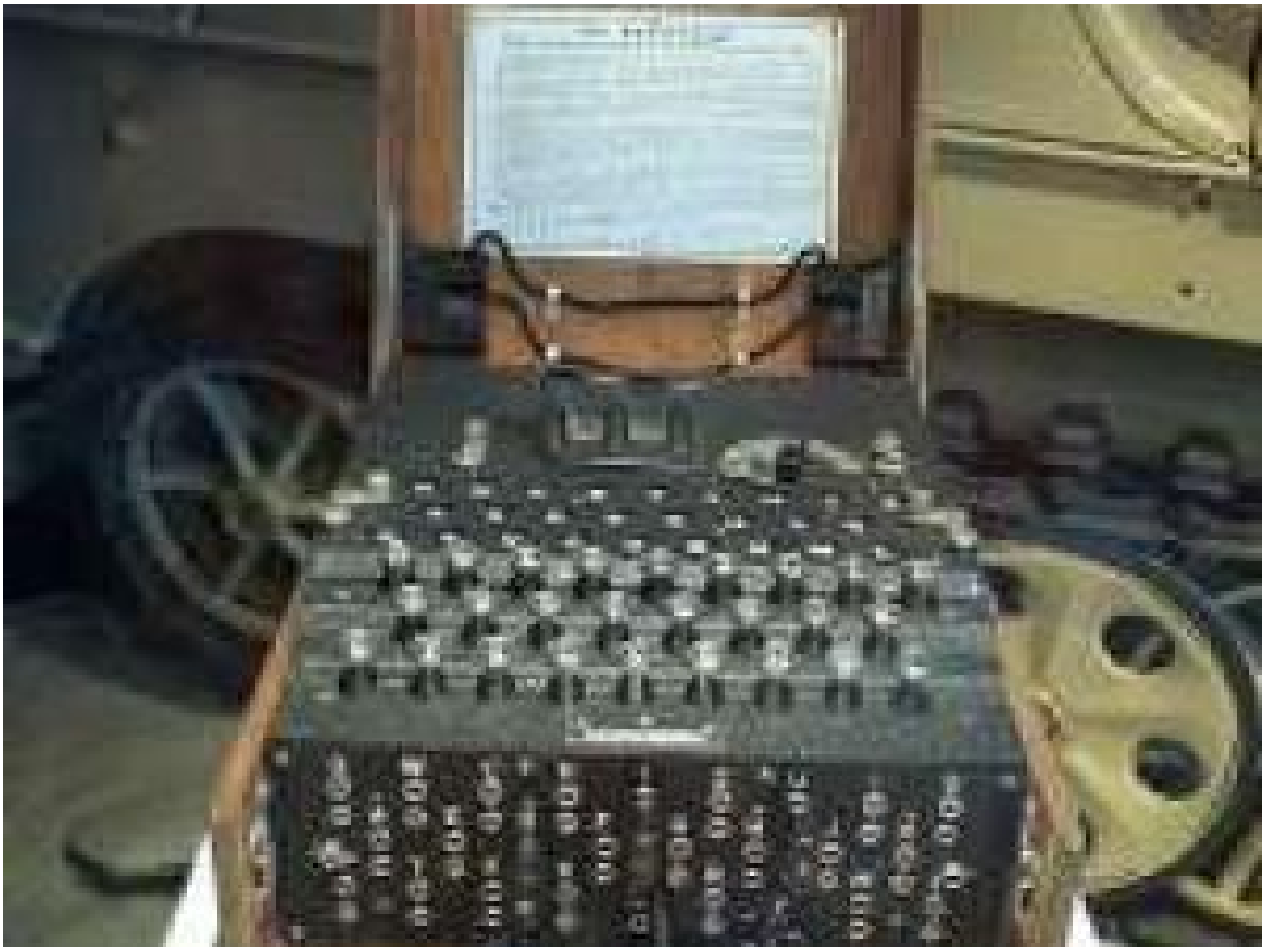
Krigen om koderne

Verdens første computer blev bygget til at bryde tyskernes Enigma-kode. Nutidens kryptologer bygger videre på principperne fra kodemaskinen fra 2. verdenskrig.



Enigmamaskinen var uhyre brugervenlig (Foto: NSA)

Charlotte Koldbye
Journalist

01 december 2008 HISTORIE IT KRIG & TERROR MATEMATIK OPFINDELSER SAMFUND

Når danske ingeniørstuderende på DTU skal lære om moderne kryptologi, så kan de hente inspiration i en lille transportabel kodemaskine fra 2. Verdenskrig.

Den tyske Enigma satte standarden for kodemaskiner, og den er et skoleeksempel på, at den part, der forstår at holde på sine hemmeligheder i en krig, er foran på point, mens den part, hvis hemmeligheder bliver afluret, er bagud.

Enigmamaskinen lignede en gammeldags skrivemaskine. Dens simplicitet og brugervenlighed gjorde, at det var muligt for enhver telegrafist at sende kodede meddelelser og modtage meddelelser i kode og afkode dem.

»De principper vi bruger i dag til kryptering er de samme som blev brugt til Enigmamaskinen. Der bruges blot endnu flere komponenter i nutidens kryptologi,« fortæller Lars Ramkilde Knudsen, der er professor på DTU Matematik.

»Det er jo også derfor, at vi har en enigmamaskine stående her ude på DTU. For at de studerende kan få lov til selv at få koden ind under fingrene.«

Fakta
Fakta +

Enigma var brugervenlig

Enigmamaskinen fungerede efter et uhyre simpelt princip. Man indstillede maskinen til en given kode ifølge en håndbog, hvor hver enkelt dag, havde sin egen kode. Så skrev man sin klartekst eksempelvis 'Ubåde ud for Anholt'.

Den besked blev af maskinen oversat til kryptotekst

:

'jfuhg mq slp rwmapo'. Telegrafisten kunne så sende beskeden afsted som almindelig morsekode, for selv om de allierede kunne opsnappe beskeden, havde de ingen jordisk chance for at forstå. Modtageren af beskeden satte sig så ned og indstillede sin Enigmamaskine til kode 915 og skrev kryptoteksten: 'jfuhg mq slp rwmapo'. Hvorefter man kunne læse klarteksten 'Ubåde ud for Anholt'.

Fakta
Fakta +

Enigmamaskinen fungerede altså både som en koder og en afkoder. Men den var oprindeligt slet ikke udviklet til militærhemmeligheder. Den var blevet udviklet knap 20 år tidligere til at udveksle fortrolige bankinformationer med, og den kunne købes af helt almindelige mennesker.

Men nu var 2. Verdenskrig i fuld gang og tyskerne brugte maskinen til at kommunikere helt uforstyrret, uden at de allierede forstod, hvad de talte om.

Station X

Den tyske kode måtte derfor brydes. Englænderne satte alt ind på det. Det engelske krigsministerium indrettede sig på et stort landsted med tilhørende landsby 80 km. uden for London.

Her på Station X, som stedet blev kaldt, kunne flere end 1.000 matematikere og ingeniører arbejde uforstyrret langt væk fra nysgerrige blikke og ikke mindst langt væk fra blitzen over London, bomberegnen, der hver nat hærgede London.

Fakta
Fakta +

Allerede inden 2.Verdenskrig brød ud, havde Polen formået at bryde en udgave af den tyske Enigma, og de havde bygget to polske udgaver af Enigmamaskinen. Da tyskerne invaderede Polen i efteråret 1939, blev Enigmakopierne i al hast hemmeligt bragt til London.

Verdens første computer brød koden

Krigsministeriet satte den brilliante matematiker Allan Turing til at lede opgaven. Han anses for at være grundlæggeren af computervidenskaben. Han konstruerede en stor maskine, som blev kaldt The Bombe Machine. I princippet var det 1.000 parallelle enigmamaskiner, der konstant stod og afprøvede mulige koder.

Den stod og kørte dag ud og dag ind og forsøgte at bryde koden. Ved hjælp af den kodede tekst og kvalificerede gæt fra englændernes side, kunne de i slutningen af krigen bryde tyskernes kode på 12 timer .

Med på en lytter

Fakta
Fakta +

I starten af 1940 fik englænderne fat på tyskernes kodebøger og andet materiale. Det var en stor hjælp til at afkode tyskerne meddelelser. »Hvis man skulle gå systematisk til værks så er der et hav af bogstavskombinationer. Og det vil tage en evighed at afprøve alle de muligheder. Så derfor benyttede man matematiske strukturer, for at indsnævre mulighederne for bogstavskombinationer,« fortæller Lars Ramkilde Knudsen.

Enigma havde desuden en lille medfødt fejl. Et bogstav kunne aldrig krypteres som sig selv. På den måde kunne man tage et element ud af ligningen, der skulle bryde tyskernes koder

»Det sjove er, man taler om Enigma og glemmer helt at både de allierede og japanerne også havde kodemaskiner, der faktisk var bedre end Enigma. Men den blev berømt, fordi man formåede at bryde koden. Man mener, at krigen blev forkortet med et år, fordi de allierede kunne lytte med på tyskernes kommunikation,« siger Lars Ramkilde Knudsen.

Moderne kryptering

Den amerikanske regering offentliggjorde i 2001 en krypteringsstandard, kaldet AES (Advanced Encryption Standard), som siden er taget i brug over hele verden. Enigmamaskinen krypterer et bogstav ad ganden, men i AES krypterer man 16 bogstaver ad gangen.

Bogstaverne sættes ind i en matrix med 4 rækker og 4 søjler. Bogstaverne krypteres herefter i alt 10 gange. En kryptering foregår på følgende måde. Først byttes hvert bogstav ud med et andet via opslag i en tabel.

Dernæst mikses de fire bogstaver i hver søjle, og til slut bytter man rundt på bogstaverne i hver række. Tabellen som benyttes er beregnet på forhånd ved hjælp af avanceret matematik. Mere præcist benytter man såkaldte multiplikative inverse i et endeligt legeme med 256 elementer.

Tabellen i AES regnes for at være den stærkest mulige af slagsen.

»Vi regner med at der vil gå ihvertifald 20 år før nogen vil være i nærheden af at knække AES,« fortæller Lars Ramkilde Knudsen, som selv var dybt involveret i udviklingen af standarden.

Kilder

- Bletchley Park hvor station X lå
- Wikipedia om Bletchley Park
- Codes and Ciphers om enigmamaskinen
- Dansk wikipedia om Enigma
- Mathematics Magazine: Artikel om de polske kodebrydere
- Centre for New Media: Billeder af enigmamaskinen

Videnskab.dk Podcast

Lyt til vores seneste podcasts herunder. Du kan også findes os i din podcast-app under navnet 'Videnskab.dk Podcast'.

Er du forsker?

KLIK HER

og meld dig til

Bestil en Forsker

FORSK NINGENS DØGN

Videnskabsbilleder

Se de flotteste forskningsfotos på vores Instagram-profil, og læs om det betagende billede af nordlys taget over Limfjorden her.

For at se dette billede fra Instagram skal du acceptere marketing-cookies.

Klik her for at ændre dit samtykke

Vis dette opslag på Instagram

» Et opslag delt af Videnskab.dk (@videnskabdk) «

Ny video fra Tjek

Tjek er en YouTube-kanal om videnskab henvendt til unge.

Indholdet på kanalen bliver produceret af Videnskab.dk's videojournalister med samme journalistiske arbejdsgange, som bliver anvendt på Videnskab.dk.

Hovsa! Her skulle en video ligge. Men da du ikke har accepteret marketing-cookies, som YouTube-afspilleren bruger, kan videoen ikke blive vist.

Klik her for at ændre dit samtykke

Hej! Vi vil gerne fortælle dig lidt om os selv

Nu hvor du er nået helt herned på vores hjemmeside, er det vist på tide, at vi introducerer os.

Vi hedder Videnskab.dk, kom til verden i 2008 og er siden vokset til at blive Danmarks største videnskabsmedie med omkring en million brugere om måneden.

Vores uafhængige redaktion leverer dagligt gratis forskningsnyheder og andet prisvindende indhold, der med solidt afsæt i videnskabens verden forsøger at give dig aha-oplevelser og væbne dig mod misinformation.

Vores journalister fortæller historier om både kultur, astronomi, sundhed, klima, filosofi og al anden god videnskab indimellem - i form af artikler, podcasts, YouTube-videoer og indhold på sociale medier.

Vi stiller meget høje krav til, hvordan vi finder og laver vores historier. Vi har lavet et manifest med gode råd til at finde troværdig information, og vi modtog i 2021 en fornem pris for vores guide til god, kritisk videnskabsjournalistik.

Vores redaktion gør en dyd ud af at få uafhængige forskere til at bedømme betydningen af nye studier, og alle interviewede forskere citat- og faktatjekker vores artikler før publicering.

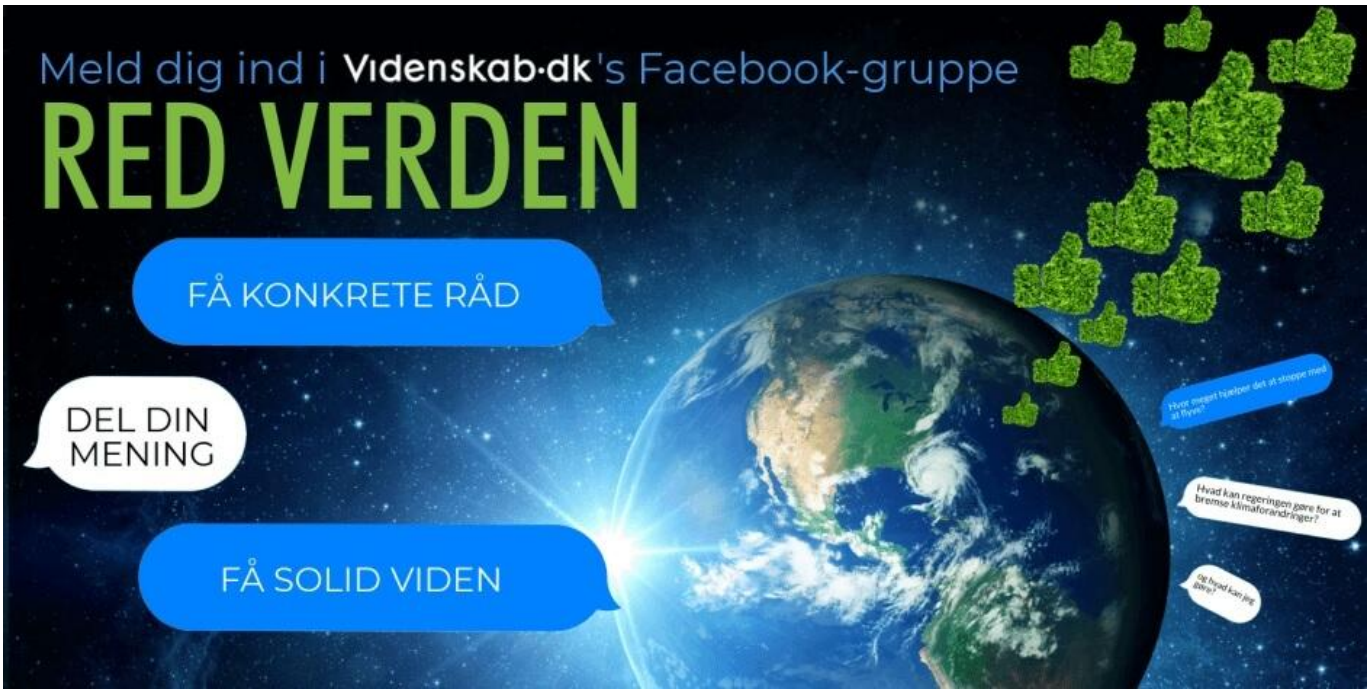
Hvis du går rundt og undrer dig over stort eller småt, vil vi elske at høre fra dig og forsøge at give dig svar med forskernes hjælp. Send bare dit spørgsmål til vores brevkasse Spørg Videnskaben.

Vi håber, at du vil følge med i forskningens forunderlige opdagelser her på Videnskab.dk.

Få et af vores gratis nyhedsbreve sendt til din indbakke. Du kan også følge os på sociale medier: Facebook, Twitter, Instagram, YouTube eller LinkedIn.

Med venlig hilsen

Videnskab.dk


Meld dig ind i Videnskab·dk's Facebook-gruppe
RED VERDEN
FÅ KONKRETE RÅD
DEL DIN MENING
FÅ SOLID VIDEN
Hvor meget hjælper det at stoppe med at flyve?
Hvad kan regeringen gøre for at bremse klimaforandringer?
Og hvad kan jeg gøre?