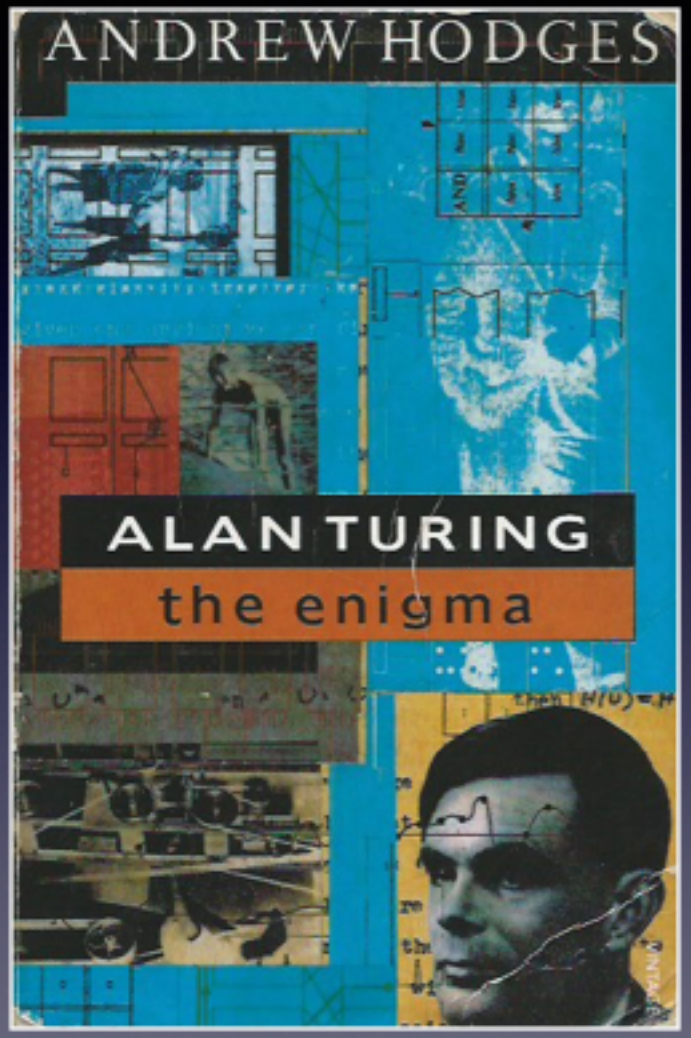
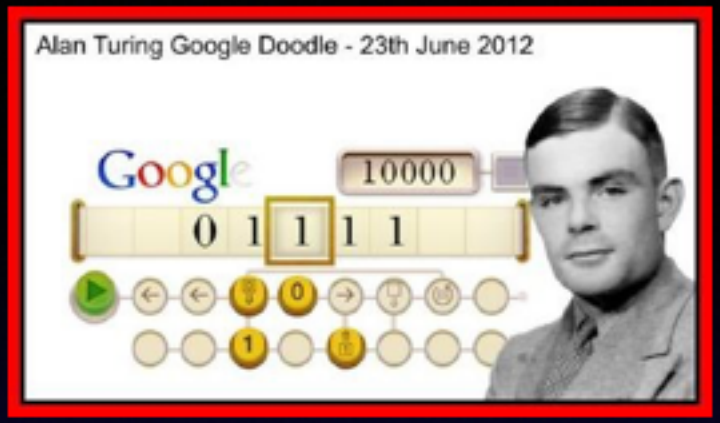
Wie kraakt het enigma van Alan Turing?

Bennie Mols
Wetenschapsjournalist, auteur en spreker
benniemols.blogspot.com


ANDREW HODGES
ALAN TURING
the enigma


Bennie Mols
Turings Tango
Waarom de mens
de computer de baas blijft
NWADAM

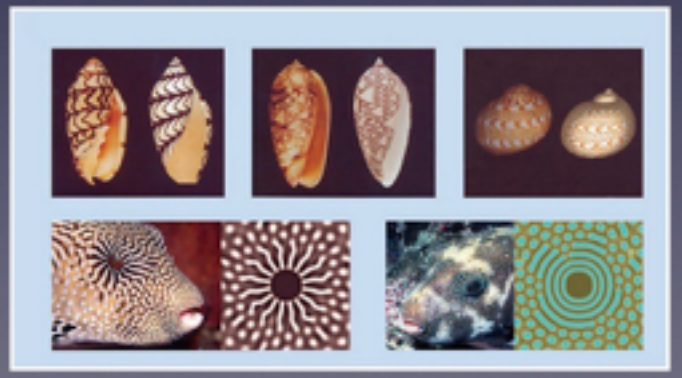
Alan Turing: 1912-1954

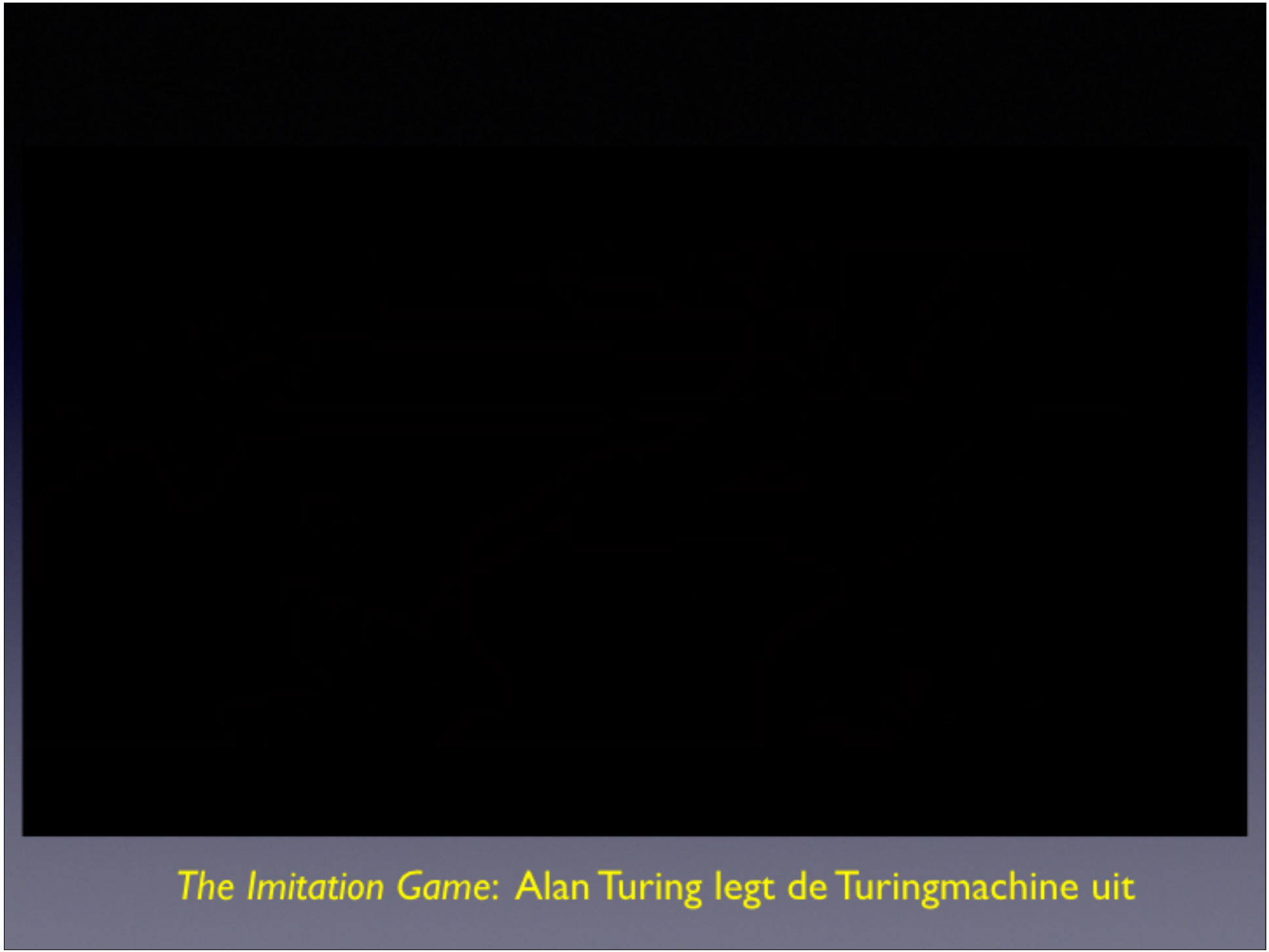

Alan Turing Google Doodle - 23th June 2012
Google
10000
0 1 1 1 1


lol :)


CODEBREAKER
CHALLENGE


e4 c6 2. d4 d5 3. Nc3 dxe4




The Imitation Game: Alan Turing legt de Turingmachine uit

What Every Child Should Know LIBRARY

NATURAL WONDERS

EVERY CHILD SHOULD KNOW

By

EDWIN TENNEY BREWSTER

Published by DOUBLEDAY, DORAN & CO., INC., *for*
THE PARENTS' INSTITUTE, INC.
Publishers of "THE PARENTS' MAGAZINE"
52 Vanderbilt Avenue, New York

THE FROG'S BIG TURN INTO A TADPOLE.

A FULL-GROWN FROG.

TADPOLES FEEDING

1922: Turing (10 jaar) krijgt boek *Natural wonders every child should know* cadeau

1931-1934: Wiskundestudie King's College Cambridge

David Hilbert (1928)

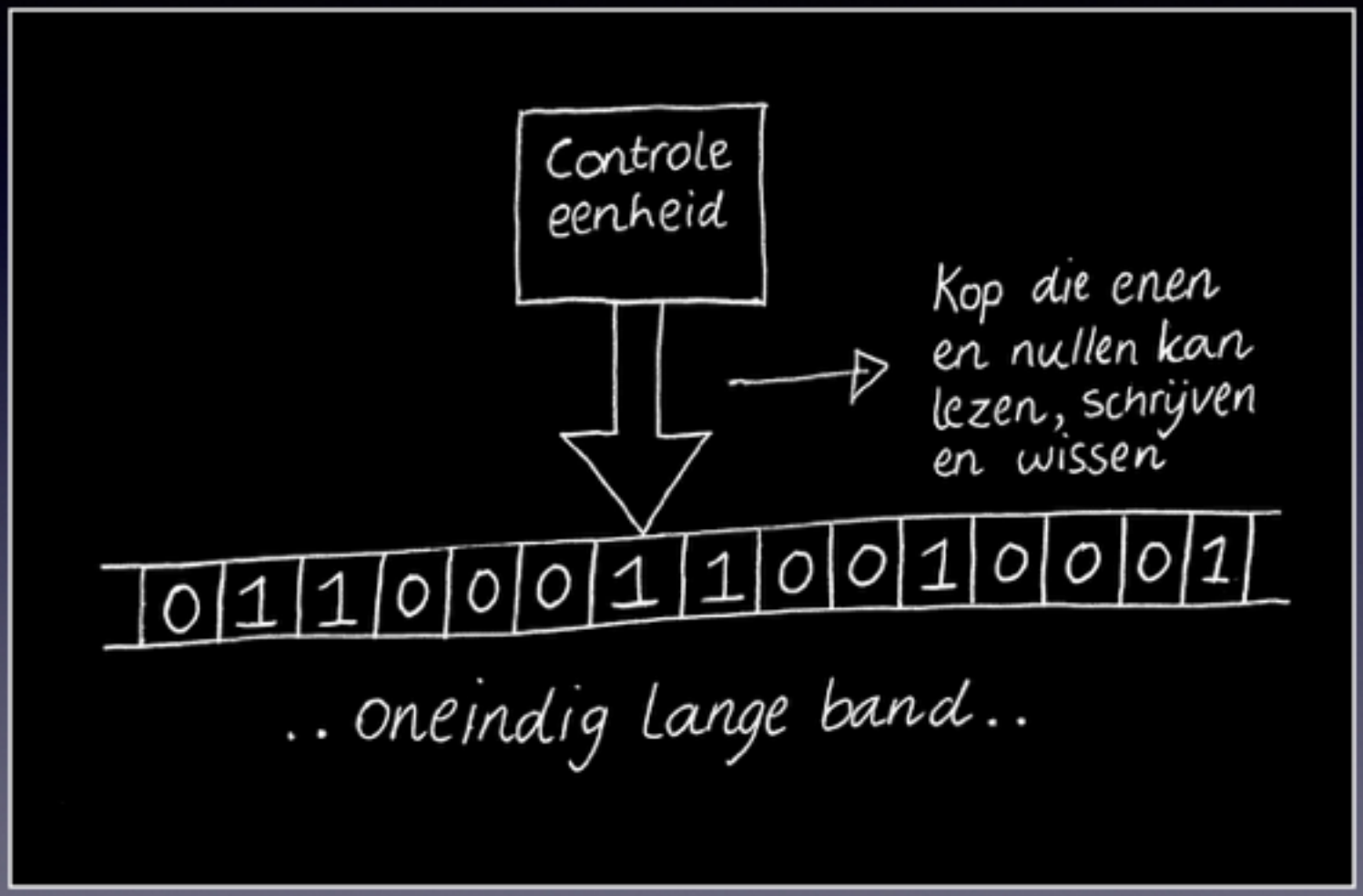
Ideaal:
Wiskunde logisch dicht timmeren

- Volledigheid: bewijs of weerlegging
- Consistentie: geen tegenspraak
- Beslisbaarheid: beslismethode voor bewijs of weerlegging

1936: Turing (24 jaar)

Wat is de meest algemene machine
die met symbolen kan omgaan?

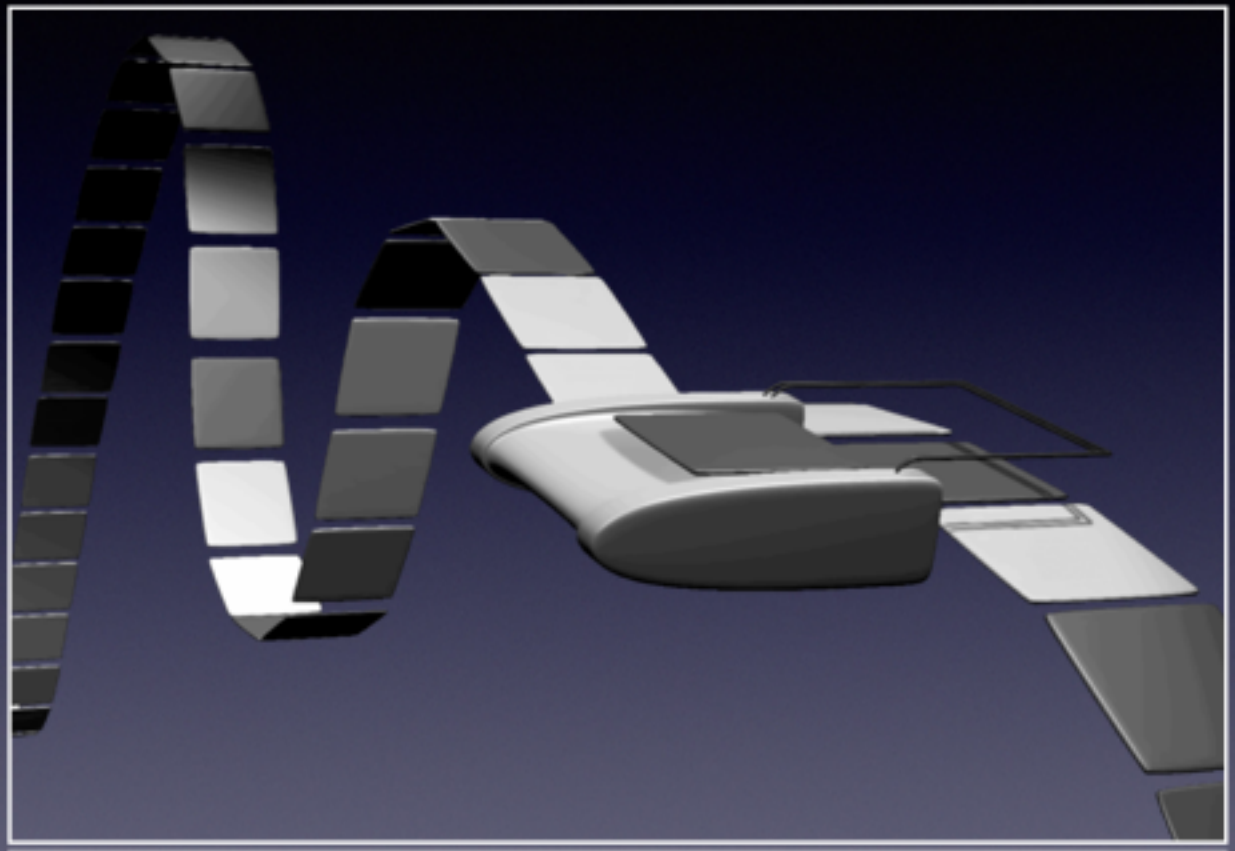
1936: Turing (24 jaar) beschrijft de Turingmachine



Model van "menselijke geest aan het werk"

Demonstratiemodel van een Turingmachine (http://aturingmachine.com door Mike Davey)

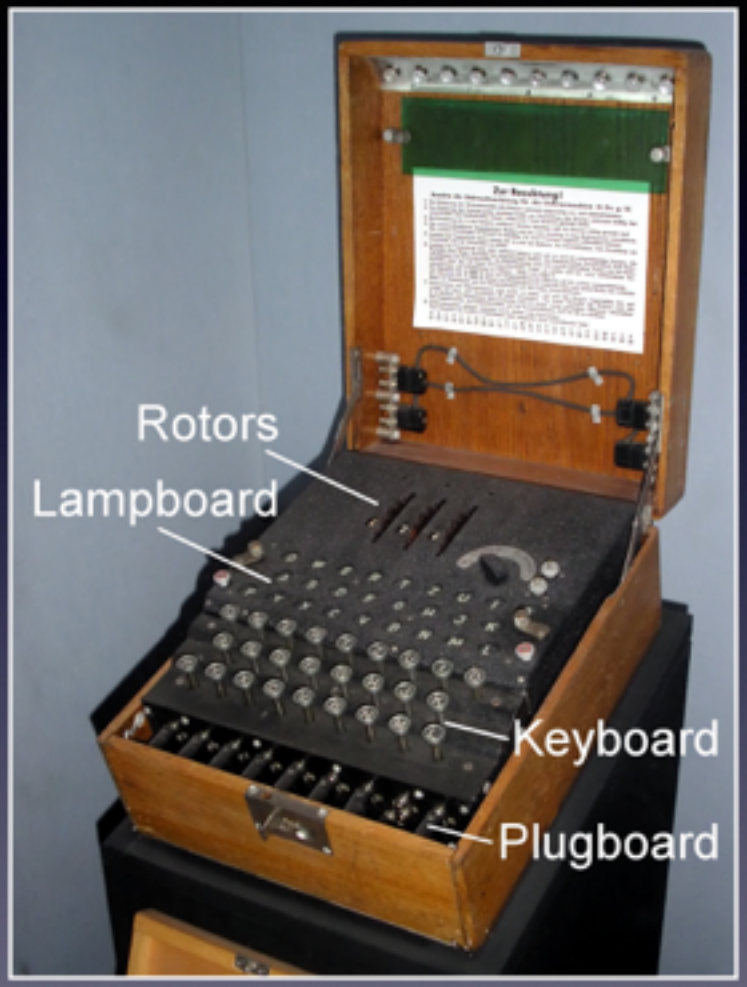
Door het oplossen van een zuiver wiskundig probleem,
ontdekt Turing het
fundament van de informatica

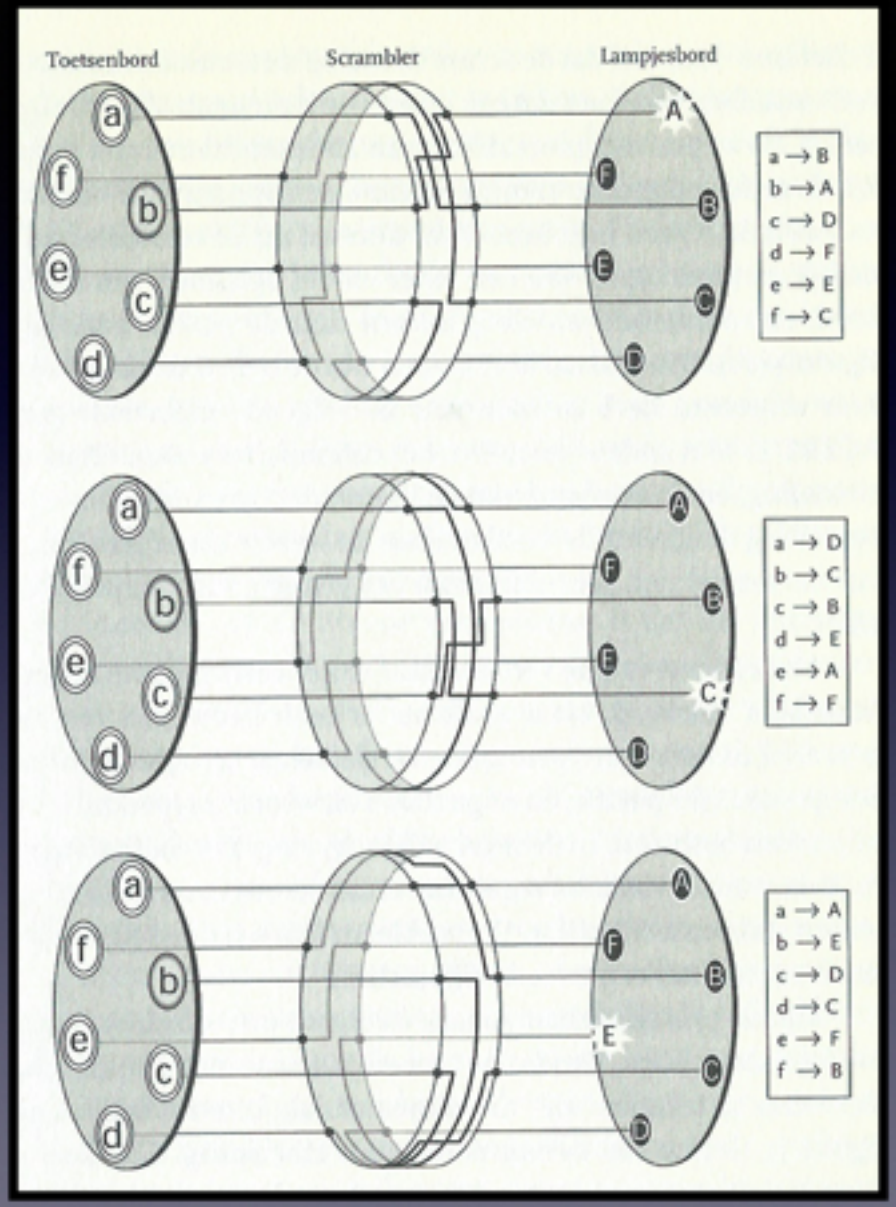


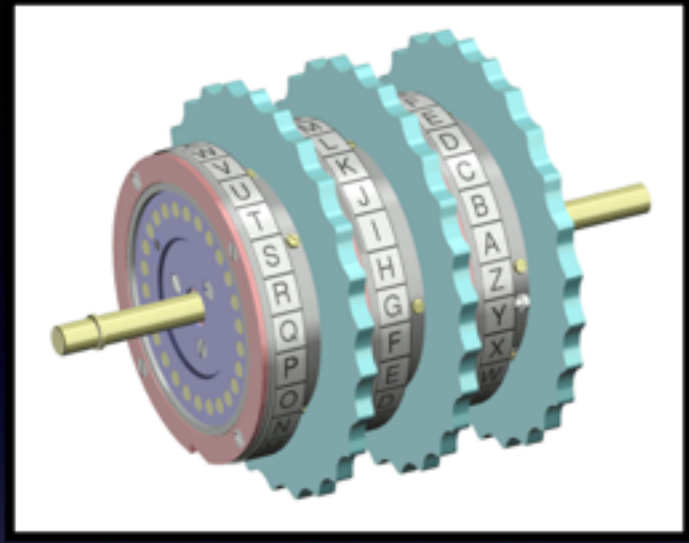
Church-Turing hypothese:
voor elk algoritme bestaat er een Turingmachine
die het kan uitvoeren

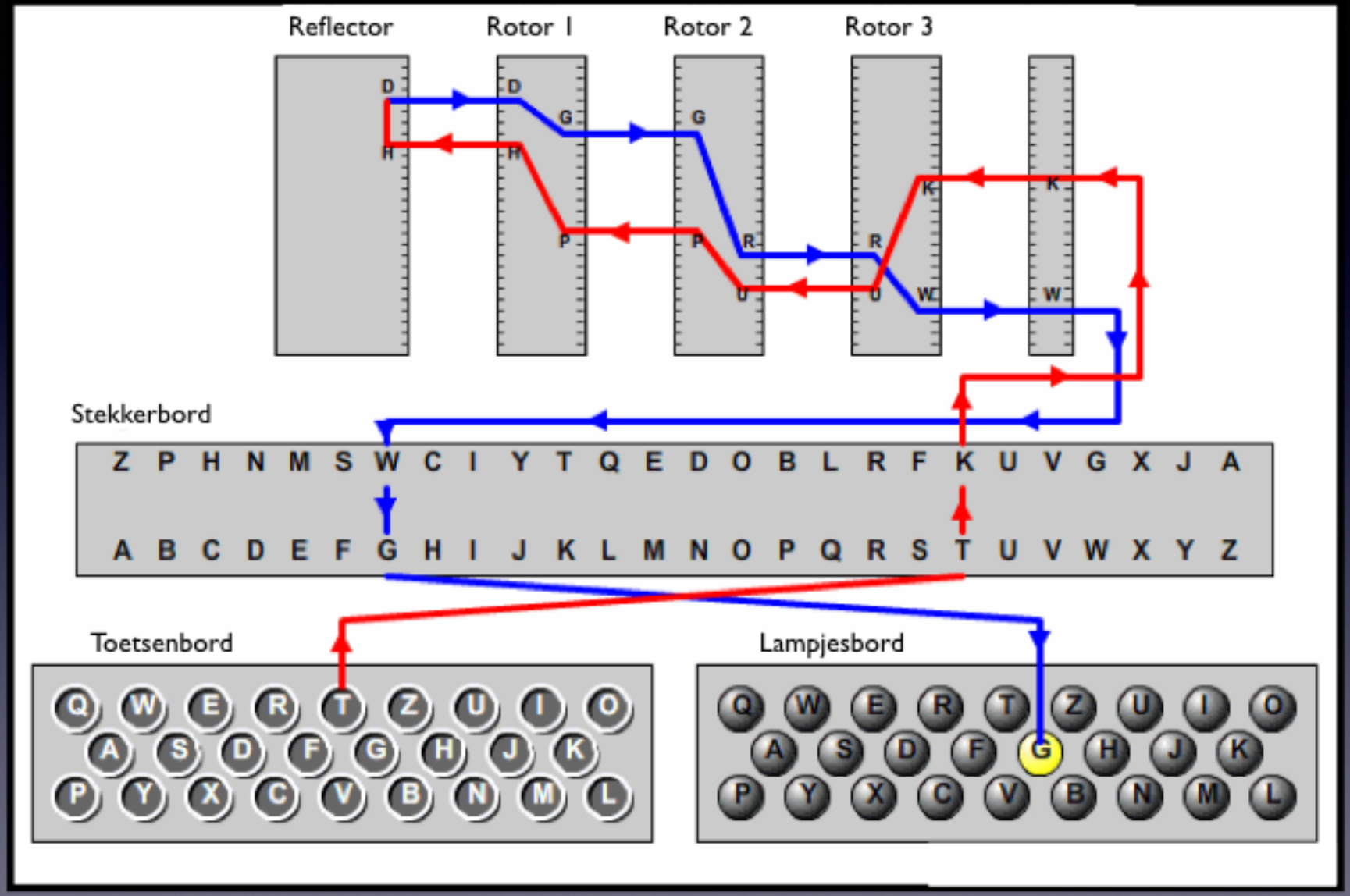
The Imitation Game: Alan Turing op sollicitatiegesprek om Enigma te kraken

Enigma-codeermachine




Toetsenbord
Scrambler
Lampjesbord
a → B
b → A
c → D
d → F
e → E
f → C
a → D
b → C
c → B
d → E
e → A
f → F
a → A
b → E
c → D
d → C
e → F
f → B




Reflector
Rotor 1
Rotor 2
Rotor 3
Stekkerbord
Z P H N M S W C I Y T Q E D O B L R F K U V G X J 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
Toetsenbord
Lampjesbord

Stekkerbord:
verwissel twee letters

3 rotors

26 letters

Aantal mogelijke sleutels:

1. volgorde 3 rotoren: 3 x 2 x 1 = 6 mogelijkheden
2. 3 rotoren met elk 26 letters: 26 x 26 x 26 = 17.576 mogelijkheden
3. stekkerbord (m kabeltjes verwisselen elk twee van 26 letters):

$$\frac{n!}{(n-2m)m!2^m}$$

205.552.193.096.250 mogelijkheden
getal met 15 nullen: 10^{15}

Totaal: in de orde van 10^{19} mogelijkheden

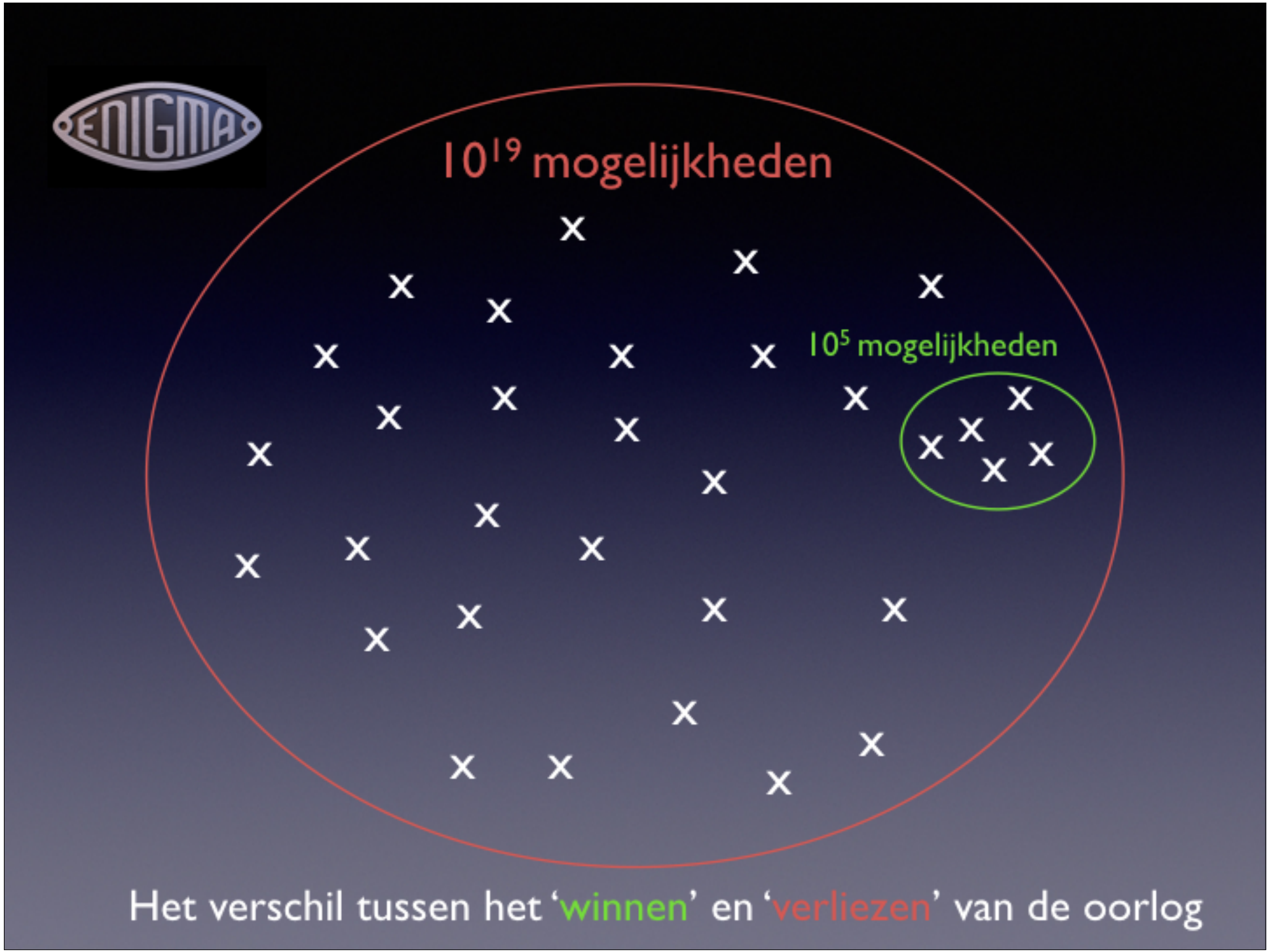
Duitse codeboeken

Geheim! 02 ❁

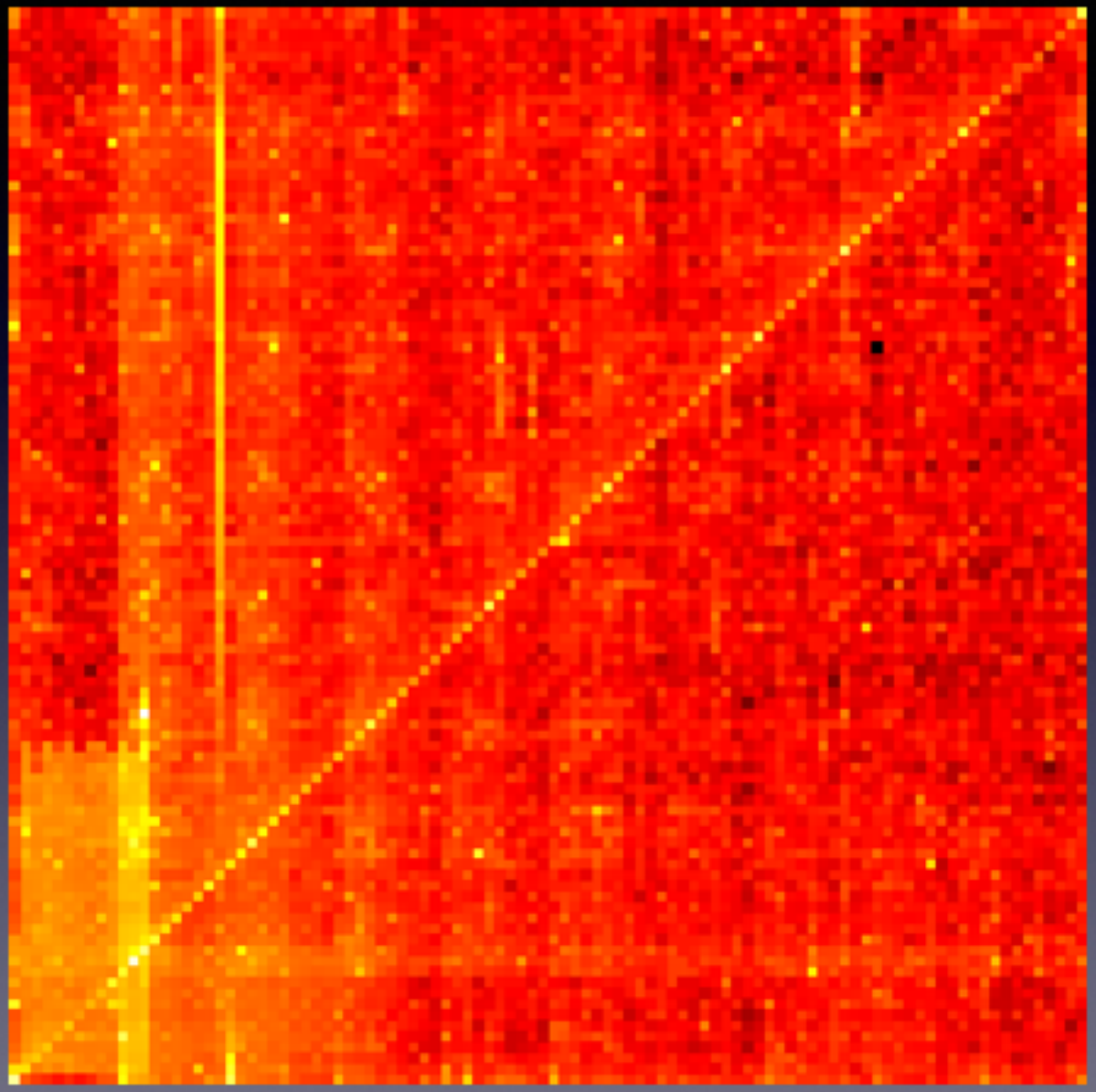
Nicht ins Flugzeug mitzunehmen!

Sonder-Maschinenschlüssel BHG

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	III II IV	24 09 04	UQ DS IH XW BM GC EZ JR YT FO	scc zod ogk oxz
30.	IV I III	11 16 14	TX ZN YP CE LD FA RW UK MH OV	gku mck mhw civ
29.	III I II	21 06 02	BR NQ AY EK FO IP MC ZU GJ XW	xcv lkw rty wqg
28.	IV III II	15 17 25	JC NZ UV DT MA XI LQ OE WY PS	mjc itl yhg aqs
27.	V IV I	03 26 20	WQ CV SM YK AF JO ZN LD HI EP	ypu zxv uzw nkw
26.	IV II I	07 19 13	RF MI GH UL EC DP YA WN TZ VK	cmz wcr uls buo
25.	I V II	25 06 15	UI SK QY WF CX VL JN HM GZ DR	zsb awv xkf cah
24.	V III I	11 04 06	WG UH CS QE ID BJ MK VL RZ TA	ksn tiq anu iwj
23.	IV II III	01 15 09	KI WU AG LJ ET PQ MR CN HO ZY	ihr rih yxe wxv
22.	III IV I	22 05 16	EA KQ TG PL SD JF IM XC BV WZ	rox toq yqx noh
21.	IV I II	20 11 04	XR ZM FY IH KN CW AB DP OG SU	rfx kic gbz kfv
20.	I IV V	16 22 12	DO CR FA GZ WE KS HV BU XP JT	ewe amy fzp pzy
19.	II IV I	19 08 21	XL RU MB OT QW AI SV FP YE CJ	gyr ona atm fyk
18.	IV I V	22 05 07	MW GB SY IZ XP NQ FK CH UL AT	fch
17.	III V I	12 18 23	HN SB TG EZ UX WM JC YV OP ID	mwr
16.	IV V III	03 15 05	YS ZI JL WD VX CB PN OM UT AK	rdi
15.	II V IV	24 17 25	AC IF JV DN MB GO SP RW TL XZ	rey
14.	III I V	04 13 23	DM KP AI PC LY QN GS ZR UX TH	ydl
13.	V IV III	21 03 17	VY AQ KR OL JX UP CT FN DI ZM	afe
12.	I II V	16 22 10	XF VW IB YO PD SM ZJ CG KU LT	avx
11.	V III II	13 26 05	MH QN IF GT WO LS ZK XV EY BP	iwn
10.	IV I III	23 01 21	PI AU QG NW TB RK LF SV CM OD	vkk
9.	V II IV	12 16 10	NJ OX BE MQ GP WY VZ FI TS RH	bqj
8.	III II V	06 02 07	UQ LI RJ XY OZ DA HS NV GT KW	pfa
7.	V II III	18 09 10	HP XJ RV GF YE CU SK WZ AB QD	haa
6.	IV II V	11 07 14	LH BJ EW RO DI QF GV PK CX MS	ppw
5.	V III I	17 20 02	QA FE ZM VI NH OJ RC PU GT KX	ede
4.	IV V III	22 07 24	SK NO FR AX QP HW DT EM VY JU	hfp
3.	V II I	12 04 02	CV DH OE PU WJ XR NS IB AZ KM	glf
2.	IV V I	18 01 23	UQ OF IK YC LR BJ WZ DH PM XN	jtn
1.	V III IV	12 09 26	QL XF VZ AT CH KU IM RP EG YW	buv

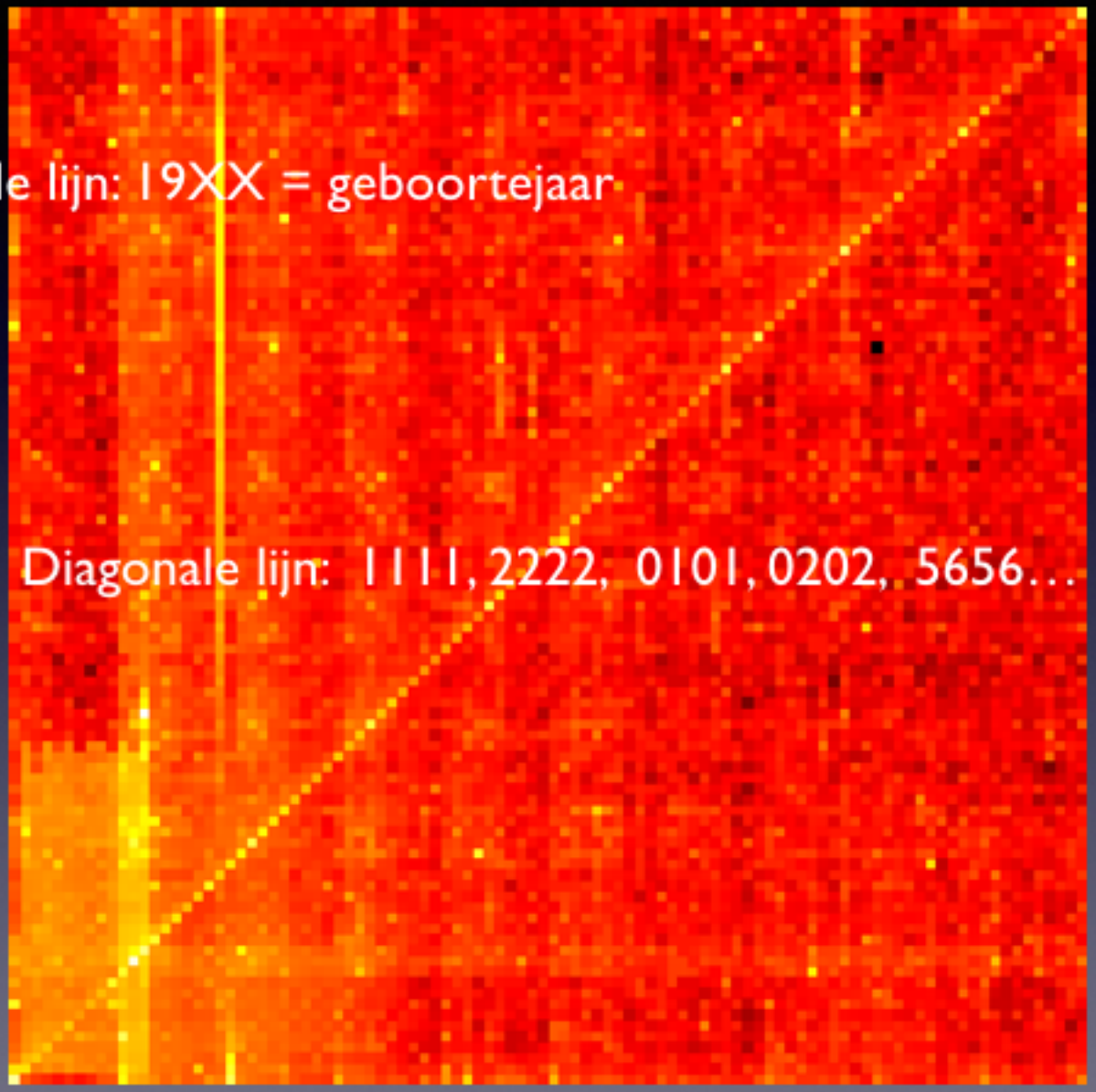

ENIGMA
10^{19} mogelijkheden
10^{5} mogelijkheden
Het verschil tussen het 'winnen' en 'verliezen' van de oorlog

Patronen in pincodes van 4 cijfers



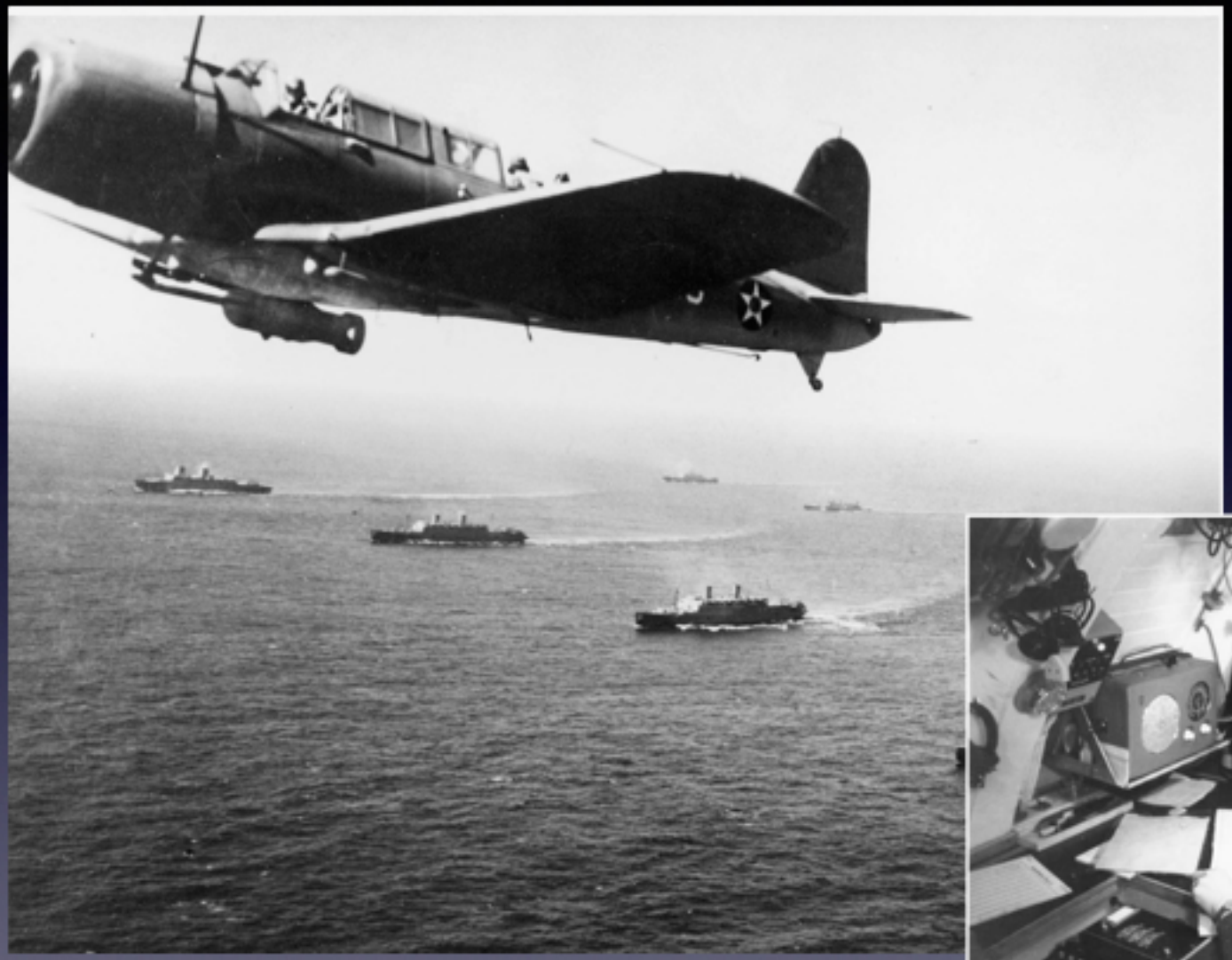
Hoe lichter de kleur
hoe vaker de
pin-code voorkomt

Patronen in pincodes van 4 cijfers



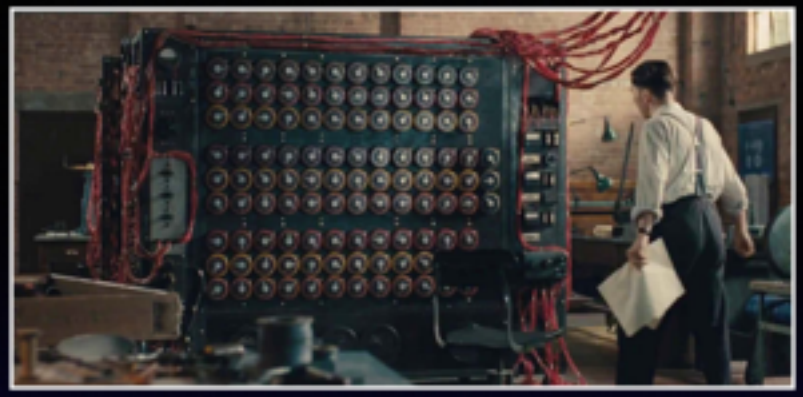
Poolse wiskundigen o.l.v. Marian Rejewski kraken Enigma voor het eerst in 1932

14 augustus 1939: Oprichting Bletchley Park
Engelse codekrakers



Slag op de Atlantische Oceaan

Enigma kraken



- Hoe zit Enigma-machine in elkaar? (gebruiksaanwijzing via spionage)
- Zwakheid 1 - Enigma: letter wordt niet zichzelf
- Zwakheid 2 - Enigma: X → Y dan Y → X
- TURING: Raad woord + positie woord in geheime bericht (wiskunde + taalkunde + psychologie)
- Codeboeken buit maken + weerberichten ontcijferen
- Bombes bouwen (machinaal mogelijkheden uitproberen)

Woord geraden in weerbericht van D-day (6 juni 1944):

WETTERVORHERSAGEBISKAYA

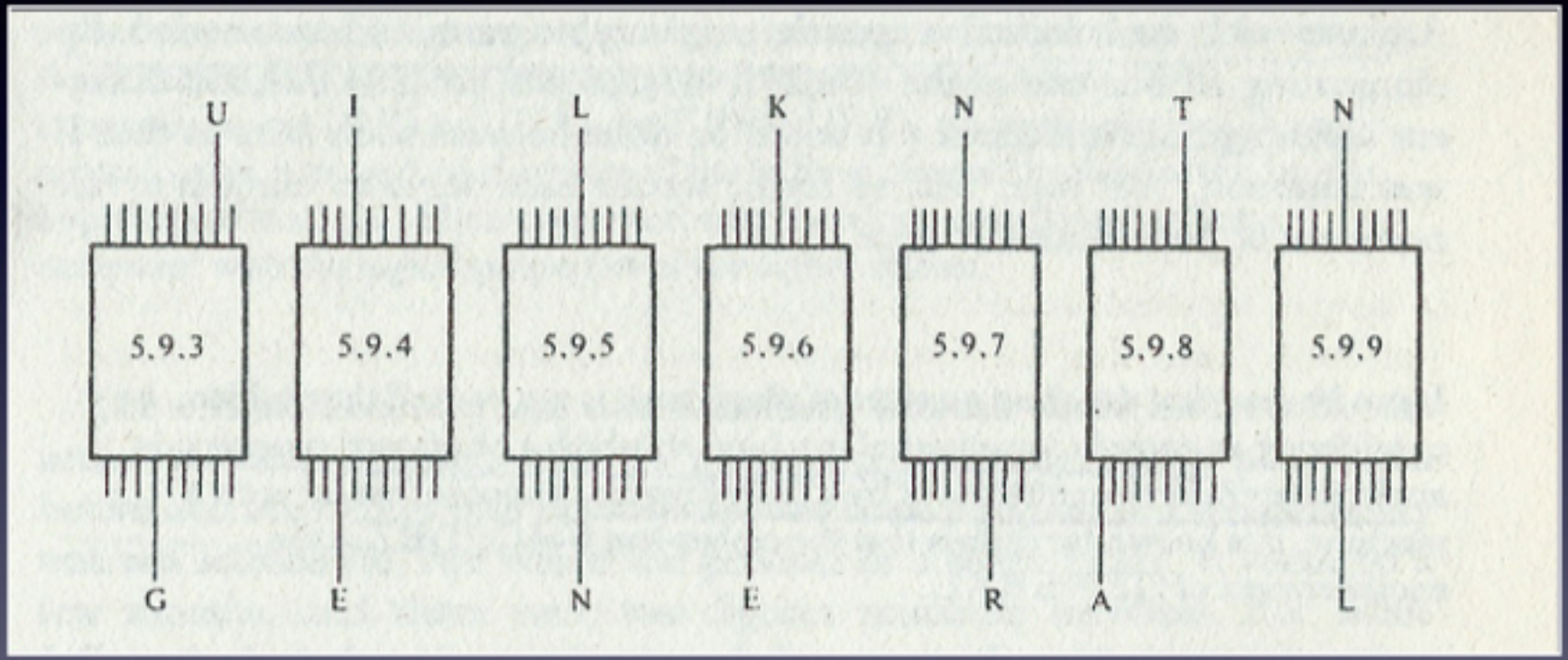
```
VPZRKHXTLDHMY[A]LQEXUN[A]KCKZJ
WETTERVORHERS[A]GEBISK[A]YA
```

```
VPZRKHXTLDHMYALQ[E]XUNAKCKZJ
 WETTERVORHERSAG[E]BISKAYA
```

```
VPZRKHXTLDHMYALQEXUNA[K]CKZJ
  WETTERVORHERSAGEBIS[K]AYA
```

```
VPZRKHXTLDHMYALQEXUNAKCKZJ
WETTERVORHERSAGEBISKAYA
```

Bij welke rotorposities volgt GENERAL uit UILKNTN?



Gebruik 7 Bombes tegelijk om voor 7 letters tegelijk
te testen welke rotorstanden kloppen
probeer alle rotorvolgordes; stekkercombinaties, beginletterinstellingen

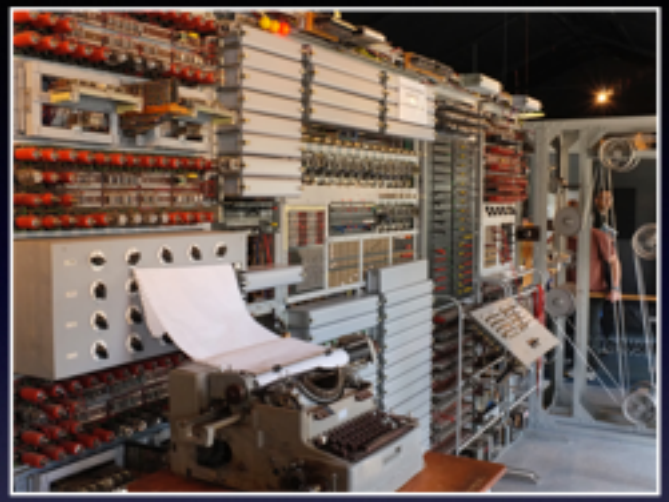
The Imitation Game: Alan Turing verdedigt zijn code-krakende machine

1942: Turing (30 jaar) en collega's kraken
de Duitse marine-Enigma met Bombes

Enigma-codeermachine

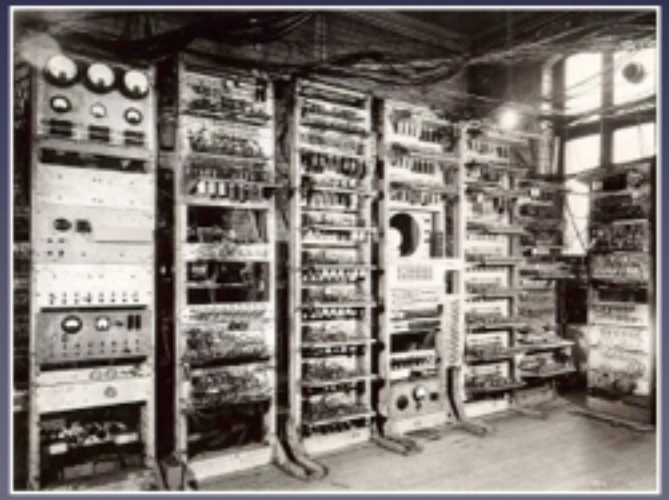
Bombe (Enigma-breker)

Is Turing de uitvinder van de computer?



Colossus (1943, UK): single purpose: codes kraken
(Tom Flowers)

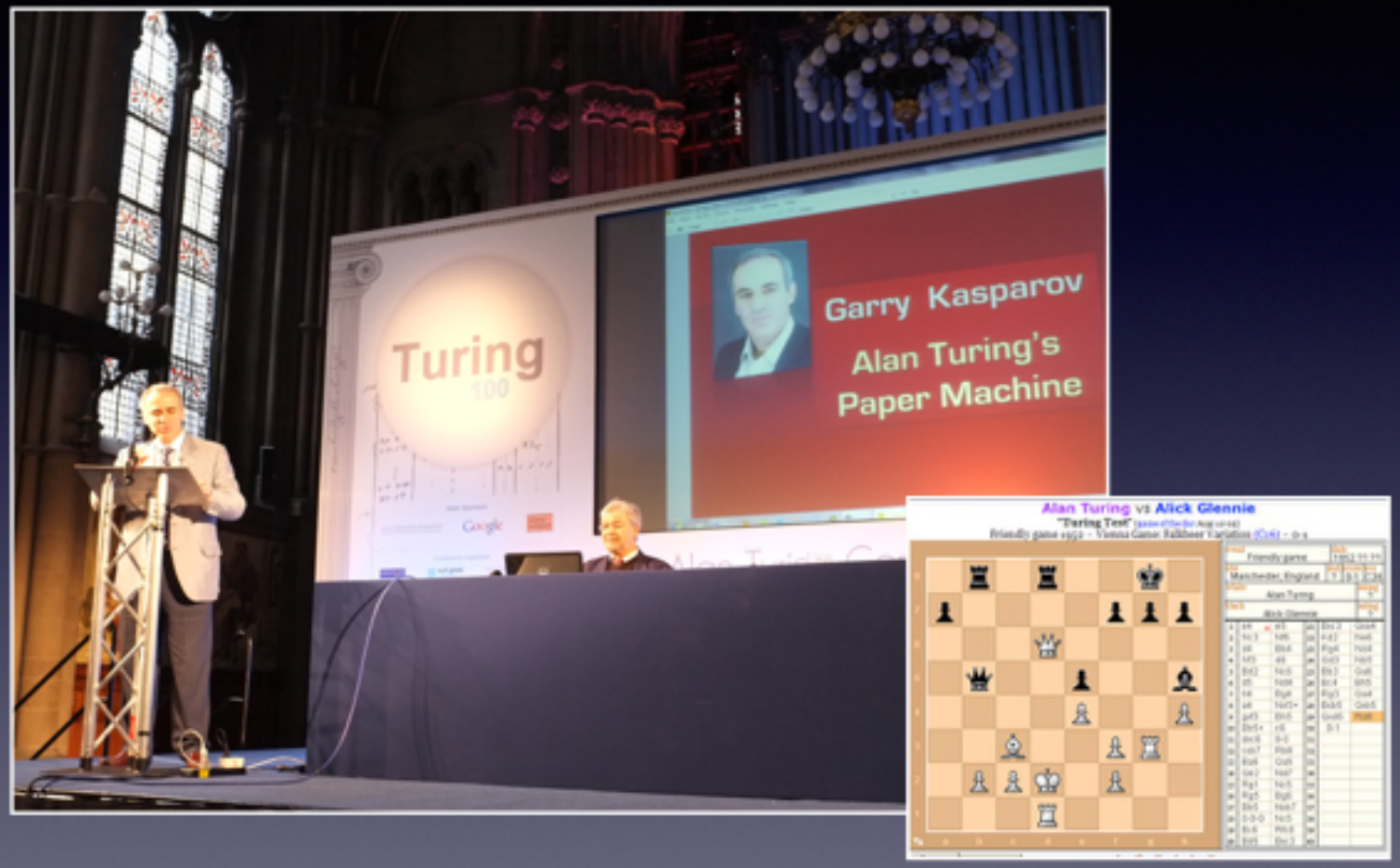
ENIAC (1946, VS): single purpose: ballistische berekeningen
(John Mauchly en J. Presper Eckert)



Manchester 'Baby' & Manchester Mark 1 (1948, 1949, UK):
stored program general purpose
(Frederic Williams en Tom Kilburn)

EDSAC (1949, UK): stored program general purpose
(Maurice Wilkes)

1941: Turing (29 jaar):
Is schaken oplosbaar door een computer?



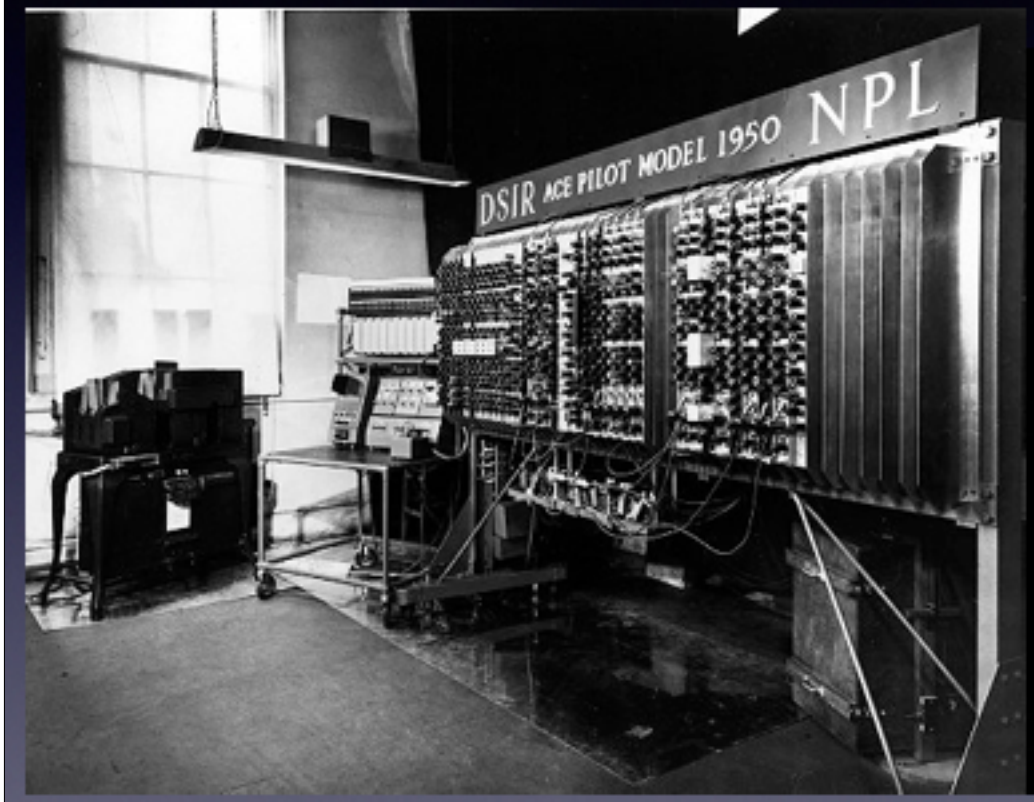
1948: Turing (36 jaar) schrijft het eerste computerschaakprogramma

Garry Kasparov over Alan Turings eerste computerschaakprogramma:

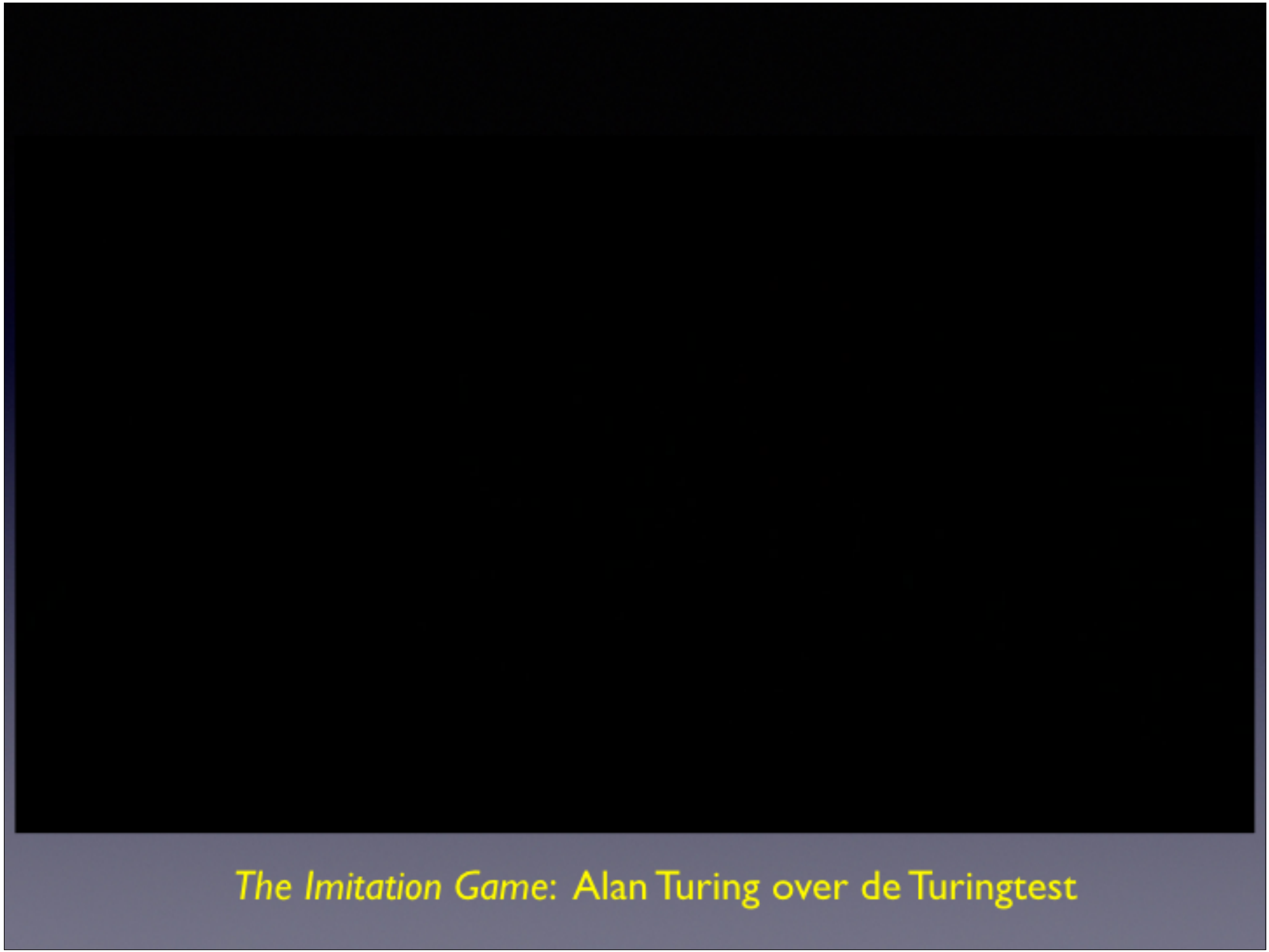
"He wrote algorithms without having a computer – many young scientists would never believe that was possible. It was an outstanding accomplishment."

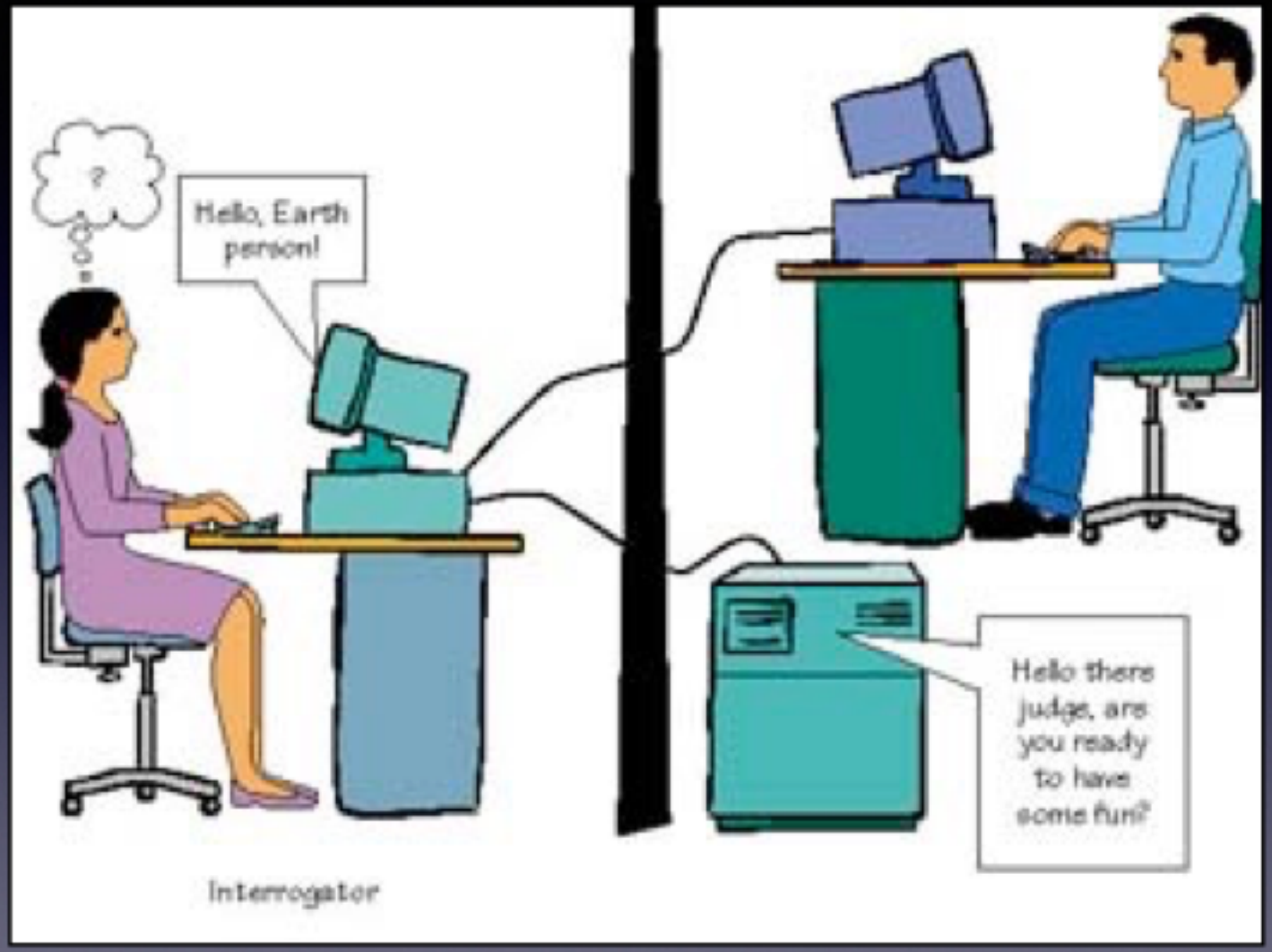
Alan Turings schaakprogramma (wit) vs. Garry Kasparov (zwart) (Manchester, juni 2012)

Alan Turing (38 jaar) in 1950:
"Kunnen machines denken?"



Turing Test


The Imitation Game: Alan Turing over de Turingtest


?
Hello, Earth person!
Hello there judge, are you ready to have some fun?
Interrogator

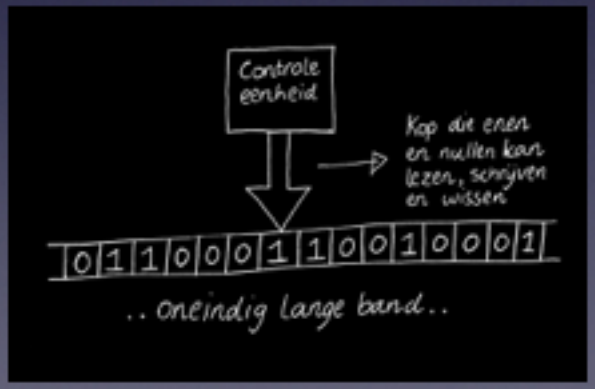
Het enigma Alan Turing

7 juni 1954: Alan Turing sterft op 41-jarige leeftijd

Alan Turing: pionier van het digitale tijdperk

"software voor elk bekend proces" (1946)

Turing machine (1936)



smartphones

tablets

computers

The Imitation Game