SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Enigma—hur det löstes och lästes

by

Björn Bergstrand

2011 - No 11

Enigma—hur det löstes och lästes

Björn Bergstrand

Självständigt arbete i matematik 15 högskolepoäng, GN

Handledare: Rikard Bögvad

2011

Innehåll

1 Inledning

Denna text kommer att befatta sig med ämnet *kryptologi* som är läran om säkra kommunikationssystem. Kryptologin delas vidare in i *kryptografi* och *kryptoanalys*. Med kryptografi menas all typ av hemlig, eller gömd skrift, eller med en förlängning som passar modernare sammanhang, *data*. Kryptoanalys handlar om att lösa och läsa dessa hemliga meddelanden. Ett system för att hemlighålla data kallar vi ett *krypto*. Vi kommer att hålla oss här till beskrivning av krypton som gömmer alfabetisk text, samt metoder för forcering av dessa. De krypton som beskrivs är av den typen som gömmer text genom att översätta, eller koda, varje bokstav i ursprungsmeddelandet mot någon bokstav i alfabetet efter en uppsättning regler. Dessa typer av krypton kallas i allmänhet *substitutionskrypton*. Målet är att så småningom beskriva kryptomaskinen *Enigma*, som användes av Tyskland under andra världskriget för att kryptera sin kommunikation. Enigman ger ett krypto som består av just substitutioner, som vi kommer att se.
Den text som återstår efter att ha blivit översatt, eller *krypterad*, av ett krypto kallas för en *kryptotext*. Att översätta en kryptotext tillbaka till ursprungsmeddelandet benämns som en *dekryptering*. När en enda bokstav krypteras eller dekrypteras används orden *koda* respektiva *avkoda*, d.v.s. "a kodas till f, f avkodas till a.
Exakt hur ett kryptos regler tillämpas på ett meddelande specificeras ofta av en extra del data som kallas *nyckel*. Den tänkte mottagaren använder sedan nyckeln för att återställa meddelandet från kryptotexten. Det ska inte gå att läsa ett meddelande som uppsnappats utan att ha tillgång till nyckeln, även om man känner till vilket krypto som använts. Att försöka lista ut vad ursprungsmeddelandet är från en kryptotext utan att ha tillgång till nyckeln är alltså kryptoanalys.

Vi kommer att beskriva sammansättningar av permutationer med den första permutationen som används först. Det vill säga $(AB)(x)$ betyder $B(A(x))$. Detta för att göra det något lättare att läsa i vilken ordning en kryptering sker när väldigt många permutationer används.

2 Substitutionskrypton

Ett substitutionskrypto gömmer text genom att byta varje tecken i ursprungsmeddelandet enligt någon uppsättning regler. Det ska jämföras med *transpositionskrypton* som gömmer text genom att byta plats på tecknen, ungefär som ett gigantiskt anagram. Ofta används en kombination av de två. Vi kommer endast att behandla substitutionskrypton.

2.1 Enkel substitution

Enkel substitution, eller monoalfabetisk substitution, använder ett enda *substitutionsalfabete*. Det betyder att varje bokstav i alfabetet har en fix bokstav som den byts emot. Det kanske enklaste exemplet på detta är det så kallade Caesarkryptot. Metoden man använder är att förflytta varje bokstav ett visst antal steg över alfabetet, så att till exempel a blir till d med ett skifte på 3 bokstäver. (Dessutom blir naturligtvis $ö$, om du använder ett svenskt alfabete, bytt mot c.)

Definition 1. *Enkel substitution genom förskjutning (Caesarkrypto)*
Låt en bokstav p representeras av dess position i alfabetet, med början i noll. Låt k vara det eftersträvade skiftet och låt a vara antalet bokstäver i alfabetet. Låt

$$c \equiv p + k \pmod{a}.$$

Då är c den kodade bokstaven från p.

Dekryptering följer direkt av definitionen

$$p \equiv c - k \pmod{a}.$$

Nyckeln i det här fallet är talet k. Utan det talet kan man inte lösa ut p från c.
Det finns (bland andra) ett stort problem med det här kryptot och det är antalet olika värden som k kan anta, eller med ett annat ord: *Nyckelmängden.* Nyckelmängden för Caesarkryptot är a, eftersom antalet möjliga skiften är samma som antalet bokstäver i alfabetet (även om ett skifte med 0 steg har ett något begränsat användingsområde).
Någon som har snappat upp en kryptotext av det här slaget, utan att känna till antalet skiften som använts, behöver alltså bara testa a olika nycklar, 29 stycken för ett svenskt alfabete, för att få fram den rätta texten.

Om vi istället tänker oss att varje bokstav byts mot en godtycklig bokstav i ett alfabete, så att till exempel a byts mot k och b mot f etc får vi ett mer generellt substitutionschiffer. Nyckeln är nu istället det givna substutitionsalfabetet.

Exempel 1. *Tabellen nedan är ett substitutionsalfabete, där varje bokstav kodas till den som ligger rakt under.*

Indata	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 å ä ö
Kryptotext	K F O G Q Ö A W S I Y T N D Å E Ä M B C J L P Z R U V X H

Ordet ”enigma” krypterad med substitutionsalfabetet i exemplet ovan blir ”QDSANK”.

Varje substitutionsalfabete av denna typ kan tolkas som en funktion från mängden bokstäver i alfabetet till sig själv. Då varje bokstav har en fix bokstav som den kodas till kan inte två olika bokstäver kodas till samma bokstav, det skulle omöjliggöra dekryptering. Vi gör följande definition.

Definition 2. *Låt A vara mängden bokstäver i alfabetet, och låt $\sigma : A \to A$ vara en funktion.*
Funktionen σ är ett substitutionsalfabete, eller utgör en enkel substitution över A, om

$$\sigma(x_1) = \sigma(x_2) \Rightarrow x_1 = x_2$$

för alla $x_1, x_2 \in A$.

Proposition 1. *Om σ är ett substitutionsalfabete över A, så är σ en permutation av A.*

Bevis. Att σ är ett substitutionsalfabete över A innebär att det är en injektiv funktion från en ändlig mängd till sig själv. Det följer att σ är surjektiv. Alltså är σ en bijektiv funktion från en mängd till sig själv och därmed en permutation. □

Det är inget konstigt resultat. En funktion som inte är bijektiv har ingen invers och skulle därför inte gå att dekryptera. Eftersom ett substitutionsalfabete är en permutation av bokstäverna kan den beskrivas på cyklisk form. I det tidigare exemplet (1) blir det

$$(akyrmndg)(bföhwpeqäxzujis)(coåvlt),$$

där bokstaven du får ut av kodningen skrivs direkt efter ursprungsbokstaven. Notera att a kodas till k som kodas till y o.s.v. och jämför med substitutionsalfabetet i exempel (1). Vad detta tillför blir tydligt när metoderna för att knäcka enigman diskuteras. För att ge ett exempel av många på hur teori för permutationer kan användas noterar vi följande resultat[1].

Definition 3. *Ordningen av en permutation är det minsta antalet gånger som du kan applicera permutationen på ett godtyckligt element och få tillbaka samma element.*

Proposition 2. *Låt σ vara en permutation skriven som en sammansättning av disjunkta cykler. Då ges ordningen för σ av den minsta gemensamma multipeln av cyklernas längder.*

Cyklerna i exempel (1) har längd 6, 8 och 15, vars minsta gemensamma multipel är 120. Det innebär att ett meddelande som kodats med det substitionsalfabetet 120 gånger om skulle förbli oförändrat.

Det finns en annan egenskap hos permutationerna som hjälper oss.

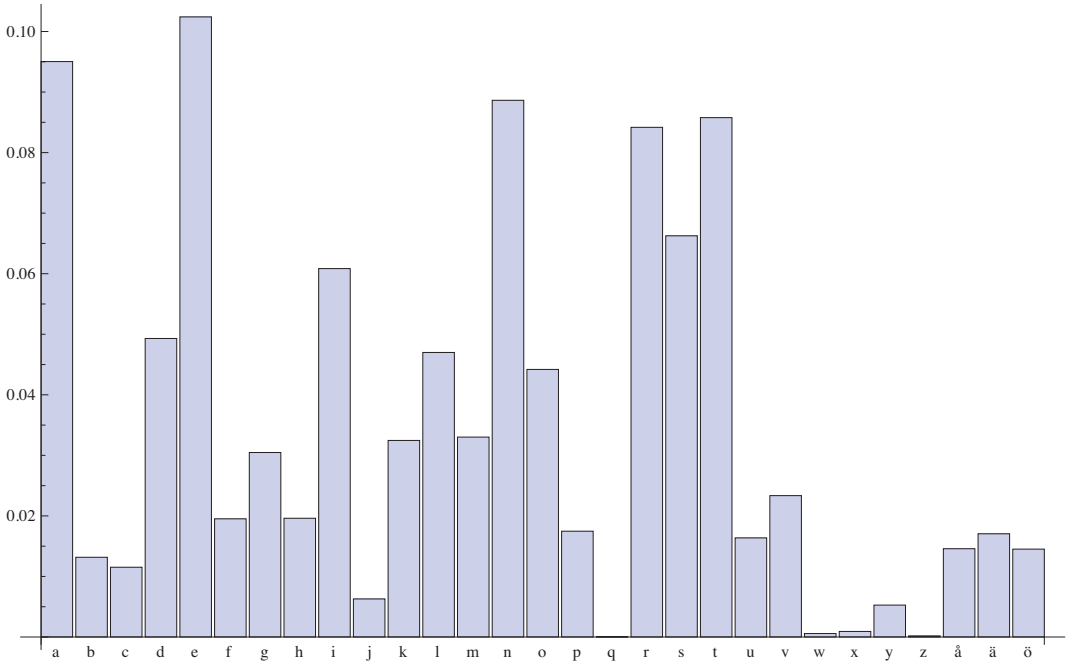
[1] Beachy, Blair - Abstract algebra sid. 80

Proposition 3. *Antalet permutationer på en mängd A ges av a! där a är antalet element i mängden A.*

Antalet permutationer är samma som antalet unika substitutionsalfabeten, alltså nyckelmängden. Vi vet således att nyckelmängden för ett enkelt substitionskrypto ges av $a!$, vilket är en betydande mängd. Det gör det i praktiken omöjligt att testa alla olika nycklar. (För ett alfabete med 29 bokstäver, som det svenska, får vi en nyckelmängd på $29! \approx 9 * 10^{30}$ olika alfabeten.) Tyvärr räcker inte detta för att få till ett tillförlitligt krypto. Då det är otympligt att forcera dessa krypton genom att pröva olika nycklar får man koncentrera sig på svagheter i själva kryptot, d.v.s. metoden att byta ut bokstäver mot andra.

2.1.1 Frekvensanalys

Ett sätt att attackera en enkel substitution är med hjälp av *frekvensanalys*.



Figur 1: Bokstavsfrekvens för svensk dagstidningstext

Figur 1 visar hur stor del av en textmassa en viss bokstav upptar. Tabellen är skapad efter ett antal artiklar hämtade från svensk dagspress[2]. Bokstäverna i en text skriven i ett visst språk tenderar att förekomma i en särskild

[2] 12 artiklar från Dagens Nyheter och Svenska Dagbladet.

frekvens. Denna frekvensdistribution gör sig dessutom märkbar vid ganska korta texter[3]. I en text skriven på svenska kan alltså bokstäverna antas dyka upp i en frekvens som liknar figur 1. Om man nu analyserar en kryptotext som är skriven på svenska och krypterad med enkel substition kan man ta ut frekvenserna på kryptotextens bokstäver och jämföra med frekvenserna för vanlig svensk text. Skulle till exempel bokstaven H förekomma med hög frekvens i texten motsvarar den förmodligen någon av de högfrekventa bokstäverna i svenskan, till exempel ett e eller ett a.

2.2 Polyalfabetisk substitution

På 1500-talet började det dyka upp krypton som använde olika substitutionsalfabeten för varje bokstav[4], vilket försvårar frekvensanalysen. Ett grundläggande sådant är Viegnérechiffret som tar ett ord som nyckel och utför ett Ceasarskifte för varje ny bokstav utifrån nyckeln.

Exempel 2. *Om vårt medelande är "plikten är angenäm först när den är gjord" och nyckeln är "AUG" kommer p att kodas till p. Detta motsvarar bokstaven A i nyckeln som ger ett skifte med 0 steg. l skiftas 20 steg (motsvarande U) till c och i skiftas 6 steg (motsvarande G) till o. När man får slut på nyckelordet börjar man bara om med det, som i tabellen nedan.*

Indata	p l i k t e n ä r a n g e n ä m f ö r s t n ä r d e n ä r g j o r d
Nyckel	A U G A U G A U G A U G A U G A U G A U G A U G A U G A
Kryptotext	p c o k k k n s x a e m e e e m z f r j z n s x d y t ä i m j f x d

Här syns att de tre bokstäverna *kte* ifrån "plikten" alla kodas till k och *enä* ifrån "angenäm" till e vilket sätter käppar i hjulen för en vanlig frekvensanalys. Vi kan skriva den här typen av kryptering som

$$c \equiv p + k(n) \pmod{a},$$

där k beror på vilken bokstav i ordningen den kodar.
Med nyckeln "AUG" får vi

$$k(n) = \begin{cases} 0 & \text{om } n \equiv 0 \pmod 3 \\ 20 & \text{om } n \equiv 1 \pmod 3 \\ 6 & \text{om } n \equiv 2 \pmod 3 \end{cases}$$

där 0, 20 och 6 är platsen i alfabetet för A, U och G respektive.

Perioden blir antalet bokstäver i nyckelordet. Det vill säga antalet tecken den kodar innan kodningen börjar om och använder samma nyckel som för

[3] H.F Gaines sid.74
[4] H.F Gaines sid.108

de tidigare tecknen. I figuren ovan motsvaras den av trean i $\pmod 3$.
Tittar man på kryptotexten i exempel (2) ser man att var tredje bokstav förblir oförändrad. Det kan vara en antydan till hur dessa krypton knäcks. Plockar man ut endast dessa okodade bokstäver ur kryptotexten och gör en frekvensanalys får man rätt frekvens på bokstäverna. En frekvensanalys av var tredje bokstav, om man börjar på den andra bokstaven i chiffertexten, ger också rätt frekvenser, men inte för rätt bokstäver. Det är att förvänta eftersom alla dessa bokstäver har skiftats 20 steg.
Om avståndet mellan bokstäverna är samma som perioden för kryptot, eller längden på nyckelordet, kommer de att ge en frekvensdistribution som man förväntar sig av en vanlig substitution. Det betyder att man kan testa perioder tills man får vanliga frekvenser på bokstäverna och sedan när perioden är hittad avgöra hur stort skiftet är för varje grupp bokstäver.

I termer av permutationer kommer en av 29 varianter för det svenska alfabetet att användas på varje bokstav.

Definition 4. *Låt R vara permutationen som skiftar varje bokstav i alfabetet till den nästföljande bokstaven i alfabetet.*

$$R = (abcdefghijklmnopqrstuvwxyzåäö).$$

Ett skifte med 2 bokstäver är R applicerat 2 gånger, eller R^2, osv till

$$\begin{aligned} R^2 &= (acegikmoqsuwyåöbdfhjlnprtvxzä), \\ &\vdots \\ R^{27} &= (aäzxvtrpnljhfdböåywusqomkigec) = R^{-2}, \\ R^{28} &= (aööäåzyxwvutsrqponmlkjihgfedcb) = R^{-1}. \end{aligned}$$

I exempel (2) med nyckeln ”AUG“ används alltså R^0 (identitet), R^{20} och R^6, i den ordningen. Vi kan i allmänhet beskriva Viegnérekryptot som $R^{k(n)}$. Man kan naturligtvis tänka sig att använda generella substitutionsalfabeten istället för R, som man skiftar mellan genom något val av nyckel. Enigman är ett exempel på ett sådant krypto.

3 Enigma

Enigmamaskinen består i grunden av 4 olika delar: rotorer, ringar, en växelpanel och en reflektor. Den har även ett tangentbord med 26 bokstäver, A-Z och en uppsättning av 26 lampor markerade med bokstäverna A-Z. När en bokstav på tangentbordet trycks in bildas en krets genom maskinens inre delar från tangentbordet till lamporna och den lampa som motsvarar den kodade bokstaven tänds. Dekrypteringen skedde genom motsatt förfarande, man tryckte in den kodade bokstaven på tangentbordet och fick ut bokstaven

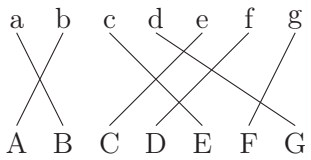
i ursprungsmeddelandet från den tända lampan. Det finns olika typer av enigmamaskiner som skiljer sig lite vad gäller antalet rotorer och liknande. För enkelhets skull beskrivs här bara en standardtyp med tre rotorplatser och fem olika rotorer samt en reflektor som inte roterar.

3.1 Rotorer

Roterande diskar, rotorer eller på tyska ”walzen”, är i princip de substitutionsalfabeten maskinen använder. Inuti rotorerna går det kopplingar som för kretsen från en position på ena sidan av disken till en annan position på den andra sidan. Rotorerna kopplas i serie och ”skiftas”, eller roteras, sedan för varje ny bokstav som skrivs in.

Ett skifte av den här typen är inte riktigt samma sak som att förflytta substitutionsalfabetet, som i fallet med caesarskiftet. Det illustreras enklast med ett exempel.

Exempel 3. *En fiktiv rotor G för ett alfabete på 7 bokstäver ser ut på följande sätt, där strecken mellan alfabetena markerar rotorns interna kopplingschema.*



I det här fallet kodas alltså b till A, c till E osv. Man kan beskriva substitutionsalfabetet i det här läget med

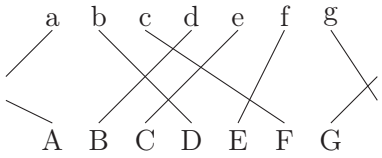
Rotor G

abcdefg
BAEGCDF

eller i cykelnotation $G = (ab)(ce)(dgf)$.

Ett skifte i denna rotor innebär att alla streck flyttas ett steg åt vänster. Då b tidigare kodats till A, följer den nu samma väg som c gjorde och kodas till D.

Exempel 4. *Kopplingarna för rotor G efter skifte med ett steg.*



Varje bokstav kodas alltså enligt det tidigare läget som om den vore nästföljande bokstav i alfabetet, men hamnar en bokstav längre bak.
Vi kan beskriva förfarandet i termer av permutationer på följande vis:

Definition 5. *Om R flyttar varje bokstav i alfabetet ett steg framåt och G är rotorns permutation för ett läge kan permutationen för nästa läge beskrivas av RGR^{-1}.*

Det följer att en rotor som skiftats n gånger från G beskrivs av R^nGR^{-n}.

Exempel 5. *En mer realistisk rotor som verkligen kan användas i enigman ser ut på nedanstående vis. Om ordet "enigma" krypteras utifrån det läget blir först e kodad till L. Sedan blir n kodad på samma sätt som o till Y men skiftas ner i alfabetet till X. I nästa steg kodas i på samma sätt som k till N och skiftas sedan ner två steg till L. På det sättet får vi till slut det krypterade meddelandet "LXLWTB".*

Rotor 1

abcdefghijklmnopqrstuvwxyz
EKMFLGDQVZNTOWYHXUSPAIBRCJ

Låt H vara permutationen som den ges av *Rotor 1* i exempel (5) ovan. R flyttar varje bokstav i alfabetet ett steg framåt. Grundinställningen för rotorn är k, hur många steg den är skiftad från början. Antalet instkrivna bokstäver är n.
Då ges substitutionsalfabetet för varje bokstav av $R^{k+n}HR^{-(k+n)}$, där k antar värden mellan 0 och 25.
Ett meddelande kodat i ett sådant system är alltså inte särskilt säkert. Känner man till hur rotorn ser ut behöver man bara testa de 26 olika utgångslägena för att hitta det rätta meddelandet.

Enigmamaskinen hade plats för 3 seriekopplade rotorer som var och en tillförde ett substitutionsalfabete. Varje bokstav översätts först av rotor 1, sedan av rotor 2 och sist av rotor 3.

Exempel 6. *Tre seriekopplade rotorer*

Indata	abcdefghijklmnopqrstuvwxyz
Rotor 1	EKMFLGDQVZNTOWYHXUSPAIBRCJ
Rotor 2	AJDKSIRUXBLHWTMCQGZNPYFVOE
Rotor 3	BDFHJLCPRTXVZNYEIWGAKMUSQO

I det här fallet skulle alltså a först kodas till E enligt Rotor 1, sedan skulle detta E kodas till S enligt Rotor 2 och sist kodas S till G vilket blir vår kodade bokstav. Detta är inte hela historien, enigmans reflektor och växelpanel som beskrivs nedan kommer att förändra bokstaven ytterligare.
I likhet med det tidigare exemplet skiftar Rotor 1 ett steg efter varje inlagd bokstav för att generera ett nytt substitutionsalfabete. När den 26:e bokstaven

är inskriven och Rotor 1 är tillbaka i sin ursprungsposition så skiftar Rotor 2 ett steg. Detta förändrar kodningen för samtliga positioner för Rotor 1 och den är fri att rotera 26 gånger till innan Rotor 2 stegar fram igen. Man kan alltså skriva in 26^2 bokstäver innan både Rotor 1 och 2 är tillbaka i sina ursprungspositioner och när det sker skiftar Rotor 3 ett steg. Tillsammans ger oss de tre rotorerna en period på $26^3 = 17576$. Det gör det i praktiken omöjligt att forcera enigman på samma sätt som för Viegnierekryptot. Visserligen kodas var 17576:e bokstav med samma substitutionsalfabete, men inget kryptomeddelande kommer att vara så långt att det skulle hjälpa.
Eftersom varje rotorposition i sig kan vara en startposition för krypteringen får vi även en nyckelmängd av rotorernas positioner på 26^3 olika nycklar. Maskinen använde visserligen 3 rotorer, men det var möjligt att plocka loss dem. Det innebar att man kunde byta själva rotorerna och sedan även vilken plats de satt på. En vanligt förekommande enigmamaskin hade 5 olika rotorer, vilket ger en nyckelmängd på

$$(5!)/(2!) \cdot 26^3 = 1054560$$

Definition 6. *Låt de tre rotorerna i användning vara J, K, L. Den första rotorn, J är den som skiftar varje gång en bokstav kodas. För varje helt varv som utförs av J skiftar K ett steg. För varje helt varv som utförs av K skiftar L ett steg.*

Hur en bokstav kodas i ett visst läge av tre seriekopplade rotorer kan då beskrivas som

$$R^x J R^{-x} R^y K R^{-y} R^z L R^{-z}$$

Eftersom J är den rotor som skiftar vid varje inslagen bokstav är det klart att exponenten x höjs med ett för varje bokstav. Det är också så att exponenten y höjs med ett för var sjugosjätte kodad bokstav och z höjs med ett för var 26^2 kodad bokstav. När dessa skiften sker är däremot inte klart. Det är något som bestäms av *ringarna*.

3.2 Ringar

Ringarna är i princip beteckningen man finner på rotorerna. På figuren i exempel (5) för Rotor 1 ser man ett substitutionsalfabete för ett visst läge på rotorn. (Där till exempel a kodas till E). Vi kallar den rotorpositionen A, vilket markeras med ett 'A' på ringen för rotorn. Efter att en bokstav skrivs in roterar rotorn som vanligt och hamnar i ett läge B, vilket markeras med ett 'B' på ringen. Det är dessa bokstäver som syns för enigmaoperatorn och som man ställer in rotorerna efter. Dessa ringar går att flytta på, så att deras relation med rotorns interna substitutionsalfabete förändras. I det här

läget kan man med rätta ifrågasätta ringarnas betydelse eftersom att ändra på ringens position är detsamma som att ändra rotorns position. En rotor där ringen är framflyttad ett steg och befinner sig i läge A kommer att koda ett meddelande på precis samma sätt som en orörd ring på rotorn i läge B. Anledningen till att ringinställningen över huvud taget spelar roll är att det är dessa som bestämmer när, under en rotors 26 steg, som nästa rotor flyttas ett steg. Figuren visar i vilken ringposition de 5 olika rotorerna har skiftat sin efterföljande rotor.

Rotor	Position
I	R
II	F
III	W
IV	K
V	A

I en maskininställning där I är den ”snabbaste” rotorn, det vill säga den som skiftas varje gång en bokstav skrivs in, kommer nästföljande rotor, den mittersta, att skifta när I går från Q till R.

Exempel 7. *Tabellen visar hur meddelandet ”Manchmal ist eine zigarre nur eine zigarre” krypteras med två olika ring- och rotorinställningar. Notera att kryptotexten blir likadan fram till att rotor II skiftar, vilket skiljer sig med tre bokstäver på grund av ringinställningarna.*

Indata	manchmalistein	ezi	garrenureinezigarre
Rotor I i läge A med ringinställning A			
I Position	ABCDEFGHIJKLMN	OPQ	RSTUVWXYZABCDEFGHIJ
II Position	AAAAAAAAAAAAAA	AAA	BBBBBBBBBBBBBBBBBB
Kodad text	HILLKKDOQBWMCE	CIU	RXXBRCLLXSDCKMZFAXL
Rotor1 i läge D med ringinställning D			
I Position	DEFGHIJKLMNOPQ	RST	UVWXYZABCDEFGHIJKLM
II Position	AAAAAAAAAAAAAA	BBB	BBBBBBBBBBBBBBBBBB
Kodad text	HILLKKDOQBWMCA	BNU	RXXBRCLLXSDCKMZFAXL

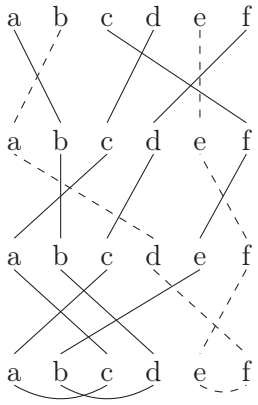
Ringarna har lika många olika lägen som rotorerna, alltså 26^3. Med ringar får vi då en nyckelmängd för Enigman av storleken

$$(5!)/(2!) \cdot 26^6 = 18534946560$$

3.3 Reflektor

Efter de tre rotorerna sitter det i enigmamaskinen en *reflektor*, eller på tyska “Umkehrwalze”. Reflektorn kopplar strömmen som kommer ur den sista rotorn

tillbaka in i rotorn igen på ett annat ställe.



Figur 2: *Enigmamaskin med tre rotorer och en reflektor så att B kodas till E, och E kodas till B.*

Strömmen går ifrån tangentbordet igenom de tre rotorerna. Reflektorn låter strömmen gå igenom de tre rotorerna igen, åt andra hållet. Den utgör ett *reciprokt* substitutionsalfabete, det vill säga ett som är sin egen invers[5]. Det innebär att om E kodas till B så kommer också B att kodas till E.

Definition 7. *En permutation där två bokstäver byts mot varandra kallas för en transposition.*

I cykelnotation blir varje transposition en cykel av längd 2. Ett reciprokt substitutionsalfabete består således endast av disjunkta transpositioner - bara cykler av längd 2. Undantaget är om en bokstav skulle kodas till sig själv, men det klarade inte reflektorn av, den måste låta strömmen gå tillbaka genom rotorerna en annan väg än den kom.

Exempel 8. *En fiktiv reflektor för ett alfabete med 6 bokstäver (a-f) ser ut på följande sätt, samma som i Figur 2:*

Reflektor

a b c d e f
C D A B F E

Den kan beskrivas med de tre disjunkta transpositionerna

$$(ac)(bd)(ef).$$

Det är reflektorn som gör så att enigmamaskinen kunde dekryptera ett meddelande på samma sätt som man krypterade det. Reflektorn roterade inte och tillförde därför inga fler möjliga nycklar. Däremot uteslöt den möjligheten för en bokstav att kodas till sig själv.

[5]Fouché Gaines, sid 70

Definition 8. *Låt T vara de disjunkta transpositioner som fås av reflektorn.*

Hur en bokstav kodas av de tre valda rotorerna tillsammans med reflektorn i ett visst läge (x, y, z) kan nu beskrivas som

$$R^x J R^{-x} R^y K R^{-y} R^z L R^{-z} T R^z L^{-1} R^{-z} R^y K^{-1} R^{-y} R^x J^{-1} R^{-x}.$$

Notera att denna permutation verkligen är reciprok. En sammansättning med sig själv ger identitetspermutationen.

3.4 Växelpanel

Enigmamaskinen var utrustad med en växelpanel, eller på tyska ”steckerverbindungen”. Den tillät två bokstäver att bli bytta mot varandra innan och efter de gått igenom rotorerna. Varje bokstav hade en motsvarande kontakt och de kunde bytas genom att koppla en sladd mellan två kontakter. Hade man till exempel kopplat en sladd mellan a och k så skulle varje a från tangentbordet kodas som ett k, och motsvarande ett k som ett a. Eftersom bytet också sker efter rotorerna blir varje bokstav som tidigare hade kodats till a istället ett k och tvärtom. Kryptot behöll sin reciproka karaktär, men antalet möjliga nycklar ökade drastiskt. Vid början av försöken att bryta enigman användes sex sådana sladdar, men det antalet steg ända upp till 10 mot slutet av kriget. Antalet sätt att koppla sex sladdar mellan 26 bokstäver ges av

$$\frac{26!}{2^6 14!} = 72282089880000.$$

Växelpanelen bidrog alltså med en faktor 72282089880000 till nyckelmängden. Det totala antalet nycklar för en enigmamaskin med tre rotorplatser, fem olika rotorer och sex sladdar i växelpanelen blir

$$(5!)/(2!) \cdot 26^6 \cdot \frac{26!}{2^6 14!} = 1339744673170916812800000.$$

Ett tal som antyder att det inte är läge att testa sig fram om man vill läsa ett meddelande krypterat med Enigman.

En enkel substitution ger som tidigare beskrivet ingen större säkerhet, men tillsammans med enigmans rotorer blev den kraftfull. Följande text exemplifierar detta.

Exempel 9. *Texten har kryperats med sex sladdar och sedan dekrypterats med samma inställningar men utan sladdar. De bokstäver som vi fått tillbaka i klartext markeras med fet stil.*

`In the thirtieth year in the fourth month on the fifth day while I was among the exiles by the Kebar River the heavens were opened and I saw visions of God`

GF RDE TXXRKKEKH TRRN IE VXE NACWTX MSTLX RF TXR QINCX DBT WFJPA J WAK BMAFG THZ EHTSEM FQ TXE KSPQR RIVEO LXL XFBSQLE WERQ SFVFPD BOF I IIW TQOISFM VN GSR

Vi ser direkt att de är alldeles för få för att det ska gå att lista ut vad ursprungsmeddelandet kan ha varit.
Växelpanelen är den sista biten som behövs för att beskriva Enigman.

Definition 9. *Låt S vara de (sex) disjunkta transpositioner som fås av kopplingarna i växelpanelen*

Nu ges permutationen som kodar varje bokstav i ett visst läge (x, y, z) av

$$SR^xJR^{-x}R^yKR^{-y}R^zLR^{-z}TR^zL^{-1}R^{-z}R^yK^{-1}R^{-y}R^xJ^{-1}R^{-x}S.$$

4 Hur Enigma lästes

De första som började angripa Enigman var kryptologerna på den Polska "kryptobyrån" Biuro Szyfrów. De var också framgångsrika med detta och kunde läsa den typ av Enigma som beskrivs här.

4.1 Polska Biuro Szyfrów

När arbetet med att knäcka Enigman drog igång, hösten 1932[6], användes maskinen på följande sätt:
Enigmamaskinisten ställde in maskinen efter dagens förutbestämda kod, eller *dagskod*. Denna distribuerades månadsmässigt[7] till de som skulle vara i samma nät så att de kunde kommunicera. Efter att dagskoden var inställd valde maskinisten själv en inställning på rotorerna, *meddelandenyckeln*, beskriven som tre bokstäver, och kodade den med dagsnyckeln. Utan en dagsnyckel hade varje kryptomeddelande som skickats den dagen kodats med samma inställningar. Det hade inneburit att den första bokstaven i varje meddelande kodats med samma substitutionsalfabete. Med tillräckligt många uppsnappade meddelanden skulle man alltså framgångsrikt kunna angripa Enigman genom att utföra en frekvensanalys på den första bokstaven i varje meddelande, sedan den andra o.s.v. tills dess att allt gick att läsa. Man valde även att denna meddelandenyckel skulle kodas *två* gånger om, för att försäkra sig om att den togs emot utan att störningar i radiosändningen skulle göra meddelandenyckeln och därmed hela meddelandet oläsligt[8]. Dessa sex bokstäver

[6]Rejewski How the polish mathematicians broke enigma. Appendix D till Kozaczuk, 1984 Enigma s.251

[7]Rejewski How the polish mathematicians broke enigma. Appendix D till Kozaczuk, 1984 Enigma s.256

[8]Rejewski How the polish mathematicians broke enigma. Appendix D till Kozaczuk, 1984 Enigma s.251

placerades först i meddelandet. Sedan ställde maskinisten in rotorerna efter sin valda meddelandenyckel och krypterade resten av meddelandet. Av de sex första bokstäverna i ett meddelande visste man att den första hade kodat samma bokstav som den fjärde, den andra som den femte och den tredje som den sjätte. Det skulle visa sig att denna dubbelinmatning var ett ödesdigert misttag. Polackerna utnyttjade detta för att knäcka kryptotexternas meddelandenycklar.

4.1.1 Meddelandenyckeln

En av kryptologerna på Biuro Szyfrów, Marian Rejewski, bjuder på ett exempel.

Exempel 10. *De sex första bokstäverna från tre olika uppsnappade meddelanden:*

$$dmq\ vbn$$
$$von\ puy$$
$$puc\ fmq$$

Det är okänt hur permutationen för den första bokstaven, kalla den A, ser ut. Det är även okänt hur permutationen för den fjärde bokstaven, D ser ut. Finns det någon möjlighet att ta reda på vad sammansättningen, AD, består av?
Från den första gruppen får vi faktiskt att för AD kodas d, den första bokstaven, till v, den fjärde. Oavsett vilken bokstav d motsvarar från början vet vi att sammansättningen AD gör d till v. Resonemanget lyder:

Låt x vara den okända första bokstaven i nyckeln.

Det är givet att $A(x) = d$ och $D(x) = v$. Reflektorn gör varje substitution reciprok, så $A(d) = x$. Från det följer $D(A(d)) = v$.
Från de två andra grupperna får vi sen att v blir p och p blir f. En del av en cykel för AD börjar visa sig:

$$dvpf$$

Med tillräckligt många meddelanden kunde man till slut återskapa hela permutationen.

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

Samma metod används för att plocka fram permutationerna för den andra till femte bokstaven och den tredje till sjätte.

$$BE = (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k),$$
$$CF = (abviktjgfcqny)(duzrehlxwpsmo).$$

Om än olika för varje dagsnyckel, ser dessa permutationer alltid ut på ett speciellt sätt. Cykler av samma längd dyker nämnligen upp parvis. I till exempel AD här så finns det två cykler av längd 10, två av längd 2 och två identiteter. Anledningen till det är reflektorn som gör att A, B, C etc. bara består av disjunkta transpositioner.

Proposition 4. *Om två permutationer X och Y har en cykeldekomposition som består av transpositioner och har samma antal transpositioner så kommer längderna på de disjunkta cyklerna i deras sammansättning, XY, förekomma parvis.*
Omvänt gäller också:

En permutation som består av disjunkta cykler, där cyklernas längder förekommer ett jämnt antal gånger, kan beskrivas som en sammansättning XY av två permutationer X och Y, som endast består av för sig disjunkta transpositioner.

Bevis. Låt X och Y vara två permutationer av samma mängd som endast består av disjunkta transpositioner.
Om en transposition (a, b) finns i både X och Y:s cykeluppdelning blir det i sammansättningen två identiteter, (a) och (b). De dyker således upp parvis.
För transpositioner som inte finns i båda, välj (a_1, b_1) i X men inte i Y. Då måste (a_2, b_1) finnas i Y. På samma sätt välj (a_2, b_2) i X men inte i Y. Då måste antingen (a_3, b_2) eller (a_1, b_2) finnas i Y. Vi kan därför anta att för något k så finns
$(a_1, b_1), (a_2, b_2) \ldots, (a_k, b_k)$ i X och
$(a_2, b_1)(a_3, b_2), \ldots, (a_1, b_k)$ i Y
XY innehåller således, $(a_1, a_2, \ldots, a_k)(b_1, b_2, \ldots, b_k)$ och varje transposition som finns i X men inte i Y tillhör en sådan kedja.
Det omvända: En permutation som består av disjunkta cykler, där cyklernas längder förekommer ett jämnt antal gånger, kan beskrivas som en sammansättning XY av två permutationer X och Y, som var för sig består av disjunkta transpositioner.
Detta ges direkt av att $(a_1, a_2, \ldots, a_k)(b_1, b_2, \ldots, b_k)$ beskrivs av sammansättningen av de för sig disjunkta transpositionerna $(a_1, b_1)(a_2, b_2) \ldots (a_k, b_k)$ och $(a_2, b_1), (a_3, b_2), \ldots, (a_1, b_k)$ □

Vidare gäller också följande resultat, som ges utan bevis men följer av liknande resonemang:

Proposition 5. *För två permutationer X och Y som i proposition* (4)

1. *Antag att (a, b) är en transposition i X eller Y. Då kommer a och b att tillhöra två distinkta cykler i XY, av samma längd.*

2. *Om två bokstäver som finns i två olika cykler av samma längd i XY tillhör samma transposition så kommer bokstäverna brevid dem (de till höger och de till vänster) också att tillhöra samma transposition.*

Tillsammans med resultaten för sammansättningar av disjunkta transpositioner räckte det nu med kvalificierade gissningar för hur enigmaoperatörerna skulle välja sina meddelandenycklar. Man antog att många av dessa nycklar skulle vara tre identiska bokstäver efter varandra. Om någon av meddelandenycklarna är "aaa", så skulle enligt proposition (5) det första a:et kodas som ett s eftersom a och s i sammansättningen AD är de enda bokstäver som utgör cykler av längd ett. Vi antar att ur de kodade meddelandena från en viss dag återfinns dessa tre nycklar som börjar med bokstaven 's':

$$sig\ smf$$
$$sjm\ spo$$
$$syx\ scw$$

Den första kodade nyckeln, "sig smf" kan inte motsvara bokstäverna "aaa" eftersom den andra bokstaven, 'i', återfinns i en cykel med längd nio i sammansättningen BE medan 'a' ligger i en cykel med längd tre. På samma sätt kan inte den andra kodade nyckeln, "sjm spo" motsvara bokstäverna "aaa" då även 'j' ligger i cykeln med längd nio. Den tredje nyckelsekvensen däremot, "syx scw" skulle kunna ha uppkommit ur bokstäverna "aaa". I AD ligger 'a' och 's' i olika cykler av längd ett. I BE finns 'y' och 'a' i olika cykler av längd tre och i CF finns 'x' och 'a' i olika cykler av längd tretton. Antar vi nu att den här nyckeln faktiskt motsvarar "aaa" och ur det antagandet kan härleda många fler nycklar som består av liknande upprepningar, "bbb", "ccc" och så vidare, sluter vi oss till att det var ett korrekt antagande. En jämförelse med dagens lösenord är inte helt främmande. Genom allt för enkelt valda meddelandenycklar lyckades matematikerna på Biuro Szyfrów att lista ut meddelandenycklarna utan kunskap om vare sig dagsnycklarna eller kopplingarna i enigmans rotorer.

4.1.2 Rotorkopplingarna

Meddelandenycklarna kunde nu bestämmas, men polackerna visste inte hur kopplingarna i rotorerna såg ut.

Det finns en egenskap hos permutationer av formen $G^{-1}NG$ som kommer till användning här.

Proposition 6. *Låt G och N vara permutationer av A. Det gäller att $G^{-1}NG$ kommer att ha samma cykliska representation som N, där varje element i cyklerna blivit permuterad av G. Vi säger att $G^{-1}NG$ är N* konjugerat *med G.*

Bevis. Låt N beskriven på cyklisk form vara något

$$N = (x_1, x_2, \ldots, x_n)(y_1, \ldots, y_m)\ldots(z_1, \ldots, z_l).$$

Betrakta elementet $G(x_1)$. Det gäller att

$$G^{-1}NG(G(x_1)) = G(N(G^{-1}(G(x_1)))).$$

Eftersom

$$G^{-1}(G(x_1)) = x_1,$$

samt, från den cykliska framställningen av N

$$N(x_1) = x_2,$$

får vi till slut

$$G(N(G^{-1}(G(x_1)))) = G(x_2)$$

och en del av en cykel visar sig

$$(G(x_1), G(x_2), \ldots).$$

Till slut har vi att

$$G(N(G^{-1}(G(x_n)))) = G(x_1),$$

och cykeln är sluten. Samma resonemang gäller naturligtvis för de andra cyklerna i N

$$G^{-1}NG = (G(x_1), G(x_2), \ldots, G(x_n))(G(y_1), \ldots, G(y_m))\ldots(G(z_1), \ldots, G(z_l)).$$

□

Det här innebär att man kan, givet ett uttryck $G^{-1}NG$, samt N, lista ut hur G skulle kunna se ut.

Exempel 11. *Vi har två permutationer givna,*

$$N = (adbc)(fe),$$
$$G^{-1}NG = (afbe)(dc).$$

Vi vet från Proposition (6) att

$$G^{-1}NG = (G(a), G(d), G(b), G(c))(G(f), G(e)), \text{ det vill säga,}$$
$$(afbe)(dc) = (G(a), G(d), G(b), G(c))(G(f), G(e)).$$

Nu skulle man kunna vara frestad att matcha varje element rakt av, så att

$$a = G(a), f = G(d), b = G(b), e = G(c), d = G(f), c = G(e),$$

och därmed få fram G.

G

adbc fe
AFBE DC

eller $G = (a)(b)(ce)(fd)$.

Genom att skriva $G^{-1}NG$ direkt under N får vi alltså ett uttryck som borde kunna vara G. Men notera att en cykelframställning inte är unik. Samtliga följande cykler beskriver samma permutation

$$(afbe),\ (fbea),\ (beaf),\ (eafb).$$

Varje cykel har alltså lika många representanter som dess längd. I exempel (11) har $G^{-1}NG$ en cykel av längd 4 och en av längd 2, och kan representeras på $4 \cdot 2 = 8$ olika sätt.

$$(afbe)(dc),\ (fbea)(dc),\ (beaf)(dc),\ (eafb)(dc),$$
$$(afbe)(cd),\ (fbea)(cd),\ (beaf)(cd),\ (eafb)(cd).$$

Var en av dessa ger alltså en egen kandidat för G när den skrivs under N.

Vi drar oss nu till minnes hur permutationerna för enigmamaskinen beskrivs

$$SR^xJR^{-x}R^yKR^{-y}R^zLR^{-z}TR^zL^{-1}R^{-z}R^yK^{-1}R^{-y}R^xJ^{-1}R^{-x}S^{-1}.$$

Lösandet av meddelandenycklarna gav dessutom sex permutationer, A till F. Under antagandet att endast den första rotorn stegade fram för de första sex inkodade bokstäverna kan de representeras som följande:

$$\begin{aligned} A &= SJKLTL^{-1}K^{-1}J^{-1}S, \\ B &= SR^1JR^{-1}KLTL^{-1}K^{-1}R^1J^{-1}R^{-1}S, \\ &\vdots \\ F &= SR^5JR^{-5}KLTL^{-1}K^{-1}R^5J^{-1}R^{-5}S. \end{aligned}$$

För att lätta upp notationen något, kallar vi det gemensamma uttrycket $KLTL^{-1}M^{-1}$ för Q.

$$KLTL^{-1}M^{-1} = Q.$$

Detta lämnar sex ekvationer med fyra okända permutationer

$$\begin{aligned} A &= SJQJ^{-1}S, \\ B &= SR^1JR^{-1}QR^1J^{-1}R^{-1}S, \\ &\vdots \\ F &= SR^5JR^{-5}QR^5J^{-1}R^{-5}S. \end{aligned}$$

I just detta läge av arbetet dimper det ner från den franska underrättelsetjänsten fotograferade bilder på två tabeller av dagsnycklar, alltså två månaders dagsnycklar för Enigmatrafiken. I dessa dagsnycklar återfinns växelpanelens inställningar vilket innebar att permutationen S kunde betraktas som känd och flyttas över till vänsterledet. Även R är känd och kunde därför också flyttas. Vi utför operationerna och betecknar de nya permutationerna med bokstäverna U till Z.

$$\begin{aligned} U &= SAS = JQJ^{-1}, \\ V &= R^{-1}SBSR = JR^{-1}QR^{1}J^{-1}, \\ &\vdots \\ Z &= R^{-5}SFSR^{5} = JR^{-5}QR^{5}J^{-1}. \end{aligned}$$

Sedan slår vi samman dem på följande vis, en operation som kan verka underlig för tillfället men vars förklaring kommer.

$$\begin{aligned} UV &= \quad J(QR^{-1}QR)J^{-1}, \\ VW &= JR^{-1}(QR^{-1}QR)RJ^{-1}, \\ &\vdots \\ YZ &= JR^{-4}(QR^{-1}QR)R^{4}J^{-1}. \end{aligned}$$

Nu kan vi, genom att eliminera det gemensamma uttrycket $QR^{-1}QR$ erhålla fyra ekvationer med endast en okänd, nämnligen JRJ^{-1}.

Vi uttrycker $QR^{-1}QR$ i termer av UV och J.

$$\begin{aligned} UV &= J(QR^{-1}QR)J^{-1} \Leftrightarrow \\ J^{-1}UVJ &= \quad QR^{-1}QR. \end{aligned}$$

Sedan inför vi den istället för $QR^{-1}QR$ i uttrycket för VW,

$$VW = JR^{-1}J^{-1}(UV)JRJ^{-1}.$$

På samma sätt får vi de nästföljande tre ekvationerna,

$$\begin{aligned} WX &= JR^{-1}J^{-1}(VW)JRJ^{-1}, \\ XY &= JR^{-1}J^{-1}(WX)JRJ^{-1}, \\ YZ &= JR^{-1}J^{-1}(XY)JRJ^{-1}. \end{aligned}$$

Nu kommer Proposition (6) in i bilden. Notera att VW är UV konjugerat med JRJ^{-1}, XY är VW konjugerat med JRJ^{-1} och så vidare. Genom att skriva WV under UV på alla möjliga sätt får vi ett gäng kandidater till JRJ^{-1}. Sedan skriver vi XY under WV på alla möjliga sätt och får igen ett antal kandidater till JRJ^{-1}. Någon av dessa kommer att vara identiska, och detta är vårt JRJ^{-1}.

Detta hade även gått att utföra utan att slå samman uttrycken $U, V, \ldots, Z$ parvis. Då hade däremot varje permutation bestått av endast transpositioner, och att skriva ut tretton transpositioner under varandra går att göra på

$$13! \cdot 2^{13} = 51011754393600$$

olika sätt. Genom att sätta samman dessa transpositioner med varandra hoppas vi på att få permutationer med längre cykler.

Nu har vi alltså uttrycket JRJ^{-1}. Vi noterar återigen att detta är R konjugerat med J^{-1}. Permutationen R består av en cykel av längd 26 vilket betyder att vi får 26 kandidater för rotorn J. Dessa kommer endast att skilja sig åt genom att det är olika mycket vridning av rotorns två sidor beroende på hur stort skifte som JRJ^{-1} har skrivits under R. Vilken av dessa som verkligen stämmer vet man inte än, men alternativen är väldigt få och skillnaden mellan dem regelbunden.

Metoden fungerar för att ta reda på rotorkopplingarna i den första rotorn. Nu behövde man bara vänta på att det skulle komma en dagsnyckel där en annan rotor tog den första positionen i maskinen för att få tag i dess interna kopplingar.

Exempel 12. *För att exemplifiera metoden som användes för att lista ut rotorkopplingarna hittar vi på följande låtsasmaskin med ett alfabete på sex bokstäver, där de tre rotorernas interna kopplingar i ursprungsläget är som i Figur 2,*

$$\begin{aligned} J &= (ab)(cfd)(e), \\ K &= (adc)(b)(ef), \\ L &= (ac)(bdfe). \end{aligned}$$

samt reflektorn given av de tre transpositionerna

$$T = (ac)(bd)(ef).$$

För enkelhetens skull skippas här växelpanelen.

Denna maskin känner vi inte till. Däremot känner vi, tack vare dåligt valda meddelandenycklar, de 4 första permutationerna (istället för 6, då vi

har ett mindre alfabet)

$$\begin{aligned}
A &= (ac)(be)(df) = JQJ^{-1},\\
B &= (ac)(bf)(de) = RJR^{-1}QRJ^{-1}R^{-1}.\\
C &= (ac)(bf)(de) = R^2JR^{-2}QR^2J^{-1}R^{-2}.\\
D &= (ab)(cd)(ef) = R^3JR^{-3}QR^3J^{-1}R^{-3}.
\end{aligned}$$

Sedan flyttas den kända permutationen R över till vänstersidan och ger oss fyra nya permutationer som vi benämner med U till X

$$\begin{aligned}
U &= (ac)(be)(df) = JQJ^{-1},\\
V &= (ac)(bd)(ef) = JR^{-1}QRJ^{-1},\\
W &= (af)(bd)(ce) = JR^{-2}QR^2J^{-1},\\
X &= (af)(bc)(de) = JR^{-3}QR^3J^{-1}.
\end{aligned}$$

Därefter slås de samman parvis till

$$\begin{aligned}
UV &= (a)(bf)(c)(de) = J(QP^{-1}QP)J^{-1},\\
VW &= (ae)(b)(cf)(d) = JR^{-1}J^{-1}(UV)JRJ^{-1},\\
WX &= (a)(be)(cd)(f) = JR^{-1}J^{-1}(VW)JRJ^{-1}.
\end{aligned}$$

Genom att nu skriva VW under UV på samtliga sätt får vi kandidater till JRJ^{-1}. Eftersom de består av två cykler av längd ett och två cykler av längd två kan detta göras på $2^4 = 16$ olika sätt. Men notera att resultatet ska bli JRJ^{-1}, alltså J^{-1} konjugerat med R. En sådan permutation har endast en cykel, i det här fallet av längd sex. Vi kan därför skippa alla alternativ där det är uppenbart att flera cykler kommer att bildas, till exempel när samma bokstav är skriven under sig själv. Några exempel där VW skrivet under UV ger upphov till endast en cykel är

UV	`a bf c de`	JRJ^{-1}
VW	`b ea d fc`	(abecdf)
VW	`d ae b fc`	(adfecb)
VW	`d ea b cf`	(adcbef)

Nu gör vi samma sak med WX skrivet under VW,

VW	`ae cf b d`	JRJ^{-1}
WX	`eb dc f a`	(aebfcd)
WX	`dc be a f`	(adfecb)

och där hittar vi ett likadant uttryck för JRJ^{-1} i de två tabellerna, nämnligen

$$JRJ^{-1} = (adfecb).$$

Nu återstår bara att skriva denna permutation under R på samtliga sex sätt.

R	`abcdef`	J^{-1}
JRJ^{-1}	`adfecb`	(a)(bdecf)
JRJ^{-1}	`dfecba`	(adcebf)
JRJ^{-1}	`fecbad`	(afdbe)(c)
JRJ^{-1}	`ecbadf`	(aed)(bc)(f)
JRJ^{-1}	`cbadfe`	(ac)(b)(d)(ef)
JRJ^{-1}	`badfec`	(ab)(cdf)(e)

Det sista av dessa uttryck för J^{-1} ger

$$J = (ab)(cfd)(e),$$

vilket är precis den yttersta rotorn i vårt exempel.

4.1.3 Dagsnycklarna

De polska matematikerna hade nu klart för sig hur maskinen såg ut, men utan nyckeln ska inte ett krypto värt namnet gå att läsa. För att lista ut vad dagsnyckeln var gick man tillbaka till de sex första permutationerna, eller snarare deras sammansättningar,

$$AD, BE, CF.$$

På grund av växelpanelens förfarande att byta bokstäver innan och efter de kodades av rotorerna betyder det att de transpositioner som den består av konjugerar permutationen som skapas av maskinens inre. Den här egenskapen överförs till sammansättningen. Om vi tittar på en av dessa blir det tydligt.

$$AD = SJQJ^{-1}R^3JR^{-3}QR^3J^{-1}R^{-3}S.$$

Detta innebar att oavsett växelpanelens inställning för en viss dag så skulle inte cykellängderna i de tre sammansättningarna förändras. Dessa tre permutationer hade den egenskapen, från Proposition (4), att cykellängderna dök upp parvis. Eftersom en viss konfiguration av de tre sammansättningarnas cykellängder inte återkommer för många rotorinställningar satte man igång att undersöka dessa längder för samtliga rotorpositioner. För att undersöka samtliga rotorposition (av vilka det finns 26^3 stycken för varje rotorkonfiguration) byggdes en maskin som kallades för *cyklometer* som bestod av två uppsättningar av tre rotorer. Den ena uppsättningen var inställd tre skiften framför den andra och genom att sluta kretsen genom båda dessa fick man till sammansättningen av de maskininställningar som var tre bokstäver från varandra. Nu kunde man katalogisera antalet cykler och dess längder för samtliga rotorpositioner. När sedan dagsnyckeln skulle lösas jämförde man

bara dess uppsättning cykler med dem i katalogen. Växelpanelns inställning följde sedan direkt genom att jämföra vilka bokstäver som blivit utbytta i dagens cykler mot katalogens cykler. När samtliga positioner hade blivit katalogiserade skriver Rejewski att det handlade om ett arbete på 10 till 20 minuter att rekonstruera dagsnyckeln.

4.2 England och Frankrike

Under möten mellan representater för underrättelsetjänsterna i Polen, England och Frankrike hade den polackerna hållit hemligt att de under en tid läst Engimakrypterad traffik. Men när kriget hängde över Polen, i juli 1939, kallades på nytt ett möte. Här avslöjades att de polska kryptologerna fullständigt hade rekonstruerat Enigmamaskinen, och att fransmännen och engelsmännen skulle få med sig en kopia var. De brittiska representaterna, som inte lyckats forcera maskinen, beskrivs som ”mållösa” över polackernas framgånger med Enigman.

Efter krigets utbrott flyr många polska kryptologer till Frankrike och fortsätter där en tid arbetet med att läsa Enigmatrafik. Engelska Bletchley Park, med den namnkunnige Alan Turing, arbetar under hela kriget med att läsa tysk trafik. Det är värt att notera att tyskarna under hela kriget genomförde förändringar i sitt sätt att använda Enigman. Bland annat så lades flera rotorer och sladdar i växelpanelen till. Sättet att kryptera meddelandenycklarna förändrades och intensiteten av förändringar i rotorpositioner och annat stegrades. För att hålla takten med dessa förändringar krävdes ett mycket skickligt kryptologiskt arbete från Bletchley Park, vars vidare beskrivning tyvärr ligger utanför omfånget för denna text.

4.3 Sverige

Slutligen är det värt att nämna att det även fanns svenska kryptologiska framgångar under andra världskriget. Uppsalaprofessorn Arne Beurling lyckades knäcka den tyska ”G-maskinen”, eller på tyska Geheimfernschreiber, som liknade Enigman. Maskinen användes för att kryptera teleprintertrafik och användes av tyskarna bland annat för att kryptera trafik mellan Tyskland och Norge, som då gick över svenska ledningar.

Referenser

[1] H. F. Gaines, *Cryptanalysis*. Dover Publications, Inc, 1956.

[2] W. Kozaczuk, *Enigma*. Arms and Armour press, 1984.

[3] J Hoffstein, J. Piper och J. H. Silverman, *An introduction to mathematical cryptography*. Springer, 2008.

[4] J. A. Beachy och W. D. Blair *Abstract algebra* Waveland Pr, Inc, 2006.

[5] B. Beckman, *Svenska kryptobedrifter*. Albert Bonniers förlag, 2006.