
1	CEGIKBOQSWUYM
2	DFHJANPRVTXLW
3	EGIZMOQUSWKVB

General Case:

Can this happen by accident?

Table 1. Collisions and entropy of one column for selected historical rotors.

rotor name	Nb.	code	dates	$ImS(R)$	$Ent(R)$
Army I	1	EKM	1930	17	3.95
Army II	2	AJD	1930	19	4.16
Army III	3	BDF	1930	20	4.21
Army IV-VIII	4-8		1938-39	23/24	≥ 4.47
Railway I-III	12-14		1941	23/24	≥ 4.47
Japan/Tirpitz	37-44		1944	23-25	≥ 4.47
Hungary G-111 I-III	12-14		193X	23/24	≥ 4.44
Swiss Airforce I-III	17-19		1938	16/17	≈ 3.85
Norway I	20	WTO	1945	13	3.46
Norway II	21	GJL	1945	16	3.80
Norway III	22	JWF	1945	15	3.66
Norway IV	23	ESO	1945	15	3.80
Norway V	24	HEJ	1945	15	3.80
Zagreb 16081 V	66	WMG	1935	25	4.62

General Case:

Can ImS=25 happen by accident?

Zagreb 16081 V	66	WMG	1935	25	4.62

Or can you win a lottery with the “means” of 1929??

Table 2. Probability distribution of $ImS(R)$ for random permutations

random permutation													
7	8	9	10	12	14	16	18	20	22	23	24	25	26
$2^{-27.1}$	$2^{-22.4}$	$2^{-17.5}$	$2^{-13.6}$	$2^{-7.4}$	$2^{-3.7}$	$2^{-2.1}$	$2^{-2.7}$	$2^{-5.6}$	$2^{-11.1}$	$2^{-14.8}$	$2^{-20.0}$	$2^{-26.4}$	$2^{-67.6}$

latin square⇔26

Differential Cryptanalysis!

Def.

We call a rotor an **anti-latin** square if for every k the differential

$$\underbrace{\Delta^i = k}_{\substack{\text{input}\\ \text{difference}}} \rightarrow \underbrace{\Delta^o = k}_{\substack{\text{output}\\ \text{difference}}}$$

has a non-zero probability.

i	$\rho^{-i} \circ R_{III} \circ \rho^{i}$
	ABCDEFGHIJKLM
0	BDFHJLCPRTXVZ
1	CEGIKBOQSWUYM
2	DFHJANPRVTXLW
3	EGIZMOQUSWKVB

UCL

Differential Cryptanalysis!

Def.

We call a rotor an **anti-latin** square if for every k the differential

$$\Delta^i = k \rightarrow \Delta^o = k$$

input difference — output difference

has a non-zero probability.

we call ImK the Nb.
of impossible k
== same as “impossible
invariant differentials”

collisions
with k=2,3,5

Theorem [our paper]

Latin Square

⇔

ImS=26

⇔

Imk=25

⇔

∀k≠ 0 differential k→k is impossible

*0 →0 always possible

Conclusion

- Between 1929 and 1945 some 66 different rotors were generated for Enigma machines…
- None of these rotors behave as random permutations!
  such result was never shown before

- Rotors also have very strong linear and differential properties.

In general:

- It is hard to obtain a latin square [and was never achieved so far] but you can get close with large lmk value.
- We claim that THE SAME properties hold for all good block ciphers when the number of rounds is small,
  and found explicit recommendations of this type in old state security archives [details will appear soon]