KRY02 - MNG

Model 2019

Kryptografie

Část 2 Rotorové stroje

Post 19/20

Souhrnné materiály

Ver 0.1

KRY

Kryptografie

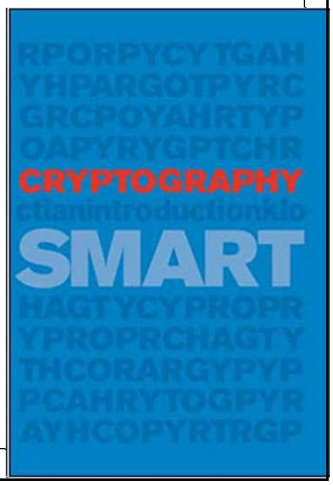
Upd 2007/8
Pre, Post 2014/15
Post 2015/16
2020 MNGprep

KRY 2

Rotorové stroje

Učebnice

- Nigel Smart: Cryptography - An Introduction, 3rd Edition,
  - Mcgraw-Hill College, 3rd Edition, 2013
  - ISBN-10: 0077099877
- Kapitoly
  - Kapitola 4
    - » Zajímavá je pro nás celá kapitola 4



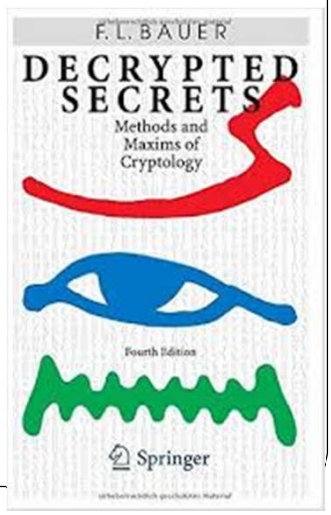
The third edition is now online. You may make copies and distribute the copies of the book as you see fit, as long as it is clearly marked as having been authored by N.P. Smart.

Učebnice je v dokumentovém skladu

Doporučená četba

2

- **Decrypted Secrets**
- **[Bauer] Friedrich L. Bauer: Decrypted Secrets - Methods and Maxims of Cryptology, ISBN-10 3-540-24502-2 Springer Berlin Heidelberg New York**



©Petr Hanáček

Posouvané a rotované abecedy

- **Založené na jednoduché substituci**
  - **Horizontálně posouvaná abeceda**
  - **Vertikálně posouvaná abeceda**
    - » **Vertikálně pokračovaná ve standardním pořadí**
  - **Rotovaná abeceda**
    - » **Diagonálně pokračovaná ve standardním pořadí**

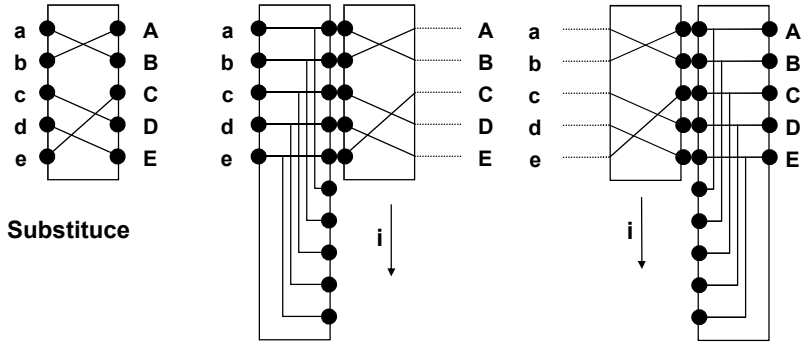
```
i  abcdefghijklmnopqrstuvwxyz

0  NEWYORKCITABDFGHJLMPQSUVXZ
1  EWYORKCITABDFGHJLMPQSUVXZN
2  WYORKCITABDFGHJLMPQSUVXZNE
```

```
i  abcdefghijklmnopqrstuvwxyz

0  NEWYORKCITABDFGHJLMPQSUVXZ
1  OFXZPSLDJUBCEGHIKMNQRTUWYA
2  PGYAQTMEKVCDFHIJLNORSUVXZB
```

```
i  abcdefghijklmnopqrstuvwxyz

0  NEWYORKCITABDFGHJLMPQSUVXZ
1  AOFXZPSIDJUBCEGHIKMNQRTVWY
2  ZBPGYAQTJEKVCDFHIJLNORSUWZ
```

©Petr Hanáček CLACRYPT Slide 4

Stroje pro posouvané abecedy



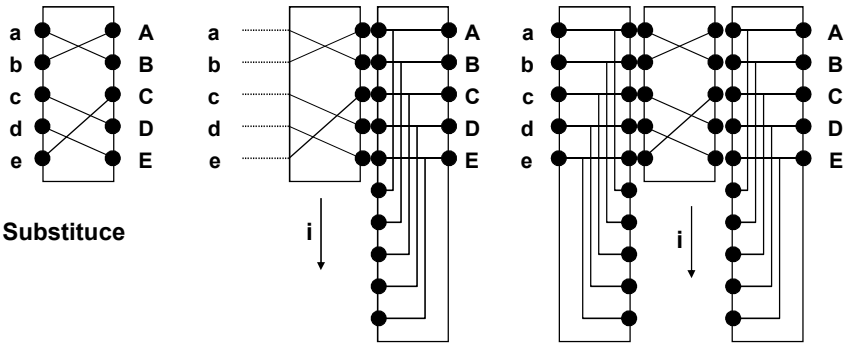
Substituce

Horizontální posuv

Vertikální posuv
(pokračování)

©Petr Hanáček CLACRYPT Slide 5

Stroje pro posouvané abecedy



Substituce

Vertikální posuv

Rotace

©Petr Hanáček CLACRYPT Slide 6

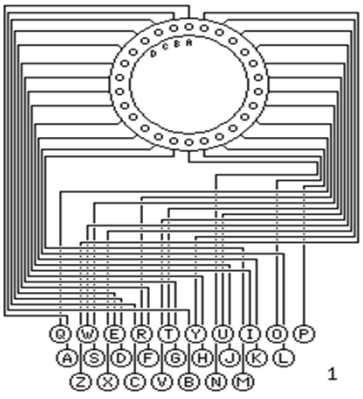
Rotorové stroje

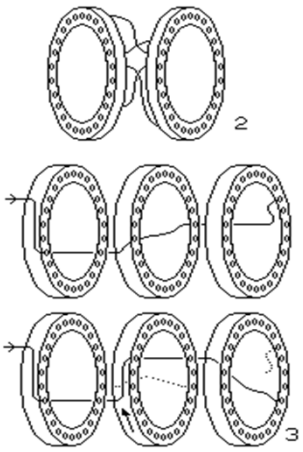
- Implementují polyalfabetické substituční šifry s dlouhou periodou pomocí sady rotorů
- Každý rotor má 26 kontaktů na obou stranách. Kontakty z přední strany jsou propojeny s kontakty ze zadní strany. Klíč je dán propojením kontaktů a počáteční pozicí rotorů.

©Petr Hanáček CLACRYPT Slide 7

Rotorové stroje

- Otevřený text vstupuje do sady rotorů na jedné straně a vystupuje zašifrovaný na druhé straně.
- Po zašifrování písmene se pootočí jeden nebo více roto





©Petr Hanáček CLACRYPT Slide 8

ENIGMA

©Petr Hanáček CLACRYPT Slide 9

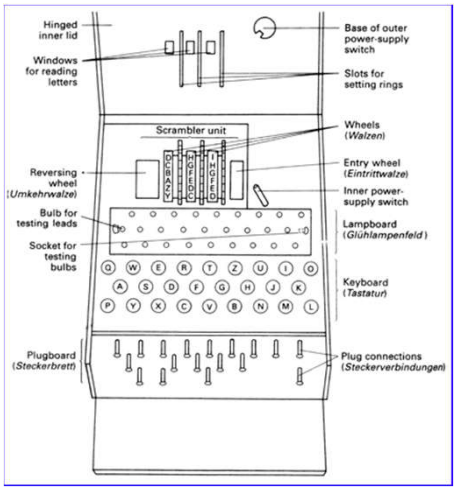
Enigma

- 1920: potřeba mechanického šifrovacího zařízení
- Ideální řešení: rotovaná abeceda
- 1917: Američan Edward Hebern: šifrovací stroj s otočnými disky
- 1918: Německý inženýr Albert Scherbius patentuje rotorový šifrovací stroj, předchůdce Enigmy
- 1923: První typ Enigma A
- Nejdříve nabízena pro civilní účely, později Wehrmacht projevil zájem
- 1926: Wehrmacht kupuje Enigmu
  - Enigma zcela mizí z civilního trhu
- 1930: Wehrmacht si Enigmu upravuje pro své účely
  - Cca. 50000 kusů
  - V průběhu války modifikována, pokládána za zcela bezpečnou
- Informace o úspěšných útocích se začaly veřejně objevovat až v 70 letech
- Detaily prolomení Enigmy v letech 1940-45 byly deklasifikovány až roce 1996

©Petr Hanáček CLACRYPT Slide 10

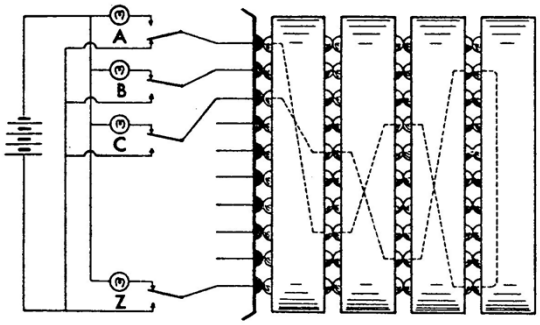
Video 0

Enigma



- Tři rotory (vybrány z pěti možných)
- Po každém znaku se první rotor pootočí
- Po dojetí na zarážku se pootočí další rotor
- Reflektor
- Propojovací deska (Plugboard, Steckerbrett)

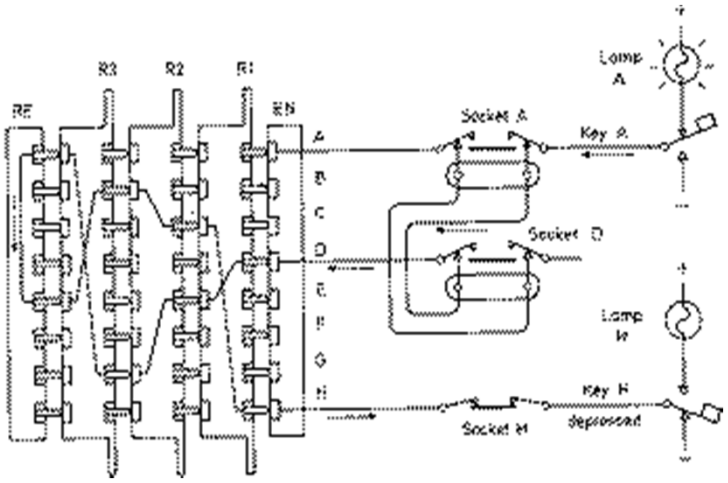
Zjednodušené schéma (bez propojovací desky)



ENIGMA CIRCUIT DIAGRAM. DOTTED LINES SHOW TYPICAL PATH OF CIRCUIT DURING ENCIPHERMENT/DECIPHERMENT.

CLACRYPT Slide 13

S propojovací deskou



CLACRYPT Slide 14

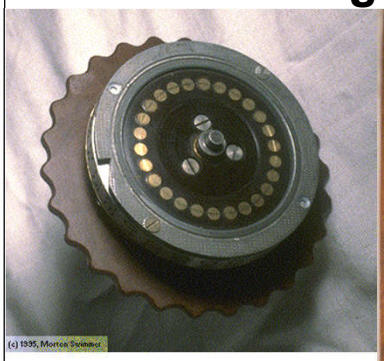
Enigma: Celkový pohled

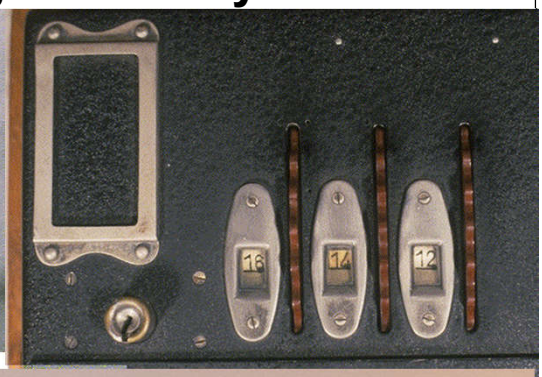
©Petr Hanáček CLACRYPT Slide 15

Enigma: Klávesnice a displej

©Petr Hanáček CLACRYPT Slide 16

Enigma: Rotory

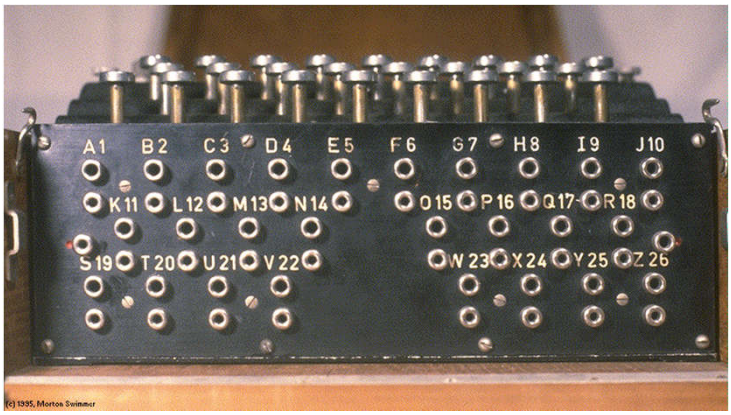




7.3.5 The substitutions performed by the stator, the three rotors, and the reflecting rotor of the ENIGMA D are (Cipher A. Deavours, Louis Kruh):

entry	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
stator	J W U L C M N O H P Q Z Y X I R A D K E G V B T S F
exit rotor 1	L P G S Z M H A E O Q K V X R F Y B U T N I C J D W
exit rotor 2	S L V G B T F X J Q O H E W I R Z Y A M K P C N D U
exit rotor 3	C J G D P S H K T U R A W Z X F M Y N Q O B V L I E
exit reflector	I M E T C G F R A Y S Q B Z X W L H K D V U P O J N

Enigma: Propojovací deska



©Petr Hanáček CLACRYPT Slide 18

KRY

Nastavení (klíč)

- **Rotory**
  - **Walzenlage**
    - » **Před rokem 1939 – Tři rotory (ze tří možných)**
    - » **Později - Tři rotory (z pěti možných)**
  - **Grundstellung**
    - » **Počáteční orientace tří rotorů**
  - **Ringstellung**
    - » **„Posunutí“ počáteční orientace rotorů**
    - » **Nastavení, kdy se pootočí další rotor**

- **Propojovací deska**
  - **Steckerverbindung**
    - » **Výměna páru znaků pomocí kabelu**
    - » **Počet kabelů se měnil (≤ 6 do roku 1939, později až 10)**

VIII. Beiſpiel.

17. Gültiger Tagesſchlüſſel:
(Ausſchnitt aus der für die Verſchlüſſelung des Klartextes in Betracht kommenden Schlüſſeltafel, z. B. »..... Maſchinenſchlüſſel für Monat Mai«)

Datum	Walzenlage	Ringſtellung	Grundſtellung
4.	I III II	16 11 13	01 12 22

Steckerverbindung	Kenngruppen-Einſatzſtelle ..... Gruppe	Kenngruppen
CO DI FR HU JW LS TX	2	adq nuz opw vxz

Nach dieſem Tagesſchlüſſel iſt die Chiffriermaſchine einzuſtellen (vgl. Ziff. 4 und 5).

Der im nachfolgenden Beiſpiel eingeſetzte Schlüſſeltext iſt aus Geheimhaltungsgründen nicht mit der Chiffriermaſchine getaſtet, ſondern willkürlich gewählt worden.

KRY

1944

Geheim! Sonder-Maschinenschlüssel BGS 08 ❊

Nicht ins Flugzeug mitnehmen!

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	I II V	10 14 02	BF SD AY HG OU QC WI RL XP ZK	yqv vuc xxo gvf
30.	V IV I	04 25 01	DI ZL RX UH QK PC VY GA SO EM	mqy vts gvt csx
29.	III V II	13 11 06	ZM BQ TP YX FK AR WH SO NJ DG	aky vdv oyo tzt
28.	I III II	09 16 12	NE MT RL OY HV IU GK FW PZ XC	nfh vco tur wnb
27.	III II I	06 03 15	BF GR SZ OM WQ TY HE JU XN KD	bec jmv vtp xdb
26.	I III V	19 26 08	GS VD CQ LE HI BO JP UZ FT RN	wvu yem buz rjk
25.	II I IV	05 01 16	KA ZH QP GR MF LJ OT EN BD YW	ktv muq cqm cpm
24.	III II IV	22 02 06	PI KM JB YU QS OV ZA GW CH XF	zcd iwo urp glg
23.	IV III II	08 11 07	SX TD QP HU FB YN CO IK WE GZ	epm mgz vqg vsm
22.	I V II	13 02 26	GP XH IW BO NU MD SA ZK QR LT	aam mvy jqq wqm
21.	IV I V	17 24 03	XC AQ OT UZ HD RG KM BL NS JW	ltl blu frk xrh
20.	IV I III	15 22 12	PO TV QC ZS EX WR BJ DK FU LA	non lic oxr usr
19.	V I III	13 24 21	HA GM DI VK JP YU EF TB ZL XQ	ecd ciq uvr ppt
18.	IV V I	23 09 20	XF PZ SQ GR AJ UO CN BV TM KI	fjh zts uqu cft
17.	III II V	21 24 15	UT ZC YN BE PK JX RS GF IA QH	oub eci pyf rqi
16.	IV III V	07 01 13	IN YJ SD UV GF BH TK QE AR OP	kex paw flw onw
15.	I IV II	15 04 25	TM IJ VK OY NX PR WL GA BU SF	sdr pbu byv khb
14.	III II IV	10 23 21	WT RE PC FY JA VD OI HK NX ZS	mhz lff lnq giy
13.	V I II	14 04 12	AN IV LH YP WM TR XU FO ZB ED	rqh ucm ldi ods
12.	II V I	07 19 02	HR NC IU DM TW GV FB ZL EQ OX	asy xza uvc fmr
11.	I V IV	13 15 11	NX EC RV GP SU DK IT FY BL AZ	gyd iuq ocb vef
10.	V II I	09 20 19	FN TA YJ SO EG PC VD KI XH WZ	pyz ace pru uyc
9.	I IV V	14 10 25	VK DW LH RF JS CX PT YB ZG MU	nyh fbd ohs jrp
8.	IV V I	22 04 16	PV XS ZU EQ BW CH AO RL JN TD	tck rts nro mkl
7.	V I IV	18 11 25	TS IK AV QP HW FM DX NG CY UE	mhw lwb mdm ybe
6.	IV I III	02 17 20	KZ FI WY MP DS HR CU XE QV NT	uwu vdk lrh mgd
5.	I V IV	26 09 14	VW LT PB FO ZK GS RI QJ HM XE	suw tsv nfp yjc
4.	IV III V	07 01 12	QS YA XW KR MP HT DU OV CL FZ	uby usi mhh mwb
3.	I II V	05 16 03	FW DL NX BV KM RZ HY IQ EC JU	tns von grw axl
2.	III I II	12 22 17	DW UO PY GR FS EQ KT CL AI ZB	smz lbl bkc sym
1.	I III II	04 18 06	ZN OM CR UI KP WQ SE JV LX TF	ghr vqv cya ayl

Video 1

©Petr Hanáček CLACRYPT Slide 22

Počet možných klíčů

- **Pokud útočník nezná propojení rotorů:**
  $(26!)^3 \approx 4 * 10^{26}$
- **Pokud útočník nezná propojení reflektoru:**
  $(26 * 25 / 2) * (24 * 23 / 2) * \ldots * (2 * 2) / 13!$
  $\approx 8 * 10^{12}$
- **Propojovací deska se šesti kabely:**
  $(26 * 25/2) * \ldots * (16*15 / 2) / 6! \approx 10^{11}$
- **Ringstellung: $26^2 = 676$**
- **Grundstellung: $26^3 = 17576$**
- **Celkem: $\approx 6 * 10^{110}$**
  (ve vesmíru je 10^{84} atomů)

©Petr Hanáček — CLACRYPT Slide 23

Útočník ukořistí jeden stroj

- **Pokud útočník nezná propojení rotorů:**
  $(26!)^3 \approx 4 * 10^{26}$ → Známé rotory: 3! = 6 Nebo 3 z 5 = 5 * 4 *3 = 60
- **Pokud útočník nezná propojení reflektoru:**
  $(26 * 25 / 2) * (24 * 23 / 2) * \ldots * (2 * 2) / 13!$
  $\approx 8 * 10^{12}$ → Známý reflektor: 1
- **Propojovací deska se šesti kabely:**
  $(26 * 25/2) * \ldots * (16*15 / 2) / 6! \approx 10^{11}$
- **Ringstellung: $26^2 = 676$**
- **Grundstellung: $26^3 = 17576$**
- **Celkem: $\approx 10^{16}$**

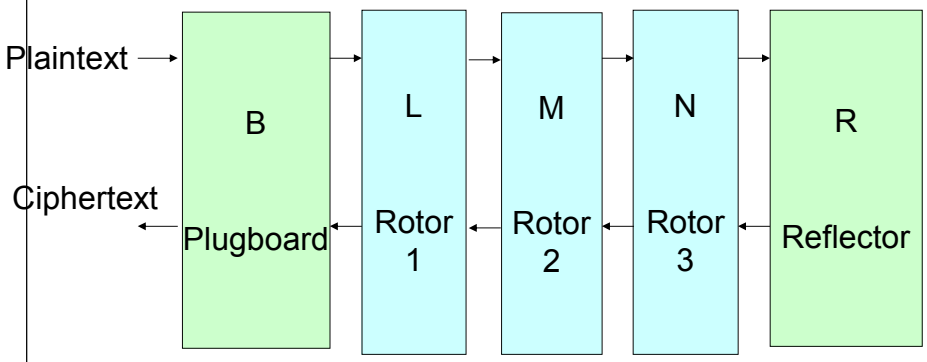
©Petr Hanáček — CLACRYPT Slide 24

Význam propojovací desky

Grundstellung	**26·26·26 = 17 576**
Walzenlagen	**3! = 6** **5*4*3 = 60**
Steckerbrett mit 6 Verbindungskabeln	**100 391 791 500**
	≈ 10 000 000 000 000 000 ≈ 10^{16}

©Petr Hanáček CLACRYPT Slide 25

Zašifrování informace



$$C = B^{-1}L^{-1}M^{-1}N^{-1}RNMLB(P)$$

©Petr Hanáček CLACRYPT Slide 26

Dešifrování tím samým strojem

$C = B^{-1}L^{-1}M^{-1}N^{-1}RNMLB(P)$

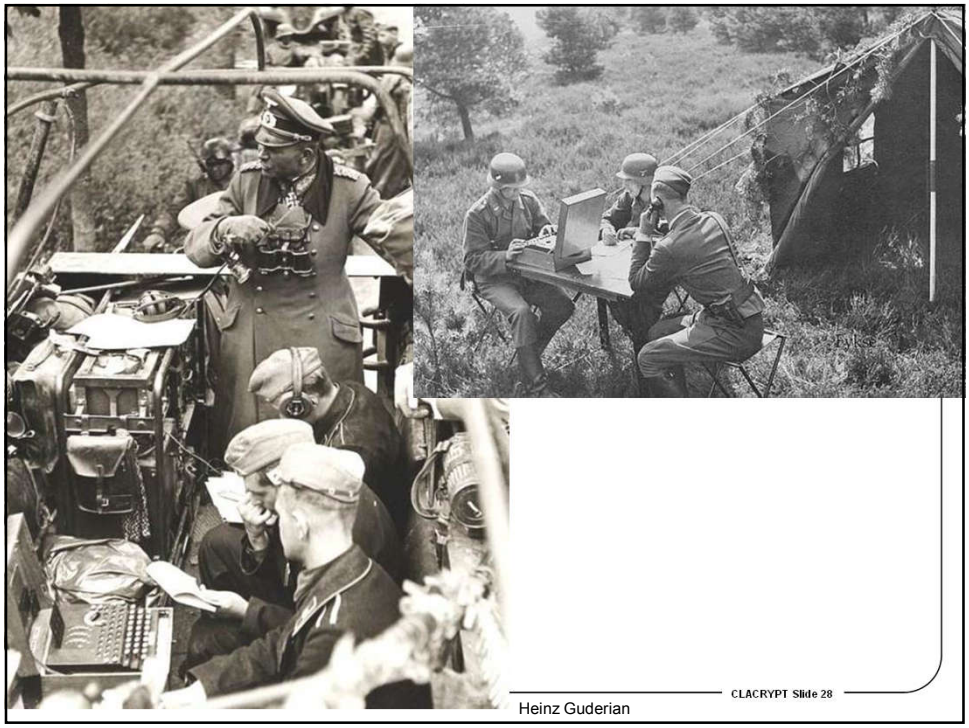
$P = B^{-1}L^{-1}M^{-1}N^{-1}RNMLB(C)$

$= B^{-1}L^{-1}M^{-1}N^{-1}RNMLB(B^{-1}L^{-1}M^{-1}N^{-1}RNMLB(P))$

R je involuce

$(A \rightarrow B \Rightarrow B \rightarrow A)$

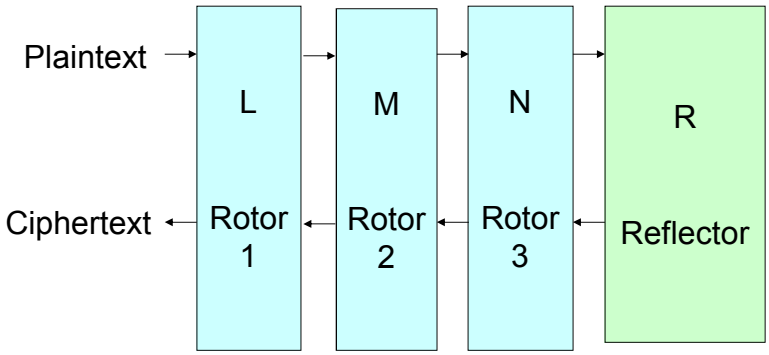
©Petr Hanáček CLACRYPT Slide 27



Heinz Guderian CLACRYPT Slide 28

Kryptoanalýza zjednodušené Enigmy

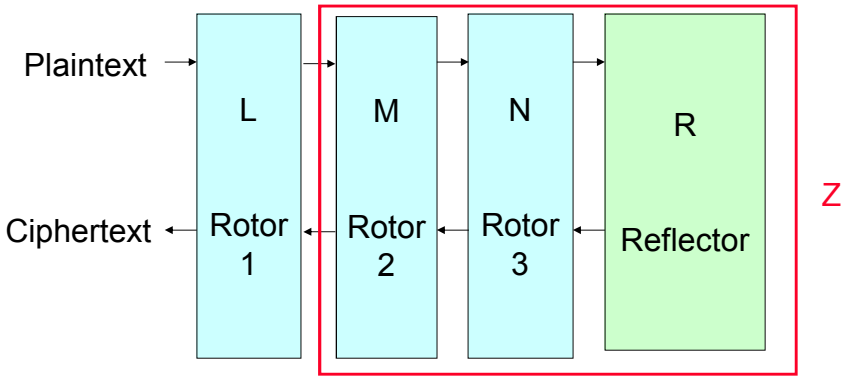
Enigma bez propojovací desky



$$C = L^{-1}M^{-1}N^{-1}RNML(P)$$

Používána v občanské válce ve Španělsku 1938-39 (všemi účastníky)

Enigma bez propojovací desky



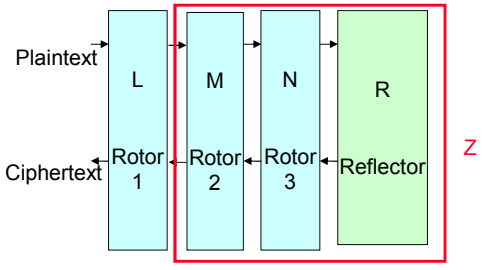
$C = L^{-1}ZL(P)$

$L(C) = ZL(P)$

Pravděpodobné slovo (crib) (4-10 písmen)
Jaká je pravděpodobnost, že se Rotor 2 a Rotor 3 nepohne během 4 písmenného cribu? = 22/26 = .85

©Petr Hanáček CLACRYPT Slide 31

Enigma bez propojovací desky



$C = L^{-1}ZL(P)$

$L(C) = ZL(P)$

Z je pevná (monoalfabetická) substituce, pokud se R2 & R3 nepohne
Uhodnu-li crib, znám C a P_{guess}

$$L(C) = ZL(P_{guess})$$

Vyzkouším možné rotory a počáteční pozice L:
3 rotory * 26 pozic = 78
L_i = efekt rotoru 1 v *I-té* pozici

©Petr Hanáček CLACRYPT Slide 32

Batonův útok

C = XTSWVUINZ
P_{guess} = wehrmacht ("armed forces")

$L_1(X) = Z\ L_1(W)$
$L_2(T) = Z\ L_2(E)$
$L_3(S) = Z\ L_3(H)$
$L_4(W) = Z\ L_4(R)$
$L_5(V) = Z\ L_5(M)$
$L_6(U) = Z\ L_6(A)$
$L_7(I) = Z\ L_7(C)$

L1 tabulka

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EKMFLGDQVZNTOWYHXUSPAIBRCJ
JEKMFLGDQVZNTOWYHXUSPAIBRC
CJEKMFLGDQVZNTOWYHXUSPAIBR
RCJEKMFLGDQVZNTOWYHXUSPAIB
BRCJEKMFLGDQVZNTOWYHXUSPAI
IBRCJEKMFLGDQVZNTOWYHXUSPA
AIBRCJEKMFLGDQVZNTOWYHXUSP
```

Pro dané nastavení rotoru 1 řeš Z

1: R = Z(B) 2: S = Z(F) 3: X = Z(G) 4: P = Z(Y)
5: U = Z(V) 6: H = Z(I) 7: M = Z(B)

Kontradikce - špatné nastavení

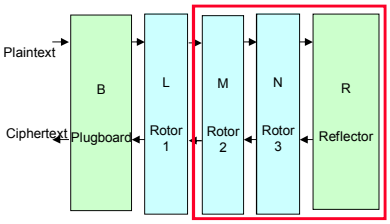
©Petr Hanáček CLACRYPT Slide 33

Batonův útok

- **Víme, že Z je:**
  - **Funkce: kontradikce pokud $Z(x) \neq Z(x)$**
  - **Involuce: kontradikce pokud $Z(x) = y$ & $Z(y) \neq x$**
- **Nalezneme postavení rotou bez kontradikcí**
  - **Prodostatečně dlouhý crib bude pouze jedno**
  - **Pokud crib je příliš dlouhý, projeví se posuv R2**
- **Vytvoříme katalog který mapuje Z na nastavení rotorů R2 a R3**

©Petr Hanáček CLACRYPT Slide 34

Zavedení propojovací desky



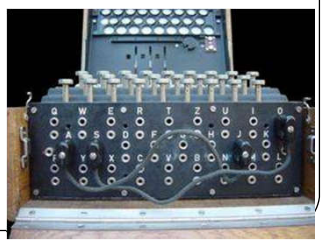
$C = B^{-1}L^{-1}M^{-1}N^{-1}RNMLB(P)$

$C = B^{-1}L^{-1}ZLB(P)$

$BL(C) = ZLB(P)$

6 kabelů: (26*25)/2 * (24*23)/2 * … * (16*15/2) / 6!

= 10^{11} obtížnější



©Petr Hanáček

©Petr Hanáček

Rejewski

Marian Rejewski
1905 – 1980 polský matematik a kryptolog

 CLACRYPT Slide 37

1928 - 1931

- **1928 Polské Biuro Szyfrów zjišťuje, že Wehrmacht začíná používat šifrovací stroje**
- **1929 Biuro Szyfrów organizuje kurs kryptografie pro 20 studentů z Poznaňské univerzity. Tři z nich si pak vybírá.**
- **1929 Biuro Szyfrów kupuje komerční verzi Enigmy**
- **Polské odposlechové stanice:**

Způsob provozu Enigmy

- Denní klíč (distribuovaný pomocí kódové knihy)
- Každá zpráva začíná přenosem klíče zprávy (pouze Grundstellung), ("náhodně" vytvořeným odesílatelem) zašifrovaným denním klíčem
- Klíč zprávy je zaslán dvakrát pro zamezení možné chyby
- Po přijetí klíče zprávy se pootočí rotory do pozice klíče zprávy

 CLACRYPT Slide 39

Přenos opakovaného klíče zprávy

Symetrie Enigmy:

if $E_{pos}(x) = y$ then $E_{pos}(y) = x$

Mějme následující začátky zpráv pro stejný denní klíč:

`DMQ VBM` $E_1(m_1) = D$ $E_4(m_1) = V$

`VON PUY` $E_1(m_2) = V$ $E_4(m_2) = P$

`PUC FMQ`

Pokud během přijmeme dost zpráv, můžeme pro každý ze tří znaků klíče vytvořit úplné cykly:

E_1E_4 = (DVPFKXGZYO) (EIJMUNQLHT) (BC) (RW) (A) (S)

Pozn.: Cykly se vyskytují ve dvojicích stejné délky

 CLACRYPT Slide 40

KRY

1.	AUQ	AMN	14.	IND	JHU	27.	PVJ	FEG	40.	SJM	SPO	53.	WTM	RAO
2.	BNH	CHL	15.	JWF	MIC	28.	QGA	LYB	41.	SJM	SPO	54.	WTM	RAO
3.	BCT	CGJ	16.	JWF	MIC	29.	QGA	LYB	42.	SJM	SPO	55.	WTM	RAO
4.	CIK	BZT	17.	KHB	XJV	30.	RJL	WPX	43.	SUG	SMF	56.	WKI	RKK
5.	DDB	VDV	18.	KHB	XJV	31.	RJL	WPX	44.	SUG	SMF	57.	XRS	GNM
6.	EJP	IPS	19.	LDR	HDE	32.	RJL	WPX	45.	TMN	EBY	58.	XRS	GNM
7.	FBR	KLE	20.	LDR	HDE	33.	RJL	WPX	46.	TMN	EBY	59.	XOI	GUK
8.	GPB	ZSV	21.	MAW	UXP	34.	RFC	WQQ	47.	TAA	EXB	60.	XYW	GCP
9.	HNO	THD	22.	MAW	UXP	35.	SYX	SCW	48.	USE	NWH	61.	YPC	OSQ
10.	HNO	THD	23.	NXD	QTU	36.	SYX	SCW	49.	VII	PZK	62.	YPC	OSQ
11.	HXV	TTI	24.	NXD	QTU	37.	SYX	SCW	50.	VII	PZK	63.	ZZY	YRA
12.	IKG	JKF	25.	NLU	QFZ	38.	SYX	SCW	51.	VQZ	PVR	64.	ZEF	YOC
13.	IKG	JKF	26.	OBU	DLZ	39.	SYX	SCW	52.	VQZ	PVR	65.	ZSJ	YWG

Abb. 148. 65 aufgefangene chiffrierte Spruchschlüssel zum gleichen Tagesschlüssel

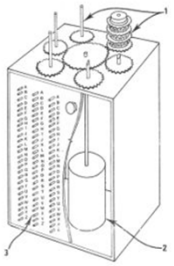
P1P4 **= (a)(s)(bc)(rw)(dvpfkxgzyo)(eijmunqlht)**

P2P5 **= (axt)(blfqveoum)(cgy)(d)(hjpswizrn)(k)**

P3P6 **= (abviktjgfcqny)(duzrehlxwpsmo)**

©Petr Hanáček — CLACRYPT Slide 41

Délky cyklů



- **Délky cyklů jsou nezávislé (invariantní) na nastavení propojovací desky !!!**
- **Vytvoření katalogu**
  - **Délky cyklů -> volba rotorů (Walzenlagen) a pozice rotorů (Grundstellung)**
  - **Jeden rok, 6 * 17 576 items**
- **Odděleně se řeší nastavení propojovací desky**
  - **Intuitivně**
- **Po změně reflektoru mohli Poláci začít znovu**
- **Katalog byl nahrazen mechanickým katalogem**
- **Bomba**

W in	
rtj	WAH WIK
dqx	DWJ MWR
hpl	RAW KTW

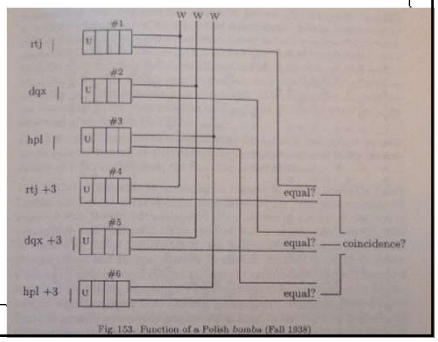


Fig. 153. Function of a Polish *bomba* (Fall 1938)

©Petr Hanáček

Nastavení propojovací desky - Cillies

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

Abb. 150. Die 40 verschiedenen Spruchschlüssel entziffert

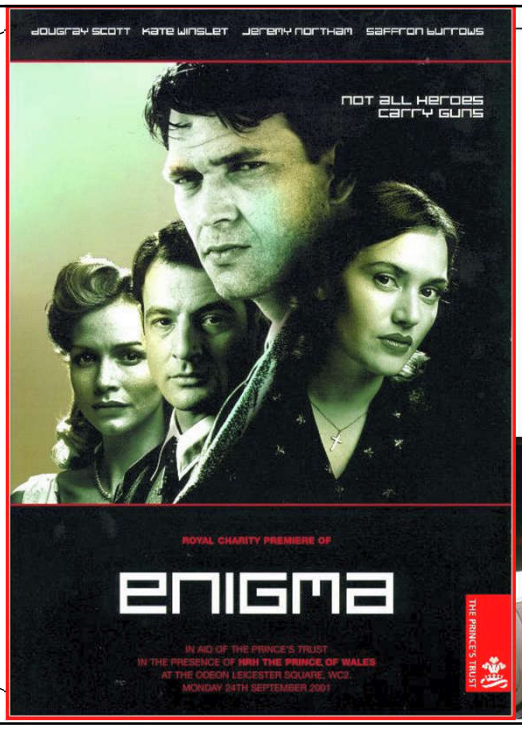
 CLACRYPT Slide 43

1939

- **Na začátku 1939 – Německo mění rotory, přidává další kabely pro propojovací desku, a *přestává používat dvojí přenos klíče zprávy***
- **Poláci již nejsou schopni dešifrovat provoz**
- **25. července 1939 – Rejewski zve zástupce francouzských a britských kryptologů, nabízí jim výsledky své práce**
- **Věnuje Anglii repliku Enigmy**
- **1. září 1939 – Německo zahajuje útok na Polsko**

 CLACRYPT Slide 44

KRY



Breaking Enigma

Bletchley Park

Bletchley Park

- Britská vláda dala dohromady skupinu matematiků v lokalitě Bletchley Park aby se pokusili dešifrovat Enigmu
- Na projektu Bletchley Parku pracovalo 30 000 lidí (pro srovnání na projektu Manhattan 100 000)
- Jedním z vedoucích mozků byl Alan Turing
- Byly používány „cribs“, například zprávy o počasí “WETTER”, přenášené každý den
- Stále byl třeba útok silou pro prozkoumání ~1M klíčů
- Pro automatizaci testů se používaly “bomby”

©Petr Hanáček CLACRYPT Slide 46

Barák 8 (Hut 8) v Bletchley Parku

©Petr Hanáček CLACRYPT Slide 47

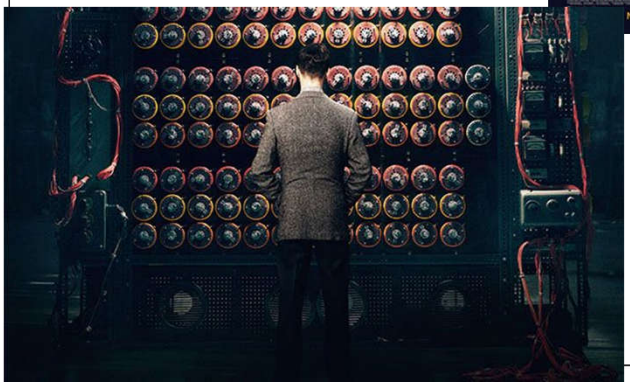
U571 Capture a Machine

"This fictional movie about a fictional U.S. submarine mission is followed by a mention in the end credits of those actual British missions. Oh, the British deciphered the Enigma code, too. Come to think of it, they pretty much did everything in real life that the Americans do in this movie."

Roger Ebert's review of U-571

©Petr Hanáček CLACRYPT Slide 48

The Imitation Game



CLACRYPT Slide 49

Kontrola cribu

- **Non-coincidence**
  - Pro polyalfabetické substituce bez pevného bodu - "žádné písmeno se nemůže zašifrovat samo na sebe"
  - Běžné u monoalfabetických substitucí
  - Všechny polyalfabetické substituce, kde dešifrování se provádí stejně jako šifrování, umožňují tento útok
    - » "complication illusoire" !!
- **Pravděpodobná fráze:**
  - "erloschen is leuchttonne" a Enigma

```
YOAQUTHNCHWSYTIWHTOJQMTCFKUSLZVSMFNGTDUQNYAVH
erloschenistleuchttonne
 erloschenistleuchttonne
  erloschenistleuchttonne
           ....
->       erloschenistleuchttonne
             ....
           ->         erloschenistleuchttonne
```

©Petr Hanáček

CLACRYPT Slide 50

OVRLJ BZMGE RFEWM LKMTA WXTSW VUINZ GYOLY FMKMS GOFTU EIU...
be the cryptotext and /oberkommandoderwehrmacht/ the probable word.
The third leftmost position not excluded by non-coincidence gives the 'crib'

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
o	b	e	r	k	o	m	m	a	n	d	o	d	e	r	w	e	h	r	m	a	c	h	t
O	V	R	L	J	B	Z	M	G	E	R	F	E	W	M	L	K	M	T	A	W	X	T	S	W	V	U	I	N	Z

where the rotor positions are numbered from 1 to 24.

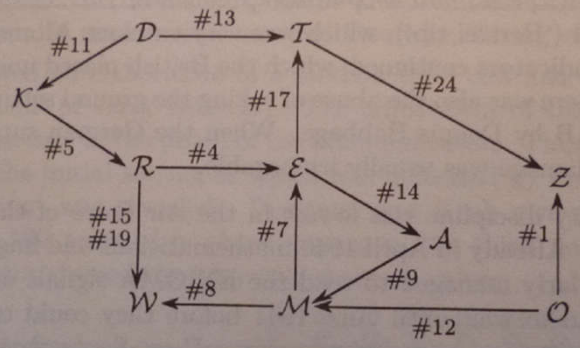
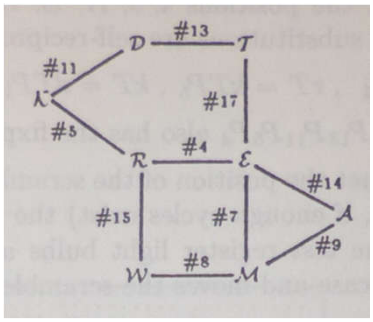
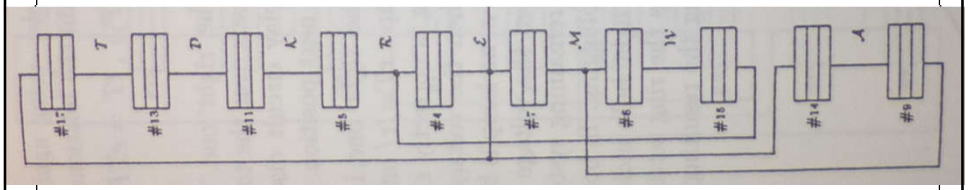


Fig. 156. Plaintext letter / ciphertext letter pairings for crib

o	b	e	r	k	o	m	m	a	n	d	o	d	e	r	w	e	h	r	m	a	c	h	t
Z	M	G	E	R	F	E	W	M	L	K	M	T	A	W	X	T	S	W	V	U	I	N	Z

Zapojení bomby podle menu



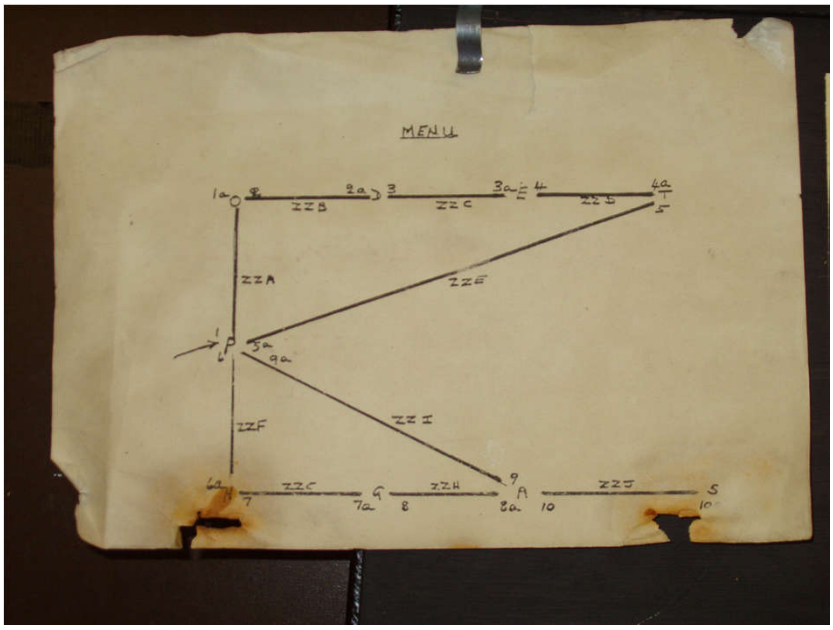


[Bauer]

©Petr Hanáček CLACRYPT Slide 52

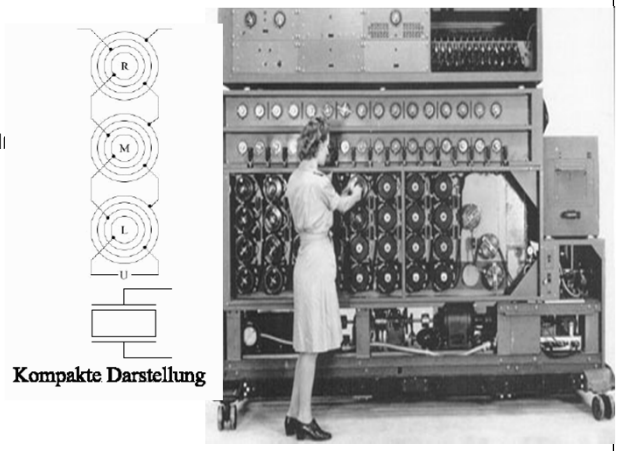
KRY

Video 3



Bomba

- **Turingovo dílo**
- **Rotory**
  - **Stejné propojení jakoEnigma**
  - **Dvojí propojení**
  - **Jedna sada tvoří Scrambler a řeší jed kombinaci rotorů**



©Petr Hanáček CLACRYPT Slide 55

Lidé za Enigmou

Erich Fellgiebel

Erich Fellgiebel byl německý generál, který se zúčastnil Stauffenbergova pokusu o převrat. Wikipedie

Narození: 4. října 1886, Popowice, Lower Silesian Voivodeship, Polsko

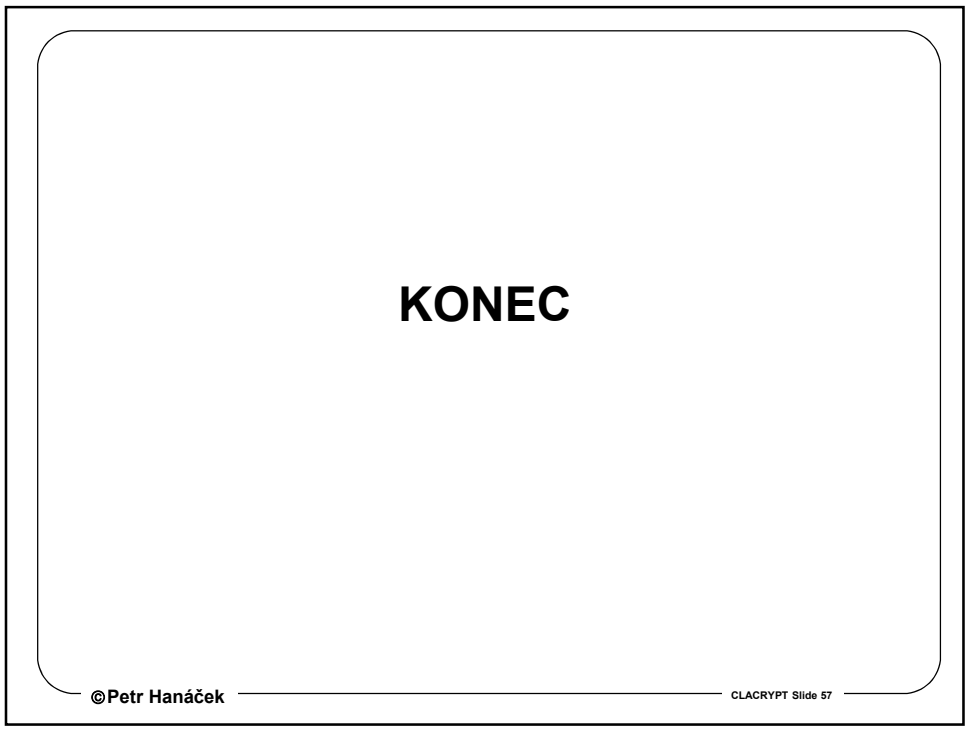
Úmrtí: 4. září 1944, Berlín, Německo

Gisbert F. R. Hasenjaeger

Picture of Gisbert_Hasenjaeger in his identity papers during his time at OKW/Chi

Born	June 1, 1919 Hildesheim
Died	September 2, 2006 (aged 87) Münster, Westphalia
Citizenship	German
Fields	Mathematics Logic
Institutions	Münster University University of Bonn University of Princeton

©Petr Hanáček


KONEC
©Petr Hanáček
CLACRYPT Slide 57

CHAPTER 4

The Enigma Machine

Chapter Goals

- To explain the working of the Enigma machine.
- To explain how the Germans used the Enigma machine, in particular how session keys were transmitted from the sender to the reciever.
- To explain how this enabled Polish and later British cryptanalysts to read the German traffic.
- To explain the use of the Bombe in mounting known plaintext attacks.

1. Introduction

With the advent of the 1920s people saw the need for a mechanical encryption device. Taking a substitution cipher and then rotating it became seen as the ideal solution. This idea had actually been used previously in a number of manual ciphers, but using machines it was seen how this could be done more efficiently. The rotors could be implemented using wires and then encryption could be done mechanically using an electrical circuit. By rotating the rotor we obtain a new substitution cipher.

As an example, suppose the rotor used to produce the substitutions is given by

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
TMKGOYDSIPELUAVCRJWXZNHBQF
```

To encrypt the first letter we use the substitutions given by

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
TMKGOYDSIPELUAVCRJWXZNHBQF
```

However, to encrypt the second letter we rotate the rotor by one position and use the substitutions

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
MKGOYDSIPELUAVCRJWXZNHBQFT
```

To encrypt the third letter we use the substitutions

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
KGOYDSIPELUAVCRJWXZNHBQFTM
```

and so on. This gives us a polyalphabetic substitution cipher with 26 alphabets.

The most famous of these machines was the Enigma machine used by the Germans in World War II. We shall describe the most simple version of Enigma which only used three such rotors, chosen from the following set of five.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EKMFLGDQVZNTOWYHXUSPAIBRCJ
AJDKSIRUXBLHWTMCQGZNPYFVOE
BDFHJLCPRTXVZNYEIWGAKMUSQO
ESOVPZJAYQUIRHXLNFTGKDCMWB
```

VZBRGITYUPSDNHLXAWMJQOFECK

Machines in use towards the end of the war had a larger number of rotors, chosen from a larger set. Note, the order of the rotors in the machine is important, so the number of ways of choosing the rotors is

$$5 \cdot 4 \cdot 3 = 60.$$

Each rotor had an initial starting position, and since there are 26 possible starting positions for each rotor, the total number of possible starting positions is $26^3 = 17\,576$.

The first rotor would step on the second rotor on each full iteration under the control of a ring hitting a notch, likewise the stepping of the third rotor was controlled by the second rotor. Both the rings were movable and their positions again formed part of the key, although only the notch and ring positions for the first two rotors were important. Hence, the number of ring positions was $26^2 = 676$. The second rotor also had a kick associated to it making the cycle length of the three rotors equal to

$$26 \cdot 25 \cdot 26 = 16\,900.$$

The effect of the moving rotors was that a given plaintext letter would encrypt to a different ciphertext letter on each press of the keyboard.

Finally, a plug board was used to swap letters twice in each encryption and decryption operation. This increased the complexity and gave another possible 10^{14} keys.

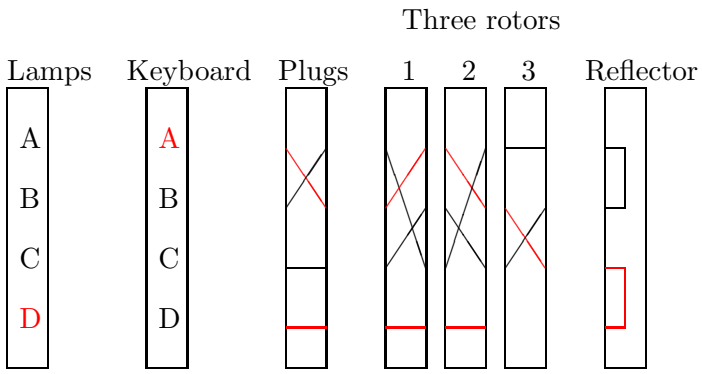
The rotors used, their order, their starting positions, the ring positions and the plug board settings all made up the secret key. Hence, the total number of keys was then around 2^{75}.

To make sure encryption and decryption were the same operation a reflector was used. This was a fixed public substitution given by

ABCDEFGHIJKLMNOPQRSTUVWXYZ
YRUHQSLDPXNGOKMIEBFZCWVJAT

The operation of a simplified Enigma machine is described in Fig. 1. By tracing the red lines one can see how the plaintext character A encrypts to the ciphertext character D. Notice that encryption and decryption can be performed by the machine being in the same positions. Now assume that rotor one moves on one step, so A now maps to D under rotor one, B to A, C to C and D to B. You should work out what happens with the example when we encrypt A again.

FIGURE 1. Simplified Enigma machine



In the rest of this chapter we present more details on the Enigma machine and some of the attacks which can be performed on it. However before presenting the machine itself we need to fix some notation which will be used throughout this chapter. In particular lower case letters will denote variables, upper case letters will denote "letters" (of the plaintext/ciphertext languages) and greek letters will denote permutations in S_{26} which we shall represent as permutations on the

upper case letters. Hence x can equal X and Y, but X can only ever represent X, whereas χ could represent (XY) or (ABC).

Permutations will usually be given in cycle notation. One always has to make a choice as to whether we multiply permutations from left to right, or right to left. We decide to use the left to right method, hence

$$(ABCD)(BE)(CD) = (AEBD).$$

Permutations hence act on the right of letters, something we will denote by x^σ, e.g.

$$A^{(ABCD)(XY)} = B.$$

This is consistent with the usual notation of right action for groups acting on sets. See Appendix A for more details about permutations.

We now collect some basic facts and theorems about permutations which we will need in the sequel.

THEOREM 4.1. *Two permutations σ and τ which are conjugate, i.e. for which $\sigma = \lambda \cdot \tau \cdot \lambda^{-1}$ for some permutation λ, have the same cycle structure.*

We define the support of a permutation to be the set of letters which are not fixed by the permutation. Hence, if σ acts on the set of letters $\mathcal{L}$, then as usual we denote by $\mathcal{L}^\sigma$ the set of fixed points and hence the support is given by

$$\mathcal{L} \setminus \mathcal{L}^\sigma.$$

THEOREM 4.2. *If two permutations, with the same support, consist only of disjoint transpositions then their product contains an even number of disjoint cycles of the same lengths.*

If a permutation with support an even number of symbols has an even number of disjoint cycles of the same lengths, then the permutation can be written as a product of two permutations each of which consists of disjoint transpositions.

In many places we need an algorithm to solve the following problem: Given $\alpha_i, \beta_i \in S_{26}$, for $i = 1, \ldots, m$ find $\gamma \in S_{26}$ such that

$$\alpha_i = \gamma^{-1} \cdot \beta_i \cdot \gamma \text{ for } i = 1 \ldots, m.$$

Note, there could be many such solutions γ, but in the situations we will apply it we expect there to be only a few.

For example suppose we have one such equation with

$$\begin{aligned} \alpha_1 &= (AFCNE)(BWXHUJOG)(DVIQZ)(KLMYTRPS), \\ \beta_1 &= (AEYSXWUJ)(BFZNO)(CDPKQ)(GHIVLMRT) \end{aligned}$$

We need to determine the structure of the permutation γ such that

$$\alpha_1 = \gamma^{-1} \cdot \beta_1 \cdot \gamma.$$

We first look at what should A map to under γ. If $A^\gamma = B$, then from α_1 and β_1 we must have $E^\gamma = W$, which in turn implies $Y^\gamma = X$. Carrying on in this way via a pruned depth first search we can determine a set of possible values for γ. Such an algorithm is relatively simple to write down in C, using a recursive procedure call. It however of course been a bit of a pain to do this by hand, as one would need to in the 1930's and 1940's.

2. An Equation For The Enigma

To aid our discussion in later sections we now describe the Enigma machine as a permutation equation. We first assume a canonical map between letters and the integers $\{0, 1, \ldots, 25\}$ such that $0 \leftarrow A$, $1 \leftarrow B$, etc and we assume a standard three wheel Enigma machine.

The wheel which turns the fastest we shall call rotor one, whilst the one which turns the slowest we shall call rotor three. This means that when looking at a real machine rotor three is the left

most rotor and rotor one is the right most rotor. This can cause confusion (especially when reading day/message settings), so please keep this in mind.

The basic permutations which make up the Enigma machine are as follows:

2.1. Choice of Rotors. We assume that the three rotors are chosen from the following set of five rotors. We present these rotors in cycle notation, but they are the commonly labelled rotors I, II, III, IV and V used in the actual Enigma machines, which were given earlier. Each rotor also has a different notch position which controls how the stepping of one rotor drives the stepping of the others.

Rotor	Permutation Representation	Notch Position
I	$(AELTPHQXRU)(BKNW)(CMOY)(DFG)(IV)(JZ)$	$16 \leftarrow Q$
II	$(BJ)(CDKLHUP)(ESZ)(FIXVYOMW)(GR)(NT)$	$4 \leftarrow E$
III	$(ABDHPEJT)(CFLVMZOYQIRWUKXSG)$	$21 \leftarrow V$
IV	$(AEPLIYWCOXMRFZBSTGJQNH)(DV)(KU)$	$9 \leftarrow J$
V	$(AVOLDRWFIUQ)(BZKSMNHYC)(EGTJPX)$	$25 \leftarrow Z$

2.2. Reflector. There were a number of reflectors used in actual Enigma machines. In our description we shall use the reflector given earlier, which is often referred to as called "Reflector B". This reflector has representation via disjoint cycles as

$$\varrho = (AY)(BR)(CU)(DH)(EQ)(FS)(GL)(IP)(JX)(KN)(MO)(TZ)(VW).$$

2.3. An Enigma Key. An Enigma key consists of the following information:

- A choice of rotors ρ_1, ρ_2, ρ_3 from the above choice of five possible rotors. Note, this choice of rotors affects the three notch positions, which we shall denote by n_1, n_2 and n_3. Also, as noted above, the rotor ρ_3 is placed in the left of the actual machine, whilst rotor ρ_1 is placed on the right. Hence, if in a German code book it says use rotors
$$I, II, III,$$
this means in our notation that ρ_1 is selected to be rotor III, that ρ_2 is selected to be rotor II and ρ_3 is selected to be rotor I.
- One must also select the ring positions, which we shall denote by r_1, r_2 and r_3. In the actual machine these are letters, but we shall use our canonical numbering to represent these as integers in $\{0, 1, \ldots, 25\}$.
- The plugboard is simply a product of disjoint transpositions which we shall denote by the permutation τ. In what follows we shall denote a plug linking letter A with letter B by $A \leftrightarrow B$.
- The starting rotor positions we shall denote by p_1, p_2 and p_3. These are the letters which can be seen through the windows on the top of the Enigma machine. Remember our numbering system is that the window on the left corresponds to p_3 and that on the right corresponds to p_1.

2.4. The Encryption Operation. We let σ denote the shift-up permutation given by

$$\sigma = (ABCDEFGHIJKLMNOPQRSTUVWXYZ).$$

The stepping of the second and third rotor is probably the hardest part to grasp when first looking at an Enigma machine, however this has a relatively simple description when one looks at it in a mathematical manner.

Given the above description of the key we wish to deduce the permutation ϵ_j, which represents the encryption of the jth letter, for $j = 0, 1, 2, \ldots,$.

We first set

$$\begin{aligned} m_1 &= n_1 - p_1 - 1 \pmod{26}, \\ m &= n_2 - p_2 - 1 \pmod{26}, \\ m_2 &= m_1 + 1 + 26m. \end{aligned}$$

The values of m_1 and m_2 control the stepping of the second and the third rotors.

We let $\lfloor x \rfloor$ denote the round towards zero function, i.e. $\lfloor 1.9 \rfloor = 1$ and $\lfloor -1.9 \rfloor = -1$. We now set, for encrypting letter j,

$$\begin{aligned} k_1 &= \lfloor (j - m_1 + 26)/26 \rfloor, \\ k_2 &= \lfloor (j - m_2 + 650)/650 \rfloor, \\ i_1 &= p_1 - r_1 + 1, \\ i_2 &= p_2 - r_2 + k_1 + k_2, \\ i_3 &= p_3 - r_3 + k_2. \end{aligned}$$

Notice, how i_3 is stepped on every $650 = 26 \cdot 25$ iterations whilst i_2 is stepped on every 26 iterations and also stepped on an extra notch every 650 iterations.

We can now present ϵ_j as

$$\begin{aligned} \epsilon_j = \tau \cdot (\sigma^{i_1+j} \rho_1 \sigma^{-i_1-j}) \cdot (\sigma^{i_2} \rho_2 \sigma^{-i_2}) \cdot (\sigma^{i_3} \rho_3 \sigma^{-i_3}) \cdot \varrho \cdot \\ \cdot (\sigma^{i_3} {\rho_3}^{-1} \sigma^{-i_3}) \cdot (\sigma^{i_2} {\rho_2}^{-1} \sigma^{-i_2}) \cdot (\sigma^{i_1+j} {\rho_1}^{-1} \sigma^{-i_1-j}) \cdot \tau. \end{aligned}$$

Note that the same equation/machine is used to encrypt the jth letter as is used to decrypt the jth letter. Hence we have

$${\epsilon_j}^{-1} = \epsilon_j.$$

Also note that each ϵ_j consists of a product of disjoint transpositions. We shall always use γ_j to represent the internal rotor part of the Enigma machine, hence

$$\epsilon_j = \tau \cdot \gamma_j \cdot \tau.$$

3. Determining The Plugboard Given The Rotor Settings

For the moment assume that we know values for the rotor order, ring settings and rotor positions. We would like to determine the plugboard settings, we are therefore given γ_j. The goal is therefore to determine τ given some information about ϵ_j for some values of j.

One often sees written that determining the plugboard given the rotor settings is equivalent to solving a substitution cipher. This is true, but often the method given in some sources is too simplistic.

If we let m denote the actual message being encrypted and c the corresponding ciphertext, and m' the ciphertext decrypted under the cipher with no plugboard, i.e. with an obvious notation,

$$\begin{aligned} m &= c^{\epsilon}, \\ m' &= c^{\gamma}. \end{aligned}$$

The following is an example value of m' for a plugboard containing only one plug

```
ZNCT UPZN A EIME, THEKE WAS A GILL CALLED SNZW WHFTE.
```

I have left the spacing's in the English words. You may then deduce that Z should really be O, or T should really be E, or E should really be T, or maybe K should map to R or L to R or F to I. But which should be the correct plug ? The actual correct plug is setting is that O should map to Z, the other mappings are the result of this single plug setting.

We now present some ways of obtaining information about the plugboard given various scenarios.

3.1. Ciphertext Only Attack. In a ciphertext only attack one can proceed as one would for a normal substitution cipher. We need a method to be able to distinguish something which could be natural language from something which is completely random. The best statistic seems to be to use one called the Sinkov statistic. Let f_i, for $i = A, \ldots, Z$, denote the frequencies of the various letters in standard English. For a given piece of text we let n_i, for $i = A, \ldots, Z$, denote the frequencies of the various letters within the sample piece of text. The Sinkov statistic for the sample text is given by

$$s = \sum_{i=A}^{Z} n_i f_i.$$

A high value of this statistic corresponds to something which is more likely to be from a natural language.

To mount a ciphertext only attack we let γ_j denote our current approximation for ϵ_j (initially γ_j has no plug settings, but this will change as the method progresses). We now go through all possible single plug settings, $\alpha^{()}$. There are $26 \cdot 25/2 = 325$ of these. We then decrypt the ciphertext c using the cipher

$$\alpha^{(k)} \cdot \gamma_j \cdot \alpha^{(k)}.$$

This results in 325 possible plaintext messages $m^{(k)}$ for $k = 1, \ldots, 325$. For each one of these we compute the Sinkov statistic s_k, we keep the value of $\alpha^{(k)}$ which results in s_k being minimized. We then set our new γ_j to be $\alpha^{(k)} \cdot \gamma_j \cdot \alpha^{(k)}$ and repeat, until no further improvement can be made in the test statistic.

This methodology seems very good at finding the missing plugboard settings. For example consider an Enigma machine with the rotors set to be Suppose we are given that the day setting is

Rotors	Rings	Pos	Plugboard
III, II, I	PPD	MDL	Unknown

The actual hidden plugboard is given by $A \leftrightarrow B$, $C \leftrightarrow D$, $E \leftrightarrow F$, $G \leftrightarrow H$, $I \leftrightarrow J$ and $K \leftrightarrow L$. We obtain the ciphertext

```
HUCDODANDHOMYXUMGLREDSQQJDNJAEXUKAZOYGBYLEWFNWIBWILSMAETFFBVPR
GBYUDNAAIEVZZKCUFNIUTOKNKAWUTUWQJYAUHMFWJNIQHAYNAGTDGTCTNYKTCU
FGYQBSRRUWZKZFWKPGVLUHYWZCZSOYJNXHOSKVPHGSGSXEOQWOZYBXQMKQDDXM
BJUPSQODJNIYEPUCEXFRHDQDAQDTFKPSZEMASWGKVOXUCEYWBKFQCYZBOGSFES
OELKDUTDEUQZKMUIZOGVTWKUVBHLVXMIXKQGUMMQHDLKFTKRXCUNUPPFKWUFCU
PTDMJBMMTPIZIXINRUIEMKDYQFMIQAEVLWJRCYJCUKUFYPSLQUEZFBAGSJHVOB
CHAKHGHZAVJZWOLWLBKNTHVDEBULROARWOQGZLRIQBVVSNKRNUCIKSZUCXEYBD
QKCVMGLRGFTBGHUPDUHXIHLQKLEMIZKHDEPTDCIPF
```

The plugboard settings are found in the following order $I \leftrightarrow J$, $E \leftrightarrow F$, $A \leftrightarrow B$, $G \leftrightarrow H$, $K \leftrightarrow L$ and $C \leftrightarrow D$. The plaintext is determined to be.

```
ITWASTHEBESTOFTIMESITWASTHEWORSTOFTIMESITWASTHEAGEOFWISDOMITWA
STHEAGEOFFOOLISHNESSITWASTHEEPOCHOFBELIEFITWASTHEEPOCHOFINCRED
ULITYITWASTHESEASONOFLIGHTITWASTHESEASONOFDARKNESSITWASTHESPRI
NGOFHOPEITWASTHEWINTEROFDESPAIRWEHADEVERYTHINGBEFOREUSWEHADNOT
HINGBEFOREUSWEWEREALLGOINGDIRECTTOHEAVENWEWEREALLGOINGDIRECTTH
EOTHERWAYINSHORTTHEPERIODWASSOFARLIKETHEPRESENTPERIODTHATSOMEO
FITSNOISIESTAUTHORITIESINSISTEDONITSBEINGRECEIVEDFORGOODORFORE
VILINTHESUPERLATIVEDEGREEOFCOMPARISONONLY
```

3.2. Known Plaintext Attack. When one knows the plaintext there are two methods one can employ. The first method is simply based on a depth first search technique, whilst the second makes use of some properties of the encryption operation.

3.2.1. *Technique One:* In the first technique we take each wrong letter in turn, from our current approximation γ_j to ϵ_j. In the above example, of the encryption of "A Tale of Two Cities", we have that the first ciphertext letter H should map to the plaintext letter I. This implies that the plugboard must contain plug settings $H \leftrightarrow p_H$ and $I \leftrightarrow p_I$, for letters p_H and p_I with

$$p_H{}^{\gamma_0} = p_I.$$

We in a similar manner deduce the following other equations

$$\begin{array}{lll} p_U{}^{\gamma_1} = p_T, & p_C{}^{\gamma_2} = p_W, & p_D{}^{\gamma_3} = p_A, \\ p_O{}^{\gamma_4} = p_S, & p_D{}^{\gamma_5} = p_T, & p_A{}^{\gamma_6} = p_H, \\ p_N{}^{\gamma_7} = p_E, & p_D{}^{\gamma_8} = p_B, & p_H{}^{\gamma_9} = p_E. \end{array}$$

The various permutations which represent the first few γ_j's for the given rotor and ring positions are as follows:

$$\begin{aligned} \gamma_0 &= (AW)(BH)(CZ)(DE)(FT)(GJ)(IN)(KL)(MQ)(OV)(PU)(RS)(XY), \\ \gamma_1 &= (AZ)(BL)(CE)(DH)(FK)(GJ)(IS)(MX)(NQ)(OY)(PR)(TU)(VW), \\ \gamma_2 &= (AZ)(BJ)(CV)(DW)(EP)(FX)(GO)(HS)(IY)(KL)(MN)(QT)(RU), \\ \gamma_3 &= (AF)(BC)(DY)(EO)(GU)(HK)(IV)(JR)(LX)(MN)(PW)(QS)(TZ), \\ \gamma_4 &= (AJ)(BD)(CF)(EL)(GN)(HX)(IM)(KQ)(OS)(PV)(RT)(UY)(WZ), \\ \gamma_5 &= (AW)(BZ)(CT)(DI)(EH)(FV)(GU)(JO)(KP)(LN)(MX)(QY)(RS), \\ \gamma_6 &= (AL)(BG)(CO)(DV)(EN)(FS)(HY)(IZ)(JT)(KW)(MP)(QR)(UX), \\ \gamma_7 &= (AI)(BL)(CT)(DE)(FN)(GH)(JY)(KZ)(MO)(PS)(QX)(RU)(VW), \\ \gamma_8 &= (AC)(BH)(DU)(EM)(FQ)(GV)(IO)(JZ)(KS)(LT)(NR)(PX)(WY), \\ \gamma_9 &= (AB)(CM)(DY)(EZ)(FG)(HN)(IR)(JX)(KV)(LW)(OT)(PQ)(SU). \end{aligned}$$

We now proceed as follows: Suppose we know that there are exactly six plugs being used. This means that if we pick a letter at random, say T, then there is a $14/26 = 0.53$ chance that this letter is not plugged to another one. Let us therefore make this assumption for the letter T, in which case $p_T = T$. From the above equations involving γ_1 and γ_5 we then deduce that

$$p_U = U \text{ and } p_D = C.$$

We then use the equations involving γ_3 and γ_8, since we now know p_D, to deduce that

$$p_A = B \text{ and } p_B = A.$$

This latter two checks are consistent so we can assume that our original choice of $p_T = T$ was a good one. From the equations involving γ_6, using $p_A = B$ we deduce that

$$p_H = G.$$

Using this in the equations involving γ_0 and γ_9 we deduce that

$$p_I = J \text{ and } p_E = F.$$

We then find that our five plug settings of $A \leftrightarrow B$, $C \leftrightarrow D$, $E \leftrightarrow F$, $G \leftrightarrow H$ and $I \leftrightarrow J$ allow us to decrypt the first ten letters correctly. To deduce the final plug setting will require a piece of ciphertext, and a corresponding piece of known plaintext, such that either the plaintext or the ciphertext involves either the letter K or the letter L.

This technique can also be used when one knows partial information about the rotor positions. For example many of the following techniques will allow us to deduce the differences $p_i - r_i$, but not the actual values of r_i or p_i. However, by following the above technique, on assuming $r_i =' A'$, we will at some point deduce a contradiction. At this point we know that a rotor turnover has either occurred incorrectly or has not occurred when it should have. Hence, we can at this point

backtrack and deduce the correct turnover. For an example of this technique at work see the latter section on the Bombe.

3.2.2. *Technique Two:* A second method is possible when less than 13 plugs used. In the plaintext obtained under γ_j a number of incorrect letters will appear. Again we let m denote the actual plaintext and m' the plaintext derived with the current (possibly empty) plugboard setting. We suppose there are t plugs left to find.

Suppose we concentrate on each places for which the incorrect plaintext letter A occurs, i.e. all occurances of A in the plaintext m which are wrong. Let x denote the corresponding ciphertext letter, there are two possible cases which can occur

- The letter x should be plugged to an unknown letter. In which case the resulting letter in the message m' will behave randomly (assuming γ_j is acts like a random permutation).
- The letter x does not occur in a plugboard setting. In which case the resulting incorrect plaintext character is the one which should be plugged to A in the actual cipher.

Assuming ciphertext letters are uniformly distributed, the first occurance will occur with probability $t/13$, whilst the alternative will occur with probability $1 - t/13$. This gives the following method to determine which letter A should be connected to. For all letters A in the plaintext m compute the frequency of the corresponding letter in the approximate plaintext m'. The letter which has the highest frequency is highly likely to be the one which should be connect to A on the plugboard. Indeed we expect this letter to occur for a proportion of the letters given by $1 - t/13$, all other letters we expect to occur with a proportion of $t/(13 \cdot 26)$ each.

The one problem with this second technique is that it requires a relatively large amount of known plaintext. Hence, in practice the first technique is more likely to be used.

3.3. Knowledge of ϵ_j for some j's. If we know the value of the permutation ϵ_j for values of $j \in \mathcal{S}$, then we have the following equation

$$\epsilon_j = \tau \cdot \gamma_j \cdot \tau \text{ for } j \in \mathcal{S}.$$

Since $\tau = \tau^{-1}$ this allows us to compute possible values of τ using our previous method for solving this conjugation problem. This might not determine the whole plugboard but it will determine enough for other methods to be used.

3.4. Knowledge of $\epsilon_j \cdot \epsilon_{j+3}$ for some j's. A similar method to the previous one applies in this case, as if we know $\epsilon_j \cdot \epsilon_{j+3}$ for all $j \in \mathcal{S}$ and we know γ_j, then we have the equation

$$(\epsilon_j \cdot \epsilon_{j+3}) = \tau \cdot (\gamma_j \cdot \gamma_{j+3}) \cdot \tau \text{ for } j \in \mathcal{S}.$$

4. Double Encryption Of Message Keys

The polish mathematicians Jerzy Rozycki, Henryk Zygalski and Marian Rejewski were the first to find ways of analysing the Enigma machine. To understand their methods one must first understand how the Germans used the machine. On each day the machine was set up with a key, as above, which was chosen by looking up in a code book. Each subnet would have a different day key.

To encipher a message the sending operator decided on a message key. The message key would be a sequence of three letters, say DHI. The message key needs to be transported to the recipient. Using the day key, the message key would be enciphered twice. The double enciphering is to act as a form of error control. Hence, DHI might be enciphered as $XHJKLM$. Note, that D encrypts to X and then K, this is a property of the Enigma machine.

The receiver would obtain $XHJKLM$ and then decrypt this to obtain DHI. Both operators would then move the wheels around to the positions D, H and I, i.e. they would turn the wheels so that D was in the leftmost window, H in the middle one and I in the rightmost window. Then the actual message would be enciphered.

For this example, in our notation, this would mean that the message key is equal to the day key, except that $p_1 = 8 \leftarrow I$, $p_2 = 7 \leftarrow H$ and $p_3 = 3 \leftarrow D$.

Suppose we intercept a set of messages which have the following headers, consisting of the encryption of the three letter rotor positions, followed by its encryption again, i.e. the first six letters of each message are equal to

UCWBLR	ZSETEY	SLVMQH	SGIMVW	PMRWGV
VNGCTP	OQDPNS	CBRVPV	KSCJEA	GSTGEU
DQLSNL	HXYYHF	GETGSU	EEKLSJ	OSQPEB
WISIIT	TXFEHX	ZAMTAM	VEMCSM	LQPFNI
LOIFMW	JXHUHZ	PYXWFQ	FAYQAF	QJPOUI
EPILWW	DOGSMP	ADSDRT	XLJXQK	BKEAKY
.....	.....	.....	.....	.....
DDESRY	QJCOUA	JEZUSN	MUXROQ	SLPMQI
RRONYG	ZMOTGG	XUOXOG	HIUYIE	KCPJLI
DSESEY	OSPPEI	QCPOLI	HUXYOQ	NYIKFW

If we take the last one of these and look at it in more detail. We know that there are three underlying secret letters, say l_1, l_2 and l_3. We also know that

$$l_1{}^{\epsilon_0} = N,\ l_2{}^{\epsilon_1} = Y,\ l_3{}^{\epsilon_2} = I,$$

and

$$l_1{}^{\epsilon_3} = K,\ l_2{}^{\epsilon_4} = F,\ l_3{}^{\epsilon_5} = W.$$

Hence, given that ${\epsilon_j}^{-1} = \epsilon_j$, we have

$$N^{\epsilon_0\epsilon_3} = l_1{}^{\epsilon_0\epsilon_0\epsilon_3} = l_1{}^{\epsilon_3} = K,\ Y^{\epsilon_1\epsilon_4} = F,\ I^{\epsilon_2\epsilon_5} = W.$$

Continuing in this way we can compute a permutation representation of the three products as follows:

$$\begin{aligned}
\epsilon_0 \cdot \epsilon_3 &= (ADSMRNKJUB)(CV)(ELFQOPWIZT)(HY),\\
\epsilon_1 \cdot \epsilon_4 &= (BPWJUOMGV)(CLQNTDRYF)(ES)(HX),\\
\epsilon_2 \cdot \epsilon_5 &= (AC)(BDSTUEYFXQ)(GPIWRVHZNO)(JK).
\end{aligned}$$

5. Determining The Internal Rotor Wirings

However, life was even more difficult for the Poles as they did not even know the rotor wirings or the reflector values. Hence, they needed to break the machine without even having a description of the actual machine. They did have access to a non-miliatary version of Enigma and deduced the basic structure. In this they had two bits of luck:

(1) They were very lucky in that they deduced that the wiring between the plugboard and the right most rotor was in the order of the alphabet. If this were not the case there would have been some hidden permutation which would also have needed to be found.
(2) Secondly, the French cryptography Gustave Bertrand obtained from a German spy, Hans-Thilo Schmidt, two months worth of day keys. Thus, for two months of traffic the Poles had access to the day settings.

From this information they needed to deduce the internal wirings of the Enigma machine.

Note, in the pre-war days the Germans only used three wheels out of a choice of three, hence the number of days keys is actually reduced by a factor of ten. This is, however, only a slight simplification (at least with modern technology).

Suppose we are given that the day setting is

Rotors	Rings	Pos	Plugboard
III, II, I	TXC	EAZ	$(AMTEBC)$

We do not know what the actual rotors are at present, but we know that the one labelled rotor I will be placed in the rightmost slot (our label one). So we have

$$r_1 = 2,\ r_2 = 23,\ r_3 = 19, p_1 = 25,\ p_2 = 0,\ p_3 = 4.$$

Suppose also that the data from the previous section was obtained as traffic for that day. Hence, we obtain the following three values for the products $\epsilon_j \cdot \epsilon_{j+1}$,

$$\begin{aligned}
\epsilon_0 \cdot \epsilon_3 &= (ADSMRNKJUB)(CV)(ELFQOPWIZT)(HY),\\
\epsilon_1 \cdot \epsilon_4 &= (BPWJUOMGV)(CLQNTDRYF)(ES)(HX),\\
\epsilon_2 \cdot \epsilon_5 &= (AC)(BDSTUEYFXQ)(GPIWRVHZNO)(JK).
\end{aligned}$$

From these we wish to deduce the values of ϵ_0, $\epsilon_1, \ldots, \epsilon_5$. We will use the fact that ϵ_j is a product of disjoint transpositions and Theorem 4.2 and its proof.

We take the first product and look at it in more detail. We take the sets of two cycles of equal degree and write them above one another, with the bottom one reversed in order, i.e.

$$\begin{array}{cccccccccc cc}
A & D & S & M & R & N & K & J & U & B & C & V\\
T & Z & I & W & P & O & Q & F & L & E & Y & H
\end{array}$$

We now run through all possible shifts of the bottom rows. Each shift gives us a possible value of ϵ_0 and ϵ_3. The value of ϵ_0 is obtained from reading off the disjoint transpositions from the columns, the value of ϵ_3 is obtained by reading off the transpositions from the "off diagonals". For example with the above orientation we would have

$$\begin{aligned}
\epsilon_0 &= (AT)(DZ)(SI)(MW)(RP)(NO)(KQ)(JF)(UL)(BE)(CY)(VH),\\
\epsilon_3 &= (DT)(SZ)(MI)(RW)(NP)(KO)(JQ)(UF)(BL)(AE)(VY)(CH).
\end{aligned}$$

This still leaves us, in this case, with $20 = 2 \cdot 10$ possible values for ϵ_0 and ϵ_3.

Now, to reduce this number we need to really on stupid operators. Various operators had a tendency to always select the same three letter message key. For example popular choices where QWE (the first letters on the keyboard). One operator used the letters of his girlfriend name, Cillie, hence such "cribs" (or guessed/known plaintexts in todays jargon) became known as "cillies". Note, for our analysis here we only need one Cillie the day when we wish to obtain the internal wiring of rotor I.

In our dummy example, suppose we guess (correctly) that the first message key is indeed QWE. This means that $UCWBLR$ is the encryption of QWE twice, this in turn tells us how to align our cycle of length 10 in the first permutation, as under ϵ_0 the letter Q must encrypt to U.

$$\begin{array}{cccccccccc}
A & D & S & M & R & N & K & J & U & B\\
L & E & T & Z & I & W & P & O & Q & F
\end{array}$$

We can check that this is consistent as we see that Q under ϵ_3 must then encrypt to B. If we guessed one more such cillies we can reduce the number of possibilities for $\epsilon_1, \ldots, \epsilon_6$. Assuming we carry on in this way we will finally deduce that

$$\begin{aligned}
\epsilon_0 &= (AL)(BF)(CH)(DE)(GX)(IR)(JO)(KP)(MZ)(NW)(QU)(ST)(VY),\\
\epsilon_1 &= (AK)(BQ)(CW)(DM)(EH)(FJ)(GT)(IZ)(LP)(NV)(OR)(SX)(UY),\\
\epsilon_2 &= (AJ)(BN)(CK)(DZ)(EW)(FP)(GX)(HS)(IY)(LM)(OQ)(RU)(TV),\\
\epsilon_3 &= (AF)(BQ)(CY)(DL)(ES)(GX)(HV)(IN)(JP)(KW)(MT)(OU)(RZ),\\
\epsilon_4 &= (AK)(BN)(CJ)(DG)(EX)(FU)(HS)(IZ)(LW)(MR)(OY)(PQ)(TV),\\
\epsilon_5 &= (AK)(BO)(CJ)(DN)(ER)(FI)(GQ)(HT)(LM)(PX)(SZ)(UV)(WY).
\end{aligned}$$

We now need to use this information to deduce the value of ρ_1, etc. So for the rest of this section we assume we know ϵ_j for $j = 0, \ldots, 5$, and so we mark it in blue.

Recall that we have,

$$\begin{aligned}\epsilon_j &= \tau \cdot (\sigma^{i_1+j}\rho_1\sigma^{-i_1-j}) \cdot (\sigma^{i_2}\rho_2\sigma^{-i_2}) \cdot (\sigma^{i_3}\rho_3\sigma^{-i_3}) \cdot \varrho \cdot \\ &\quad \cdot (\sigma^{i_3}{\rho_3}^{-1}\sigma^{-i_3}) \cdot (\sigma^{i_2}{\rho_2}^{-1}\sigma^{-i_2}) \cdot (\sigma^{i_1+j}{\rho_1}^{-1}\sigma^{-i_1-j}) \cdot \tau\end{aligned}$$

We now assume that no stepping of the second rotor occurs during the first six encryptions under the day setting. This occurs with quite high probability, namely $20/26 \approx 0.77$. If this assumption turns out to be false we will notice this in our later analysis and it will mean we can deduce something about the (unknown to us at this point) position of the notch on the first rotor.

Given that we know the day settings, so that we know τ and the values of i_1, i_2 and i_3 (since we are assuming $k_1 = k_2 = 0$ for $0 \leq j \leq 5$), we can write the above equation for $0 \leq j \leq 5$ as

$$\begin{aligned}\lambda_j &= \sigma^{-i_1-j} \cdot \tau \cdot \epsilon_j \cdot \tau \cdot \sigma^{i_1+j} \\ &= \rho_1 \cdot \sigma^{-j} \cdot \gamma \cdot \sigma^{j} \cdot {\rho_1}^{-1}.\end{aligned}$$

Where λ_j is now known and we wish to determine ρ_1 for some fixed but unknown value of γ. The permutation γ is in fact equal to

$$\gamma = (\sigma^{i_2-i_1}\rho_2\sigma^{-i_2}) \cdot (\sigma^{i_3}\rho_3\sigma^{-i_3}) \cdot \varrho \cdot (\sigma^{i_3}{\rho_3}^{-1}\sigma^{-i_3}) \cdot (\sigma^{i_2}{\rho_2}^{-1}\sigma^{i_1-i_2}).$$

In our example we get the following values for λ_j,

$$\begin{aligned}\lambda_0 &= (AD)(BR)(CQ)(EV)(FZ)(GP)(HM)(IN)(JK)(LU)(OS)(TW)(XY), \\ \lambda_1 &= (AV)(BP)(CZ)(DF)(EI)(GS)(HY)(JL)(KO)(MU)(NQ)(RW)(TX), \\ \lambda_2 &= (AL)(BK)(CN)(DZ)(EV)(FP)(GX)(HS)(IY)(JM)(OQ)(RU)(TW), \\ \lambda_3 &= (AS)(BF)(CZ)(DR)(EM)(GN)(HY)(IW)(JO)(KQ)(LX)(PV)(TU), \\ \lambda_4 &= (AQ)(BK)(CT)(DL)(EP)(FI)(GX)(HW)(JU)(MO)(NY)(RS)(VZ), \\ \lambda_5 &= (AS)(BZ)(CV)(DO)(EM)(FR)(GQ)(HK)(IL)(JT)(NP)(UW)(XY).\end{aligned}$$

We now form, for $j = 0, \ldots, 4$,

$$\begin{aligned}\mu_j &= \lambda_j \cdot \lambda_{j+1}, \\ &= \rho_1 \cdot \sigma^{-j} \cdot \gamma \cdot \sigma^{-1} \cdot \gamma \cdot \sigma^{j+1} \cdot {\rho_1}^{-1}, \\ &= \rho_1 \cdot \sigma^{-j} \cdot \delta \cdot \sigma^{j} \cdot {\rho_1}^{-1},\end{aligned}$$

where $\delta = \gamma \cdot \sigma^{-1} \cdot \gamma \cdot \sigma$ is unknown.

Eliminating δ via $\delta = \sigma^{j-1}{\rho_1}^{-1}\mu_{j-1}\rho_1\sigma^{-j+1}$ we find the following equations for $j = 1, \ldots, 4$,

$$\begin{aligned}\mu_j &= (\rho_1 \cdot \sigma^{-1} \cdot {\rho_1}^{-1}) \cdot \mu_{j-1} \cdot (\rho_1 \cdot \sigma \cdot {\rho_1}^{-1}), \\ &= \alpha \cdot \mu_{j-1} \cdot \alpha^{-1},\end{aligned}$$

where $\alpha = \rho_1 \cdot \sigma^{-1} \cdot {\rho_1}^{-1}$.

Hence, μ_j and μ_{j-1} are conjugate and so by Theorem 4.1 have the same cycle structure. For our example we have

$$\begin{aligned}\mu_0 &= (AFCNE)(BWXHUJOG)(DVIQZ)(KLMYTRPS), \\ \mu_1 &= (AEYSXWUJ)(BFZNO)(CDPKQ)(GHIVLMRT), \\ \mu_2 &= (AXNZRTIH)(BQJEP)(CGLSYWUD)(FVMOK), \\ \mu_3 &= (ARLGYWFK)(BIHNXDSQ)(CVEOU)(JMPZT), \\ \mu_4 &= (AGYPMDIR)(BHUTV)(CJWKZ)(ENXQSFLO).\end{aligned}$$

At this point we can check whether our assumption of no-stepping, i.e. a constant value for the values of i_2 and i_3 is valid. If a step did occur in the second rotor then the above permutations would be unlikely to have the same cycle structure.

We need to determine the structure of the permutation α, this is done by looking at the four equations simultaneously. We note that since σ and α are conjugates, under ρ_1, we know that α has cycle structure of a single cycle of length 26.

In our example we only find one possible solution for α, namely

$$\alpha = (AGYWUJOQNIRLSXHTMKCEBZVPFD).$$

To solve for ρ_1 we need to find a permutation such that

$$\alpha = \rho_1 \cdot \sigma^{-1} \cdot {\rho_1}^{-1}.$$

We find there are 26 such solutions

$$\begin{array}{l}
(AELTPHQXRU)(BKNW)(CMOY)(DFG)(IV)(JZ)\\
(AFHRVJ)(BLU)(CNXSTQYDGEMPIW)(KOZ)\\
(AGFIXTRWDHSUCO)(BMQZLVKPJ)(ENY)\\
(AHTSVLWEOBNZMRXUDIYFJCPKQ)\\
(AIZN)(BOCQ)(DJ)(EPLXVMSWFKRYGHU)\\
(AJEQCRZODKSXWGI)(BPMTUFLYHVN)\\
(AKTVOER)(BQDLZPNCSYI)(FMUGJ)(HW)\\
(AL)(BR)(CTWI)(DMVPOFN)(ESZQ)(GKUHXYJ)\\
(AMWJHYKVQFOGLBS)(CUIDNETXZR)\\
(ANFPQGMX)(BTYLCVRDOHZS)(EUJI)(KW)\\
(AOIFQH)(BUKX)(CWLDPREVS)(GN)(MY)(TZ)\\
(APSDQIGOJKYNHBVT)(CX)(EWMZUL)(FR)\\
(AQJLFSEXDRGPTBWNIHCYOKZVUM)\\
(ARHDSFTCZWOLGQK)(BXEYPUNJM)\\
(ASGRIJNKBYQLHEZXFUOMC)(DT)(PVW)\\
(ATE)(BZYRJONLIKC)(DUPWQM)(FVXGSH)\\
(AUQNMEB)(DVYSILJPXHGTFWRK)\\
(AVZ)(CDWSJQOPYTGURLKE)(FXIM)\\
(AWTHINOQPZBCEDXJRMGV)(FYUSK)\\
(AXKGWUTIORNP)(BDYV)(CFZ)(HJSLM)\\
(AYWVCGXLNQROSMIPBEF)(DZ)(HK)(JT)\\
(AZEGYXMJUVD)(BF)(CHLOTKIQSNRP)\\
(BGZFCIRQTLPD)(EHMKJV)(NSOUWX)\\
(ABHNTMLQUXOVFDCJWYZG)(EISP)\\
(ACKLRSQVGBITNUY)(EJXPF)(HOWZ)\\
(ADEKMNVHPGCLSRTOXQW)(BJY)(IUZ)
\end{array}$$

These are the values of $\rho_1 \cdot \sigma^i$, for $i = 0, \ldots, 25$.

So with one days messages we can determine the value of ρ_1 upto multiplication by a power of σ. The Polish had access to two months such data and so were able to determine similar sets for ρ_2 and ρ_3 (as different rotor orders are used on different days). Note, at this point the Germans did not use a selection of three from five rotors.

If we select three representatives $\hat{\rho}_1$, $\hat{\rho}_2$ and $\hat{\rho}_3$, from the sets of possible rotors, then we have

$$\begin{aligned}
\hat{\rho}_1 &= \rho_1 \cdot \sigma^{l_1},\\
\hat{\rho}_2 &= \rho_2 \cdot \sigma^{l_2},\\
\hat{\rho}_3 &= \rho_3 \cdot \sigma^{l_3}.
\end{aligned}$$

However, we still do not know the value for the reflector ϱ, or the correct values of l_1, l_2 and l_3. To understand how to proceed next we present the following theorem.

THEOREM 4.3. *Consider an Enigma machine $\mathcal{E}$ that uses rotors ρ_1, ρ_2 and ρ_3, and reflector ϱ. Then there is an enigma machine $\hat{\mathcal{E}}$ using rotors $\hat{\rho}_1$, $\hat{\rho}_2$ and $\hat{\rho}_3$, and a different refelector $\hat{\varrho}$ such that, for every setting of $\mathcal{E}$, there is a setting of $\hat{\mathcal{E}}$ such that the machines have identical behaviour. Furthermore, $\hat{\mathcal{E}}$ can be constructed so that the machines use identical daily settings except for the ring positions.*

PROOF. The following proof was shown to me by Eugene Luks who I thank for allowing me to reproduce it here. The first claim is that $\hat{\varrho}$ is determined via

$$\hat{\varrho} = \sigma^{-(l_1+l_2+l_3)}\varrho\sigma^{-(l_1+l_2+l_3)}.$$

We can see this by the following argument (and the fact that the reflector is uniquely determined by the above equation). We first define the following function

$$\begin{aligned} P(\phi_1,\phi_2,\phi_3,\psi,t_1,t_2,t_3) = \tau\cdot(\sigma^{t_1}\phi_1\sigma^{-t_1})\cdot(\sigma^{t_2}\phi_2\sigma^{-t_2})\cdot(\sigma^{t_3}\phi_3\sigma^{-t_3})\cdot\psi\cdot \\ \cdot(\sigma^{t_3}\phi_3^{-1}\sigma^{-t_3})\cdot(\sigma^{t_2}\phi_2^{-1}\sigma^{-t_2})\cdot(\sigma^{t_1}\phi_1^{-1}\sigma^{-t_1})\cdot\tau \end{aligned}$$

We then have the relation,

$$P(\hat{\rho}_1,\hat{\rho}_2,\hat{\rho}_3,\hat{\varrho},t_1,t_2,t_3) = P(\rho_1,\rho_2,\rho_3,\varrho,t_1,t_2+l_1,t_3+l_1+l_2).$$

Recall the following expressions for the functions which control the stepping of the three rotors:

$$\begin{aligned} k_1 &= \lfloor(j-m_1+26)/26\rfloor, \\ k_2 &= \lfloor(j-m_2+650)/650\rfloor, \\ i_1 &= p_1-r_1+1, \\ i_2 &= p_2-r_2+k_1+k_2, \\ i_3 &= p_3-r_3+k_2. \end{aligned}$$

The Enigma machine $\mathcal{E}$ is given by the equation

$$\epsilon_j = P(\rho_1,\rho_2,\rho_3,\varrho,i_1+j,i_2,i_3)$$

where we interpret i_2 and i_3 as functions of j as above. We now set the ring positions in $\hat{\mathcal{E}}$ to be given by

$$r_1, r_2+l_1, r_3+l_1+l_2$$

in which case we have the output of this Enigma machine is given by

$$\hat{\epsilon}_j = P(\hat{\rho}_1,\hat{\rho}_2,\hat{\rho}_3,\hat{\varrho},i_1+j,i_2-l_1,i_3-l_1-l_2).$$

But then we conclude that $\epsilon_j = \hat{\epsilon}_j$. □

We now use this result to fully determine $\mathcal{E}$ from the available data. We pick values of $\hat{\rho}_1$, $\hat{\rho}_2$ and $\hat{\rho}_3$ and determine a possible refelector by solving for $\hat{\varrho}$ in

$$\begin{aligned} \epsilon_0 = \tau\cdot(\sigma^{i_1}\hat{\rho}_1\sigma^{-i_1})\cdot(\sigma^{i_2}\hat{\rho}_2\sigma^{-i_2})\cdot(\sigma^{i_3}\hat{\rho}_3\sigma^{-i_3})\cdot\hat{\varrho}\cdot \\ \cdot(\sigma^{i_3}\hat{\rho}_3{}^{-1}\sigma^{-i_3})\cdot(\sigma^{i_2}\hat{\rho}_2{}^{-1}\sigma^{-i_2})\cdot(\sigma^{i_1}\hat{\rho}_1{}^{-1}\sigma^{-i_1})\cdot\tau \end{aligned}$$

We let $\hat{\mathcal{E}}^1$ denote the Enigma machine with rotors given by $\hat{\rho}_1,\hat{\rho}_2,\hat{\rho}_3$ and reflector $\hat{\varrho}$, but with ring settings the same as in the target machine $\mathcal{E}$ (we know the ring settings of $\mathcal{E}$ since we have the day key remember). Note $\hat{\mathcal{E}}^1 \neq \hat{\mathcal{E}}$ from the above proof, since the rings are in the same place as the target machine.

Assume we have obtained a long messages, with a given message key. We put the machine $\hat{\mathcal{E}}^1$ in the message key configuration and start to decrypt the message. This will work (i.e. produce a valid decryption) upto a point when the sequence of permutations $\hat{\epsilon}^1_j$ produced by $\hat{\mathcal{E}}^1$ differs from the sequence ϵ_j produced by $\mathcal{E}$.

At this point we cycle through all values of l_1 and fix the first permutation (and also the associated reflector) to obtain a new Enigma machine $\hat{\mathcal{E}}^2$ which allows us to decrypt more of the long message. If a long enough message is obtained we can also obtain l_2 is this way, or alternatively wait for another day when the rotors order is changed.

Thus the entire internal workings of the Enigma machine can be determined.

6. Determining The Day Settings

Now having determined the internal wirings, given the set of two months of day settings obtained by Bertrand, the next task is to determine the actual key when the day settings are not available. At this stage we assume the Germans are still using the encrypt the message setting twice routine.

The essential trick here is to notice that if we write the cipher as

$$\epsilon_j = \tau \cdot \gamma_j \cdot \tau,$$

then

$$\epsilon_j \cdot \epsilon_{j+3} = \tau \cdot \gamma_j \cdot \gamma_{j+3} \cdot \tau.$$

So $\epsilon_j \cdot \epsilon_{j+3}$ is conjugate to $\gamma_j \cdot \gamma_{j+3}$ and so by Theorem 4.1 they have the same cycle structure. More importantly the cycle structure does not depend on the plug board τ.

Hence, if we can use the cycle structure to determine the rotor settings then we are only left with determining the plugboard settings. If we can determine the rotor settings then we know the values of γ_j, for $j = 1, \ldots, 6$, from the encrypted message keys we can compute ϵ_j for $j = 1, \ldots, 6$ as in the previous section. Hence, determining the plugboard settings is then a question of solving one of our conjugacy problems again, for τ. But this is easier than before as we have that τ must be a product of disjoint transpositions.

We have already discussed how to compute $\epsilon_j \cdot \epsilon_{j+3}$ from the encryption of the message keys. Hence, we simply compute these values and compare their cycle structures with those obtained by running through all possible

$$60 \cdot 26^3 \cdot 26^3 = 18,534,946,560$$

choices for the rotors, positions and ring settings. Note, that when this was done by the Poles in the 1930's there was only a choice of the ordering of three rotors. The extra choice of rotors did not come in till a bit later. Hence, the total choice was 10 times less than this figure.

The above simplifies further if we assume that no stepping of the second and third rotor occurs during the calculation of the first six ciphertext characters. Recall this happens around 77 percent of the time. In such a situation the cycle structure depends only on the rotor order and the difference $p_i - r_i$ between the starting rotor position and the ring setting. Hence, we might as well assume that $r_1 = r_2 = r_3 = 0$ when computing all of the cycle structures. So, for 77 percent of the days our search amongst the cycle structures is then only among

$$60 \cdot 26^3 = 1,054,560 \text{ (resp. } 105,456)$$

possible cycle structures.

After the above procedure we have determined all values of the initial day setting bar p_i and r_i, however we know the differences $p_i - r_i$. We also know for any given message the message key p'_1, p'_2, p'_3. Hence, in breaking the actual message we only require the solution for r_1, r_2, the value for r_3 is irrelevant as the third rotor never moves a fourth rotor. Most German messages started with the same two letter word followed by space (space was encoded by 'X'). Hence, we only need to go through 26^2 different positions to get the correct ring setting. Actually one goes through 26^2 wheel positions with a fixed ring, and use the differences to infer the actual ring settings.

Once, r_i is determined from one message the value of p_i can be determined for the day key and then all messages can be trivially broken. Another variant here, if a suitable piece of known plaintext can be deduced, is to apply the technique from Section 3.2.1 with the obvious modification to deduce the ring settings as well.

7. The Germans Make It Harder

In Sept 1938 the German's altered the way that day and message keys were used. Now a day key consisted of a rotor order, the ring settings and the plugboard. But the rotor positions were not part of the day key. A cipher operator would now choose their own initial rotor positions, say AXE and their own message rotor positions, say GPI. The operator would put their machine in the AXE setting and then encrypt GPI twice as before, to obtain say $POWKNP$. The rotors would then be placed in the GPI position and the message would be encrypted. The message header would be $AXEPOWKNP$.

This procedure makes the analysis of the previous section useless. As each message would now have its own "day" rotor position setting, and so one could not collect data from many messages so as to recover $\epsilon_0 \cdot \epsilon_3$ etc, as in the previous section.

What was needed was a new way of characterising the rotor positions. The way invented by Zygalski was to use so-called "females". In the six letters of the enciphered message key a female is the occurance of the same letter in the same position in the string of three. For example, the header $POWKNP$ contains no females, but the header $POWPNL$ contains one female in position zero, i.e. the repeated values of P, seperated by three positions.

Let us see what is implied by the existence of such females: Firstly suppose we receive $POWPNL$ as above and suppose the unknown first key setting is x. Then we have that, if ϵ_i represents the Enigma setting in the ground setting,

$$x^{\epsilon_0} = x^{\epsilon_3} = P.$$

In other words

$$P^{\epsilon_0 \cdot \epsilon_3} = x^{\epsilon_0 \cdot \epsilon_0 \cdot \epsilon_3} = x^{\epsilon_3} = P.$$

In other words P is a fixed point of the permutation $\epsilon_0 \cdot \epsilon_3$.

Since the number of fixed points is a feature of the cycle structure and the cycle structure is invariant under conjugation, we see that the number of fixed points of $\epsilon_0 \cdot \epsilon_3$ is the same irrespective of the plugboard setting.

The use of such females was made easier by so-called Zygalski sheets. The following precomputation was performed, for each rotor order. An Enigma machine was set up with rings in position AAA and then, for each position A to Z of the third (leftmost rotor) a sheet was created. This sheet was a table of 51 by 51 squares, consisting of the letters of the alphabet repeated twice in each direction minus one row and column. A square was removed if the Enigma machine with first and second rotor with that row/column position had a fixed point in the permutation $\epsilon_0 \cdot \epsilon_3$. So for each rotor order there was a set of 26 sheets.

Note, we are going to use the sheets to compute the day ring setting, but they are computed using different rotor positions but with a fixed ring setting. This is because it is easier with an Enigma machine to actually rotate the rotor positions than the rings, then converting between ring and rotor settings is simple.

In fact, it makes sense to also produce a set of sheets for the permutation $\epsilon_1 \cdot \epsilon_4$ and $\epsilon_2 \cdot \epsilon_5$, as without these the number of keys found by the following method is quite large. Hence, for each rotor order we will have 26×3 perforated sheets. The Poles used the following method when only 3 rotors where used, extending it to 5 rotors is simple but was time consuming at the time.

To see how the sheets are used we now proceed with an example. Suppose a set of message headers are received in one day. From these we keep all those which possesses a female in the part corresponding to the encryption of the message key. For example we obtain the following message headers,

HUXTBPGNP	DYRHFLGFS	XTMRSZRCX	YGZVQWZQH
BILJWWRRW	QYRZXOZJV	SZYJPFBPY	MWIBUMWRM
YXMHCUHHR	FUGWINCIA	BNAXGHFGG	TLCXYUXYC

RELCOYXOF	XNEDLLDHK	MWCQOPQVN	AMQCZQCTR
MIPVRYVCR	MQYVVPVKA	TQNJSSIQS	KHMCKKCIL
LQUXIBFIV	NXRZNYXNV	AMUIXVVFV	UROVRUAWU
DSJVDFVTT	HOMFCSQCM	ZSCTTETBH	SJECXKCFN
UPWMQJMSA	CQJEHOVBO	VELVUOVDC	TXGHFDJFZ
DKQKFEJVE	SHBOGIOQQ	QWMUKBUVG	

Now assuming a given rotor order, say the rightmost rotor is rotor I, the middle one rotor II and the leftmost rotor is III, we remove all those headers which could have had a stepping action of the middle rotor in the first six encryptions. To compute these we take third character of the above message headers, i.e. the position p_1 of the rightmost rotor in the encryption of the message key, and the position of the notch on the rightmost rotor assuming the rightmost rotor is I, i.e. $n_1 = 16 \leftarrow' Q'$. We compute the value of m_1 from the Section 2

$$m_1 = n_1 - p_1 - 1 \pmod{26}.$$

and remove all those for which

$$\lfloor (j - m_1 + 26)/26 \rfloor \neq 0 \text{ for } j = 0, 1, 2, 3, 4, 5.$$

This leaves us with the following message headers

HUXTBPGNP	DYRHFLGFS	YGZVQWZQH	QYRZXOZJV
SZYJPFBPY	MWIBUMWRM	FUGWINCIA	BNAXGHFGG
TLCXYUXYC	XNEDLLDHK	MWCQOPQVN	AMQCZQCTR
MQYVVPVKA	LQUXIBFIV	NXRZNYXNV	AMUIXVVFV
DSJVDFVTT	ZSCTTETBH	SJECXKCFN	UPWMQJMSA
CQJEHOVBO	TXGHFDJFZ	DKQKFEJVE	SHBOGIOQQ

We now consider each of the three sets of females in turn. For ease of discussion we only consider those corresponding to $\epsilon_0 \cdot \epsilon_3$. We therefore only examine those message headers which have the same letter in the fourth and seventh positions, i.e.

QYRZXOZJV	TLCXYUXYC	XNEDLLDHK	MWCQOPQVN
AMQCZQCTR	MQYVVPVKA	DSJVDFVTT	ZSCTTETBH
SJECXKCFN	UPWMQJMSA	SHBOGIOQQ	

We now perform the following operation, for each letter P_3. We take the Zygalski sheet for rotor order III, II, I and permutation $\epsilon_0 \cdot \epsilon_3$ and letter P_3 and we place this down on the Table. We think of this sheet first sheet as corresponding to the ring setting

$$r_3 = Q - Q = A,$$

where the Q comes from the first letter in the first message header. Each row r and column c of the first sheet corresponds to the ring setting

$$\begin{aligned} r_1 &= R - r, \\ r_2 &= Y - c. \end{aligned}$$

We now take repeat the following process for each message header with a first letter which we have not yet met before. We take the first letter of the next message header, in this case T and we take the sheet with label

$$P_3 + T - Q.$$

This sheet then has to be placed on top of the other sheets at a certain offset to the original sheet. This offset is computed by taking the top left most square of the new sheet should be placed on top of the square (r, c) of the first sheet given by

$$\begin{aligned} r &= R - C, \\ c &= Y - L, \end{aligned}$$

i.e. we take the difference between the third (resp. second) letter of the new message header and the third (resp. second) letter of the first message header.

This process is repeated until all of the given message headers are used up. Any square which is now clear on all sheets then gives a possible setting for the rings for that day. The actual setting being read off the first sheet using the correspondence above.

This process will give a relatively large number of possible ring settings for each possible rotor order. However, when we intersect the possible values obtained from considering the females in the 0/3 position, with those in the 1/4 and the 2/5 position we find that the number of possibilities shrinks dramatically. Often this allows us to uniquely determine the rotor order and ring setting for the day.

We determine in our example that the rotor order is given by III, II and I, with ring settings given by $r_1 = A$, $r_2 = B$ and $r_3 = C$.

To determine the plugboard settings for the day we can either use a piece of known plaintext as before. However, if no such text is available we can use the females to help drastically reduce the number of possibilities for the plugboard settings.

8. Known Plaintext Attack And The Bombe's

Turing (among others) wanted a technique to break Enigma which did not really on the way the German's used the system, which could and did change. Turing settled on a known plaintext attack, using what was known at the time as a "crib". A crib was a piece of plaintext which was suspected to lie in the given piece of ciphertext.

The methodology of this technique was to from a given piece of ciphertext and a suspected piece of corresponding plaintext to first deduce a so-called "menu". A menu is simply a graph which represents the various relationships between ciphertext and plaintext letters. Then the menu was used to program a electrical device called a Bombe. A Bombe was a device which enumerated the Enigma wheel positions and, given the data in the menu, deduced the possible settings for the rotor orders, wheel positions and some of the plugboard. Finally, the ring positions and the remaining parts of the plugboard needed to be found.

In the following we present a version of this technique which we have deduced from various sources. We follow a running example through so as to explain the method in more detail.

8.1. From Ciphertext to a Menu. Suppose we receive the following ciphertext

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
```

and suppose we know, for example because we suspect it to be a shipping forecast, that the ciphertext encrypts at some point the plaintext

```
DOGGERFISHERGERMANBIGHTEAST
```

Now we know that in the Enigma machine that a letter cannot decrypt to itself. This means that there are only a few positions for which the plaintext will align correctly with the ciphertext. Suppose we had the following alignment

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
-DOGGERFISHERGERMANBIGHTEAST---------------
```

then we see that this is impossible since the S in the plaintext `FISHER` cannot correspond to the S in the ciphertext. Continuing in this way we find that there are only six possible alignments of the plaintext fragment with the ciphertext:

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DOGGERFISHERGERMANBIGHTEAST----------------
---DOGGERFISHERGERMANBIGHTEAST-------------
-----DOGGERFISHERGERMANBIGHTEAST-----------
--------DOGGERFISHERGERMANBIGHTEAST--------
```

```
----------DOGGERFISHERGERMANBIGHTEAST------
---------------DOGGERFISHERGERMANBIGHTEAST
```

In the following we will focus on the first alignment, i.e. we will assume that the first ciphertext letter H decrypts to D and so on. In practice the correct alignment out of all the possible ones would need to be deduced by skill, judgement and experience. However, in any given day a number of such cribs would be obtained and so only the most likely ones would be accepted for use in the following procedure.

As is usual with all our techniques there is a problem if the middle rotor turns over in the part of the ciphertext which we are considering. Our piece of chosen plaintext is 26 letters long, so we could treat it in two sections each of 13 letters. The advantage of this is that we know the middle rotor will only advance once every 26 turns of the fast rotor. Hence, by selecting two groups of 13 letters we can obtain two possible alignments which we know one of which does not contain a middle rotor movement.

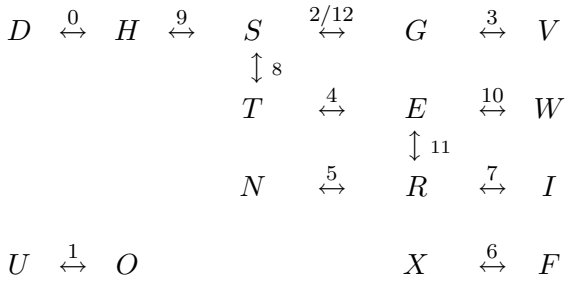
We therefore concentrate on the following two alignments:

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DOGGERFISHERG-----------------------------
-------------ERMANBIGHTEAS-----------------
```

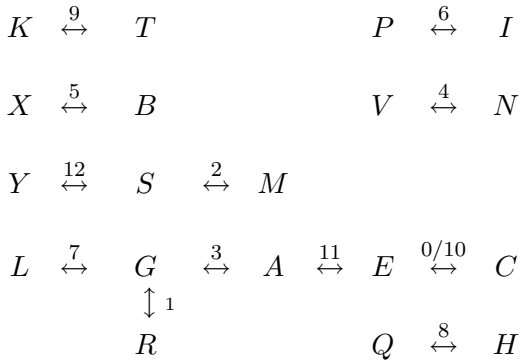
We now deal with each alignment in turn and examine the various pairs of letters. We note that if H encrypts to D in the first position then D will encrypt to H in the same Enigma configuration. We make a record of the letters and the positions for which one letter encrypts to the other. These are placed in a graph with vertices being the letters and edges being labelled by the positions of the related encryptions.

This results in the following two graphs (or menus)

Menu 1:



Menu 2:



These menu's tell us a lot about the configuration of the Enigma machine, in terms of its underlying permutations. Each menu is then used to program a Bombe. In fact we program one

Bombe not only for each menu, but also for each possible rotor order. Thus if five rotor orders are in use, we need to program $2 \cdot 60 = 120$ such Bombe's.

8.2. The Turing/Welchmann Bombe. There are many descriptions of the Bombe as an electrical circuit. In the following we present the basic workings of the Bombe in terms of a modern computer, note however that this is in practice not very efficient. The Bombe's electrical circuit was able to execute the basic operations at the speed of light, (i.e. the time it takes for a current to pass around a circuit), hence simulating this with a modern computer is therefore very inefficient.

I have found the best way to think of the Bombe is as a computer with 26 registers each of which are 26 bits in length. In a single "step" of the Bombe a single bit in this register bank is set. Say we set bit F of register H, this corresponds to us wishing to test whether F is plugged to H in the actual Enigma configuration. The Bombe then passes through a series of states until it stabilises, in the actual Bombe this occurs at the speed of light, in a modern computer simulation this needs to be actually programmed and so occurs at the speed of a computer. Once the register bank stabilises, each set bit is means that if the tested condition is true then so must this condition be true, i.e. if bit J of register K is set then J should be plugged to K in the Enigma machine. In other words the Bombe deduces a "Theorem" of the form

$$\text{If } F \to H \text{ Then } K \to J.$$

With this interpretation the diagonal board described in descriptions of the Bombe is then the obvious condition that if K is plugged to J, then J is plugged to K, i.e. if bit J of register K is set, then so must bit K of register J. In the real Bombe this is achieved by use of wires, however in a computer simulation it means that we always set the "transpose" bit when setting any bit in our register bank. Thus, the register bank is symmetric down the leading diagonal. The diagonal board, which was Welchmann's contribution to basic design of Turing, drastically increases the usefulness of the Bombe in breaking arbitrary cribs.

To understand how the menu acts on the set of registers we define the following permutation for $0 \leq i < 26^3$, for a given choice of rotors ρ_1, ρ_2 and ρ_3 We write $i = i_1 + i_2 \cdot 26 + i_3 \cdot 26^2$, and define

$$\begin{aligned}\delta_{i,s} &= (\sigma^{i_1+s+1}\rho_1\sigma^{-i_1-s-1}) \cdot (\sigma^{i_2}\rho_2\sigma^{-i_2}) \cdot (\sigma^{i_3}\rho_3\sigma^{-i_3}) \cdot \varrho \cdot \\ &\quad \cdot (\sigma^{i_3}{\rho_3}^{-1}\sigma^{-i_3}) \cdot (\sigma^{i_2}{\rho_2}^{-1}\sigma^{-i_2}) \cdot (\sigma^{i_1+s+1}{\rho_1}^{-1}\sigma^{-i_1-s-1}).\end{aligned}$$

Note, how similar this is to the equation of the Enigma machine. The main difference is that the second and third rotor's cycle through at a different rate (depending only on i). The variable i is used to denote the rotor position which we wish to currently test and the variable s is used to denote the action of the menu, as we shall now describe.

The menu acts on the registers as follows: For each link $x \xrightarrow{s} y$ in the menu we take register x and for each set bit x_z we apply $\delta_{i,s}$ to obtain x_w. Then bit x_w is set in register y (and due to the diagonal board) bit y is set in register x_w. Also we need to apply the link backwords, so for each set bit y_z in register y we apply $\delta_{i,s}$ to obtain y_w. Then bit y_w is set in register x (and due to the diagonal board) bit x is set in register y_w.

We now let l denote the letter which satisfies at least one of the following, and hopefully all three

(1) A letter which occurs more often than any other letter in the menu.
(2) A letter which occurs in more cycles than any other letter.
(3) A letter which occurs in the largest connected component of the graph of the menu.

In the above two menus we have a number to choose from in Menu 1, so we select $l = S$, in Menu 2 we select $l = E$. For each value of i we then perform the following operation

- Unset all bits in the registers.
- Set bit l of register l.

- Keep applying the menu, as above, until the registers no longer change at all.

Hence, the above algorithm is working out the consequences of the letter l being plugged to itself, given the choice of rotors ρ_1, ρ_2 and ρ_3. It is the third line in the above algorithm which operates at the speed of light in the real Bombe, in a modern simulation this takes a lot longer.

After the the registers converge to a steady state we then test them to see if a possible value of i, i.e. a possible value of the rotor positions has been found. We then step i on by one, which in the real Bombe is achieved by rotating the rotors, and repeat. A value of i which corresponds to a valid value of i is called a "Bombe Stop".

To see what is a valid value of i, suppose we have the rotors in the correct positions. If the plugboard hypothesis, that the letter l is plugged to itself, is true then the registers will converge to a state which gives the plugboard settings for the registers in the graph of the menu which are connected to the letter l. If however the plugboard hypothesis is wrong then the registers will converge to a different state, in particular the bit of each register which corresponds to the correct plugboard configuration will never be set. The best we can then expect is that this wrong hypothesis propagates and all registers in the connected component become set with 25 bits, the one remaining unset bit then corresponds to the correct plugboard setting for the letter l. If the rotor position is wrong then it is highly likely that all the bits in the test register l converge to the set position.

To summarize we have the following situation upon convergence of the registers at step i.

- All 26 bits of test register l are set. This implies that the rotors are not in the correct position and we can step on i by one and repeat the whole process.
- One bit of test register l is set, the rest being unset. This is a possible correct configuration for the rotors. If this is indeed the correct configuration then in addition the set bit corresponds to the correct plug setting for register l, and the single bit set in the registers corresponding to the letters connected to l in the menu will give us the plug settings for those letters as well.
- One bit of the test register l is unset, the rest being set. This is also a possible correct configuration for the rotors. If this is indeed the correct configuration then in addition the unset bit corresponds to the correct plug setting for register l, and any single unset set in the registers corresponding to the letters connected to l in the menu will give us the plug settings for those letters as well.
- The number of set bits in register l lies in $[2, \ldots, 24]$. These are relatively rare occurances, and although they could correspond to actual rotor settings they tell us little directly about the plug settings. For "good" menu's we find they are very rare indeed.

A Bombe stop is a position where the machine decides one has a possible correct configuration of the rotors. The number of such stops per rotor order depends on structure of the graph of the menu. Turing determined the expected number of stops for different types of menus. The following table shows the expected number of stops per rotor order for a connected menu (i.e. only one component) with various numbers of letters and cycles.

	Number of Letters								
Cycles	8	9	10	11	12	13	14	15	16
3	2.2	1.1	0.42	0.14	0.04	≈ 0	≈ 0	≈ 0	≈ 0
2	58	28	11	3.8	1.2	0.3	0.06	≈ 0	≈ 0
1	1500	720	280	100	31	7.7	1.6	0.28	0.04
0	40000	19000	7300	2700	820	200	43	7.3	1.0

This gives an upper bound on the number of stops for an unconnected menu in terms of the the size of the largest connected component and the number of cycles within the largest connected component.

Hence, a good menu is not only one which has a large connected component but which also has a number of cycles. Our second example menu is particularly poor in this respect. Note, that a large number of letters in the connected component not only reduces the expected number of Bombe stops but also increases the number of deductions about possible plugboard configurations.

8.3. Bombe Stop to Plugboard. We now need to work out how from a Bombe stop we can either deduce the actual key, or deduce that the stop has occurred simply by chance and does not correspond to a correct configuration. We first sum up how many stops there are in our example above. For each menu we specify, in the following table, the number of Bombe stops which arise and we also specify the number of bits in the test register l which gave rise to the stop.

	Number of Bits Set									
Menu	1	2	3	4	5-20	21	22	23	24	25
1	137	0	0	0	0	0	0	0	9	1551
2	2606	148	9	2	0	2	7	122	2024	29142

Here we can see the effect of the difference in size of the largest connected component. In both menus the largest connected component has a single cycle in it. For the first menu we obtain a total of 1697 stops, or 28.3 stops per rotor order. The connected component has eleven letters in it, so this yield is much better than the yield expected from the above table. This is due to the extra two letter component in the graph of menu one. For menu two we obtain a total of 34062 stops, or 567.7 stops per rotor order. The connected component in the second menu has six letters in it, so although this figure is bad it is in fact better than the maximum expected from the above table, again this is due to the presence of other components in the graph.

With this large number of stops we need a way of automating the further checking. It turns out that this is relatively simple as the state of the registers allow other conditions to be checked automatically. Apparently in more advanced versions of the Bombe the following checks were performed automatically without the Bombe actually stopping

Recall the Bombe stop gives us information about the state of the supposed plugboard. The following are so-called "legal contradictions", which can be eliminated instantly from the above stops.

- If any Bombe register has 26 bits set then this Bombe configuration is impossible.
- If the Bombe registers imply that a letter is plugged to two different letters then this is clearly a contradiction.

Suppose we know that the plugboard has uses a certain number of plugs (in our example this number is ten) then if the registers imply that there are more than this number of plugs then this is also a contradiction.

Applying these conditions mean we are down to only 19750 possible Bombe stops out of the 35759 total stops above. Of these 109 correspond to the first menu and the rest correspond to the second menu.

We clearly cannot cope with all of those corresponding to the second menu so lets suppose that the second rotor does not turn over in the first thirteen characters. This means we now only need to focus on the first menu.

In practice a number of configurations could be eliminated due to operational requirements set by the Germans (e.g. not using the same rotor orders on consecutive days).

8.4. Finding the final part of the key. We will focus on the first two remaining stops. Both of these correspond to rotor order where the rightmost (fastest) rotor is rotor I, the middle one is rotor II and the leftmost rotor is rotor III.

The first remaining stop is at Bombe configuration $i_1 = p_1 - r_1 = Y$, $i_2 = p_2 - r_2 = W$ and $i_3 = p_3 - r_3 = K$. These follow from the following final register state in this configuration, where rows represent registers and columns the bits

```
 ABCDEFGHIJKLMNOPQRSTUVWXYZ
A00011011100001000111011000
B00011011100001100111111000
C00001111100001000111011100
D11011111111111111111111111
E11111111011111111111111111
F00111111100110000111011110
G11111101111111111111111111
H11111111101111111111111111
I11110111111111111111111111
J00011010100001100111111000
K00011011100001100111111000
L00011111100001100101111000
M00011111100001000011111000
N11111011111111111111111111
O01011011111101001111101111
P00011011100001000111011000
Q00011011100001100111111000
R11111111111101111111111111
S11111111111011111111111111
T11111111111111111111111110
U01011011111111101111010011
V11111111111111011111111111
W11111111111111111111011111
X00111111100001100111011110
Y00011111100001100111111100
Z00011011100001100110111000
```

The test register has 25 bits set, so in this configuration each bit implies that a letter is not plugged to another letter. The plugboard setting is deduced to contain the following plugs

$$C \leftrightarrow D,\ E \leftrightarrow I,\ F \leftrightarrow N,\ H \leftrightarrow J,\ L \leftrightarrow S,$$

$$M \leftrightarrow R,\ O \leftrightarrow V,\ T \leftrightarrow Z,\ U \leftrightarrow W,$$

whilst the letter G is known to be plugged to itself, assuming this is the correct configuration.

So we need to find one other plug and the ring settings. We can assume that $r_3 = 0 = A$ as it plays no part in the actual decryption process. Since we are using the rotor I as the rightmost rotor we know that $n_1 = 16 \leftarrow Q$, which combined with the fact that we are assuming that no stepping occurs in the first thirteen characters implies that p_1 must satisfy

$$j - ((16 - p_1 - 1) \pmod{26}) + 26 \leq 25 \text{ for } j = 0, \ldots, 12.$$

i.e. $p_1 = 0, 1, 2, 16, 17, 18, 19, 20, 21, 22, 23, 24$ or 25.

With the Enigma setting of $p_1 = Y$, $p_2 = W$, $p_3 = K$ and $r_1 = r_2 = r_3 = A$ and the above (incomplete) plugboard we decrypt the fragment of ciphertext and compare the resulting plaintext with the crib.

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DVGGERLISHERGMWBRXZSWNVOMQOQKLKCSQLRRHPVCAG
DOGGERFISHERGERMANBIGHTEAST----------------
```

This is very much like the supposed plaintext. Examine the first incorrect letter, the second one. This cannot be incorrect due to a second rotor turnover, due to our assumption, hence it must be incorrect due to a missing plugboard element. If we let γ_1 denote the current approximation to the

permutation representing the Enigma machine for letter one and τ the missing plugboard setting then we have

$$U^{\gamma_1} = V \text{ and } U^{\tau\cdot\gamma_1\cdot\tau} = O.$$

This implies that τ should contain either a plug involving the letter U or the letter O, but both of these letters are already used in the plugboard output from the Bombe. Hence, this configuration must be incorrect.

The second remaining stop is at Bombe configuration $i_1 = p_1 - r_1 = R$, $i_2 = p_2 - r_2 = D$ and $i_3 = p_3 - r_3 = L$. The plugboard setting is deduced to contain the following plugs

$$D \leftrightarrow Q,\ E \leftrightarrow T,\ F \leftrightarrow N,\ I \leftrightarrow O,\ S \leftrightarrow V,\ W \leftrightarrow X,$$

whilst the letters G, H and R are known to be plugged to themselves, assuming this is the correct configuration. These follow from the following final register state in this configuration,

```
 ABCDEFGHIJKLMNOPQRSTUVWXYZ
A00011011100001000111011000
B00011111100001000111011100
C00011111100001000111011000
D11111111111111110111111111
E11111111111111111110111111
F01111011100000100111111110
G11111101111111111111111111
H11111110111111111111111111
I11111111111111011111111111
J00011011100001000111011100
K00011011100001000111011000
L00011011100001100111111000
M00011011100001100111111000
N11111011111111111111111111
O00001111100011111011111001
P00011011100001100111111000
Q00001011100001000111011100
R11111111111111111011111111
S11111111111111111111101111
T11110111111111111111111111
U00011111100111110111011001
V11111111111111111101111111
W11111111111111111111111011
X01011111110001001111010110
Y00011111100001000111011100
Z00011011100001100111111000
```

So we need to find four other plug settings and the ring settings.

Again we can assume that $r_3 = A$ as it plays no part in the actual decryption process, and again we deduce that p_1 must be one of $0, 1, 2, 16, 17, 18, 19,\ 20, 21, 22, 23, 24$ or 25.

With the Enigma setting of $p_1 = R$, $p_2 = D$, $p_3 = L$ and $r_1 = r_2 = r_3 = A$ and the above (incomplete) plugboard we decrypt the fragment of ciphertext and compare the resulting plaintext with the crib.

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DOGGERFISHERGNRAMNCOXHXZMORIKOEDEYWEFEYMSDQ
DOGGERFISHERGERMANBIGHTEAST----------------
```

We now look at the first incorrect letter, this is in the 14 position. Using the same notation as before, i.e. γ_j for the current approximation and τ for the missing plugs, we see that if this incorrect operation is due to a plug problem rather than a rotor turnover problem then we must have

$$C^{\tau\cdot\gamma_{13}\cdot\tau} = E.$$

Now, E already occurs on the plugboard, via $E \leftrightarrow T$, so τ must include a plug which maps C to the letter x where

$$x^{\gamma_{13}} = E.$$

But we can compute that

$$\gamma_{13} = (AM)(BE)(CN)(DO)(FI)(GS)(HX)(JU)(KP)(LQ)(RV)(TY)(WZ),$$

from which we deduce that $x = B$. So we include the plug $C \leftrightarrow B$ in our new approximation and repeat to obtain the plaintext

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DOGGERFISHERGERAMNBOXHXNMORIKOEMEYWEFEYMSDQ
DOGGERFISHERGERMANBIGHTEAST----------------
```

We then see in the 16th position that we either need to step the rotor or there should be a plug which means that S maps to M under the cipher. We have, for our new γ_{15} that

$$\gamma_{15} = (AS)(BJ)(CY)(DK)(EX)(FW)(GI)(HU)(LM)(NQ)(OP)(RV)(TZ).$$

The letter S already occurs in a plug, so we must have that A is plugged to M. We add this plug into our configuration and repeat

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DOGGERFISHERGERMANBOXHXNAORIKVEAEYWEFEYASDQ
DOGGERFISHERGERMANBIGHTEAST----------------
```

Now the 20th character is incorrect, we need that P should map to I and not O under the cipher in this position. Again assuming this is due to a missing plug we find that

$$\gamma_{19} = (AH)(BM)(CF)(DY)(EV)(GX)(IK)(JR)(LS)(NT)(OP)(QW)(UZ).$$

There is already a plug involving the letter I so we deduce that the missing plug should be $K \leftrightarrow P$. Again we add this new plug into our configuration and repeat to obtain

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DOGGERFISHERGERMANBIXHJNAORIPVXAEYWEFEYASDQ
DOGGERFISHERGERMANBIGHTEAST----------------
```

Now the 21st character is wrong as we must have that L should map to G. We know G is plugged to itself, from the Bombe stop configuration and given

$$\gamma_{20} = (AI)(BJ)(CW)(DE)(FK)(GZ)(HU)(LX)(MQ)(NT)(OV)(PY)(RS),$$

we deduce that if this error is due to a plug we must have that L is plugged to Z. We add this final plug into our configuration and find that we obtain

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DOGGERFISHERGERMANBIGHJNAORIPVXAEYWEFEYAQDQ
DOGGERFISHERGERMANBIGHTEAST----------------
```

All the additional plugs we have added have been on the assumption that no rotor turnover has yet occurred. Any further errors must be due to rotor turnover, as we now have a full set of plugs (as we know our configuration only has ten plugs in use). If when correcting the rotor turnover we still do not decrypt correctly we need to backup and repeat the process.

We see that the next error occurs in position 23. This means that a rotor turnover must have occurred just before this letter was encrypted, in other words we have

$$22 - ((16 - p_1 - 1) \pmod{26}) + 26 = 26.$$

This implies that $p_1 = 19$, i.e. $p_1 = T$, which implies that $r_1 = C$. We now try to decrypt again, and we obtain

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DOGGERFISHERGERMANBIGHTZWORIPVXAEYWEFEYAQDQ
DOGGERFISHERGERMANBIGHTEAST----------------
```

But we still do not have correct plaintext. The only thing which could have happened is that we have had an incorrect third rotor movement. Rotor II has its notch in position $n_2 = 4 \leftarrow E$. If the third rotor moved on at position 24 then we have, in our earlier notation

$$\begin{aligned} m_1 &= n_1 - p_1 - 1 \pmod{26} = 16 - 19 - 1 \pmod{26} = 22, \\ m &= n_2 - p_2 - 1 \pmod{26} = 4 - p_2 - 1 \pmod{26}, \\ m_2 &= m_1 + 1 + 26 \cdot m = 23 + 26 \cdot m \\ 650 &= 23 - m_2 + 650 \end{aligned}$$

This last equation implies that $m_2 = 23$, which implies that $m = 0$, which itself implies that $p_2 = 3$, i.e. $p_2 = D$. But this is exactly the setting we have for the second rotor. So the problem is not that the third rotor advances, it is that it should not have advanced. We therefore need to change this to say $p_2 = E$ and $r_2 = B$, (although this is probably incorrect it will help us to decrypt the fragment). We find that we then obtain

```
HUSVTNXRTSWESCGSGVXPLQKCEYUHYMPBNUITUIHNZRS
DOGGERFISHERGERMANBIGHTEASTFORCEFIVEFALLING
DOGGERFISHERGERMANBIGHTEAST----------------
```

Hence, we can conclude, apart from a possible incorrect setting for the second ring we have the correct Enigma setting for this day.

9. Ciphertext Only Attack

The following attack allows one to break the Enigma machine when only a single ciphertext is given. The method relies on the fact that enough ciphertext is given and that a not a full set of plugs is used. Suppose we have a reasonably large amount of ciphertext, say 500 odd characters, and that p plugs are in use. Suppose in addition that we could determine the rotor settings. This would mean that around $((26 - 2p)/26)^2$ of the letters would decrypt exactly, as the letters would neither pass through a plug either before or after the rotor stage. Hence, one could distinguish the correct rotor positions by using some statistic to distinguish a random plaintext from a plaintext in which $((26 - 2p)/26)^2$ of the letters are correct.

Gillogly suggests using the index of Coincidence. To use this statistic we compute the frequency f_i of each letter in the resulting plaintext of length n and compute

$$IC = \sum_{i=A}^{Z} \frac{f_i(f_i - 1)}{n(n-1)}.$$

To use this approach we set the rings to position A, A, A and then run through all possible rotor orders and rotor starting positions. For each setting we compute the resulting plaintext and the associated value of IC. We keep those settings which have a high value of IC.

Gillogly then suggests for the settings which give a high value of IC to run through the associated ring settings, adjusting the starting positions as necessary, with a similar test. The problem with this approach is that it is susceptible to the effect of turnover of the various rotors. Either a rotor could turn over when we did not expect it, or it could have turned over by error. This is similar to the situation we obtained in our example using the Bombe in a known plaintext attack.

Consider the following ciphtext, of 734 characters in length

RSDZANDHWQJPPKOKYANQIGTAHIKPDFHSAWXDPSXXZMMAUEVYYRLWVFFTSDYQPS
CXBLIVFDQRQDEBRAKIUVVYRVHGXUDNJTRVHKMZXPRDUEKRVYDFHXLNEMKDZEWV
OFKAOXDFDHACTVUOFLCSXAZDORGXMBVXYSJJNCYOHAVQYUVLEYJHKKTYALQOAJ
QWHYVVGLFQPTCDCAZXIZUOECCFYNRHLSTGJILZJZWNNBRBZJEEXAEATKGXMYJU
GHMCJRQUODOYMJCXBRJGRWLYRPQNABSKSVNVFGFOVPJCVTJPNFVWCFUUPTAXSR
VQDATYTTHVAWTQJPXLGBSIDWQNVHXCHEAMVWXKIUSLPXYSJDUQANWCBMZFSXWH
JGNWKIOKLOMNYDARREPGEZKCTZNPQKOMJZSQHYEADZTLUPGBAVCVNJHXQKYILX
LTHZXJKYFQEBDBQOHMXBTVXSRGMPVOGMVTEYOCQEOZUSLZDQZBCXXUXBZMZSWX
OCIWRVGLOEZWVVOQJXSFYKDQDXJZYNPGLWEEVZDOAKQOUOTUEBTCUTPYDHYRUS
AOYAVEBJVWGZHGLHBDHHRIVIAUUBHLSHNNNAZWYCCOFXNWXDLJMEFZRACAGBTG
NDIHOWFUOUHPJAHYZUGVJEYOBGZIOUNLPLNNZHFZDJCYLBKGQEWTQMXJKNYXPC
KAPJGAGKWUCLGTFKYFASCYGTXGZXXACCNRHSXTPYLSJWIEMSABFH

We ran through all possible $60 \cdot 26^3$ possible values for the rotors and for the rotor positions, with ring settings equal to A, A, A. We obtain the following "high" values for the IC statistic.

IC	ρ_1	ρ_2	ρ_3	p_1'	p_2'	p_3'
0.04095	I	V	IV	P	R	G
0.0409017	IV	I	II	N	O	R
0.0409017	IV	V	I	M	G	Z
0.0408496	V	IV	II	I	J	B
0.040831	IV	I	V	X	D	A
0.0408087	II	I	V	E	O	J
0.040805	I	IV	III	T	Y	H
0.0407827	V	I	II	J	H	F
0.040779	III	IV	II	R	L	Q
0.0407121	II	III	V	V	C	C
0.0406824	IV	V	III	K	S	D
0.0406675	IV	II	III	H	H	D
0.04066	III	I	IV	P	L	G
0.0406526	IV	V	II	E	E	O
0.0406415	I	II	III	V	D	C
0.0406303	I	II	IV	T	C	G
0.0406266	V	IV	II	I	I	A
0.0406229	II	III	IV	K	Q	I
0.0405969	V	II	III	K	O	R
0.0405931	I	III	V	K	B	O
0.0405931	II	IV	I	K	B	Q
⋮	⋮	⋮	⋮	⋮	⋮	⋮

For the 300 or so such high values we then ran through all possible values for the rings r_1 and r_2 (note the third ring plays no part in the process) and we set the rotor starting positions to be

$$\begin{aligned} p_1 &= p_1' + r_1 + i_1, \\ p_2 &= p_2' + r_2 + i_2, \\ p_3 &= p_3' \end{aligned}$$

The addition of the r_j value is to take into account the change in ring position from A to r_j. The additional value of i_j is taken from the set $\{-1, 0, 1\}$ and is used to accommodate issues to do with rotor turnovers which our crude IC statistic is unable to pick up.

Running through all these possibilities we find the values with the highest values of IC are given by

IC	ρ_1	ρ_2	ρ_3	p_1	p_2	p_3	r_1	r_2	r_3
0.0447751	I	II	III	K	D	C	P	B	A
0.0444963	I	II	III	L	D	C	Q	B	A
0.0444406	I	II	III	J	D	C	O	B	A
0.0443848	I	II	III	K	E	D	P	B	A
0.0443588	I	II	III	K	I	D	P	F	A
0.0443551	I	II	III	K	H	D	P	E	A
0.0443476	I	II	III	K	F	D	P	C	A
0.0442807	I	II	III	L	E	D	Q	B	A
0.0442324	I	II	III	J	H	D	O	E	A
0.0442064	I	II	III	K	G	D	P	D	A
0.0441357	I	II	III	J	G	D	O	D	A
0.0441097	I	II	III	J	E	D	O	B	A
0.0441097	I	II	III	L	F	D	Q	C	A
0.0441023	I	II	III	L	C	C	Q	A	A
0.0440837	I	II	III	J	F	D	O	C	A
0.0440763	I	II	III	J	I	D	O	F	A
0.0440242	I	II	III	K	C	C	P	A	A
0.0439833	I	II	III	L	G	D	Q	D	A
0.0438904	I	II	III	L	I	D	Q	F	A
0.0438607	I	II	III	L	H	D	Q	E	A
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Finally using our previous technique for finding the plugboard settings given the rotor settings in a ciphertext only attack (using the Sinkov statistic) we determine that the actual settings are

ρ_1	ρ_2	ρ_3	p_1	p_2	p_3	r_1	r_2	r_3
I	II	III	L	D	C	Q	B	A

with plugboard given by eight plugs which are

$$A \leftrightarrow B,\ C \leftrightarrow D,\ E \leftrightarrow F,\ G \leftrightarrow H,$$

$$I \leftrightarrow J,\ K \leftrightarrow L,\ M \leftrightarrow N,\ O \leftrightarrow P.$$

With these settings one finds that the plaintext is the first two paragraphs of “A Tale of Two Cities”.

Chapter Summary

- We have described the Enigma machine and shown how poor session key agreement was used to break into the German traffic.
- We have also seen how stereotypical messages were also used to attack the system.
- We have seen how the plugboard and the rotors worked independently of each other, which led to attackers being able to break each component seperately.

Further Reading

The paper by Rejweski presents the work of the Polish cryptographers very clearly. The pure ciphertext only attack is presented in the papers by Gillogly and Williams. There are a number of excellent sites on the internet which go into various details, of particular note are Tony Sale's web site and the Bletchley Park site.

J. Gillogly. *Ciphertext-only cryptanalysis of Enigma*. Cryptologia, **14**, 1995.

M. Rejewski. *An application of the theory of permutations in breaking the Enigma cipher*. Applicationes Mathematicae, **16**, 1980.

H. Williams. *Applying statistical language recognition techniques in the ciphertext-only cryptanalysis of Enigma*. Cryptologia, **24**, 2000.

Bletchley Park Web Site. `http://www.bletchleypark.org.uk/`.

Tony Sale's Web Site. `http://www.codesandciphers.org.uk/`.