Åbo Akademi

FAKULTETSOMRÅDET FÖR
NATURVETENSKAPER OCH TEKNIK

Pro Gradu

Marian Rejewski och tyska Enigma

Skribent:

Christian Enlund

Handledare:

Mikael Lindström

September 2018

Förord

Arbetet med avhandlingen började under sommaren 2018, när jag och min professor funderade på möjliga arbetsrubriker. Jag nämnde att talteori och kryptering är intressant och snabbt därefter hade vi landat på att skriva om Enigma under andra världskriget.

Under arbetets gång har jag fått bekanta mig med en sida av andra världskriget som inte tas upp ofta och därmed har jag fått en bättre överblick av polackernas insatser och vad som hände med informationskrigsföringen före och under kriget.

Arbetet har involverat mycket läsande, man märker stor skillnad mellan texter skrivna av britter och personer från andra länder. Mycket av arbetet gick ut på att bena ut det sanna händelseförloppet. Även viktigt under arbetet var att återskapa polackernas arbete med Enigma för att kunna ge en bra överblick.

Jag vill tacka min professor Mikael Lindström som läst igenom och gett förslag om förbättringar för att att föra texten lättläst och sammanhängande. Jag vill även tacka de från min familj och mina vänner som varit intresserade av arbetet, läst det och gett hjälpsamma kommentarer för att texten ska vara förståelig även för icke-matematiker.

Christian Enlund

Åbo den 04.09.2018

Innehåll

Kapitel 1

Introduktion

För en del betyder Enigma att något är underligt eller svårt att förstå, och för de allierade under åren 1930-1945 var Enigma deras största utmaning. Som en stor del kanske har hört var nämligen Enigma tyskarnas krypteringsmaskin under andra världskriget (1939-1945) och åren före kriget (1928-1939). Detta arbete kommer att fokusera på tiden fram till andra världskriget, åren 1932-1939, under tiden då Tyskland långsamt började rusta upp sin militär för krig.

Enigma var den första rent mekaniska kryteringsmaskinen som använts i någon större utsträckning. Man lät tillverka och använde Enigma eftersom mekanisk kryptering tillät mera säkerhet än tidigare så kallade linjära krypteringsalgoritmer, såsom Hills chiffer, Viginére chiffer och liknande kryteringsalgoritmer som bygger på utbyte av bokstäver enligt förutbestämt mönster. Dessa kryperingsalgoritmer var dock inte särskilt säkra, och om en motståndare utnyttjade exempelvis frekvensanalys eller jämförde klartext med chiffertext, var det möjligt att lista ut hur texten var krypterad.

Enigma satte stopp för majoriteten av språkligt baserade metoder[1] och kan i viss mån anses vara början på att anställa matematiker som kodlösare, istället för lingvister. I detta arbete ska vi noggrant gå igenom Enigma, hur den fungerar, hur säker den är och slutligen hur tyskarnas oförsiktigthet, [8], gav en polsk matematiker möjlighet att bryta sig in i maskinen.

Denna polska matematiker, *Marian Rejewski*, förtjänar titeln *personen som knäckte Enigma*, och även om han ofta glöms bort, så lyfts han fram i detta arbete.

[1] Åtminstone de metoder som fanns tillgängliga på den tiden.

Kapitel 2

Enigma

Enigma är en krypterings- och dekrypteringsmaskin och en av de första maskiner som använde sig av mekaniska metoder för att överföra ett meddelande från klartext till chiffertext och tillbaka igen (i praktiken en avancerad strömkrets). Den användes flitigt av tyskarna under tiden mellan världskrigen och under andra världskriget.

Arthur Scherbius[1] uppfann Enigma år 1918 och patenterade[2] maskinen den 23 februari 1918 [9], några månader före slutet på första världskriget. Scherbius försökte sälja maskinen till olika företag som behövde eller ville kryptera interna meddelanden, och bland annat den polska krypteringsbyrån (pol. Biuro Szyfrow) köpte en Enigma [20].

> *If you have no good coding system, you are always running a considerable risk. Transmitted by cable or without wire, your correspondence will always be exposed to every spy, your letters, to being opened and copied, your intended or settled contracts, your offers and important news to every inquisitive eye. Considering this state of things, it is almost inconceivable that persons interested in those circumstances should delay securing themselves better against such things. Yet, ciphering and deciphering has been a troublesome art hitherto... Now, we can offer you our machine "Enigma". being a universal remedy for all those inconveniences.*
>
> - Enigma försäljningsbrochyr från 1920-talet [2].

Baserat på Scherbius design tillverkade tyskarna en modifierad Enigma, en så kallad

[1] Född: 1878; Tysk el-ingenjör från Frankfurt; utbildad vid Münchens tekniska universitet
[2] Patentnummer (tys. Patentschrift) Nr. 416291

militär Enigma, som var säkrare än den kommerisiella. Enigma togs i bruk av den tyska flottan år 1926 och slutligen av den tyska armén år 1928 [9]. Först när armén hade tagit den i bruk så började tyskarna skicka Enigma krypterade meddelanden [20].

2.1 Kommersiell modell

Figur 2.1: Kommersiell Enigma.

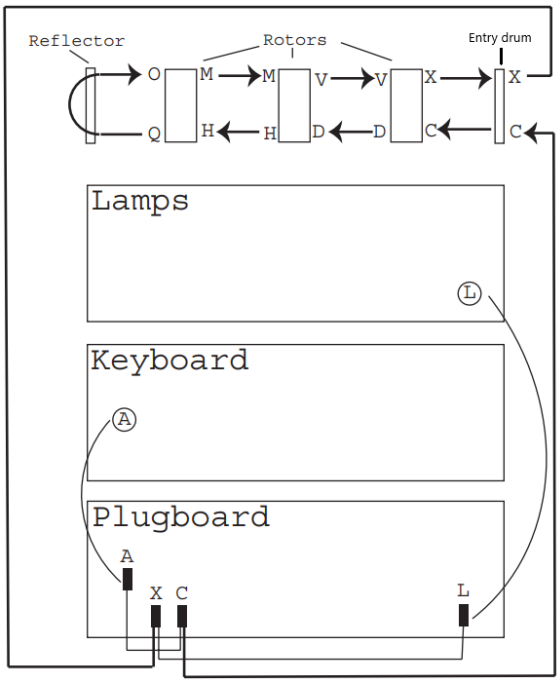
Enigma är en krypterings- och dekrypteringsmaskin, vilket betyder att det var möjligt att dekryptera ett meddelande som är krypterat av Enigma ifall man använder samma inställningar på maskinen vid kryptering och dekryptering. Till exempel krypteras $A \rightarrow X$ och $X \rightarrow A$ för en specifikt inställning på Enigma. Detta var behändigt, men även en säkerhetsrisk, bland annat för att det innebar att Enigma aldrig kunde kryptera en bokstav till sig själv. Det här betyder att utnyttjandet av en "känd klartextattack"[3] är effektivt för att knäcka krypteringen. Vi kommer att se på hur de allierade utnyttjade denna säkerhetsrisk för att ta sig in i tyskarnas kryptering.

2.1.1 Uppbyggnad

Baserat på beskrivningarna i bland annat [1], [2], [14] och [20], så ingår följande delar i Enigma:

[3]Attackeraren har kännedom om vad en klartext krypteras till, dvs. känner till chiffertexten som hör ihop med någon klartext [6], [22].

- ett tyskt QWERTZ tangentbord
- ett batteri
- en “ingångstrumma” (eng. entry drum)
- fyra rotorer (eng. rotors) (tre stycken i militära, från och med avsnitt 2.2 beaktar vi enbart den militära.)
- en reflektor
- en lamppanel.



Figur 2.2: Ett diagram över en militär Enigmas kopplingar, notera att den kommersiella versionen inte har ett “Plugboard”, kopplingsbord. Diagrammet visar strömkretsen som krypterar knapptryckningen A till chiffertexten L. Observera att detta är en militär version, den kommerisiella har inget kopplingsbord och strömmen skulle gå direkt från tangentbordet till ingångstrumman.

Rotor I Figur 2.2 är rotorerna högst upp, de tre rektanglarna. Det finns tre entydiga rotorer som används i Enigma[4], de är numrerade I, II och III och kan monteras in i maskinen i valfri ordning dock ej bak och fram. Alla tre rotorer har 26 kontakter på vänster och höger sida och inuti finns 26 isolerade sladdar som entydigt kopplar ihop kontakterna på höger sida med kontakterna på vänster

[4]Vid krigets slut hade detta tal stigit till åtta.

sida. Figur 2.4 visar hur en rotor ser ut på insidan, och komponent nummer 5 i figur 2.4 visar de isolerade sladdarna. Rotorerna var alla olika och kunde specialbeställas med en specifik koppling. Mottagaren och avsändaren måste ha exakt likadana rotorer för att kunna läsa varandras meddelanden. I grund och botten utför dessa rotorer ett bokstavsbyte eller permutation när ström går genom rotorn. Ett exempel på en rotors kopplingar kan ses i tabell 2.1:

Tabell 2.1: Exempel på hur en rotor kunde förändra en bokstav, A blir Q, B blir W osv.

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

De tre seriekopplade rotorna snurrar inte samtidigt. Den högra (snabba) rotorn, snurrar $\frac{1}{26}$ varv varje gång man trycker ner en knapp, den mellersta roterar var 26:e bokstav, dvs. när den snabba rotorn snurrat ett helt varv och den vänstra (långsamma) rotorn roterar enbart var 26:e gång den mellersta rotorn roterar, alltså var $26 \cdot 26 = 676$ knapptryckning. Vid vilken bokstav nästa rotor roterar beror på vilken rotor man använder. Alla rotorer hade sin egen "svängbokstav". I figur 2.3 ser man ett hack (eng. notch) vid 08/07. Positionen för detta hack var rotorspecifikt och när hacket passeras, kommer även nästa rotor att rotera $\frac{1}{26}$ varv.

Figur 2.3: En Enigma rotor där man ser "hacket" vid 08/07 som bestämmer när nästa rotor roterar.

Rotorerna har även en så kallad ringinställning med vilken man kan rotera

insidan av rotorn, dvs. signalen A kommer till rotorn, träffar kontakt A på höger sida, innanför är A kopplad till B, varefter strömmen går genom sladden till J som byter signalen till ett I. Denna inställning ger Enigma ytterligare säkerhet.

Siffrorna på rotorn används för att bestämma grundinställningen, och man bestämmer även ringinställningen med siffrorna. Detta möjliggör att man kan ha samma rotor- och startposition, men de inre kopplingarna är olika, och dessa inställningar varierade varje dag. I figur 2.3 ser man att när rotorn är i position 08 och man krypterar en bokstav kommer också nästa rotor att rotera. Vid varje rotation flyttas alfabetet ett steg, dvs. om tabell 2.1 hör till den snabba rotorn, så antar den efter en knapptryckning utseendet i tabell 2.2:

Tabell 2.2: Nedre raden flyttad ett steg åt vänster, jäntemot tabell 2.1

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

Tabell 2.1, den ursprungliga tabellen:

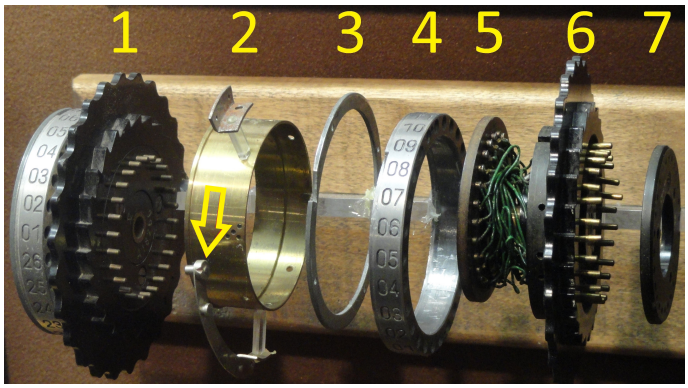
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Detta ger en period på $26 \cdot 26 \cdot 26 = 17\ 576$, dvs. först efter 17 567 knapptryckningen repeteras chiffret. Meddelanden fick vanligtvis inte överskrida 200 tecken i längd, eftersom det var enklare att utföra "känd-klartextattack" på långa meddelanden.

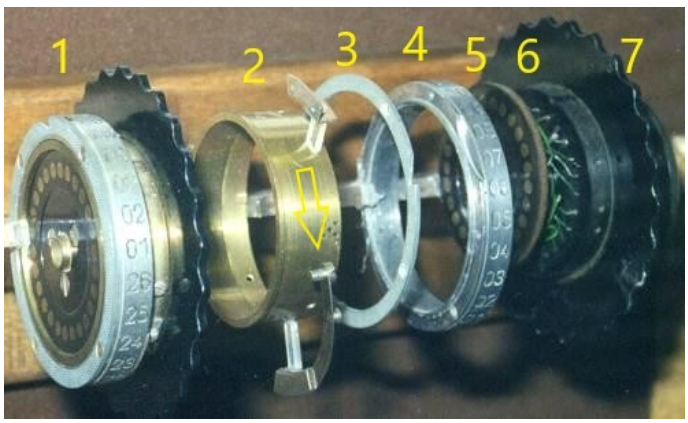
Med tre rotorer som kan sättas in i valfri ordning, fås $3! = 6$ möjliga ordningar. Man väljer sedan en grundinställning för alla tre rotorer, och denna kan väljas på 26 olika sätt för varje rotor, dvs. $26^3 = 17\ 576$ olika grundinställningar. Dessutom finns 26 möjligheter för varje rotors ringinställning, dvs. ytterligare $26^3 = 17\ 576$ möjligheter. Detta ger sammanlagt $6 \cdot 26^3 \cdot 26^3 = 1\ 853\ 494\ 656$ grundinställningar för Enigma, eller alternativt uttryck, det existerar 1 853 494 656 nycklar. För att kunna dekryptera ett Enigma meddelande måste båda parterna sätta upp sin Enigma med exakt samma nyckel. Om en spion har tillgång till enbart papper och penna är Enigma väldigt säker. Det finns dock ett antal

svagheter i Enigma, och i tyskarnas användning av Enigma, som utnyttjades av polska matematiker för att knäcka Enigmas kryptering. Se kapitel 4 för en noggrann beskrivning, men speciellt det att Enigma aldrig krypterade en bokstav till sig själv, var en stor svaghet. Antalet nycklar är dock stort nog för att avskräcka alla icke-seriösa försök att knäcka koden.

Slutligen noteras att eftersom 26 bokstäver ska kopplas ihop med varandra, ger det $26! = 403\ 291\ 461\ 126\ 605\ 635\ 584\ 000\ 000$ olika sätt att konstruera en rotor. Chansen att man råkar skapa två identiska rotorer är $\frac{1}{26!} \cdot 100\ \% \approx 2,479596 \cdot 10^{-25}\ \%$. Med andra ord fanns det en försvinnande liten chans att kryptologer skulle ha kunnat gissa sig fram till de korrekta rotorkopplingarna.



Figur 2.4: En öppnad Enigmarotor.



Figur 2.5: Samma Enigmarotor som i figur 2.4, men från andra sidan.

Förklaringar till siffrorna i figur 2.4 och figur 2.5:

1. Ihopmonterad Enigmarotor.
2. Kroppen (eng. body): strukturen för rotorn ser till att alla delar kan monteras ihop. I denna del finns även ringinställningen, med vilken man kan rotera insidan av rotorn i förhållande till utsidan. (Man kan se inställaren framför kroppen, se pilen i figur 2.4 och eventuellt tydligare i figur 2.5.)
3. Ringen med "hacket". Denna del bestämmer vid vilken siffra rotorn roterar.
4. Sifferringen, denna ring är den del som operatören ser. Med hjälp av denna ställer man in grundinställningarna, och kan även kontrollera vilken position rotorn är i. Man kan se hål på sidan, där man bestämmer ringinställningarna för rotorn.
5. Sladdarna i rotorn, dessa sladdkopplingar roterar när man ställer in ringen. Av figur 2.5 framgår att denna del har glidkontakter på vänstra sidan, dvs. den sida som vätter emot reflektorn i Enigma. Dessa sladdkopplingar är rotorspecifika.
6. Kugghjulet, med denna del är det möjligt för operatören att manuellt ställa in rotorns grundinställning, eller att annars bara rotera rotorn. Till exempel om ett misstag gjordes, så kunde man rotera tillbaka ett steg. På höger sida ser man kontakter som kopplar ihop med glidkontakterna i rotorn till höger. Detta möjliggör rotation för rotorn.
7. Skyddsdel, ingen större funktion, skyddar och isolerar kopplingarna.

Lamppanel En uppsättning lampor över vilken en panel med alla bokstäver placeras (se figur 2.1). En lampa lyser upp när man trycker på en bokstav, och lampan indikerar vilken chifferbokstav som klartextsbokstaven motsvarar. Denna skrivs sedan ner.

Tangentbord Ett gammalt skrivmaskinstangentbord. När man trycker på en knapp så roterar först den långsamma rotorn $\frac{1}{26}$ varv och eventuellt andra rotorer, **varefter** ström flyter genom kretsen och tänder en lampa. Lampan lyser upp en bokstav i lamppanelen som ger krypteringsbokstaven.

Ingångstrumma Efter att en knapp har tryckts ner och ström börjar gå i kretsen kommer strömmen först till ingångstrumman. Trumman fungerar som en ytterligare omkastare (eng. scrambler), alltså att den byter ut bokstaven som kom från tangentbordet emot en annan. Den nya bokstaven matas sedan in i rotorerna.

Reflektor Längst till vänster, efter de tre rotorerna (se figur 2.2) placeras en reflektor. Detta är en "halvrotor". Den har sladdkopplingar enbart på höger sida, och totalt kan man skapa $\frac{26!}{2^{13}\cdot 13!} = 7\ 905\ 853\ 580\ 025$ olika reflektorer. Reflektorn är kopplad så att två bostäver alltid är parvis, t.ex. blir A alltid X och X alltid A, och det finns alltså 13 kopplingar eller sladdar inne i reflektorn (till skillnad från de 26 i rotorerna).

Reflektorn roterar aldrig och är ansvarig för att ta emot signalen som kommer ifrån den tredje (långsamma) rotorn, t.ex. byter ut A mot X, och skickar sedan X tillbaka genom rotorerna. Den här gången från den vänstra till den högra rotorn. Denna parkoppling gör Enigma till en krypterings- och dekrypteringsmaskin. Om man trycker ner den bokstav som lyses upp, och har samma inställningar, så går strömmen den motsatta vägen i Enigma och lyser upp den ursprungliga bokstaven. Detta betyder att när signalen når lamppanelen har den blivit omblandad $1+3+1+3+1$ gånger (ingångstrumma, 3 rotorer, reflektor, 3 rotorer, ingångstrumma).

Notera i figur 2.8 hur reflektorn är namngiven B. Tyskarna hade först en reflektor A, men denna byttes ut under kriget till reflektor B och senare till reflektor C för att tyskarna ville försvåra de allierades dekrypteringsarbete. De allierade tvingades varje gång återskapa den nya reflektorn innan de hade möjlighet att attackera krypteringen, eftersom kopplingarna i reflektorn förändrades, och därmed Enigmas strömkrets.

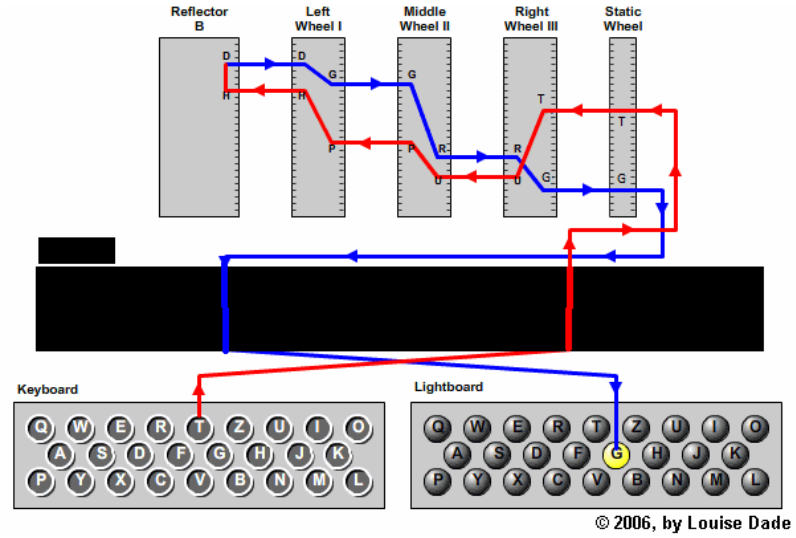
Batteri Denna komponent ger upphov till strömmen som lyser upp lamporna och gjorde Enigma enkel att flytta och därmed lämplig för arbete ute på fältet.

Enigma fungerar som en elektrisk krets: signaloperatören trycker ner en bokstav på

Enigmas tangentbord, den snabba (höger) rotorn roterar och ström passerar sedan genom kretsen och lyser upp en lampa som indikerar den krypterade bokstaven. Figurerna 2.6 och 2.2 (militär) visar kretsen.

Om man följer den vänstra linjen i figur 2.6, går den först genom ingångstrumman (Static Wheel) och sedan successivt genom de tre rotorerna. Varje gång blir signalen en annan bokstav $T \to U \to P \to H \to D$. D går in i reflektorn där D är kopplat till H. Vi återvänder sedan genom rotorerna, fast en annan väg, enligt den linje som slutar till höger vid "lightboard" $D \to G \to R \to G$. I det här fallet har ingångshjulet ingen inverkan på bokstaven[5], men ifall man vill blanda om bokstaven i ingångshjulet så är det möjligt.

Signalen kommer fram till lamppanelen och lyser upp bokstaven G, varpå signaloperatören skriver ner bokstaven och skickar meddelandet när alla bokstäver är krypterade. Notera att ifall man hade tryckt ner G istället för T, så skulle bokstaven T ha lyst upp [1].



Figur 2.6: Modell av den kommerisiella Enigmas strömkrets.

[5]Det hade den inte heller när tyskarna använde maskinen.

2.2 Militär modell

Tyskarna förbättrade Enigmas säkerhet, jämfört med den kommersiella modellen, innan den togs i bruk inom den tyska flottan och armén. De lade till ett kopplingsbord (tyska. steckerbrett, eng. plugboard), vars funktion var att blanda sex par av bostäver[6] (totalt tolv bokstäver) innan de matades in i ingångstrumman. Detta var ett tillägg som avsevärt ökade på Enigmas säkerhet, vars nyckelmängd nu steg till:

$$26^3 \cdot 26^3 \cdot 6 \cdot \frac{26!}{2^6 \cdot 6! \cdot 14!} = 186\ 075\ 649\ 051\ 516\ 224\ 000,$$

jämfört med "enbart" 1 853 494 656 möjliga kombinationer eller nycklar för den kommerisiella Enigman. Detta var en ökning med

$$\frac{186\ 075\ 649\ 051\ 516\ 224\ 000 - 1\ 853\ 494\ 656}{1\ 853\ 494\ 656} \cdot 100\ \% = 10\ 039\ 179\ 149\ 900\ \%.$$

Antalet ökade möjligheter kommer från startpositionerna för rotorerna, ordningen i vilken rotorerna är installerade, möjligheten att para ihop sex bokstäver med varandra, och dessutom måste man beakta att det finns dubletter samt bokstäver som inte blir kopplade. Denna siffra steg under kriget, när tyskarna ökade antalet sladdar på kopplingsbordet till åtta och slutligen tio, se tabell 2.3, [20], [2].

Kopplingsbord Se längst fram i figur 2.7 för att se hur kopplingsbordet ser ut. Sladdarna gavs ut i samband med Enigma och erbjöd ett ytterligare krypteringssteg. Om bokstav A är kopplad med B, så kommer Enigma tro att bokstav B tryckts ner när operatören trycker ner bokstav A, och vice versa, [2]. Se tabell 2.3 för antalet möjliga kombinationer för olika antal sladdar.

[6] Antalet kontakter ökade under kriget till 8 och slutligen 10, och detta gjorde Enigma hela tiden säkrare.

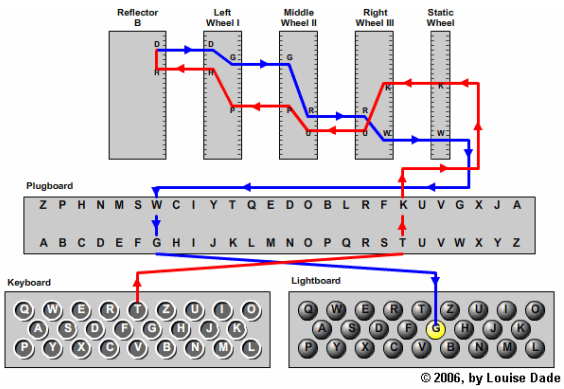
Tabell 2.3: Antalet möjliga kopplingar eller par, där n är antalet sladdar i kopplingsbordet [2].

n	Antalet möjliga kopplingar	n	Antalet möjliga kopplingar
0	1	7	1 305 093 289 500
1	325	8	10 767 019 638 375
3	3 453 450	10	150 738 274 937 250
4	164 038 875	11	205 552 193 096 250
5	5 019 589 575	12	102 776 096 548 125
6	100 391 791 500	13	7 905 853 580 625

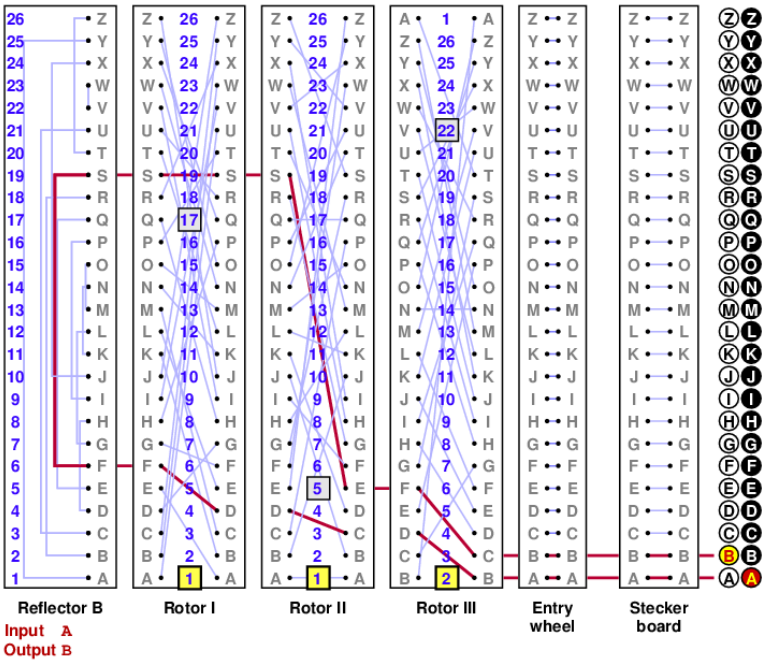
För en noggrannare överblick av Enigma och rotornas kopplingar se på figur 2.9.

Figuren 2.9 antar att kopplingsbordet (Stecker board) inte har sladdar.

Figur 2.7: Militär Enigmamaskin med kopplingsbord (tys. steckebrett, eng. plugboard) längst fram.



Figur 2.8: Modell av den militära Enigmas strömkrets.



Figur 2.9: Ytterligare exempel på Enigmas kopplingsschema.

2.2.1 Flottans Enigma

Tyska armén och flygvapnet nöjde sig med att använda Enigma med tre rotorer av fem. Tyska flottan, under ledning av Amiral Doenitz [24], ansåg att Enigma behövde mera säkerhet. Flottan var inte nöjd med att välja tre rotorer av fem, utan de valde fyra rotorer av åtta, numrerade I–VIII[7]. Inte nog med det, flottan var även noga med att utföra dubbelkryptering. Innan ett meddelande krypterades användes en kodbok för att byta ut alla normala ord till slumpmässiga "ord". Mottagaren hade en likadan kodbok för att dekryptera meddelandet efter att Enigma-krypteringen tagits bort.

Tack vara dessa åtgärder hade de allierade stora svårigheter med att dekryptera flottans meddelanden. Under stora delar av år 1942 led de allierade svåra förluster ute på Atlanten. Tyska u-båtar kunde operera i stort sett obehindrat, eftersom de allierade inte kunde läsa deras meddelanden och veta var de rörde sig [24].

[7]Rotorna numrerade I–V användes även av armén, flygvapnet etc.

2.3 Krypterings- och dekrypteringsexempel

Härnest presenteras ett krypterings- och dekrypteringsexempel. Vi använder Enigma datorprogrammet som beskrivs i bilaga A. Enigma har de rotor- och reflektorkopplingar som beskrivs i tabell 4.1 på sidan 58. Vi bestämmer först de dagliga inställningarna som kommer att användas i tabell 2.4.

Tabell 2.4: De dagliga inställningarna för Enigma

Rotorordning	Reflektor	Grundinställning	Ringinställning	Kopplingsbord
III-I-II	B	14-12-05	21-16-24	CH TY JK AB QW MN

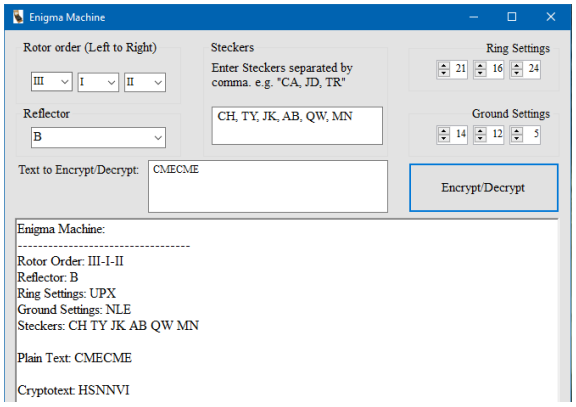
Vi vill kryptera följande meddelande:

> *In a hole in the ground there lived a hobbit.*
> *Not a nasty, dirty, wet hole, filled with the ends of worms and an oozy smell, nor yet a dry, bare, sandy hole with nothing in it to sit down on or to eat: it was a hobbit-hole, and that means comfort.*
>
> - J.R.R. Tolkien.

Först bör vi skriva om meddelandet så att det kan skrivas in i Enigma. För att göra det måste alla specialtecken tas bort. Dessutom skriver vi alla bokstäver som versaler, och "Enter" (dvs. ny rad) representeras av 'X'.

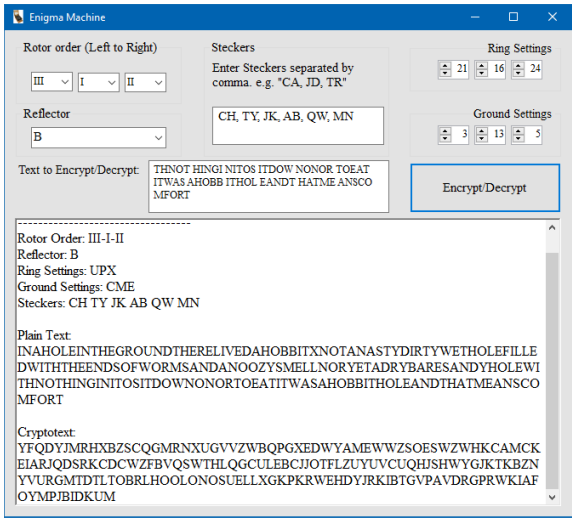
```
INAHO LEINT HEGRO UNDTH ERELI VEDAH OBBIT XNOTA NASTY DIRTY WETHO LEFIL
LEDWI THTHE ENDSO FWORM SANDA NOOZY SMELL NORYE TADRY BARES ANDYH OLEWI
THNOT HINGI NITOS ITDOW NONOR TOEAT ITWAS AHOBB ITHOL EANDT HATME ANSCO
MFORT
```

Innan vi kan kryptera meddelandet, måste vi skapa en meddelandenyckel (se kapitel 4 för mera information). Vi väljer CME, krypterar dessa tre bokstäver två gånger och får: $HSNNVI$.



Figur 2.10: Ställer in Enigma maskinen enligt dagliga inställningarna och krypterar CME, dvs. meddelandenyckeln.

Detta läggs till i början av det krypterade meddelandet (inte i klartexten!) och vi ställer nu om Enigma till grundpositionen CME, eller $3 - 13 - 5$, vartefter vi krypterar meddelandet, se figur 2.11.

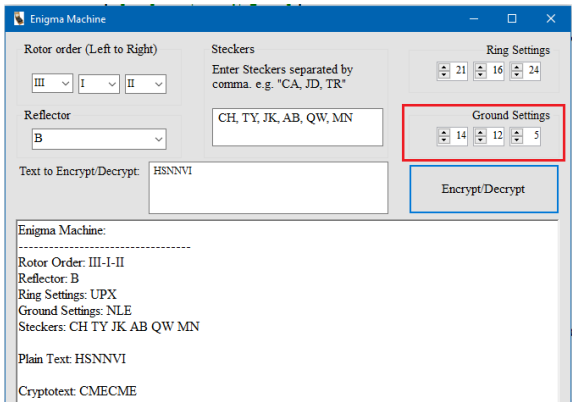


Figur 2.11: Vi ställer in Enigmamaskinen enligt den dagliga inställningarna och krypterar meddelandet.

Vårt krypterade meddelande blir:

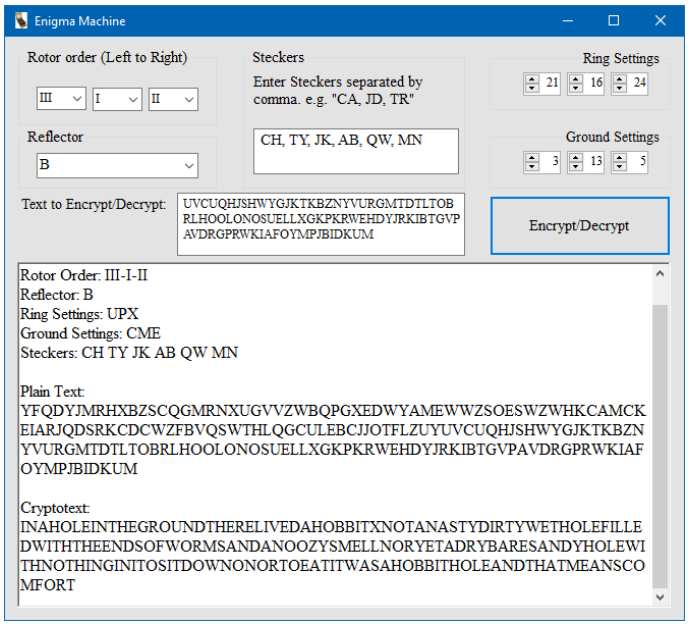
```
HSNNV IYFQD YJMRH XBZSC QGMRN XUGVV ZWBQP GXEDW YAMEW WZSOE SWZWH KCAMC
KEIAR JQDSR KCDCW ZFBVQ SWTHL QGCUL EBCJJ OTFLZ UYUVC UQHJS HWYGJ KTKBZ
NYVUR GMTDT LTOBR LHOOL ONOSU ELLXG KPKRW EHDYJ RKIBT GVPAV DRGPR WKIAF
OYMPJ BIDKU M
```

Detta är vad operatören skickar iväg över radion, där de sex första bokstäverna är meddelandenyckeln. För att mottagaren ska kunna läsa detta meddelande, måste mottagaren först dekryptera de sex första bokstäverna med Enigma inställt enligt de dagliga inställningarna. Mottagaren dekrypterar först meddelandenyckeln $HSNNVI$.



Figur 2.12: Vi ställer in Enigma enligt de dagliga inställningarna och dekrypterar meddelandenycklen.

Mottagaren får alltså ut meddelandenyckeln CME, eller $3 - 13 - 5$, och ställer nu in sina rotorer till denna grundinställning och skriver in resten av meddelandet i Enigma, inte meddelandenyckeln.



Figur 2.13: Vi ställer in Enigma enligt meddelandenyckeln och dekrypterar meddelandet.

Av Enigma får vi utskriften:

```
INAHO LEINT HEGRO UNDTH ERELI VEDAH OBBIT XNOTA NASTY DIRTY WETHO LEFIL
LEDWI THTHE ENDSO FWORM SANDA NOOZY SMELL NORYE TADRY BARES ANDYH OLEWI
THNOT HINGI NITOS ITDOW NONOR TOEAT ITWAS AHOBB ITHOL EANDT HATME ANSCO
MFORT
```

Vi skriver om detta i läsbar form, lägger in nya rader och punkter etc:

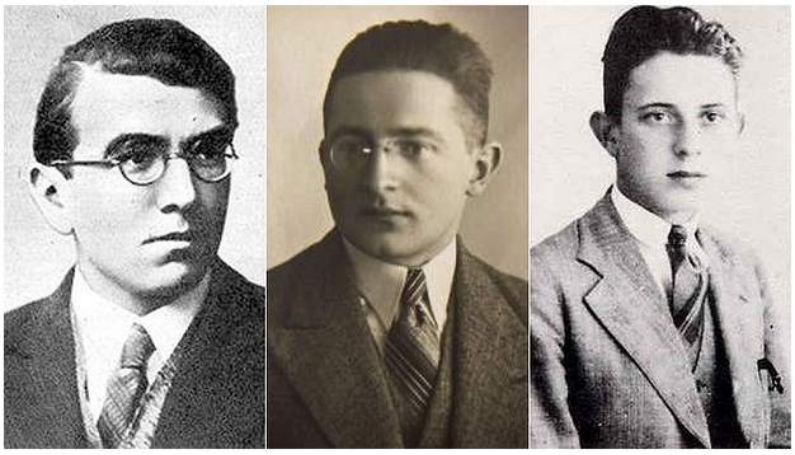
> *In a hole in the ground there lived a hobbit.*
> *Not a nasty, dirty, wet hole, filled with the ends of worms and an oozy smell, nor yet a dry, bare, sandy hole with nothing in it to sit down on or to eat: it was a hobbit-hole, and that means comfort.*

Som synes är detta samma text som vi matade in i Enigma från början. Vi har därmed lyckats kryptera och dekryptera ett meddelande med hjälp av ett Enigma-program, se bilaga A för detaljer om programmet. Se även kapitel 4 för en mera noggrann beskrivning av krypteringen och dekrypteringen.

Kapitel 3

Historia

Av alla de kryptologer som under andra världskriget (1939-1945), samt åren före kriget, hade i uppgift att knäcka tyskarnas krypteringsmaskin Enigma, förtjänar tre polska matematiker att bli framlyfta. Dessa tre matematiker är: *Marian Rejewski*[1], *Jerzy Różycki*[2] och *Henryk Zygalski*[3], figur 3.1. Av dessa var speciellt Rejewski ansvarig för mycket av det kryptologiska arbete som utfördes i Poznań och Warszawa för den poslak krypteringsbyrån [2], [20],[21].



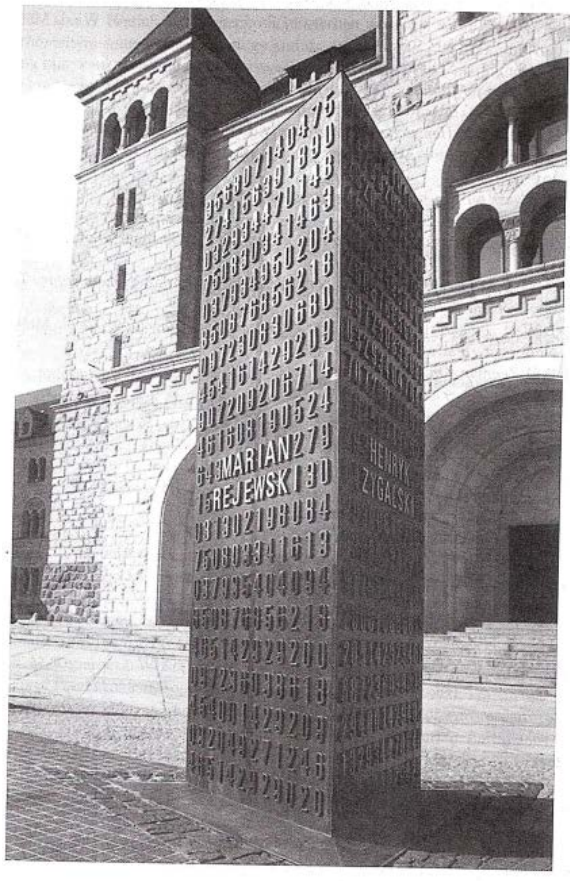
Figur 3.1: Från vänster *Zygalski, Rejewski* och *Różycki*, de tre polska kryptologerna som knäckte Enigma.

Detta kapitel handlar om hur dessa tre kryptologer listade ut rotorkopplingarna i Enigma och därmed kunde läsa Tysklands militära meddelanden och rapporter. Historiker anser att detta arbete förkortade kriget med ungefär två år [10]. Kapitelet ger främst en historisk överblick, och kapitel 4 innehåller den bakomliggande matematiken.

[1]Rejewski: `https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/hall-of-honor/2014/mrejewski.shtml`

[2]Różycki: `https://en.wikipedia.org/wiki/Jerzy_Rozycki`

[3]Zygalski: `http://www-groups.dcs.st-and.ac.uk/history/Biographies/Zygalski.html`



Figur 3.2: Monument i Poznań, Polen, till minne av *Marian Rejewski, Jerzy Różycki* och *Henryk Zygalski*.

3.1 Slutet av 1927 - september 1932

Sedan slutet på första världskriget (1918), letade Tyskland efter metoder för att förbättra sin förmåga att kryptera viktiga (stats, militära, diplomatiska etc.) meddelande. En faktor i Tysklands förlust i första världskriget var okrypterad kommunikation som avlyssnades av den andra sidan [24]. Arthur Scherbius uppfann och patenterade krypterings- och dekrypteringsmaskinen Enigma år 1918. Enigma köptes av den tyska staten, och efter några modifikationer (kapitel 2), började tyskarna massproducera Enigma för att utrusta staten, militären samt liknande viktig organisationer med Enigma [2]. Det tog fram till år 1928 innan maskinen togs i bruk och började användas för att kryptera meddelanden. Bland annat polackerna avlyssnade tyska Enigma meddelanden och försökte deciffrera dem. Polska försök lyckades inte och de slutade snabbt att försöka. Även Frankrike och Storbritannien

försökte knäcka Enigma, men gav upp relativt snabbt [20].

År 1929 (sent 1928) startade en kryptografikurs vid Poznańs universitet för matematikstuderanden som var i slutskedet av sina studier. Kursen anordnades eftersom Polens "krypteringsbyrås" (eng. Cipher Bureau, pol. Biuro Szyfrow) chef, *Major F. Pokorny*, ansåg att det var viktigt att satsa resurser på att lösa Enigma. Vem som helst blev inte antagen till kursen, endast ytterst begåvade studerande som kunde flytande tyska fick ansöka. Ytterst få fick veta att kursen existerade ty kursen var inte öppet annonserad för att tyskarna inte skulle mistänka att polackerna försökte knäcka deras kryptering [12], [20]. Bland deltagarna i kursen valdes tre personer: *Marian Rejewski, Jerzy Różycki* och *Henryk Zygalski*, som år 1932 blev heltidsanställda[4] av krypteringsbyrån med uppgift att knäcka Enigma.

[4]De hade arbetat deltid för Byrån under åren efter krypteringskursen 1929.

3.1.1 Marian Rejewski

> *It is a well known phenomenon that man, as a being edowed with consciousness and memory, cannot imitate chance perfectly, and it is the cryptologist's task, among other things, to discover and make proper use of these deviations from chance.*
>
> - Marian Rejewski [2]

Figur 3.3: Marian Rejewski

Av de tre utvalda för att arbeta vid krypteringsbyrån, är *Marian Rejewski* den person som mest förtjänar att bli omtalad. Rejewski var hjärnan bakom polackernas försök att lösa Enigma och utan honom är det mycket möjligt att Enigma aldrig blivit löst.

Rejewski föddes 16 august år 1905 i Bydgoszcz, Polen. Han gick gymnasiet i Bydgoszcz, efter vilket han studerade matematik vid Poznańs universitet och utexaminerades 1929. Efter examen studerande han försäkringsmatematik i Göttingen i ett år. Han återvände till Poznańs universitet som föreläsare under åren 1930-1932. Under sin tid som föreläsare arbetade Rejewski samtidigt för polska krypteringsbyrån på deltid, och blev år 1932 fast anställd av byrån för att arbeta som kryptolog.

Efter kriget återvände Rejewski från Storbritannien till Polen. Han arbetade som kontorist i olika företag fram tills pensionen, och dog den 13 februari år 1980. Det tog fram till år 1973 före Rejewski och hans kollegor fick det erkännande de förtjänade. Före detta år visste ingen om att Enigma blivit löst. Britterna försökte 1973 ge all ära åt Alan Turing, men Frankrike och Polen var snabba med att ge äran åt Rejewski och hans kollegor och korrigerade Storbritanniens försök att ge all ära till Alan Turing [3], [10], [12], [20].

3.1.2 Jerzy Różycki

Różycki föddes den 24 juli 1909 i Vilshana i Ukraina. Fram till 1918 gick han i skola och bodde i Kiev. År 1918 flyttade Różycki till Wyszków i östra Polen där han avklarade gymnasiet år 1926.

Efter gymnasiet flyttade Różycki till Poznań för att studera matematik 1927-1932. Różycki var en av de tre som deltog i kryptologikursen som anordnades av krypteringsbyrån, och blev anställd av byrån för att arbeta med Enigmas kryptering.

Figur 3.4: Jerzy Różycki

Różycki, Rejewski och Zygalski arbetade tillsammans från och med tidigt 1933 (efter att Rejewksi hade listat ut rotorkopplingarna) med att leta efter och hitta de dagliga nycklarna för att kunna dekryptera Enigma meddelanden. Różyckis största bidrag kan anses vara "klockmetoden" (avsnitt 4.2.2) som underlättade kryptologernas arbete med att lista ut vilken rotor som var den "snabba" (högra) rotorn för en specifik dag. Detta var den första, och kanske enda, metoden som polackerna utvecklade baserad på språkliga kunskaper om det tyska språket, till skilland från de andra metoderna som var baserade på matematik.

Różycki avled den 9:e januari 1942, när en båt i Medelhavet som han var passagerare på. Różycki var på väg tillbaka till Frankrike efter ett besök till Nord-Afrika.

3.1.3 Henryk Zygalksi

Zygalski föddes den 15 juli 1908 i Poznań. Zygalski studerade till matematiker vid Poznań universitet och gick kryptologikursen som krypteringsbyrån anordnade år 1929.

Figur 3.5: Henryk Zygalski

Zygalski var en av de tre personer som krypteringsbyrån bestämde sig för att anställa efter att kryptologikursen var avklarad. Från och med tidigt 1933 (när Rejewski anställdes på heltid) efter att Rejewski listat ut Enigmas rotorkopplingar, arbetade Zygalski, Rejewski och Różycki tillsammans med att utveckla metoder som kunde användas för att dekryptera Enigma meddelanden på ett effektivt sätt.

Dessa tre kryptologer samarbetade med att tillverka en katalog som användes för att lista ut Enigmas inställningar. Denna användes ända tills Tyskland bytte ut reflektor A till reflektor B.

Zygalskis största bidrag kom runt slutet på 1939, när han presenterade sina "Zygalskipapper" (se avsnitt 4.3.1) som ett alternativ till den kryptologiska bomben. De tre kryptologerna försökte skapa dessa papper, men hade inte tillräckliga resurser för att tillverka dem tillräckligt snabbt. Det dröjde ända tills kryptologerna flytt till Frankrike innan britterna, med mera resurser, skapade Zygalskipappren och skickade dem till de polska kryptologerna.

Efter kriget stannade Zygalski i England, han arbetade som en föreläsare i statistisk matematik vid "University of Surrey". Fram tills 1973 var han förbjuden av sekretesslagar att prata om sina framgångar inom kryptologi och hans insatser i lösandet av Enigma.

En kort tid innan han avled, blev han tilldelad titeln "hedersdoktor vid Polish University in Exile", ett polskt universitet i London.

3.2 September 1932 - augusti 1935

Rejewski började sitt arbete utrustad enbart med en kommersiell Enigma, tysk korrespondens, papper och penna. Utrustad med dessa påbörjade han arbetet med att hitta mönster i meddelandena. Som Rejewski själv uttrycker det:

> *Whenever there is arbitrariness, there is also a certain regularity. There is no avoiding it.*
>
> - Marian Rejewski [2]

Fritt översatt: "Var det finns godtycklighet, finns det även ett visst mönster. Det är omöjligt att undvika."
Med andra ord, Rejewski menar att även om Enigmachiffret verkar sakna ett mönster, så är det möjligt att hitta ett mönster om man letar tillräckligt länge.

Under hösten 1932 arbetade Rejewski ensam med att leta efter mönster i de tyska meddelandena. Innan kriget bryter ut 1939 är tyskarna ovarsamma med hur de skickar meddelanden (se Kapitel 4). Tyskarna hade tre rotorer (se sid. 8) i användning och deras ordning böt enbart en gång per 3 månader (4 gånger per år) [20], [2], [12], [8].

För att kunna läsa meddelandena, behövde polska underrättelsetjänsterna känna till följande saker:

- kopplingarna inne i rotorerna (dvs. hur bokstäverna byts)
- reflektorns kopplingar
- rotorernas ordning
- kopplingsbordets sladdkopplingar
- rotorernas grundinställningar
- rotorernas ringinställningar
- meddelandenyckeln[5].

[5]En skild nyckel som var specifik för varje meddelande.

En ganska lång lista med saker som Rejewski hade i uppgift att finna. Kapitel 2 berättar mera noggrant om dessa komponenter.

Rejewski visste att tyskarna hade ett kod-papper som gav de dagliga inställningarna, sladdar, ordning etc. Tyskarna insåg dock att om enbart kod-pappret användes, så kunde motståndaren läsa alla dagens meddelanden ifall de knäckte ett av dagens meddelanden. För att motverka denna svaghet, instruerades tyska signalister att i början av varje meddelande ange en "meddelandenyckel" (eng. message key). Tyskarna ställde in Enigma enligt kod-pappret för den dagen (se figur 3.6[6] för exempel på ett kodpapper från kriget). Operatören valde sedan tre bokstäver (först helt fritt men striktare regler kom med åren), t.ex. ABC. Dessa tre bostäver motsvarar siffrorna 1, 2, 3 på rotorn i figur 2.3, och berättar att operatören har ställt in sina rotorer med inställnignarna 1 (långsamma), 2 (mellan), 3 (snabba). Operatören börjar sitt meddelande med att sätta dessa tre bokstäver i början av meddelandet för att mottagaren ska kunna dekryptera meddelandet.

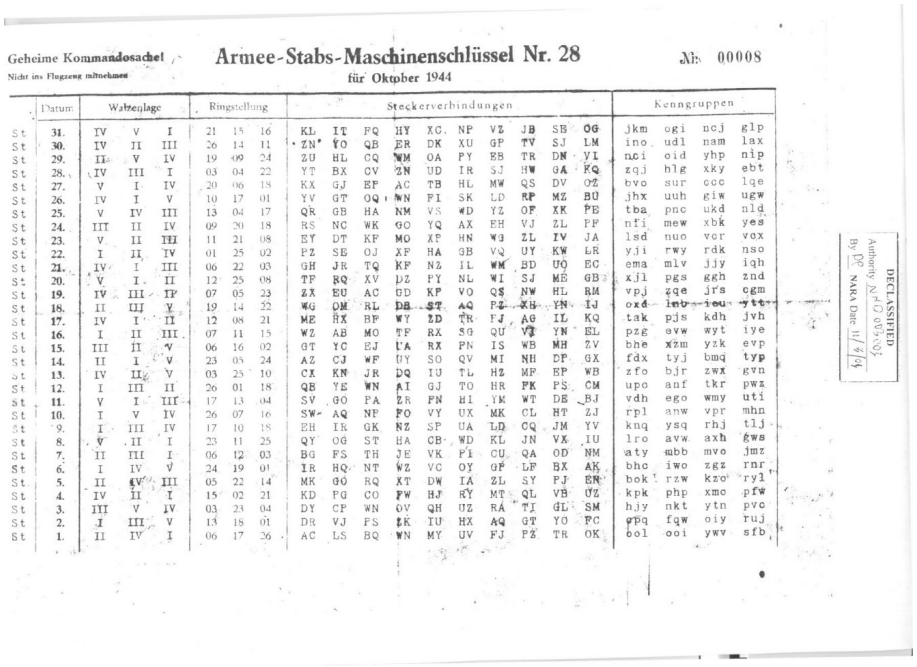
Tyskarna ansåg att dessa tre bostäver måste krypteras och dessutom, för att förhindra fel vid överföring av meddelandet, bifogas två gånger. Operatorn ställde in Enigma enligt kod-pappret, väljer sina tre bokstäver, hen krypterar bokstäverna två gånger enligt dagliga inställningarna. Operatören ställer sedan in Enigma enligt sin egen meddelande-nyckel (snurrar rotorerna till positionerna $A(1), B(2)$ och $C(3)$). vartefter hen krypterar sitt meddelande och skickar det, med $ABCABC$ i krypterad form i början av meddelandet.

Antag att operatören har valt nyckeln ABC, låt oss säga att dessa bokstäver krypteras till $GHTPRV$, detta sätts i början av meddelandet. Detta var ett av tyskarnas misstag, Rejewski insåg att dessa sex bostäver var krypterade med grundinställningen och att de angav så kallade nyckelpar.

$$ABC\ ABC \overset{\text{Krypteras}}{\longrightarrow} GHT\ PRV$$

detta ger oss att

[6]Noterbart är att flottan använde mera komplicerade lappar och kodböcker.



Geheime Kommandosache!
Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28
für Oktober 1944

№ 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SB	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	YI	nci	oid	yhp	nlp
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	coc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jbx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QR	GB	HA	NM	VS	WD	YZ	OP	XK	PE	tba	pnc	ukd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nfi	mew	xbk	yes
St	23.	V	II	III	11	21	08	EY	DT	KF	MO	XP	HN	WJ	ZL	IV	JA	lsd	nuo	vcr	vox
St	22.	I	II	IV	01	25	02	PZ	SE	OJ	XF	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KP	NA	IL	WM	BD	UQ	EC	ema	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TP	RQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
St	19.	IV	III	IV	07	05	23	ZX	EU	AC	DD	KP	VO	QS	NW	HL	RM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	WG	OM	RL	DB	ST	AQ	PZ	XH	YN	IJ	oxd	lnb	icu	ytt
St	17.	IV	I	II	12	08	21	ME	HX	BP	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VZ	YN	EL	pzg	avw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	UA	RX	PN	IS	WB	MH	ZV	bhe	xzm	yzk	evp
St	14.	II	I	V	23	03	24	AZ	CJ	WF	UY	SO	QV	MI	NH	DP	GX	fdx	tyj	bmq	typ
St	13.	IV	II	V	03	25	10	CX	KN	JR	DQ	IU	TL	HZ	MP	EP	WB	zfo	bjr	zwx	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	GJ	TO	HR	FK	PS	CM	upo	anf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ZR	FN	HI	YM	WT	DE	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NF	FO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	18	EH	IR	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CB	WD	KL	JN	VX	IU	lro	avw	axh	gws
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	PI	CU	QA	OD	NM	aty	ubb	mvo	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	GF	LP	BX	AK	bhc	iwo	zgz	rnr
St	5.	II	V	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	PJ	EN	bok	rzw	kzo	ryl
St	4.	IV	II	I	15	02	21	KD	FG	CO	FW	HJ	RY	MT	QL	VB	UZ	kpk	php	xmo	pfw
St	3.	III	V	IV	03	23	04	DY	CF	WN	OV	QH	UZ	RA	TJ	GL	SM	hjy	nkt	ytn	pvc
St	2.	I	III	V	13	18	01	DR	VJ	FS	EK	IU	HX	AQ	GT	YO	PC	ypq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PZ	TR	OK	bol	ooi	ywv	sfb

DECLASSIFIED
Authority NND 969192
By DR NARA Date 11/24/14

Figur 3.6: Ett exempel på kodlapp som tyskarna använde under kriget för sina dagliga inställningar, från oktober 1944.

$$A = G \text{ samt} \quad A = P$$

$$B = H \text{ samt} \quad B = R$$

$$C = T \text{ samt} \quad C = V,$$

Det här var en väg in för att finna rotorernas kopplingar. Kryptologi bygger på att hitta mönster, och här har tyskarna berättat vilka två chifferbokstäver som samma klartextbokstav krypteras till.

Kombinerar man denna kunskap, matematiska uträkningar (se kapitel 4) samt kodpapper som en tysk landsförädare (fransk spion[7]) lyckades ge till Rejewski i december 1932, listar Rejewski ut exakt hur de olika rotorerna är kopplade [20], [2].

När Rejewski vet hur rotorerna är kopplade tillverkar polackerna polska "Enigmor" som har rotorer med samma kopplingar som tyskarnas rotorer. När dessa maskiner är klara, är det upp till Rejewski och hans kollegor (*Zygalski* och *Różycki*) att uppfinna metoder för bestämmande av de dagliga nycklarna, dvs. bestämma grundinställningarna utan kodpapper. De lyckas uppfinna ett antal metoder för det-

[7]Hans-Thilo Schmidt; kodnamn: Asché, [24]

ta ändamål, och inom kort har polackerna möjlighet att läsa tyskarnas korrespondens dagligen [20], [2]. Detta pågick i ca tre år, fram till 1935, tills tyskarna började göra förändringar i Enigmas användning.

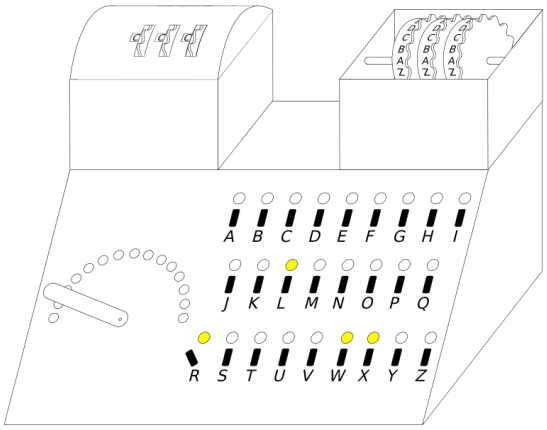
3.3 Augusti 1935 - augusti 1938

I februari 1936 började tyskarna byta rotorordningen varje månad, och efter november 1936 byttes ordningen dagligen. Detta gav Rejewski och hans kollegor mera arbete, men de lyckades lista ut de dagliga nycklarna. Detta gjordes de med Różyckis klockmetod (eng. clock method). Av alla metoder som matematikerna hittills uppfunnits var det här den första som inte byggde enbart på matematik, utan använde kunskap om hur det tyska språket är uppbyggt, dvs. en språklig metod [20]. Även rutnäts-metoden uppfanns, se avsnitt 4.2.1 på sida 59.

Augusti år 1935 innebar mera bekymmer för de polska matematikerna, när tyskarna började rusta upp för krig. Upprustandet innebar att antalet Enigma användare ökade. Vilket leder till att tyskarna delar upp sitt nätverk, det tyska flygvapnet fick ett eget nätverk med egna koder, tyska armén fick ett eget nätverk osv. Detta sysselsatte Rejevski och hans kollegor, eftersom de nu var tvugna att hitta de dagliga nycklarna för alla dessa nätverk och inte bara för ett nätverk.

Oktober år 1936 ändrade tyskarna antalet sladdar som användes på kopplingsbordet. Istället för sex stycken användes mellan fem och åtta stycken sladdar. Detta gjorde arbetet för de polska kryptologerna ytterligare mera tisdkrävande och de var tvugna att förbättra sina metoder för att lista ut de dagliga nycklarna i rimlig tid.

I början av 1936 var det tidskrävande att finna de dagliga nycklarna, men kryptologerna kom på en lösning. De kände till rotorernas kopplingar och reflektorns kopplingar, de lät tillverka en cyklometer (se avsnitt 4.2.3, och figur 3.7). Cyklometern består av Enigmas tre rotorer och reflektor, och den tillät kryptologerna att mer effektivt bestämma de dagliga nycklarna. Rejewski och hans kollegor skapade en katalog som bestod av alla möjliga kombinationer, dvs. de arrangerade rotorerna i alla sex ordningar och gick systematiskt igenom de 26^3 kombinationer av



Figur 3.7: Bild på polsk cyclometer som Rejewski och hans kollegor tillverkade.

grundinställningarna. De gjorde detta genom att vrida på en knapp vid bostäverna i cyclometern, figur 3.7. Då lyste den bokstavens lampa upp, men även de bokstäver som var kopplade till den (noggrannare i kapitel 4). Detta arbete tog ungefär ett år, men när det var klart gick det snabbt att finna de dagliga nycklarna.

3.3.1 Katalog

Rejewski och hans kollegor hade listat ut Enigmas rotorkopplingar. De hade även byggt flera polska Enigmor som använde samma rotorer som de tyska, och med dessa kunde polackerna dekryptera den tyska korrespondensen förutsatt att de dagliga nycklarna var kända.

För att hitta dessa dagliga nycklar så snabbt som möjligt, bestämde sig Rejewski och hans kollegor för att tillverka en kortkatalog som innehåller alla möjliga rotor kombinationer. Katalogen innehåller $6 \cdot 26^2 = 4056$ stycken kort, där varje kort korresponderar till en rotorordning och en grundinställning för den ordningen. Ifall Rejewski och hans kollegor lyckades bestämma startpositionen och vilken rotor som var i snabba positionen behövde de enbart undersöka $2 \cdot 26^2 = 1352$ olika kort för att finna maskinens uppställningen. Det fanns dessutom operatormisstag och oförsiktigthet vilket gjorde att man snabbt kunde utesluta möjligheter. På det här sättet kunde Rejewski och hans kollegor varje dag bestämma vilken position den snabba rotorn var i med meddelandenyckeln, och dessutom vilken rotor som var

den snabba, varefter man med uteslutningsmetoden bestämde positionerna och inställningarna för de två andra rotorerna.

När Rejewski och kollegor, efter ett år, hade katalogen klar behövde de enbart kontrollera karakteristiken från korten för att bestämma ordningen på rotorerna, samt deras grundinställningar. Det tog enbart 10 till 15 minuter att finna grundinställningarna.

Katalogen kunde dock inte användas en längre tid. I november år 1937, bytte tyskarna ut sin reflektor A till en ny reflektor B. Detta innebar att hela katalogen blev värdelös, eftersom den var skapad specifikt för reflektor A. Rejewski och kollegor var tvugna att lista ut den nya reflektorns kopplingar, vartefter de måste skapa en ny katalog. Denna gång tog det kortare tid att skapa katalogen [20], [2].

3.3.2 Underrättelsenärverk, SD (tyska. Sicherheitsdienst)

I september 1937, lite innan tyskarna byter ut reflektorn, dyker ett nytt nätverk upp,[8] en underrättelsetjänst som kan liknas vid Gestapo. De utnyttjade Enigma för att skicka krypterade meddelanden. Innan pariet lät operatorerna kryptera meddelanden måste de, användea en kodbok. Med andra ord, de utförde dubbelkryptering. Först bytte de ut alla ord mot 4 bokstavs långa "ord" som sedan krypterades.

Det är viktigt att vi nämner detta SD nätverk, eftersom SD nätverket inte följde de nya instruktionerna för skickadet av meddelandenycklar (dvs. de första sex bokstäverna). Därmed hade Rejewski och hans kollegor möjlighet att via detta (slarviga) SD nätverk lista ut kopplingar i nya rotorer och reflektorer när tyskarna introducerade sådana [20]. Alla nätverk använder sig av samma rotorer och reflektorer men de dagliga inställningarna för nätverken var olika, dessutom var SD nätverket det ända som inte ändrade hur de skickade meddelandenycklar.

[8] Sicherheitsdienst eller SD.

3.4 September 1938 - september 1939

September år 1938 ändrade tyskarna instruktionerna för skickandet av meddelandenycklar. Istället för att operatörerna själva fick välja tre bokstäver, som sedan krypterades två gånger, måste operatörerna "välja" tre slumpmässiga bokstäver. De slumpmässigt valda bokstäverna användes sedan som startpositioner. En operatör valde tre bokstäver, kalibrerade rotorerna enligt dessa, valde tre **andra** bokstäver som hen sedan krypterade två gånger. Varför? Tyskarna ansåg att man måste sätta meddelandenyckeln i början av meddelandet två gånger, eftersom radiokommunikationen inte var kristallklar, och för att det fanns en risk att nyckeln skulle misförstås. Om man skickade nyckeln två gånger, fanns det en chans att åtminstone den ena nyckeln skulle gå att förstå.

Exempel 1. *För att skapa en meddelandenyckel tar en operatör tre slumpmässiga bokstäver, t.ex.* YDS (24 4 19)*. Hen ställer in rotorerna enligt nyckeln.*

Därefter tar operatören tre nya bokstäver som hen krypterar två gånger, t.ex. TRS*, låt oss säga att dessa tre krypteras till* OLK*, och till* KPT*.*

Operatören skriver YDS*,* $OLKKPT$ *i början av meddelandet, vartefter hen ställer in rotorerna till startpositionen* TRS *och krypterar sitt meddelande.*

Detta tillvägagångssätt gjorde att Rejewskis och hans kollegors metoder för att finna dagliga nycklar inte längre fungerade. Kryptologerna kunde nu för en tid framöver enbart lista ut SD nätverkets nycklar. Kryptologerna gav inte upp, och inom ett par veckor hade de utvecklat två nya metoder för att lista ut de dagliga nycklarna. De kom på idén att tillverka en maskin som automatiskt kan kontrollera de olika dagliga nyckelkombinationerna, de kallar denna maskin "Bomba kryptologiczna" (eng. the cryptological bomb), samt en annan metod kallad Zygalskis papper (eng. Zygalski Papers).

3.4.1 Kryptologisk bomb

Vi visar nu tre möjliga nycklar som kunde ha skickats i början av tyska meddelanden enligt det nya systemet:

$$RTJ, \mathbf{W}AH\ \mathbf{W}IK$$

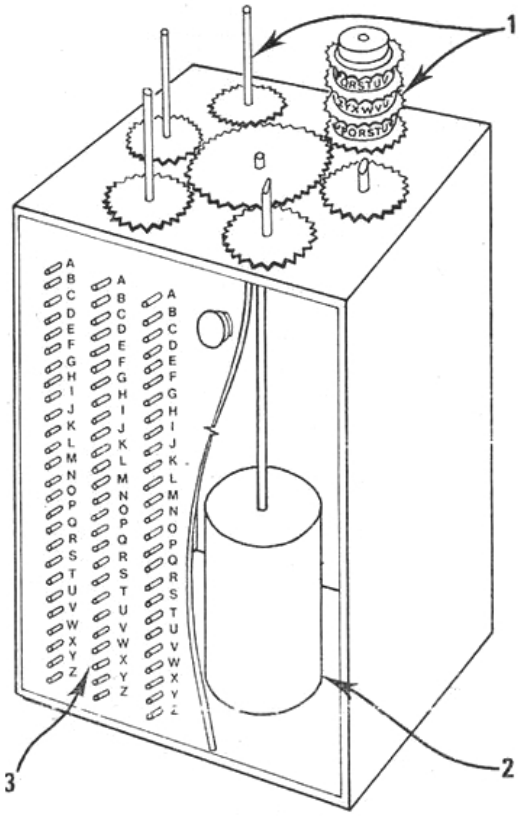
$$HPN, RA\mathbf{W}\ KT\mathbf{W}$$

$$DQY, D\mathbf{W}J\ M\mathbf{W}R$$

Här representerar de tre första bokstäverna de okrypterade bokstäverna och de andra sex är meddelandenyckeln krypterad två gånger. Ifall Rejewski och hans kollegor hade tillgång till meddelanden där en bokstav, t.ex. W. Dyker upp på platserna: ett och fyra, två och fem eller tre och sex. Ifall man även antog att kopplingsbordet inte påverkade dessa bokstäver, och om man känner till i vilken ordning rotorerna är placerade i maskinen. Kan man ställa in sin egna Enigma till den startpositionen. Man trycker sedan ner W tre gånger vilket gör att samma lampa kommer att lysas upp, förutsatt att ringinställningarna var korrekta. Tanken är här att eftersom kopplingsbordet inte påverkar längden på cykler (mer om detta senare), är W en cykel med längd ett. Alltså kommer tryckandet av bokstav W att ge samma krypterade bokstav tre gånger. Det som vi inte känner till här är vilken inställning som rotorernas ringar har eller kopplingarna på kopplingsbordet, och därmed vet vi inte hur vi ska ställa in resten av maskinen.

Rejewski och hans kollegor fick idén att låta tillverka så kallade "kryptologiska bomber", med vars hjälp det var möjligt att kontrollera alla möjliga positioner på rotorerna samt rotorernas ordning inom två timmar. Eftersom det fanns sex möjliga rotor ordningar ansåg Rejewski det bäst att tillverka sex stycken bomber. Bomberna kör samtidigt och markerar när de hittat en kombination av rotorer och grundinställningar som ger upphov till samma lampa (bokstav) tre gånger. Bomberna går igenom alla $26^3 = 17\ 576$ startpositioner för en specifik rotor ordning, "trycker" W, när samma lampa lyser tre gånger i rad hade man med stor sannolikhet hittat den eftersökta startpositionen.

Vi får inte glömma bort kopplingsbordet. Ifall man hittade en kombination av bokstäver som dök upp sex gånger dvs. en gång i varje position, enligt exemplet, kunde man anta att just den bokstaven, W, med stor sannolikhet inte förändras av kopplingsbordet.



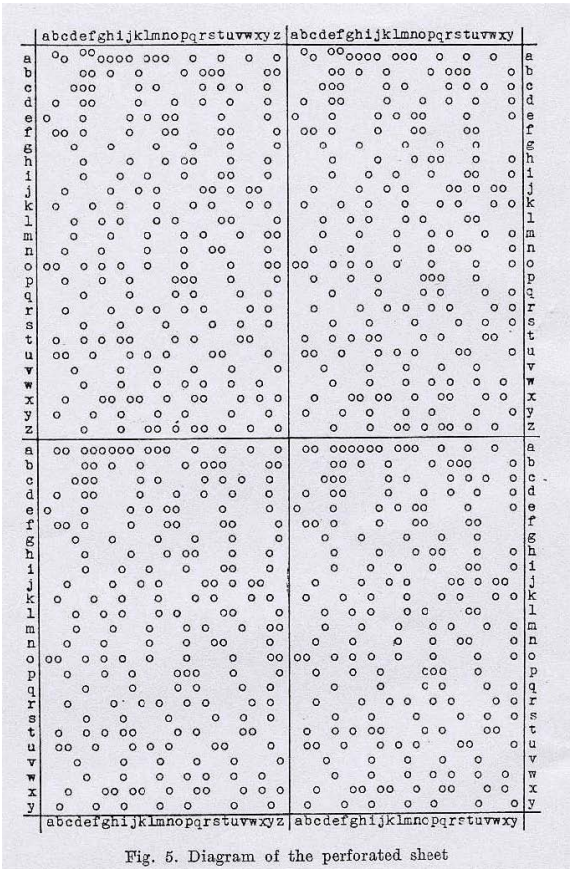
Figur 3.8: Bild av polsk kryptologisk bomb, endast en rotorkombination syns här.

Figur 3.8 är en återskapning av hur en sådan polsk bomb kunde ha sett ut. De olika rotorkombinationerna placerades på toppen och man kunde sedan välja bokstav från framsidan. Efter att denna tickat igenom alla möjligheter hade man sannolikt hittat de dagliga inställningarna.

Vi noterar att denna bomb hittade, "en-längds cyklerna" i Enigma för en dag, se kapitel 4 för noggrann beskrivning av dessa cykler. När man lyckats lista ut vilken/vilka en-längds cykler som finns kan man jämföra dessa med ett register som liknade katalogen (3.3.1). Problemet var att det krävdes flera och komplicerade kataloger för att kunna utföra jämförelserna än tidigare. Det var här som *Zygalski*

kom med idén om att tillverka stora pappersark med noggrant utplacerade hål, dessa kallas för Zygalskipapper, exempel i figur 3.9.

3.4.2 Zygalski papper



Figur 3.9: Bild av ett Zygalski papper, hålen visar var en-längds cykler finns.

Figur 3.9 visar ett Zygalskipapper. Papprena var gjorda i tjockt papper och hade rektanglar med storleken 51×51. Varje startposition på långsamma rotorn L fick ett eget papper, på $x-$ och $y-$axlarna hittar vi de två andra rotorernas positioner. At skapa papprena var ett stort arbete, eftersom det fanns nästan tusen hål på ett papper och det var nödvändigt att tillverka sex hela knippen, ett knippe per rotorkombination. Det var alltså nödvändigt att tillverka $26 \cdot 6 = 156$ papper (26, ty de representerade alla 26 möjliga startpositioner för L). Detta gjordes samtidigt som de letade efter dagliga nycklar med mindre effektiva metoder.

Meningen med pappren var att lägga de ovanpå varandra enligt vilka en längds cykler

de hittat. När tillräckligt med papper låg på varandra fanns det troligen endast ett fåtal hål som syntes igenom alla papper. Koordinaterna för hålena indikerade möjliga inställningar för rotorerna.

När Rejewski och kollegor hade tillverkat två hela knippen, dvs. 52 papper (15 december 1938) beslöt tyskarna att införa två nya rotorer. De använde fortfarande endast tre, men kunde nu välja från fem stycken. Detta innebat att istället för sex kombinationer, så fanns det $5 \cdot 4 \cdot 3 = 60$ möjliga sätt att installera rotorerna på. Detta innebar att antalet Zygalski papper som behövdes steg till $60 \cdot 26 = 1560$, och denna mängd var helt enkelt för stor för de tre polska kryptologerna.

Tack vare att SD nätverket fortfarande existerarde och använde sig av det gamla signalprotokollet, dvs. skicka meddelandenyckeln krypterad två gånger, kunde Rejwski och hans kollegor lista ut kopplingarna i de två nya rotorerna IV och V. Med samma metod som förr. Dessa nya rotorer introducerades efter att det nya kommunikationsprotokoll tagits i bruk och därför kunde kryptologerna inte lista ut kopplingarna från något annat nätverk än SD [2], [12], [20], [21].

3.4.3 Hjälp

Den 25 juli år 1939, när det verkade troligt att krig skulle bryta ut, kallade Polen representanter från Storbritannien och Frankrike för att dela med sig av sina framgångar rörande Enigma. De träffades i Warszawa där det snabbt blev klart för polackerna att deras allierade, Frankrike och Storbritannien inte hade möjlighet att läsa Enigma meddelanden. De kände inte till rotorkopplingarna och hade därmed ingen möjlighet att läsa vad tyskarna höll på med. Krypteringsbyrån gav två stycken polska Enigmor med tillhörande fem rotorer åt sina allierade. Dessa Enigmor var ytterst viktigt för de allierade, eftersom det gav fransmännen och britterna möjlighet att läsa Enigma meddelanden och förbereda sig för tyska attacker. Med dessa kunde Storbritannien utveckla metoder för att hitta de dagliga nycklarna som krävde mera manskap. Både Frankrike samt Storbritannien kunde satsa mera resurser på kryptologi och hade stora baracker i landet för kryptologer som arbetade dag och

med med lista ut de dagliga nycklarna och dekryptera Enigma meddelanden.

Det visar sig att Polen kontaktade sina allierade i sista minuten, knappt en månad senare (1:a september 1939) anföll tyskarna Polen utan förvarning [2], [20], [21].

3.5 September 1939 - 1945 (kriget börjar)

Tyskland anföll den polska staden Danzig mitt i natten den 1:a september 1939. Tyskarna hade ankrat ett slagsskepp[9] utanför staden med den ursäkten att de var där för att hedra de tyska soldater som gått på grund utanför staden under första världskriget. Dock visade det sig att tyskarna använde detta svepskäl för att komma nära staden för att kunna skjuta med kanoner på en polsk militäranläggning som låg nära hamnen mitt i natten. Utan en officiell krigsförklaring hade tyskarna angripit Polen [10].

En knapp vecka senare, (5:e september, 1939 [2]), beordrades krypteringsbyrån att evakuera. Rejewski och hans kollegor förstörde alla spår av Enigma forskningen, för att tyskarna inte skulle misstänka att Enigma blivit löst. Rejewski höll dock två polska Enigmor som de tillverkat [2], [20].

Rejewski och hans kollegor flyr med tåg från den hotade staden Warszawa till Frankrike, via Rumänien och Italien. När de till slut anländer till Frankrike den 20 oktober 1939 fortsätter matematikerna lösa tyska krypteringar. De stationerade sig i slottet "castle at Vignolles", vilket ligger ca 40 km från Paris, och deras arbetsstation döptes till BRUNO [20].

Kort efter att polackerna anlände till Frankrike, skickar britterna en fullständig samling av Zygalski papper, dvs. 60 knippen med 26 papper var till polackernas station i Frankrike [20].

Vid det här laget, efter att Polen delat med sig av hemligheterna med Enigma till Storbritannien och Frankrike, märker man snabbt att *Rejewski, Zygalski* och *Różycki* tillsammans med de 12 andra kryptologer och annan personal som flydde från Polen

[9] Schleswig-Holstein.

inte har möjlighet att hålla samma takt som britterna. Sorbritannien har vid det här laget närmare 10 000 anställda kryptologer och annan personal vid Bletchley Park.

Figur 3.10: Från vänster: Zygalski, Różycki och Rejewski i castle Les Fouzes, Frankrike, trädgård 1941.

Den 22 juni 1940 delades Frankrike i två delar och de polska kryptologerna tvingades fly igen, denna gång söderut till det då ännu fria södra Frankrike (eng. Vichy France) figur 3.10 de tre polska kryptologerna.

I södra Frankrike hade polackerna tillgång till ytterst lite tysk korrespondens, inte alls i den mängd som krävdes för att kunna hjälpa de allierade med dekryptering. När de allierade invaderar Nord-Afrika den 8:e november 1943, rör sig tyskarna in i det område av Frankrike där de polska kryptologerna gömmer sig. De polska kryptologerna flyr till Spanien. De är bara två nu Różycki avled när ett transportskepp han var på sjönk 9:e januari 1942 på väg tillbaka till Frankrike från Nord-Afrika. När de anländer till Spanien[10] blir de tillfångatagna. De blir frisläppta efter ett antal dagar och blir sedan transporterade av ett brittiskt skepp till Storbritannien. Väl där, blir de engagerade att lösa tyska krypteringar, dock inte meddelanden krypterade med Enigma. Under resten av kriget rör inte Rejewski eller Zygalski Enigma meddelanden igen för att Storbritannien inte ansåg det nödvändigt [20].

[10]Spanien var vid det här skedet neutralt, men sympatiserande med Tyskland i kriget.

3.6 Efter kriget

Efter kriget återvände Rejewski till Polen, som 1 av de 20 000 soldater som återvände till Polen efter kriget. Omkring 200 000 soldater lämnade Polen under kriget. Rejewskis hemkomst blev inte sådan man väntat sig.

Rejewski och Zygalski fick båda av polska staten en liten summa pengar som belöning för sitt arbete med att lösa Enigma under kriget. Det dröjde dock ända tills 1973 förrän de blev erkända som de personer som faktiskt löst Enigma. Fram tills 1973 var det ytterst få som var medvetna om att Enigma blivit löst[11]. År 1973 försöker Storbritannien sedan påstå att Alan Turing var hjärnan bakom Enigma framgångarna i ett försök att få äran av att ha löst tyskarnas kryptering (USA var missnöjd av den anledningen att de tycker denna hemlighet avslöjades allt för tidigt). Det här är något som Frankrike och speciellt Polen är väldigt måna om att rätta till i världshistorien och ge äran åt rätta personer, dvs. de polska kryptologerna.

Rejewski arbetar ungefär 20 år efter kriget för olika företag med konsultuppdrag. Han ansåg själv att det inte var passande att söka efter en kryptologitjänst efter kriget. Dessutom hade han problem med att få anställning inom matematikfältet (han går inte in i detalj varför).

Zygalski blev kvar i London var han undervisade vid Battersea Technical College tills han dog år 1978 [20], [12].

3.7 Sammanfattaning

Fram tills krigets början i september 1939, var de tre polska kryptologernas insatser oerhört viktiga. Historiker har argumenterat att lösandet av Enigma förkortade kriget med ungefär två år, vilket i sin tur räddade otaliga människoliv. Det är viktigt att man inte glömmer bort de insatser dessa tre gjorde, inte bara för de allierade,

[11]Både Storbritannien och USA var måna om att hålla denna information hemlig, ifall att Tyskland skulle fortsätta använda maskinen, men även för att kunna sälja Enigma till andra länder och påstå att den var oknäckbar. Samtidigt som Storbritannien och USA kunde läsa meddelandena.

men även för området kryptologi. Innan andra världskriget var kryptologi något som ansågs bäst lämpat för linguister, eftersom att största delen chiffer var ordbytes chiffer, inte mekaniska chiffer, som Enigma. Detta ändrades när Rejewski med sin matematikutbildning kunde tillämpa strikta matematiska metoder för att lösa något som både Frankrike och britterna hade konstaterat vara "omöjligt att lösa".

Man kan spekulera över varför britterna inte ville att Rejewski och Zygalski skulle arbeta med Enigma när de anlänt till Storbritannien. Finns det vettiga anledningar för att inte låta dem arbeta med det? Enligt mig finns det inte det, förutom det faktum att britterna efter kriget från och med 1973 kunde påstå att Alan Turing, en engelsman, hade varit hjärnan bakom hela operationen. Som vi vet i dagens läge, fungerade denna brittiska taktik ett tag innan Rejewski och Zygalski äntligen fick den uppmärksamhet och ära som de förtjänar.

Kapitel 4

Lösandet av Enigma

Andra världskriget medför många förändringar, inte minst inom kryptografi. Under första världskriget var det linguister och personer som var bra på korsord och ord jakter som var ansvariga för att kryptera och dektryptera meddelande. När man talade om kryptering tänkte man inte på matematiker. Det visar sig att när maskiner som Enigma och mera komplicerade krypteringsmetoder uppfanns, ökade behovet av att ha matematiker inom kryptering som med sitt strikta matematiskt tillvägagångssätt kunde knäcka dessa koder (och skapa dem). Linguister använde sig allt som oftast av likheter mellan chiffertext och klartext, som t.ex. antalet gånger som en viss bokstav dyker upp i chiffertexten[1], man kan sedan gissa att denna bokstav motsvarar den mest använda bokstaven i det språk som klartexten är skriven i och fortsätta därifrån [7].

Enigma förhindrar frekvensanalys, eftersom en klartext bokstav oftast inte krypteras till samma chifferbokstav flera gånger. Detta innebar att de flesta av linguisternas metoder inte fungerade för att angripa Enigma. Speciellt polackerna insåg att det behövdes matematiker som kan tillämpa ett matematiskt tillvägagångssätt för att det ska gå att lösa Enigma. Detta leder till startande av en hemlig krypteringskurs vid universitetet i Poznań, Polen, varifrån *Marian Rejewski, Jerzy Różycki* och *Henryk Zygalski* anställs för att försöka lösa Enigma. Rejewskis tillvägagångssätt bygger på relativt grundläggande kunskap om permutationer och det räcker för att polackerna ska kunna rekonstruera tyskarnas rotorer och därmed hela Enigma [7].

[1] Frekvensanalys.

4.1 Tyska rotorkopplingar

Detta avsnitt bygger på arbete presenterat i bl.a. [2], [12], [13], [17], [20], [21], [23], [26], [15], [19].

Se bilaga B för ett mera djupgående exempel med alla mellansteg som utnyttjar min egen Enigmamaskin beskriven i Bilaga A.

I början av 1932 anställdes *Rejewski* för att lösa Enigma. Till sitt förfogande hade han tyska meddelanden, en kommerisiell Enigma, papper och penna. I slutet av år 1932 får Rejewski även tillgång till två kodlappar och en instruktionsbok med tillhörande krypteringsexempel som användes av tyskarna, och som kom från en fransk spion (Asché). Det är möjligt att det inte varit möjligt att lista ut Enigmas rotorkoppligar utan Aschés information (trots att Rejewski lär ska ha haft en metod som inte behövt kodlappar).

Rejewski noterar att de första sex bokstäverna i ett meddelande var en följd av tre bokstäver som krypterats två gånger i rad, dvs. meddelandenyckeln. Låt oss ta de sex bokstäverna från tre olika meddelanden (från [20], [2]):

$$dmq\ vbn$$

$$von\ puy$$

$$puc\ fmq$$

Vi kallar de olika krypteringarna A, B, C, D, E och F. Krypteringarna $A-F$ referera till transformationen från klartextbokstav till kryptotextbokstav, A krypterar den första bokstaven, B följande osv.

Det är viktigt att notera här att samma bokstav, betecknad med ?, har blivit krypterad två gånger, med rotorerna i olika positioner, $A :? \rightarrow d$ och $D :? \rightarrow v$, även B och E samt C och F krypterar samma klartextbokstav. Eftersom vi vet att Enigma är en krypterings- och dekrypteringsmaskin, betyder det att ifall man har Enigma inställd med kryptering A och sedan D och trycker på den kryptotextbokstav som finns i meddelandet på position ett respektive fyra, vet vi att de kommer att de-

krypteras till samma klartextbokstav, $d \rightarrow ?$ och $v \rightarrow ?$. Detta betyder att vi kan skriva $AD: \ d \rightarrow ? \rightarrow v$. Ty, ifall ? krypteras till d så måste d dekrypteras till ?. Dessutom, ifall vi börjar med d och får ? så kommer ? att bli v under förändring D. Alltså utför sammansättningen AD bytet:

$$AD: \ d \rightarrow v$$

Vi fortsätter enligt detta mönster och plockar kombinationer av bokstäver. Vi ser från det andra meddelandet att $AD: \ v \rightarrow ? \rightarrow p$. Vi har ett v i första meddelandet, så att:

$$AD: \ d \rightarrow v \rightarrow p$$

Slutligen med det tredje meddelandet:

$$AD: \ d \rightarrow v \rightarrow p \rightarrow f$$

Ett enklare skrivsätt är $AD = (dvpf)$. Med tillräckligt många meddelanden, ungefär 80 per dag, borde alla bokstäver dyka upp i alla sex positioner (i meddelandenyckeln) och man kan lista ut hur bokstäverna relaterar till varandra. Ifall vi har tillräckligt med meddelanden kan vi lista ut att AD har utseendet:

$$AD = (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s).$$

När man följer bokstäverna enligt vår metod så kommer vi förr eller senare att gå runt i cirkel. Se på första parentesen, den börjar med d och fortsätter man genom dem kommer man till o, och o kommer att bli till d enligt AD, vilket är varför vi slutar där och innesluter dem i parenteser. När vi har tillräckligt med meddelanden så kan vi bygga upp hur de olika sammansättningarna av operationerna AD, BE och CF ser ut. Alla bokstäver kommer att ha en annan bokstav, eller sig själv, som den förändras till. Nedan listas alla tre sammansättningar (från [20]):

$$\begin{aligned} AD &= (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s) \\ BE &= (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k) \\ CF &= (abviktjgfcqny)(duzrehlxwpsmo). \end{aligned} \tag{1}$$

Vi noterar att

- det finns ett jämnt antal permutationer[2]/förändringar i alla tre fall
- alla bokstäver i alfabetet finns med i sammansättningarna
- alla permutationer dyker upp parvis, dvs. det finns ett jämnt antal lika långa parenteser/permutationer.

Definition 1. *Vi definierar AD, BE och CF som ett meddelandes* ***karakteristiska struktur*** *(eng. characteristic structure) eller enbart meddelandets* ***karakteristik****.*

Definition 2. *Vi definierar en* ***permutation*** *som en bijektiv avbildning av en mängd M på sig själv. Permutationerna av M bildar en grupp $S(M)$ [18].*
I detta arbete refereras ofta till permutationer som "cykler".

Exempel 2. *En cykel* (2 4 5) *för mängden $M = \{1, 2, 3, 4, 5\}$ är ekvivalent med permutationen*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$$

eller skrivet med cykler, $(1)(2\ 4\ 5)(3)$*. Ifall vi har en cykel (i) där $i \in M$, kallar vi (i) för intentitetspermutation.*

Definition 3. *Vi definierar en* ***transposition*** *som en cykel med längden 2, dvs. en permutation som enbart byter ut två tal [18].*

Exempel 3. *En transposition* (2 5) *för mängden $M = \{1, 2, 3, 4, 5\}$ är ekvivalent med*

[2]Permutationerna är parenteserna ovan, och de beskriver hur man ska förändra en bokstav till en annan bokstav (eller sig själv).

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix},$$

eller med cykelbeteckning $(1)(2\ 5)(3)(4)$.

Det är även möjligt att ha flera transpositioner för en mängd, exempelvis $(2\ 5)(1\ 4)(3)$ *har två transpositioner för mängden* M.

Rejewski presenterade ett antal satser om hur cykler/permutationer uppför sig:

Sats 1. *Ifall två permutationer* X *och* Y *är av samma grad, har lika många element, och består enbart av disjunkta transponeringar, är antalet av disjunkta cykler med samma längd i produkten* XY *jämnt.*

Bevis. Låt $X = (a_1a_2)(a_3a_4)(a_5a_6)\dots(a_{2k-3}a_{2k-2})(a_{2k-1}a_{2k})$
och $Y = (a_2a_3)(a_4a_5)(a_6a_7)\dots(a_{2k-2}a_{2k-1})(a_{2k}a_1)$,

då är $XY = (a_1a_3a_5\dots a_{2k-3}a_{2k-1})(a_{2k}a_{2k-2}\dots a_6a_4a_2)$. □

Detta var den enkla delen. Vad Rejewski måste göra, var att faktorisera AD för att få enbart A och D. Han presenterar omvändningen till den ovanstående satsen:

Sats 2. *Om en permutation av jämn grad innehåller cykler av samma längd i ett jämnt antal, så kan denna permutation anses vara en produkt av två permutationer som består enbart av disjunkta transpositioner.*

Bevis. Detta är en direkt omvändning av det vi har ovan.

Givet $XY = (a_1a_3a_5\dots a_{2k-3}a_{2k-1})(a_{2k}a_{2k-2}\dots a_6a_4a_2)$,
så kan vi skriva $X = (a_1a_2)(a_3a_4)(a_5a_6)\dots(a_{2k-3}a_{2k-2})(a_{2k-1}a_{2k})$
och $Y = (a_2a_3)(a_4a_5)(a_6a_7)\dots(a_{2k-2}a_{2k-1})(a_{2k}a_1)$.

Vi observerar här att detta är enbart en av lösningarna. För ett allmänt bevis ska man flytta på elementen i XY:s ena cykel. Detta påverkar inte cykeln men det påverkar faktoriseringen

$$XY = (a_3a_5a_7 \dots a_{2k-3}a_{2k-1}a_1)(a_{2k}a_{2k-2} \dots a_6a_4a_2).$$

Detta ger faktoriseringen

$$X = (a_3a_2)(a_5a_4)(a_7a_6) \dots (a_{2k}a_{2k-4})(a_{2k-1}a_{2k-2})(a_1a_{2k})$$
$$Y = (a_2a_5)(a_4a_7) \dots (a_{2k-2}a_1)(a_{2k}a_3).$$

Man går sedan igenom alla k möjligheter för XY, där man flyttar elementen i den första cykeln.

För att bestämma den "rätta" faktoriseringen krävs mera information. □

Med dessa satser kunde Rejewski faktorisera AD, BE och CF till sina faktorer, dvs. förändringarna A, B, C, D, E, F, han kunde med andra ord lista ut vilken bokstav som en klartextbokstav skulle krypteras till, för dessa sex positioner. Dock ska här noteras att Rejewski inte beaktade kopplingsbordet, eftersom kopplingsbordet inte har inverkan på cykellängderna i permutationerna. Rejewski lyckades med andra ord ignorera kopplingsbordet och lösa ut karakteristikerna (och sedan Enigmas kopplingar) utan att bekymra sig över kopplingsbordets inverkan. (Detta är fascinerande, eftersom Tyskland satte mycket tillit till den säkerhet som kopplingsbordet medförde. Här har nu Rejewski lyckats förbise denna åtgärd.)

Rejewski presenterade även två följdsatser som baseras på beviset för Sats 1:

Följdsats 3. *Bokstäver som ligger i samma transposition av permutationer X eller Y, ligger alltid i två olika cykler av permutation XY.*

Följdsats 4. *Ifall två bokstäver som finns i två olika cykler av samma längd i permutationer XY hör till samma transposition, så hör bokstäverna bredvid (en till vänster, en till höger) också till samma transposition.*

Sats 5. *Om $H(i) = j$ dvs. $H = (\dots i\ j \dots)$; då är $T^{-1}HT = (\dots T(i)\ T(j) \dots)$. Detta implicerar att $H = (\dots i\ j \dots)$ samt $T^{-1}HT = (\dots T(i)\ T(j) \dots)$ har samma disjunkta cykel sammansättning.*

Bevis. Notera $T(i)(T^{-1}HT) = i(HT) = H(i)T = T(j)$.
Detta innebär att vi kan ordna permutationerna så att

$$H = (\dots i\ j \dots)$$
$$T^{-1}HT = (\dots T(i)\ T(j) \dots)$$

vilket beskriver permutationen T, där T består av två rader, dvs. en permutation [21]. □

4.1.1 Beräkningar med meddelandekarakteristikerna

Genom att använda sig av tyskarnas misstag/oförsiktighet att kryptera nyckeln (de tre bokstäverna) två gånger kunde Rejewski bestämma kopplingarna i rotorerna utgående från karakteristikerna AD, BE och CF. Nedan följer en genomgång om hur Rejewski gick till väga (se Bilaga B för en annan genomgång med alla mellansteg, [2]):

Vi kommer ihåg våra karakteristiker:

$$AD = (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)$$
$$BE = (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k)$$
$$CF = (abviktjgfcqny)(duzrehlxwpsmo)$$

Vi vill nu faktorisera dessa, ser först på AD och på dess cykler.
Två en-längds cykler:
Enligt Sats 2, ser vi att om $(a_1)(a_2)$ finns i XY så finns (a_1a_2) i X och (a_2a_1) i Y. Alltså, $(a)(s)$ finns i AD så (as) finns i både A och D.

Två två-längds cykler:
Igen enligt Sats 2, ifall $(a_1a_3)(a_4a_2)$ finns i XY så finns $(a_1a_2)(a_3a_4)$ i X och $(a_2a_3)(a_4a_1)$ i Y.
Två möjligheter: $AD = (bc)(rw)$ eller $AD = (bc)(wr)$, denna skillnad är inte viktig när vi enbart skriver ut kombinationen AD, men för faktorisering, betraktas de som **två olika möjligheter** och därmed:

A innehåller $(br)(cw)$ och D innehåller $(rc)(wb)$; **Eller**
A innehåller $(bw)(cr)$ och D innehåller $(wc)(rb)$

Slutligen de två tio-längds cyklerna:

Sats 2 ger oss för $(dvpfkxgzyo)(eijmunqlht)$ 10 olika möjligheter:

Ordning 1:

$$\begin{aligned} AD &= (dvpfkxgzyo)(eijmunqlht) \\ A &= (dt)(hv)(pl)(fq)(kn)(xu)(gm)(zj)(yi)(oe) \\ D &= (tv)(hp)(lf)(qk)(nx)(ug)(mz)(jy)(io)(ed) \end{aligned}$$

⋮

Ordning 3:

$$\begin{aligned} AD &= (dvpfkxgzyo)(jmunqlhtei) \\ A &= (di)(ve)(pt)(fh)(kl)(xq)(gn)(zu)(ym)(oj) \\ D &= (iv)(ep)(tf)(hk)(lx)(qg)(nz)(uy)(mo)(jd) \end{aligned}$$

⋮

Ordning 10:

$$\begin{aligned} AD &= (dvpfkxgzyo)(teijmunqlh) \\ A &= (dh)(vl)(pq)(fn)(ku)(xm)(gj)(zr)(ye)(ot) \\ D &= (hv)(lp)(qf)(nk)(ux)(mg)(jz)(iy)(eo)(td). \end{aligned}$$

Detta ger oss $1 \cdot 2 \cdot 10 = 20$ möjliga faktoriseringar av AD. Hur ska den rätta väljas?

Ifall de tyska singaloperatörena använt slumpmässigt genererade meddelandenycklar hade Rejewskis arbete varit betydligt svårare. Rejewski utförde välgrundade gissningar om operatörernas metoder, han antog att operatörer troligtvis väljer enkla nycklar, som t.ex. AAA, bokstäver som bildar diagonal på tangentbordet etc. Med dessa gissningar, och en tillräcklig mängd krypterade meddelanden, lyckades Rejewski sålla bort de faktoriseringar som inte ger korrekta lösningar och lyckades

avgöra de korrekta faktoriseringarna[3]:

$$A = (as)(br)(cw)(di)(ev)(fh)(gn)(jo)(kl)(my)(pt)(qx)(uz)$$
$$B = (ay)(bj)(ct)(dk)(ei)(fn)(gx)(hl)(mp)(ow)(qr)(su)(vz)$$
$$C = (ax)(bl)(cm)(dg)(ei)(fo)(hv)(ju)(kr)(np)(qs)(tz)(wy)$$
$$D = (as)(bw)(cr)(dj)(ep)(ft)(gq)(hk)(iv)(lx)(mo)(nz)(uy)$$
$$E = (ac)(bp)(dk)(ez)(fh)(gt)(io)(jl)(ms)(nq)(rv)(uw)(xy)$$
$$F = (aw)(bx)(co)(df)(ek)(gu)(hi)(jz)(lv)(mq)(ns)(py)(rt)$$

Vad betyder alltså dessa? Jo, Rejewski lyckades, utan att känna till rotorpositioner, startpositioner eller kopplingsbord, bestämma hur sex stycken på varandra följande positioner på Enigma krypterade en klartextbokstav till en chifferbokstav. Alla dessa kopplingar $A - F$ bestämmer ett bokstavspar, dvs. trycker man ner t.ex. a när transform A är inställd, så kommer s att ges ut, och vice versa. Försedd med dessa så hade Rejewski möjlighet att bestämma kopplingarna inne i den snabba (högra) rotorn.

4.1.2 Kopplingarna i högra (snabba) rotorn

Enigmas kryptering av en bokstav kan beskrivas som ett antal permutationer eller förändringar. Vi namnger nu alla de delar som utför en förändring på signalen.

S - Permutation som uppkommer av kopplingsbord.

L, M* och *N - Permutationer som uppkommer av de olika rotorerna, (L-vänster (långsamma), M-mitten N-höger (snabba)).

R - Permutation som reflektorn ger upphov till.

H - Permutation som ingångstrumman ger upphov till (i tyskarnas fall var denna ekvivalent med att multiplicera med en etta eller identitetsmatrisen, men inkluderar den för fullständighetens skull).

[3]Utför samma operationer på BE och CF som gjordes på AD.

Detta ger en krypteringsfunktion som kunde skrivas:

$$E(x) = SHNMLRL^{-1}M^{-1}H^{-1}S^{-1}(x)$$

Uppenbart att dekrypteringen är ekvivalent, eftersom Enigma fungerar som kryptering och dekrypteringsmaskin.
Krypteringsfunktionen är entydig för varje enskild rotorposition, ringinställning osv. Vi måste också beakta det att snabba rotorn svänger $\frac{1}{26}$ varv vid varje knapptryckning och i vissa fall även den mellersta och långsamma rotorn. Kalla denna rotation/förändring för P. P beaktar även de föränderliga kopplingarna inne i rotorn tillsammans med N (dvs. ringinställningarna).

$$\begin{aligned} P &= (abcdefghijklmnopqrstuvwxyz) \\ P^2 &= (acegikmoqsuwy)(bdfhjlnprtvxz) \\ &\vdots \end{aligned}$$

Vi skriver våra förändringar:

$$\begin{aligned} A &= SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1} \\ B &= SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1} \\ C &= SHP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^{-3}H^{-1}S^{-1} \\ D &= SHP^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4}H^{-1}S^{-1} \\ E &= SHP^5NP^{-5}MLRL^{-1}M^{-1}P^5N^{-1}P^{-5}H^{-1}S^{-1} \\ F &= SHP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1} \end{aligned}$$

Notera att här inte finns P-permutationer vid de andra rotorerna, enbart vid den högra (snabba) rotorn. Det är för att man kan anta att under dessa sex krypteringar så roterar enbart den snabba rotorn, och för 21 av 26 grundinställningar för den snabba rotorn är det sant, eftersom den mellersta rotorn inte hinner rotera. Med andra ord, det är ett helt acceptabelt antagande. Vi antar alltså att L, M är stationära och behöver ej permutationer P runt dessa rotorers förändringar.

Notera att $MLRL^{-1}M^{-1}$ finns i alla $A - F$, vi skriver

$$Q = MLRL^{-1}M^{-1}$$

Detta förenklar våra uttryck och lämnar oss med sex ekvationer:

$$\begin{aligned} A &= SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1} \\ &\vdots \\ F &= SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1} \end{aligned}$$

Obekanta är Q, S, H och N. Det kan anses vara möjligt att lösa denna typ av ekvationssystem med fyra obekanta och sex ekvationer, dock är det ännu till denna dag okänt ifall systemet är lösbart. Rejewski utvecklade en metod med vilken han trodde det var möjligt att lösa systemet, metoden var dock arbetsdryg och turligt nog behövde han aldrig använda den, istället utförde Rejewski förenklingar, samt utnyttjade information som en fransk spion (Asché) gav åt honom.

Rejewski antog att ingångstrumman, H, var känd och kunde därmed lägga den till vänstra sidan som en känd variabel. **Varför**?

Det visar sig att till skillnad från ingångstrumman i den kommerisiella Enigma, där H kastade om bokstäverna, ändrade tyskarna på H så att trumman inte utförde en förändring. Med andra ord, den finns bara där för att föra över signalen från tangentbordet (kopplingsbordet) till den högra rotorn (kan ses som identitetsmatrisen I). Rejewski gissade sig till detta efter flera misslyckade försök med andra ingångstrummor. Rejewskis gissning lönade sig, och gjorde H känd [20]. Denna gissning var så oväntad, och enkel att fransmännen och britterna aldrig funderade på det. Kryptologer från dessa länder (inkluderande Alan Turing) var chockerade när de fick reda på hur enkla ingångstrummans kopplingar var.

Nu var enbart Q, S och N okända och Rejewski behövde metoder för att lösa dem. Den 9 december 1932 fick Rejewski en tidig julklapp i och med att franska underrättelsetjänsten förmedlade *Hans-Thilo Schmidts (kodnamn: Asché)* kodlappar

och intruktionsbok (som han stulit från Tyskland) till Polen och vidare till Rejewski. Med hjälp av dessa två kodlappar (liknande som i figur 3.6) som täckte månaderna september och oktober år 1932 fick Rejewski reda på Enigmas grundinställningar, kopplingar för kopplingsbordet och ringinställningarna för dessa två månader. Det här var under tiden när tyskarna bytte rotorordningen var tredje månad. Dessa lappar var turligt nog i olika kvartal så Rejewski fick information som rörde två olika snabba rotorer. Med denna information kunde han att bestämma 26 kandidater för två av rotorerna (de två snabba) och från det, med hjälp av instruktionsboken, kunde han sedan bestämma rotorkopplingarna.

Rejewski kunde därmed anse permutationen S som känd eftersom den gavs på kodpappret,

$$S = (ap)(bl)(cz)(fh)(jk)(qu) \quad \text{ett exempel på kopplingar i kopplingsbordet [2].}$$

Eftersom han kände till kopplingarna hade han enbart Q och N kvar som obekanta. Uttryckena antar formerna:

$$\begin{aligned} P^{-1}H^{-1}S^{-1}ASHP &= NP^{-1}QPN^{-1} \\ P^{-2}H^{-1}S^{-1}BSHP^{2} &= NP^{-2}QP^{2}N^{-1} \\ &\vdots \\ P^{-6}H^{-1}S^{-1}FSHP^{6} &= NP^{-6}QON^{-1} \end{aligned} \tag{2}$$

För att förenkla beteckningarna så betecknar vi den vänstra (kända) sidan med $U - Z$:

$$\begin{aligned} U &= NP^{-1}QPN^{-1} \\ V &= NP^{-2}QP^{2}N^{-1} \\ &\vdots \\ Z &= NP^{-6}QP^{6}N^{-1} \end{aligned}$$

Vi kan nu, med våra kända variabler i $U - Z$ (vänstra sida), beräkna $U - Z$. Vi behöver egenligen enbart $U - X$, och dessa beräknas till:

$$\begin{aligned} U &= (ax)(bu)(ck)(dr)(ej)(fw)(gi)(lp)(ms)(nz)(oh)(qt)(vy) \\ V &= (ar)(bv)(co)(dh)(fl)(gk)(iz)(jp)(mn)(qy)(su)(tw)(xe) \\ W &= (as)(bz)(cp)(dq)(eo)(fw)(gj)(hl)(iy)(kr)(mu)(nt)(vx) \\ X &= (ap)(bf)(cu)(dv)(ei)(gr)(ho)(jn)(ky)(lx)(mz)(qs)(tw). \end{aligned}$$

Vi utför multiplikationer med två uttryck som följer efter varandra:

$$\begin{aligned} UV &= (NP^{-1}QPN^{-1})(NP^{-2}QP^2N^{-1}) = NP^{-1}(QP^{-1}QP)PN^{-1}(\star) \\ VW &= NP^{-2}(QP^{-1}QP)P^2N^{-1} \\ &\vdots \\ YZ &= NP^{-5}(QP^{-1}QP)P^5N^{-1}. \end{aligned}$$

Vi beräknar UV, VW och WX (igen med den vänsta (kända) sidan):

$$\begin{aligned} UV &= (aepftybsnikod)(rhcgzmuvqwljx) \\ VW &= (akjcevzydlwnu)(smtfhqibxopgr) \\ WX &= (aqvloikgnwbmc)(puzftjryehxds). \end{aligned}$$

Alla ekvationer har utrycket $(QP^{-1}QP)$ gemensamt. Vi löser det ur UV och sätter in i VW:

$$(QP^{-1}QP) = N^{-1}P(UV)P^{-1}N \quad \text{från ekvationen } UV\ (\star).$$

Vi sätter sedan in denna i VW, sedan från VW in i WX osv.:

$$\begin{aligned} VW &= NP^{-2}(QP^{-1}QP)P^2N^{-1} \\ &= NP^{-1}N^{-1}(NP^{-1}(QP^{-1}QP)PN^{-1})NPN^{-1} \\ &= NP^{-1}N^{-1}(\mathbf{UV})NPN^{-1} \\ &= (NPN^{-1})^{-1}(\mathbf{UV})(NPN^{-1}). \end{aligned}$$

Alla fyra får utseendena:

$$VW = NP^{-1}N^{-1}(UV)NPN^{-1}$$
$$WX = NP^{-1}N^{-1}(VW)NPN^{-1}$$
$$XY = NP^{-1}N^{-1}(WX)NPN^{-1}$$
$$YZ = NP^{-1}N^{-1}(XY)NPN^{-1}.$$

Vid det här laget finns det inte mycket kvar att göra, förutom att konstatera att VW kan fås från UV med en förändring NPN^{-1}. Vi skriver därför ut alla möjliga uttryck för VW, man får dussintals möjliga lösningar. Samma metod tillämpas för att få WXs möjligheter från VW. Man får igen ett dussintal av lösningar för NPN^{-1}. I dessa två transformationer: $UV \to VW$ och $VW \to WX$ finns ett gemensamt uttryck för NPN^{-1}. Detta gemensamma uttryck är vår lösning, och vi kan konstatera att de restrerande två transformationerna är överflödiga.

Med hjälp av uteslutningsmetoden, se bilaga B för detaljer, kom Rejewski fram till:

$$UV = (\mathbf{a}epft\mathbf{y}bsn\mathbf{i}kod)(rhcgzm\mathbf{u}vqwljx)$$
$$\frac{VW = (\mathbf{y}dlwn\mathbf{u}akj\mathbf{c}evz)(ibxopg\mathbf{r}smtfhq)}{VW = (\mathbf{y}dlwnu\mathbf{a}kj\mathbf{c}evz)(ibxopg\mathbf{r}smtfhq)}$$
$$WX = (\mathbf{u}zftjr\mathbf{y}eh\mathbf{x}dsp)(caqvlo\mathbf{i}kgnwbm).$$

Från dessa transformationer: $UV \to VW$ samt $VW \to WX$ följer vi bokstäverna (tjocka) och får att NPN^{-1} har formen:

$$NPN^{-1} = (\mathbf{ayuricx}qmgovskedzplfwtnjhb),\ [2].$$

Vi kan nu använda Sats 5 för att bestämma 26 olika versioner av N. En av dessa möjligheter är:

$$N = \begin{pmatrix} abcdefghijklmnopqrstuvwxyz \\ azfpotjyexnsiwkrhdmvclugbq \end{pmatrix}.$$

För att Rejewski skulle kunna välja korrekt uttryck för N behövde han kandidater för åtminstone en till rotor. Detta får han genom att utföra samma beräkningar för meddelanden från den andra månaden (eftersom en annan rotor då var den snabba). När Rejewski hade tillgång till kandidater för två olika rotorer kunde han gå igenom kretsen tills "stigar" som passade in hittades, och han finner samtidigt reflektorn och den sista rotorn [21]. Notera att Rejewski finner 26 stycken möjliga lösningar för de olika rotorerna och reflektorn, genom att gå igenom Enigma med sina olika kandidater. Han finner slutligen de korrekta rotorkopplingarna tack vare instruktionsboken som Asché tillhandahållit, eftersom där finns ett krypteringsexempel med alla inställningar för Enigma. Genom att följa detta exemepel kan han utesluta kopplingar som inte fungerar och har till slut endast ett alternativ kvar för varje rotor och reflektorn.

Därmed var Enigma löst! I Tabell 4.1 listas rotorernas kopplingar.

Därefter tillverkas polska Enigmor, dessa använde samma rotorer som den tyska. Vilket betydde att ifall polackerna lyckades lista ut vad de dagliga inställningarna var, kunde de dekryptera tyska meddelanden för den dagen.

Notera, att även om Rejewski inte hade haft tillgång till materialet från Asché, hade Rejewski fortfarande en teoretisk metod för att beräkna rotorkopplingarna [16]. Metoden anses fungera, men är ytterst arbetskrävande och det finns inga garantier för att man faktiskt lyckas lösa ekvationssystemet. Aschés insats kan därmed anses vara av stor betydelse [11]. Notera att även om Frankrike påstår att det var deras spion som gav informationen som möjliggjorde lösandet av Enigma, så hade fransmännen och britterna sett materialet och konstaterat att Enigma var omöjlig att lösa innan materialet skickades till Polen och Rejewski. Dessutom hade Rejewski en möjlig metod för lösandet av Enigma, med andra ord, materialet som fransmännen tillhandahöll var viktigt, men det var inte ensamt ansvarig för att knäcka Enigma.

Tabell 4.1: Tabell över kopplingarna i tyskarnas rotorer, och reflektorerna.

Rotor #	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Date Introduced	Model Name & Number
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ	1930	Enigma I
II	AJDKSIRUXBLHWTMCQGZNPYFVOE	1930	Enigma I
III	BDFHJLCPRTXVZNYEIWGAKMUSQO	1930	Enigma I
IV	ESOVPZJAYQUIRHXLNFTGKDCMWB	December 1938	M3 Army
V	VZBRGITYUPSDNHLXAWMJQOFECK	December 1938	M3 Army
VI	JPGVOUMFYQBENHZRDKASXLICTW	1939	M3 & M4 Naval (FEB 1942)
VII	NZJHGRCXMYSWBOUFAIVLPEKQDT	1939	M3 & M4 Naval (FEB 1942)
VIII	FKQHTLXOCBJSPDZRAMEWNIUYGV	1939	M3 & M4 Naval (FEB 1942)
Rotor #	**ABCDEFGHIJKLMNOPQRSTUVWXYZ**	**Date Introduced**	**Model Name & Number**
Beta	LEYJVCNIXWPBQMDRTAKZGFUHOS	Spring 1941	M4 R2
Gamma	FSOKANUERHMBTIYCWLQPZXVGJD	Spring 1942	M4 R2
Reflector A	EJMZALYXVBWFCRQUONTSPIKHGD		
Reflector B	YRUHQSLDPXNGOKMIEBFZCWVJAT		
Reflector C	FVPJIAOYEDRZXWGCTKUQSBNMHL		
Reflector B Thin	ENKQAUYWJICOPBLMDXZVFTHRGS	1940	M4 R1 (M3 + Thin)
Reflector C Thin	RDOBJNTKVEHMLFCWZAXGYIPSUQ	1940	M4 R1 (M3 + Thin)
ETW	ABCDEFGHIJKLMNOPQRSTUVWXYZ		Enigma I

4.2 Dagliga nycklar

Rejewski lyckades återskapa rotorkopplingarna inne i tyskarnas Enigma runt slutet av 1932, vartefter Polen lät tillverka ett antal egna Enigmor med tyska rotorkopplingar för att dekryptera de tyska meddelandena. Det som saknades var inställningarna för Enigma, dvs. ringpositionerna, rotorordningen, kopplingsbordet och grundinställningarna för rotorerna. Detta var nu nästa steg för kryptologerna. Alltså att uppfinna en metod med vars hjälp det var möjligt att inom en realistisk tidsram hitta de dagliga inställningarna. Krypteringsbyrån hade vid det här laget anställt personer vars enda uppgift var att sitta vid de polska Enigmorna och dekryptera tyska meddelanden, förutsatt att kryptologerna kunde tillhandahålla dagens inställningar.

En metod som Rejewski och hans kollegor tog fram var “rutnätmetoden” (eng. grid/grill method). Det var en arbetskrävande metod, som krävde stor koncentration, metoden tillhandahöll grundinställningarna, samt kopplingsbordets kopplingar

men ringinställningarna och rotorordningen måste bestämmas på annat sätt [12], [21], [2], [20], [23].

4.2.1 Rutnätsmetoden

Vid årsskiftet 1932-1933, efter att Rejewski listat ut rotorkopplingarna utvecklades rutnätsmetoden för att finna de dagliga inställningarna. Runt den här tiden använde tyskarna enbart sex sladdar på kopplingsbordet, 12 bokstäver bytte alltså plats av totalt 26 stycken. Med en tillräcklig mängd meddelanden från en dag, ca. 80 stycken, samt en gnutta tur gällande hur tyskarna kopplat sladdarna på kopplingsbordet och hur de valt meddelandenyckeln (ifall sladdarna var kopplade så att signalen från tangentbordet inte gick igenom sladdarna) kunde man genom jämförelse försöka lista ut de dagliga inställningarna med hjälp av denna metod. Detta försvårades dock när tyskarna ökade antalet sladdar.

Rejewski antog att S var identitetspermutationen. Med lite tur och operatörer som väljer meddelandenycklar så att bokstäverna inte går igenom kopplingsbordet, så är detta en acceptabel gissning. Vi kommer ihåg ekvationerna från (2) (sida. 54), lämnar bort H, ty den är identitetspermutationen I, och flyttar allt utom Q till vänster sida:

$$\begin{aligned}
(P^1N^{-1}P^{-1})S^{-1}AS(P^1NP^{-1}) &= Q \\
(P^2N^{-1}P^{-2})S^{-1}BS(P^2NP^{-2}) &= Q \\
(P^3N^{-1}P^{-3})S^{-1}CS(P^3NP^{-3}) &= Q \\
(P^4N^{-1}P^{-4})S^{-1}DS(P^4NP^{-4}) &= Q \\
(P^5N^{-1}P^{-5})S^{-1}ES(P^5NP^{-5}) &= Q \\
(P^6N^{-1}P^{-6})S^{-1}FS(P^6NP^{-6}) &= Q
\end{aligned} \tag{3}$$

Vi vet att alla dessa förändringar kommer efter varandra ty A, B, C etc. är efter varandra, samt antar att S är identitetsmatrisen (för de sex förändringarna $A - F$). Vi tar även i beaktande att mellan och långsamma rotorerna knappast är i grundpositionerna. Vi skriver:

$$\begin{aligned} P^x N^{-1} P^{-1} A P^x N P^{-x} &= Q \\ P^{x+1} N^{-1} P^{-x-1} B P^{x+1} x N P^{-x-1} &= Q \\ &\vdots \\ P^{x+5} N^{-1} P^{-x-5} F P^{x+5} N P^{-x-5} &= Q \end{aligned} \tag{4}$$

Här står x för startpositionen för rotor N. Utgå t.ex. från att $x = 1$ är grundinställningen, dvs. rotorn är inställd i positionen 1/A. Från detta ekvationssystem ser vi att alla dessa karakteristiker $A - F$ bör ge samma värde för Q. Dock existerar S och ifall man inte har tur och ingen av de upp till 12 bokstäver som används för krypteringen har en sladdkoppling, kommer Q inte att vara exakt samma för alla sex ekvationer. Det kommer att finnas likheter mellan de olika Q:na, så det gäller att hitta de positioner som för permutationerna $A - F$ ger liknande värden för Q. Det är ett väldigt arbetskrävande att utföra dessa kalkyler för hand, så Rejewski uppfann därför rutnätsmetoden (eng. grid/grill - method).

Rejewski skapade två papper, ett där han skrev alla möjliga permutationer $P^x N P^{-x},\ x = 0, \ldots, 25$, tabell 4.2 samt figur 4.1, för N (snabba rotorn) på följande sätt (detta är för den rotor Rejewski använder i [20] och antas vara den snabba rotorn):

Vi skriver ner alla former som N kan anta, totalt 31, de extra fem för att det ska vara möjligt att jämföra sex permutationer som kommer efter varandra. Det ska gå att undersöka oavsett vilken av rotorns 26 positioner den är i. Rejewski skapade ett sådant papper för alla tre rotorer, I-III (se figur 4.1 för exempel på rutnätsmetoden).

Det andra pappret, kallat rutnätet, har sex öppningar (eng. slits) och Rejewski skrev permutationerna $A - F$ under varandra, och skar ut en öppning under varje permutation.

Utrustad med detta verktyg, rutnätet, letar han efter likheter i alla sex permutationer $A - F$, figur 4.1. Med beaktande av ekvation (3) letade kryptologerna efter likheter i alla Q:n, denna metod fungerar men är tidkrävande samt kräver stor koncentration, eftersom sambanden ibland är svåra att hitta.

Vi undersöker nu exemplet i figur 4.1. Kryptologen känner till att i A byts $a \to s$,

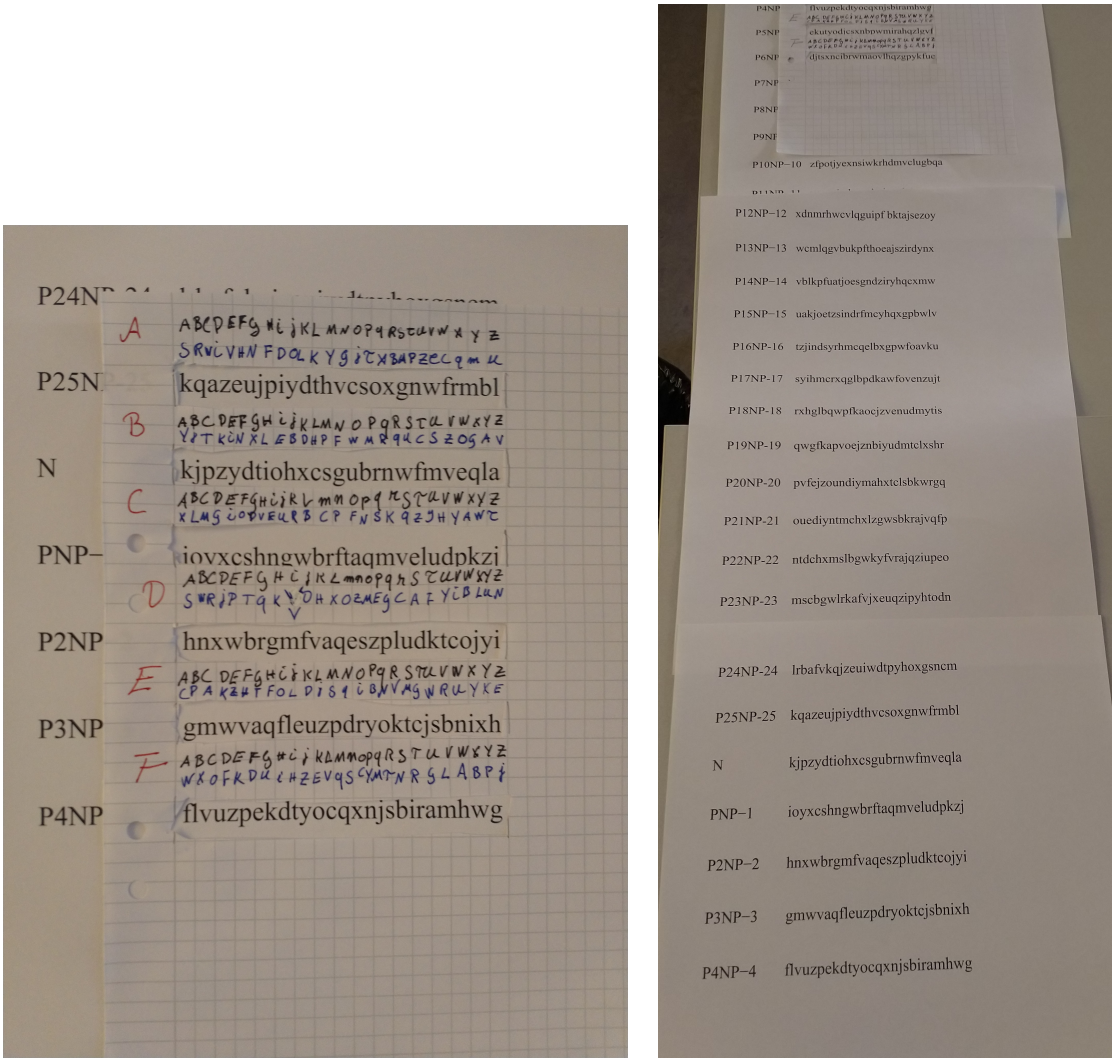
Tabell 4.2: Tabell där N permuterats 26 gånger.

N	$kjpzydtiohxcsgubrnwfmveqla$	$P^{16}NP^{-16}$	$tzjindsyrhmcqelbxgpwfoavku$
PNP^{-1}	$ioyxcshngwbrftaqmveludpkzj$	$P^{17}NP^{-17}$	$syihmcrxqglbpdkawfovenzujt$
P^2NP^{-2}	$hnxwbrgmfvaqeszpludktcojyi$	$P^{18}NP^{-18}$	$rxhglbqwpfkaocjzvenudmytis$
P^3NP^{-3}	$gmwvaqfleuzpdryoktcjsbnixh$	$P^{19}NP^{-19}$	$qwgfkapvoejznbiyudmtclxshr$
P^4NP^{-4}	$flvuzpekdtyocqxnjsbiramhwg$	$P^{20}NP^{-20}$	$pvfejzoundiymahxtclsbkwrgq$
P^5NP^{-5}	$ekutyodjcsxnbpwmirahqzlgvf$	$P^{21}NP^{-21}$	$ouediyntmchxlzgwsbkrajvqfp$
P^6NP^{-6}	$djtsxncibrwmaovlhqzgpykfue$	$P^{22}NP^{-22}$	$ntdchxmslbgwkyfvrajqziupeo$
P^7NP^{-7}	$cisrwmbhaqvlznukgpyfoxjetd$	$P^{23}NP^{-23}$	$mscbgwlrkafvjxeuqzipyhtodn$
P^8NP^{-8}	$bhrqvlagzpukymtjfoxenwidsc$	$P^{24}NP^{-24}$	$lrbafvkqjzeuiwdtpyhoxgsncm$
P^9NP^{-9}	$agqpukzfyotjxlsienwdmvhcrb$	$P^{25}NP^{-25}$	$kqazeujpiydthvcsoxgnwfrmbl$
$P^{10}NP^{-10}$	$zfpotjyexnsiwkrhdmvclugbqa$	P^0NP^{-0}	$kjpzydtiohxcsgubrnwfmveqla$
$P^{11}NP^{-11}$	$yeonsixdwmrhvjqgclubktfapz$	P^1NP^{-1}	$ioyxcshngwbrftaqmveludpkzj$
$P^{12}NP^{-12}$	$xdnmrhwcvlqguipfbktajsezoy$	P^2NP^{-2}	$gmwvaqfleuzpdryoktcjsbnixh$
$P^{13}NP^{-13}$	$wcmlqgvbukpfthoeajszirdynx$	P^3NP^{-3}	$gmwvaqfleuzpdryoktcjsbnixh$
$P^{14}NP^{-14}$	$vblkpfuatjoesgndziryhqcxmw$	P^4NP^{-4}	$flvuzpekdtyocqxnjsbiramhwg$
$P^{15}NP^{-15}$	$uakjoetzsindrfmcyhqxgpbwlv$		

dvs. $(a\ s)$. Dessutom vet kryptologen att rotorn byter $(a\ k)$, ty k finns under a i alfabetet (i första hålet för permutation A). Sedan, framgår det att rotorn kopplar ihop $(s\ g)$ (s från att permutation A byter ut a till s). Ifall vi kan bortse från kopplingsbordet för tillfället (dvs. hoppas att ingen av bokstäverna a, s, k eller g är kopplade) kan man säga att permutationen Q kopplar $(k\ g)$. Vi utnyttjar alltså det att A kopplar $(a\ s)$ och rotorn kopplar $(a\ k)$ och sedan vidare att rotorn kopplar $(s\ g)$.

För att Q ska kunna anses känd måste de sex permutationerna vara lika, dvs. sambandet $(s\ g)$ måste gälla i alla sex permutationer $A - F$. Vi ser nu på permutation B, B kopplar $(a\ y)$, och vi vet att rotorn kopplar $(a\ k)$. Vidare vet vi att rotorn kopplar $(y\ l)$. Vi säger då att permutation Q kopplar $(y\ l)$. Sedan fortätter vi på detta sätt tills antingen alla kopplingar är lika över $A - F$, eller en koppling som inte duger hittas.

För att undersöka om kopplingarna är lika, B kopplar $(u\ s)$ och rotorn kopplar $(u\ m)$



Figur 4.1: Exempel på rutnätsmetoden, alla möjliga startpositioner för en rotor N och sedan letar man efter mönster med rutnätet (rutiga pappret). Högra bilden visar de olika N efter varandra.

vidare kopplar rotorn $(s\ w)$. Detta stämmer inte överrens med den permutation Q som vi fick från A, därmed är detta inte rotorns positionen. Det är naturligtvis möjlight att antingen w eller g är kopplade med sladdar, i vilket fall det här kan vara en koppling. Uppenbart är att sladdarna och kopplingsbordet försvårade sökandet. Det är dock möjligt att bestämma Q på det här sättet, förutsatt att man har lite tur och tålamod, med erfarenhet blir detta också enklare och snabbare.

De två andra rotorernas startpositioner

När rutnätsmetoden ger ett bra förslag för Q, gäller det fortfarande för kryptologerna att bestämma startpositionerna för de andra två rotorerna. Rutnätsmetoden kan används när man kände till N (dvs. vet vilken rotor som var den snabba rotorn) för att bestämma dess startposition, samt kopplingsbordets kopplingar, kommer vi ihåg att Q skrevs som:

$$Q = P^y M P^{-y} P^z L P^{-z} R P^z L^{-1} P^{-z} P^y M^{-1} P^{-y},$$

där y och z beskriver positionerna för rotorerna M och L respektive. För att bestämma y och z hade kryptologerna inte många val, utan tvingades gå igenom alla de $26 \cdot 26 = 676$ startpositioner tills ett bra läge hittats. Dock var det inte slut här, eftersom rotorerna även hade en ringinställning, med vilken insidan av rotorn kunde roteras. Dessa måste också bestämmas av kryptologerna.

Kryptologerna kunde bestämma grundinställningarna för rotorerna genom att anta att ringkopplingarna var i grundläge, dvs. insidan var inte roterad, eftersom de hittills enbart beräknat samband mellan meddelandenycklens bokstäver och inte titat på själva meddelandet. När grundinställningarna är hittade, började Rejewski söka efter samband i de meddelanden som dekrypterats från tiden när kodlappar var tillgängliga. Av dessa meddelanden lärde sig Rejewski flera saker. Nämligen att de flesta meddelanden som skickades tenderade att börja med ANX, “an” är tyska för “till” (som i, “till löjtnant...”), X används som punkt eller mellanslag. När grundinställningarna var kända kunde Rejewski kontrollera ringinställningarna,genom att gå igenom alla 26 ringinställningar för de tre rotorerna tills “ANX” krypterades till de tre första bokstäverna i det infångade meddelandet (alternativt andra vägen, försöka dekryptera meddelandets första tre bokstäver tills “ANX” dök upp). Detta var tidkrävande och tråkigt arbete, så Rejewski och hans kollegor letade därför efter metoder för att förenkla arbetet.

Vi noterar att det var efter att grundinställningarna blivit kända och ringinställningarna

enbart återstår, som Rejewski och hans kollegor började utnyttja meddelandets innehåll. Fram till denna punkt hade de enbart använt matematisk teori för permutationer och cykler för att lista ut grundinställningarna för rotorerna, kopplingsbordet samt rotorkopplingarna från meddelandenyckeln. Ringställningarna krävde att Rejewski och hans kollegor utnyttjade det att tyskarna började de flesta meddelanden med "ANX". Kryptologerna utförde med andra ord en kändklartext attack för att bestämma ringinställningarna [20].

Katalog

Rejewski och hans kollegor tillbringade åren 1933-1935 med att förbättra sina metoder för att lista ut tyskarnas dagliga nycklar. Under de här åren utförde tyskarna i princip inga förändringar för hur Enigma användes och kryptologerna bestämde sig för att skapa en katalog för att snabbt kunna lista ut vad den dagliga nyckeln är.

Ifall kryptologerna lyckats lista ut grundpositionen för rotorn N med t.ex. rutnätsmetoden, kände de även till permutationen Q. Rejewski och hans kollegor tillverkade därför en katalog som bestod av de $6 \cdot 26^2 = 4056$ olika möjligheterna för Q. Detta gjorde det enklare och snabbare att finna grundpositionerna för de olika rotorerna, ty de kunde jämföra den permutation Q som hittats av rutnätsmetoden med de olika korten. Korten var markerade för de olika rotorordningarna, samt för alla olika grundinställningar.

Detta försnabbade en del av arbetet, men kryptologerna behövde fortfarande lista ut ringinställningarna. Även detta förenklades när Rejewski och hans kollegor noterade att om man kan anta att ett meddelande börjar med "ANX". Detta var troligt för åtminstone ett dussin olika meddelanden per dag, var det möjligt att utesluta många positioner för N, de positioner som omöjligt kunde resultera i den kryptotext som fångats in. Denna metod var effektiv i och med att den lyckades reducera antalet möjligheter till en handfull (runt ett dussin) (Rejewski har inte beskrivit hur dessa kalkyler utfördes [20]).

4.2.2 Klockmetoden

Under åren 1933-1935 utvecklade Różycki en metod, kallad klockmetoden (eng. clock method) [20], för att bestämma vilken rotor som var den snabba rotorn i ett meddelande. Denna metod hade inte stor användning förän 1935, då tyskarna började byta rotorordningen varje månad och slutligen varje dag[4], till skillnad från en gång var tredje månad. Metoden var den första som baserade sig enbart på linguistik och egenskaper hos det tyska språket. Före klockmetoden hade alla metoder byggt enbart på matematiska samband.

Metoden fungerar på följande sätt: man skriver två tyska texter under varandra t.ex.:

W	E	M	G	O	T	T	W	I	L	L	R	E	C	H	T	E	G	U	N	S	T	E	R	W	E
U	E	B	I	M	M	E	R	T	R	E	U	U	N	D	R	E	D	L	I	C	H	K	E	I	T

Różycki observerade att inom 26 bokstäver i båda texterna kunde man normalt hitta i medeltal två stycken kolonner som har samma bokstav, i exemplet ser man detta i positionerna 2 och 17. Denna egenskap kan även observeras ifall vi har två stycken kryptotexter som krypterats med samma nyckel. Ifall två olika nycklar har använts för skapandet av kryptotexterna dyker i medeltal enbart en kolonn med samma bokstav upp. Orsaken till detta kommer från egenskaper i det tyska språket [20], men med enbart 26 bokstäver är detta ej särskilt användbart. Ifall två meddelanden med minst 260 bokstäver är tillgängliga är det oftast möjligt att avgöra ifall de två meddelandena blivit krypterade med samma eller olika meddelandenycklar. **Varför är detta viktigt och intressant?**

Rejewski och hans kollegor kan antas ha tillgång till en stor mängd krypterade meddelanden varje dag. Av dessa är det sannolikt att ungefär ett dussin meddelande "par" kan hittas, där ett par består av två meddelanden vars meddelandenycklar har samma första två bokstäver och en annan tredje bokstav, exempel: ABC och ABD är två meddelandenycklar som uppfyller detta krav. Betraktar sedan dessa två meddelanden och skriver dem under varandra, på samma sätt som tidigare.

[4]Från 1 februari 1936 byttes rotorordningen varje månad; från och med 1 november 1936 byttes rotorordningen dagligen.

Vi skriver dem så att de bokstäver som krypterats av samma rotopositioner skrivs under varandra. Beroende på vilken rotor som var i den högra (snabba) positionen så kunde man skriva meddelandet på olika sätt. Alla rotorer hade bestämda och kända positioner för när de roterar följande rotor, dvs. vid vilken bokstav på den tidigare rotorn som även den följande rotorn kommer att rotera (hacken på rotorerna). Dessa var olika och man testade sig fram i klockmetoden genom att lägga meddelandena under varandra enligt var hacken på rotorerna fanns. Detta gjordes tills antalet kolonner med samma bokstav matchade den mängd man visste att indikerar samma krypteringsnyckel. När man hittat rätt antal kolonner mellan de två meddelandena kunde man vara väldigt säker på att man hittat vilken rotor som är i den högra (snabba) positionen.

Denna metod togs i bruk ordentligt först efter att tyskarna började byta rotorordning dagligen. Klockmetoden gav kryptologerna ett bra verktyg för att bestämma vilken rotor som var den snabba för dagen och skar därmed ner på antalet test de behövde göra, i och med att de kunde välja rätt papper för rutnätsmetoden på en gång. Därmed kunde de effektivt hitta Q och därefter kunde de använda katalogen.

4.2.3 Cyklometer

Den 1 augusti 1935 skapades ett nytt nätverk för det tyska flygvapnet och gradvis efter detta skapades fler och fler tyska nätverk för olika grenar av den tyska staten[5], alla använde samma Enigma men hade egna kodpapper och därmed egna dagliga inställningar. Denna ökning av nätverk ökade arbetsbördan för de polska kryptologerna som fick allt fler nätverk för vilka de dagliga nycklarna måste bestämmas. Utöver detta ändrade tyskarna antalet sladdar som användes i kopplingsbordet den 1 oktober 1936. Det fanns nu mellan fem och åtta sladdar. Då antalet sladdar ökade försvårades användandet av rutnätsmetoden, eftersom metoden fungerar bäst ifall man hade turen att hitta bokstäver som inte påverkats av kopplingsbordet. Klart att antalet bokstäver som inte påverkats sjönk och därmed försvårade arbetet med att finna permutationen Q [2], [13], [20].

[5]Armén, flottan, flygvapnet, SD osv.

Denna ökade arbetsbörda för Rejewski och hans kollegor fick dem att fundera ut alternativa metoder för att bestämma de dagliga nycklarna och de återvände till karakteristikerna AD, BE och CF och deras egenskaper, speciellt kan det nämnas att AD, BE och CF:s cykelsammansättning repeteras med ytterst låg frekvens och kan därmed användes som indikator för en dags nycklar (dvs. antalet och längderna av cykler i karakteristikerna var väldigt långt unika). Vi kommer ihåg uttrycket för AD:

$$AD = SPNP^{-1}QPN^{-1}P^3NP^{-1}QP^4N^{-1}P^{-4}S^{-1},$$

samt liknande uttryck för BE och CF. Rejewski noterade att permutation S, kopplingsbordet, enbart byter ut bokstavspar. Kopplingsbordet påverkar inte längden på de cykler som AD ger upphov till:

$$\begin{aligned} AD &= (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s) \\ BE &= (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k) \\ CF &= (abviktjgfcqny)(duzrehlxwpsmo). \end{aligned}$$

Denna uppsättning av cykler, längd och mängd, för en karakteristik är så gott som unik och detta utnyttjades för att skapa en katalog.

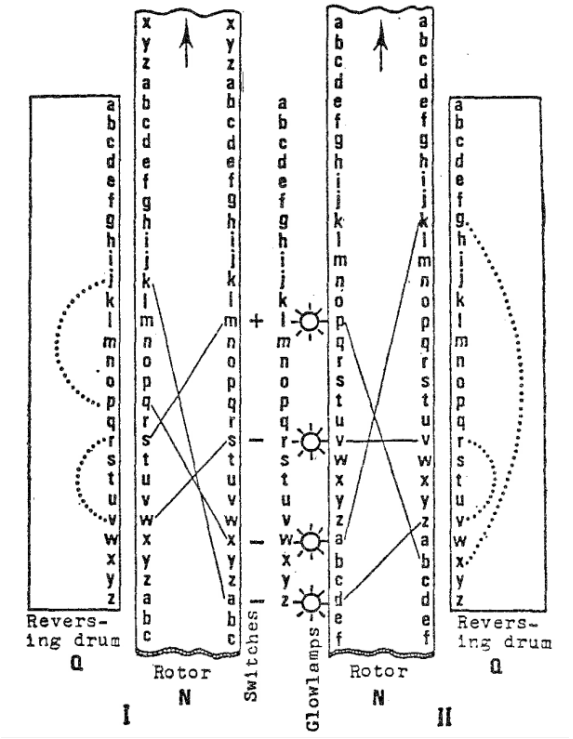
Här har AD två stycken tio-längdscykler, två stycken två-längdscykler samt två stycken en-längdscykler, permutationen S kommer inte att inverka på längden eller mängden av dessa cykler, enbart bokstäverna i dem. Rejewski och hans kollegor lät därför tillverka en maskin som de kallar cyklometer (se Figur 4.2) och med hjälp av denna cyklometer kunde kryptologerna snabbt bestämma längden samt antalet av cykler för en given rotor uppsättning. Cyklometern består av två uppsättningar av Enigma rotorer, i figur 4.2 uppe till vänster och höger, en lamppanel med knappar, samt en spänningsinställare. Rotorerna i cyklometern var insatta i samma ordning, den långsamma och mellersta rotorn var inställd på samma position och den snabba rotorn varierade med tre steg. Alltså i den ena uppsättningen var snabba rotorn inställd på 1/A och i andra uppsättningen var den inställd på 4/D för att representera

karkateristiken AD, där skillnaden också var tre steg.

Figur 4.2: Ett möjligt utseende för den polska cycklometern som Rejewski och hans kollegor utvecklade.

När maskinen var tillverkad så fungerade den som en "cykelvisare", dvs. man kunde ställa in den för alla olika rotorpositioner, samt rotorordningar, totalt: $6 \cdot 26^3 = 105\ 456$ inställningar. Rejewski och hans kollegor gjorde nu följande: de skapade 105 456 kort, ett kort för varje möjlig inställning för rotorerna samt rotorordningen. De gick sedan systematiskt igenom alla dessa positioner och skrev ner på det tillhörande kortet hur många cykler samt cyklernas längder för en specifik uppställning. Figur 4.3 ger en överblick över kopplingen i cyklometern. Tyvärr måste katalogen förstöras när tyskarna anföll Polen.

Figur 4.3 är ett diagram över hur ström passerade inuti cyklometern, Q står i figuren för reflektorn och rotorerna L och M för att förenkla diagrammet, i verkligheten var dessa tre åtskiljda. Se figur 4.4 för två på varandra följande positioner för rotorn N samt alla rotorer plus reflektorn. Vi ser i figur 4.3 två likadana uppställningar, en till vänster, markerad med I, samt en till höger, markerad med II, i mitten finns 26 stycken lampor, se figur 4.2. I diagrammet ser man ett litet + vid bokstaven l, bredvid en liten lampfigur. Detta + indikerar var man tryckt på en knapp för att låta ström gå genom kretsen. Maskinen fungerar genom att man väljer valfri bokstav och trycker ner knappen vid den bokstaven, ström kommer då att gå från den lampan, igenom de tre rotorerna, reflektorn och rotorerna igen, vartefter strömmen passerar från sida I till sida II. När strömmen flyttar till andra uppsättningen/sidan, passerar den mittersta delen (lampbordet), där den lyser upp en lampa, markerad med − r,w

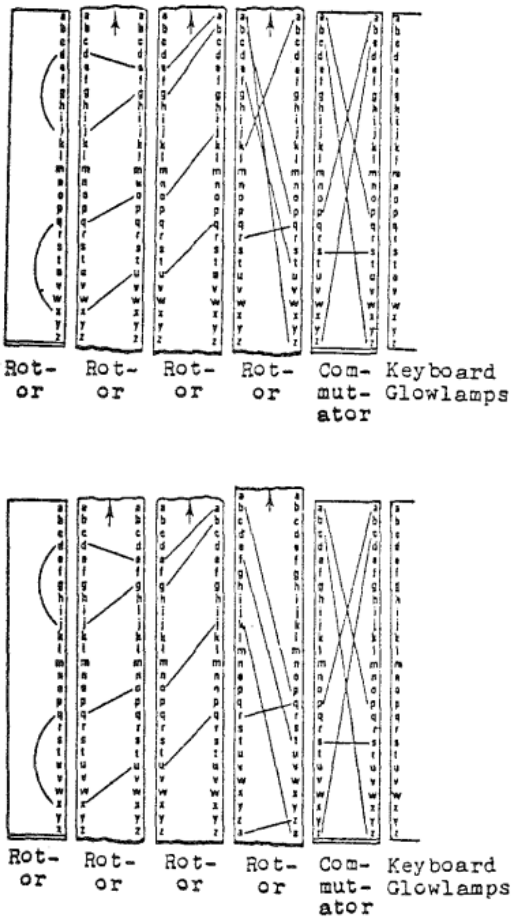


Figur 4.3: Diagram över kopplingarna i cyklometern.

och z i detta exempel.

Strömmen kommer att gå igenom cyklometern på detta sätt tills den återvänder till den bokstav man tryckte på, dvs. l, vartefter kretsen är sluten. Kryptologerna kunde räkna hur många lampor som tändes, i detta exempel fyra, antalet var alltid jämnt, och dessa fyra lampor berättar att denna specifika uppställning av rotorerna ger upphov till två stycken två-längdscykler. Kryptologerna markerade på kortet att den här Enigma uppställningen ger två stycken två-längdscykler, vartefter de släcker lamporna och tänder en lampa som inte varit tänd. Genom att gå igenom denna uppställning av rotorer så att alla 26 lampor lyst fick kryptologerna veta hur många och långa cyklerna var. Därefter roterar kryptologerna rotorerna så att nästa inställning kunde testas. Såhär gick kryptologerna igenom de 105 456 olika inställningarna och kunde katalogisera cykellängderna, samt mängden cykler för de olika inställningarna.

När Rejewski och hans kollegor efter ett års arbete katalogiserat alla cykellängder, tog det enbart 10-15 minuter att finna de dagliga inställningarna. Różyckis klock-



Figur 4.4: Diagram över den elektriska strömmen genom Enigma vid två efter varandra följande positioner för rotorn N.

metod angav vilken rotor som var i den snabba positionen och sedan jämfördes cykel längderna och antalen i AD, BE och CF med kortkatalogen. Från detta fann man sedan grundinställningen och permutationen S. Med hjälp av t.ex. ANX metoden kunde man bestämma ringinställningarna varefter man hittat de dagliga inställningarna för nätverket och kunde läsa Enigma meddelandena.

Dock gick allt detta arbete till spillo den 2 november 1937 när tyskarna bytte ut reflektorn A mot en ny reflektor B. Rejewski och hans kollegor måste lista ut kopplingarna i den nya reflektorn på samma sätt som tidigare, varefter kortkatalogen måste återskapas. Den andra gången var de skickligare och arbetet gick snabbare att utföra.

4.3 Meddelandenyckeln ändras

Cyklometern och kortkatalogen fungerade utmärkt fram till den 15:e september 1938, när tyskarna helt ändrade hur operatörerna använde Enigma. I kodlapparna fanns det inte längre en grundinställning för rotorerna, utan det var operatörens uppgift att välja startposition för rotorerna. Denna position sattes sedan i början av meddelandet i klartext, vartefter operatören ställde in Enigma till denna startposition, valde ut en **ny** startposition som krypterades två gånger. Sedan ställde operatören in Enigma till denna nya startposition och krypterade meddelandet [20], [21].

För att lista ut startpositionen måste mottagaren ställa in sin Enigma till den position som de tre okrypterade bokstäverna visar, varefter hen kunde dekryptera den riktiga meddelandenyckel. Sedan ställa om Enigma till denna startposition och slutligen dekryptera meddelandet.

Exempel 4. *En operatör får sin kodlapp och ställer in Enigma enligt den, hen väljer sedan tre bokstäver TFF, ställer in de tre rotorerna till dessa positioner. Operatören väljer nu tre nya bokstäver t.ex. EWQ som hen krypterar från postition TFF.*

Låt oss säga att EWQ krypteras till TUI samt BTY. Operatören ställer sedan in sin Enigma på position EWQ och krypterar sitt meddelande. Meddelandet som skickas har nu TFF, TUI BTY i början och den krypterade texten kommer efter.

Skillanden ligger här i att alla meddelanden utgick från olika grundinställningar på rotorerna, tidigare hade alla meddelanden för en specifik dag börjat från t.ex. TDS, och nu var alla meddelanden krypterade utgående från olika grundinställningar. Det existerar dock fortfarande ett samband mellan den första och fjärde, andra och femte samt tredje och sjätte krypterade bokstaven i meddelandenyckeln. Rejewski och hans kollegor måste nu uppfinna nya metoder för att kunna knäcka detta nya sätt att skicka meddelandenycklar. Två metoder för att göra detta utvecklades runt samma tid. De var Zygalskipapper (eng. Zygalski Sheets), utvecklade av Henryck Zygalski, samt den kryptologiska bomben (avsnitt 4.3.2).

4.3.1 Zygalski papper

Låt oss i tabell 4.3 lista ett antal (tio) meddelandenycklar, där den okrypterade och den krypterade delen separeras med ett kommatecken:

Tabell 4.3: En tabell med tio meddelandenycklar där samma bokstav dyker upp i första och fjärde, andra och femte eller tredje och sjätte positionerna, [20].

KLT, $WO\mathbf{C}\ DR\mathbf{C}$	GRA, $F\mathbf{D}RY\mathbf{D}P$
SVW, $D\mathbf{K}RI\mathbf{K}C$	MDO, $CT\mathbf{W}\ YZ\mathbf{W}$
BWK, $\mathbf{T}CL\ \mathbf{T}SD$	AGH, $SL\mathbf{M}\ PZ\mathbf{M}$
EDV, $P\mathbf{R}S\ Z\mathbf{R}T$	JBR, $LP\mathbf{S}\ TO\mathbf{S}$
GRN, $\mathbf{U}ST\ \mathbf{U}QA$	ITY, $A\mathbf{P}O\ Z\mathbf{P}D$

Vi kommer ihåg från ekvation (1) (sida. 46) gällande karakteristikerna för en inställning att ifall samma bokstav finns i position ett och fyra, två och fem eller tre och sex (se de tjocka bokstäverna i tabell 4.3). Dessa indikerar en cykel av längd ett, dvs. i karakteristiken AD finns en cykel av stilen (t), från tredje raden i vänstra kolonnen i tabell 4.3. Genom att minnas att permutationen S, som uppkommer av kopplingsbordet, inte påverkar längderna av cyklerna utan enbart bokstäverna i dem, behövde Rejewski och hans kollegor tillverka en katalog som listar alla karakteristiker som innehåller en cykel av längden ett, för att sedan jämföra dessa med nycklarna från tyskarnas meddelanden för att avgöra grundinställningarna. Grundinställningarna för rotorern från vilken man krypterade meddelandenyckeln var känd, ty den placerades i klartext i början av meddelandet. Dock skulle jämförandet av en-längds cykler kräva att man gick igenom alla $26^3 = 17\ 576$ positioner genom att enbart klicka på den bokstav som dök upp i krypterade meddelandenyckeln, tills samma klartext bokstav dök upp tre gånger, vilket är ytterst tidskrävande. Henryck Zygalski kom på ett annat sätt att utföra denna kontroll.

Zygalski kom med förslaget att låta tillverka papper med hål på specifika platser som representerar existensen av en-längdscykler, se figur 4.5 för exempel på ett sådant papper. Det var nödvändigt att tillverka ett knippe papper för varje rotor kombination, dvs. 6 kippen totalt, där varje knippe innehöll 26 papper, ett papper stod för en rotorkombination samt för den **långsamma** (vänstra) rotorns startposition.

Pappret delades in i fyra likadana rektanglar, där $x-$axeln stod för positionen som den mellersta rotorn var i och $y-$axeln stod för positionen den snabba (högra) rotorn var i. Hål skulle sedan göras i pappret för de rotorpositioner där en-längdscykel existerade.

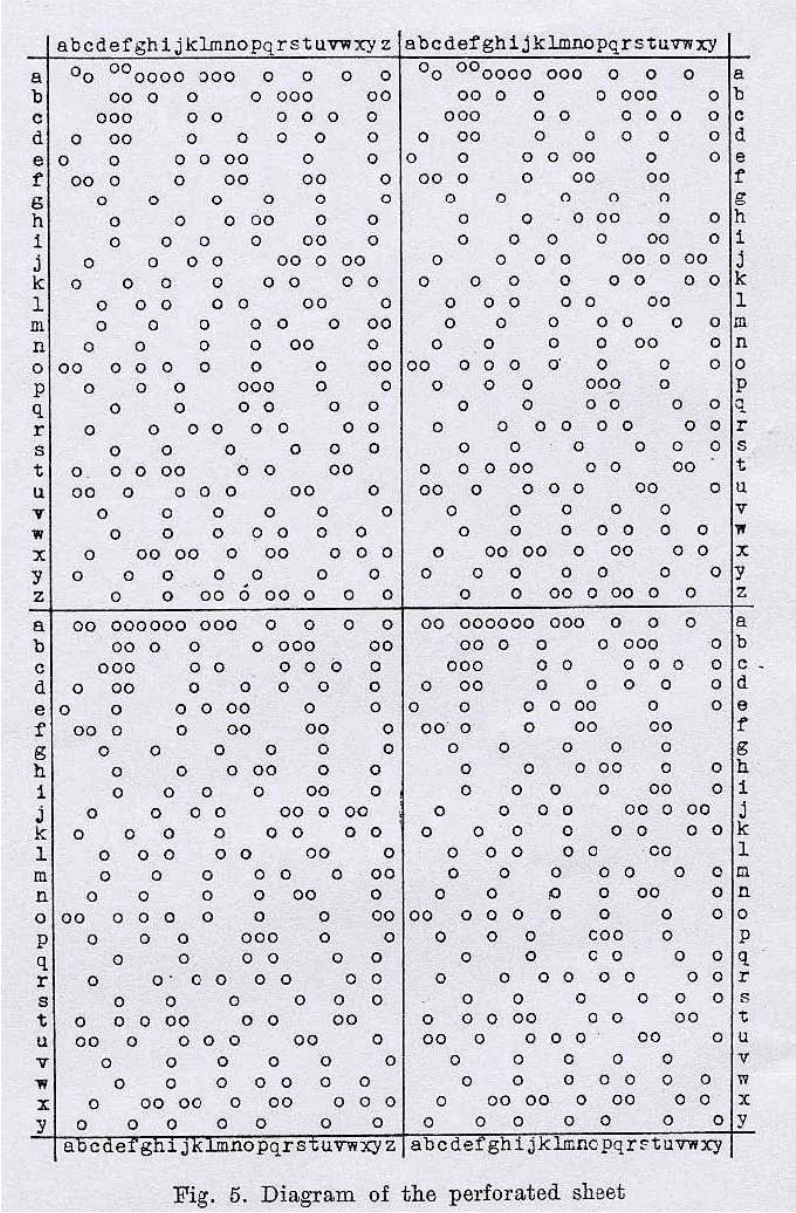


Fig. 5. Diagram of the perforated sheet

Figur 4.5: Bild av ett Zygalski papper, hålen visar var en-längds cykler dök upp.

Arbetet med att göra upp dessa papper var krävande och tog lång tid, eftersom kryptologerna utförde detta arbete samtidigt som de letade efter de dagliga nycklarna med metoder som rutnätsmetoden etc. Varje papper skulle ha runt 1000 noggrant utsatta hål och totalt måste $6 \cdot 26^2 = 156$ papper göras. När pappren var klara, skulle

man lägga pappren ovanpå varandra enligt noggranna beräkningar. Ifall man hade tillräckligt med information och kunde lägga pappren på varandra korrekt försvann så småningom alla utom ett fåtal hål, som syntes genom alla papper. Från dessa kunde man sedan beräkna permutationen S, ringinställningarna för rotorerna, dvs. all den information som behövdes för att kunna bestämma den dagliga nyckeln.

Det visar sig dock att arbetet var för stort för de tre kryptologerna eftersom den 15:e december 1938 (då Tyskland implementerade två nya rotorer, så att man valde tre från fem) var enbart två knippen av dessa papper klara. Med implementationen av dessa två nya rotorer ökade antalet knippen som måste tillverkas, från sex till 60, dvs. totalt $60 \cdot 26^2 = 40\ 560$ ark behövde tillverkas. För de tre kryptologerna var detta för mycket, och kort efter implementationen av dessa två nya rotorer delar polackerna med sig av sina framgångar inom Enigma med sina allierade, Frankrike och Storbritannien. Detta gav dem möjlighet att börja lösa och läsa Enigma meddelanden. Polen ger även båda allierade två stycken polska Enigma var.

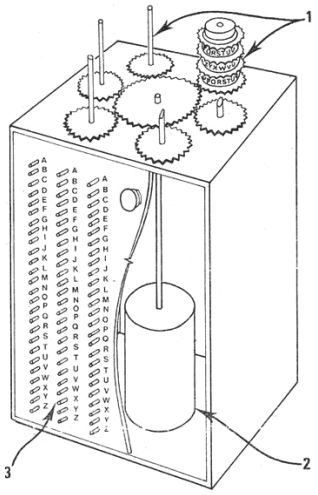
De polska kryptologerna kommer senare i Frankrike att få 60 knippen av Zygalski papper från Storbritannien, som hade resurser att engagera personal för skapandet av dessa papper.

4.3.2 Kryptologisk bomb

Zygalskipappren var den ena metoden som utvecklades för att kontra tyskarnas nya metod för skickande av meddelandenycklar. Den andra var mera mekanisk och handlar om att med "brute-force" metoden finna de dagliga nycklarna utgående från meddelandenycklar som de i tabell 4.3. Med andra ord gick metoden ut på att gå igenom alla möjliga grundinställningar för rotorerna tills ett bra läge hittades. (Ett bra läga indikerades ifall samma lampa lystes upp på lamppanelen tre gånger i rad då samma bokstav trycktes ner.)

Arbetet med att mekaniskt och för hand leta efter korrekta grundinställningar var klart tråkigt och jobbigt samt tidskrävande. Rejewski och hans kollegor kom därför på ett sätt att snabba på arbetet nämligen de uppfann den krypologiska bomben,

figur 4.6. Den kryptologiska bombens uppgift var att automatiskt gå igenom alla möjliga grundinställningar och meddela när den hittat ett läge som får samma lampa att lysa upp tre gånger i rad. Bomben är i grund och botten sex knippen av tre rotorer, egentligen sex Enigmor, som alla samtidigt snurrar på och undersöker kopplingar. Alla knippen med rotorer var i olika ordning för att representera att rotorerna kunde ordnas på sex stycken olika sätt. Sex sådana maskiner beställdes för att smidigt kunna testa alla ordningar på en gång. Med hjälp av den här maskinen sjönk den tid som krävdes för att hitta de dagliga nycklarna till ungefär 2 timmar, i vissa fall till och med snabbare, ifall man hade tur. Denna utvecklades samtidigt som Zygalskis papper [20], [21].



Figur 4.6: Bild av en polsk kryptologisk bomb, endast en rotorkombination syns här.

Från meddelandenyckelns klartext del, vet man vad grundinställningarna för de olika rotorerna var. Användande av t.ex. klockmetoden kan avslöja vilken rotor som är i första positionen, men i övrigt känner man ej till rotorernas ordning. Vidare känner man enbart till den yttre inställningen för rotorerna ty ringinställningarna för rotorerna var okända. När kryptologerna kännde till det relativt avstånd mellan de olika rotorerna, dvs. man visste vilka positioner de olika rotorerna var i, samt hur stort avstånd var mellan dem. Med hjälp av denna bomb, figur 4.6, kunde Rejewski och hans kollegor köra igenom alla 26^3 olika möjliga ringinställningnar samtidigt som det relativa avståndet för yttre sidan av Enigma rotorn hölls konstant.

Kopplingsbordets effekt på krypteringen ignorerades på grund av att ifall man hade tillräckligt, ca 100 meddelande [5], kunde man i vissa fall anta att en bokstav var oförändrad med tillräckligt stor sannolikhet. Speciellt om man fann nycklar med följande utseende:

$$RJT, \mathbf{W}AH\ \mathbf{W}IK$$

$$DQW, D\mathbf{W}J\ M\mathbf{W}R$$

$$HPN, RA\mathbf{W}\ KT\mathbf{W}$$

Ifall en bokstav, W i det här fallet, kunde hittas i samma position bland de första tre samt sista tre bokstäverna, kunde man med stor säkerhet säga att bokstaven W inte påverkades av kopplingsbordet och var därmed en en-längdscykel. Från detta satte man upp maskinen för att testa sig fram, genom att t.ex. testa bokstaven W tre gånger i rad. Ifall samma lampa lystes upp tre gånger, var man ganska säker på att man hittat grundpositionen för den dagen och man kunde lista ut all information för den dagen. Noggranna beskrivningar över bomben finns inte kvar, men [5] försöker presentera en möjlig uppbyggnad av bomben. Författaren anseratt bomben istället för att lysa upp samma tre lampor var kopplad så att en lampa lystes upp enbart ifall alla tre "nedtryckningar" av W lyckades sluta en strömkrets. Båda versionerna är ungefär lika sannolika och det är inte möjligt att säga vilken som definitivt är rätt.

Kapitel 5

Storbritanniens insatser

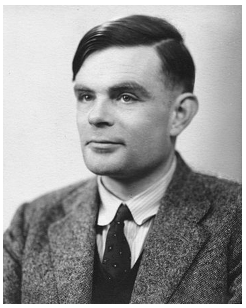
Hittills har enbart polska matematiker och Polens framgångar diskuterats, och även om det var polackerna som gjorde det möjligt att läsa Enigma meddelanden genom att bestämma rotorkopplingarna. Var det Storbritannien (och i viss mån USA) med sina cirka 10 000 anställda vid Bletchley Park[1] [25], som drog det tyngsta lasset när det kom till att kriga emot Tyskland på kryptografifronten under kriget. Därför ska vi också kort bekanta oss med två brittiska matematiker som var viktiga för krigsinsatserna, *Alan Turing*[2] och *Gordon Welchman*[3], [24], [4].

Dessa två är kanske de mest kända från Bletchley Park och överlag mest kända från andra världskriget som kryptologer. Dock bör man komma ihåg att utan alla män och kvinnor som arbetade dag och natt i Bletchley Park (och andra platser), kunde kriget dragit ut i upp till två år (om inte mera) till. Men tack vare dessa personer och deras insatser kunde de allierade förse sig med information om vad Tyskland ämnade göra och därmed förbereda sig för attackerna och lida lindrigare förluster eller vinna större vinster.

[1] Platsen där kryptologerna arbetade i Storbritannien, norr om London.
[2] Alan Turing, 1912-1954, `https://www.britannica.com/biography/Alan-Turing`.
[3] Gordon Welchman, 1906-1985, `https://bletchleypark.org.uk/roll-of-honour/9590`.

5.1 Alan Turing

Alan Mathison Turing föddes den 23:e juni 1912 i London och dog den 7:e juni 1954 i sitt hem i Wilmslow, Cheshire. Turing var en matematiker men tillförde även forskning och idéer till områden som: *logik, biologi, filosofi, kryptoanalys, datorvetenskap, artificiell inteligens* samt *artificiellt liv.* Turing utbildade sig först vid "Sherborne School" i Dorset, varefter han studerade matematik vid "King's College" i Oxford 1931. Turing utexaminerades år 1934.



Figur 5.1: Alan Turing.

Redan vid en ålder av 23 år, 1936, presenterade Turing ett av sitt livs viktigaste teoretiska arbeten, "On Computable Numbers, with an Application to the Entscheidungsproblem [eng. Decision Problem]", fritt översatt "Arbete med kalkylerbara tal som har en tillämpning inom beslutsproblem". Detta arbete lade grunden för den moderna datorn, och efter kriget arbetade Turing med att utveckla en dator baserad på detta arbete [4].

Turing tillbringade två år i USA, 1936-1938, där han avlade en doktorsexamen med ett arbete med rubriken "Systems of Logic Based on Ordinals". I detta arbete, samt i kommade arbeten, fortsatte Turing utveckla den teori som han presenterat i "On Computable Numbers". Han studerade och beskrev problem som ansågs "för svåra" även om man hade tillgång till en maskin med oändligt minne och tid.

Kort före kriget bryter ut i september 1939, flyttas Turing till Bletchley Park, där "Government Code and Cypher School" (GC och CS) håller till. Turings arbete i Bletchley park är ytterst viktigt, eftersom Turing, med hjälp av Gordon Welchman (och de polska kryptologerna), lyckas utveckla en metod för att knäcka den tyska flottans Enigma. Den tyska flottans krypteringar var den i särklass svåraste att knäcka, inte enbart för att flottan använde sig av flera rotorer än resten av tyska staten[4], utan också för att de använde sig av dubbelkryptering och andra knep för att försvåra de allierades arbete.

[4]De valde fyra rotorer av åtta.

Efter att kriget är över, arbetar Turing för bland annat "National Physical Laboratory" där han och ett forskarlag har i uppgift att utveckla Turings forskning för att försöka skapa den första "moderna datorn".

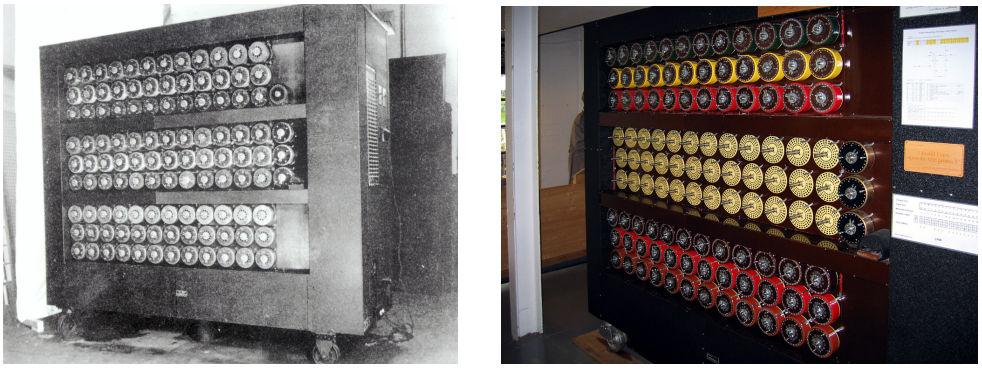
5.1.1 Turings maskin "Bomben"

De polska kryptologerna *Marian Rejewski, Henryk Zygalski* och *Jerzy Różyck* hade tillverkat en metod för att lista ut och lösa de dagliga Enigma nycklarna som de delade med britterna i mitten av 1939. De polska metoderna, cyklometern, Zyglaski pappren etc. byggde på att avlyssnarna attackerade själva meddelandenyckeln och sambanden bland karakteristikerna. Turing insåg att denna metod var ineffektiv. I och med att det var en relativt enkel sak för tyskarna att ändra metoderna med vilka de skickar meddelandenycklar. Tyskarna hade redan gjort detta år 1938, när de började skicka klartext meddelandenyckeln åtföljt av den krypterade materialet (se avsnitt 3.4) vilket hade den effekten att polackernas metoder blev värdelösa och måste återskapas eller uppfinnas helt på nytt. Turing insåg att tyskarna när som helst kunde göra förändringar på nytt och utvecklade därför en metod som var oberoende av hur tyskarna skickade meddelandenycklar.

Turings metod baserade sig på "antagen text", dvs. kryptologerna i Bletchley Park gissade vad tyskarna hade krypterat, försökte passa in denna gissning i kryptotexten och använde sedan en brittisk "bomb", Bombe, som effektivt kunde köra igenom en stor mängd Enigma inställningar. Bombe finner slutligen den inställning som gav upphov till korrekt kryptotext. Maskinen gav i vissa fall upphov till flera möjliga inställningar, men dessa gick att snabbt kontrollera manuellt av de anställda kryptologerna [4].

Turings maskin, figur 5.2, tog flera månader att bygga och först i augusti 1940 anlände den första Turing "bomben" till Bletchley Park. Under krigets gång tillverkades ca. 210 bomber för GC och CS. Dessa maskiner fungerade genom att de roterande rotorerna som var monterade på bomben snurrade med ungefär 50,4 varv per minut. Rotorerna var kopplade så att de hela tiden försöka sluta en strömkrets i

maskinen. Låt oss säga att vi har kryptobokstaven 'B', och vi antar att den dekrypteras till klartextbokstaven 'K'. Bombe körde igenom Enigmas olika inställningar och ignorerade dem som inte klarade av att ta kryptobokstaven och dekryptera den till rätt klartextbokstav (eller andra vägen). På detta sätt kunde man med Bombes hjälp ignorera tusentals Enigma inställningar, dvs. de som inte gav rätt klartextbokstav. När maskinen klarade av att sluta strömkretsen, stannade maskinen, inställningen för Enigma skrevs ner, maskinen startades på nytt och någon kontrollerade ifall tyska meddelanden dekrypterades till "vettiga" klartext meddelanden. Ifall man lyckades dekryptera ett helt meddelande hade rätt Enigma inställningar hittats och maskinen ställdes in för att användes på ett annat nätverk. På det här sättet hittades oftast alla nätverks dagliga inställningar, och britternas kunde läsa tyska meddelanden lika enkelt som de tyska kunde, efter att nyckeln hittats.



Figur 5.2: Alan Turings "Bombe" som användes i Bletchley Park under kriget i svartvit och i färg.

Meddelandena som britterna fångade upp var oftast relevanta endast för en kort tid, dvs. meddelandena som fångades upp kanske beskrev en attack som var på väg att hända ganska snart. Därför var det av stor vikt att kryptologerna kunde snabbt lista ut vad den dagliga inställningen för Enigma var för att kunna utnyttja informationen i tid.

Man kan notera här att ifall tyskarna följt uppmaningarna om att skicka enbart korta meddelanden, så hade britterna haft svårare att hitta bra gissningar att jämföra med kryptotexten, eftersom det funnits färre tecken i meddelandena.

Gissning av krypterad text

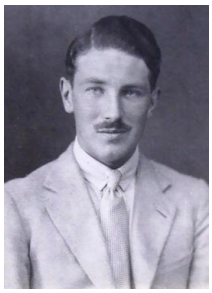
Till skillnad från de polska kryptologerna, använde Turing gissad, antagen eller till och med känd klartext för att hitta de dagliga nycklarna. Denna klartexts gissning kallades för "crib" eller "cribs" och var t.ex. *en hälsningsfras, meddelande innehåll* eller *rubriken för ett meddelande*. En vanlig "crib" var *Wetterbericht* - väderleksrapport, eller rapporter från fältet efter en drabbning ty då kunde man anta att signalisterna som var med i drabbningen skickade meddelande om vad som skett. Om t.ex. Tyskland klarat av att förstöra en storbritannisk tank eller dylikt, kunde kryptologerna anta att information om detta skulle finnas i meddelandet.

När en bra "crib" hittats, var det dags att hitta en plats i meddelandet där den passade in. Som tidigare nämnts i denna avhandling, kunde Enigma aldrig kryptera en bokstav till sig själv, kryptologerna gick igenom hela det infångade tyska meddelandet och letade efter en plats där t.ex. *wetterbericht* passade in utan att en bokstav blev till sig själv. Detta gjordes genom att skapa två pappersremsor, ett med meddelandet (i krypterad form) och ett annat med endast "crib":en på, sedan flyttades ordremsan under meddelanderemsan tills en bra plats hittades, dvs. där ingen bokstav krypterades till sig själv.

När en bra plats hittats, tar man bokstäverna, kanske W blev till ett T osv. Detta matades sedan in i Bomben, som kontrollerade alla Enigmas inställningar och stannade till när ett W krypterades till T. Dessa relativt få möjligheter kontrollerades sedan för hand och ganska snabbt kunde därmed rätt inställning hittas.

5.2 Gordon Welchman

Gordon Welchman föddes 15 juni 1906 i Bristol, England och dog 8 oktober 1985 i Newburyport, Massachusetts, USA, [24]. Fram till år 1925 arbetade Welchman som en präst och missionär för den engelska kyrkan "Church of England", samt som en ansvarsperson för prästskapet i Bristol.



Figur 5.3: Gordon Welchman.

Welchman bytte inriktning runt år 1925, i och med att han började studera matematik vid "Trinity College", Camebridge. Han studerade i tre år, utexaminerades 1928 vartefter han forskade vid skolan i ytterligare tre år. Welchman var en av fyra personer[5] som blev rekryterade till GC och CS vid Bletchley Park innan kriget bryter ut. Dessa fyra var alla viktiga för framgångarna inom kryptologisektorn under kriget.

Welchman arbetade inte direkt med Enigmas kryptering, utan mera med att undersöka hur meddelandena skickades, dvs. med *rubriker, datum, mottagare, avsändare* osv. Denna information, om än enklare att lista ut än själva innehållet i meddelandena, var fortfarande ytterst viktigt för att man skulle kunna skapa en fullständig bild av det material som avlyssnades. Man kan säga att Welchman undersökte "metadatan" för meddelandena, dvs. information om informationen.

Efter kriget arbetade Welchman i Storbritannien som ledande forskare vid "Johan Lewis Partnership" fram till år 1948, varefter han flyttade till USA. Han blev USA medborgare och började undervisa datorkurser vid MIT. Under sin tid i USA arbetade han även för militären, där han hjälpte utveckla säkra kommunikationssystem. Han blev pensionär år 1971 men fortsatte arbeta som konsult även efter det.

[5] *Alan Turing, Hugh Alexander, Stuart Milner-Barry* och *Gordon Welchman.*

5.2.1 Delaktighet i "Bomben"

Som nämndes arbetade Welchman inte direkt med Bombe tillsammans med Turing. Trots detta utvecklade Welchman en "diagonal board", dvs. en diagonal platta som användes tillsammans med Bombe. När Welchman presenterade sin uppfinning hade Turings maskin redan börjat byggas, men Welchmans uppfinning ansågs så viktig att maskinen omdesignades för att inkludera plattan.

Denna diagonalplatta, som Welchman uppfann, skapade kopplingar mellan alla bokstäver, med andra ord, den kopplade alla bokstäver med varandra. **Vad var nyttan med den?** Enigma använder sig av ett kopplingsbord, sladdkopplingarna med vilka tyskarna kunde koppla två bokstäver med varandra. Detta hade Turing inte tagit i beaktande, eller kanske mera korrekt, det hade krävts mera arbete för att undersöka alla inställningar som Turings maskin rapporterade till operatören. Denna enkla diagonalplatta simulerade alla möjliga kopplingsbordskopplingar och skar därmed ner på det antal Enigmainställningar som behövde kontrolleras för hand. Med Turings maskin, utan denna platta, hade man behövt kontrollera flera möjligheter för att beakta kopplingsbordet. Antalet inställningar för Enigma lär ska ha sjunkit från ett tusental till endast ett fåtal [24].

Kapitel 6

Avslutning

Detta arbete har fokuserat på att lyfta fram *Marian Rejewskis* insatser inom kryptologi under 1930-talet. De kalkyler och det arbete som Rejewski utförde är ytterst imponerande. Genom att personligen räkna igenom hela processen för att lista ut en Enigma rotorkopplingar, får man en bra insikt i hur mycket arbete och tid som gått åt för att lista ut denna viktiga information. Personligen räknade jag enbart ut en rotor, medans Rejewski beräknade 3 rotorer, samt reflektorn och även de nya rotorerna när de väl togs i bruk.

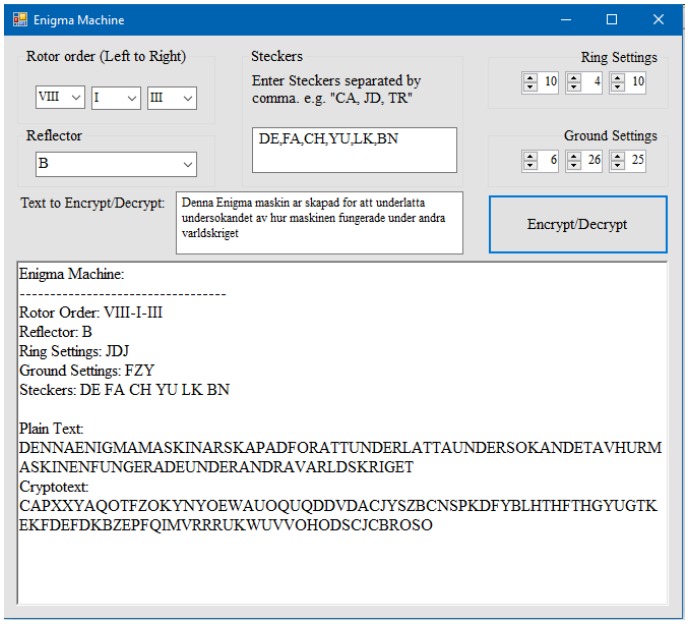
En del av de satser som Rejewski tagit fram och som har presenterats i detta arbete, har blivit namngivna som "Satserna som vann andra världskriget". Även om det är ett aningen överdrivet påstående, så är jag villig att hålla med om att arbetet var ytterst viktigt för att knäcka tyskarnas krypteringsmaskin Enigma. I detta arbete behandlade vi också de andra matematiska metoderna och maskiner som kryptologerna tillverkade när de arbetade i Polen. Tyvärr finns det mindre information dokumenterat om dessa metoder vilket leder till att de får mindre uppmärksamhet i avhandlingen, men de var trots detta ytterst viktiga.

Förhoppningsvis ger denna avhandling en bra inblick i arbetet av att vara en matematiker inom kryptologifältet på 1930-talet, i alla fall i Polen. Vidare är det förhoppningsvis möjligt för läsarna att få en överblick av hur mycket arbete somingått i lösandet av Enigma och därmed knäckandet av Tysklands kod. Slutligen kan man notera att tyskarna själva inte visste hur man skulle lösa Enigma (beräkna rotorerna etc.) [20], [8].

Bilaga A

Enigma maskinkod

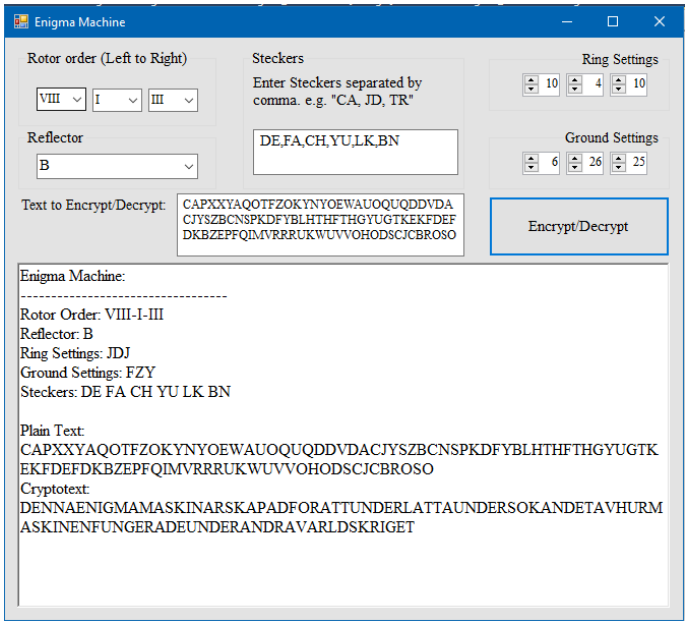
Koden är baserad på "joacand"s kod, som finns att hittas på `https://github.com/joacand/EnigmaMachineEmulator`. Jag hämtade koden därifrån den 7.6.2018. Min kod bygger på hens, men innehåller egna förändringar. Största skillnaden ligger i att koden "joacan" skrivit innebär att Enigma körs i kommandotolken, vilket gör det klumpigt att återanvända och kryptera meddelanden efter varandra. Mitt program kör i fönster format och gör att man snabbt och enkelt kan kryptera och dekryptera meddelanden. Koden är skriven i C# (C Sharp). Kommentarerna och liknande är skrivna på engelska av den anledningen att det är enklare att programmera på engelska eftersom bokstäverna å, ä och ö tenderar att bråka.



Figur A.1: Skärmdump av min Enigma maskin med inställningarna synligt och krytotexten.

Programkoden finns att hitta på addressen:

`https://github.com/Melvalan/Graphical-Enigma-Machine-in-C-Sharp`. Linken



Figur A.2: Enigma dekryptering av texten som krypterades i A.1, som synes blir texten samma klartext.

tar en till min GitHub sida, där man har möjlighet att kontrollera och ladda ner koden för att köra den på egen dator. Notera att kompilator för C# krävs för att köra programmet, t.ex. Visual Studio Code. (Mening var att inkludera koden här, men kodmängden gjorde dokumentet för långt.)

Se tabell 4.1 på sida 58 för rotorkopplingarna som används i programmet.

Bilaga B

Exempel på Rejewski uträkningar

B.1 Snabba rotorn

Kapitel 4 går igenom den teoretiska idén för bestämmande av en Enigma rotors kopplingar. Här presenteras ett fullt exempel som utnyttjar den Enigma maskin som beskrivs i bilaga A, dvs. den programmerade Enigma maskinen. Kryptotext skapas för de olika meddelandenycklarna. Här kommer även klartextnyckeln att visas, men den kände naturligtvis Rejewski inte till. Först, ett antal nycklar:

5:43
Plain: ABCABC
Crypto: ZRJZGG

5:49
Plain: UIIUII
Crypto: CKPGUW

5:56
Plain: QQQQQQ
Crypto: SNNTAK

5:59
Plain: WWWWWW
Crypto: HFTKTI

6:03
Plain: QAZQAZ
Crypto: SGUTQE

6:07
Plain: WDWWDV
Crypto: HMMKHR

6:11
Plain: RGNRGN
Crypto: LAQOBP

6:14
Plain: RGBRGB
Crypto: LASOBH

6:19
Plain: CHMCHM
Crypto: UTVBDL

6:23
Plain: CMECME
Crypto: UDGBNZ

6:27
Plain: TYUTYU
Crypto: EXZQVT

6:30
Plain: TYOTYO
Crypto: EXFQVF

6:33
Plain: ASDASD
Crypto: ZOXZXX

6:36
Plain: ASFASF
Crypto: ZOOZXO

6:39
Plain: GHJGHJ
Crypto: YTCUDS

6:43
Plain: POIPOI
Crypto: MSPJRW

6:46
Plain: LKJLKJ
Crypto: RICEZS

6:52
Plain: YJMYJM
Crypto: GZVXFL

6:55
Plain: THNTHN
Crypto: ETQQDP

7:05
Plain: TTTTTT
Crypto: EHWQWU

7:09
Plain: YYYYYY
Crypto: GXRXVA

7:12
Plain: VVVVVV
Crypto: XUMMYR

7:15
Plain: ABCABC
Crypto: ZRJZGG

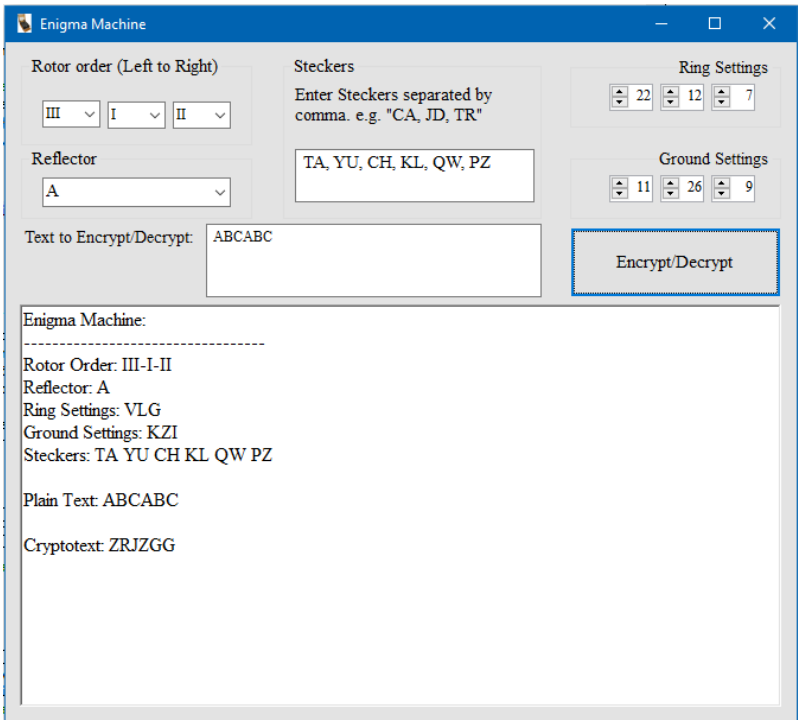
7:19
Plain: AABAAB
Crypto: ZGSZQH

7:23
Plain: CCBCCB
Crypto: UESBPH

7:26
Plain: DDDDDD
Crypto: NMXFHX

7:30	8:12	8:53	54:01
Plain: FFDFFD	Plain: HJKHJK	Plain: YXZYXZ	Plain: QQQQQQ
Crypto: IWXDJX	Crypto: WZLNFQ	Crypto: GYUXSE	Crypto: SNNTAK
7:33	8:17	8:58	54:08
Plain: HHTHHT	Plain: YUIYUI	Plain: FEYFEY	Plain: SSSSSS
Crypto: WTWNDU	Crypto: GVPXIW	Crypto: ICRDLA	Crypto: QOBIXJ
7:37	8:22	9:01	54:21
Plain: AAZAAZ	Plain: YYZYYZ	Plain: GASGAS	Plain: DDDDDD
Crypto: ZGUZQE	Crypto: GXUXVE	Crypto: YGBUQJ	Crypto: NMXFHX
7:40	8:28	9:04	54:34
Plain: AAQAAQ	Plain: QQWQQW	Plain: TAPTAP	Plain: QQWQQW
Crypto: ZGNZQK	Crypto: SNTTAI	Crypto: EGIQQN	Crypto: SNTTAI
7:44	8:31	47:33	54:42
Plain: ENLENL	Plain: TTRTTR	Plain: JJJJJJ	Plain: BBBBBB
Crypto: TQKLMM	Crypto: EHYQWV	Crypto: IHOMVP	Crypto: KRSCGH
7:49	8:36	48:31	54:55
Plain: LKILKI	Plain: XCVXCV	Plain: FEYFEY	Plain: FFFFFF
Crypto: RIPEZW	Crypto: VEMYPR	Crypto: BQCHMN	Crypto: IWODJO
7:52	8:40	52:17	55:05
Plain: GHTGHT	Plain: XXCXXC	Plain: FEYFEY	Plain: RRRRRR
Crypto: YTWUDU	Crypto: VYJYSG	Crypto: ICRDLA	Crypto: LBYOOV
7:56	8:42	53:20	55:14
Plain: QONQON	Plain: VVYVVY	Plain: JJJJJJ	Plain: WWWWWW
Crypto: SSQTRP	Crypto: XURMYA	Crypto: OZCPFS	Crypto: HFTKTI
8:01	8:46	53:40	55:19
Plain: MOQMOQ	Plain: YYXYYX	Plain: BBBBBB	Plain: IIIIII
Crypto: PSNVRK	Crypto: GXDXVD	Crypto: KRSCGH	Crypto: FKPSUW
8:07	8:50	53:51	55:22
Plain: VBQVBQ	Plain: YXYYXY	Plain: HHHHHH	Plain: OOOOOO
Crypto: XRNMGK	Crypto: GYRXSA	Crypto: WTANDB	Crypto: JSFRRF

66 meddelandenycklar har krypterats, se Figur B.1 för exempel på första (där finns även alla maskinens inställningar för detta exempel). I medeltal behövdes 80 meddelande under en dag för att man skall kunna bygga upp karakteristikerna AD, BE och CF. Dock har nycklarna valts så att alla bokstäver antingen dyker upp i alla positioner, eller så att det är enkelt att sluta sig till hur permutationerna måste se



Figur B.1: Kryptering av en meddelandenyckel med Enigmamaskinen i bilaga A.

ut, t.ex. när man vet att olika längders cykler alltid dyker upp i par. Med uteslutningsmetoden kan man därmed bilda karakteristikerna även av färre meddelanden (i vissa fall). Vi skriver ner karakteristikerna som fås ur nycklarna:

$$AD = (Z)(A)(WNFSTLOPVYUB)(HKCGXMJREQID)$$
$$BE = (CL)(EP)(KUYSRGQMHWJ)(OXVIZFTDNAB)$$
$$CF = (F)(X)(O)(D)(YVLQPWUECSH)(BJGZTINKMRA)$$

B.1.1 Faktorisering

Nu gäller det att lyckas faktorisera dessa till A, B, C, D, E och F. För detta använder vi Rejewskis Satser 1 och 2.

$$\mathbf{AD} = (Z)(A)(WNFSTLOPVYUB)(HKCGXMJREQID)$$

En-längdscykel Det finns två en-längdscykler (Z) och (A), enligt sats 2 betyder detta att (za) finns i både A och D.

Tolv-längdscykel Det finns två tolv-längdscykler, dessa kommer att resultera i 12 möjliga faktoriseringar, beroende på var cykeln "börjar". Var cykeln börjar har ingen inverkan på karakteristiken, men nog på dess faktorisering:

Ordning 1

$$AD = (WNFSTLOPVYUB)(HKCGXMJREQID)$$
$$A = (wd)(in)(fq)(es)(tr)(jl)(om)(xp)(vg)(cy)(uk)(hb)$$
$$D = (dn)(if)(qs)(et)(rl)(jo)(mp)(xv)(gy)(cu)(kb)(hw)$$

Ordning 2

$$AD = (WNFSTLOPVYUB)(KCGXMJREQIDH)$$
$$A = (wh)(dn)(fi)(qs)(te)(rl)(oj)(mp)(vx)(gy)(uc)(bk)$$
$$D = (hn)(df)(is)(qt)(el)(ro)(jp)(mv)(xy)(gu)(cb)(kw)$$

Ordning 3

$$AD = (WNFSTLOPVYUB)(CGXMJREQIDHK)$$
$$A = (wk)(hn)(fd)(is)(tq)(el)(or)(jp)(vm)(xy)(ug)(cb)$$
$$D = (kn)(hf)(ds)(it)(ql)(eo)(rp)(jv)(my)(xu)(gb)(cw)$$

Ordning 4

$$AD = (WNFSTLOPVYUB)(GXMJREQIDHKC)$$
$$A = (wc)(kn)(fh)(ds)(ti)(ql)(oe)(rp)(vj)(my)(ux)(gb)$$
$$D = (cn)(kf)(hs)(dt)(il)(qo)(ep)(rv)(jy)(mu)(xb)(gw)$$

Ordning 5

$$AD = (WNFSTLOPVYUB)(XMJREQIDHHKCG)$$
$$A = (wg)(cn)(fk)(hs)(td)(il)(oq)(ep)(vr)(jy)(um)(xb)$$
$$D = (gn)(cf)(ks)(ht)(dl)(io)(qp)(ev)(ry)(ju)(mb)(xw)$$

Ordning 6

$$AD = (WNFSTLOPVYUB)(MJREQIDHKCGX)$$
$$A = (wx)(gn)(fc)(ks)(th)(dl)(oi)(qp)(ve)(ry)(uj)(mb)$$
$$D = (xn)(gf)(cs)(kt)(hl)(do)(ip)(qv)(ey)(ru)(jb)(mw)$$

Ordning 7

$$AD = (WNFSTLOPVYUB)(JREQIDHKCGXM)$$
$$A = (wm)(xn)(fg)(cs)(tk)(hl)(od)(ip)(vq)(ey)(ur)(jb)$$
$$D = (mn)(xf)(gs)(ct)(kl)(ho)(dp)(iv)(qy)(eu)(rb)(jw)$$

Ordning 8

$$AD = (WNFSTLOPVYUB)(REQIDHKCGXMJ)$$
$$A = (wj)(mn)(fx)(gs)(tc)(kl)(oh)(dp)(vi)(qy)(ue)(rb)$$
$$D = (jn)(mf)(xs)(gt)(cl)(ko)(hp)(dv)(iy)(qu)(eb)(rw)$$

Ordning 9

$$AD = (WNFSTLOPVYUB)(EQIDHKCGXMJR)$$
$$A = (wr)(jn)(fm)(xs)(tg)(cl)(ok)(hp)(vd)(iy)(uq)(eb)$$
$$D = (rn)(jf)(ms)(xt)(gl)(co)(kp)(hv)(dy)(iu)(qb)(ew)$$

Ordning 10

$$AD = (WNFSTLOPVYUB)(QIDHKCGXMJRE)$$
$$A = (we)(rn)(fj)(ms)(tx)(gl)(oc)(kp)(vh)(dy)(ui)(qb)$$
$$D = (en)(rf)(js)(mt)(xl)(go)(cp)(kv)(hy)(du)(ib)(qw)$$

Ordning 11

$$AD = (WNFSTLOPVYUB)(IDHKCGXMJREQ)$$
$$A = (wq)(en)(fr)(js)(tm)(xl)(og)(cp)(vk)(hy)(ud)(ib)$$
$$D = (qn)(ef)(rs)(jt)(ml)(xo)(gp)(cv)(ky)(hu)(db)(iw)$$

Ordning 12

$$AD = (WNFSTLOPVYUB)(DHKCGXMJREQI)$$
$$A = (wi)(qn)(fe)(rs)(tj)(ml)(ox)(gp)(vc)(ky)(uh)(db)$$
$$D = (in)(qf)(es)(rt)(jl)(mo)(xp)(gv)(cy)(ku)(hb)(dw).$$

Dessa cykler ger oss tolv olika möjliga faktoriseringar. Vi ska nu göra som Rejewski och försöka lista ut vilken som är korrekt (klartexten är känd, vilket gör att vi kan kontrollera vårt svar). Rejewski antog att operatörerna brukade använda meddelandenycklar som bestod av samma bokstav tre gånger, tre bokstäver som låg bredvid varandra på tangentbordet osv. Ifall vi antar att operatören har använt QQQ som meddelande-nyckel så kan vi med våra olika faktoriseringar kontrollera vad bokstaven Q blir: Ordning 1: $A : q \to f, D : q \to s$, ordning 2 $A : q \to s, D : q \to t$ osv. Nu letar man igenom våra krypterade meddelandenycklar och ser ifall där finns fall med ett f i första position och s i andra. Ifall detta inte hittas går vi vidare till ordning 2 och försöker hitta s i position 1 och t i position 2.

Detta lyckas, se tredje meddelandenyckeln. Man fortsätter sedan, t.ex. med tre W:n och med lite tur, sluga gissningar samt oförsiktiga operatörer (vi var själva oförsiktiga med meddelandenycklarna i Exemplet) lyckas man lista ut att Ordning 2 är korrekta faktorisering (detta kan enkelt kontrolleras när klartexten är känd).

A och D får utseendena:

$$\begin{aligned} AD &= (z)(a)(wnfstlopvyub)(hkcgxmjreqid) \\ A &= (za)(wh)(dn)(fi)(qs)(te)(rl)(oj)(mp)(vx)(gy)(uc)(bk) \\ D &= (za)(hn)(df)(is)(qt)(el)(ro)(jp)(mv)(xy)(gu)(cb)(kw). \end{aligned}$$

$$\mathbf{BE} = (CL)(EP)(KUYSRGQMHWJ)(OXVIZFTDNAB)$$

Två-längscykler Det finns två två-längdscykler. Vi använder Sats 2 och får två möjligheter:

Ordning 1

$$\begin{aligned} BE &= (CL)(EP) \\ B &= (CP)(EL) \\ E &= (PL)(EC) \end{aligned}$$

Ordning 2

$$\begin{aligned} BE &= (CL)(PE) \\ B &= (CE)(PL) \\ E &= (EL)(PC). \end{aligned}$$

En av dessa möjligheter är korrekt, vi beräknar elva-längdscyklerna och bestämmer sedan vilken som är korrekt.

Elva-längds cykler Det finns två elva-längdscykler, så vi har 11 möjligheter för faktoriseringen. Vi skriver ner dessa:

Ordning 1

$$\begin{aligned} BE &= (KUYSRGQMHWJ)(OXVIZFTDNAB) \\ B &= (kb)(au)(yn)(ds)(rt)(fg)(qz)(im)(hv)(xw)(jo) \\ E &= (bu)(ay)(ns)(dr)(tg)(fq)(zm)(ih)(vw)(xj)(ok) \end{aligned}$$

Ordning 2

$$BE = (KUYSRGQMHWJ)(XVIZFTDNABO)$$
$$B = (ko)(bu)(ya)(ns)(rd)(tg)(qf)(zm)(hi)(vw)(jx)$$
$$E = (ou)(by)(as)(nr)(dg)(tq)(fm)(zh)(iw)(vj)(xk)$$

Ordning 3

$$BE = (KUYSRGQMHWJ)(VIZFTDNABOX)$$
$$B = (kx)(ou)(yb)(as)(rn)(dg)(qt)(fm)(hz)(iw)(jv)$$
$$E = (xu)(oy)(bs)(ar)(ng)(dq)(tm)(fh)(zw)(ij)(vk)$$

Ordning 4

$$BE = (KUYSRGQMHWJ)(IZFTDNABOXV)$$
$$B = (kv)(xu)(yo)(bs)(ra)(ng)(qd)(tm)(hf)(zw)(ji)$$
$$E = (vu)(xy)(os)(br)(ag)(nq)(dm)(th)(fw)(zj)(ik)$$

Ordning 5

$$BE = (KUYSRGQMHWJ)(ZFTDNABOXVI)$$
$$B = (ki)(vu)(yx)(os)(rb)(ag)(qn)(dm)(ht)(fw)(jz)$$
$$E = (iu)(vy)(xs)(or)(bg)(aq)(nm)(dh)(tw)(fj)(zk)$$

Ordning 6

$$BE = (KUYSRGQMHWJ)(FTDNABOXVIZ)$$
$$B = (kz)(iu)(yv)(xs)(ro)(bg)(qa)(nm)(hd)(tw)(jf)$$
$$E = (zu)(iy)(vs)(xr)(og)(bq)(am)(nh)(dw)(tj)(fk)$$

Ordning 7

$$BE = (KUYSRGQMHWJ)(TDNABOXVIZF)$$
$$B = (kf)(zu)(yi)(vs)(rx)(og)(qb)(am)(hn)(dw)(jt)$$
$$E = (fu)(zy)(is)(vr)(xg)(oq)(bm)(ah)(nw)(dj)(tk)$$

Ordning 8

$$BE = (KUYSRGQMHWJ)(DNABOXVIZFT)$$
$$B = (kt)(fu)(yz)(is)(rv)(xg)(qo)(bm)(ha)(nw)(jd)$$
$$E = (tu)(fy)(zs)(ir)(vg)(xq)(om)(bh)(aw)(nj)(dk)$$

Ordning 9

$$BE = (KUYSRGQMHWJ)(NABOXVIZFTD)$$
$$B = (kd)(tu)(yf)(zs)(ri)(vg)(qx)(om)(hb)(aw)(jn)$$
$$E = (du)(ty)(fs)(zr)(ig)(vq)(xm)(oh)(bw)(aj)(nk)$$

Ordning 10

$$BE = (KUYSRGQMHWJ)(ABOXVIZFTDN)$$
$$B = (kn)(du)(yt)(fs)(rz)(ig)(qv)(xm)(ho)(bw)(ja)$$
$$E = (nu)(dy)(ts)(fr)(zg)(iq)(vm)(xh)(ow)(bj)(ak)$$

Ordning 11

$$BE = (KUYSRGQMHWJ)(BOXVIZFTDNA)$$
$$B = (ka)(nu)(yd)(ts)(rf)(zg)(qi)(vm)(hx)(ow)(jb)$$
$$E = (au)(ny)(ds)(tr)(fg)(zq)(im)(vh)(xw)(oj)(bk).$$

Det finns $2 \cdot 11 = 22$ möjliga faktoriseringar för BE. Vi utför nu likadana gissningar för samma tre bokstäver som för AD och jämför B och E med våra krypterade nycklar tills vi hittar något som passar. (Vi har det uppenbart lättare än Rejewski, eftersom vi känner till klartexten för kontroll, men principen är exakt den samma.)

Det visar sig att Ordning 2 faktoriseringen för två-längdscyklerna och Ordning 5 faktoriseringen för elva-längdscyklerna är korrekt:

$$BE = (cl)(ep)(kuysrgqmhwj)(oxvizftdnab)$$
$$B = (ce)(pl)(ki)(vu)(yx)(os)(rb)(ag)(qn)(dm)(ht)(fw)(jz)$$
$$E = (el)(pc)(iu)(vy)(xs)(or)(bg)(aq)(nm)(dh)(tw)(fj)(zk).$$

CF $= (F)(X)(O)(D)(YVLQPWUECSH)(BJGZTINKMRA)$

Använder Sats 2 för att faktorisera de fyra en-längdcyklerna samt de två elva-längdscyklerna.

En-längdscyklerna Det finns fyra en-längdscykler. Till skillnad från AD betyder detta att man måste betrakta tre olika möjligheter, vi får faktoriseringar:

Ordning 1

$$CF = (f)(x)(o)(d)$$
$$C = (fx)(od)$$
$$F = (fx)(od)$$

Ordning 2

$$CF = (f)(x)(o)(d)$$
$$C = (fo)(xd)$$
$$F = (fo)(xd)$$

Ordning 3

$$CF = (f)(x)(o)(d)$$
$$C = (fd)(xo)$$
$$F = (fd)(xo).$$

Faktoriseringarna är lika i både C och F, ty vi har en-längdscykler. Bestämmer korrekta efter att elva-längdscykelns faktoriseringar beräknats.

Elva-längdscyklerna Det finns två elva-längdscykler, listar alla elva möjliga faktoriseringar.

Ordning 1

$$CF = (yvlqpwuecsh)(bjgztinkmra)$$
$$C = (ya)(rv)(lm)(kq)(pn)(iw)(ut)(ze)(cg)(js)(hb)$$
$$F = (av)(rl)(mq)(kp)(nw)(iu)(te)(zc)(gs)(jh)(by)$$

Ordning 2

$$CF = (yvlqpwuecsh)(jgztinkmrab)$$
$$C = (yb)(av)(lr)(mq)(pk)(nw)(ui)(te)(cz)(gs)(hj)$$
$$F = (bv)(vl)(rq)(mp)(kw)(nu)(ie)(tc)(zs)(gh)(jy)$$

Ordning 3

$$CF = (yvlqpwuecsh)(gztinkmrabj)$$
$$C = (yj)(bv)(la)(rq)(pm)(kw)(un)(ie)(ct)(zs)(hg)$$
$$F = (jv)(bl)(aq)(rp)(mw)(ku)(ne)(ic)(ts)(zh)(gy)$$

Ordning 4

$$CF = (yvlqpwuecsh)(ztinkmrabjg)$$
$$C = (yg)(jv)(lb)(aq)(pt)(mw)(uk)(ne)(ci)(ts)(hz)$$
$$F = (gv)(jl)(bq)(ap)(rw)(mu)(ke)(nc)(is)(th)(zy)$$

Ordning 5

$$CF = (yvlqpwuecsh)(tinkmrabjgz)$$
$$C = (yz)(gv)(lj)(bq)(pa)(wr)(mu)(ek)(nc)(si)(th)$$
$$F = (zv)(gl)(jq)(bp)(aw)(ru)(me)(kc)(ws)(ih)(ty)$$

Ordning 6

$$CF = (yvlqpwuecsh)(inkmrabjgzt)$$
$$C = (yt)(zv)(lg)(jq)(pb)(aw)(ur)(me)(ck)(ns)(hi)$$
$$F = (tv)(zl)(gq)(jp)(bw)(au)(re)(mc)(ks)(nh)(iy)$$

Ordning 7

$$CF = (yvlqpwuecsh)(nkmrabjgzti)$$
$$C = (yi)(tv)(lz)(gq)(pj)(bw)(ua)(re)(cm)(ks)(hn)$$
$$F = (iv)(tl)(zq)(gp)(jw)(bu)(ae)(rc)(ms)(kh)(ny)$$

Ordning 8

$$CF = (yvlqpwuecsh)(kmrabjgztin)$$
$$C = (yn)(iv)(lt)(zq)(pg)(jw)(ub)(ae)(cr)(ms)(hk)$$
$$F = (nv)(il)(tq)(zp)(gw)(ju)(be)(ac)(rs)(mh)(ky)$$

Ordning 9

$$CF = (yvlqpwuecsh)(mrabjgztink)$$
$$C = (yk)(nv)(li)(tq)(pz)(gw)(uj)(be)(ca)(rs)(hm)$$
$$F = (kv)(nl)(iq)(tp)(zw)(gu)(je)(bc)(as)(rh)(my)$$

Ordning 10

$$CF = (yvlqpwuecsh)(rabjgztinkm)$$
$$C = (ym)(kv)(ln)(iq)(pt)(zw)(ug)(je)(cb)(as)(hr)$$
$$F = (mv)(kl)(nq)(ip)(tw)(zu)(ge)(jc)(bs)(ah)(ry)$$

Ordning 11

$$CF = (yvlqpwuecsh)(abjgztinkmr)$$
$$C = (yr)(mv)(lk)(nq)(pi)(tw)(uz)(ge)(cj)(bs)(ha)$$
$$F = (rv)(ml)(kq)(np)(iw)(tu)(ze)(gc)(js)(bh)(ay).$$

Det finns $3 \cdot 11 = 33$ möjliga faktoriseringar. Vi utför likadana antaganden gällande operatörerna som för AD och BE och konstaterar att de korrekta faktoriseringarna är Ordning 2 för en-längdscyklerna och Ordning 11 för elva-längdscyklerna. För en-längdscyklerna är det nödvändigt att hitta två olika meddelandenycklar. En var $C, F : f \to o$ samt en var $C, F : x \to d$, eller egentligen räcker att man hittar en av dessa, men för att vara på säkra sidan letar man efter båda.

Detta ger faktoriseringen:

$$CF = (F)(X)(O)(D)(YVLQPWUECSH)(BJGZTINKMRA)$$
$$C = (fo)(xd)(yr)(mv)(lk)(nq)(pi)(tw)(uz)(ge)(cj)(bs)(ha)$$
$$F = (fo)(xd)(rv)(ml)(kq)(np)(iw)(tu)(ze)(gc)(js)(bh)(ay).$$

Anmärkning 1. *Det är enkelt att förstå att ifall operatörerna hade varit mera försiktiga med hur de valde sina meddelandenycklar så hade Rejewskis arbete med att gissa meddelandenycklar att jämföra med, varit klurigare och kanske gett fel faktorisering.*

Dessutom var svårare att bestämma faktoriseringarna när klartexten ej var känd, ty det krävde att Rejewski noggrant kontrollerade alla sina gissningar flera gånger så att de faktiskt blev korrkta.

$A - F$ ser ut på följande sätt:

$$A = (za)(wh)(dn)(fi)(qs)(te)(rl)(oj)(mp)(vx)(gy)(uc)(bk)$$
$$B = (ce)(pl)(ki)(vu)(yx)(os)(rb)(ag)(qn)(dm)(ht)(fw)(jz)$$
$$C = (fo)(xd)(yr)(mv)(lk)(nq)(pi)(tw)(uz)(ge)(cj)(bs)(ha)$$
$$D = (za)(hn)(df)(is)(qt)(el)(ro)(jp)(mv)(xy)(gu)(cb)(kw)$$
$$E = (el)(pc)(iu)(vy)(xs)(or)(bg)(aq)(nm)(dh)(tw)(fj)(zk)$$
$$F = (fo)(xd)(rv)(ml)(kq)(np)(iw)(tu)(ze)(gc)(js)(bh)(ay).$$

B.1.2 Rotorns kopplingar

Vet nu hur Enigma krypterar de första sex bokstäverna för denna inställning. Nu gäller det att bestämma rotorkopplingarna för den snabba rotorn. Notera att Enigma maskinen var inställd på position 9 för snabba rotorn, så detta ger att vi kan bra anta att enbart den snabba rotorn rör sig under dessa sex krypteringar. Rejewski utförde detta antagande och oftast är det korrekt (i 21 fall av 26). Vi kommer ihåg permutationerna från kapitel 4:

$$
\begin{aligned}
A &= SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1} \\
B &= SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1} \\
C &= SHP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^{-3}H^{-1}S^{-1} \\
D &= SHP^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4}H^{-1}S^{-1} \\
E &= SHP^5NP^{-5}MLRL^{-1}M^{-1}P^5N^{-1}P^{-5}H^{-1}S^{-1} \\
F &= SHP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1},
\end{aligned}
$$

där, P är alfabetet och representerar att (snabba) rotorn roterar, S är kopplingsbordet, N är snabba rotorn, M mellan rotorn, L långsamma rotorn och R reflektorn (H är ingångstrumman men $H = I$, så den kommer att tas bort). Enligt vårt antagande att enbart den första rotorn roterar är det möjligt att förenkla:

$$Q = MLRL^{-1}M^{-1}$$

vilket ger

$$
\begin{aligned}
A &= SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1} \\
B &= SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1} \\
C &= SHP^3NP^{-3}QP^3N^{-1}P^{-3}H^{-1}S^{-1} \\
D &= SHP^4NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1} \\
E &= SHP^5NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1} \\
F &= SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}.
\end{aligned}
$$

Emedan $H = I$, så vi kan plocka bort den. Eftersom det är vi som har ställt upp Enigma maskinen (medan Rejewski fick kodlappar av den franska spionen Asché) kan S anses känd och flyttar även över kända permutationen P. Detta lämnar Q och N som obekanta på höger sida. Vi skriver nu om ekvationerna så de bekanta variablerna är på vänster sida:

$$P^{-1}S^{-1}ASP = NP^{-1}QPN^{-1}$$
$$P^{-2}S^{-1}BSP^{2} = NP^{-2}QPN^{-1}$$
$$P^{-3}S^{-1}CSP^{3} = NP^{-3}QPN^{-1}$$
$$P^{-4}S^{-1}DSP^{4} = NP^{-4}QPN^{-1}$$
$$P^{-5}S^{-1}ESP^{5} = NP^{-5}QPN^{-1}$$
$$P^{-6}S^{-1}FSP^{6} = NP^{-6}QPN^{-1}.$$

Betecknar sedan vänster led med bokstäver $U - Z$:

$$U = NP^{-1}QPN^{-1}$$
$$V = NP^{-2}QPN^{-1}$$
$$W = NP^{-3}QPN^{-1}$$
$$X = NP^{-4}QPN^{-1}$$
$$Y = NP^{-5}QPN^{-1}$$
$$Z = NP^{-6}QPN^{-1}.$$

Som konstaterats i Kapitel 4, behöver man enbart känna till $U - Z$ och därmed beräknar vi dessa. Stegvis för U, de andra tre analogt, observera att permutationerna S och S^{-1} har en-längdscykler när ingen bokstav nämns (de skrivs inte ut):

$$
\begin{aligned}
U &= P^{-1}S^{-1}ASP \\
&= \underbrace{[(zyxwvutsrqponmlkjihgfedcba)]}_{=P^{-1}} \underbrace{[(zp)(wq)(lk)(hc)(uy)(at)]}_{=S^{-1}} \\
&\quad \underbrace{[(za)(wh)(dn)(fi)(qs)(te)(rl)(oj)(mp)(vx)(gy)(uc)(bk)]}_{=A} \\
&\quad \underbrace{[(ta)(yu)(ch)(kl)(qw)(pz)]}_{=S} \underbrace{[(abcdefghijklmnopqrstuvwxyz)]}_{=P} \\
&= \underbrace{[(zyxwvutsrqponmlkjihgfedcba)]}_{=P^{-1}} \underbrace{[(zmpact)(wsqhugyc)(lbkr)(dn)(fi)(jo)(vx)]}_{S^{-1}A} \\
&\quad \underbrace{[(ta)(yu)(ch)(kl)(qw)(pz)]}_{S} \underbrace{[(abcdefghijklmnopqrstuvwxyz)]}_{=P} \\
&= \underbrace{[(zyxwvutsrqponmlkjihgfedcba)]}_{=P^{-1}} \underbrace{[(zm)(pt)(ae)(ws)(qc)(hy)(ug)(lb)(kr)(dn)(fi)(jo)(vx)]}_{S^{-1}AS} \\
&\quad \underbrace{[(abcdefghijklmnopqrstuvwxyz)]}_{=P} \\
&= (zi)(hv)(uq)(pk)(jg)(fb)(an)(eo)(yw)(xt)(dr)(cm)(ls).
\end{aligned}
$$

Vi får:

$$
\begin{aligned}
U &= (zi)(hv)(uq)(pk)(jg)(fb)(an)(eo)(yw)(xt)(dr)(cm)(ls) \\
V &= (zw)(uq)(of)(dt)(rl)(jg)(ax)(vi)(hs)(mb)(yp)(nk)(ce) \\
W &= (xu)(ri)(fw)(td)(qz)(cl)(on)(km)(jh)(ev)(sb)(yp)(ga) \\
X &= (zq)(mw)(sv)(rg)(ck)(nd)(oi)(ea)(yb)(xt)(pu)(fl)(hj).
\end{aligned}
$$

Utför multiplikation med två på varandra följande uttryck:

$$
\begin{aligned}
UV &= (NP^{-1}QPN^{-1})(NP^{-2}QP^2N^{-1}) \quad = NP^{-1}(QP^{-1}QP)PN^{-1} \\
VW &= NP^{-2}(QP^{-1}QP)P^2N^{-1} \\
WX &= NP^{-3}(QP^{-1}QP)P^2N^{-1}.
\end{aligned}
$$

Beräknar UV, VW och WX:

$$UV = (zvsrtaky)(iwpnxdlh)(fme)(ocb)(u)(q)(j)(g)$$
$$VW = (zfnmsjau)(wqxghbko)(rcv)(iel)(d)(t)(y)(p)$$
$$WX = (xpbvarod)(utnigesy)(fmc)(wlk)(h)(j)(q)(z).$$

Alla tre ekvationer har uttrycket $(QP^{-1}QP)$ gemensamt. Detta löses ut ur första uttrycket och sätts sedan in i följande:

$$(QP^{-1}QP) = N^{-1}P(\mathbf{UV})P^{-1}N \quad \text{ur uttrycket } UV.$$

Skriver om uttryckena

$$\begin{aligned} VW &= NP^{-2}(QP^{-1}QP)P^2N^{-1} \\ &= NP^{-1}N^{-1}(NP^{-1}(QP^{-1}QP)PN^{-1})NPN^{-1} \\ &= NP^{-1}N^{-1}(\mathbf{UV})NPN^{-1} \\ &= (NPN^{-1})^{-1}(\mathbf{UV})(NPN^{-1}) \end{aligned}$$

och får båda uttryckena

$$VW = NP^{-1}N^{-1}(\mathbf{UV})NPN^{-1}$$
$$WX = NP^{-1}N^{-1}(\mathbf{VW})NPN^{-1}.$$

Från detta ser man att de olika uttryckena bygger på varandra och påverkas enbart av NPN^{-1}. Detta innebär att om man skriver ett antal olika möjligheter för NPN^{-1}, och jämför transformationerna UV, VW samt WX med varandra så ska det existera en version av NPN^{-1} som passar in för alla tre, vilket ger 26 möjliga rotorkopplingar.

Vi använder Sats 5 för att bestämma NPN^{-1}, satsen säger att ifall vi har $T^{-1}HT = (\ldots T(i)T(j)\ldots)$ där $H(i) = j$ eller $H = (\ldots ij\ldots)$ så kommer H och $T^{-1}HT$ att ha samma disjunkta cykelsammansättning. Med detta skriver vi UV, VW och WX ovanför varandra på sådant sätt att man kan följa en kontinuerlig linje genom uppställningen, se avsnitt 4.1.2 för exempel på detta.

Vi börjar skriva dem ovanför varandra:

$$UV = (\mathbf{v}srtakyz)(iwpnxdlh)(fme)(ocb)(u)(q)(j)(g)$$

$$\frac{VW = (\mathbf{z}fnmsjau)(wqxghbko)(rcv)(iel)(d)(t)(y)(p)}{VW = (zfnmsjau)(wqxghbko)(rc\mathbf{v})(iel)(d)(t)(y)(p)}$$

$$WX = (utnigesy)(xpbvarod)(fm\mathbf{c})(wlk)(h)(j)(q)(z).$$

Denna uppställning fungerar inte, ty (se tjocka bokstäver) NPN^{-1} blir ej samma, ($UV - VW$ ger (vzu) $VW - WX$ ger (vc)). Detta betyder att man kan sluta leta för denna konfiguration och prövar en annan:

$$UV = (takyzvsr)(iwpnxdlh)(fme)(ocb)(u)(q)(j)(g)$$

$$\frac{VW = (zfnmsjau)(wqxghbko)(rcv)(iel)(d)(t)(y)(p)}{VW = (zfnmsjau)(wqxghbko)(rcv)(iel)(d)(t)(y)(p)}$$

$$WX = (syutnige)(xpbvarod)(fmc)(wlk)(h)(z)(q)(j).$$

Denna uppställning fungerar inte heller.

$$UV = (akyzvsrt)(iwpnxdlh)(fme)(ocb)(u)(q)(j)(g)$$

$$\frac{VW = (ghbkowqx)(uzfnmsja)(lie)(rcv)(d)(t)(y)(p)}{VW = (nmsjauzf)(wqxghbko)(rcv)(iel)(d)(t)(y)(p)}$$

$$WX = (syutnige)(xpbvarod)(fmc)(wlk)(h)(z)(q)(j).$$

Inte heller denna fungerar. (slutar skriva ut dessa tills vi hittar den korrekta).

$$UV = (akyzvsrt)(iwpnxdlh)(ocb)(mef)(u)(q)(g)(j)$$

$$\frac{VW = (xghbkowq)(msjauzfn)(eli)(rcv)(p)(y)(t)(d)}{VW = (xghbkowq)(msjauzfn)(eli)(rcv)(p)(y)(t)(d)}$$

$$WX = (utnigesy)(rodxpbva)(cfm)(wlk)(j)(h)(q)(z).$$

Denna uppställning ger samma uttryck för NPN^{-1} när man går igenom bokstäverna för kombinationen $UV - VW$ såväl som $VW - WX$:

$$NPN^{-1} = (axupjdzbimrwsoeclfvkgtqyhn)$$

För att hitta rätt "stig" användes en metod där alla bokstäver som a kunde kopplas

ihop med listades i $UV - VW$, vartefter man kontrollerade ifall samma bokstäver dök upp för den andra kombinationen enligt $(VW - WX)$:

$$UV - VW : a - \underline{xgboaunsq}hkwjzfm$$
$$VW - WX : a - \underline{sungxbaoy}tiepvrd,$$

där de understräckade bokstäverna dyker upp i båda fallen. Vi fortsätter:

$$UV - VW : a - x - \underline{uns}jzfms$$
$$VW - WX : a - x - \underline{uns}ytige.$$

Det är viktigt att man håller koll på var i cyklerna de olika bokstäverna finns, vartefter man kontrollerar ifall cyklerna redan är bundna med varandra, dvs. om det redan finns ett bokstavspar, och kontrollerar sedan avståndet. På detta sätt lyckas man hitta den kombination för NPN^{-1} som faktiskt fungerar aningen mera effektivt än att testa olika kombinationer. Detta fortsätter tills man kommer runt tillbaka till a och resultatet var:

$$NPN^{-1} = (axupjdzbimrwsoeclfvkgtqyhn)$$

Nu finns ett resultat för NPN^{-1}. Vi skriver därför detta över en vanlig bokstavspermutation P, ty

$$P = N^{-1}(NPN^{-1})N = (abcdefghijklmnopqrstuvwxyz).$$

Återigen med hjälp av Sats 5 kan man lista NPN^{-1} ovanför denna permutation P för att lista ut rotorkombinationen N:

$$N = \begin{pmatrix} NPN^{-1} \\ P \end{pmatrix} = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ abcdefghijklmnopqrstuvwxyz \end{pmatrix}.$$

Vi placerar detta i bokstavsordning enligt NPN^{-1}, dvs. organiserar om övre raden:

$$N = \begin{pmatrix} abcdefghijklmnopqrstuvwxyz \\ ahpforuyietqjzndwkmvcslbxg \end{pmatrix}.$$

Detta är en möjlig koppling för $N = (ahpforuyietqjzndwkmvcslbxg)$, dock ska man komma ihåg att rotorna kan rotera och att det därmed finns flera möjliga kombinationer för N. Det finns med andra ord 26 möjliga kombinationer för N. Vi listar dessa genom att skriva NPN^{-1} över alla 26 möjliga P, dvs. vi börjar cykeln P med olika bokstäver, samt plockar ut N, vi placerar övre raden i bokstavsordning och N finns sedan på undre raden.

Ordning 1 $N = (ahpforuyietqjzndwkmvcslbxg)$

Ordning 2

$$N = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ bcdefghijklmnopqrstuvwxyza \end{pmatrix}$$

$N = (biqgpsvzjfurkaoexlnwdtmcyh)$.

Ordning 3

$$N = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ cdefghijklmnopqrstuvwxyzab \end{pmatrix}$$

$N = (cjrhqtwakgvslbpfymoxeundzi)$.

Ordning 4 Korrekt lösning.

$$N = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ defghijklmnopqrstuvwxyzabc \end{pmatrix}$$

$N = (dksiruxblkwtmcqgznpyfvoeaj)$.

Ordning 5

$$N = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ efghijklmnopqrstuvwxyzabcd \end{pmatrix}$$

$N = (eltjsvycmixundrhaoqzgwpfbk)$.

Ordning 6

$$N = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ fghijklmnopqrstuvwxyzabcde \end{pmatrix}$$

$N = (fmuktwzdnjyvoesibprahxqgcl)$.

Ordning 7

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{ghijklmnopqrstuvwxyzabcdef}$$

$N = (gnvluxaeokzwpftjcqsbiyrhdm)$.

Ordning 8

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{hijklmnopqrstuvwxyzabcdefg}$$

$N = (howmvybfplaxqgukdrtcjzsien)$.

Ordning 9

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{ijklmnopqrstuvwxyzabcdefgh}$$

$N = (ipxnwzcgqmbyrhvlesudkatjfo)$.

Ordning 10

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{jklmnopqrstuvwxyzabcdefghi}$$

$N = (jqyoxadhrnczsiwmftvelbukgp)$.

Ordning 11

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{klmnopqrstuvwxyzabcdefghij}$$

$N = (krzpybeisodatjxnguwfmcvlhq)$.

Ordning 12

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{lmnopqrstuvwxyzabcdefghijk}$$

$N = (lsaqzcfjtpebukyohvxgndwmir)$.

Ordning 13

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{mnopqrstuvwxyzabcdefghijkl}$$

$N = (mtbradgkuqfcvlzpiwyhoexnjs)$.

Ordning 14

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{nopqrstuvwxyzabcdefghijklm}$$

$N = (nucsbehlvrgdwmaqjxzipfyokt)$.

Ordning 15

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{opqrstuvwxyzabcdefghijklmn}$$

$N = (ovdtcfimwshexnbrkyajqgzplu)$.

Ordning 16

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{pqrstuvwxyzabcdefghijklmno}$$

$N = (pweudgjnxtifyocslzbkrhaqmv)$.

Ordning 17

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{qrstuvwxyzabcdefghijklmnop}$$

$N = (qxfvehkoyujgzpdtmaclsibrnw)$.

Ordning 18

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{rstuvwxyzabcdefghijklmnopq}$$

$N = (rygwfilpzvkhaqeunbdmtjcsox)$.

Ordning 19

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{stuvwxyzabcdefghijklmnopqr}$$

$N = (szhxgjmqawlibrfvocenukdtpy)$.

Ordning 20

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{tuvwxyzabcdefghijklmnopqrs}$$

$N = (taiyhknrbxmjcsgwpdfovleuqz)$.

Ordning 21

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{uvwxyzabcdefghijklmnopqrst}$$

$N = (ubjziloscynkdthxqegpwmfvra)$.

Ordning 22

$$N = \binom{axupjdzbimrwsoeclfvkgtqyhn}{vwxyzabcdefghijklmnopqrstu}$$

$N = (vckajmptdzoleuiyrfhqxngwsb)$.

Ordning 23

$$N = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ wxyzabcdefghijklmnopqrstuv \end{pmatrix}$$

$$N = (wdlbknqueapmfvjzsgiryohxtc).$$

Ordning 24

$$N = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ xyzabcdefghijklmnopqrstuvw \end{pmatrix}$$

$$N = (xemclorvfbqngwkathjszpiyud).$$

Ordning 25

$$N = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ yzabcdefghijklmnopqrstuvwx \end{pmatrix}$$

$$N = (yfndmpswgcrohxlbuiktaqjzve).$$

Ordning 26

$$N = \begin{pmatrix} axupjdzbimrwsoeclfvkgtqyhn \\ zabcdefghijklmnopqrstuvwxy \end{pmatrix}$$

$$N = (zgoenqtxhdspiymcvjlubrkawf).$$

Vi vet från tabell 4.1 på sidan 58 att ordning 4 ($N = (dksiruxblkwtmcqgznpyfvoeaj)$. är den korrekta. Hur ska man annars veta detta? Dessa lösningar varierar egentligen inte mycket från varandra och enda skillnaden mellan de olika ordningarna är att man har roterat den högra sidan (ingångssidan) jämfört med den västra sidan (utgångssidan) på rotorn.

Man kan dock inte välja ut denna rotorkoppling bland med alla möjligheter, innan man har kandidater för rotorkopplingarna för alla tre rotorer. Dvs. Rejewski behövde meddelanden där det var två olika rotorer i den "snabba" positionen för att kunna bestämma vilken av alla dessa 26 möjligheter som var korrekt. När dessa kandidater var kända, kunde Rejewski även beräkna den tredje rotorn och reflektorn genom att gå igenom "stigen" från klartext till kryptotext och se till att kopplingarna var korrekta och gav bra svar. Vi noterar även här att vår rotor av Ordning 4 är förskjuten en aning, enligt tabell 4.1 ska $a \to a$, men i vårt fall så gäller $a \to d$. Detta är något som man noterar och kan korrigera när man känner till kandidater för flera rotorer och kan gå igenom stigen från klartext till chiffertext.

Bestämma rätt koppling

Med hjälp av metoden beskriven i detta kapitel kunde Rejewski finna 26 möjligheter för de tre rotorerna, samt för reflektorn. Hur bestämde han de korrekta kopplingarna?

Som nämns i slutet av det förra avsnittet så följer man kopplingarna igenom Enigma tills man hittar de kopplingar för rotorn som faktiskt ger rätt resultat. Men hur skulle Rejewski veta att han funnit rätt? Man ska komma ihåg att Polen vid det här laget inte har tillgång till en Enigmamaskin och därmed kan de inte dekryptera tyska meddelanden, och har därmed inga meddelanden som man kan kontrollera med ifall kryptotexten blir rätt klartext. Rejewski hade kunnat gissa sig fram till vad tyskarna skrev i sina meddelanden och sedan se ifall hela meddelandet blev vettigt, dock hade detta varit ytterst tidskrävande och antagligen frustrerande arbete.

Vi bör komma ihåg att den franska spionen, Hans-Thilo Schmidt (Asché), tillhandahöll kodlappar med Enigmas dagliga inställningar, men han tillhandahöll även en instruktionsbok för hur Enigma skulle användas. I denna instruktionsbok fanns det ett exempel på ett Enigm meddelande, dvs. där stod alla inställningar för Enigma och dessutom ett klartext och kryptotext par. Detta var uppenbart en säkerhetsmiss från tyska sidan och i senare versioner av instruktionsboken var meddelande bara påhittat. Med detta meddelande hade Rejewski tillgång till ett så kallat “crib” för att testa rotorkopplingar.

Rejewski hade nu en ganska enkel uppgift i och med att ställa rotorerna i ordning, alla 26 möjligheter för de tre rotorerna och reflektorn och testa dem en och en tills strömkretsen lyckades kryptera klartextmeddelandet i instruktionsboken till kryptotexten i instruktionsboken. Egentligen utförde Rejewski samma arbete som Turings maskiner senare kom att utföra i Bletchley Park, dvs. han “brute force” testa ett antal lösningar tills den korrekta hittats.

Och därmed, genom att enbart ha beräknat 26 möjligheter för två av rotorerna kunde Rejewski sluta sig till 26 möjligheter för den tredje rotorn samt reflektorn och sedan igen tack vare den franska spionen kunde Rejewski sluta sig till vilken av de

26 möjligheterna som var den korrekta. Hans-Thilo Schmidts insatser var med andra ord, ytterst viktiga för Polens framgångar med att lista ut Enigmas rotorkopplingar [26]. Denna process är beskriven detaljerat i [26].

B.2 Sammanfattning

Arbetet Rejewski utförde för att finna rotorkopplingen var tidskrävande och noggrant arbete. Det var dock ögonöppnande att räkna igenom detta för hand och gav mig en mycket djupare förståelse över vad Rejewski gjorde på 1930-talet. Hans insatser var ytterst imponerande!

Litteraturförteckning

[1] NSA - National Security Agency. On the enigma. *Cryptolog*, 18(2):31–35, 1991.

[2] Chris Christensen. Polish Mathematicians Finding Patterns in Enigma Messages. *Mathematics Magazine*, 80(4):247–273, October 2007.

[3] Chris Christensen. Review of Memories of My Work at the Cipher Bureau of the General Staff Second Department 1930–1945 by Marian Rejewski. *Cryptologia*, 37(2):167–174, apr 2013.

[4] B. Jack Copeland, editor. *The Essential Turing*. Oxford University Press, December 2004.

[5] Donald W. Davies. The Bombe a Remarkable Logic Machine. *Cryptologia*, 23(2):108–138, apr 1999.

[6] James J. Gillogly. Ciphertext-Only Cryptanalysis of Enigma. *Cryptologia*, 19(4):405–413, oct 1995.

[7] Marek Grajek. Vanguard of mathematicians in cryptology. *Polskie Towarzystwo Matematyczne*, 48(2):97–107, 2012.

[8] David Kahn. Why Germany lost the Code War. *Cryptologia*, 6(1):26–31, jan 1982.

[9] David Kahn. An Enigma Chronology. *Cryptologia*, 17(3):237–246, jul 1993.

[10] David Kahn. The Polish Enigma Conference and some Excursions. *Cryptologia*, 29(2):121–126, apr 2005.

[11] David Kahn. How I Discovered World War II's Greatest Spy. *Cryptologia*, 34(1):12–21, dec 2009.

[12] Christopher Kasparek and Richard A. Woytak. In Memoriam Marian Rejewski. *Cryptologia*, 6(1):19–25, jan 1982.

[13] Wldyslaw Kozaczuk. Enigma Solved. *Cryptologia*, 6(1):32–33, jan 1982.

[14] Louis Kruh. How to use the German Enigma Cipher Machine: a Photographic Essay. *Cryptologia*, 7(4):291–296, oct 1983.

[15] John Lawrence. The Versatility of Rejewski's Method: Solving for the Wiring of the Second Rotor. *Cryptologia*, 28(2):149–152, apr 2004.

[16] John Lawrence. Factoring for the Plugboard – was Rejewski's Proposed Solution for Breaking the Enigma Feasible? *Cryptologia*, 29(4):343–366, oct 2005.

[17] Philip Marks and Frode Weierud. Recovering the Wiring of Enigma's Umkehrwalze A. *Cryptologia*, 24(1):55–66, jan 2000.

[18] Klaus Pommerening. Permutations and rejewski's theorem. Fachbereich Mathematik der Johannes-Gutenberg-Universität, January 2011.

[19] Marian Rejewski. An Application of the Theory of Permutations in breaking the Enigma Cipher. *Applicationes Mathematicae*, 16(4):543–559, 1980.

[20] Marian Rejewski. How Polish Mathematicians Deciphered the Enigma. *IEEE Annals of the History of Computing*, 3(3):213–234, jul 1981.

[21] Marian Rejewski. Mathematical Solution of the Enigma Cipher. *Cryptologia*, 6(1):1–18, jan 1982.

[22] Ari Renvall. Kryptografia I. Matematiikan Laitos; Turun Yliopisto, 2008.

[23] Manuel Vázquez and Paz Jiménez–Seral. Recovering the military Enigma using permutations—filling in the details of Rejewski's solution. *Cryptologia*, 42(2):106–134, apr 2017.

[24] Jennifer Wilcox. Solving the Enigma: History of the Cryptanalytic Bombe. Center for Cryptologic History - National Security Agency (NSA), https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/wwii/assets/files/solving_enigma.pdf, 2006.

[25] Frederick William Winterbotham. *The Ultra Secret*. Harper & Row, 1 edition, 1974.

[26] John Wright. Rejewski's Test Message as a Crib. *Cryptologia*, 40(1):92–106, aug 2015.

Figurer

Tabeller