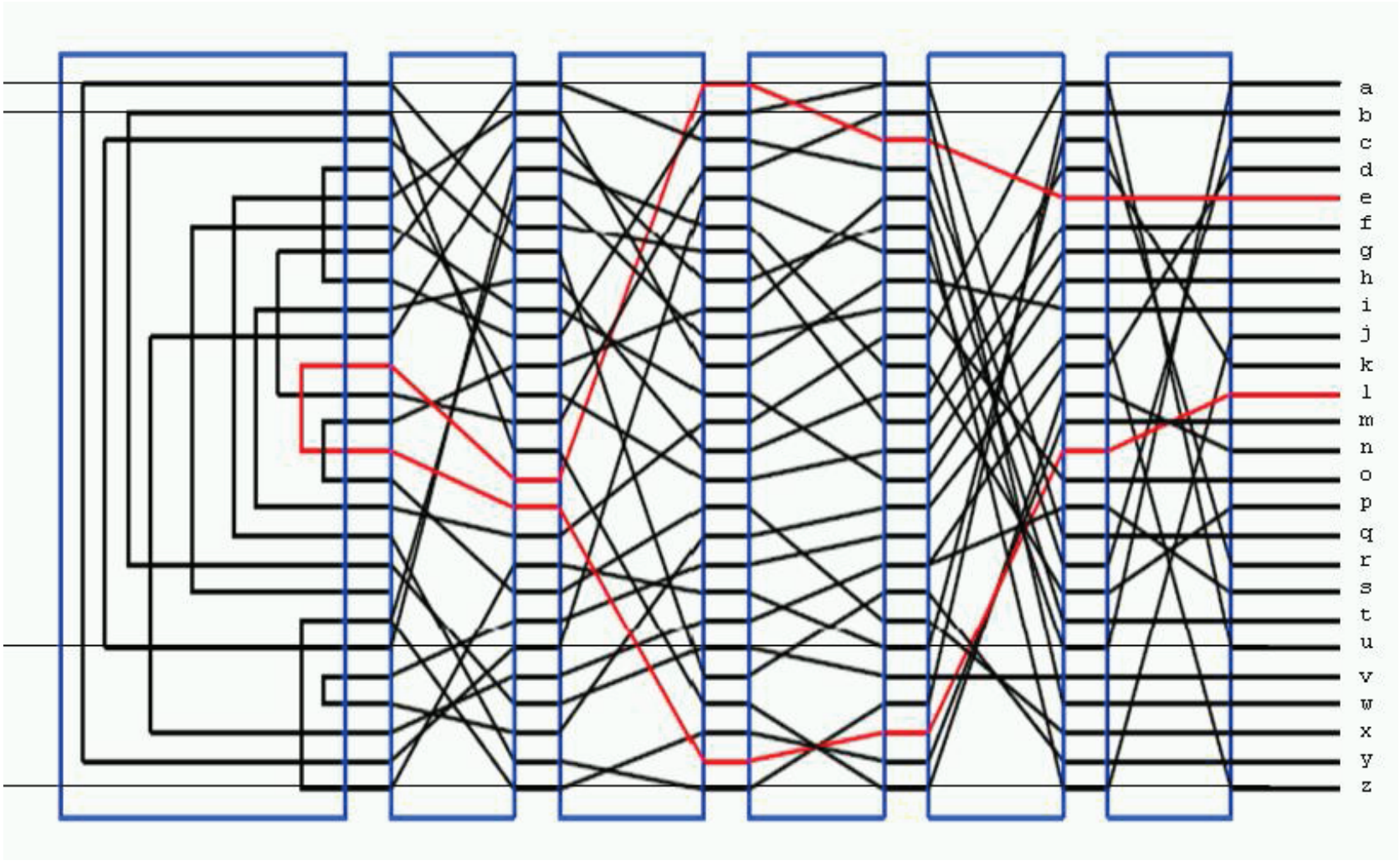
Kapitola 3

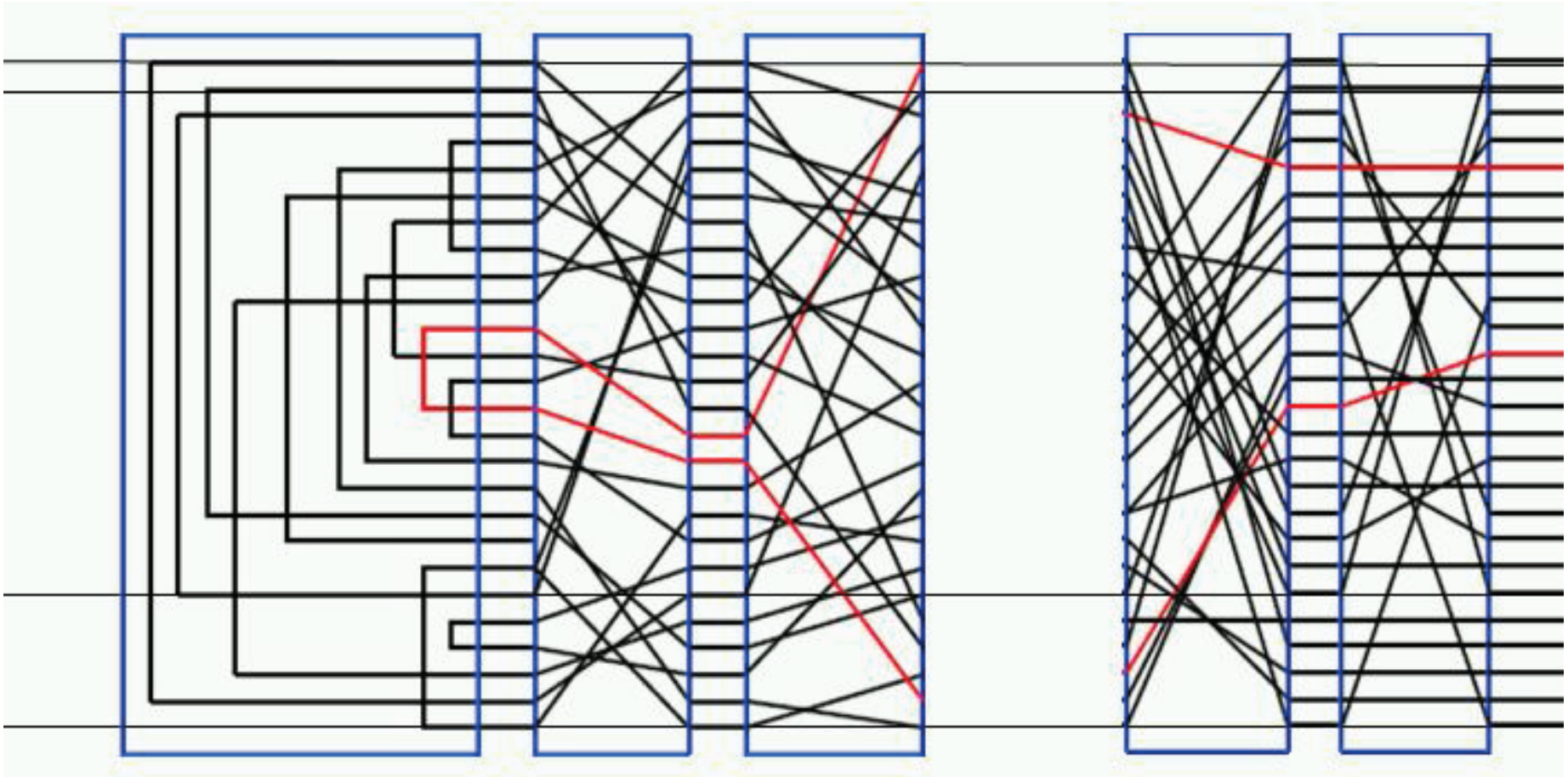
Výpočet rotorů v Enigmě – 2. část

Matematické modely Enigmy - obsah

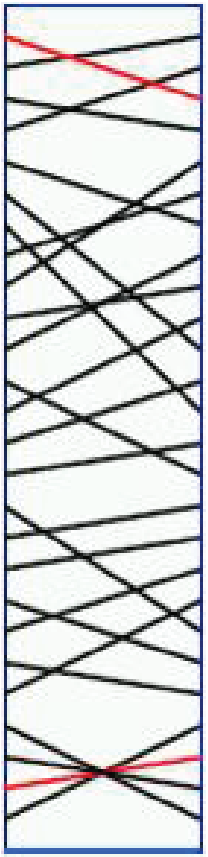
Statický model Enigmy



Dynamický model Enigmy



Volný rotor



Prvních šest písmen zprávy

je zašifrováno postupně permutacemi

Charakteristiky dne

- všechny permutace A, B, C, D, E, F mají 13 cyklů délky 2
- proto $A^2 = B^2 = \cdots = F^2 = I$, I je identita
- to znamená $A^{-1} = A$, $B^{-1} = B$, $\ldots$, $F^{-1} = F$
- prvních šest písmen otevřeného textu je `xyzxyz`
- odposlechneme `rstuvw`
- čemu se rovná DA`(r)=`
- `podobně` BE`(s)=,` CF`(t)=`

Manévry

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

Charakteristiky dne

během manévrů byly

Proč to tak vyšlo

Co způsobilo šifrování klíče zprávy

Nastupuje psychologie

původní soustavu

$$
\begin{aligned}
A &= S^{-1}H^{-1}P^{-1}N^{-1}PQP^{-1}NPHS \\
B &= S^{-1}H^{-1}P^{-2}N^{-1}P^{2}QP^{-2}NP^{2}HS \\
C &= S^{-1}H^{-1}P^{-3}N^{-1}P^{3}QP^{-3}NP^{3}HS \\
D &= S^{-1}H^{-1}P^{-4}N^{-1}P^{4}QP^{-4}NP^{4}HS \\
E &= S^{-1}H^{-1}P^{-5}N^{-1}P^{5}QP^{-5}NP^{5}HS \\
E &= S^{-1}H^{-1}P^{-6}N^{-1}P^{6}QP^{-6}NP^{6}HS
\end{aligned}
$$

by Rejewski uměl vyřešit, pokud by znal permutace A, B, C, D, E, F

a ty mu sdělili šifranti svojí leností

Stereotypní volby klíčů zpráv

co kdyby během manévrů zvolil nějaký šifrant klíč zprávy aaa ?

vzhledem k charakteristice
DA =(a),(s),(bc),(rw),(dvpfkxgzyo),(eijmunqlht)

musí být A(a)=

jsou tedy tři možnosti pro šifrovou podobu klíče zprávy aaa

35. SYX SCW 40. SJM SPO 43. SUG SMF

musí být ale také kompatibilní s charakteristikami

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

FC=(abviktjgfcqny),(duzrehlxwpsmo)

zbývá jediná možnost 35. SYX SCW

Vyšlo mu

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

Výpočet propojení v rotorech - obsah

Zpátky k původní soustavě

v původní soustavě

$$A = S^{-1}H^{-1}P^{-1}N^{-1}PQP^{-1}NPHS$$
$$B = S^{-1}H^{-1}P^{-2}N^{-1}P^{2}QP^{-2}NP^{2}HS$$
$$C = S^{-1}H^{-1}P^{-3}N^{-1}P^{3}QP^{-3}NP^{3}HS$$
$$D = S^{-1}H^{-1}P^{-4}N^{-1}P^{4}QP^{-4}NP^{4}HS$$
$$E = S^{-1}H^{-1}P^{-5}N^{-1}P^{5}QP^{-5}NP^{5}HS$$
$$E = S^{-1}H^{-1}P^{-6}N^{-1}P^{6}QP^{-6}NP^{6}HS$$

teď už permutace A, B, C, D, E, F znal

S znal od špiona

H zkusil stejné, jako na komrčním přístroji

První pokus

soustavu upravil na

Okamžik pravdy

Kde hledat chybu ?

nová volba H

To fungovalo !

permutace UV, VW, WX, XY, YZ měly stejný cyklický typ

vyšlo několik deítek možností pro permutaci $N^{-1}PN$

Jediné řešení

z dalších rovnic dostal jiné možnosti řešení

nakonec vyšla jediná možnost pro $N^{-1}PN$, která měla jeden cyklus délky 26

a z toho vyšlo pouhých 26 možností pro N

Konec jednoho příběhu, začátek druhého

- z dat z druhého měsíce vypočítal jiný rotor
- jak vypočetl třetí, se nikde nezmiňuje
- z různých pořadí rotorů v různých měsících zjistil, které N je to pravé
- pak už se snadno zjistily i zářezy na abecedních kroužcích
- v lednu 1933 vyrobili repliku Enigmy
- pak 7 let vymýšleli a zdokonalovali metody odhalování denních klíčů
- v červenci 1939 vše předali Britům a Francouzům
- v Polsku všechno zničili a uprchli přes Rumunsko do Francie