Indledning

I krig er det afgørende, at man kan kommunikere med sine egne styrker, uden at fjenden kan følge med. *Kryptering* er derfor en vigtig disciplin.

Før og under Den Anden Verdenskrig brugte tyskerne en særlig krypteringsmaskine ved navn *Enigma*. Man troede, at det var umuligt at knække koderne fra Enigma, men faktisk lykkedes det allerede før krigen polske matematikere at afkode maskinen. Hen imod slutningen af krigen blev også englænderne i stand til at læse tyskernes hemmelige meddelelser - ikke mindst til de berygtede ubåde i Nordatlanten.

Der er skrevet meget god litteratur om emnet herunder de matematiske aspekter. Jeg vil her fremhæve *Erik Vestergaards* matematiksider om emnet.

Når jeg alligevel skriver om Enigma, er det for at samle de vigtigste matematiske aspekter på en kortfattet måde.

Kapitlet indeholder følgende afsnit:

Indhold

1. Maskinens virkemåde
2. Kombinationer
3. Den polske metode I
4. Permutationer
5. Den polske metode II

Titelbladet

Titelbladet viser en velbevaret Enigma-maskine.

1: Maskinens virkemåde

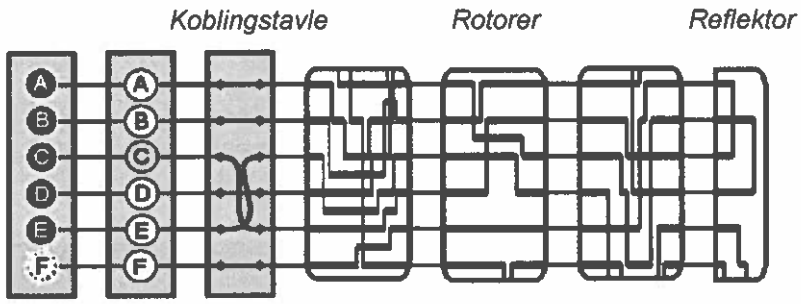
Virkemåde

Jeg vil her forsimplet forklare, hvordan Enigma-maskinen virker. Hvis du vil have flere detaljer, så kig i litteraturlisten.

Komponenter

Apparatet består af følgende komponenter - se også fotoet på næste side:

- Tastatur.
- Lyspanel.
- Koblingstavle (på engelsk *plug-board*, på tysk *steckerbrett*).
- Rotorer (på engelsk *scramlers*, på tysk *Walzen*).
- Reflektor (på tysk *Umkehrwalze*).



Figur: Enigma-maskinens komponenter. (Inspireret af Kodebogen.)

Alle komponenter er forbundet elektrisk via ledninger, men forbindelserne varierer, som du skal se.

Kodning

Kodning foregår således:

- Man trykker på én af de 26 taster med alfabetet. Det sender en elektrisk strøm gennem maskinen.
- Strømmen passerer koblingstavlen, som har 26 bogstav-indgange og 26 bogstav-udgange. Alle indgange er som udgangspunkt forbundet til de tilsvarende udgange, men ved hjælp af særlige ledninger kan man bytte rundt. Disse ledninger har to ledere og et dobbeltstik i hver ende. Hvis f.eks. C og E er forbundet, går den ene leder fra indgang C til udgang E, mens den anden går fra udgang C til indgang E.
- Strømmen når nu den første rotor, som er et hjul med 26 indgange forbundet til koblingstavlen og 26 udgange. Det afhænger helt af den aktuelle rotor, hvordan indgange og udgange er forbundet. Lige før strømmen passerer gennem hele maskinen, drejer den første rotor ét trin i forhold til koblingstavlen, således at indgangene bliver rykket én plads.
- Strømmen når derpå den anden rotor, som er opbygget som den første. Den anden rotor drejer også, men først når den første rotor har drejet en hel omgang, dvs. efter 26 indtastninger.
- Den tredje rotor fungerer tilsvarende. Den drejer først, når den anden rotor har drejet en hel omgang, dvs. med 26 gange 26 indtastninger.
- Strømmen rammer nu reflektoren, der har 26 indgange, som også fungerer som udgange. Strømmen går ind gennem et stikhul og ud gennem et andet svarende til, at bogstaver parvist bliver byttet rundt. Derfra går strømmen retur gennem maskinen, men i modsat rækkefølge, dvs. gennem rotor tre, to og en samt omvendt gennem koblingstavlen, hvor den endelig får en pære på lyspanelet til at lyse op ved et bestemt bogstav.

Tegningen

Tegningen ovenover er lavet, som du kan følge kodningen fra venstre mod højre gennem maskinen og tilbage igen. Men set forfra går strømmen faktisk modsat i en rigtig Enigma-maskine, idet reflektoren sidder til venstre. Man kan sige, at tegningen ovenover viser maskinen bagfra.

Afkodning

Afkodning foregår således:

- Man taster bogstaverne fra koden ind i maskinen på samme måde, som når man skal kode. Strømmen går gennem komponenterne på helt samme måde, som ved kodning.
- Pga. af symmetrien i maskinen kommer de afkodede bogstaver nu ud på lyspanelet. Strømmen har passeret nøjagtig det samme kredsløb blot i omvendt retning.

NB:

Fordi strømmen passerer det samme kredsløb både ved kodning og afkodning, kan intet bogstav blive kodet til sig selv.

Begyndelsesbetingelser

Hvordan en konkret meddelelse bliver kodet, afhænger naturligvis af, hvordan Enigma-maskinen er indstillet til at begynde med. Mere om det senere!

Opgaver	
1	Gå på internettet og find billeder af de enkelte komponenter i Enigma-maskinen!
2	Prøv en online Enigma-simulator på internettet, f.eks. *http://enigma.louisedade.co.uk/enigma.html*

Foto: En Enigma-maskine.

2: Kombinationer

Antallet af mulige indstillinger

En kodemaskines succes afhænger af antallet af måder, som man kan indstille den på. Hvis antallet af kombinationer er lavt, kan fjenden gennemgå dem fra en ende af og tjekke, hvilken der giver mening til en given kodet besked. Enigma-maskinen er konstrueret, så antallet af kombinationer er stort - men hvor stort? Det vil jeg regne på nu:

Komponent	***Antal muligheder***
Rotor-rækkefølge	Der er tre pladser til de tre rotorer, og man kan selv bestemme, hvilken rotor, som sidder hvor. Antallet af muligheder er derfor $3 \cdot 2 \cdot 1 = 6$
Rotor-positioner	Hver af de tre rotorer har 26 mulige startpositioner. Det samlede antal kombinationer er derfor $26 \cdot 26 \cdot 26 = 17576$
Koblingstavle	Med f.eks. 6 ledninger skal man vælge at forbinde 6 bogstaver i den ene ende med 6 andre bogstaver i den anden. Man kan altså først vælge 12 bogstaver ud af 26. Denne udvælgelse er i første omgang *uordnet*, så antallet er muligheder er K(26;12). Hver af disse muligheder består af 12 forskellige bogstaver med huller, som man skal forbinde parvist med ledninger. Når man skal forbinde den første ledning, så er der 12 mulige huller for den ene ende og 11 mulige huller for den anden. Altså 12·11 muligheder. Kigger jeg imidlertid på en bestemt kombination, vil den gå igen 12 gange i det samlede regnskab, for den vil optræde med hver af de 6 ledninger samt ved at bytte rundt på de 6 ledningsender. F.eks. kan man opnå ombytningen AB med 6 forskellige ledninger samt via den omvendte kobling BA med 6 forskellige ledninger. Det giver 12 gengangere. Jeg skal derfor dividere antallet 12·11 med 12. Tilbage bliver der 11 muligheder i det samlede regnskab. For næste ledning er der som udgangspunkt 10 mulige huller for den ene ende af ledningen og 9 for den anden, altså 10·9, men tilsvarende skal med dividere med 10, så antallet af muligheder bliver 9. Det samlede antal muligheder med 6 ledninger i koblingstavlen bliver derfor: $K(26;12) \cdot 11 \cdot 9 \cdot 7 \cdot 5 \cdot 3 \cdot 1$ $= 100391791500$
I alt	$6 \cdot 17576 \cdot 100391791500 \approx 10^{16}$

Med dette astronomiske antal kombinationer troede tyskerne sig sikre på deres maskine, men der var nogle svagheder, som jeg skal vise dig i næste afsnit.

NB:

Bemærk, at jeg har brugt begrebet *kombinationer* i to betydninger ovenover: Dels bredt som antallet af indstillingsmuligheder og dels specifikt matematisk ved udtrykket K(26,12).

Koblingstavlen

De store antal muligheder kommer fra koblingstavlen, som jeg her vil se lidt nærmere på. Formlen for 6 ledninger er:

$$K(26;12)\cdot 11\cdot 9\cdot 7\cdot 5\cdot 3\cdot 1$$

Jeg omskriver udtrykket:

$$K(26;12)\cdot 11\cdot 9\cdot 7\cdot 5\cdot 3\cdot 1 = K(26;12)\cdot\frac{12\cdot 11\cdot 10\cdot 9\cdots 2\cdot 1}{12\cdot 10\cdot 8\cdots 2}$$

$$= K(26;12)\cdot\frac{12!}{(2\cdot 6)\cdot(2\cdot 5)\cdot(2\cdot 4)\cdots(2\cdot 1)} = K(26;12)\cdot\frac{12!}{6!\cdot 2^6}$$

$$= \frac{26!}{(26-12)!\cdot 12!}\cdot\frac{12!}{6!\cdot 2^6} = \frac{26!}{(26-12)!\cdot 6!\cdot 2^6}$$

Formel

Generelt er antallet af muligheder for en koblingstavle med n ledning givet ved formlen:

$$f(n) = \frac{26!}{(26-2n)!\cdot n!\cdot 2^n}$$

Optimalt antal muligheder

Da man maksimalt kan forbinde den ene halvdel af bogstaver med den anden halvdel, er det største antal ledninger 13. Spørgsmålet er så, hvilket antal ledninger, der giver det størst mulige antal kombinationer. Med andre ord: For hvilken værdi af n topper antallet af muligheder givet ved formlen ovenover?

For at afgøre dette er det nemmest at lave en tabel over antallet af muligheder f(n) som funktion af n. Det synes jeg, du skal prøve!

n	f(n)
1	
2	
3	
...	
13	

Jeg vil derimod vise to alternative metoder til at løse problemet.

Grafisk løsning

Først vil jeg lave en pæn grafisk løsning. Her benytter jeg mig af et lille trick til at udregne fakultetsfunktionen:

Matematik

Gamma-funktionen

Gamma-funktionen er defineret ved integralet

$$\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}\,dt$$

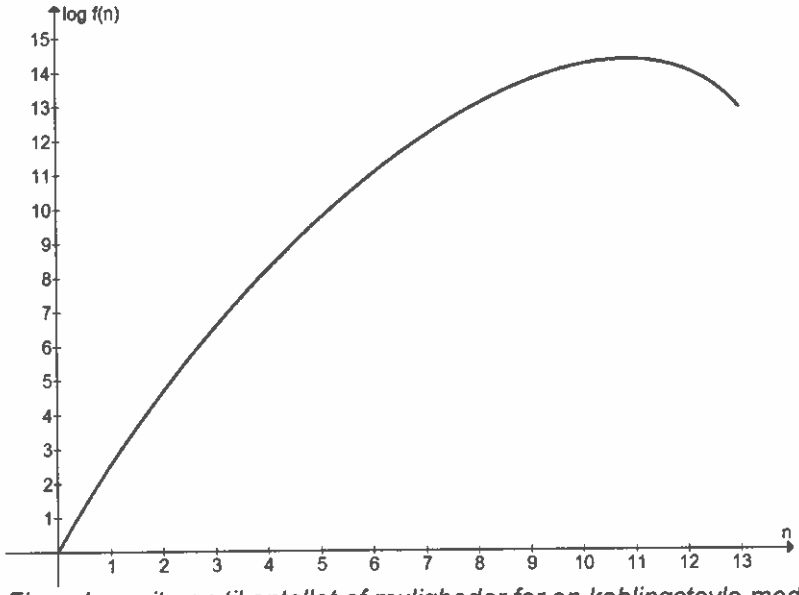
Der gælder følgende formel:

$$n! = \Gamma(n+1)$$

Bemærk, at denne formel gør det muligt at udvide fakultetsfunktionen til også at virke på ikke-heltallige tal.

Jeg bruger nu et matematikprogram til at tegne grafen for funktionen f(n). Jeg bruger gamma-funktionen til at beregne fakulteter og får derfor en kontinuert funktion. Da funktionsværdierne bliver så enormt store, tager jeg logaritmen. Alt i alt kigger jeg på følgende funktion:

$$g(x) = \log f(x) = \log\frac{\Gamma(26+1)}{\Gamma(26-2x+1)\cdot\Gamma(x+1)\cdot 2^x}$$



Figur: Logaritmen til antallet af muligheder for en koblingstavle med n ledninger.

Beregningsløsning

Den anden metode har jeg fra bogen *Enigma - et dilemma*. Ideen er at kigge på uligheden

$$f(n) \le f(n+1)$$

Hvis uligheden er opfyldt, så får man flere kombinationer ved at tilføje en ledning på koblingstavlen.

Udskrevet hedder uligheden:

$$f(n) = \frac{26!}{(26-2n)!\cdot n!\cdot 2^n} \le \frac{26!}{(26-2(n+1))!\cdot (n+1)!\cdot 2^{n+1}} \quad \text{dvs.}$$

$$\frac{26!}{(26-2n)!\cdot n!\cdot 2^n} \le \frac{26!}{(26-2n-2)!\cdot (n+1)n!\cdot 2^n 2} \quad \text{dvs.}$$

$$2(n+1) \le \frac{(26-2n)!}{(26-2n-2)!} \quad \text{dvs.}$$

$$2(n+1) \le (26-2n)(26-2n-1) \quad \text{dvs.}$$

$$2n+2 \le 26^2 - 52n - 26 - 52n + 4n^2 + 2n \quad \text{dvs.}$$

$$4n^2 - 104n + 648 \ge 0 \quad \text{dvs.}$$

$$n^2 - 26n + 162 \ge 0$$

Denne andengradsulighed har løsningen n≤10,35 eller n≥15,65, hvor kun det første tal er relevant for Enigma-maskinen.

Konklusion

Det optimale antal ledninger er altså 11.

Opgaver	
1	På hvor mange måder kan man indstille en Enigma-maskine med 8 ledninger på koblingstavlen?
2	Nyere Enigma-maskiner havde 5 rotorer. På hvor mange måder kan man indstille sådan en maskine med 11 ledninger på koblingstavlen?
3	Argumentér direkte for formlen $f(n) = \frac{26!}{(26-2n)!\cdot n!\cdot 2^n}$
4	Vis, at gamma-funktionen opfylder ligningen $\Gamma(n+1) = n\Gamma(n)$ Vis derpå formlen $n! = \Gamma(n+1)$

3: Den polske metode I

Den polske metode

Hvordan en konkret meddelelse bliver kodet, afhænger som nævnt af indstillingen af Enigma-maskinen, dvs.

- placeringen af ledninger på koblingstavlen,
- rækkefølgen af rotorer samt
- rotor-orienteringen, dvs. valget af startbogstav på hver rotor.

Ændring af rotor-orientering via meddelelsesnøgle

Tyskerne lavede hver måned kodebøger med *dagsnøglen*, dvs. den daglige indstilling. Men som en ekstra sikkerhed brugte de for hver meddelelse dagsnøglen til at transmittere en ændring af rotor-orienteringen. De tre bogstaver blev sendt to gange i træk for at være sikker. F.eks.

Klartekst: BMWBMW
Kodet tekst: AKTOLV

Netop denne gentagelse skulle vise sig at blive fatal, idet den var forudsætningen for, at polakkerne kunne knække koden.

Antag, at fjenden opsnapper et antal meddelelser i løbet af en bestemt dag. Han kigger på de 6 første bogstaver - der, hvor ændringen af rotor-orienteringen bliver angivet. Det kunne se sådan ud:

	Bogstav					
Meddelelse	*1*	*2*	*3*	*4*	*5*	*6*
1	K	A	B	T	W	C
2	T	C	V	H	G	X
3	F	P	D	S	E	M
4	X	B	L	F	Q	Y

Bogstaver 1 og 4 er forskellige kodninger af samme bogstav. Tilsvarende for bogstav 2 og 5 samt 3 og 6.

Jeg prøver at kortlægge disse kodninger:

1. bogstav	ABCDEFGHIJKLMNOPQRSTUVWXYZ
4. bogstav	S T H F

Med tilstrækkeligt mange beskeder kan man udfylde hele skemaet. Det kunne f.eks. se sådan ud:

1. bogstav	ABCDEFGHIJKLMNOPQRSTUVWXYZ
4. bogstav	GNQCJSBLWATRPIMDVUYHKXEFZO

Kæder

I skemaet fremgår det, at A kobler til G, og G kobler til B, osv. Det svarer til følgende kæder:

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

Pointen ved disse kæder er, at deres længde kun afhænger af rotorernes placering - ikke af koblingstavlen. Hvorfor? Jo, hvis man f.eks. i stedet for at bytte rundt på A og B på koblingstavlen bruger ledning til at bytte rundt på C og D, så ser kæderne sådan ud:

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

Enkelte af bogstaverne har skiftet plads, men kædernes længde er den samme.

Polakkerne indså, at rotor-orienteringen var afspejlet direkte i kædernes længde. Da de havde adgang til kopier af Enigma-maskiner, gik de derfor i gang med at lave et katalog over sammenhængen mellem rotor-orientering og mønstre af kæde-længder.

Der er
$6 \cdot 17576 = 105456$
kombinationer, og arbejdet med at kortlægge de tilhørende kædelængder tog et år.

Indstillingen af rotorerne var nu til at gennemskue, men uden kendskab til koblingstavlen var det stadig svært at læse beskederne. Imidlertid dukkede der ofte små brudstykker op i koderne, som afslørede koblingstavlen, f.eks. ordet

BAFBHRTNBCHAERLIN

som minder om sætningen

ABFAHRT-NACH-BERLIN

hvis man altså bytter rundt på A og B. Med andre ord en indikation af en given ledning på koblingstavlen.

Man kunne også lave frekvensanalyse af bogstavernes hyppigheder for at aflure koblingstavlen.

Opgaver

1 Find kæder ud fra følgende tabel:

1. bogstav	ABCDEFGHIJKLMNOPQRSTUVWXYZ
4. bogstav	MNBVCXZASDFGHJKLPOIUYTREWQ

Foto: Den polske matematiker Marian Rejewski, der knækkede Enigma-koden.

4: Permutationer

I de næste afsnit bruger jeg matematik til at analysere Enigma-maskinen.

Som beskrevet koder maskinen en tekst ved at bytte rundt på bogstaver. Denne ombytning sker ikke bare ét sted, men i en række komponenter:

- Koblingstavlen.
- Rotorerne.
- Reflektoren.

Disse komponenter udgør tilsammen en kompleks maskine med så mange kombinationer af indstillinger, at den tilsyneladende er umulig at afkode.

Men ved at beskrive Enigma-maskinen med matematiske begreber er det alligevel muligt at finde smuthuller i systemet. Det centrale begreb er her de såkaldte *permutationer*.

Permutationer

En *permutation* er en funktion, der på en én-til-én måde bytter rundt på elementerne i en mængde f.eks. af tal eller bogstaver.

Eksempel

Her er en mængde af tal:

$\{1,2,3,4,5,6\}$

Jeg definerer permutationen F sådan:

$F(1)=3,\quad F(2)=6,\quad F(3)=5,\quad F(4)=4,\quad F(5)=1,\quad F(6)=2$

Det kan jeg også gøre ved hjælp af følgende skema:

$$F=\begin{pmatrix}1&2&3&4&5&6\\3&6&5&4&1&2\end{pmatrix}$$

Eksempel

Her er en anden permutation. Denne gang med bogstaver:

$$A=\begin{pmatrix}a&b&c&d&e&f\\c&f&e&d&a&b\end{pmatrix}$$

Læg mærke til ligheden med permutationen F fra eksemplet ovenover!

Sammensætning af permutationer

Hvis man har to permutationer, kan man sammensætte dem på samme måde, som man sammensætter funktioner:

Eksempel

Givet

$$A=\begin{pmatrix}a&b&c&d&e&f\\c&f&e&d&a&b\end{pmatrix}\quad\text{og}\quad B=\begin{pmatrix}a&b&c&d&e&f\\d&c&f&e&a&b\end{pmatrix}$$

Skemaet for den sammensatte permutation AB får jeg ved at se, hvad sker med elementerne i B og derefter følge dem over i A:

$$AB=\begin{pmatrix}a&b&c&d&e&f\\d&e&b&a&c&f\end{pmatrix}$$

Bemærk, at rækkefølgen ikke er ligegyldig:

$$BA=\begin{pmatrix}a&b&c&d&e&f\\f&b&a&e&d&c\end{pmatrix}$$

Man siger, at den *kommutative lov* ikke gælder for permutationer.

Hvis man har tre permutationer A, B og C, påstår jeg, at der gælder:

$A(BC)=(AB)C$

Man kan altså selv bestemme, i hvilken orden man udregner resultatet. Det hedder den *associative lov* for permutationer.

Når man skal beskrive Enigma-maskinen, er det smart at bruge en permutation for hver komponent i systemet og så se på, hvad der sker, når man sammensætter dem. Det vil jeg gøre i næste afsnit, men først lidt mere matematik.

Identitetspermutationen

Identitetspermutationen I er bytter ikke rundt på elementerne:

$$I = \begin{pmatrix} a & b & c & d & e & f \\ a & b & c & d & e & f \end{pmatrix}$$

Invers permutation

Hvis man har en permutation A, så findes der en såkaldt *invers permutation* A^{-1} sådan at

$$A^{-1}A = I \quad \text{og} \quad AA^{-1} = I$$

Eksempel

Givet

$$A = \begin{pmatrix} a & b & c & d & e & f \\ c & f & e & d & a & b \end{pmatrix}$$

Sæt

$$A^{-1} = \begin{pmatrix} a & b & c & d & e & f \\ e & f & a & d & c & b \end{pmatrix}$$

Tjek nu, at

$$A^{-1}A = I \quad \text{og} \quad AA^{-1} = I$$

NB:

Bemærk, at man får den inverse permutation ved at bytte rundt på de to rækker og så sortere efter bogstaverne i øverste række.

Jeg påstår, at der gælder følgende regel:

Sætning

$$(AB)^{-1} = B^{-1}A^{-1}$$

Bevis

Prøv selv at bevise reglen!

Cykler

Her er skemaet for en permutation

$$A = \begin{pmatrix} a & b & c & d & e & f \\ c & f & e & d & a & b \end{pmatrix}$$

Bemærk, at a bliver sendt over i c, som igen bliver sendt over i e, hvorefter e ryger tilbage til a. Man kalder dette en *cykel*, fordi man har en serie ombytninger, som kører i ring. Det skriver man sådan:

(ace)

Denne cykel er ikke den eneste i A. Der er faktisk to andre:

(bf) og (d)

Alt i alt skriver man:

$A = (ace)(bf)(d)$

Cykel-længde

Man siger, at permutationen A består af en 3-cykel, en 2-cykel og en 1-cykel. Tallene 3, 2 og 1 kalder man cyklernes *længde*.

Cykel-struktur

Man siger, at to permutationer A og B har samme *cykel-struktur*, hvis de har samme antal cykler af de forskellige længder.

Man kan opfatte cyklen (ace), som en permutation, som ombytter a, c og e, men lader de øvrige bogstaver stå. Tilsvarende kan man se på cyklerne (bf) og (d).

På den måde kan man opfatte

$A = (ace)(bf)(d)$

som en sammensætning af tre permutationer. Resultatet er netop A (overvej), så det er ok at skrive lighedstegn.

Konjugeret permutation

Nu er jeg nået til det sidste begreb, som skal være på plads, inden jeg kan beskrive Enigma-maskinen matematisk.

Definition

For to permutationer A og T definerer man den *konjugerede permutation* sådan:

$$K = TAT^{-1}$$

Der gælder en lille, men nyttig sætning her:

Sætning

Givet to vilkårlige permutationer A og T.

Hvis man har en cykel

$(a_1 a_2 ... a_k)$ i A

findes der en cykel med samme længde

$(T(a_1)T(a_2)...T(a_k))$ i $K = TAT^{-1}$

Korollar

Det følger af sætningen, at A og den konjugerede permutation TAT^{-1} har samme cykel-struktur! (Overvej!) Det får store konsekvenser i analysen af Enigma-maskinen!

Inden beviset skal du se, hvordan sætningen fungerer i praksis.

Eksempel

Givet to permutationer:

$$A = \begin{pmatrix} a & b & c & d & e & f \\ c & f & e & d & a & b \end{pmatrix} \quad \text{og}$$

$$T = \begin{pmatrix} a & b & c & d & e & f \\ d & c & f & e & a & b \end{pmatrix} \quad \text{med} \quad T^{-1} = \begin{pmatrix} a & b & c & d & e & f \\ e & f & b & a & d & c \end{pmatrix}$$

Jeg udregner nu den konjugerede:

$$TAT^{-1} = \begin{pmatrix} a & b & c & d & e & f \\ d & c & b & f & e & a \end{pmatrix}$$

Nu kommer det spændende så! Hvordan ser cyklerne ud i A og dens konjugerede?

$(ace)(bf)(d)$ i A

$(adf)(bc)(e)$ i TAT^{-1}

Altså samme cykelstruktur!

Bemærk, hvordan den konjugerede permutation forskyder tingene:
a går i c i A, mens T(a)=d går i T(c)=f i TAT^{-1}.

Bevis

Kig på to på hinanden følgende elementer i en cykel i A:

$(...a_i a_j ...)$

Der gælder altså:

$A(a_i) = a_j$

Nu ser jeg på, hvad der sker, når jeg anvender den konjugerede K permutation på $T(a_i)$:

$$K(T(a_i)) = TAT^{-1}(T(a_i)) = TA(a_i) = T(a_j)$$

Hvis a_i og a_j følger efter hinanden i en cykel i A, vil $T(a_i)$ og $T(a_j)$ følge efter hinanden i en cykel i den konjugerede permutation TAT^{-1}.

QED

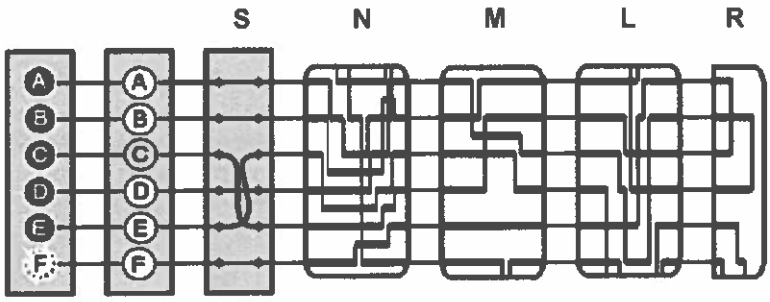
Opgaver

1	Find ud af, hvad en *gruppe* er i matematik. Vis derpå, at permutationerne for en mængde med n elementer udgør en gruppe! Man kalder denne gruppe Sym(n) - den *symmetriske gruppe*.
2	Vis, at antallet af elementer i Sym(n) er n!.

5: Den polske metode II

Analyse

Jeg vil nu analysere Enigma-maskinen matematisk og forklare, hvordan polakkerne med Marian Rejewski i spidsen kunne knække koden.



Jeg begynder med at indføre følgende permutationer:

- S = koblingstavlens ombytning af bogstaver.
- N = den første rotors ombytning UDEN drejninger.
- N_1 = den første rotors ombytning efter én drejning.
- M = den anden rotors ombytning UDEN drejninger.
- L = den sidste rotors ombytning UDEN drejninger.
- R = reflektorens ombytning.

Antagelser

Bemærk, at jeg har gjort flere antagelser her:

- Jeg kigger på den simple førkrigsversion af Enigma med 3 rotorer.
- Jeg ser bort fra, at rotor M og L drejer, selvom jeg ved, at f.eks. M drejer efter 26 bogstaver.

Vigtig notationsændring!

Jeg ændrer nu den måde, hvorpå jeg noterer sammensatte permutationer:

Hvor jeg tidligere skrev

$$AB(x) = A(B(x))$$

og derfor først anvendte B på x og siden A på B(x). bytter jeg nu rundt og skriver

$$AB(x) = B(A(x))$$

Jeg anvender simpelthen A først og B bagefter. Man kan også skrive det bagvendt:

$$(x)AB = ((x)A)B$$

Fordelen ved denne notation er, at man kan læse lange sammensætninger af permutationer fra venstre mod højre, altså i den normale læseretning.

Den vigtigste konsekvens af denne notationsændring er, at den konjugerede permutation nu bliver

$$B = T^{-1}AT$$

Enigma-permutationen

Enigma-maskinen efter én drejning af første rotor svarer nu til følgende permutation:

$$E_1 = SN_1MLRL^{-1}M^{-1}N_1^{-1}S^{-1}$$

Du kan følge permutationerne gennem maskinen: Gennem koblingstavlen, gennem rotorerne, vendt i reflektoren og tilbage igen via de inverse permutationer.

Bemærk, at denne måde at følge kodningen på svarer til at følge tegningen fra venstre mod højre og tilbage igen. Men som nævnt er retningen modsat for en rigtig Enigma-maskine set forfra. Tegningen viser altså den rigtige maskine bagfra.

Første pointe

Drejning svarer til konjugering

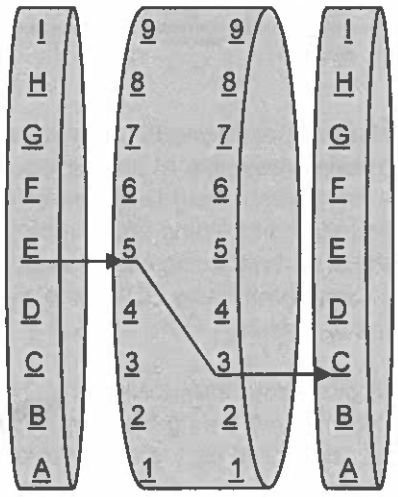
Som nævnt antager jeg, at det kun er den første rotor, som drejer. Det er også slemt nok, for det betyder matematisk, at den tilsvarende permutation ikke er konstant. Men man kan overraskende nemt løse problemet. Jeg påstår nemlig, at der gælder følgende:

$$N_1 = T^{-1}NT$$

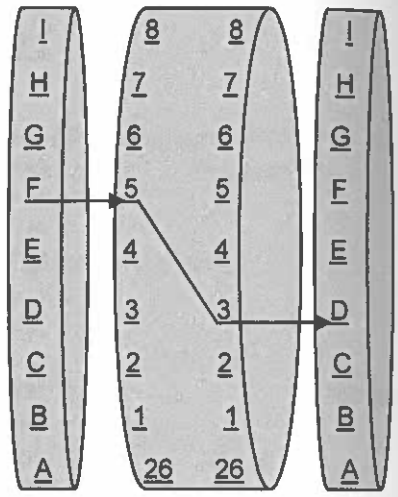
hvor

$$T = (abc...xyz)$$

Man kan med andre ord finde permutationen for den første rotor efter én drejning ved at konjugere med den permutation, som forskyder alle bogstaver netop ét trin! Det er nemlig sådan Enigma-maskinen fungerer, men det kræver en forklaring:



Før drejning.



Efter drejning.

I dette eksempel går strømmen fra venstre mod højre, og rotorens øverste del drejer ind i papiret. (Det svarer til en Enigma-maskine set bagfra.)

Antag, at E bliver til C. Efter én drejning er det hele forskudt ét trin således, at F bliver til D. (På tegningen har jeg kun tegnet ledningen for denne ombytning.)

Men ifølge sætningen fra sidste afsnit er det præcis sådan, konjugeringen fungerer:

Hvis a_i og a_j følger efter hinanden i en cykel A, vil $T(a_i)$ og $T(a_j)$ følge efter hinanden i en cykel i den konjugerede permutation $T^{-1}AT$.

På tegningen følger E og C efter hinanden i en cykel i N, mens F=T(E) og D=T(C) følger efter hinanden i en cykel i N_1

Det samme gælder for de øvrige bogstaver. Derfor er

$$N_1 = T^{-1}NT$$

Enigma-permutationen ovenover bliver med andre ord:

$$E_1 = ST^{-1}NTMLRL^{-1}M^{-1}(T^{-1}NT)^{-1}S^{-1}$$

Flere drejninger

Hvis man skal regne på flere drejninger, skal man blot konjugere flere gange. F.eks.

$$N_4 = T^{-1}T^{-1}T^{-1}(T^{-1}NT)TTT = T^{-4}NT^4$$

NB:

I noget af litteraturen ser man Enigma-maskinen forfra. Så går strømmen fra højre mod venstre, og rotoren drejer modsat. Permutationerne i udregningerne bliver derfor anderledes end her.

Anden pointe

Meddelelsesnøglen

Når tyskerne brugte Enigma-maskinen, sendte de først en *meddelelsesnøgle* på tre bogstaver, som gav modtageren information om indstillingen af de tre rotorer. De tre bogstaver blev sendt to gange i træk for at være sikker. F.eks.

Klartekst: BMWBMW
Kodet tekst: AKTOLV

Dette udnyttede de polske matematikere, for det giver jo information om, hvordan Enigma-maskinen koder bogstaver efter 1 og 4 drejninger af rotor 1. F.eks. bliver B først til A, mens B 4 drejninger senere bliver til O.

Lad E_1 som før være permutationen svarende til 1 drejning, mens E_4 er permutationen svarende til 4 drejninger.

Jeg har altså:

$E_1(B) = A$ og $E_4(B) = O$

Men da maskinen koder og afkoder (den er *selv-reciprok*) i samme omgang, gælder der:

$E_1(A) = B$

Der giver alt i alt:

$E_1E_4(A) = O$

hvor jeg altså benytter den bagvendte notation.

Nu ved jeg altså, hvordan permutationen E_1E_4 koder bogstavet A.

Ved at indsamle data fra en masse kodede beskeder kunne de polske matematikere fuldstændig kortlægge permutationen E_1E_4.

Matematisk har jeg som før:

$$E_1 = ST^{-1}NTMLRL^{-1}M^{-1}(T^{-1}NT)^{-1}S^{-1}$$

Den sammensatte permutation bliver:

$$E_1E_4 =$$
$$(ST^{-1}NTMLRL^{-1}M^{-1}(T^{-1}NT)^{-1}S^{-1})(ST^{-4}NT^4MLRL^{-1}M^{-1}(T^{-4}NT^4)^{-1}S^{-1})$$

Dette udtryk kan man regne videre på, og resultatet er følgende:

(*) $E_1E_4 = ST_1T_4S^{-1} = (S^{-1})^{-1}T_1T_4(S^{-1})$

hvor

$T_1 = T^{-1}NTMLRL^{-1}M^{-1}T^{-1}N^{-1}T$ og

$T_4 = T^{-4}NT^4MLRL^{-1}M^{-1}T^{-4}N^{-1}T^4$

Identisk cykelstruktur

Formlen (*) siger noget meget interessant:

Permutationen E_1E_4 opstår som konjugeret til permutationen T_1T_4. De to permutationer har derfor samme cykelstruktur. Når de polske matematikere fandt E_1E_4, kunne de også finde cykelstrukturen, som altså var identisk med cykelstrukturen i T_1T_4.

Bemærk nu, at S slet ikke indgår i T_1T_4. Denne permutation påvirker derfor ikke koblingstavlens funktion, men kun rotorerne og reflektoren. Antallet af kombinationer er her:

$(3 \cdot 2 \cdot 1)(26 \cdot 26 \cdot 26) = 105456$

Det betyder, at der maksimalt kan være et tilsvarende antal cykelstrukturer.

Katalog

De polske matematikere lavede nu et fuldstændigt katalog over hvilke Enigma-indstillinger, der gav hvilke cykelstrukturer. Disse strukturer fungerede som et slags fingeraftryk for maskinen.

Dette arbejde var stort, men slet ikke så uoverkommeligt som at kigge på samtlige kombinationer for Enigma-maskinen MED koblingstavlen medregnet.

Hvad polakkerne gjorde var med andre ord at afkoble koblingstavlen fra de øvrige komponenter i Enigma-maskinen. Derved reducerede de afkodningsopgaven betydeligt.

Ud fra meddelelsesnøglerne i de kodede beskeder afdækkede man cykelstrukturen i permutationen E_1E_4 og sammenlignede med kataloget over cykelstrukturen i permutation T_1T_4. Når der var et eller flere match, indstillede man sin Enigma-maskine og afkodede beskederne. Uden kendskab til koblingstavlen ville beskederne stadig være svære at læse, men ofte dukkede der som nævnt små brudstykker op i koderne, som afslørede koblingstavlen, f.eks. ordet

BAFBHRTNBCHAERLIN

som minder om sætningen

ABFAHRT-NACH-BERLIN

hvis man altså bytter rundt på A og B. Med andre ord en indikation af en given ledning på koblingstavlen.

Opgaver

1 Vis udtrykkene for P_1 og P_2

Referencer

- Simon Singh: Kodebogen (ISBN: 87-0045556-3)
- Chris Christensen. Polish Mathematicians Finding Patterns in Enigma Messages. Mathematics Magazine, Vol. 80, No. 4, October 2007, page 247-273 (Mathematical Association of America)
- Jesper Frandsen: Enigma - et dilemma (ISBN: 978-87-616-2485-7)
- Erik Vestergaard: Den tyske kodemaskine Enigma (http://www.matematiksider.dk/enigma.html)
- Erik Vestergaard: Matematikken bag løsningen af Enigma (http://www.matematiksider.dk/enigma/enigma_matematik.pdf)
- Crypto Museum (http://www.cryptomuseum.com)