

Tysklands brug af koder under Anden Verdenskrig, særligt i U-bådskrigen mod England

Studieretningsprojekt i matematik (A) og historie (A)

Introduktion

I 1940 var England tilbage som det sidste allierede land i Europa med mulighed for at føre krig mod Tyskland. De øvrige europæiske lande var enten erobrede eller allierede med Tyskland eller ikke i stand til at føre angrebskrig mod aksemagterne.

Den engelske befolkning og krigsmaskineri var i de første år af Anden Verdenskrig fuldstændig afhængig af forsyninger bragt med fragtkonvojer fra USA. Det var derfor i Tysklands største interesse at sænke disse forsyninger og til dette formål var U-både uovertrufne.

De tyske styrker kodede deres kommunikation med Enigma-maskiner, maskiner der med en blanding af mekanik og elektronik hurtigt kunne omsætte en almindelig tekst til en ulæselig bogstavrækkefølge og senere oversætte denne kode til den oprindelige meddelelse hos modtageren, når denne havde en Enigma-maskine og det rette kodeord.

Gennem snedighed og forståelse af matematikken bag Enigmaen, lykkedes det englænderne at knække koden og således læse store dele af tyskernes kommunikation. Denne bedrift menes at have været mere væsentlig end mange af begivenhederne ved fronten og at have forkortet Anden Verdenskrig med cirka to år.

Til kodebrydningen udviklede englænderne forløberen for den moderne computer.

Et emne så spændende at det har affødt flere romaner og en film med internationale stjerner!

Faglige forudsætninger (matematik):

Matematisk handler projektet om talteori og kryptografi – emner, som eleverne formodentlig ikke har stiftet bekendtskab med i undervisningen. Projektet kræver derfor ikke andre forudsætninger end et vist flair for tal og almindelig matematisk interesse.

Faglige mål (matematik):

- Eleverne skal opnå grundlæggende kendskab til kryptografi og den nødvendige talteori i den forbindelse, de centrale krypteringsformer for opgaven er monoalfabetisk og polyalfabetisk substitution (ambitionsgraden i matematikken kan varieres som skitseret senere, men behøver ikke være meget høj).
- Grundlæggende forståelse for, hvordan kryptologimodeller er opbygget. Hvorfor havde tyskerne så blind tillid til Enigmaen under Anden Verdenskrig?
- Anvendelse af sandsynlighedsregning i forbindelse med frekvensanalyse.

Faglige forudsætninger (historie):

- Eleverne bør have kendskab til Anden Verdenskrig og til den generelle europæiske politik og blokdannelse i 1900-tallet.

Faglige mål (historie):

- Eleverne skal opnå indgående kendskab til dele af Anden Verdenskrig og aspekter af Tysklands krigsførelse.
- Eleverne skal opnå kendskab til nødvendigheden af hemmelig kommunikation i forbindelse med politik og krigsførelse.
- Opgaven kan perspektiveres til moderne aspekter af hemmelig kommunikation fx under den kolde krig.

Nærmere beskrivelse af projektemnet

Matematisk del:

For at uddybe Enigmaens betydning under Anden Verdenskrig og for at forstå de kryptologiske aspekter, er det passende at give en kort gennemgang af, hvordan kryptologiske metoder har gennemgået en udvikling gennem historien.

Foruden grundbegreber i kryptologimodellen som klartekst, kryptotekst, nøgle osv., bør både mono- og polyalfabetiske substitutionssystemer belyses, ligesom der skal gøres rede for principperne i frekvensanalyse.

Sandsynlighedsregning kan inddrages ved at gennemgå Friedmans test, der bruges til at knække den polyalfabetiske Vigenere-kode (Landrock, Nissen, s. 43-47). Dette var medvirkende til at tyskerne udviklede Enigmaen, som selvfølgelig skal beskrives nøje med en analyse af dens styrke og de svagheder, som til sidst blev udnyttet (Kodebogen, s. 138-204). Der bør dog i den forbindelse nok fokuseres på de kryptologiske aspekter af Enigma-maskinen, da denne som apparat er indviklet og nok også mindre interessant både matematisk og historisk (det skal sikres at opgaven ikke udvikler sig til en teknisk manual).

Historisk del:

I den historiske ses dels på de generelle historiske aspekter vedrørende Englands rolle i starten af Anden Verdenskrig og hvorfor flådekrigen spillede så stor en rolle for England. Dels ses specifikt på forskellige historikers syn på betydningen af Tysklands brug af koder og af, at det lykkedes englænderne at knække den tyske kode. Som et lille men konkret eksempel på vigtigheden af at opsnappe information under krigen kan nævnes fundet af en Enigma-maskine samt manualer ombord på U-110 i maj 1942 (http://cadigweb.ew.usna.edu/~wdj/sm230_cooper_enigma.html).

Variationsmuligheder

Det synes at være oplagt at inkludere specifikke krypteringsopgaver i et projekt og på denne måde kan den matematiske del af opgaven varieres, hvis flere elever skriver om samme historiske emne. Mere generelt gælder det, at da kryptologiske metoder har været anvendt et utal af steder i historien, så er der rig mulighed for variation, hvad angår det historiske emne. Her kan nævnes

- Cæsars substitutionssystem, som blev anvendt i Romerriget.
- Herodot beretter om eksempler på anvendelse i Oldtidens Grækenland (Kodebogen, s. 18).
- Den første anvendelse af frekvensanalyse i den blomstrende kultur i Mellemøsten ca. 700-800 (Kodebogen, s.28).
- Den første anvendelse af polyalfabetiske substitutionssystemer af Alberti i Renæssancen (Kodebogen, 59).
- Louis XIV's anvendelse af det "det store cifferskrift" (Kodebogen, 69-72).
- Zimmerman-telegrammets indflydelse på 1. Verdenskrig (Kodebogen, 117-129).

- Mary Stuarts anvendelse af nomenklator til korrespondancen med sine medsammensvorne, og hvorledes de kodede meddelelser førte til hendes dom og straf (Kodebogen, s. 51-58). Her er der masser af materiale at hente på nettet. Vi mener også at projektet har ganske meget kød på rent historisk set. Den engelske dronning Elisabeth lægger afstand til de sydeuropæiske, katolske kongehuse, i og med hun er protestant. Den tragiske historie om Mary Stuart spinder sig omkring et ønske om at få det katolske kongehus tilbage. Man kunne lade et historieprojekt dreje sig om Katolicisme/Protestantisme i Nordeuropa. Vi har (vist nok) den første kongelige, som bliver dømt ved civil domstol, hvilket er uhørt på den tid. Man kunne kigge specifikt på retssagen, og se på retssamfundet dengang.

Ambitionsniveauet i den matematiske del af opgaven kan hæves for den interesserede elev:

- Gruppeteori og specielt permutationer i forbindelse med monoalfabetiske substitutionssystemer kan inddrages.
- RSA-systemet (som er langt mere ambitiøst matematisk set) kan inddrages som den historiske udvikling i kodesystemer efter Anden Verdenskrig (Enigma blev jo brudt og computerens tidsalder var på vej, så man måtte finde på noget nyt).
- Inddragelse af fejlrettende koder (<http://www.matilde.mathematics.dk/arkiv/M12/hoeholdtd.pdf>).

Henvisninger (pr. 07.04.2007)

Kryptering:

Singh, S.: "Kodebogen", Gyldendal 2001 (En meget læseværdig ikke-matematisk introduktion til anvendelsen af kryptografi gennem historien)

Erlandsen, M. K.: "Introduktion til Kryptologi". PDF-udgave:

<http://www.imf.au.dk/besogsservice/arrangementer/kryptologi.pdf>

(Meget fin introduktion til kryptering. Indeholder også et afsnit om RSA-kryptering)

Landrock, P. & Nissen, K.: "Kryptologi – fra viden til videnskab", Abacus 1997.

Landrock, P. & Nissen, K. (1990) "Kryptologi". Forlaget ABACUS

(Matematisk gennemgang af krypteringsmetoder lige fra monoalfabetisk kryptering til RSA).

Carstensen, J.: "Talteori". Systime 1993 (Indeholder ikke særskilte afsnit om kryptografi, men giver en meget enkelt fremstillet introduktion til talteori.)

Hansen, J. P. & Spalk, H. G.: "Algebra og talteori". Gyldendalske Boghandel Nordiske Forlag 2002.

Kilder specielt til RSA-kryptering:

"Algebraen og talteorien bag offentlig nøgle kryptering og signering". Noter til kursus Fuglsø, okt.

2000 af Johan P. Hansen. PDF-fil på: <http://home.imf.au.dk/matjph/fuglsoe.pdf>

(Fin indgang til matematikken bag kryptologien. Kap. 8 og 9 er om de generelle idéer bag RSA systemet.)

Andersen, Henning E. "Kryptologi og krypteringssystemer". Institut for Matematiske Fag. Aalborg Universitet. (2004). PDF-udgave: <http://www.math.aau.dk/highschool/kryptologi.pdf> (Meget fin introduktion til RSA-systemet. Indeholder desuden flere gode links videre)

"Elementær Talteori" af Thorup, Anders, Københavns Universitet 2006. PDF-udgave:

<http://www.math.ku.dk/noter/elmtal.pdf> (Udførlig gennemgang af matematikken bag RSA-systemet, som introduceres på side 67. Niveauet måske lidt højt).

Om fejlrettende koder:

<http://www.matilde.mathematics.dk/arkiv/M12/hoeholdtdt.pdf>

Gruppeteori:

<http://home.imf.au.dk/besog/arrangementer/grupper.pdf> (Fin og enkel fremstilling af de basale ingredienser i gruppeteori. Kap. 3 om symmetriske grupper er særlig relevant.)

"Kryptografi, primtal og Riemannshypotesen" artikel af Ben Johnsen, publiceret i tidsskriftet NORMAT Vol. 34 (1986). Omtales som nr. 10031 på <http://www.imf.au.dk/da/ydelser/3g-gym/artikelbase.html>.

Skønlitterære kilder:

”Enigma” af Robert Harris (1995). Roman om det historiske forløb omkring Enigma.

”Enigma” (2002)- filmatisering af ovenstående bog med bla. Kate Winslet og Nikolaj Coster-Waldau. Instruktør: Michael Apted.

”Enigma: The Battle for the Code” (2000). Roman af Hugh Sebag-Montefiore.

Kilder om Anden Verdenskrig

- Roskill (2004) “The war at sea”. Forlag Naval & Military Press Ltd. Link: <http://www.amazon.co.uk/War-Sea-1939-45-Defensive-Official/dp/1843428032>
- Churchill, W. “The second world war”. Link: <http://www.amazon.com/Second-World-War-Six-Boxed/dp/039541685X> (Churchill var en ivrig skribent og meget historieinteresseret. Desuden var hans tidlige embede marineminister, så han var særligt interesseret i denne del af krigen. Bogen er en mastodont og bør nok læses i udvalg)
- Alanbrooke. “War diaries 1939-1945”. Link: http://www.amazon.com/Diaries-1939-1945-Field-Marshal-Alanbrooke/dp/0520239024/ref=pd_bbs_sr_1/102-5468274-3314555?ie=UTF8&s=books&qid=1174141492&sr=1-1 (Alanbrooke var Churchills Chief of Staff)
- Jackson, R “The German Navy in WWII”. Link: http://www.amazon.com/German-Navy-Wwii-Robert-Jackson/dp/186227066X/ref=sr_1_1/102-5468274-3314555?ie=UTF8&s=books&qid=1174141595&sr=1-1
- Jackson, R. “Kriegsmarine: The Illustrated History of the German Navy in WWII”. Link: http://www.amazon.com/Kriegsmarine-Illustrated-History-German-Navy/dp/0760310262/ref=sr_1_2/102-5468274-3314555?ie=UTF8&s=books&qid=1174141595&sr=1-2
- Kahn, David: Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939-1943. Link: <http://www.amazon.com/Seizing-Enigma-German-U-Boats-1939-1943/dp/0395427398>
- <http://hitlernews.cloudworth.com/enigma-machine-secret-code-bletchley-park.php> (Enigma-relateret emne i nyhederne)
- Generelt, så returnerer søgemaskiner som Google rigtig mange links af historisk interesse med forskellige indgangsvinkler, i fald man kombinerer søgeord som ”submarine”, ”cryptography” og ”World War”.

Kilder om Første Verdenskrig og Zimmermann-telegrammet:

Tuchman, Barbara W.: ”Telegrammet fra Zimmermann. Da USA i 1917 valgte side.” Forum. 1988.

Websider

Om Kryptering:

- <http://www.smithsrisca.demon.co.uk/crypto-ancient.html>
(Kryptologiens Historie i England) Engelsk.
- <http://www.otr.com/ciphers.html>
(Kort om ciffer-kodning. Gode links til andre sider, blandt andet meget om Enigmaen og ubådskrigen) Engelsk.
- <http://www.math.ku.dk/famos/arkiv/10-4/node6.html>
(Fin introducerende artikel af Lars Winther Christiansen både om kryptering generelt og om Enigmaen) Dansk.
- <http://www.matilde.mathematics.dk/arkiv/Matilde12>
(Nogle artikler om kryptering) Dansk
- http://www.simonsingh.net/Crypto_Corner.html
(Singh’s hjemmeside om kryptering) Engelsk
- <http://www.xramp.com/resources/vigenerecipher/>
(Hjemmeside, hvor man kan kryptere i Vigenere-kode) Engelsk

- <http://www.nationalcodescentre.org/edu/teachers/mathsr.htm>
(For lærere om koder) Engelsk
- <http://www.nku.edu/~christensen/cryptology%20notes.pdf>
(Om forskellige metoder til kodebrydning) Engelsk
- <http://www.nku.edu/~mcs/mat494/>
(Blandet om kryptering. Blandt andet henvisninger til hjemmesider og programmer, hvor man kan kryptere/dekryptere tekster) Engelsk
- <http://da.wikipedia.org/wiki/Kryptologi>
(Wikipedia om Kryptologi) Dansk.
- <http://cadigweb.ew.usna.edu/~wdj/papers/cryptoday.html>
(Artikler om forskellige typer kodning bla. enigma, men også andre interessante perspektiver)

Om Enigmaen:

- http://www.ieee.org/portal/cms_docs_iportals/iportals/aboutus/history_center/wesolkowski.pdf
(Om Enigmaen, sepecielt det polske gennembrud før Anden Verdenskrig) Engelsk.
- http://www.armyradio.com/publish/Articles/The_Enigma_Code_Breach/The_Enigma_Code_Breach.htm#3.%20The%20Methods%20Of%20Cipher%20Breach
(Gennemgang af Enigmaens historie og af forskellige Enigma-maskiner) Engelsk.
- <http://www.cryptographic.co.uk/enigmareview.html>
(Review af filmen ”Enigma”) Engelsk.
- <http://da.wikipedia.org/wiki/Enigma>
(Dansk Wikipedea om Enigmaen) Dansk
- <http://www.nsa.gov/publications/publi00004.cfm>
(Om matematikken bag Enigmaen)
- <http://www.xat.nl/enigma/>
(Indeholder bl.a. en simulator af Enigmaen)
- <http://puzzles.about.com/library/weekly/aa000825.htm>
(Om Enigmaens konkrete betydning under Anden Verdenskrig)
- http://cadigweb.ew.usna.edu/~wdj/sm230_cooper_enigma.html
(En kort gennemgang af nogle vigtige hændelser under Anden Verdenskrig, set med kryptologiske øjne.)

Om Mary Stuart:

- <http://query.nytimes.com/gst/fullpage.html?res=9407E1DF1339F932A25757C0A9629C8B63&sec=&spon=&pagewanted=print>
(Om Mary Stuart) Engelsk.
- <http://heritage.scotsman.com/myths.cfm?id=1512902006>
(Om Mary Stuart) Engelsk.
- http://en.wikipedia.org/wiki/Mary_I_of_Scotland
(Wikipedia om Mary Stuart)
- http://departments.kings.edu/womens_history/marystuart.html
(Kort om Mary Stuart. God litteraturliste til (engelske) bøger om Mary Stuart) Engelsk.
- <http://www.marie-stuart.co.uk/>
(Link til Mary Stuart Society's webside) Engelsk.
- http://www.bbc.co.uk/history/british/tudors/launch_gms_spying.shtml
(BBC-kodespil baseret på Mary Stuart-episoden. Useriøst, men lidt sjovt) Engelsk.