

Het raadsel Enigma

Nationale Wiskunde Dagen 2024

Stijn Maatje

5 april 2024

Inhoud

Deel I

- Context
- Werking Enigmamachine
- Gekraakt door de Polen
- Gekraakt door de Britten

Deel II

- Zelf aan de slag!

Cryptografie

Cryptografie

Cryptografie

Cryptografie is het gebruik van geheimschrift.

Cryptografie

Cryptografie is het gebruik van geheimschrift.

Crypto-analyse is het (proberen te) kraken van geheimschrift.

Cryptografie

Cryptografie is het gebruik van geheimschrift.

Crypto-analyse is het (proberen te) kraken van geheimschrift.

nationale wiskunde dagen

Cryptografie

Cryptografie is het gebruik van geheimschrift.

Crypto-analyse is het (proberen te) kraken van geheimschrift.

```
nationale wiskunde dagen  
QDWLRQDOH ZLVNXQGH GDJHQ
```

Cryptografie

Cryptografie is het gebruik van geheimschrift.

Crypto-analyse is het (proberen te) kraken van geheimschrift.

```
nationale wiskunde dagen  
QDWLRQDOH ZLVNXQGH GDJHQ
```

Notatie: $\sigma = (\text{adgjmpsvybehknqtwzcfilorux}) \in \mathcal{S}_{26}$

Cryptografie

Cryptografie is het gebruik van geheimschrift.

Crypto-analyse is het (proberen te) kraken van geheimschrift.

```
nationale wiskunde dagen  
QDWLRQDOH ZLVNXQGH GDJHQ
```

Notatie: $\sigma = (\text{adgjmpsvybehknqtwzcfilorux}) \in \mathcal{S}_{26}$

Cryptografie: Caesarversleuteling

Cryptografie

Cryptografie is het gebruik van geheimschrift.

Crypto-analyse is het (proberen te) kraken van geheimschrift.

```
    nationale wiskunde dagen  
    QDWLRQDOH ZLVNXQGH GDJHQ
```

Notatie: $\sigma = (\text{adgjmpsvybehknqtwzcfilorux}) \in S_{26}$

Cryptografie: Caesarversleuteling

Crypto-analyse: Frequentieanalyse door Al-Kindi in de 9e eeuw.

Cryptografie

Cryptografie is het gebruik van geheimschrift.

Crypto-analyse is het (proberen te) kraken van geheimschrift.

```
nationale wiskunde dagen  
QDWLRQDOH ZLVNXQGH GDJHQ
```

Notatie: $\sigma = (\text{adgjmpsvybehknqtwzcfilorux}) \in S_{26}$

Cryptografie: Caesarversleuteling

Crypto-analyse: Frequentieanalyse door Al-Kindi in de 9e eeuw.

Cryptologie: wedstrijd tussen cryptografie en crypto-analyse.

Rotormachine

Rotormachine

- 1915: Theo van Hengel en Rudolf Spengler

Rotormachine

- 1915: Theo van Hengel en Rudolf Spengler
- 1918: Arthur Scherbius

Rotormachine

- 1915: Theo van Hengel en Rudolf Spengler
- 1918: Arthur Scherbius: *Enigma*

Rotormachine

- 1915: Theo van Hengel en Rudolf Spengler
- 1918: Arthur Scherbius: *Enigma*



Figuur: Een Enigmamachine

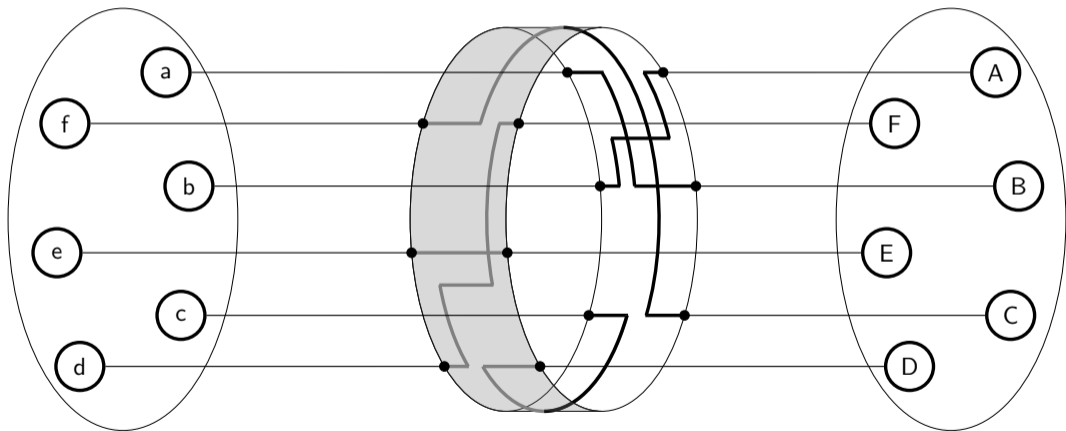
Rotormachine

- 1915: Theo van Hengel en Rudolf Spengler
- 1918: Arthur Scherbius: *Enigma*
- 30.000 exemplaren verkocht aan leger

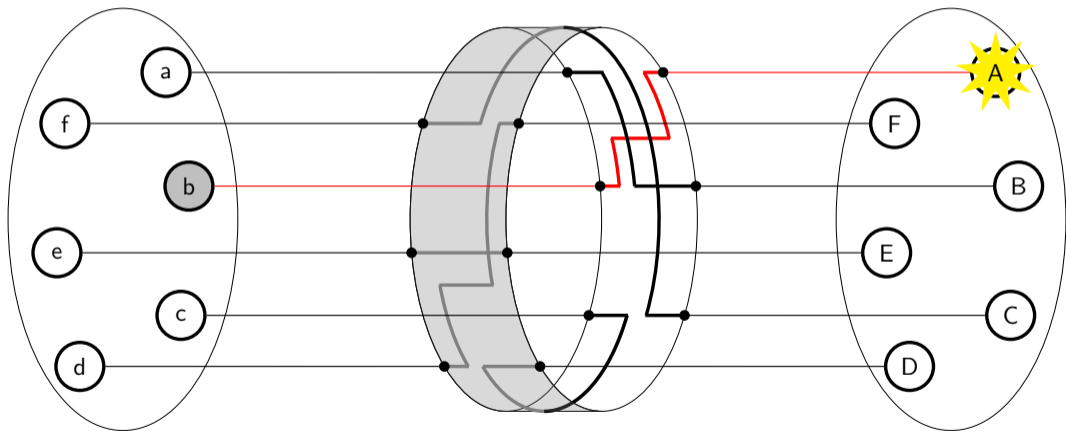


Figuur: Een Enigmamachine

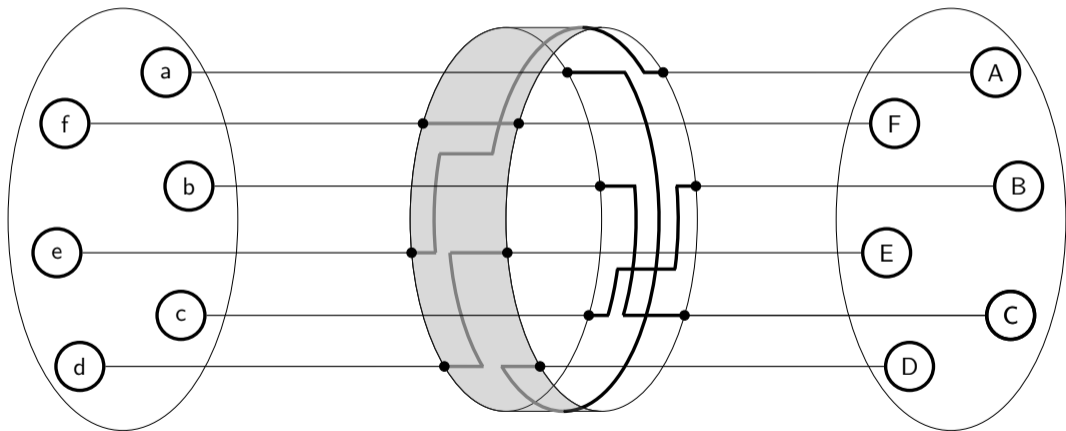
Werking Enigma (1)



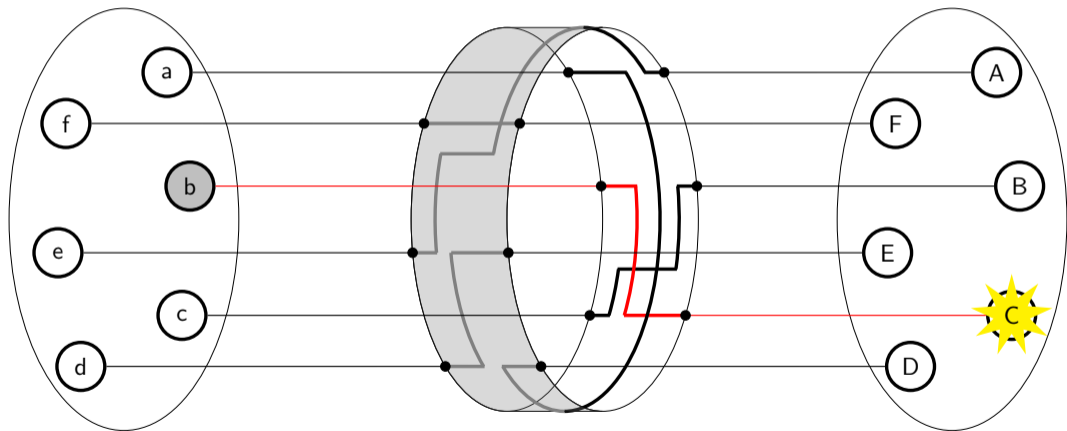
Werking Enigma (2)



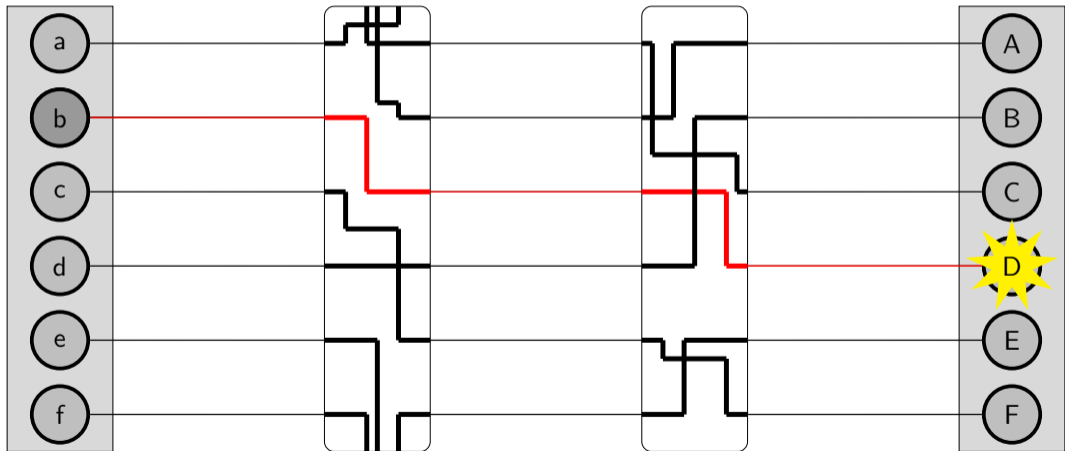
Werking Enigma (3)



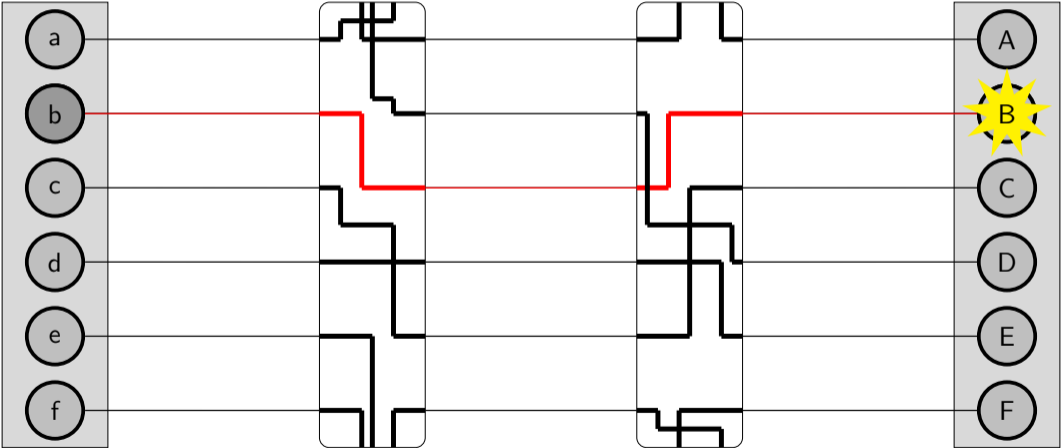
Werking Enigma (4)



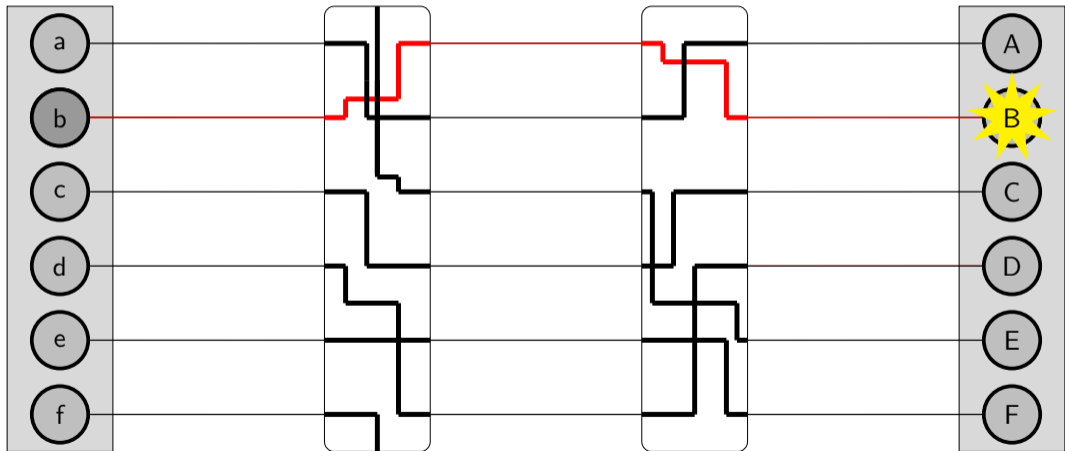
Werking Enigma (5)



Werking Enigma (6)



Werking Enigma (7)



1 Bericht gaat op slot met een sleutel

- 1 Bericht gaat op slot met een sleutel
- 2 $1,59 \cdot 10^{20}$ sleutels

- ① Bericht gaat op slot met een sleutel
- ② $1,59 \cdot 10^{20}$ sleutels

Geheim - Heer - Maschinenschlüssel für Monat Mai 1938 - Allgemeine

Tag	Walzenlage	Ringstellung	Grundstellung	Steckerverbindungen	K.E.G.	Kennguppen
31.	III I II	A P L	B O I	HZ RV BG AD EY LP	2	zpe vtm hxz vms
30.	I III II	I V K	W S N	CP EZ IQ FT WX HJ	3	vjc sjw vtk ziw
29.	III I II	Y E C	D Y H	BZ KS IV EP DR JU	3	lqo var xmx tsw
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Tabel: Sleutelblad voor de periode 1937-1938

Enigma in Polen (1932)

- Dreiging van Duitsland in het westen en de Sovjet-Unie in het oosten

Enigma in Polen (1932)

- Dreiging van Duitsland in het westen en de Sovjet-Unie in het oosten
- Het *Buro Szyfrów* in Warschau

Enigma in Polen (1932)

- Dreiging van Duitsland in het westen en de Sovjet-Unie in het oosten
- Het *Buro Szyfrów* in Warschau
- Rejewski, Różycki, Zygalski



Figuur: Marian Rejewski (1905-1980)



De Polen hadden twee doelen:

- 1 Interne bedrading van de rotoren bepalen
- 2 Een snelle, betrouwbare manier ontwikkelen om Enigmaberichten te ontcijferen

De Polen hadden twee doelen:

- 1 **Interne bedrading van de rotoren bepalen**
- 2 Een snelle, betrouwbare manier ontwikkelen om Enigmaberichten te ontcijferen

Procedure (1932)

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

We willen `euler` versleutelen

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

We willen `euler` versleutelen

Stel machine in volgens **Tagesschlüssel**.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

We willen `euler` versleutelen

Stel machine in volgens **Tagesschlüssel**.

Bedenk berichtsleutel:

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

We willen `euler` versleutelen

Stel machine in volgens **Tagesschlüssel**.

Bedenk berichtsleutel: LBD.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

We willen `euler` versleutelen

Stel machine in volgens **Tagesschlüssel**.

Bedenk berichtsleutel: LBD.

Versleutel de berichtsleutel twee keer:

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

We willen `euler` versleutelen

Stel machine in volgens **Tagesschlüssel**.

Bedenk berichtsleutel: `LBD`.

Versleutel de berichtsleutel twee keer: `BXUQJH`.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

We willen `euler` versleutelen

Stel machine in volgens **Tagesschlüssel**.

Bedenk berichtsleutel: LBD.

Versleutel de berichtsleutel twee keer: BXUQJH.

Stel **Ringstellung** in volgens berichtsleutel, LBD.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

We willen `euler` versleutelen

Stel machine in volgens **Tagesschlüssel**.

Bedenk berichtsleutel: LBD.

Versleutel de berichtsleutel twee keer: BXUQJH.

Stel **Ringstellung** in volgens berichtsleutel, LBD.

Typ nu `euler` in, dan krijgen we KSPPB.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Vercijferen:

We willen `euler` versleutelen

Stel machine in volgens **Tagesschlüssel**.

Bedenk berichtsleutel: LBD.

Versleutel de berichtsleutel twee keer: BXUQJH.

Stel **Ringstellung** in volgens berichtsleutel, LBD.

Typ nu `euler` in, dan krijgen we KSPPB.

We versturen BXUQJHKSPPB.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Ontcijferen van BXUQJHKSPPB:

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Ontcijferen van BXUQJHKSPPB:
Stel machine in volgens **Tagesschlüssel**.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Ontcijferen van BXUQJHKSPPB:
Stel machine in volgens **Tagesschlüssel**.
Typ de eerste zes letters, BXUQJH in.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Ontcijferen van BXUQJHKSPPB:
Stel machine in volgens **Tagesschlüssel**.
Typ de eerste zes letters, BXUQJH in.
We krijgen dan LBDLBD.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Ontcijferen van BXUQJHKSPPB:

Stel machine in volgens **Tagesschlüssel**.

Typ de eerste zes letters, BXUQJH in.

We krijgen dan LBDLBD.

Stel **Ringstellung** in volgens berichtsleutel, LBD.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

Procedure (1932)

Ontcijferen van BXUQJHKSPPB:

Stel machine in volgens **Tagesschlüssel**.

Typ de eerste zes letters, BXUQJH in.

We krijgen dan LBDLBD.

Stel **Ringstellung** in volgens berichtsleutel, LBD.

Typ nu KSPPB in, we krijgen dan euler.

Tagesschlüssel

- **Datum:** 5
- **Walzenlage:**
III I II
- **Grundstellung:**
R K P
- **Steckerverbindungen:**
AI NR JF PX KW TQ

We kijken steeds naar de eerste zes letters van een bericht, bijvoorbeeld BXUQJH.

We kijken steeds naar de eerste zes letters van een bericht, bijvoorbeeld BXUQJH.
Permutatie π_1 verticijfert de eerste letter, permutatie π_2 verticijfert de tweede letter, ...,
permutatie π_6 verticijfert de zesde letter.

We kijken steeds naar de eerste zes letters van een bericht, bijvoorbeeld BXUQJH.
Permutatie π_1 verticaalfert de eerste letter, permutatie π_2 verticaalfert de tweede letter, ...,
permutatie π_6 verticaalfert de zesde letter.

$$B \xrightarrow{\pi_1} \alpha \quad \alpha \xrightarrow{\pi_4} Q$$

$$X \xrightarrow{\pi_2} \beta \quad \beta \xrightarrow{\pi_5} J$$

$$U \xrightarrow{\pi_3} \gamma \quad \gamma \xrightarrow{\pi_6} H$$

We kijken steeds naar de eerste zes letters van een bericht, bijvoorbeeld BXUQJH.
Permutatie π_1 verticaalfert de eerste letter, permutatie π_2 verticaalfert de tweede letter, ...,
permutatie π_6 verticaalfert de zesde letter.

$$B \xrightarrow{\pi_1} \alpha \quad \alpha \xrightarrow{\pi_4} Q$$

$$X \xrightarrow{\pi_2} \beta \quad \beta \xrightarrow{\pi_5} J$$

$$U \xrightarrow{\pi_3} \gamma \quad \gamma \xrightarrow{\pi_6} H$$

$$\pi_1\pi_4 = (\dots)(\dots b q \dots)(\dots)$$

$$\pi_2\pi_5 = (\dots)(\dots x j \dots)(\dots)$$

$$\pi_3\pi_6 = (\dots)(\dots u h \dots)(\dots)$$

AUQ	AMN	IND	JHU	PVJ	FEG	SJM	SPO	WTM	RAO
BNH	CHL	JWF	MIC	QGA	LYB	SJM	SPO	WTM	RAO
BCT	CGJ	JWF	MIC	QGA	LYB	SJM	SPO	WTM	RAO
CIK	BZT	KHB	XJV	RJL	WPX	SUG	SMF	WKI	RKK
DDB	VDV	KHB	XJV	RJL	WPX	SUG	SMF	XRS	GNM
EJP	IPS	LDR	HDE	RJL	WPX	TMN	EBY	XRS	GNM
FBR	KLE	LDR	HDE	RJL	WPX	TMN	EBY	XOI	GUK
GPB	ZSV	MAW	UXP	RFC	WQQ	TAA	EXB	XYW	GCP
HNO	THD	MAW	UXP	SYX	SCW	USE	NWH	YPC	OSQ
HNO	THD	NXD	QTU	SYX	SCW	VII	PZK	YPC	OSQ
HXV	TTI	NXD	QTU	SYX	SCW	VII	PZK	ZZY	YRA
IKG	JKF	NLU	QFZ	SYX	SCW	VQZ	PVR	ZEF	YOC
IKG	JKF	OBU	DLZ	SYZ	SCW	VQZ	PVR	ZSJ	YWG

Tabel: Eerste 6 letters van 65 onderschepte berichten

$\pi_1\pi_4 = (a) (bc) (dvpfkxgzyo) (eijmunqlht) (rw) (s)$
 $\pi_2\pi_5 = (axt) (blfqveoum) (cgy) (d) (hjpswizrn) (k)$
 $\pi_3\pi_6 = (abviktjgfcqny) (duzrehlxwpsmo)$

$\pi_1\pi_4 = (a) (bc) (dvpfkxgzyo) (eijmunqlht) (rw) (s) \quad 1, 1, 2, 2, 10, 10$
 $\pi_2\pi_5 = (axt) (blfqveoum) (cgy) (d) (hjpswizrn) (k) \quad 1, 1, 3, 3, 9, 9$
 $\pi_3\pi_6 = (abviktjgfcqny) (duzrehlxwpsmo) \quad 13, 13$

$$\begin{aligned}
 \pi_1\pi_4 &= (a) (bc) (dvpfkxgzyo) (eijmunqlht) (rw) (s) && 1, 1, 2, 2, 10, 10 \\
 \pi_2\pi_5 &= (axt) (blfqveoum) (cgy) (d) (hjpswizrn) (k) && 1, 1, 3, 3, 9, 9 \\
 \pi_3\pi_6 &= (abviktjgfcqny) (duzrehlxwpsmo) && 13, 13
 \end{aligned}$$

Stelling van Rejewski

Een permutatie $\sigma \in S_{26}$ is gekoppeld dan en slechts dan als σ het product is van twee permutaties van de vorm

$$\tau = (a_1 a_2)(a_3 a_4) \dots (a_{23} a_{24})(a_{25} a_{26}).$$

AUQ	AMN	IND	JHU	PVJ	FEG	SJM	SPO	WTM	RAO
BNH	CHL	JWF	MIC	QGA	LYB	SJM	SPO	WTM	RAO
BCT	CGJ	JWF	MIC	QGA	LYB	SJM	SPO	WTM	RAO
CIK	BZT	KHB	XJV	RJL	WPX	SUG	SMF	WKI	RKK
DDB	VDV	KHB	XJV	RJL	WPX	SUG	SMF	XRS	GNM
EJP	IPS	LDR	HDE	RJL	WPX	TMN	EBY	XRS	GNM
FBR	KLE	LDR	HDE	RJL	WPX	TMN	EBY	XOI	GUK
GPB	ZSV	MAW	UXP	RFC	WQQ	TAA	EXB	XYW	GCP
HNO	THD	MAW	UXP	SYX	SCW	USE	NWH	YPC	OSQ
HNO	THD	NXD	QTU	SYX	SCW	VII	PZK	YPC	OSQ
HXV	TTI	NXD	QTU	SYX	SCW	VII	PZK	ZZY	YRA
IKG	JKF	NLU	QFZ	SYX	SCW	VQZ	PVR	ZEF	YOC
IKG	JKF	OBU	DLZ	SYZ	SCW	VQZ	PVR	ZSJ	YWG

Tabel: Eerste 6 letters van 65 onderschepte berichten

AUQ	AMN	IND	JHU	PVJ	FEG	SJM	SPO	WTM	RAO
BNH	CHL	JWF	MIC	QGA	LYB	SJM	SPO	WTM	RAO
BCT	CGJ	JWF	MIC	QGA	LYB	SJM	SPO	WTM	RAO
CIK	BZT	KHB	XJV	RJL	WPX	SUG	SMF	WKI	RKK
DDB	VDV	KHB	XJV	RJL	WPX	SUG	SMF	XRS	GNM
EJP	IPS	LDR	HDE	RJL	WPX	TMN	EBY	XRS	GNM
FBR	KLE	LDR	HDE	RJL	WPX	TMN	EBY	XOI	GUK
GPB	ZSV	MAW	UXP	RFC	WQQ	TAA	EXB	XYW	GCP
HNO	THD	MAW	UXP	SYX	SCW	USE	NWH	YPC	OSQ
HNO	THD	NXD	QTU	SYX	SCW	VII	PZK	YPC	OSQ
HXV	TTI	NXD	QTU	SYX	SCW	VII	PZK	ZZY	YRA
IKG	JKF	NLU	QFZ	SYX	SCW	VQZ	PVR	ZEF	YOC
IKG	JKF	OBU	DLZ	SYZ	SCW	VQZ	PVR	ZSJ	YWG

Tabel: Eerste 6 letters van 65 onderschepte berichten

Vermoeden: SYXSCW is twee keer de bericht sleutel **AAA**.

$$S \xrightarrow{\pi_1} \alpha \quad \alpha \xrightarrow{\pi_4} S$$

$$Y \xrightarrow{\pi_2} \beta \quad \beta \xrightarrow{\pi_5} C$$

$$X \xrightarrow{\pi_3} \gamma \quad \gamma \xrightarrow{\pi_6} W$$

Vermoeden: SYXSCW is twee keer de bericht sleutel **AAA**.

$$S \xrightarrow{\pi_1} \mathbf{A} \quad \mathbf{A} \xrightarrow{\pi_4} S$$

$$Y \xrightarrow{\pi_2} \mathbf{A} \quad \mathbf{A} \xrightarrow{\pi_5} C$$

$$X \xrightarrow{\pi_3} \mathbf{A} \quad \mathbf{A} \xrightarrow{\pi_6} W$$

Vermoeden: SYXSCW is twee keer de bericht sleutel **AAA**.

$$S \xrightarrow{\pi_1} \mathbf{A} \quad \mathbf{A} \xrightarrow{\pi_4} S$$

$$Y \xrightarrow{\pi_2} \mathbf{A} \quad \mathbf{A} \xrightarrow{\pi_5} C$$

$$X \xrightarrow{\pi_3} \mathbf{A} \quad \mathbf{A} \xrightarrow{\pi_6} W$$

$$\pi_1 = (as) \dots$$

$$\pi_2 = (ay) \dots$$

$$\pi_3 = (ax) \dots$$

$$\pi_4 = (as) \dots$$

$$\pi_5 = (ac) \dots$$

$$\pi_6 = (aw) \dots$$

Vermoeden: SYXSCW is twee keer de bericht sleutel **AAA**.

$$S \xrightarrow{\pi_1} \mathbf{A} \quad \mathbf{A} \xrightarrow{\pi_4} S$$

$$Y \xrightarrow{\pi_2} \mathbf{A} \quad \mathbf{A} \xrightarrow{\pi_5} C$$

$$X \xrightarrow{\pi_3} \mathbf{A} \quad \mathbf{A} \xrightarrow{\pi_6} W$$

$\pi_1 = (as) (br) (cw) (di) (ve) (pt) (fh) (kl) (xq) (gn) (zu) (ym) (oj)$

$\pi_2 = (ay) (bj) (ct) (dk) (ei) (fn) (gx) (hl) (mp) (ow) (qr) (su) (vz)$

$\pi_3 = (ax) (bl) (vh) (ie) (kr) (tz) (ju) (gd) (fo) (cm) (qs) (np) (yw)$

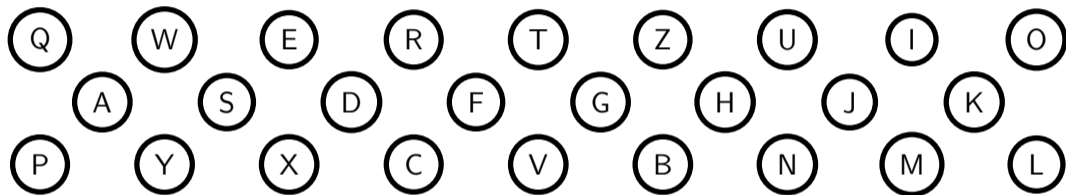
$\pi_4 = (as) (rc) (wb) (iv) (ep) (tf) (hk) (lx) (qg) (nz) (uy) (mo) (jd)$

$\pi_5 = (ac) (yx) (gc) (dk) (jl) (hf) (nq) (rv) (ze) (io) (wu) (sm) (pb)$

$\pi_6 = (aw) (xb) (lv) (hi) (ek) (rt) (zj) (ug) (df) (oc) (mq) (sn) (py)$

sss:	AUQ	AMN	ddd:	IKG	JKF	xxx:	QGA	LYB	ert:	VQZ	PVR
rfv:	BNH	CHL	dfg:	IND	JHU	bbb:	RJL	WPX	ccc:	WTM	RAO
rtz:	BCT	CGJ	ooo:	JWF	MIC	bnm:	RFC	WQQ	cde:	WKI	RKK
wer:	CIK	BZT	lll:	KHB	XJV	aaa:	SYX	SCW	qqq:	XRS	GNM
ikl:	DDB	VDV	kkk:	LDR	HDE	abc:	SJM	SPO	qwe:	XOI	GUK
vbn:	EJP	IPS	yyy:	MAW	UXP	asd:	SUG	SMF	qay:	XYW	GCP
hjk:	FBR	KLE	ggg:	NXD	QTU	ppp:	TMN	EBY	mmm:	YPC	OSQ
nml:	GPB	ZSV	ghj:	NLU	QFZ	pyx:	TAA	EXB	uvw:	ZZY	YRA
fff:	HNO	THD	jjj:	OBU	DLZ	zui:	USE	NWH	uio:	ZEF	YOC
fgh:	HXV	TTI	tzu:	PVJ	FEG	eee:	VII	PZK	uuu:	ZSJ	YWG

Tabel: Tabel van ontcijferde bericht sleutels



Figuur: De QWERTZ-layout van het toetsenbord van een Engimachine

$\pi_1 = (as) (br) (cw) (di) (ve) (pt) (fh) (kl) (xq) (gn) (zu) (ym) (oj)$
 $\pi_2 = (ay) (bj) (ct) (dk) (ei) (fn) (gx) (hl) (mp) (ow) (qr) (su) (vz)$
 $\pi_3 = (ax) (bl) (vh) (ie) (kr) (tz) (ju) (gd) (fo) (cm) (qs) (np) (yw)$
 $\pi_4 = (as) (rc) (wb) (iv) (ep) (tf) (hk) (lx) (qg) (nz) (uy) (mo) (jd)$
 $\pi_5 = (ac) (yx) (gc) (dk) (jl) (hf) (nq) (rv) (ze) (io) (wu) (sm) (pb)$
 $\pi_6 = (aw) (xb) (lv) (hi) (ek) (rt) (zj) (ug) (df) (oc) (mq) (sn) (py)$

Voor bepalen rotorbedrading nog wat nodig:

$\pi_1 = (as) (br) (cw) (di) (ve) (pt) (fh) (kl) (xq) (gn) (zu) (ym) (oj)$
 $\pi_2 = (ay) (bj) (ct) (dk) (ei) (fn) (gx) (hl) (mp) (ow) (qr) (su) (vz)$
 $\pi_3 = (ax) (bl) (vh) (ie) (kr) (tz) (ju) (gd) (fo) (cm) (qs) (np) (yw)$
 $\pi_4 = (as) (rc) (wb) (iv) (ep) (tf) (hk) (lx) (qg) (nz) (uy) (mo) (jd)$
 $\pi_5 = (ac) (yx) (gc) (dk) (jl) (hf) (nq) (rv) (ze) (io) (wu) (sm) (pb)$
 $\pi_6 = (aw) (xb) (lv) (hi) (ek) (rt) (zj) (ug) (df) (oc) (mq) (sn) (py)$

Voor bepalen rotorbedrading nog wat nodig:

- 1 Heel wat algebra gepriegel

$\pi_1 = (as) (br) (cw) (di) (ve) (pt) (fh) (kl) (xq) (gn) (zu) (ym) (oj)$
 $\pi_2 = (ay) (bj) (ct) (dk) (ei) (fn) (gx) (hl) (mp) (ow) (qr) (su) (vz)$
 $\pi_3 = (ax) (bl) (vh) (ie) (kr) (tz) (ju) (gd) (fo) (cm) (qs) (np) (yw)$
 $\pi_4 = (as) (rc) (wb) (iv) (ep) (tf) (hk) (lx) (qg) (nz) (uy) (mo) (jd)$
 $\pi_5 = (ac) (yx) (gc) (dk) (jl) (hf) (nq) (rv) (ze) (io) (wu) (sm) (pb)$
 $\pi_6 = (aw) (xb) (lv) (hi) (ek) (rt) (zj) (ug) (df) (oc) (mq) (sn) (py)$

Voor bepalen rotorbedrading nog wat nodig:

- 1 Heel wat algebra gepriegel
- 2 Informatie verkregen vanuit spionage

$\pi_1 = (as) (br) (cw) (di) (ve) (pt) (fh) (kl) (xq) (gn) (zu) (ym) (oj)$
 $\pi_2 = (ay) (bj) (ct) (dk) (ei) (fn) (gx) (hl) (mp) (ow) (qr) (su) (vz)$
 $\pi_3 = (ax) (bl) (vh) (ie) (kr) (tz) (ju) (gd) (fo) (cm) (qs) (np) (yw)$
 $\pi_4 = (as) (rc) (wb) (iv) (ep) (tf) (hk) (lx) (qg) (nz) (uy) (mo) (jd)$
 $\pi_5 = (ac) (yx) (gc) (dk) (jl) (hf) (nq) (rv) (ze) (io) (wu) (sm) (pb)$
 $\pi_6 = (aw) (xb) (lv) (hi) (ek) (rt) (zj) (ug) (df) (oc) (mq) (sn) (py)$

Voor bepalen rotorbedrading nog wat nodig:

- 1 Heel wat algebra gepriegel
- 2 Informatie verkregen vanuit spionage
- 3 Heel veel gepuzzel

De volgende stap (1939/1940)

- Duitsers maken de code ingewikkelder

De volgende stap (1939/1940)

- Duitsers maken de code ingewikkelder
- 30 juni 1939: “Il y a du nouveau”

De volgende stap (1939/1940)

- Duitsers maken de code ingewikkelder
- 30 juni 1939: “Il y a du nouveau”
- Ontmoeting in Pyry, Warschau

De volgende stap (1939/1940)

- Duitsers maken de code ingewikkelder
- 30 juni 1939: “Il y a du nouveau”
- Ontmoeting in Pyry, Warschau
- Alle informatie wordt naar Bletchley Park (GC&CS) gebracht

De volgende stap (1939/1940)

- Duitsers maken de code ingewikkelder
- 30 juni 1939: "Il y a du nouveau"
- Ontmoeting in Pyry, Warschau
- Alle informatie wordt naar Bletchley Park (GC&CS) gebracht



Figuur: Alan Turing (1912-1954)

Rejewski en Turing

Rejewski

Turing

Rejewski en Turing

Rejewski

- Maakte alleen gebruik van de tekst

Turing

Rejewski en Turing

Rejewski

- Maakte alleen gebruik van de tekst
- *Ciphertext-only attack*

Turing

Rejewski en Turing

Rejewski

- Maakte alleen gebruik van de tekst
- *Ciphertext-only attack*
- Procedures Duitsers veranderen

Turing

Rejewski en Turing

Rejewski

- Maakte alleen gebruik van de tekst
- *Ciphertext-only attack*
- Procedures Duitsers veranderen
- Enigma wordt complexer

Turing

Rejewski en Turing

Rejewski

- Maakte alleen gebruik van de tekst
- *Ciphertext-only attack*
- Procedures Duitsers veranderen
- Enigma wordt complexer

Turing

- Gokken een deel van de tekst

Rejewski en Turing

Rejewski

- Maakte alleen gebruik van de tekst
- *Ciphertext-only attack*
- Procedures Duitsers veranderen
- Enigma wordt complexer

Turing

- Gokken een deel van de tekst
- *Known-plaintext attack*

Rejewski en Turing

Rejewski

- Maakte alleen gebruik van de tekst
- *Ciphertext-only attack*
- Procedures Duitsers veranderen
- Enigma wordt complexer

Turing

- Gokken een deel van de tekst
- *Known-plaintext attack*

WETTERVORHERSAGEXBISKAYA

Rejewski en Turing

Rejewski

- Maakte alleen gebruik van de tekst
- *Ciphertext-only attack*
- Procedures Duitsers veranderen
- Enigma wordt complexer

Turing

- Gokken een deel van de tekst
- *Known-plaintext attack*

WETTERVORHERSAGEXBISKAYA
KEINEXBESONDERENXVORKOMMISSE
KEINEXBESONDERENXEREIGNISSE

We denken te weten dat dit bericht het weerbericht voor de Golf van Biskaje bevat.

QFZWRWIVTYRESXBFOGKUHQBAlSEZ

We denken te weten dat dit bericht het weerbericht voor de Golf van Biskaje bevat.

QFZWRWIVTYRESXBFQKUHQBAlSEZ
WETTERVORHERSAGEBISKAYA

We denken te weten dat dit bericht het weerbericht voor de Golf van Biskaje bevat.

QFZWRWIVTYRE**S**XBFOGKUHQBAISEZ
WETTERVORHER**S**AGEBISKAYA

We denken te weten dat dit bericht het weerbericht voor de Golf van Biskaje bevat.

QFZWRWIVTYRESXBFQKUHQBAlSEZ
WETTERVORHERSAGEBISKAYA

We denken te weten dat dit bericht het weerbericht voor de Golf van Biskaje bevat.

QFZWRWIVTYRESXBFOGKUHQBAISEZ
WETTERVORHERSAGEBISKAYA

We denken te weten dat dit bericht het weerbericht voor de Golf van Biskaje bevat.

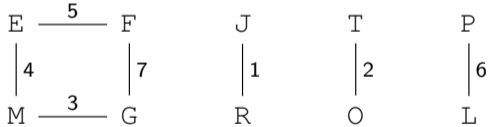
QFZWRWIVTYRESXBFQKUHQBAlSEZ
WETTERVORHERSAGEBISKAYA

Menus

1234567
JTGEFPG
ROMMELF

Menus

1234567
JTGEFPG
ROMMELF

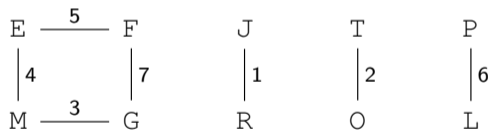


Figuur: Voorbeeld van een menu

Menus

1234567
JTGEFPG
ROMMELF

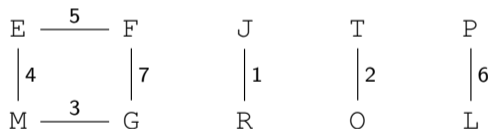
$$\pi_3(M) = G \text{ en } \pi_3(G) = M$$



Figuur: Voorbeeld van een menu

Menus

1234567
JTGEFPG
ROMMELF



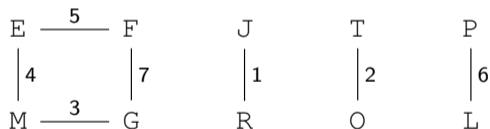
Figuur: Voorbeeld van een menu

$$\pi_3(M) = G \text{ en } \pi_3(G) = M$$

We testen de hypothese:
G is verbonden met A op het stekkerbord

Menus

1234567
JTGEFPG
ROMMELF



Figuur: Voorbeeld van een menu

$$\pi_3(M) = G \text{ en } \pi_3(G) = M$$

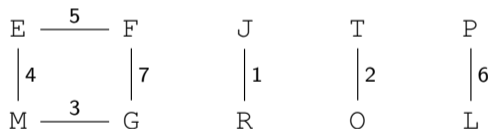
We testen de hypothese:

G is verbonden met A op het stekkerbord



Menus

1234567
JTGEFPG
ROMMELF



Figuur: Voorbeeld van een menu

$$\pi_3(M) = G \text{ en } \pi_3(G) = M$$

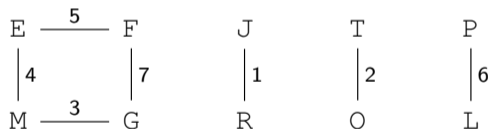
We testen de hypothese:

G is verbonden met A op het stekkerbord



Menus

1234567
JTGEFPG
ROMMELF



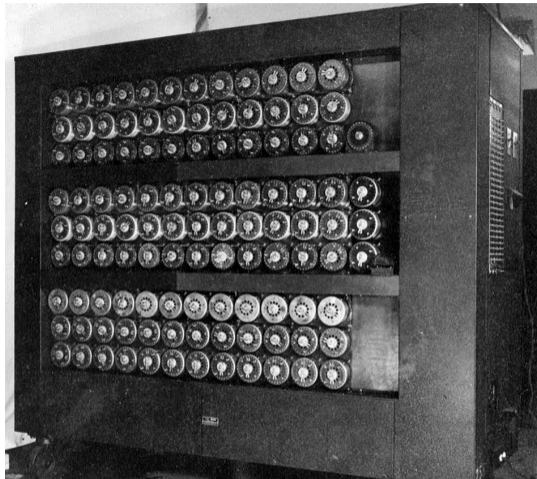
Figuur: Voorbeeld van een menu

$$\pi_3(M) = G \text{ en } \pi_3(G) = M$$

We testen de hypothese:

G is verbonden met A op het stekkerbord





Figuur: De Turing-Welchman Bombe



Invloed cykels op Bombestop

Bombestops

Laat $c < 4$ het aantal cykels in een menu. Het aantal Bombestops wordt dan gegeven door

$$26^{4-c} \times \text{H-M factor}$$

Invloed cykels op Bombestop

Bombestops

Laat $c < 4$ het aantal cykels in een menu. Het aantal Bombestops wordt dan gegeven door

$$26^{4-c} \times \text{H-M factor}$$

Aantal letters	H-M	Aantal letters	H-M
2	0.92	10	0.016
3	0.79	11	0.0060
4	0.62	12	0.0018
5	0.44	13	0.00045
6	0.29	14	0.000095
7	0.17	15	0.000016
8	0.087	16	0.0000023
9	0.041		

Foute Bombestops

	Aantal letters in menu										
Cykels	6	7	8	9	10	11	12	13	14	15	16
3	7.54	4.42	2.26	1.07	0.42	0.16	0.05	0.01	0	0	0
2	196.04	114.92	58.81	27.72	10.82	4.06	1.22	0.3	0.06	0.01	0
1	5097.04	2987.92	1529.11	720.62	281.22	105.46	31.64	7.91	1.67	0.28	0.04
0	132523	77685.9	39756.9	18736	7311.62	2741.86	822.56	205.64	43.41	7.31	1.05

Foute Bombestops

Cykels	Aantal letters in menu										
	6	7	8	9	10	11	12	13	14	15	16
3	7.54	4.42	2.26	1.07	0.42	0.16	0.05	0.01	0	0	0
2	196.04	114.92	58.81	27.72	10.82	4.06	1.22	0.3	0.06	0.01	0
1	5097.04	2987.92	1529.11	720.62	281.22	105.46	31.64	7.91	1.67	0.28	0.04
0	132523	77685.9	39756.9	18736	7311.62	2741.86	822.56	205.64	43.41	7.31	1.05

- Slechts één stop geeft de juiste sleutel

Foute Bombestops

Cykels	Aantal letters in menu										
	6	7	8	9	10	11	12	13	14	15	16
3	7.54	4.42	2.26	1.07	0.42	0.16	0.05	0.01	0	0	0
2	196.04	114.92	58.81	27.72	10.82	4.06	1.22	0.3	0.06	0.01	0
1	5097.04	2987.92	1529.11	720.62	281.22	105.46	31.64	7.91	1.67	0.28	0.04
0	132523	77685.9	39756.9	18736	7311.62	2741.86	822.56	205.64	43.41	7.31	1.05

- Slechts één stop geeft de juiste sleutel
- Bombe niet genoeg: Banburismus, Rodding, Checking Machine

Bletchley Park

Bletchley Park

- *The biggest bloody lunatic asylum in Britain*

Bletchley Park

- *The biggest bloody lunatic asylum in Britain*
- *The geese who laid golden eggs and never cackled*

Bletchley Park

- *The biggest bloody lunatic asylum in Britain*
- *The geese who laid golden eggs and never cackled*
- *ACTION THIS DAY: Make sure they have all they want on extreme priority and report to me that this has been done*

Bletchley Park

- *The biggest bloody lunatic asylum in Britain*
- *The geese who laid golden eggs and never cackled*
- *ACTION THIS DAY: Make sure they have all they want on extreme priority and report to me that this has been done*



Figuur: Dilly Knox (1884 – 1943)

Bletchley Park

- *The biggest bloody lunatic asylum in Britain*
- *The geese who laid golden eggs and never cackled*
- *ACTION THIS DAY: Make sure they have all they want on extreme priority and report to me that this has been done*
- Zimmerman Telegram (1917)



Figuur: Dilly Knox (1884 – 1943)

Bletchley Park

- *The biggest bloody lunatic asylum in Britain*
- *The geese who laid golden eggs and never cackled*
- *ACTION THIS DAY: Make sure they have all they want on extreme priority and report to me that this has been done*
- Zimmerman Telegram (1917)
- Dilly's Fillies



Figuur: Dilly Knox (1884 – 1943)

Bletchley Park

Bletchley Park



Figuur: Mavis Batey (1921 - 2013)

Bletchley Park

- *Oh, hello, we're breaking machines, have you got a pencil?*
- Italian Marine Enigma (1941)



Figuur: Mavis Batey (1921 - 2013)

Bletchley Park

- *Oh, hello, we're breaking machines, have you got a pencil?*
- Italian Marine Enigma (1941)
- *Today's the day minus three*



Figuur: Mavis Batey (1921 - 2013)

Bletchley Park

- *Oh, hello, we're breaking machines, have you got a pencil?*
- Italian Marine Enigma (1941)
- *Today's the day minus three*
- De Slag bij Kaap Matapan



Figuur: Mavis Batey (1921 - 2013)

Bletchley Park

- *Oh, hello, we're breaking machines, have you got a pencil?*
- Italian Marine Enigma (1941)
- *Today's the day minus three*
- De Slag bij Kaap Matapan
- Abwehr Enigma



Figuur: Mavis Batey (1921 - 2013)

Bletchley Park

- *Oh, hello, we're breaking machines, have you got a pencil?*
- Italian Marine Enigma (1941)
- *Today's the day minus three*
- De Slag bij Kaap Matapan
- Abwehr Enigma
- Operation XX



Figuur: Mavis Batey (1921 - 2013)

Bletchley Park

- *Oh, hello, we're breaking machines, have you got a pencil?*
- Italian Marine Enigma (1941)
- *Today's the day minus three*
- De Slag bij Kaap Matapan
- Abwehr Enigma
- Operation XX
- Operation Fortitude



Figuur: Mavis Batey (1921 - 2013)

Impact van Ultra

Impact van Ultra

- Op hoogtepunt 84.000 berichten per maand ontcijferen (10.000 mensen)

Impact van Ultra

- Op hoogtepunt 84.000 berichten per maand ontcijferen (10.000 mensen)
- Oorlog verkort met twee jaar, miljoenen levens gered

Impact van Ultra

- Op hoogtepunt 84.000 berichten per maand ontcijferen (10.000 mensen)
- Oorlog verkort met twee jaar, miljoenen levens gered
- *Very few Armies ever went to battle better informed of their enemy*

Impact van Ultra

- Op hoogtepunt 84.000 berichten per maand ontcijferen (10.000 mensen)
- Oorlog verkort met twee jaar, miljoenen levens gered
- *Very few Armies ever went to battle better informed of their enemy*
- *Battle of the Atlantic*

Impact van Ultra

- Op hoogtepunt 84.000 berichten per maand ontcijferen (10.000 mensen)
- Oorlog verkort met twee jaar, miljoenen levens gered
- *Very few Armies ever went to battle better informed of their enemy*
- *Battle of the Atlantic*

Impact van Ultra

- Op hoogtepunt 84.000 berichten per maand ontcijferen (10.000 mensen)
- Oorlog verkort met twee jaar, miljoenen levens gered
- *Very few Armies ever went to battle better informed of their enemy*
- *Battle of the Atlantic*
- Openbaar sinds 2009

Meer weten?



Meer weten?

- The Code Book, Simon Singh

Meer weten?

- The Code Book, Simon Singh
- Alan Turing: The Enigma, Andrew Hodges

Meer weten?

- The Code Book, Simon Singh
- Alan Turing: The Enigma, Andrew Hodges
- The Hut Six Story, Gordon Welchman
- Cryptology, Classical and Modern, Klima & Sigmon

Meer weten?

- The Code Book, Simon Singh
- Alan Turing: The Enigma, Andrew Hodges
- The Hut Six Story, Gordon Welchman
- Cryptology, Classical and Modern, Klima & Sigmon
- Cryptomuseum: cryptomuseum.com

Meer weten?

- The Code Book, Simon Singh
- Alan Turing: The Enigma, Andrew Hodges
- The Hut Six Story, Gordon Welchman
- Cryptology, Classical and Modern, Klima & Sigmon
- Cryptomuseum: cryptomuseum.com
- The Queen of Codes, Jackie Uí Chionna

Meer weten?

- The Code Book, Simon Singh
- Alan Turing: The Enigma, Andrew Hodges
- The Hut Six Story, Gordon Welchman
- Cryptology, Classical and Modern, Klima & Sigmon
- Cryptomuseum: cryptomuseum.com
- The Queen of Codes, Jackie Uí Chionna
- The Rose Code, Kate Quinn

Meer weten?

- The Code Book, Simon Singh
- Alan Turing: The Enigma, Andrew Hodges
- The Hut Six Story, Gordon Welchman
- Cryptology, Classical and Modern, Klima & Sigmon
- Cryptomuseum: cryptomuseum.com
- The Queen of Codes, Jackie Uí Chionna
- The Rose Code, Kate Quinn
- The Imitation Game (2014)

Bedankt voor de aandacht!