Marian Rejewskis brydning af Enigma

Allan Lind Jensen

March 4, 2020

1 Indledning

Denne artikel forklarer den polske matematiker, Marian Rejewskis, brydning af den tyske hærs kodemaskine, Enigma, i 1931. Metoden er forklaret i [1], som denne artikel bygger på. Det er også interessant at læse Rejewskis egen forklaring, se [3]. Formålet er at forklare Rejewskis metode på den enklest mulige måde. Læseren lærer at gennemføre Rejewskis beregning, dog med en forsimplet Enigma og med et alfabet med kun seks bogstaver. Efter at have arbejdet med denne forklaring, kan man prøve at læse [1] med den fulde forklaring brugt på den fulde maskine.

Enigma er navnet på mange forskellige maskiner startende med den kommercielle fra cirka 1920 og sluttende med den tyske marines langt mere sikre maskine fra 1942. I [2] findes et appendix med tidslinien.

Læseren formodes at kende til opbygningen af Enigma. Den er forklaret mange steder på internettet, for eksempel

http://www.matematiksider.dk/enigma.html

Denne artikel har to dele. Den første drejer sig om at beskrive kodningen ved en matematisk afbildning og finde et udtryk for den. I den anden del forklares først, hvordan Marian Rejewski kunne afkode de første seks bogstaver - beskedens nøgle. Endelig vises beregningen af ledningsføringen i den roterende ring og reflektoren. Dette er det første og sværeste trin i brydningen af Enigma. I december 1932 begyndte polakkerne at kunne læse beskeder koden med Enigma.

2 Matematiseringen

Enigmaen er en maskine der erstatter hvert bogstav med et andet, der er altså tale om en substitutionskode. Pointen er, at hvert bogstav har sin egen oversættelse, fordi hjulene skifter ved hvert bogstav. Man kan derfor ikke anvende frekvensanalyse på den enkelte besked. Hvis beskederne er sendt med forskellige startindstillinger kan man end ikke bruge frekvensanalyse på første bogstav.

For at gøre matematikken overskuelig betragter vi en maskine, der består af en reflektor og kun ét hjul. Først betragtes reflektoren og hjulet hver for sig, bagefter betragtes kombinationen af dem.

2.1 Reflektoren

I dette afsnit antages at reflektoren forbinder tasterne direkte til pærene, altså at rotoren er taget ud. Operatøren taster et bogstav, og når strømmen sluttes, lyser en af pærene op, og viser det resulterende bogstav. For eksempel taster operatøren et "A", og pæren "Q" lyser. Vi skriver

$$R(A) = Q \ ,$$

hvor A'et og Q'et er bogstaverne, og R'et angiver virkningen af reflektoren på bogstavet[1]. Det er den samme notation, som bruges for funktioner, for eksempel $f(2) = 5$. Reflektoren forbinder ledningerne mellem tasten og pæren "A" med ledningen mellem tasten og pæren "Q". Når operatøren taster "A" afbrydes først forbindelsen til pæren "A". Lidt senere forbindes ledningen til batteriet, og strømmen løber gennem pæren "Q".

Der blev brugt et alfabet med de 26 bogstaver "A" til "Z". Reflektoren bestod af 13 ledninger, der forbandt bogstaverne parvis.

Opgave 1 *Med et alfabet med kun fire bogstaver ville reflektoren have tre mulige ledningsføringer. Med et alfabet med seks bostaver ville reflektoren have* 15 *mulige ledningsføringer. Gør rede for dette, og beregn antallet af mulige ledningsføringer i Enigmas reflektor.*

Opgave 2 *Gør rede for at hvis $R(x) = y$, så gælder også $R(y) = x$.*

Opgave 3 *Gør rede for at der ikke findes nogen bogstaver x, der opfylder $R(x) = x$.*

Opgave 4 *Tegn en ledningsføring i en reflektor til et alfabet med kun seks bogstaver. Lav en tabel, $R(A), R(B), \ldots R(F)$. Lav en tabel,*

$$R(R(A)), R(R(B)), \ldots R(R(F)) \ .$$

I det følgende vil vi kortere skrive $RR(A), RR(B), \ldots RR(F)$, eller endnu kortere $R^2(A), R^2(B), \ldots R^2(F)$

2.2 Rotoren

Rotoren forbinder 26 kontakter på den ene side med 26 kontakter på den anden side. Alle kontakterne skal forbindes, og der udgår præcis én ledning fra hver kontakt. Den hurtigste rotor betegnes ofte N, så afbildningen af bogstaverne betegnes her med samme bogstav, N.

Antag at $N(A) = A, N(B) = C, N(C) = D$ og $N(D) = B$ i et alfabet med fire bogstaver. Den omvendte afbildning N^{-1} afbilder så $A \mapsto A, B \mapsto D, C \mapsto B$ og $D \mapsto C$. [2]

Opgave 5 *Tegn de to sæt af fire kontakter og ledningsføringen fra eksemplet ovenfor. Marker retningen af de to afbildninger N opg N^{-1}. Traditionelt går N fra højre mod venstre. Udfør tegningen, så det er opfyldt.*

[1] Bogstavet R bruges både som et bogstav i meddleelsen og i koden, og som afbildningen foretaget af reflektoren. Formlen $R(R) = N$ betyder at bogstavet "R" afbildes over i "N" ved afbildningen R.

[2] Hvis dette ikke er klart, skal du måske læse afsnittet om omvendte funktioner i lærebogen igen.

Det næste trin er at forbinde rotoren og reflektoren.

Opgave 6 *Tegn en rotor i et alfabet med seks bogstaver, og forbind den med reflektoren fra opgave 4. Følg ledningen fra hvert bogstav til højre på rotoren, til den ender igen. Det er kodningen af det før ste bogstav. Lav en tabel over resultaterne. Opskriv også afbildningerne N, R og N^{-1}. Lav endelig en tabel over afbildningerne NRN^{-1} og $N^{-1}RN$. Hvilken passer med kodningen?*

Fra tasten af går ledningen gennem rotoren N, dernæst gennem reflektoren, R, og endelig baglæns gennem rotoren N. Derfor skulle afbildningen gerne være givet ved den sidste formel i opgave 6.

2.3 Rotoren drejes

Opgave 7 *Brug rotoren fra opgave 5. Drej den én tak fra A mod B. Opskriv en tabel over virkningen af den drejede rotor.*

At finde afbildningen af den drejede rotor ud fra N selv er ikke helt enkelt. Man skal bruge en afbildning, der drejer alfabetet. Den kaldes s, og er defineret ved

$$s(A) = B, s(B) = C, \ldots, s(Z) = A \ ,$$

eller kortere

$$s : A \mapsto B \mapsto \ldots \mapsto Z \mapsto A \ .$$

Opgave 8 *I et alfabet med fire bogstaver er drejningen $s : A \mapsto B \mapsto C \mapsto D \mapsto A$. Opskriv en tabel over de fire afbildninger $sN, s^{-1}N, Ns$ og Ns^{-1}. Minder nogen af dem om virkningen af den drejede rotor? Gentag øvelsen med rotoren fra opgave 6*

Ved arbejdet med opgaven ovenfor kan man nå frem til at den drejede rotor har afbildningen sNs^{-1}. Det er faktisk ikke så svært af indse. Man kan lade rotoren stå stille og i stedet for dreje resten af verden ét hak den modsatte vej. Bogstavet B kommer derfor ind i A's kontakt. På venstre side sker det samme, men retningen er modsat: bogstavet A kommer ud i B's kontakt.

Kodningen af det første bogstav starter faktisk med den drejede rotor. Når operatøren trykker på en taste sker der tre ting: Først afbrydes forbindelsen til pæren; så drejes rotoren ét hak, og endelig forbindes ledningen til batteriets pluspol.

Først føres strømmen gennem den drejede rotor. Dernæst gennem reflektoren. Endelig føres ledningen baglæns gennem den drejede rotor. Det er den modsatte afbildning af sNs^{-1}. Der skal bruges et udtryk for denne afbildning.

Opgave 9 *Brug eksemplerne med de drejede rotorer fra de tidligere opgaver. Lav en tabel over den omvendte afbildning. Lav også en tabel med afbildningerne $sN^{-1}s^{-1}$ og $s^{-1}N^{-1}s$.*

Nu kan kodningen af hvert bogstav i teksten opskrives,

$$A = s^1N^{-1}s^{-1}Rs^1Ns^{-1} \tag{1}$$
$$B = s^2N^{-1}s^{-2}Rs^2Ns^{-2} \tag{2}$$
$$C = s^3N^{-1}s^{-3}Rs^3Ns^{-3} \tag{3}$$
$$D = s^4N^{-1}s^{-4}Rs^4Ns^{-4} \tag{4}$$
$$\vdots$$

Vi følger Rejewski og kalder de første seks kodninger for $A, B, \ldots, F$.

Opgave 10 *Hvad i alverden betyder med s^{-2}? Opskriv en tabel over afbildningerne s^2 og s^{-2}.*

Man kan se ud fra regneudtrykket afkodningen foretages på samme måde som kodningen. Der gælder

$$\begin{aligned}
A^2 &= (s^1N^{-1}s^{-1}Rs^1Ns^{-1}) \circ (s^1N^{-1}s^{-1}Rs^1Ns^{-1}) \\
&= s^1N^{-1}s^{-1}Rs^1Ns^{-1}s^1N^{-1}s^{-1}Rs^1Ns^{-1} \\
&= s^1N^{-1}s^{-1}Rs^1NN^{-1}s^{-1}Rs^1Ns^{-1} \\
&= s^1N^{-1}s^{-1}Rs^1s^{-1}Rs^1Ns^{-1} \\
&= s^1N^{-1}s^{-1}RRs^1Ns^{-1} \\
&= s^1N^{-1}s^{-1}s^1Ns^{-1} \\
&= s^1N^{-1}Ns^{-1} \\
&= s^1s^{-1} = Identiteten\ .
\end{aligned}$$

Identiteten er afbildningen, der fører ethvert bogstav over i sig selv. Der gælder altså $Identiteten(A) = A$ og så videre.

Opgave 11 *Reducer på tilsvarende måde B^2 og C^2 Forklar hvert trin i udregningen.*

Opgave 12 *Gør rede for at kodningerne hver består af 13 parvise ombytninger af bogstaver. Gør specielt rede for at intet bogstav kan kodes over i sig selv. (Det anses i dag som en svaghed ved systemet, der i sig selv ville være tilstrækkeligt at at afvise krypteringsalgoritmen.)*

3 Brydningen

Et kryptosystem omfatter alt det, der er nødvendigt for at hemmeligholde den overførte information. Regler for hvor ofte en bestemt nøgle må bruges; hvor lange beskeder der må sendes med samme nøgle; hvordan nøglerne, som jo også skal hemmeligholdes, fordeles til brugerne; og selvfølgelig algoritmer til kodningen og afkodningen af informationen.

Man går ud fra, at dem der lytter, kender princippet i algoritmen. For eksempel kendte polakkerne opbygningen af maskinen og protokollen for den daglige brug i felten. Man havde købt et eksemplar af den kommercielle Enigma, og en spion havde købt en instruktionsbog til hærens operatører af en tysk officer med ondt i karrieren. Derimod var ledingsføringen i reflektoren og hjulene ukendte.

Der er økonomiske faktorer i valget af kryptosystem. Enigma var en relativt billig og robust maskine. Når nogen skal beslutte at afsætte resourcer til brydningen af en kode, skal de afveje prisen på brydningen med værdien af informationerne. Rejewskis arbejde viste englænderne, at det rimeligvis kunne betale sig at ansætte matematikere for at arbejde med at bryde Aksemagternes koder. Churchill handlede effektivt ud fra den præmis.

3.1 Protokolfejlen

Hver måned havde sin rækkefølge af hjulene, og hver dag sin indstilling af "das Steckerbrett", stiktavlen, og startstilling af hjulene. Man anså det for usikkert at sende en hel dags beskeder med samme nøgle; det ville være nemt og billigt at bryde koden med frekvensanalyse af hvert bogstav for sig. Derfor skulle operatøren vælge sin egen startindstilling af hjulene; han skulle vælge en sekvens på tre bogstaver, som viste hjulenes startindstilling i beskeden. Dette ord på tre bogstaver kaldes beskednøglen. Operatøren sender først disse tre bostaver med dagens kode. Så indstiller han til beskednøglen og sender meddelelsen. Dette er sikkert nok, hvis de tre bogstaver er tilfældigt valgt, men de meninge forstod ikke vigtigheden deraf. Desuden er det næsten umuligt for et menneske at vælge et tilfældigt "ord" på tre bogstaver. Efter Rejewski havde fundet ledningsføringen i reflektoren og hjulene var denne protokolfejl en stor hjælp i arbejdet med at finde dagens nøgle.

Gentagelser er gift for sikkerheden. Hvis man bruger den samme nøgle alt for længe, får en der lytter med, alt for mange ensartede data at arbejde med. Hvis man møder på arbejde hver morgen klokken 9:00, ved folk hvor man er lidt i ni. Den tyske hær havde indbygget en gentagelse i protokollen for brugen af Enigma.

Det var besluttet at beskednøglen skulle sendes to gange, ikke bare én. I dag er det svært at forstå at man indlagde en gentagelse i starten af hver besked, og det var også dette, der gjorde det muligt for Rejewski at få hul på afkodningen og beregne ledningsføringen i hjulene.

Antag at en operatør sender nøglen til en besked to gange kodet som "BRGRTH". De ukendte beskednøgle betegnes "xyz". Kodningen af de første seks bogstaver betegnes henholdsvis A, B, C, D, E og F. Heraf fås oplysningen at

$$A(x) = B, B(y) = R, C(z) = G, D(x) = R, E(y) = T \text{ og } F(z) = H \ .$$

Kodningen og afkodningen af bogstaverne er samme afbildning. Altså gælder

$$x = A(B), y = B(R), z = C(G), x = D(R), y = E(T) \text{ og } z = F(H) \ .$$

Heraf fås $A(B) = D(R)$, at $B(R) = E(T)$ og $C(G) = F(H)$. Udfør A på begge sider af den første formel. Det giver $AA(B) = AD(R)$, som giver $AD(R) = B$. De andre giver tilsvarende $BE(T) = R$ og $CF(H) = G$. I løbet af en dag fik man på denne måde en fuld tabel over afbildningerne AD, BE og CF. De næste to afsnit handler om, hvordan Rejewski kunne afkode denne information.

3.2 Om at finde A opg D ud fra AD

Kodningen af hvert bogstav består i en parvis ombytning. Det viser sig, at når to sådanne afbildninger samensættes, får resultatet en bestemt struktur[3]. Først skal strukturen opdages, så bevises, og endelig anvendes. Her springes beviset dog over. Strukturen kan bedst opdages ved at gennemregne en række eksempler.

Det er tilstrækkeligt at arbejde med et alfabet med 10 bogstaver. Antag at A og D er givet ved

$$A = (AD)(BC)(EH)(FI)(GJ) \ , \quad D = (AI)(BF)(CJ)(DE)(GH) \ .$$

[3]Det er formentlig denne struktur, Christensen henviser til i titlen på [1]

Notationen skal læses således, at A bytter om på "A" og "D", og på "B" og "C" og så videre. Man kan udfærdige et sildeben for A,

x	A	B	C	D	E	F	G	H	I	J
A(x)	D	C	B	A	H	I	J	E	F	G

men erfarne regnere finder den første notation letter at anvende.

Den sammensatte afbildning AD skal beregnes. Først skal billedet af bogstavet "A", altså $AD(A)$ findes. Afbildningen D fører det over i $D(A) = I$, og A fører I over i $A(I) = F$. Altså er

$$AD(A) = A(D(A)) = A(I) = F.$$

Man skriver nu $AD = (AF$. Hvorfor fremgår senere.

Dernæst findes billedet af F. Det viser sig, at $AD(F) = C$. Så tilføjes C, så man har $AD = (AFC$. Fortsættes fås $AD = (AFCGE$. Det viser sig, at E afbildes over i A. Derfor afsluttes den første blok med en højreparentes: $AD = (AFCGE)$. Ved gentagne afbildninger cykler billederne rundt i denne rækkefølge. Den kaldes derfor en cyklus (eng. cycle). Den næste cyklus starter man normalt med det første ledinge bogstav, her B. Men ender med

$$AD = (AFCGE)(BIDHJ) \ .$$

Opgave 13 *Regn i et alfabet med* 10 *bogstaver. Digt fem mulige kodninger som A og D ovenfor. Beregn* 9 *forskellige sammensætninger af dem.*

Opgave 14 *Betragt resultaterne af forrige opgave. Hvilke egenskaber har de allesammen? Er for eksempel* $(AB)(CDE)(FGHIJ)$ *et muligt resultat? Er identiteten*

$$Identiteten = (A)(B)(C)(D)(E)(F)(G)(H)(I)(J)$$

et muligt resultat? Eller $(A)(BCD)(EFG)(HIJ)$*?*

Nu skal de mulige afbildninger A og D, der giver $AD = (AFCGE)(BIDHJ)$ findes.

Opgave 15 *Efter det du har opdaget, hvor mange løsninger A og D findes der? Kan du opskrive nogle flere end det givne par?*

Både A og D består af par sammensat af et bogstav fra hver cyklus. Vælg makkeren til "A", for eksempel "D". Så fås resten af parrene ved at følge cyklerne rund i modsat retning. Med dette valg ender man med afbildningen A. Derefter er der kun én mulighed for $D = A(AD)$. Den kan lettest opskrives ved at finde billedet af "A". Man får $D(A) = A(AD)(A) = A(F) = I$. Men man får resten ved at gå modsat rundt i de to cykler i AD og ender selvfølgelig med den kendte D.

Andre muligheder er

$$A = (AB)(FJ)(CH)(GD)(EI) = (AB)(CH)(DG)(EI)(FJ) \ ,$$

og

$$D = (AI)(FB)(CJ)(GH)(ED) = (AI)(BF)(CJ)(DE)(GH) \ .$$

Det viser sig at der kun findes fem mulige løsninger i dette tilfælde.

Mener du, at du har for stået princippet, kan du springe til den følgende Opgave. Antag at $AD = (A)(B)(CD)(EF)(GH)(IJ)$. Det er klart, at "$A$" må være parret med "$B$" i både A og D. Men C kan være parret med ethvert af bogstaverne EFGHIJ; her er der seks valgmuligheder. Derefter er der to par tilbage. De kan passer på to måder. I dette eksempel ender man med på tolv mulige kodninger A og D.

Opgave 16 *Tag nogle af resultaterne fra opgave 13, og opskriv de mulige kodninger A og D.*

3.3 Afkodning af nøglerne

Lad os antage, at polakkerne ved simpel spionage har fået kendskab til 20 operatører, som har pralet af at bruge nemme nøgler såsom "ABC" og "AAA", altså med bogstaver i rækkefølge eller ens bogstaver. Oplysningerne fremkommer typisk ved at lytte til menige i knejperne lørdag aften og tale med prostituerede om søndagen. Når hjulene lige er sat i, står de på "AAA". Det er derfor dovent at lade dem stå eller kun dreje lidt til "B" eller "F".

Beskederne en bestemt dag fra disse operatører starter flere gange med "EAEEEF", "EBFEFD" OG "BCDDAE". Ved at tage flere starter med, så alle bogstaver kombineres, får vi

EAEEEF, EBFEFD, BCDDAE, FFACDB, AEEACF, CDBFBC, BDADBB, DECBCA.

Ved at bruge metoden fra afsnit 3.2, når man frem til to muligheder for A, og tre for hver af B og C, nemlig

$$A_1 = (AE)(BC)(DF) \qquad A_2 = (AE)(BF)(CD) \quad (5)$$

$$B_1 = (AB)(CF)(DE) \quad B_2 = (AD)(BC)(EF) \quad B_3 = (AF)(BE)(CD) \quad (6)$$

$$C_1 = (AD)(BF)(CE) \quad C_2 = (AE)(BD)(CF) \quad C_3 = (AF)(BE)(CD) \quad (7)$$

Det giver $2 \cdot 3 \cdot 3 = 18$ mulige kombinationer. Familien af nøgler skal nu udregnes for hvert af disse kombinationer.

Man kan få adskillige timer til at gå med den beregning, hvis man ikke griber den rationelt an. Først bemærkes at man kun behøver at oversætte de første tre bogstaver. De sidste giver nødvendigvis samme resultat; sådan er afbildningerne A, B og C jo bestemt. Det halverer arbejdet!

Dernæst skal de mulige kombinationer listes på en systematisk måde. Endelig skal man udfylde en søjle ad gangen.

$A_iB_jC_k$	EAE	EBF	BCD	FFA	AEE	CDB	BDA	DEC
111	ABC	AAB	CFA	DCD	BEF	EDC	CED	FDE
112	ABA	AAC	CFB	DCE	BED	EDA	CEE	FDF
113	ABB	AAA	CFC	DCF	BEE	EDB	CEF	FDD
121	ADC	ACB	CBA	DED	BAF	EFC	CAD	FFE
122	ADA	ACC	CBB	EED	BAD	EFA	CAE	FFF
123	ADB	ACA	CBC	DEF	BAE	EFB	CAF	FFD
131	AFC	AEB	CDA	DAD	BCF	EBC	CCD	FBE
132	AFA	AEC	CDB	DAE	BCD	EBA	CCE	FBF
133	AFB	AEA	CDC	DAF	BCE	EBB	CCF	FBD
211	ABC	AAB	FFA	BCD	DEF	EDC	FED	CDE
212	ABA	AAC	FFB	BCE	DED	EDA	FEE	CDF
213	ABB	AAA	FFC	BCF	DEE	EDB	FEF	CDD
221	ADC	ACB	FBA	BED	DAF	EFC	FAD	CFE
222	ADA	ACC	FBB	BEE	DAD	EFA	FAE	CFF
223	ADB	ACA	FBC	BEF	DAE	EFB	FAF	CFD
231	AFC	AEB	FDA	BAD	DCF	EBC	FCD	CBE
232	AFA	AEC	FDB	BAE	DCD	EBA	FCE	CBF
233	AFB	AEA	FDC	BAF	DCE	EBB	FCF	CBD

Først oversættelsen af E i "EAE" Det skal enten oversættes med A_1 eller A_2, men det giver i begge tilfælde $A_1(E) = A_2(E) = A$. Derfor udfyldes den første søjle med "A".

Den anden søjle skal udfyldes med

$$(B_1(A), B_2(A), B_3(A)) = (B, D, F) \ .$$

Hvert bogstav forekommer tre gange. Så gentages mønstret.

Den tredje søjle skal udfyldes med

$$(C_1(E), C_2(E), C_3(E)) = (C, A, B) \ .$$

Mønstret gentages hele vejen ned.

Bruges disse principper tager det 10-15 minutter at udfylde skemaet.

Opgave 17 *Der er en fejl i tabellen. Den kan findes blot ved at checke mønstret.*

Rækken "211" springer i øjnene med valg af ens bogstaver og bogstaver i rækkefølge. Vi har fundet koderne af de første seks bogstaver!

Opgave 18 *Næste dag opsnappes beskeder med følgende indledninger fra de samme operatører:*

FCFEFD, FFEEEF, DFFBED, ACDDFE, EABCDA, CDAFBC, BEEACF, FBCEAB.

Beregn afkodningen af de første seks bogstaver. (Afsæt mindst en time til det. De første fire skal bruges i næste afsnit.)

3.4 Beregning af ledningsføringen i rotoren

I slutningen af 1931 erklærede "Le Deuxième Bureau français", som var det kontor i den franske kodetjeneste der beskæftigede sig med Tyskland, Enigma for uløselig. I december 1932 havde Rejewski seks ligninger til at bestemme ledningsføringen i hjulet og reflektoren. Med eksemplet fra forrige sektion lyder de første fire

$$A = s^1N^{-1}s^{-1}Rs^1Ns^{-1} = (AE)(BF)(CD) \tag{8}$$
$$B = s^2N^{-1}s^{-2}Rs^2Ns^{-2} = (AB)(CF)(DE) \tag{9}$$
$$C = s^3N^{-1}s^{-3}Rs^3Ns^{-3} = (AD)(EF)(DF) \tag{10}$$
$$D = s^4N^{-1}s^{-4}Rs^4Ns^{-4} = (AE)(BC)(DF) \tag{11}$$

Det er fire ligninger med kun to ubekendte afbildninger. De kan ikke løses i den forstand, at man kan udtrykke R og N ud fra A, B, C og D. Men det er muligt at analysere sig frem til løsningen.

I et alfabet med kun seks bogstaver er der kun 720 muligheder for N. Man kan isolere R i ligningern ovenfor, for eksempel $R = sNs^{-1}AsN^{-1}s^{-1}$. Man kan så prøve alle mulighederne for N og se, for hvilke man får samme afbildning R. (Man får faktisk seks løsninger, men forskellen er blot at man har placeret bogstavet "A" forskellige stede på forbindelsen mellem rotoren og reflektoren. Denne beregning kan relativt nemt udføres i Maple.

Opgave 19 *Sammen med dette dokument findes et Maple dokument, der simulerer denne forsimplede Enigma. Den har også et afsnit der finder ledningsføringen ved metoden beskrevet ovenfor. Brug den til at regne tilbage fra dine afbildninger $A \ldots D$ fra opgave 18 til ledningsføringerne.*

Opgave 20 *Brug lednigsføringerne fra sidste opgave til at afkode meddelelsen*

"ADBEEBECBACBADDECCFEAFEEFECF".

Den er sendt uden nogen beskednøgle. Indsæt passende mellemrum, og beskeden giver en vis mening.

I (8) udføres s^{-1} fra venstre, og s fra højre. Det giver

$$s^{-1}As = N^{-1}s^{-1}RsN \ .$$

Denne afbildning kaldes U og kan udregnes trin for trin; Billedet af "A" udregnes

$$A \overset{s}{\mapsto} B \overset{A}{\mapsto} F \overset{s^{-1}}{\longmapsto} E \ .$$

Man får

$$U = s^{-1}As = N^{-1}s^{-1}RsN = (AE)(BC)(DF) \tag{12}$$

Tilsvarende defineres

$$V = s^{-2}Bs^2 = N^{-1}s^{-2}Rs^2N = (AD)(BC)(EF) \tag{13}$$
$$W = s^{-3}Bs^3 = N^{-1}s^{-3}Rs^3N = (AD)(BF)(CE) \tag{14}$$
$$X = s^{-4}Bs^4 = N^{-1}s^{-4}Rs^4N = (AC)(BF)(DE) \tag{15}$$

Opgave 21 *Gennemfør denne beregning med afbildningerne fra opgave 18*

Dernæst udregnes

$$UV = N^{-1}s^{-1}Rs^{-1}Rs^2N = (AF)(B)(C)(DE) \tag{16}$$
$$VW = N^{-1}s^{-2}Rs^{-1}Rs^3N = (A)(BE)(CF)(D) \tag{17}$$
$$WX = N^{-1}s^{-3}Rs^{-1}Rs^4N = (AE)(B)(CD)(F) \tag{18}$$

Opgave 22 *Regn efter at produkterne kan reduceres til det angivne udtryk, og regn efter, at afbildningerne faktisk er som givet.*

Opgave 23 *Gennemfør denne beregning med afbildningerne fra opgave 18*

Bemærkede du, at de tre afbildninger UV, VW og WX har samme cykelstruktur? I arbejdet med matematiske problemer, skal man hele tiden være opmærksom på gentagne mønstre. Og her er der ét!

Opgave 24 *Lad afbildningen Z være $Z = (ADJC)(B)(EIG)(FH)$. Beregn sZs^{-1}, og beregn s^2Zs^{-2}.*

Opdagede du systemet? Afbildningerne har samme cykelstruktur, og cyklerne kan direkte skrives op! For eksempel er

$$sZs^{-1} = (s(A)s(D)s(J)s(C))(s(B))(S(E)s(I)s(G))(s(F)s(H))$$
$$= (BEAD)(C)(FJH)(GI) = (ADBE)(C)FJH)(GI) \ .$$

Denne sammenhæng er ganske vigtig, og det er værd at huske den. Man kan skrive princippet på denne måde: Hvis en afbildning, F, har cykelstrukturen

$$F = \ldots(\ldots xy\ldots)\ldots \ ,$$

så har afbildningen TFT^{-1} samme cykelstruktur, nemlig

$$TFT^{-1} = \ldots(\ldots T(x)T(y)\ldots)\ldots \ .$$

Vi skal nu se, at vi faktisk kan udtrykke VW ud fra UV på denne måde. I ligningen (16) udføres N fra venstre og N^{-1} fra højre. Det giver

$$NUVN^{-1} = s^{-1}Rs^{-1}Rs^2 \ .$$

Nu udføres s^{-1} fra venstre, og s fra højre.

$$s^{-1}NUVN^{-1}s = s^{-2}Rs^{-1}Rs^3 \ .$$

Vi har nu opnået, at højresiden passer nøjagtigt med indmaden i udtrykket for VW. Erstat det,

$$VW = N^{-1}s^{-2}Rs^{-1}Rs^3N = N^{-1}s^{-1}NUVN^{-1}sN \ .$$

Indfør afbildningen

$$T = N^{-1}s^{-1}N \tag{19}$$

Vi er nået frem til at

$$VW = T(UV)T^{-1} \tag{20}$$

Opgave 25 *Udled på samme måde at*

$$WX = T(VW)T^{-1} \tag{21}$$

Opgave 26 *Måske er det ikke helt klart, at* $T^{-1} = N^{-1}sN$. *Opskriften er at regne nogle eksempler. Vælg en ledningsføring* N *og udregn* $T(A)$. *Gå så baglæns gennem udregningen.*

Opgave 27 *Isoler* s^{-1} *i formel (19)*

$$s^{-1} = NTN^{-1} \ .$$

Cyklerne i s^{-1} *fremkommer ved at operere med* N *på cycklerne i* T. *(Det er samme princip som i opgave 24.) Hvad kan man sige om cykelstrukturen af* T*?*

Vi ved nu at UV, VW og WX skal have samme cykelstruktur, og cyklerne fremkommer af hinanden ved afbildningen T. På den baggrund kan T findes!

Start med "A". Det optræder som et en 1-cykel (A) i VW, der afbildes enten på "B" eller "F", fordi de er de eneste 1-cykler i WX. Tag muligheden "B" først, $T = (AB\ldots)$. Betragt afbildningen af cyklerne i UV. det fremgår, at "B" skal afbildes på enten "A" eller "D". Men "A" er jo umulig, for så ville cyklen være slut, og T har kun én cyklus i følge opgave 27.

Vi har nu $T = (ABD\ldots)$. Man fortsætter på samme måde og ender med

$$T = (ABDFEC) \tag{22}$$

Der er også den anden mulighed, $A \mapsto TF$. Afbildningen UV har cyklen (AF), som må føres over i cyckeln (CF) i afbildningen VW. Derfor afbildes $F \mapsto TC$. Men C er en 1-cyklus, som enten afbildes i A eller D. Imidlertid er A udelukket, fordi det ville afslutte cyklen. Atls har vi $T = (AFCDB\ldots)$. Nu kom jeg til at køre lidt længere. Men det er langt nemmere at tænke selv, end at følge en andens forklaringer. Men nu går det i stå for B kan kun føres over i A, og det afslutter cyklen ét bogstav for tidligt. Vi må forkaste muligheden $A \mapsto F$.

Opgave 28 *Bestem* T *ud fra dine afbildninger fra opgave 23*

De sidste to trin er nemme. Det første trin er at opskrive N. Vi kender $s^{-1} = (AFEDCB)$ og $T = (ABDFEC)$. Det giver faktisk seks muligheder for N, men de svarer blot til at den ene side af hjulet drejes i forhold til den anden, og at kontakterne på reflektoren flyttes tilsvarende. Der vil være tale om samme maskine med samme kodning. Det er nemmest at skrive cyklerne op

	$T = ($	A	B	D	F	E	C	$)$
under hinanden	N:	↓	↓	↓	↓	↓	↓	
	$s^{-1} = ($	A	F	E	D	C	B	$)$

Endelig kan ledningsføringen i reflektoren findes ved at isolere R i formlen for A og udregne afbildningen

$$R = sNs^{-1}AsN^{-1}s^{-1} = (AC)(BD)(EF) \tag{23}$$

Det nemmeste er nok at opskrive $N = (A)(BFDEC)$ og transformere den til $sNs^{-1} = (B)(CAEFD)$. Endelig transformeres A til udtrykket ovenfor. Men man kan også gennemregne udtrykket ovenfor for bogstaverne "A", "B" og "E".

Opgave 29 *Beregn ledningsføringen i rotoren og reflektoren ud fra* A *og* T *fra opgave 13 og 27.*

References

[1] Chris Christensen. Polish mathematicians finding patterns in enigma messages. *Mathematics Magazine*, 80:247–273, 2007.

[2] Kris Gaj and Arkadiusz Orlowski. Facts and myths of enigma: breaking stereotypes.

[3] Marian Rejewski. Mathematical solution of the enigma cipher. *Cryptologia*, 6, 1982.