Enigma
podle učebního textu doc. RNDr. Jiřího Tůmy, DrSc.

L'ubomíra Balková

Úvod do kryptologie

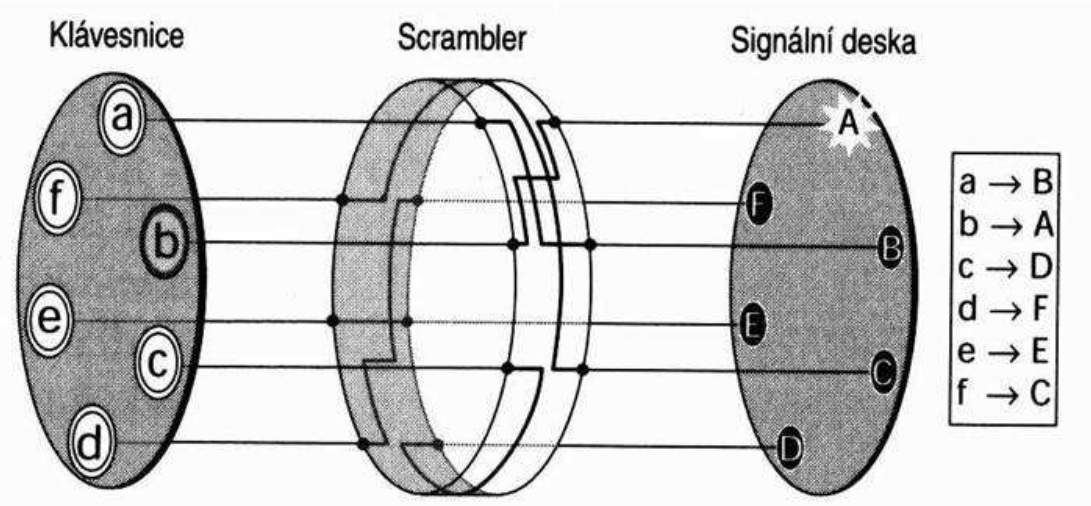
28. února 2011

Program

Program

Základní součásti

- *klávesnice*, *scrambler* = *rotor* (tlustý gumový kotouč protkaný dráty), *signální deska*

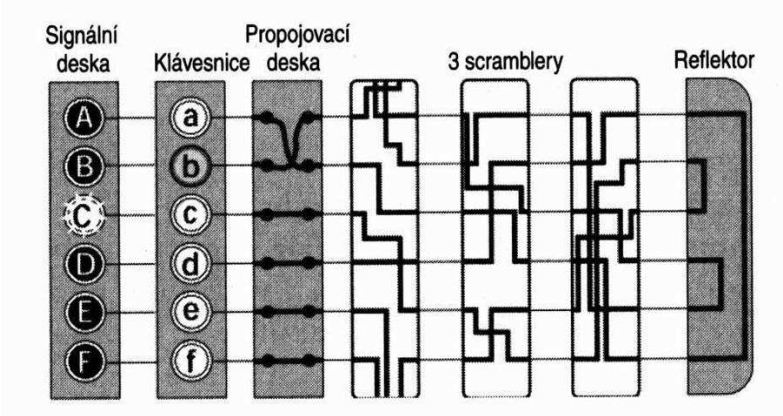


Obrázek: Zjednodušená verze Enigmy, jen 6-písmenná abeceda a 1 scrambler. Napíšeme-li na klávesnici b, prochází scramblerem el. proud, sleduje vnitřní vedení a na výstupu rozsvítí žárovku A.

Rotory

- kdyby se rotor neotáčel $\Rightarrow$ monoalfabetická substituce
- kdyby Enigma obsahovala 1 v každém kroku se otáčející rotor $\Rightarrow$ polyalfabetická substituce s periodickým klíčem (perioda délky 26)
- Enigma obsahuje *3 rotory*
  - 1. rotor se otáčí o 1 dílek v každém kroku
  - 2. rotor se otočí, až když 1. rotor vykoná celou otočku (26 dílků)
  - 3. rotor se otočí, až když 2. rotor vykoná celou otočku (26 dílků)
- rotory navíc vyměnitelné

Další součásti



Obrázek: Zjednodušený model Enigmy, místo 26 písmen pouze 6.

- *reflektor* - podobný scrambleru, ale neotáčí se $\Rightarrow$ šifrování a dešifrování "zrcadlové operace"
- *propojovací deska* - 6 kabelů, tedy prohození 6 párů písmen $\Rightarrow$ zvyšuje počet klíčů, sama o sobě jen monoalfabetická substituce
- *prstence* - kroužky na rotorech $\Rightarrow$ určují, po kolika otočkách 1. rotoru se otočí 2. a po kolika otočkách 2. rotoru se otočí 3.

Program

- vyměnitelné rotory: $6 \times 26 \times 26 \times 26 = 105\ 456$
- propojovací deska:
  $\frac{1}{6!}\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2} = 100\ 391\ 791\ 500$
- prstence: $26 \times 26 \times 26 = 17\ 576$

Program

- kompaktní skříňka o rozměrech $34 \times 28 \times 15$ cm, 12 kg

Obrázek: Wehrmacht Enigma

- Scherbius vyrábí verze pro obchodníky, vojsko, luxusní diplomatickou pro ministerstvo zahraničí

Program

Hans-Thilo Schmidt (Asche)

- provoz Enigmy zahájen 1926, Britové, Francouzi i Američani se vzdávají snahy o rozluštění, Poláci vytrvalí
- nově založené Biuro Szyfrów disponuje obchodní verzí Enigmy
- Hans-Thilo Schmidt dodává fr. agentu Rexovi návody k použití Enigmy spolu s kódovými knihami $\Rightarrow$ rekonstrukce vojenské Enigmy Poláky
- najati matematici z poznaňské univerzity (hovořili plynně německy), 3 z 20 prokázali talent

Marian Rejewski

- nejlepší Marian Rejewski (23-letý student statistiky) - rekonstrukce Enigmy a po celá 30. léta dešifrování něm. zpráv
- konstrukce bomb - nalezení správného nastavení scramblerů ze 17576 možných během 2 hodin (6 bomb - 1 pro každé ze 6 uspořádání)
- Langer tají před Rejewským existenci Schmidta $\Rightarrow$ příprava na horší chvíle
- prosinec 1938 - Němci přidávají 2 nové scramblery (z 5 výběr 3) $\Rightarrow$ meze Rejewského finančních možností (vzorky nových scramblerů schopen určit, ale k zjišťování nastavení scramblerů potřeba 60 bomb)

Bletchley Park

- leden 1938 - Němci zvyšují počet kabelů propojovací desky na 10
- Schmidt přestává dodávat denní klíče
- červen 1939 - Langer předává repliky Enigmy a detailní plány bomb Britům a Francouzům
- 1. září 1939 - Německo napadá Polsko
- Rejewski po vpádu Němců prchá nejprve do Francie, poté do Británie, kde zařazen do malé zpravodajské jednotky, nikoliv do Bletchley Parku, o existenci GC&CS se dozvídá až při odtajnění info v 70. letech

Program

Denní klíč byl potřeba jeden denně (existovaly měsíční kódové knihy):

- nastavení propojovací desky (Steckerverbindungen): $a/U - c/R - d/K - j/Z - l/N - p/S$
- uspořádání scramblerů (Walzenlage): 231 (zpočátku se měnilo jednou za 3 měsíce)
- orientace scramblerů (Grundstellung): *ufw* (písmena, která jsou vidět v okénkách)
- poloha abecedních kroužků na rotorech (Ringstellung): *kub*

Program

Denním klíčem se šifruje jen *klíč zprávy* - stejné zapojení propojovací desky i uspořádání scramblerů, odlišná orientace scramblerů:

1. odesílatel nastaví Enigmu podle denního klíče
2. **2krát** zašifruje náhodnou 3-písmennou sekvenci (např. *htshts* na *NEVGWY*)
3. nastaví Enigmu na orientaci *hts* a v té zašifruje otevřený text

Stejným denním klíčem se šifruje málo textu - jen klíče zpráv

$$ahoj \rightarrow NEVGW\ \ YMMVH$$

Program

Identifikace šifry

- odposlechnuté zprávy stejné frekvence písmen jako náhodný text
- ale! IC dvojic zpráv shodujících se v prvních 6 znacích a zachycených ve stejný den

NEVGW YCJUM IYFCW JXMDR TBIFU PQDMH RPCOX WYXTJ YQXZG CQMSP
NEVGW YIPUC AVKHH FTAPT ZVYXV KRJIG APWAT LWBQH UJASR JMBSF

shodný s IC běžného něm. textu $\Rightarrow$ zprávy zašifrované stejnou polyalfabetickou substitucí

- objem zpráv $\Rightarrow$ jde o šifrátor
- prosinec 1932 - k dispozici: obchodní Enigma (bez propojovací desky a jiné rotory), operační manuál, denní klíče na září a říjen 1932 (potvrzeno, že první 6-tice písmen je klíč zprávy)

Slabiny Enigmy

1. reflektor $\Rightarrow$ žádné písmeno nešifrováno samo na sebe
2. reflektor $\Rightarrow$ substituce v každém kroku dána permutací o cyklech délky 2
3. při libovolné volbě polohy kroužku pouze 6 z 26 možných orientací 1. scrambleru způsobilo, že se při šifrování klíče zprávy pohnul i 2. a případně 3. rotor

Charakteristiky dne

- při stejném denním klíči všechny klíče zpráv šifrovány stejnými 6 permutacemi A, B, C, D, E, F
- stejné písmeno otevřeného textu x bylo permutací A zobrazeno jako y, tj. $Ax = y$, a permutací D jako z, tj. $Dx = z$
- A, D permutace s cykly délky 2 $\Rightarrow A = A^{-1}$ a $D = D^{-1}$, a tedy $DAy = z$
- podobně pro 2. a 5. a 3. a 6. písmeno klíče zprávy
- během dne se dají získat ze zašifrovaných klíčů zpráv permutace DA, EB, FC a jejich cykly
- Rejewski jim říká *charakteristiky dne*

Příklad: charakteristiky dne

1.	AUQ AMN	17.	KHB XJV	33.	RJL WPX	49.	VII PZK
2.	BNH CHL	18.	KHB XJV	34.	RFC WQQ	50.	VII PZK
3.	BCT CGJ	19.	LDR HDE	35.	SYX SCW	51.	VQZ PVR
4.	CIK BZT	20.	LDR HDE	36.	SYX SCW	52.	VQZ PVR
5.	DDB VDV	21.	MAW UXP	37.	SYX SCW	53.	WTM RAO
6.	EJP IPS	22.	MAW UXP	38.	SYX SCW	54.	WTM RAO
7.	GPB ZSV	23.	NXD QTU	39.	SYX SCW	55.	WTM RAO
8.	GPB ZSV	24.	NXD QTU	40.	SJM SPO	56.	WKI RKK
9.	HNO THD	25.	NLU QFZ	41.	SJM SPO	57.	XRS GNM
10.	HNO THD	26.	OBU DLZ	42.	SJM SPO	58.	XRS GNM
11.	HXV TTI	27.	PVJ FEG	43.	SUG SMF	59.	XOI GUK
12.	IKG JKF	28.	QGA LYB	44.	SUG SMF	60.	XYW GCP
13.	IKG JKF	29.	QGA LYB	45.	TMN EBY	61.	YPC OSQ
14.	IND JHU	30.	RJL WPX	46.	TMN EBY	62.	ZZY YRA
15.	JWF MIC	31.	RJL WPX	47.	TAA EXB	63.	ZEF YOC
16.	JWF MIC	32.	RJL WPX	48.	USE NWH	64.	ZSJ YWG

$$DA = (a)(s)(bc)(rw)(dvpfkxgzyo)(eijmunqlht)$$

$$EB = (d)(k)(axt)(cgy)(blfqveoum)(hjpswizrn)$$

$$FC = (abviktjgfcqny)(duzrehlxwpsmo)$$

získání A, B, C, D, E, F ze znalosti DA, EB, FC

1. skvělý Rejewského nápad - teo permutací

Věta

Pokud dvě permutace na stejné množině obsahují pouze cykly délky 2, pak jejich složení obsahuje vždy sudý počet cyklů jakékoliv délky.

Pozn.

Prvky stejného cyklu délky 2 se ve složené permutaci objevují ve dvou různých cyklech stejné délky.

získání A, B, C, D, E, F ze znalosti DA, EB, FC

Věta

Pokud nějaká permutace obsahuje sudý počet cyklů libovolné délky, pak ji lze psát jako složení 2 permutací obsahujících pouze cykly délky 2.

Pozn.

Pokud se 2 prvky objevují v součinu permutací XY ve dvou cyklech stejné délky a zároveň tvoří cyklus délky 2 v jedné z permutací, pak i jejich sousední prvky tvoří cykly v dané permutaci.

Příklad

Nechť $XY = (\dots a_{k-1} a_k a_{k+1} \dots)(\dots b_{l-1} b_l b_{l+1} \dots) \dots$
a $Y = (a_k b_l) \dots$, *pak* $Y = (a_{k-1} b_{l+1})(a_k b_l)(a_{k+1} b_{l-1}) \dots$.

získání A, B, C, D, E, F ze znalosti DA, EB, FC

$$DA = (a)(s)(bc)(rw)(dvpfkxgzyo)(eijmunqlht)$$

$$EB = (d)(k)(axt)(cgy)(blfqveoum)(hjpswizrn)$$

$$FC = (abviktjgfcqny)(duzrehlxwpsmo)$$

Z předchozích tvrzení plyne:

- DA lze rozložit na součin permutací obsahujících pouze cykly délky 2 celkem $2 \cdot 10$ způsoby
- EB $3 \cdot 9$ způsoby
- FC 13 způsoby

získání A, B, C, D, E, F ze znalosti DA, EB, FC

2. skvělý Rejewského nápad - předpoklad stereotypních klíčů

1.	AUQ AMN	17.	KHB XJV	33.	RJL WPX	49.	VII PZK
2.	BNH CHL	18.	KHB XJV	34.	RFC WQQ	50.	VII PZK
3.	BCT CGJ	19.	LDR HDE	35.	SYX SCW	51.	VQZ PVR
4.	CIK BZT	20.	LDR HDE	36.	SYX SCW	52.	VQZ PVR
5.	DDB VDV	21.	MAW UXP	37.	SYX SCW	53.	WTM RAO
6.	EJP IPS	22.	MAW UXP	38.	SYX SCW	54.	WTM RAO
7.	GPB ZSV	23.	NXD QTU	39.	SYX SCW	55.	WTM RAO
8.	GPB ZSV	24.	NXD QTU	40.	SJM SPO	56.	WKI RKK
9.	HNO THD	25.	NLU QFZ	41.	SJM SPO	57.	XRS GNM
10.	HNO THD	26.	OBU DLZ	42.	SJM SPO	58.	XRS GNM
11.	HXV TTI	27.	PVJ FEG	43.	SUG SMF	59.	XOI GUK
12.	IKG JKF	28.	QGA LYB	44.	SUG SMF	60.	XYW GCP
13.	IKG JKF	29.	QGA LYB	45.	TMN EBY	61.	YPC OSQ
14.	IND JHU	30.	RJL WPX	46.	TMN EBY	62.	ZZY YRA
15.	JWF MIC	31.	RJL WPX	47.	TAA EXB	63.	ZEF YOC
16.	JWF MIC	32.	RJL WPX	48.	USE NWH	64.	ZSJ YWG

získání A, B, C, D, E, F ze znalosti DA, EB, FC

- mezi přijatými zprávami často stejné klíče (SYX SCW 5×)
- co kdyby $aaaaaa \rightarrow SYXSCW$?
  1. $A = (as)\ldots$, $D = (as)\ldots$
  2. $B = (ay)\ldots$, $E = (ac)\ldots$, ze znalosti EB a z předchozích vět plyne $B = (ay)(xg)(tc)\ldots$ a $E = EB \circ B = (ac)(xy)(tg)$
  3. $C = (ax)\ldots$, $F = (aw)\ldots$, ze znalosti FC a z předchozích vět plyne

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

$$F = FC \circ C = (aw)(bx)(co)(df)(ek)(gu)(hi)(jz)(lv)(mq)(ns)(py)(rt)$$

získání A, B, C, D, E, F ze znalosti DA, EB, FC

předpoklad stereotypních klíčů

1.	AUQ AMN	17.	KHB XJV	33.	RJL WPX	49.	VII PZK
2.	BNH CHL	18.	KHB XJV	34.	RFC WQQ	50.	VII PZK
3.	BCT CGJ	19.	LDR HDE	35.	SYX SCW	51.	VQZ PVR
4.	CIK BZT	20.	LDR HDE	36.	SYX SCW	52.	VQZ PVR
5.	DDB VDV	21.	MAW UXP	37.	SYX SCW	53.	WTM RAO
6.	EJP IPS	22.	MAW UXP	38.	SYX SCW	54.	WTM RAO
7.	GPB ZSV	23.	NXD QTU	39.	SYX SCW	55.	WTM RAO
8.	GPB ZSV	24.	NXD QTU	40.	SJM SPO	56.	WKI RKK
9.	HNO THD	25.	NLU QFZ	41.	SJM SPO	57.	XRS GNM
10.	HNO THD	26.	OBU DLZ	42.	SJM SPO	58.	XRS GNM
11.	HXV TTI	27.	PVJ FEG	43.	SUG SMF	59.	XOI GUK
12.	IKG JKF	28.	QGA LYB	44.	SUG SMF	60.	XYW GCP
13.	IKG JKF	29.	QGA LYB	45.	TMN EBY	61.	YPC OSQ
14.	IND JHU	30.	RJL WPX	46.	TMN EBY	62.	ZZY YRA
15.	JWF MIC	31.	RJL WPX	47.	TAA EXB	63.	ZEF YOC
16.	JWF MIC	32.	RJL WPX	48.	USE NWH	64.	ZSJ YWG

- nyní klíč AUQ AMN
- už víme $s?ss?s \longrightarrow AUQAMN$
- co kdyby $ssssss \longrightarrow AUQAMN$?
- pak (su) je cyklus v B, proto

$$B = (dk)(ay)(xg)(tc)(us)(mp)(bj)(lh)(fn)(qr)(vz)(ei)(ow)$$

$$E = (ac)(bp)(dk)(ez)(fn)(gt)(hq)(io)(jl)(ms)(rv)(uw)(xy)$$

získání A, B, C, D, E, F ze znalosti DA, EB, FC

1.	AUQ AMN	17.	KHB XJV	33.	RJL WPX	49.	VII PZK
2.	BNH CHL	18.	KHB XJV	34.	RFC WQQ	50.	VII PZK
3.	BCT CGJ	19.	LDR HDE	35.	SYX SCW	51.	VQZ PVR
4.	CIK BZT	20.	LDR HDE	36.	SYX SCW	52.	VQZ PVR
5.	DDB VDV	21.	MAW UXP	37.	SYX SCW	53.	WTM RAO
6.	EJP IPS	22.	MAW UXP	38.	SYX SCW	54.	WTM RAO
7.	GPB ZSV	23.	NXD QTU	39.	SYX SCW	55.	WTM RAO
8.	GPB ZSV	24.	NXD QTU	40.	SJM SPO	56.	WKI RKK
9.	HNO THD	25.	NLU QFZ	41.	SJM SPO	57.	XRS GNM
10.	HNO THD	26.	OBU DLZ	42.	SJM SPO	58.	XRS GNM
11.	HXV TTI	27.	PVJ FEG	43.	SUG SMF	59.	XOI GUK
12.	IKG JKF	28.	QGA LYB	44.	SUG SMF	60.	XYW GCP
13.	IKG JKF	29.	QGA LYB	45.	TMN EBY	61.	YPC OSQ
14.	IND JHU	30.	RJL WPX	46.	TMN EBY	62.	ZZY YRA
15.	JWF MIC	31.	RJL WPX	47.	TAA EXB	63.	ZEF YOC
16.	JWF MIC	32.	RJL WPX	48.	USE NWH	64.	ZSJ YWG

- poté klíč RJL WPX
- už víme $?bb?bb \longrightarrow RJLWPX$
- co kdyby $bbbbbb \longrightarrow RJLWPX$?
- pak (br) je cyklus v A
- nakonec klíč LDR HDE
- už víme $?kk?kk \longrightarrow LDRHDE$
- co kdyby $kkkkkk \longrightarrow LDRHDE$?
- pak (kl) je cyklus v A
- z předchozích vět a znalosti DA dostaneme

$$A = (as)(br)(cw)(kl)(xq)(ng)(uz)(my)(jo)(di)(ev)(pt)(fh)$$

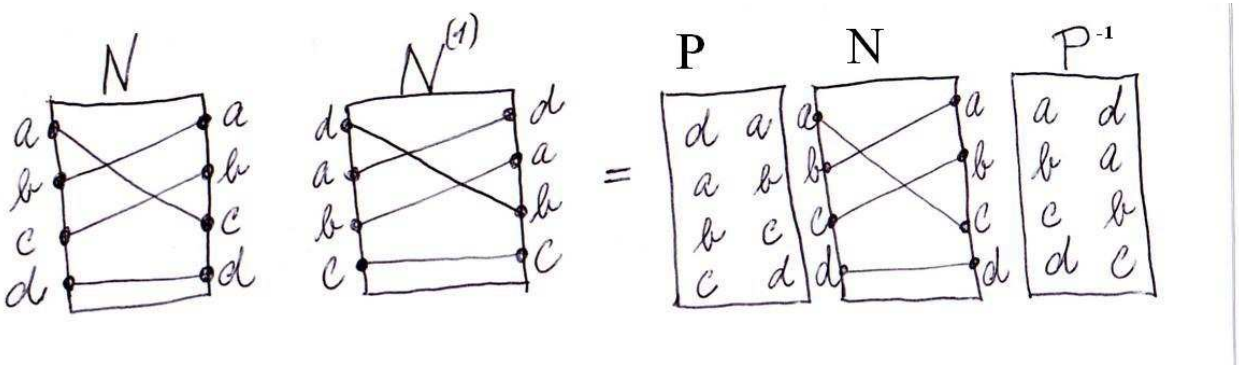
$$D = (as)(bw)(cr)(dj)(ep)(ft)(gq)(hk)(iv)(lx)(mo)(nz)(uy)$$

- pomocí získaných permutací dešifrujeme klíče zpráv
- šokující zjištění: jen 2 náhodné klíče abc, uvw, ve zbylých 38 případech ze 40 se opakuje stejné písmeno nebo jsou volena sousední písmena z klávesnice!
- 1933 zákaz používat sousední a stejná písmena, už pozdě

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

Q	W	E	R	T	Z	U	I	O
A	S	D	F	G	H	J	K	
P	Y	X	C	V	B	N	M	L

- co se znalostí A, B, C, D, E, F?
- předpokládejme, že se v prvních 6 krocích otáčí jen 1. rotor (to je pravda průměrně ve 20 z 26 případů)
- označme permutace
  1. rotorů L, M, N (N je první rotor)
  2. reflektoru R (platí $R = R^{-1}$ kvůli vnitřnímu zapojení, které má 13 cyklů délky 2)
  3. propojovací desky S (platí $S = S^{-1}$, protože obsahuje pouze 6 nebo 10 cyklů délky 2 - pro písmena spojená kabely - a zbylé cykly jsou délky 1)
  4. zapojení mezi propojovací deskou a vstupním rotorem V
  5. označme $P = (abcdefghijklmnopqrstuvwxyz)$ cyklickou permutaci, pak po první otáčce se z permutace rotoru N stane $N^{(1)} = P^{-1}NP$



- platí tedy:

$$A = S^{-1}V^{-1}P^{-1}N^{-1}PM^{-1}L^{-1}RLMP^{-1}NPVS$$

$$B = S^{-1}V^{-1}P^{-2}N^{-1}P^{2}M^{-1}L^{-1}RLMP^{-2}NP^{2}VS$$

$$C = S^{-1}V^{-1}P^{-3}N^{-1}P^{3}M^{-1}L^{-1}RLMP^{-3}NP^{3}VS$$

$$D = S^{-1}V^{-1}P^{-4}N^{-1}P^{4}M^{-1}L^{-1}RLMP^{-4}NP^{4}VS$$

$$E = S^{-1}V^{-1}P^{-5}N^{-1}P^{5}M^{-1}L^{-1}RLMP^{-5}NP^{5}VS$$

$$F = S^{-1}V^{-1}P^{-6}N^{-1}P^{6}M^{-1}L^{-1}RLMP^{-6}NP^{6}VS$$

to je 6 rovnic pro neznámé permutace N, M, L, S, V

- nastavení propojovací desky S znají Poláci z kódových knih pro září a říjen 1932
- spojení V mezi vstupním rotorem a propojovací deskou Rejewski uhádl (německému smyslu pro pořádek odpovídá identická permutace)

- označme $Q = M^{-1}L^{-1}RLM$, Rejewskému zbyla soustava pro neznámé permutace N, Q, z které ho zajímalo $N =$ zapojení 1. rotoru:

$$T := PSAS^{-1}P^{-1} = N^{-1}PQP^{-1}N$$

$$U := P^2SBS^{-1}P^{-2} = N^{-1}P^2QP^{-2}N$$

$$W := P^3SCS^{-1}P^{-3} = N^{-1}P^3QP^{-3}N$$

$$X := P^4SDS^{-1}P^{-4} = N^{-1}P^4QP^{-4}N$$

$$Y := P^5SES^{-1}P^{-5} = N^{-1}P^5QP^{-5}N$$

$$Z := P^6SFS^{-1}P^{-6} = N^{-1}P^6QP^{-6}N$$

- ze soustavy získal rovnice:

$$TU = N^{-1}P(QPQP^{-1})P^{-1}N$$

$$UW = N^{-1}P^2(QPQP^{-1})P^{-2}N$$

$$WX = N^{-1}P^3(QPQP^{-1})P^{-3}N$$

$$XY = N^{-1}P^4(QPQP^{-1})P^{-4}N$$

$$YZ = N^{-1}P^5(QPQP^{-1})P^{-5}N$$

- z těch vyloučil výraz $QPQP^{-1}$ a zůstalo při označení $H = N^{-1}PN$:

$$UW = H(TU)H^{-1}$$

$$WX = H(UW)H^{-1}$$

$$XY = H(WX)H^{-1}$$

$$YZ = H(XY)H^{-1}$$

- všechny tyto rovnice stejného typu (známá rovnice z teorie permutací): $J = HKH^{-1}$, takovým permutacím J, K říkáme *konjugované*

Věta (která vyhrála druhou světovou válku)

Dvě permutace na téže množině jsou konjugované, právě když mají stejnou cyklickou strukturu, tj. stejný počet cyklů téže délky.

- každá z rovnic poslední soustavy zvlášť má řešení, protože všechny permutace TU, UW, WX, XY, YZ konjugované s $QPQP^{-1}$
- hledané společné řešení H navíc konjugované s cyklickou permutací P, a má tedy jediný cyklus délky 26
- to už řešit umíme
- pokud řešení neexistuje, znamená to, že se při šifrování prvních 6 znaků klíče zprávy pootočil i prostřední rotor M
- takto Rejewski našel vnitřní zapojení rotoru N a poté i M a L, protože i ty se objevovaly na prvních místech, na závěr i reflektoru R

- pomocí repliky Enigmy Rejewski prozkoušel všech $105456 = 6 \times 26^3$ nastavení scramblerů
- strávil rok sestavením katalogu, který obsahoval cyklické typy pro permutace DA, EB, FC v jednotlivých nastaveních scramblerů, pro náš příklad by to bylo $(1, 2, 10), (1, 3, 9), (13)$
- s katalogem byl schopen zjišťovat nastavení scramblerů bez znalosti zapojení propojovací desky

- ze zašifrovaných klíčů zpráv určil permutace DA, EB, FC (silně využívá opakování klíče zprávy), permutace A, B, C, D, E, F znát nepotřeboval
- tyto permutace prostřednictvím propojení S konjugované s permutacemi danými nastavením scramblerů
- nahlédl do svého katalogu a vyhledal trojici cyklických typů: dána jednoznačně - katalog jako otisky prstů!
- se správným nastavením scramblerů snadno dešifroval monoalfabetickou substituci odpovídající permutaci S propojovací desky (snadno odhalitelná: "plijedtedobelrina")

Program

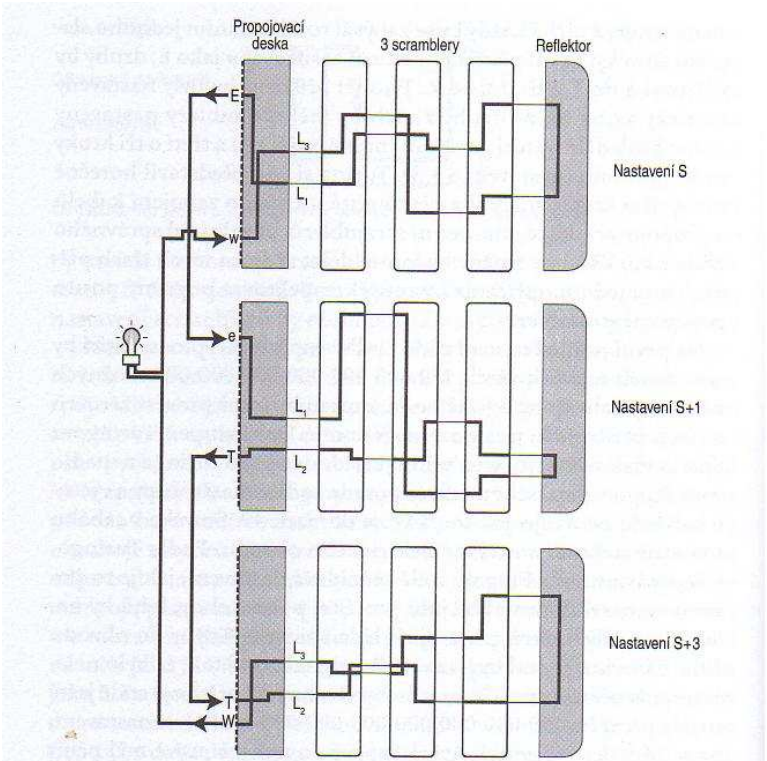
Luštění Enigmy bez opakujícího se klíče

- *tahák (crib)* = slovo otevř. textu, které se určitě vyskytuje v šifr. textu
- užití taháků k určení nastavení scramblerů (hledá v nich smyčky, bez znalosti zapojení propojovací desky):

nastavení scramblerů	S	S+1	S+2	S+3	S+4	S+5
odhadovaný otevřený text	w	e	t	t	e	r
šifrový text	E	T	J	W	P	X

shrnutí:

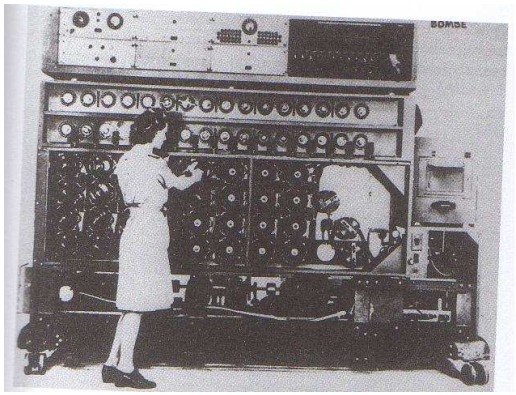
  - v nastavení S Enigma zašifruje w jako E
  - v nastavení S+1 Enigma zašifruje e jako T
  - v nastavení S+3 Enigma zašifruje t jako W



Obrázek 49: Smyčka v taháku může být analogická elektrické smyčce. Tři přístroje Enigmy jsou nastaveny identicky až na to, že druhý přístroj má scramblery nastaveny o jeden krok dopředu oproti prvnímu přístroji (nastavení S + 1) a třetí nastavení je posunuto o tři kroky oproti prvnímu (nastavení S + 3). Výstup z každé Enigmy je poté napojen na vstup další Enigmy. Tři sady scramblerů se pak otáčejí společně až do okamžiku, kdy je obvod uzavřen a světlo se rozsvítí. V tu chvíli se dosáhne hledaného nastavení. V diagramu nahoře je obvod uzavřen, takže odpovídá správnému nastavení.

- 12 sad po 3 scramblerech (použití dlouhých smyček)
- písmena L_1, L_2, L_3 neznámá
- po nalezení správného nastavení určení zapojení propojovací desky

Využití slabin



m		w	e	t	t	e	r	n	u	l	l	s	e	c	h	s	
c	R	E	N	L	W	K	M	J	J	S	X	C	P	L	E	J	W

- Enigma nešifruje stejné písmeno na stejné! $\Rightarrow$ správné umístění taháku
- cilky = stereotypní klíče (z ang. cillis nebo sillies, protože jeden z něm. radistů často používal jako klíč zprávy CIL, zřejmě iniciály manželky)
- v kódové knize při přechodu na nový denní klíč nezůstává žádný scrambler ve stejné poloze
- na propojovací desce žádný kabel nespojuje sousední písmena