Knæk koden, Alan!

– En fortælling om matematikere og verdenshistorien

Søren Wengel Mogensen

Når en kemiker, en fysiker og en matematiker sidder på Caféen? og diskuterer emner af akut vigtighed, som fx deres respektive fags indflydelse på verdenshistoriens gang, vil kemikeren vel med rette kunne hævde at 1. verdenskrig i høj grad var kemiens krig med den ukritiske anvendelse af kemiske våben som verden for første gang stiftede bekendtskab med. Fysikeren vil nok fremhæve, igen med en vis berettigelse, 2. verdenskrig og Manhattanprojektet, som satte et effektivt punktum for den amerikansk-japanske del af 2. verdenskrig. Matematikeren vil naturligvis som en standardrefleks påpege, at matematikken jo netop er grundlaget for mange andre videnskaber. Imidlertid skal en stolt matematiker heller ikke glemme, at verdenshistorien faktisk rummer tilfælde, hvor matematikken, eller i hvert fald matematikere, var i forreste linje og ikke gemt bag fysiske love, kemiske forbindelser eller lignende. 2. verdenskrig og de allieredes kamp for at bryde de tyske koder er netop et af de tilfælde, hvor matematikere viste sig mere nyttige for krigsindsatsen som skrivebordskrigere end som fodsoldater. Disse matematikere blev naturligvis til en vis grad misforstået af deres samtid, men det skal jo ikke forhindre Famøs i at se tilbage på en stor fortælling om matematik, liv og død.

Enigma

Når talen falder på kodebrydning og 2. verdenskrig, dukker briten Alan Turings navn op i manges hoveder. Turing blev født i 1912 og få år efter grundlagde tyskerne Arthur Scherbius og Richard Ritter en virksomhed, hvis mest kendte produkt skulle vise sig

at have afgørende indflydelse på Turings liv. Scherbius og Ritter forsøgte sig med alt fra turbiner til opvarmede puder, men af eftertiden blev de især husket for Enigma, krypteringssystemet, som Turing skulle spille en prominent rolle i kampen mod. Selvom Alan Turing fortjent har fået meget af æren for at bryde den tyske Enigmakode, må det nævnes, at en bedrift af den kaliber sjældent kommer fra ét menneske alene. Allerede i 20'erne begyndte den proces, der skulle muliggøre det, som tyskerne troede umuligt, nemlig at Turing og hans hold under 2. verdenskrig formåede at udkode dele af tyskernes krypterede kommunikation. Allerede i mellemkrigstiden havde tyskerne verdens mest sikre, bredt anvendelige krypteringssystem i Enigma. Tidens teknologi muliggjorde en stærkere kryptering, ligesom man også dengang kunne anvende teknikker, der praktisk talt gjorde en tredjeparts dekryptering umulig, men ingen systemer kombinerede kommunikationssikkerhed og anvendelighed, som Enigma gjorde det. Især polakkerne var meget bekymrede over dette, da retorikken fra det tyske nationalsocialistiske parti var skarp over for især Polen. Frankrig og England følte sig derimod godt tilpas som Europas stærkeste nationer efter sejren i 1. verdenskrig og følte derfor ikke noget behov for at læse, hvad tyskerne skrev til hinanden. En fransk spion fik ved lidt af et tilfælde fat i håndbogen til Enigma, ud fra hvilken det var muligt at lave en præcis kopi af maskinen. Franskmændene brugte ikke ressourcer på at prøve at bryde tyskernes koder, men overgav derimod håndbogen til polakkerne, som gerne ville forberede sig på en fremtidig krig.

En hård nød

Historisk set havde kryptografi og kryptoanalyse været udført af sprogkyndige, men den øgede mekanisering fik Biuro Szyfrów

(det polske cifferbureau) til at satse på bl.a. matematikere, som kryptoanalytikere. Især den unge matematiker Marian Rejewski udviste stort talent for disciplinen. Hvor franskmændende havde opgivet at bryde koderne, havde polakkerne stadig truslen om et tysk angreb hængende over hovedet, hvilket motiverede dem til at forsøge at bryde Enigmakoden. Enigma var kort fortalt en mekanisering af ind- og udkodning af beskeder. Den bestod af et tastatur, et antal scramblere (tre i den oprindelige militære udgave af Enigma), en reflektor, et plugboard og en lampe for hvert bogstav. Hvis operatøren ville kode fx A, trykkede han på A-knappen, hvorefter der blev skabt forbindelse gennem plugboardet, ledningerne på scramblerne, hen til reflektoren, tilbage gennem scramblerne og hen til plugboard og op til en lampe, hvor operatøren kunne aflæse, hvad A skulle indkodes som. Ind- og udkodning var fuldstændig symmetriske processer, så når operatøren modtog et A og ville udkode det, trykkede han ligeledes på A. Hele pointen var, at man skulle kende de præcise indstillinger for at kunne udkode korrekt. Scramblerne var bevægelige og for hvert ind- eller udkodet bogstav rykkede den yderste sig ét hak. Når den yderste havde bevæget sig en hel omgang, rykkede den næste ét hak og så fremdeles. Dermed gav scramblerne i sig selv en polyalfabetisk substitutionskode med en periode på 17.576 (26^3), da der er 26 bogstaver i det tyske alfabet. Det vil kort sagt sige, at hvert 17.576. bogstav blev indkodet med samme ombytninger af bogstaver og derfor ville man kunne, hvis man havde nok materiale, samle de bogstaver der var indkodet med samme ombytning af bogstaver og anvende frekvensanalyse på hver af disse ombytninger af bogstaver. Frekvensanalyse er en metode, hvor man kigger på hvilke bogstaver (i kodeteksten) der fremgår flest gange og så anvender statistik over anvendelse af bogstaver i fx det tyske sprog for at gætte sig frem til, hvilke bogstaver

der er blev indkodet som hvad. Dette kan klart nok kun gøres, når man ved, at alle bogstaver, man betragter, er indkodet med samme substitutionsalfabet, hvorfor man først ville skulle opdele kodeteksten i 17.576 samlinger af bogstaver. Nu kan man jo så overveje, om FAMØS har brudt Enigma på en halv side, men tyskerne var jo ikke dummere end som så, så det var vanskeligere, end det er blevet gjort her. Plugboardets effekt er nemlig blevet glemt i det ovenstående. Plugboardet havde et hul til hvert bogstav og et antal kabler, som kunne forbinde disse huller. Dermed kunne der foretages et antal parvise ombytninger af bogstaver. I starten blev der anvendt seks kabler og dermed seks parvise ombytninger af bogstaver. For den overambitiøse FAMØS-redaktør er det et alvorligt problem, da vores fremgangsmåde med at betragte Enigma som en polyalfabetisk substitutionskode nu er mere eller mindre nytteløs. I stedet for at forsøge selv at arbejde videre med Enigma, så lad os se på, hvad andre kloge hoveder har gjort tidligere.

Polsk opfindsomhed og tysk naivitet

Den store udfordring for Biuro Szyfrów i tiden op til 2. verdenskrig var at adskille de forskellige komponenters virkning, som det også blev antydet herover. Hvis man kunne isolere plugboardets virkning, ville man faktisk bare have med parvise ombytninger af bogstaver at gøre. Hvis man kunne isolere scramblernes virkning, ville det være en svær, men overkommelig opgave at bryde koden. Marian Rejewski og hans kolleger begyndte derfor at studere strukturen i maskinens ind- og udkodning.

Tyskerne havde imidlertid selv indlagt en svaghed i deres brug af Enigma. Hver måned blev der til Enigmaoperatørerne distribueret en kodebog indeholdende en startindstilling for hver dag.

Denne startindstilling foreskrev altså, hvordan scramblerne skulle indstilles, scramblernes rækkefølge og hvilke bogstaver, der parvist skulle ombyttes. Tyskerne ønskede dog ikke at give deres fjender for mange beskeder, der var krypteret med samme nøgle, hvorfor de tyske operatører kun brugte dagsnøglen til at kryptere seks bogstaver i starten af hver besked. Disse seks bogstaver var faktisk de nye scramblerindstillinger, som resten af beskeden var indkodet med. Scramblerindstillinger udgjorde kun tre bogstaver, men for at sikre sig mod slåfejl valgte tyskerne at lade deres operatører gentage de tre bogstaver. Det var en fejl. Det var netop denne form for systematik og gentagelse, som Marian Rejewski og hans kolleger havde brug for. Når tyskerne fx startede en besked med PKHJOK vidste de polske kodebrydere, at 1. og 4., 2. og 5. samt 3. og 6 parvist var indkodninger af samme bogstav. Det er umiddelbart ikke meget at arbejde med, men polakkerne var ikke færdige med at få gode idéer. Nu begyndte et møjsommeligt arbejde. Hvis nemlig polakkerne havde nok beskeder fra samme dag (altså hvor de første seks bogstaver var indkodet med samme dagskode) kunne de betragte 1. og 4. bogstav i beskederne, hvor bogstaverne i 4. position var en permutation af bogstaverne i 1. position. Polakkerne brugte nu et år på at kortlægge, hvilke initialindstillinger af scramblerne (rækkefølge og orientering), der gav hvilke cykeltyper i disse permutationer. Der var 105.456 indstillinger, der skulle tjekkes. Til hvilken nytte, kunne man spørge. Hvordan skulle dette give dagskoden? Polakkerne lader til fuldstændig at have glemt, at der også er et plugboard, som bytter om på bogstaverne. Imidlertid ændrer disse ombytninger ikke cykeltypen af en given permutation. Denne erkendelse var et gennembrud. Nu kunne polakkerne med deres dugfriske katalog over hvilke scramblerindstillinger, der giver hvilke cykeltyper simpelthen analysere en given dagskode, finde dens cykeltype og derefter

slå op i kataloget, hvilke indstillinger, der giver netop sådan en cykeltype. Dette blev gjort for både 1. og 4., 2. og 5. samt 3. og 6. bogstav. Hermed var arbejdet ikke færdigt. Scramblerindstillinger kunne findes på denne måde, men man havde jo stadig set bort fra plugboardet, der jo byttede parvist om på et antal bogstaver. Inden krigen var dette antal 12, altså seks par. Biuro Szyfrów havde imidlertid også et svar på dette. De indstillede simpelthen en kopi af en Enigmamaskine med de fundne indstillinger. Derefter begyndte de at udkode teksten. Det blev for det meste noget volapyk, men indimellem kunne man genkende brudstykker af forståelig tekst. Disse brudstykker gav et fingerpeg om, hvilke bogstaver der var byttet om, og hvilke der ikke var. Ved på denne måde prøve sig lidt frem kunne polakker nå helt i mål, og de blev altså de første, der brød Enigma. Senere lavede Rejewski en mekanisering af processen med at finde scramblerindstillinger. Der var seks forskellige scramblerrækkefølger (3!), hvorfor seks maskiner blev opstillet til mekanisk at afprøve de 17.576 (26^3) forskellige scramblerindstillinger givet en rækkefølge af scramblerne. Disse maskiner blev kaldt bomber.

Invasionen af Polen

Polakkerne lagde en stor mængde arbejde for dagen af nødvendighed, kan man hævde. Krigstruslen var da også til at tage og føle på for polakkerne, men faktisk havde chefen for Biuro Szyfrów hele tiden haft de tyske dagskoder liggende på sit kontor, da en fransk spion havde været i stand til løbende at få fat på dem. Chefen for Biuro Szyfrów, major Langer, havde dog ment, at hans folk skulle trænes til den dag, hvor krigen brød ud, og det ikke længere ville være muligt at få fat i koderne. Set i det helt store historiske perspektiv må man sige, at det nok har været en god disposition, da

Biuro Szyfróws arbejde senere lagde grund for de britiske kryptoanalytikeres forsøg på at bryde Enigmakoden. Rejewskis anstrengelser betød desværre ikke meget for det praktiske forløb af Hitlers invasion af Polen. I 1938 fik alle Enigmaoperatører nemlig to nye scramblere. Nu skulle der pludselig bruges 60 bomber til at tjekke indstillingerne (nemlig (5*4*3)). Man indførte også fire ledninger mere i plugboardet så antallet af ombyttede bogstaver nu steg til hele 20. Den elegante polske fremgangsmåde var fuldstændig afhængig af den faktiske ledningsføring i Enigmamaskinerne, hvorfor selv små ændringer i anvendelsen eller opbygning af det tyske kodesystem betød, at de polske kryptoanalytikere var tilbage på bar bund. Desværre modtog Biuro Szyfrów nu heller ikke længere dagskoderne fra den fransk spion. Hele den tyske Blitzkrieg var ellers dybt afhængig af kommunikation for at koordinere de store og voldsomme angreb, men nu kunne polakkerne ikke længere følge med i denne kommunikation. Major Langer ville ikke lade sine folks arbejde gå til spilde, hvorfor han i 1939 inviterede franske og britiske kolleger til Polen, hvor han overdrog arbejdstegningerne til bomberne samt to Enigmamaskiner til dem. Kort efter blev Polen invaderet.

Kampen flyttes til de britiske øer

I Storbritannien var det Government Code and Cypher School i Bletchley Park, der havde forsøgt at dekryptere tyskernes kommunikation. Inden kontakten med de polske kolleger uden stor succes. Briterne byggede dog videre på de polske fremskridt, men med den indsigt, at kodebrydningen ideelt set ikke skulle afhænge af lavpraktiske omstændigheder som tyskernes indkodningsprocedurer samt ændringer i ledningsføring og lignende. Kodebrydningen skulle derimod afhænge af mere generelt anvendelige

fremgangsmåder. En af disse fremgangsmåder var at gætte et ord i klarteksten samt dets præcise placering. På den måde kunne man afprøve hvilke indstillinger, der ville give anledning til en given indkodning af et gættet ord. Dette kunne endda afprøves mekanisk med dertil indrettede maskiner. Igen var svaret på den tyske mekanisering af kryptering en mekanisering af kodebrydningen. Den kritiske læser vil nok studse over, hvorvidt det at gætte et ord samt dets placering i klarteksten (en såkaldt crib) er en overkommelig opgave. Imidlertid var kommunikationen i de tyske væbnede styrker naturligvis underlagt visse restriktive normer, hvilket gjorde denne kommunikation meget rutinepræget. Gentagelse er kryptoanalytikerens bedste ven, og netop denne tankeløse anvendelse af Enigma muliggjorde denne fremgangsmåde. Kommunikationen, der blev opsnappet, blev udsendt over radio, hvorfor den var let for de britiske lyttestationer at få fingre i. På den måde kunne briterne fx hver morgen opsnappe vejrmeldinger fra tyskerne. Igen vil den kritiske læser nok fare op af stolen og hævde, at briterne ville kunne kigge ud af vinduet, hvis de var interesseret i vejret. Imidlertid viste det sig at fx vejrmeldingerne var meget rutineprægede og ord som Wetter (tysk: vejr) indgik som oftest. Dermed kunne briterne bruge denne viden til at finde frem til dagskoden som senere kunne anvendes til at dekryptere mere interessant information. Turing og hans kolleger videreudviklede bomberne, så man mekanisk kunne finde frem til hvilke indstillinger meddelsen var indkodet med givet en crib. Hele fremgangsmåden var dybt afhængig af operativ efterretningsindhentning. Man havde simpelthen brug for at kende tyskernes procedurer så præcist som muligt. Man havde heldigvis succes med dristige operationer, hvor britiske flådefartøjer kaprede tyske skibe og u-både og fik fat i kodemateriale, inden skibene blev sænket.

Britiske efterretninger og tyske fodfejl

I 1941 havde Turing og hans kolleger udviklet de metoder, som sammen med det opsnappede kodemateriale i perioder muliggjorde dekryptering af store dele af den tyske flådes kommunikation. I starten blev den information anvendt forholdsvis naivt. Det udmøntede sig bl.a. i sænkningen af det tyske slagskib Bismarck, som sammen med en række andre vellykkede britiske flådeoperationer fik den tyske fjende til at overveje muligheden for at Storbritannien havde adgang til hemmelige oplysninger. Heldigvis for briterne var de tyske efterretningstjenester dog lige så naive, da de fuldstændig udelukkede muligheden for, at Enigma var blevet brudt. I stedet konkluderede de, at de britiske efterretningstjenester havde infilteret centrale dele af det tyske krigsapparat, og oplysningerne altså stammede derfra. Hvis tyskerne ikke havde haft denne naive tiltro til Enigmas fortræffeligheder, ville de fx have kunnet indføre dobbeltindkodning af alle meddelser, hvilket ville havde gjort Ultras (briternes kryptoanalystiske enhed) cribstrategi ubrugelig. Hvor den britiske side straks herefter indså, at oplysninger der stammede fra dekryptering af tyskerne kommunikation skulle anvendes med meget stor varsomhed, vedblev den tyske modpart med at forholde sig naivt til Enigma og dens formåen. I løbet af krigen steg Ultras kapacitet løbende og med tiden blev puljen af kryptoanalytikere fordelt mellem forskellige tyske kodesystemer. Turing blev sat til at arbejde med kryptoanalyse af den tyske flådes kommunikation, hvilket også var en af de stærkeste. Der var imidlertid også grene af den tyske værnemagt, hvis kommunikation aldrig blev mulig at læse for Ultra. I februar 1942 forbedrede den tyske flåde Enigmasystemet ved at indføre en fjerde scrambler i maskinen. Denne scrambler var ikke udskiftelig. Det første problem for Turing og hans kolleger var at

fastlægge ledningsføringen inden i denne nye scrambler. Igen var det tyske fodfejl, der gjorde det muligt. Siden 1941 havde denne fjerde scrambler nemlig siddet i en neutral position, altså uden at ændre krypteringsprocessen, i Enigmamaskinerne. I december 1941 havde en operatør ved en fejl indkodet en meddelelse med tre normale scramblere og denne fjerde scrambler, som af den ene eller anden årsag ikke havde siddet i en neutral position. Det blev opsnappet af Ultra, som jo ikke kendte til den fjerde scrambler og derfor ikke vidste, hvorfor de ikke kunne dechiffrere meddelelsen. Imidlertid indså operatøren fejlen og udsendte den præcis samme meddelelse, men nu korrekt krypteret altså uden brug af den fjerde scrambler. Denne meddelelse kunne Ultra godt dechifrere og ved at sammenligne de to meddelelser kunne Turing og hans kolleger nu fastlægge ledningsføringen i den fjerde scramber, så da den blev taget i brug, var de et skridt foran. Imidlertid gav den nye scrambler stadig 26 gange flere mulige indstillinger, som bomberne skulle kontrollere, når der var blevet gættet en crib. Det gav store problemer, da man simpelthen manglede kapacitet. Derfor blev 1942 et år med mange allierede tab i Atlanterhavet, da man ikke længere havde adgang til u-bådenes kommunikation, hvorfor man ikke kunne føre konvojerne uden om de jagende u-både. Hen mod slutningen fik den britiske kryptoanalyse dog igen vind i sejlene. Man kaprede nemlig en tysk u-båd, hvorved man fik adgang til de nye procedurer. Derudover begik tyskerne endnu en gang en fodfejl. De krypterede nemlig vejrmeldingerne med samme indstillinger som alle andre meddelelser, men med den fjerde scrambler i neutral position. Derved kunne Ultra igen finde cribs og bruge bomberne til at afprøve indstillingerne. Derefter manglede man kun at finde ud af hvordan det fjerde skulle indstilles, før man var klar til at udkode de tyske meddelelser. Dette var overkommeligt, da den fjerde scrambler kun kunne stilles i 26 forskellige

positioner. Dette nye gennembrud medførte, at de allierede igen kunne føre deres konvojer uden om de tyske u-både. Igen mente den tyske flåde, at forklaringen på de allieredes kendskab til tyske planer måtte stamme fra spionage og ikke fra udkodning af tyskernes egen kommunikation.

Indflydelsen på krigen

Hvis vi vender tilbage til vores udgangspunkt, nemlig diskussionen mellem kemikeren, fysikeren og matematikeren, så kan man med rette spørge sig selv, hvilken effekt de allieredes (amerikanere kom hen mod slutningen af krigen også ind over kryptoanalysen af tysk kommunikation) evne til at læse Værnemagtens kommunikation havde på udfaldet af krigen. Den slags kontrafaktiske overvejelser er selvfølgelig ligeså spændende, som de er spekulative. Det er blevet hævdet, at de allieredes overlegenhed på dette felt forkortede den europæiske krig med to år, da man simpelthen kunne opbygge kapacitet til invasionen af Frankrig hurtigere, når man til dels kunne føre sine konvojer uden om de glubske, tyske u-både. Det siger sig selv, at to år i bedste fald er et godt gæt og i værste fald bare et tal, men i diskussionen på Caféen, skal læseren selvfølgelig føle sig velkommen til at bruge tallet og citere Famøs som en pålidelig kilde. Derudover skal det også med rette nævnes at selvom Rejewski, Turing og deres kolleger ydede en heroisk og imponerede indsats, ville det ikke være gået uden hjælp fra tyskerne. Gang på gang brød de med alle kryptografiens helligste principper i en blind tiltro til Enigmasystemet. Efter krigen var hele Ultraprogrammet stadig mørklagt fra den britiske regerings side og offentligheden blev først oplyst om det i 70'erne. Briterne ønskede naturligvis ikke at afsløre at de kunne læse med i det meste, herunder naboernes interne post. Derfor fik disse

kodebrydende frihedskæmpere først oprejsning mange år senere. Mange af de lokale, der boede tæt på Bletchley Park, havde endda bemærket det besynderlige i, at den slags unge, våbenføre mænd ikke var ved fronten.

Turing fortsatte sit arbejde inden for forskellige felter, men kunne ikke længere sikkerhedsgodkendes til officielle formål, da han var homoseksuel, hvilket i efterkrigstidens bornerte Storbritannien var yderst mistænkeligt i regeringens øjne. I 1952 blev han arresteret for at have et homoseksuelt forhold. Som straf blev han idømt et års østrogenbehandlinger. Disse gjorde ham både overvægtig og impotent. I 1954 spiste han af et cyanidforgiftet æble, hvilket blev hans endeligt. Hans mor mente, at det var et uheld efter et amatøragtigt kemiforsøg, der havde efterladt rester af cyanid på hans fingre. Retsmedicineren, der undersøgte ham, konkluderede, at det var selvmord.

Litteratur

[1] Andrew Hodges. *Alan Turing: the Enigma*

[2] Richard Owen. *Why the Allies Won*

[3] Andrew Williams. *Slaget om Atlanten*

[4] Simon Singh. *Kodebogen*

[5] Famøs, *10. årgang, nr. 4, maj 1997, side 9 sætningen: Ultra*