Den tyske kodemaskine Enigma og Bletchley Park

Erik Vestergaard, Haderslev Katedralskole,
vestergaard@matematiksider.dk,
www.matematiksider.dk

Enigma var en elektro-mekanisk kodemaskine, som blev brugt af tysk militær til kryptering og dekryptering af meddelelser. Her berettes om Enigma – også som emne for et studieretningsprojekt.

I slutningen af september 2007 var jeg med min gode kollega Benned Bennedsen og min dygtige matematikklasse 3F fra Haderslev Katedralskole på studietur til London. Et af de programsatte punkter var en tur til *Bletchley Park*, beliggende i nærheden af Milton Keynes, ca. 90 km nordvest for London. En togtur på ca. 50 min. fra Euston Station i det centrale London.

Bletchley Park under krigen

Idéen med at tage til Bletchley Park havde jeg fået af en tidligere studiekammerat. Stedet er ikke umiddelbart så kendt, men besøget viste sig at være et rigtig fint fagligt indslag i faget matematik, skulle det vise sig. Sagen er, at under 2. verdenskrig arbejdede flere tusinde englændere her i den dybeste hemmelighed med at løse tyskernes kodede meddelelser.

Den mest berømte af bedrifterne i Bletchley Park er uden tvivl dekrypteringen af den tyske kodemaskine *Enigma*. I vedvarende perioder lykkedes det englænderne at læse de krypterede meddelelser, der blev sendt via morsesignaler til de relevante tyske krigsenheder: Hæren (Wehrmacht), luftvåbnet (Luftwaffe) og flåden (Kriegsmarine). Signalerne blev opsnappet på et antal modtagestationer, såkaldte *Y-Stations* i

Min kollega og en del af klassen på 22 elever foran hovedbygningen i Bletchley Park.

England eller på kontinentet og sendt til Bletchley Park (*Station X*). Her sad unge folk, som i al hemmelighed var blevet rekrutteret fra forskellige undervisningsanstalter eller som var blevet anbefalet af folk indenfor systemet. Man søgte efter folk, som havde talent for at tænke logisk og med evnen til at kombinere: matematikere, kryptologer, skakspillere samt krydsordsløsere. Desuden havde man brug for folk med sprogkendskab, herunder naturligvis tysk. Men også folk med kendskab til lingvistik, ægyptiske hieroglyffer og oldgræsk. I det hele taget mange intellektuelle. En del personer kom fra det nærliggende Cambridge University.

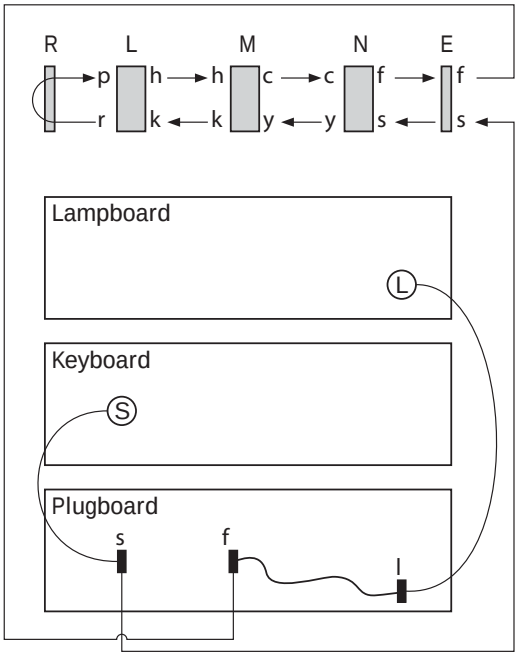
Den helt store helt fra Bletchley Park er Alan Turing, som var en genial matematiker fra Kings College, Cambridge. Allerede før krigen havde han markeret sig med en banebrydende artikel indenfor "teorien for beregnbarhed" (*The Theory of Computation*), en gren af den matematiske logik. De såkaldte *Turing-maskiner*, som han derved lagde navn til, er et højst abstrakt begreb. I Bletchley Park viste Alan Turing dog også sine mere praktiske sider ved at designe de såkaldte *bombs*, der var elektromekaniske maskiner, som kunne prøve en masse muligheder af på ret kort tid, når man forsøgte at bryde dagens krypterede meddelelser. Anvendelsen af disse bombs var en essentiel del af hele processen med at dekryptere. Den efterretning, som under krigen fremkom ved at dekryptere fjendens radiokommunikation, gik under betegnelsen ULTRA for *ultra secret*. Kontrafaktisk historie er en svær disciplin, men kendte historikere har vurderet, at ULTRAs resultater forkortede krigen med 2 år! Ikke mindst i ubådskrigen – The Battle of The Atlantic – leverede ULTRA efterretninger, som sparede mange allieredes liv.

Besøget

Fra pladsen foran Bletchley Rail skulle vi blot gå til højre i fem minutter, så var vi ved indgangen til *Bletchley Park National Codes Center*. Her blev vi mødt af en repræsentant for stedet, som viste os op i Block B, hvor vi hørte på et foredrag om Enigma, noget af dens matematik og dens historie – et foredrag, som vi havde bestilt på forhånd

En rigtig Enigma-maskine.

før afrejsen fra Danmark. Under foredraget, som varede ca. 1 time, fik vi også forevist en rigtig Enigma-maskine. I den forbindelse skal det lige nævnes, der er mulighed for at sammensætte et besøg på forskellige måder. Man kan også overvære et mere generelt foredrag "Codes and Ciphers" eller "Breaking Lorenz". Sidstnævnte handler om en anden af tyskernes kodemaskiner. Lorenz-cifferet blev også løst af englænderne, denne gang ved hjælp af en kæmpe maskine kaldet *Colossus*, som blev bygget af Tommy Flowers i 1943-44. Det skulle efter sigende være verdens første programmerbare maskine. Maskinen omta-



Principdiagram for ENIGMA.

les i dag som en forløber til den moderne computer. Historien om ULTRAs succes med at knække Enigma og Lorenz under krigen blev faktisk først frigivet af den britiske efterretningstjeneste i 1974! På grund af den store hemmeligholdelse selv efter krigen, blev de oprindelige Colussusmaskiner skilt ad. En ældre, meget dedikeret mand ved navn Tony Sale byggede i 90'erne en kopi af den gamle Colossus. Tony var også tilstede under vort besøg, og han er meget villig til at give en demonstration af maskinens virkemåde foran apparatet.

Efter foredraget om Enigma gik vi en tur i parken og fik forklaret lidt om bygningerne og de personer, som havde boet der. Herefter var vi godt sultne og fik indtaget et måltid i en kantine, som var indrettet i en af de gamle *Huts*, som husede kodebryderne under krigen. Efter spisning fortsatte turen i parken, hvor vi blandt andet kom forbi det hus, som Alan Turing havde boet i, og vi lyttede til anekdoter om ham. Han gik for at være lidt af en excentriker. Vi fik også besøgt et lille museum med ting fra krigen samt en shop. Alt i alt et vellykket arrangement!

Enigmamaskinens virkning

Det er på tide, at vi kigger lidt på, hvordan Enigma fungerer. Maskinen, som er afbildet på figuren på forrige side, ligner en skrivemaskine. Man indtaster et bogstav på keyboardet, som har 26 bogstaver fra a til z. Det krypterede bogstav lyser derefter straks op på lampboardet. Krypteringen foregår på følgende måde, som anskueliggjort på skitsen til venstre: Lad os sige, at man trykker på s. En strøm går da til s i det såkaldte *Plugboard*, hvori nogle af bogstaverne er forbundet to og to via ledninger. Da der ikke er nogen plug i bogstavet s, fortsætter strømmen direkte til s i *indgangshjulet* E, som ikke gør andet end at sende signalet videre til de tre bevægelige hjul *N*, *M* og *L*, hvis indre består af ledninger kombineret på kryds og tværs. Det bevirker, at bogstaverne indirekte bliver permuteret. Efter passage af de tre hjul, er signalet nået til *reflektoren R*, som udover at permutere bogstavet r til p, sender signalet tilbage igennem de tre bevægelige hjul, tilbage til plugboardet i bogstavet f. Da f og l er forbundet med en ledning, går signalet til bogstavet l, som endeligt lyser op på lampboardet.

Polakkernes bidrag

Sjovt nok var det slet ikke englænderne, der var de første til at knække Enigma, men derimod polakkerne. Det er en længere og absolut interessant historie, men det vil føre for vidt at komme ind på i detaljer her. Det skal dog nævnes, at polakkerne efter 1. verdenskrig oprettede en efterretningsenhed, Biuro Szyfrów. En ung student i statistik, *Marian Rejewski*, skulle vise sig at have et specielt talent for at løse den kode, som tyskerne anså for ubrydelig. Ved hjælp af matematisk snilde og vedholdende hårdt arbejde lykkedes det ham at knække koden. Særligt udnyttede han en svaghed i den måde tyskerne krypterede på.

Her bør det lige nævnes, at Enigma i princippet er en elektromekanisk realisering af et polyalfabetisk kryptosystem. Det betyder, at et nyt alfabet bliver benyttet for hvert nyt bogstav, der bliver krypteret. Alligevel var tyskerne – fornuftigt nok – bekymrede for det problem, som på engelsk betegnes *depth*, hvormed menes, at man ved hjælp af mange meddelelser med den samme dagsnøg-

le vil være i stand til at samle nok statistik til at kunne bryde koden. Derfor krypterede tyskerne *dobbelt*, ved inddragelse af en *meddelelsesnøgle* for hver eneste ny meddelelse! Meddelelsesnøglen fortalte, hvordan de tre bevægelige hjul skulle indstilles og bestod af tre bogstaver. Tyskerne begik imidlertid én fejltagelse: De var for grundige! For at modvirke det problem, at bogstaverne undertiden blev forvanskede under transmissionen, skrev tyskerne meddelelsesnøglen på de tre bogstaver to gange efter hinanden i starten af ethvert dokument! Denne kendsgerning kunne Rejewski udnytte, idet han så vidste, at 1. og 4. bogstav i enhver krypteret meddelelse stammede fra det samme alfabet. Samme for 2. og 5. bogstav og 3. og 6. bogstav. Herefter skulle der dog en genial anvendelse af den matematiske teori om *permutationer* til at blotlægge Enigma. I princippet er enhver kryptering med Enigma resultatet af en permutation af 26 bogstaver. Rejewski gjorde den opdagelse, at permutationens *cykelstruktur* er uafhængig af indstillingerne i plugboardet. Det betød reelt, at arbejdet med at prøve indstillinger af blev meget kraftigt reduceret.

Studieretningsopgave i matematik om Enigma

Efter studieturen besluttede en af mine elever at skrive om Enigma i studieretningsopgaven i fagene matematik og historie. Her var jeg så heldig, at amerikaneren Chris Christensen netop havde skrevet en artikel om den matematik, som polakkerne benyttede til at bryde Enigma. Der er tale om herlig matematik, hvor *permutationer og kombinatorik* kommer i spil og med lidt instruktion gik opgaven fint! I øjeblikket arbejder jeg på en hjemmeside om Enigma, som forventeligt er færdig, når denne artikel udkommer på LMFK:

www.matematiksider.dk/enigma.html

Forfatteren til artiklen i *Mathematics Magazine*, Chris Christensen har givet mig lov til at anbringe sin artikel på min hjemmeside til download! For at gøre artiklen mere tilgængelig for danske gymnasieelever, har jeg skrevet en lille hjælpenote. Heri indfører jeg permutationsbegrebet, og noten er ellers udformet som en guide til nævnte artikel, med en række opgaver, så en elev kan komme med selvstændige bidrag til en studieretningsopgave. På min hjemmeside vil man også kunne læse mere detaljeret om Enigma maskinen end tilfældet er i denne kortfattede artikel.

Måske nogle kender Simon Singhs bog, som på dansk har titlen *Kodebogen*? Det er på mange måder en fremragende bog, som omtaler vigtige dele af kryptologiens historie og også historien om Marian Rejewski og Alan Turing. Hvad angår matematikken i Alan Turings bidrag, så betegnes den af kendere dog for at være beskrevet for simplificerende. I det hele taget findes der en mængde materiale på nettet om Enigma. Man kan endda downloade flere gratis Enigma simulatorer. Jeg har givet et link til en af de bedste! Historien om Bletchley Park er desuden filmatiseret i filmen *Enigma* af Robert Harris.

Litteratur

- Chris Christensen: Polish Mathematicians Finding Patterns in Enigma Messages. *Mathematics Magazine*, Vol. 80, No. 4, October 2007, side 247-273 (The Mathematical Association of America).
- Simon Singh: *Kodebogen – Videnskaben om hemmelige budskaber fra oldtidens Ægypten til kvantekryptering*. Gyldendal, 2001.
- Andrew Hodges: *Alan Turing: the enigma*. Vintage, 1992 (oprindeligt 1983).
- F.H. Hinsley, Alan Stripp (editors): *Code Breakers – The inside Story of Bletchley Park*. Oxford University Press, 1993.

Links

- *www.bletchleypark.org.uk.* Bletchley Parks officielle hjemmeside.
- *www.matematiksider.dk/enigma.html.* Min egen hjemmeside om Enigma.
- *users.telenet.be/d.rijmenants/en/enigmasim.htm*. En glimrende Enigma simulator kan downloades og benyttes gratis. ◊