ENIGMA

STUDIERETNINGSPROJEKT

Odense Tekniske Gymnasium 3.I

Vejleder: Steen Heide (sth)
&
Vejleder: Ole Torsten Sørensen (os)

21/12/2016

Enigma

Abstract

This paper examines the combinatorics that is attached to Enigma, and the structure of the Enigma-machine. The paper takes a look into Enigma's part in World War 2, were it also explains what the decryption of Enigma meant for the war. The assignment examines what a permutation is, and how it is used. This paper also examines the differences between Enigma and RSA, where it is evaluated who uses encryption and against whom. Through an examination of the structure of the Enigma-machine and calculation on the combinatorics, the study shows that the Enigma-machine can be adjusted in 158.962.555.217.826.360.000 different ways. An examination of Enigma's part in World War 2, and an impact assessment for what the decryption of Enigma meant for the war, after the decryption, it shows that Enigma eventually was to more use for Great Britain than it was for Germany. It states that the idea behind Enigma is, that it can swap letters, which is called a permutation. It also states how to calculate possible numbers of permutations. The differences between Enigma and RSA states that RSA is much harder to decrypt nowadays compared to Enigma was during World War 2. Through an evaluation of who uses encryption and against whom, it states that civilians and companies use cryptosystems like RAS to protect themselves against organizations like FBI and NSA. The conclusion of this study is that even Enigma could be adjusted in 158.962.555.217.826.360.000 different ways, the code could still be solved. And that encryption and decryption has its consequences.

Indholdsfortegnelse

Indledning

Enigma-maskinen blev brugt af Tyskland under 2. verdenskrig til at kryptere hemmelige beskeder. Det var gældende for tyskerne, at Enigma ikke blev knækket. Derfor var antallet af mulige måder, man kunne indstille maskinen på utrolig stort. Tyskerne stolede derfor blindt på, at Enigma ikke kunne knækkes. Tilliden til maskinen, kom dog til at koste dem dyrt i sidste ende. Indholdet af disse beskeder kunne nemlig være afgørende for krigens forløb. Derfor satte Storbritannien et stort hold af matematikkere af til at knække Enigma.

I denne opgave starter jeg med at give en grundig redegørelsen for Enigma-maskinens opbygning og den kombinatorik, der tilknytter sig systemet. Efterfølgende vil jeg kort redegøre for Enigmas rolle i 2. Verdenskrig, hvor jeg vil fortage en konsekvensvurdering, af hvad dekrypteringen af Enigma betød for krigen. Ideen bag Enigma er, at man kan bytte rundt på bogstaver. Det kaldes en permutation. Jeg vil definere, hvad man forstår ved en permutation, og udlede nogle resultater for permutationer og sammensætningen af permutationer. Til sidst i opgaven vil jeg perspektivere

Enigma til RSA, som er et nutidigt kryptosystem, og herunder vurdere, hvem der anvender kryptering i moderne IT kommunikation og mod hvem.

Sådan virker Enigma

I følgende afsnit vil jeg redegøre for opbygningen af Enigma-maskinen og den kombinatorik, som knytter sig til systemet. For at kunne forstå Enigma-maskinen, vil jeg forklare, hvilken funktion den enkelte del i Enigma har, og hvor mange mulige kombinationer den kan indstilles.

Inden redegørelsen er det vigtigt at pointere, at jeg tager udgangspunk i den Enigma-maskine med plads til tre rotorer. På bilag 1 ses Enigma-maskinen uden dækkepladen, så man bedre kan se rotorerne. Som der fremgår på bilaget består Enigma-maskinen af et tastatur, en koblingstavle også kaldt plugboard, tre rotorer navngivet en scramblerenhed, en lampeplade, en reflektor og en kodebod. Kodebogen forekommer ikke på bilag 1.

Inden vi kigger på hvordan hver del virker, giver jeg en kort beskrivelse på krypteringsprocessen. For at kryptere et bogstav, fx s, skal man først indstille koblingstavlen og scramblerenheden efter kodebogens instrukser. Når det er gjort, kan man derefter indtaste s på tastaturet, hvor s'et bliver sendt til koblingstavlen via en ledning, derefter videre til rotorerne, hvor den fortsætter ind i reflektoren, som sender den en anden vej tilbage igennem rotorerne og koblingstavlen, hvorefter den så slutter ved lampepladen, hvor man kan se, hvad s er blevet krypteret til. Operatøren sender derefter bogstavet videre til modtageren, hvor han kan indtaste bogstavet på sin Enigma-maskine, hvor han så vil få s'et til at lyse op på pladen, hvis maskinen er indstillet rigtigt.[1]
På bilag 2 fremgår kredsløbet som et diagram.

Alle delene i Enigma-maskinen har hver sin funktion, som var med til at gøre Enigma næsten udbrydelig. Jeg vil nu gennemgå alle delene, og hvilken funktion de bidrager med.

[1] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)

Tastatur (se bilag 3)

Tastaturet er et alment tastatur fra en skrivemaskine. Her indtastes bogstavet, der derefter bliver sendt til koblingstavlen via en ledning[2].

Koblingstavle/plugboard (se bilag 4)

Med koblingstavlen kan man bytte om på bogstaverne ved at tilkoble ledninger fra bogstav til bogstav. På plugboardet er der 26 bogstaver, ligesom der er på tastaturet, derfor er det muligt at anvende op til 13 ledninger til at bytte rundt på bogstaverne. Det betyder derimod ikke, at det er optimalt at bruge alle 13 ledninger[3] [4]. For at gøre rede for antallet af mulige kombinationer som koblingstavlen gøre gavn med anvendes fakultetsfunktionen. Fakultetsfunktionen går ud på, at man må gange et tal med det tal, som er mindre end det forrige hver gang[5] (se bilag 5).
Det optimale brug af ledninger er 11, tyskerne anvendte dog kun 10 ledninger under krigen[6]. Jeg vil finde frem til antallet af mulige kombinationer, som koblingstavlen kunne indstilles på, når der bliver brugt 10 ledninger som tyskerne brugte, samt se hvad sandsynligheden for at lave den rigtige kombination med 11 ledninger er. Derefter vil jeg gennemgå formlen, hvor man indtaster antallet af ledninger, hvorved man får et antal af kombinationer, som vil forekommer ved præcis det antal brugte ledninger. Samt vil jeg påvise, hvor mange forskellige måder koblingstavlen vil kunne indstilles, hvis antallet af ledninger ikke var opgivet.

Den ene ende af den første ledning kan sættes i 26 forskellige bogstaver, den anden ende af ledningen kan derfor kun blive sat i 25 forskellige bogstaver. Mønstret fortsætter indtil man i princippet står med den 13 lednings anden ende og kun har et bogstav tilbage at vælge i mellem. Det er det samme som at skrive $26 \cdot 25 \cdot \ldots \cdot 2 \cdot 1$, det kan omskrives ved brug af

---

[2] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog).
[3] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)
[4] Vestergaards MATEMATIK SIDER: ENIGMA.
Internetadresse: http://www.matematiksider.dk/enigma.html#how_enigma_works - (Internet)
[5] Webmatematik: Fakultetsfunktionen. Udgivet af Matematikcenter.
Internetadresse: http://www.webmatematik.dk/lektioner/matematik-b/sandsynlighed-og-kombinatorik/fakultetsfunktionen - (Internet)
[6] Crypto Museum: Enigma. Udgivet af Cryptomuseum.com.
Internetadresse: http://www.cryptomuseum.com/crypto/enigma/working.htm - (Internet)

fakultetsfunktionen[7](se bilag 5). Omskrivningen gør at man nu kan skrive 26!. Det er dog ikke alle 26 bogstaver tyskerne brugte, de brugte kun 20 af dem. Derfor skal jeg dividere med 6!. Ligningen hedder nu $\frac{26!}{6!}$. Når en tysker satte en ledning i Enigma-maskinen, havde det ikke nogle betydning, om han satte ledning 1 i a og b, eller han satte ledning 2 i a og b. Resultatet ville være det samme. Tyskerne tilsluttede 10 ledninger, derfor skal jeg dividere med 10!. Det skrives på ligningen $\frac{26!}{6!\cdot 10!}$. Der skal divideres med yderlige 2^{10}, fordi det ikke betød noget hvilken ende, der blev sat i først. Hvis man satte en ledning i a og b, ville der ikke kun stå a og b, der ville også stå b og a. Ledningen ville kunne gå begge veje. Derfor ville det ikke betyde noget, om det var et a som skulle blive et b, eller et b som skulle blive et a. Når det er med, hedder ligningen $\frac{26!}{6!\cdot 10!\cdot 2^{10}}$. Nu har vi altså ligningen, som viser hvor mange kombination, man kan sætte 10 ledninger ind i koblingstavlen. Dvs. at det kan gøres på $\frac{26!}{6!\cdot 10!\cdot 2^{10}} = 150.738.274.937.250$ måder[8]. Som nævnt ville det optimale brug af ledninger være 11. Det kan vises ved brug af samme metode som ved 10 ledninger. Der er 26 bogstaver, 4 af bogstaverne skal ikke udfyldes med ledninger, derfor ser ligning og resultat således ud, $\frac{26!}{4!\cdot 11!\cdot 2^{11}} = 205.552.193.096.250$. Det ville altså have givet flere forskellige kombinationer, hvis tyskerne havde brugt 11 ledninger i stedet for 10. Det skal dog siges, at når man er oppe i sådan en mængde forskellige kombinationer, har det ikke den store betydning om der er ca. 55.000.000.000.000 flere muligheder.

Metoden jeg fandt antallet af kombinationer af henholdsvis 10 og 11 ledninger, kan også bruges til at finde antallet af kombinationer af 0 til 13 ledninger. For at gøre det mere overskueligt, kan metoden skrives, som følgende formel $\frac{26!}{(26-2n)!\cdot n!\cdot 2^n}$. I ligningen står n for antallet af ledninger[9]. Den øverste del af formlen, (26!), beskriver antallet af mulige bogstaver, hvor man kan placere ledningerne, når man skal udfylde alle hullerne en for en. Første del en den nederste del, $26 - 2n$, viser, at man skal trække 26 fra antallet af ledning ender, der er to ender pr. ledning, derfor skrives der $2 \cdot n$. Det sidste i formlen fremstilles som 2^n. For den del gælder det, at skal dividere med 2^n

[7] Webmatematik: Fakultetsfunktionen. Udgivet af Matematikcenter. Internetadresse: http://www.webmatematik.dk/lektioner/matematik-b/sandsynlighed-og-kombinatorik/fakultetsfunktionen - (Internet)
[8] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)
[9] Crypto Museum: Enigma. Udgivet af Cryptomuseum.com. Internetadresse: http://www.cryptomuseum.com/crypto/enigma/working.htm - (Internet)

for hver ledning. Man skal dividere med 2^n, fordi det er ligegyldigt, om man sætter ledningen i a og b eller b og a, ledningen kan altså gå begge veje. Som det forekommer i beskrivelsen af formlen, er det præcis det samme der sker, som da jeg selv fandt antallet af kombinationer for 10 og 11 ledninger. Med formlen kan man finde antallet af kombinationer, når n er antal ledninger. Hvis man derimod ikke ved hvor mange ledninger, der er tilkoblet koblingstavlen, vil antallet af forskellige kombinationer være endnu større[10]. På bilag 6 ses en tabel over antallet af kombinationer ud fra antallet af brugte ledninger, samt et eksempel med brug af formlen. I tabellen fremgår det også, at det største antal af mulige kombinationer er ved brug af 11 ledninger. Som nævnt vil antallet af kombinationer være større, hvis man ikke ved hvor mange ledninger, der er i brug. For at komme frem til antallet af mulige kombinationer, skal jeg bruge additionsprincippet[11]. Additionsprincippet går ud på, at man skal finde antallet af mulige kombinationer for enten opgave 1 eller opgave 2. Her skal jeg finde antallet af mulige kombinationer for enten 0 eller 1 eller 2… eller 12 eller 13 ledninger. Det gælder derfor om, at lægge antallet af mulige kombinationer for hvert antal brugte ledning sammen. Lagt sammen vil antallet af mulige kombinationer, når man ikke kender antallet af brugte ledninger, være $\sum_{n=0}^{13} \frac{26!}{(26-2n)!\cdot n!\cdot 2^n}$ =532.985.208.200.576. Som nævnt tidligere brugte tyskerne præcis 10 ledninger, når de indstillede koblingstavlen, derfor skulle briterne kun regne med 150.738.274.937.250 forskellige kombinationer.

Scramblerenheden (se bilag 7)

Man kan dele scramblerenheden op i to dele. Den ene del består af placeringen af rotorerne, den anden del består af rotorernes indstilling, hvilket bogstav der vender op.

Scramblerenheden består af 3 hjul, navngivet rotorer. Til hver Enigma-maskine er der 5 rotorer, derfor skulle man vide hvilke 3, man skulle bruge til givende dag. Der er altså flere muligheder for, hvordan hjulene skal stå. For at bestemme hvor mange kombinationer rotorerne kan stå, skal jeg bruge multiplikations princippet[12]. Multiplikations princippet går ud på følgende, hvis opgave P_1 kan løses på m antal måder, og opgave Q_1 kan løses på n antal måder, så kan opgaven P_1 og P_2 udføres på $m \cdot n$ antal måder. Jeg bruger nu multiplikations princippet til at finde antallet af

[10] Bauer, Craig P.: Secret History The story Of Cryptology. 1. udg. CRC Press, 2013. (Bog)
[11] Webmatematik: Multiplikations- og additionsprincipperne. Udgivet af Matematikcenter. Internetadresse: http://www.webmatematik.dk/lektioner/matematik-b/sandsynlighed-og-kombinatorik/multiplikations-og-additionsprincipperne - (Internet)
[12] Borch, Tommy og Helle Nørbjerg: Sandsynlighedsregning og statestik. Side 47-57. 1. udg. FAG, 1989. (Bog)

kombinationer rotorerne kan stå. Da der er 5 rotorer, udvælges en af de 5 rotor til det første. Den næste rotor kan derfor vælges ud fra 4, og den sidste rotor ud fra de resterende 3 rotorer. I alt er der altså $5 \cdot 4 \cdot 3 = 60$ måder man kan vælge hvilke rotorer man skal bruge[13].

Inde i hver rotor er der et ledningsnet (se bilag 8), som bytter om på bogstaverne. Dvs. hvis det var et s som kom ind i roter 1, vil det ikke være et s som kom ud af den igen. Hver gang man trykker på et nyt bogstav på tastaturet, ville rotor 1 rykke sig et hak. Hver rotor kan rykke sig 26 gange, lige som antallet af bogstaver på tastaturet, før det starter forfra. Når rotor 1 har roteret en hel omgang, altså 26 hak, ville rotor 2 rykke sig et hak. Samme regel gælder for rotor 3. Når roter 2 havde roteret en hel omgang vil rotor 3 rykke et hak. For at gætte hvordan rotorerne skal indstilles, altså hvilket bogstav som skal være øverst (se bilag 9), skal man ramme et tal ud af 17.576 muligheder. Det kan forklares således. Man skal først få rotor 1 til at stå korrekt, der er 26 forskellige bogstaver, altså 26 forskellige muligheder. Derefter skal rotor 2 indstilles korrekt, det er yderlige 26 muligheder. Dvs. at der nu er $26^2 = 676$ muligheder for at få 2 rotorer til at stå korrekt. Hvis man får de to rotor til at stå korrekt ud af 676 forskellige kombinationer, skal man have den tredje og sidste rotor til at være indstillet rigtigt. Igen er der 26 mulige bogstaver at vælge imellem. Dvs. at der er $26^3 = 17.576$ forskellige kombinationer de tre bogstaver kan stå i forhold til hinanden. Det vil også sige, der skal trykkes 17.576 gange på tastaturet, før den tredje rotor har drejet en hel omgang.

Når scramblerenheden skal indstilles, skal man udvælge de tre rotorer og deres indstillinger. Man kan derfor sætte scramblerenheden op på $60 \cdot 17.576 = 1.054.560$ forskellige måder[14].

Reflektoren (se bilag 10).

Efter den sidste rotor går bogstavet ind i reflektoren. Her bliver antallet af kryptoalfabeter ikke forøget, bogstavet bliver blot sendt retur, dog ikke samme vej, som det kom ind. Inde i reflektoren er der et ledningsnet, ligesom der er i rotorerne, hvor hver ende af ledningerne blot er i samme side på reflektoren (se bilag 10). Reflektoren sender nemlig ikke bogstavet den samme ved tilbage, som det kom fra i det tredje hjul. Derfor vil det bogstav som blev trykket ind på tastaturet, aldrig være det samme som det der lyser op på lampepladen. Det smarte ved reflektoren er, at den gør det

[13] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)
[14] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)

muligt at dekryptere den krypterede besked, som er tilsendt en[15]. Et eksempel kunne værre, hvis jeg ville kryptere ost. Jeg skriver ost ind på tastaturet, hvor efter Enigma-maskinen kryptere det til f.eks. jdp. Jeg sender nu beskeden af sted til en allierede, hvor han så skriver den krypterede besked, jdp, ind på sin Enigma-maskine og får ost til at lyse op på lampepladen. Det vil altså sige, at maskinen kan gå begge veje. Hvis man fjernede reflektoren ville Enigma-maskinen kun kunne kryptere beskeder. Så ville bogstavet gå direkte fra 3. rotor til lampepladen, den ville altså mangle tilbagevejen. Uden tilbagevejen ville man få et helt nyt bogstav, når man prøvede at dekryptere det givet bogstav. Så reflektorens funktion er derfor, at sende bogstavet tilbage igennem maskinen igen.

Lampepladen (se bilag 11).

Lampepladens funktion er at lyse det krypterede bogstav op.

Kodebogen (bilag 12)

Som nævnt følger der en kodebog[16] med til Enigma-maskinen. Kodebogen indeholder 28 nøgler, en nøgle til hver dag i 4 uger. Hver dag skulle tyskerne derfor indstille Enigma-maskinen på ny. Hvis det skulle lykkes for fjenden, at løse Enigma-koden den ene dag, skulle de starte helt forfra den næste. Som ses på bilag 12, står der skrevet dato, rækkefølgen på rotorerne, hvilket tal der skulle vende opad på rotorerne (bogstaverne kan skrives som tal fra 1-26), hvilke bogstaver de 10 ledninger skulle sidde i, og hvilken afdeling koderne var til, fx om det var til en afdeling i flåden eller en afdeling i luften. Hvis man altså havde en kodebog og en Enigma-maskine, ville man nemt kunne dekryptere Enigma-koderne. Derfor var der også meget sikkerhed omkring kodebøgerne. Flåden kunne fx få kodebøger med vandopløseligt blæk og vandsugende papir[17]. Hvis der skulle gå noget galt, kunne de smide kodebogen i vandet, og den ville blive ulæselig. Det var altså afgørende for tyskerne, at kodebogen blev inde for det tyske militær.

Antal indstillinger

Til sidst i redegørelsen af Enigma vil jeg beregne antallet af mulige kombinationer, der er for at indstille maskinen korrekt uden kodebogen. Scramblerenheden kan indstilles på 1.054.560 forskellige måder, koblingstavlen med 10 ledninger i brug kan indstilles på 150.738.274.937.250 måder. Derfor vil antallet af mulige måder, tyskerne kunne indstille Enigma-maskinen på være

[15] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)
[16] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)
[17] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)

følgende: $1.054.560 \cdot 150.738.274.937.250 = 158.962.555.217.826.360.000$. For at kunne forstå antallet af kombinationer bedre, skal man forstille sig, at man laver 1 million kombinationer i sekundet. Hvis man gør det, vil det tage ca. $5{,}04 \cdot 10^6$ år at gennemgå alle måderne Enigma-maskinen kan indstilles[18].

Enigmas rolle i 2. verdenskrig

I dette afsnit redegøres der kort for Enigmas rolle i 2. verdenskrig. Samt foretages en teknologivurdering som konsekvensvurdering[19], af hvad dekrypteringen af Enigma koden betød for krigen. Hvor jeg dog vil undlade af komme ind på teknikken, da det er gjort tidligere i opgaven.

Enigmas rolle i 2. verdenskrig var, for tyskerne, at være i stand til at sende beskeder, uden fjenden kunne forstå dem. Beskederne kunne indeholde informationer lige fra dagens vejrudsigten til en kamphandling[20]. Det gjorde det umuligt for fjenden at kende tid og sted for næste angreb. Som nævnt tidligere havde det ikke nogen betydning om fjenden havde en Enigma-maskine eller ej, for uden den månedlige kodebog ville beskederne ikke kunne dekrypteres. Derfor var det alt afgørende for tyskerne, at fjenden ikke fik fat i en kodebog. Enigmas rolle for tyskerne var derfor, at gøre kommunikation ufarlig. Det var dog kun i de begyndelsen, at Enigma var en fordel for tyskerne. Storbritannien lagde nemlig stor vægt på at knække Enigma. Det lykkes dem også, takket være et stort hold matematikkere, men især pga. en ung matematikker, Alan Turing[21], og hans Turingmaskine[22]. Det var derefter afgørende, hvad de gjorde, nu hvor de var i stand til at dekryptere tyskernes beskeder. Hvis de stoppede alle angrebene, ville tyskerne vide, at Enigma var knækket. De stod altså overfor et dilemma efter det andet hver dag. Skulle der redes en allieret ubåde, men dermed risikere at tyskerne ville stoppe med at bruge Enigma. Skulle de lade en konvoj[23] med

[18] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)
[19] Systime: 1.4. Teknologivurdering. Udgivet af Systime.
Internetadresse: https://teknologi.systime.dk/index.php?id=471 - (Internet)
[20] Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)
[21] Wikipedia: Alan Turing. Udgivet af Wikipedia.
Internetadresse: https://da.wikipedia.org/wiki/Alan_Turing - (Internet)
[22] Wolftram Math World: Turing machine. Udgivet af Wolftram.
Internetadresse: http://mathworld.wolfram.com/TuringMachine.html - (Internet)
[23] Wikipedia: Konvoj. Udgivet af Wikipedia.
Internetadresse: https://da.wikipedia.org/wiki/Konvoj - Besøgt (Internet)

mange bemandede skibe sinke, for at kunne skyde en af tyskernes Milk cows[24] i sænk. Selvom dilemmaerne var mange og hårde, gjorde dette det muligt for briterne at vinde krigen. Rollen Enigma derfor spillede for Storbritannien under krigen, omhandlede først og fremmest at knække Enigma, og derefter hvad man skulle stille op med dekrypteringerne, så Tyskland ikke vidste, at Enigma var knækket.

Konsekvensvurderingen

For at kunne vurdere, hvad dekrypteringen af Enigma betød for krigen, vil jeg starte med at tage udgangspunkt i, hvilke konsekvenser Enigma havde for Tyskland. Jeg stiller mig i tidspunktet, hvor Enigma blev introduceret for de tyske tropper i krigen og kigger på konsekvenserne. Jeg opstiller konsekvenserne i punktform.

- De kunne udsende radiosignaler, som alle kunne modtage, men kun selv forstå.
- For at forstå beskederne krævede det, at modtager havde en Enigma-maskinen selv samt månedens kodebog.
- Der skulle fremstilles Enigma-maskiner til alle, som skulle modtage signalet.
- Hver måned skulle man have en ny kodebog, for at kunne indstille maskinen korrekt.
- De kunne kommunikere frit omkring næste operation.
- Enigma-koden er umulig for fjenden at knække.

Tyskland stod overfor overstående konsekvenser, da de blev introduceret for Enigma i 2. verdenskrig. For at få et overblik over heldige og uheldige konsekvenser, opstiller jeg dem i nedstående skema.

[24] Wikipedia: German Type XIV submarine. Udgivet af Wikipedia. Internetadresse: https://en.wikipedia.org/wiki/German_Type_XIV_submarine - Besøgt d. (Internet)

Heldige konsekvenser	Uheldige konsekvenser
De kunne udsende radiosignaler, som alle kunne modtage, men kun selv forstå.	For at forstå beskederne krævede det, at modtager havde en Enigma-maskinen selv samt månedens kodebog.
De kunne kommunikere frit omkring næste operation.	Der skulle fremstilles Enigma-maskiner til alle, som skulle modtage signalet.
Enigma-koden er umulig for fjenden at knække.	Hver måned skulle man have en ny kodebog, for at kunne indstille maskinen korrekt.

For Storbritannien så konsekvenserne anderledes ud i starten af krigen, for deres job var at knække koden. Derfor vil jeg også kigge på konsekvenserne Enigma havde for Storbritannien i starten af krigen. Igen bliver konsekvenserne skrevet i punktform.

- De var ikke i stand til at forstå tyskernes beskeder.
- De skulle sætte et stort antal ressourcer af til at arbejde på løsningen.
- De kunne ikke hindre uforudsete angreb.

Alle de overstående konsekvenser er uheldige. Enigma gjorde altså, at tyskerne havde en stor fordel i starten af krigen. Det blev dog ikke ved, konsekvenserne for Storbritannien ændrede sig nemlig, da de løste koden. De ændrede sig fra overstående konsekvenser til nedstående konsekvenser.

- De kunne forstå tyskernes beskeder.
- De kunne stoppe tyske operationer, som kunne have stor påvirkning for krigens gang.
- Det måtte ikke komme ud, at de kunne dekryptere beskederne, derfor var de tvunget til at lade egne soldater og civile dø.
- Der var store dilemmaer, der skulle tages stilling til.

Jeg skriver dem op i heldige og uheldige konsekvenser.

Heldige konsekvenser	Uheldige konsekvenser
De kunne forstå tyskernes beskeder.	Det måtte ikke komme ud, at de kunne dekryptere beskederne, derfor var de tvunget til at lade egne soldater og civile dø.
De kunne stoppe tyske operationer, som kunne have stor påvirkning for krigens gang.	Der var store dilemmaer, der skulle tages stilling til.

Briterne var så gode til at holde det hemmeligt, at de havde knækket Enigma, at konsekvenserne ikke ændrede sig fra tyskernes synspunkt. Tyskland mente stadig, at Enigma ikke kunne knækkes. Grunden til at Storbritannien kunne holde det hemmeligt, var fordi de traf nogen valg, som betød tab for dem selv. Hvis de valgte at reagere på alle beskederne, ville der være en risiko for, at tyskerne vidste, at Enigma var knækket, og de ville dermed stoppe med at bruge den. Hvis tyskerne stoppede med at bruge Enigma, ville både tyskernes og briternes konsekvenser ændre sig igen. Derfor var Storbritannien også klar til at gøre, hvad der var nødvendigt for at holde det hemmelig.

Permutationer

Ideen bag Enigma er, at man kan bytte rundt på bogstaver, altså et e kan blive til et k som bliver til et t. Det kaldes en permutation. Permutation er derfor et vigtigt begreb, når man snakker om Enigma. Man kan definere en permutation som følgende. En permutation er en afbildning, hvor der byttes ud på elementerne i en givende mængde[25]. For at forstå det bedre opstiller jeg et eksempel. Eks 1: En given mænge $A = \{a, b, c, d, e, f, g\}$(A=mængde), hvor der sket en permutation, kan se således ud$\begin{pmatrix} a, b, c, d, e, f, g \\ d, a, e, b, f, g, c \end{pmatrix}$. Det er en permutation som sender $a \to d, b \to a, c \to e, d \to b, e \to f, f \to g \; og \; g \to c$. Man skriver en permutation op som en permutations cykel. Når man laver en cykel er princippet, at man altid kommer tilbage til udgangspunktet. Overstående permutation kan skrives som følgende $A = (adb)(cefg)$, den består af en 3-cykel og en 4-cykel. Denne permutation viser, bogstavet a bliver til d, d bliver til b, og b går tilbage til at blive a, og at c bliver til e, som bliver til f, der bliver til g, og g bliver til c igen. Det går altså i ring for hver del. Når man er tilbage til udgangspunkt, ligesom da b blev til a, lukker man parentesen, og starter med det næste bogstav i rækken, som ikke er brugt endnu (se bilag 13). I Enigma skete der mange permutationer, før et bogstav lyste op på lampepladen. Det skete i koblingstavlen, scramblerenheden, og reflektoren. Derfor skal man altså kunne sammensætte permutationer til en endelig løsning. Jeg fortsætter på eks.1, hvor jeg skal sammensætte cykel permutationerne $A = (adb)(cef)$ med $B = (ag)(be)(cfd)$. Jeg skal altså finde AB permutation. Jeg skriver A og B op ved siden af hinanden.

[25] Vestergaards MATEMATIK SIDER: ENIGMA - matematikken bag løsningen af Enigma. Udgivet af MATEMATIK SIDER.
Internetadresse: http://www.matematiksider.dk/enigma/enigma_matematik.pdf - (Internet)

$$AB = (adb)(cefg)(ag)(be)(cfd).$$

Jeg kan nu vælge mellem to muligheder, enten starte fra venstre eller starte fra højre side. Det er ikke klart, hvilken side man skal starter fra[26] [27]. Jeg vælger at starte fra venstre side, da jeg synes det virker mest logisk. Jeg fremstiller en fremgangsmåde, der viser hvordan man laver sammensætningen af AB.

Jeg starter med a i venstre side.

$$(a$$

Den første cykel i A-permutationen, (ade), sender a videre til d. Derefter sender B-permutationens tredje cykel, (cfd), d videre til c. Nu har vi derfor.

$$(ac$$

c bliver sendt videre til e af A-permutationens anden cykel, $(cefg)$. Den anden cykel i B-permutationen, (be), sender e videre til b.

$$(acb$$

Som ses i den første cykel i A-permutationen, (adb), bliver b skubbet til a. Hvor a derefter bliver til g i første cykel i B-permutationen, (ag). AB permutation ser indtil videre således ud.

$$(acbg$$

g bliver til c i den anden cykel i A-permutationen, (cfd). Derefter bliver c sendt videre til f i tredje cykel i B-permutationen, (cfd). AB er nu.

$$(acbgf$$

I anden cykel i A-permutationen, $(cefg)$, bliver f lavet om til et g. Det specielle sker i B-permutationens første cykel, (ag), her bliver g nemlig a, som allerede har været brugt. Dvs. at f bliver sendt tilbage til udgangspunktet, a. Derfor lukker man parenteserne.

$$(acbgf)$$

Man kigger nu på næste ubrugte bogstav i rækken efter a i alfabetet. Da a, b og c er brugt, må det næste bogstav være d. Det skal skrives på AB-permutationen

$$(acbgf)(d$$

---

[26] Vestergaards MATEMATIK SIDER: ENIGMA - matematikken bag løsningen af Enigma. Udgivet af MATEMATIK SIDER.
Internetadresse: http://www.matematiksider.dk/enigma/enigma_matematik.pdf - (Internet)

[27] MATHEMATCIS: Multiplication in Permutation Groups Written in Cyclic Notation. Udgivet af Ukendt.
Internetadresse: http://math.stackexchange.com/questions/31763/multiplication-in-permutation-groups-written-in-cyclic-notation - (Internet)

I første cykel i permutation A, (adb), bliver d sendt til b. Bogstavet b bliver derefter sendt til e i den anden cykel i B-permutation, (be). Det var det sidste bogstav, derfor lukker man parentesen.

$$(acbgf)(de)$$

Jeg kan dermed konkludere, når A og B permutation sammensættes, fås følgende permutation.

$$AB = (adb)(cefg)(ag)(be)(cfd) = (acbgf)(de)$$

Som ses i eksempel 1, kan man lave permutationer med bogstaver, man kan dog også lave dem tal. For at vise, at det også kan laves med tal, laver jeg et nyt eksempel, eksempel 2. Pga. fremgangsmåden er den samme, vælger jeg at undlade mellemregningerne.

Eksempel 2:

En mængde $C = \{1,2,3,4,5,6\}$ og en mængde $D = \{1,2,3,4,5,6\}$, sker der en permutation i hver mængde. Således, $C = \binom{1,2,3,4,5,6}{6,5,4,3,2,1}$ og $D = \binom{1,2,3,4,5,6}{2,6,5,3,1,4}$. Jeg starter med at lave begge permutationer om til cykler:

$$C = \binom{1,2,3,4,5,6}{6,5,4,3,2,1} = (16)(25)(34)\ og\ D = \binom{1,2,3,4,5,6}{2,6,5,3,1,4} = (126435)$$

A består af 3 cykler hvorimod B kun består af 1.

Jeg sammensætter nu permutationerne til AB.

$$CD = (16)(25)(34)(126435) = (14562)(3)$$

Jeg kan dermed konkludere, at når man sammensætter C og D får man 2 cykler, CD=(14562)(3).

En anden del af permutation er, når man ikke kender permutationen, men man gerne vil kende antallet af permutationer, som mængden kan opstilles som. Man har altså en mængde, A, hvor man ønsker at udvælge r elementer af n elementer mulige. Rækkefølgen ikke er ligegyldig, og hvert element må kun bruge en gang[28]. Fx vil mængden $\{abc\}$ give anledning til 6 ordnede mængder: $\{abc\}, \{acb\}, \{bac\}, \{bca\}, \{cab\}\ og\ \{cba\}$. Da jeg tidligere fandt frem til mulige antal kombinationer, som Enigma-maskinen kan indstilles som, fandt jeg ud af, at der var 60 forskellige kombinationer, man kunne sætte rotorerne ned i scramblerenheden på. Jeg regnede det ud ved at sige, at der var 5 muligheder for den første rotor, 4 for den anden og 3 for den sidste: $5 \cdot 4 \cdot 3 = 60$. Det var simpelt nok, til at jeg kunne gøre det på den måde. Det hænder dog, at man støder på langt

[28] Borch, Tommy og Helle Nørbjerg: Sandsynlighedsregning og statistik. Side 47-57. 1. udg. FAG, 1989. (Bog)
Systime: 1.4. Teknologivurdering. Udgivet af Systime.
Internetadresse: https://teknologi.systime.dk/index.php?id=471 - (Internet)

større tal, som hurtigt kan blive uoverskuelige. Her kan man bruge følgende formel: $P_{(n,r)} = \frac{n!}{(n-r)!}$.

Vi ved at n er antal elementer i mængden A, og at r er det antal af elementer, vi vil udvælge af n mulige. Jeg vil starte med at vise, hvordan man kan bruge formlen til at komme frem til de 60 mulige kombinationer, man kan sætte rotorerne ned i scramblerenheden på.

Eksempel 3:

n er antallet af elementer i mængden A, n er derfor antallet af rotorer. n=5. r er det antal af elementer vi vil udvælge fra n mulige, derfor er r antallet af pladser i scramblerenheden. r=3. Værdierne skrives ind i formlen.

$$P_{(5,3)} = \frac{5!}{(5-3)!} = 60\ mulige\ kombinationer$$

Jeg kan konkludere, at hypotesen var korrekt. Der er 60 forskellige kombinationer rotorerne kan sættes i scramblerenheden på.

Som nævnt ville det give mest mening at bruge $P_{(n,r)}$ formlen, når det omhandler mere uoverskuelige tal.

Eksempel 4:

I et maraton deltager en mængde på 50 personer, der skal uddeles præmier til de første 7. Rækkefølgen på præmierne er ikke ligegyldige. Jeg vil finde ud af, hvor mange forskellige kombinationer præmierne kan uddeles blandt de 50 deltagere.

n er antallet af deltagere, 50.

r er antallet af præmiere, 7.

$$P_{(50,7)} = \frac{50!}{(50-7)!} = 503.417.376.000\ mulige\ kombinationer$$

Der ville altså være $503.417.376.000$ mulige kombinationer, som præmierne kunne fordeles.

Enigma omhandler altså begge dele af permutation regning. Både hvordan man sammensætter permutation cykler, og hvordan man finder frem til antallet af mulige permutationer. Ligesom princippet bag Enigma var at lave permutation, var princippet i Turingmaskinen at checke de mulige permutationer. Derfor er kendskabet til permutaioner nødvendigt, i forståelsen af Enigma.

Perspektivering af Enigma til RSA

Under dette punkt laves der en perspektivering af Enigma til et nutidigt krypteringssystem, RSA[29]. Herunder vurderes der, hvem der anvender kryptering i moderne IT kommunikationer, og mod hvem.

Enigma og RSA er begge krypteringssystemer med samme formål, at kunne kommunikere frit, uden fjenden kan forstå det. Det foregår under samme princip. En krypteret besked udsendes, som kun modtageren kan dekryptere ved brug af en nøgle. Forskellen er, at afsenderen ikke kender til nøglen i RSA kryptering, som afsenderen gør i Enigma. Den eneste som kender til nøglen, i RSA, er modtageren. For at forklare hvad det betyder, opstiller jeg et eksempel. Bob ønsker at sende en sine kortoplysninger til sin bank, han får derfor en kasse til lægge hans oplysninger ned i, samt får en han hængelås af banken. Den hængelås han får af banken, låser han sin kasse med og sender den af sted mod banken. Når banken får kassen, kan de låse hængelåsen op med nøglen, som de selv beholdte. Ideen med denne slags kryptering er, at hvis kassen var blevet stjålet af en tyv, ville de ikke kunne åbne den, da det kun er banken som har nøglen. I virkeligheden foregår det selvfølgelig ikke med hængelåse og kasser, men med tal og bogstaver, princippet er dog det samme.

Enigma har en anden svaghed, som RSA ikke lider af, nemlig at et bogstav ikke kan blive til sig selv. Et m kan altså ikke blive til et m igen. Den svaghed brugte briterne, når de havde mistanke om at et ord i en klartekst[30] blev nævnt i en krypterede besked. Briterne kaldte et stykke klartekst en crib, hvis de havde mistanke om, at det var det, der stod i den krypterede besked[31]. Briterne vidste at ordet wettervorhersage, som betyder vejrudsigt, blev brugt i klarteksten, fordi vejrudsigten ofte betyder en stor rolle i forberedelsen til en kamphandling. Måden briterne kunne se om ordet var en crib, var ved at man sammenlignede den krypterede besked, som ofte blev skrevet uden mellemrum,

---

[29] Ask a Mathematician / Ask a Physicist: Q: How do you write algorithms to enycrypt things?. Udgivet af Ask a Mathematician / Ask a Physicist.
Internetadresse: http://www.askamathematician.com/2012/03/q-how-do-you-write-algorithms-to-enycrypt-things/ - (Internet)

[30] Vestergaards MATEMATIK SIDER: ENIGMA. Udgivet af Ukendt.
Internetadresse: http://www.matematiksider.dk/enigma.html#how_enigma_works - (Internet)

[31] Vestergaards MATEMATIK SIDER: ENIGMA. Udgivet af Ukendt.
Internetadresse: http://www.matematiksider.dk/enigma.html#how_enigma_works - (Internet)

med crib'en. På bilag 14 fremgår et eksempel, hvor ordet wettervorhersage er placeret under den krypterede besked. Det ses at t'et i den krypterede og t'et i klarteksten er det samme. De passede altså ikke sammen der, derfor rykker man klarteksten en tak til højre, og som ses er ingen af bogstaverne ens. Det kunne altså være det ord, som stod i beskeden. Det er dog ikke sikkert, da der er flere ord, som også kunne have matchet. I RSA kryptering kan et bogstav godt blive til sig selv igen, derfor ville det være en umulighed at bruge samme metode. Metoden hjalp til at Alan Turing senere kunne bygge sin Turingmaskine.

Enigma blev knækket, som nævnt tidligere, af Turingmaskinen. Maskinen fastlagde de væsentligste træk ved den computer vi kender i dag[32]. Dengang var dekrypterings teknologien altså stærkere end Enigma. I dag vil det tage en super computer længere tid, end det vil tage for solen af brænde ud, at dekryptere en 2048 bit RSA kryptering[33]. Krypteringssystemer har altså forbedret sig gevaldigt siden Enigma. Det er ikke kun krypteringssystemerne som har ændret sig, brugen af kryptering har ligeledes. Tilbage i 2. verdenskrig var det lande og stater som brugte kryptering[34], de brugte det som beskyttelse mod andre lande. De kunne altså beskytte sig fra at nabolandet vidste, at de ville invadere dem næste dag. I dag bliver kryptering brugt af civile og virksomheder mod hacker angreb, stater, men også mod organisationer som FBI og NSA[35]. Alt foregår på internettet i dag. Man har ens kortoplysninger, Cpr nummer, ens private samtaler osv. flere steder på internettet. Det gør enhver sårbare. Selvom det umiddelbart lyder som en god ide, at virksomheder som Apple og Google bruger kryptering, så deres brugere kan være sikre på, at deres oplysninger ikke komme videre, mener USA's præsident, Barack Obama, FBI og NSA, at FBI og NSA skal have retten til at kunne gennemgå hele befolkningens beskeder og private oplysninger, for at finde frem til teorister og pædofile[36]. De ser gerne et samarbejde med Apple og Google mod mulige angrib. Her opstår der

[32]computerworld: How Alan Turing set the rules for computing. Udgivet af computerworld. Internetadresse: http://www.computerworld.com/article/2504774/data-center/how-alan-turing-set-the-rules-for-computing.html - (Internet)
[33] Matlex: Koder og ciffre. Udgivet af Matlex. Internetadresse: http://www.matlex.dk/kode.html - (Internet)
[34]Frandsen, Jesper og Mads Rangvis: *ENIGMA - ET DILEMMA*. 1. udg, Systime, 2010. (Bog)
[35] Version 2: Dansk krypto-ekspert: NSA kan stadig ikke knække dine krypterede data. Udgivet af Version 2. Internetadresse: https://www.version2.dk/artikel/kryptoprofessor-nsa-har-ingen-genvej-til-kodeknaekning-5362 - (Internet)
[36] The Washington Post: What President Obama is getting wrong about encryption. Udgivet af The Washington Post. Internetadresse: https://www.washingtonpost.com/news/the-

et dilemma for virksomhederne, de skal nemlig vurdere, om de vil sikre brugernes oplysninger, eller om de vil udlevere dem til organisationer som NSA. Hvis de vælger at samarbejde med NSA, kan de muligvis være med til at stoppe den næste pædofile eller det næste terrorangreb. De mister derimod en stor tillid fra deres brugere, som forventer at deres oplysninger er sikre ved dem. Hvis de derimod vælger ikke at samarbejde, får de USA's regering på nakken, men beholder derimod tilliden fra brugerne. Appels svar på dilemmaet er at nægte at samarbejde[37]. Det er gjort klart i en artikel fra computerworld.dk[38]. De Amerikanske myndigheder har haft Apple i retten, hvor Apple blev dømt til at udvikle et program, som FBI kunne bruge til at åbne Syed Rizwan Farooks[39] iPhone. Det har Apple nægtet, da de mener at FBI vil kunne anvende programmet som en bagdør til alle verdens iPhones. Ved at Apple har nægtet, at udvikle sådan et program, kan det betyde, at man aldrig finder ud af hvem Syed Rizwan Farook har haft kontakt med. Det betyder derimod også, at Apple går ind for folks rettigheder, med at have ens private oplysninger for sig selv.

Tiderne har altså ændret sig siden 2. verdenskrig, hvor man ikke havde alle ens oplysninger inden for alle andres rækkevide, og den eneste trussel der var, var de andre stater. Til at man, hele tiden er sårbar overfor ens private oplysninger bliver misbrugt af myndigheder og forskellige hackere. Tiden har også ændret sig på det punkt, hvor regeringen ønskede, at have den stærkeste form for kryptering, til at regeringen prøver at få nedsat de krypteringssystemer som findes i dag.

Konklusion

Det viste sig, at Enigma kan indstilles på 158.962.555.217.826.360.000 forskellige måder. Hvor alle delene i Enigma-maskinen har hver sin funktion, som gør dette muligt. For at

---

switch/wp/2015/02/19/what-president-obama-is-getting-wrong-about-encryption/?utm_term=.a80fbe983d7e - (Internet)

[37] Computerworld: Apple vil stramme kryptering til nye højder i kølvandet på spionsag: Glemmer du din kode, er der nul hjælp at hente. Udgivet af Computerworld. Internetadresse: http://www.computerworld.dk/art/236452/apple-vil-stramme-kryptering-til-nye-hoejder-i-koelvandet-paa-spionsag-glemmer-du-din-kode-er-der-nul-hjaelp-at-hente - (Internet)

[38] Computerworld: Apple vil stramme kryptering til nye højder i kølvandet på spionsag: Glemmer du din kode, er der nul hjælp at hente. Udgivet af Computerworld. Internetadresse: http://www.computerworld.dk/art/236452/apple-vil-stramme-kryptering-til-nye-hoejder-i-koelvandet-paa-spionsag-glemmer-du-din-kode-er-der-nul-hjaelp-at-hente - (Internet)

[39] En terrorist som dræbte 14 personer den 2. December 2015

knække koden, ville det tage en person ca. $5{,}04 \cdot 10^6$ år, hvis han altså afprøvede 1 million kombinationer i sekundet. Derfor troede tyskerne også, at Enigma-koden var ubrydelig. Det lykkes dog alligevel Storbritannien, pga. Alan Turings Turingmaskine, at knække den. Det betød, at briterne kunne dekryptere beskederne, som tyskerne sendte ud. Det var derfor afgørende for Storbritannien, at de kunne holde det hemmeligt. At holde sådan en vigtig opdagelse hemmelig, havde sine konsekvenser. Briterne var tvunget til at opgive soldater og civiles liv, for at tyskerne ikke fandt ud af, at Enigma var knækket. For at det var muligt for Alan Turing at knække Enigma, skulle han først have styr på, hvad permutationer er. En permutation er det der sker i Enigma, når a bliver til et b. Dvs. at en permutation er en afbildning, hvor der byttes ud på elementer i en mængde. Når man vil finde antallet af mulige permutationer, skal man bruge kombinatorikregning.
Kryptering har forbedret sig gevaldigt siden Enigma. I dag bruges kryptosystemer som RSA. RSA er så stærkt et program, at det ville tage længere tid for solen af brænde ud, end det ville tage for en super computer af knække en 2048 bits kryptering. Det er dog ikke de samme fjender, som man beskytter sig fra i dag, som det var i 2. verdenskrig. Dengang brugte man kryptering mod andre lande og stater, i dag bliver krypteringen brugt mod ens eget land, organisationer som NSA og FBI og hackere. Der er stod uenigheder om, hvorvidt USA må have adgang til hele verdensoplysninger eller ej. Indtil videre ser det dog ikke ud til, at virksomheder som Apple vil gå ned på kryptering, tværtimod.

Litteraturliste

Vestergaards MATEMATIK SIDER: ENIGMA. Udgivet af Matematik sider.
Internetadresse: http://www.matematiksider.dk/enigma.html#how_enigma_works - Besøgt d. 14.12.2016 (Internet)

Frandsen, Jesper og Mads Rangvis: ENIGMA - ET DILEMMA. 1. udg. Systime, 2010. (Bog)
Webmatematik: Fakultetsfunktionen. Udgivet af Matematikcenter.
Internetadresse: http://www.webmatematik.dk/lektioner/matematik-b/sandsynlighed-og-kombinatorik/fakultetsfunktionen - Besøgt d. 14.12.2016 (Internet)

Crypto Museum: Enigma. Udgivet af Cryptomuseum.com.
Internetadresse: http://www.cryptomuseum.com/crypto/enigma/working.htm - Besøgt d. 15.12.2016 (Internet)

Bauer, Craig P.: Secret History The story Of Cryptology. 1. udg. CRC Press, 2013. (Bog)

Webmatematik: Multiplikations- og additionsprincipperne. Udgivet af Matematikcenter.
Internetadresse: http://www.webmatematik.dk/lektioner/matematik-b/sandsynlighed-og-kombinatorik/multiplikations-og-additionsprincipperne - Besøgt d. 15.12.2016 (Internet)

Borch, Tommy og Helle Nørbjerg: Sandsynlighedsregning og statestik. Side 47-57. 1. udg. FAG, 1989. (Bog)

Systime: 1.4. Teknologivurdering. Udgivet af Systime.
Internetadresse: https://teknologi.systime.dk/index.php?id=471 - Besøgt d. 21.12.2016 (Internet)

Wikipedia: Alan Turing. Udgivet af Wikipedia.
Internetadresse: https://da.wikipedia.org/wiki/Alan_Turing - Besøgt d. 20.12.2016 (Internet)

Wolftram Math World: Turing machine. Udgivet af Wolftram.

Internetadresse: http://mathworld.wolfram.com/TuringMachine.html - Besøgt d. 20.12.2016 (Internet)

Wikipedia: Konvoj. Udgivet af Wikipedia. Internetadresse: https://da.wikipedia.org/wiki/Konvoj - Besøgt d. 20.12.2016 (Internet)

Wikipedia: German Type XIV submarine. Udgivet af Wikipedia. Internetadresse: https://en.wikipedia.org/wiki/German_Type_XIV_submarine - Besøgt d. 20.12.2016 (Internet)

Vestergaards MATEMATIK SIDER: ENIGMA - matematikken bag løsningen af Enigma. Udgivet af MATEMATIK SIDER. Internetadresse: http://www.matematiksider.dk/enigma/enigma_matematik.pdf - Besøgt d. 16.12.2016 (Internet)

MATHEMATCIS: Multiplication in Permutation Groups Written in Cyclic Notation. Udgivet af Ukendt. Internetadresse: http://math.stackexchange.com/questions/31763/multiplication-in-permutation-groups-written-in-cyclic-notation - Besøgt d. 16.12.2016 (Internet)

Ask a Mathematician / Ask a Physicist: Q: How do you write algorithms to enycrypt things?. Udgivet af Ask a Mathematician / Ask a Physicist. Internetadresse: http://www.askamathematician.com/2012/03/q-how-do-you-write-algorithms-to-enycrypt-things/ - Besøgt d. 17.12.2016 (Internet)

computerworld: How Alan Turing set the rules for computing. Udgivet af computerworld. Internetadresse: http://www.computerworld.com/article/2504774/data-center/how-alan-turing-set-the-rules-for-computing.html - Besøgt d. 20.12.2016 (Internet)

Matlex: Koder og ciffre. Udgivet af Matlex. Internetadresse: http://www.matlex.dk/kode.html - Besøgt d. 20.12.2016 (Internet)

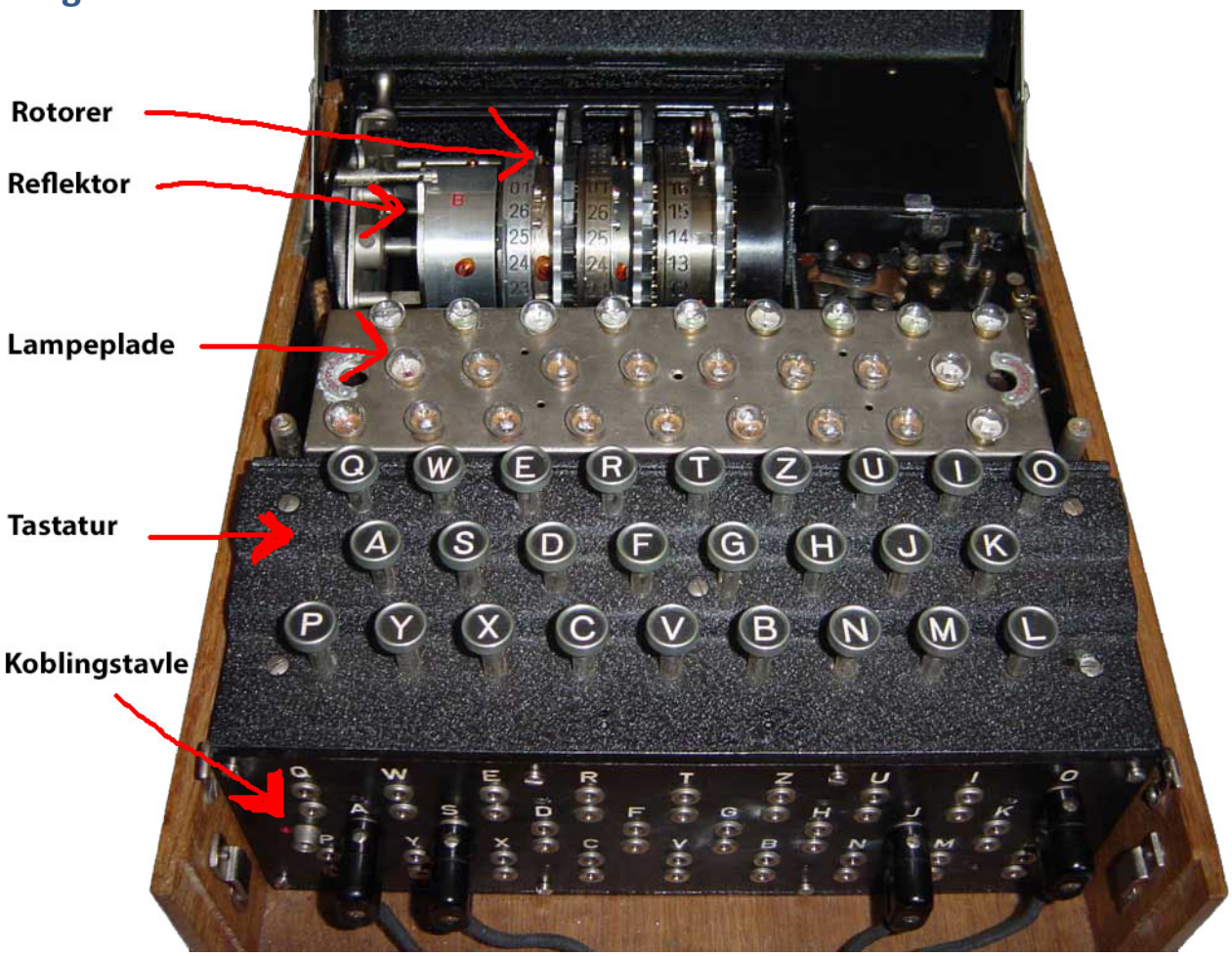
Version 2: Dansk krypto-ekspert: NSA kan stadig ikke knække dine krypterede data. Udgivet af

Version 2. Internetadresse: https://www.version2.dk/artikel/kryptoprofessor-nsa-har-ingen-genvej-til-kodeknaekning-5362 - Besøgt d. 20.12.2016 (Internet)

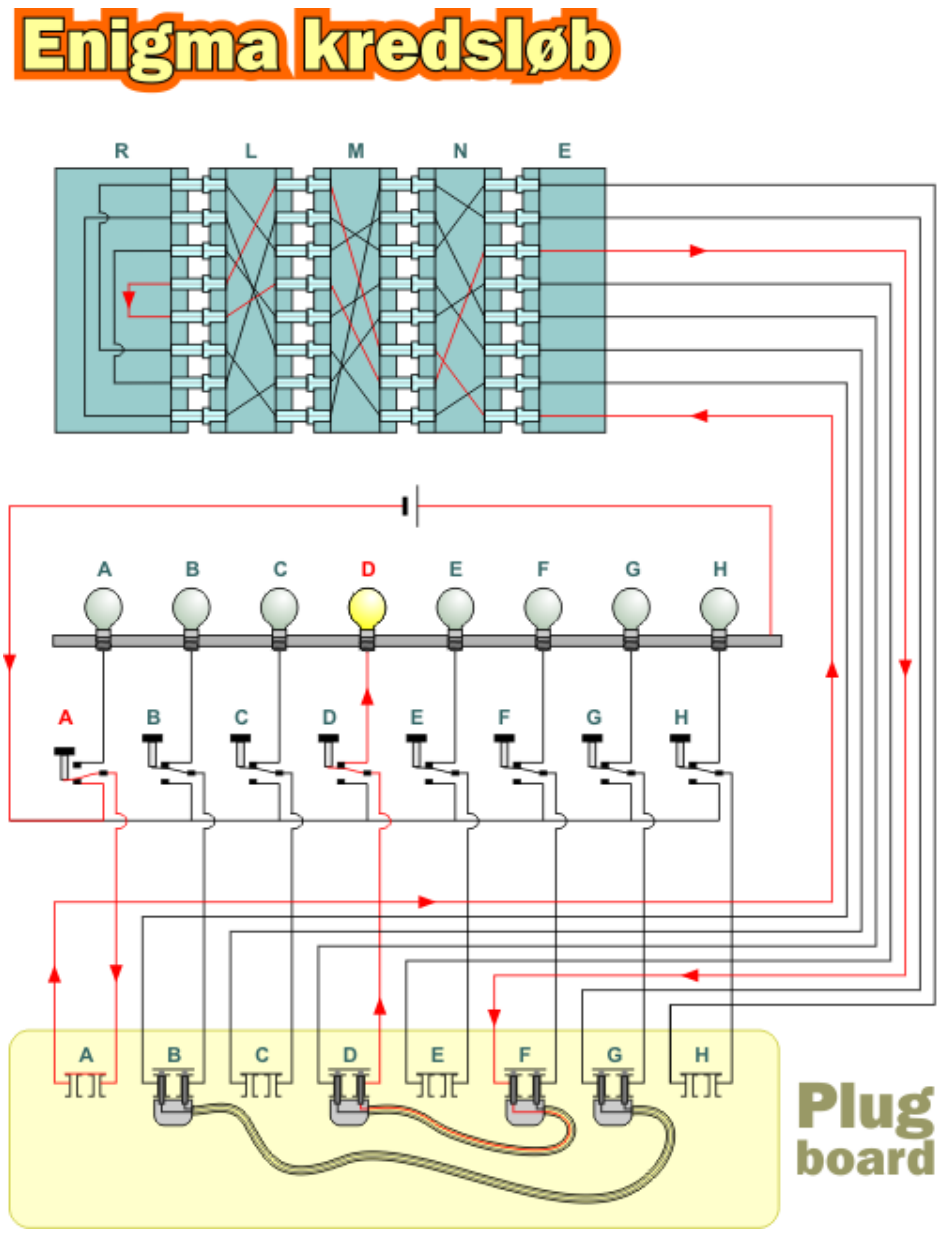
The Washington Post: What President Obama is getting wrong about encryption. Udgivet af The Washington Post. Internetadresse: https://www.washingtonpost.com/news/the-switch/wp/2015/02/19/what-president-obama-is-getting-wrong-about-encryption/?utm_term=.a80fbe983d7e - Besøgt d. 19.12.2016 (Internet)

Computerworld: Apple vil stramme kryptering til nye højder i kølvandet på spionsag: Glemmer du din kode, er der nul hjælp at hente. Udgivet af Computerworld. Internetadresse: http://www.computerworld.dk/art/236452/apple-vil-stramme-kryptering-til-nye-hoejder-i-koelvandet-paa-spionsag-glemmer-du-din-kode-er-der-nul-hjaelp-at-hente - Besøgt d. 20.12.2016 (Internet)

Bilag



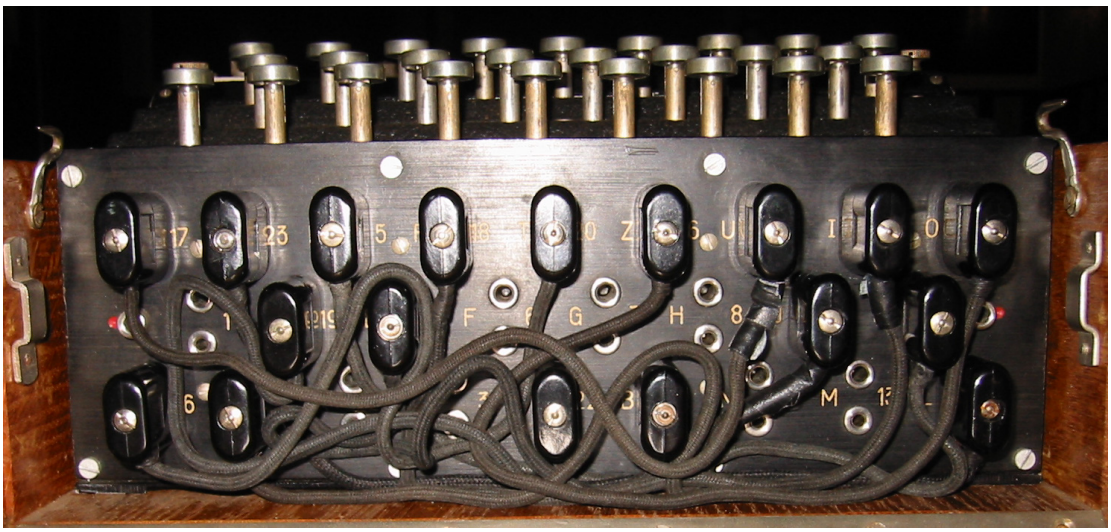
Bilag 1 - På billedet fremstår Enigma-maskinen uden dækpladen. Kilde: http://ilord.com/enigma.html med egne tilføjelser .



Bilag 2 - Diagram af Enigma krypteringssystem. Kilde:

http://www.matematiksider.dk/enigma.html#how_enigma_works

Bilag 3 - et billede af tastaturet - taget fra https://www.google.dk/search?q=enigma+tastatur&espv=2&biw=1177&bih=630&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjCm9euu_TQAhVDjywKHdB7DxMQ_AUIBigB#imgrc=_rlc-LVniRafMM%3A



Bilag 4 - et billede af koblingstavlen/plugboardet - Kilde: https://www.google.dk/search?q=enigma+tastatur&espv=2&biw=1177&bih=630&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjCm9euu_TQAhVDjywKHdB7DxMQ_AUIBigB#tbm=isch&q=enigma+plugboard&imgrc=SajxlmaEFh7JpM%3A

Fakultetsfunktion betegnes med et udråbstegn. Det er kun naturlige tal samt 0, man kan tage fakultet af. Det gælder at $0! = 1$. Man skriver fakultetsfunktionen således:

$$n! = n \cdot (n-1) \cdot (n-2) \cdot (n-3) \ldots 3 \cdot 2 \cdot 1$$

F.eks.

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$$

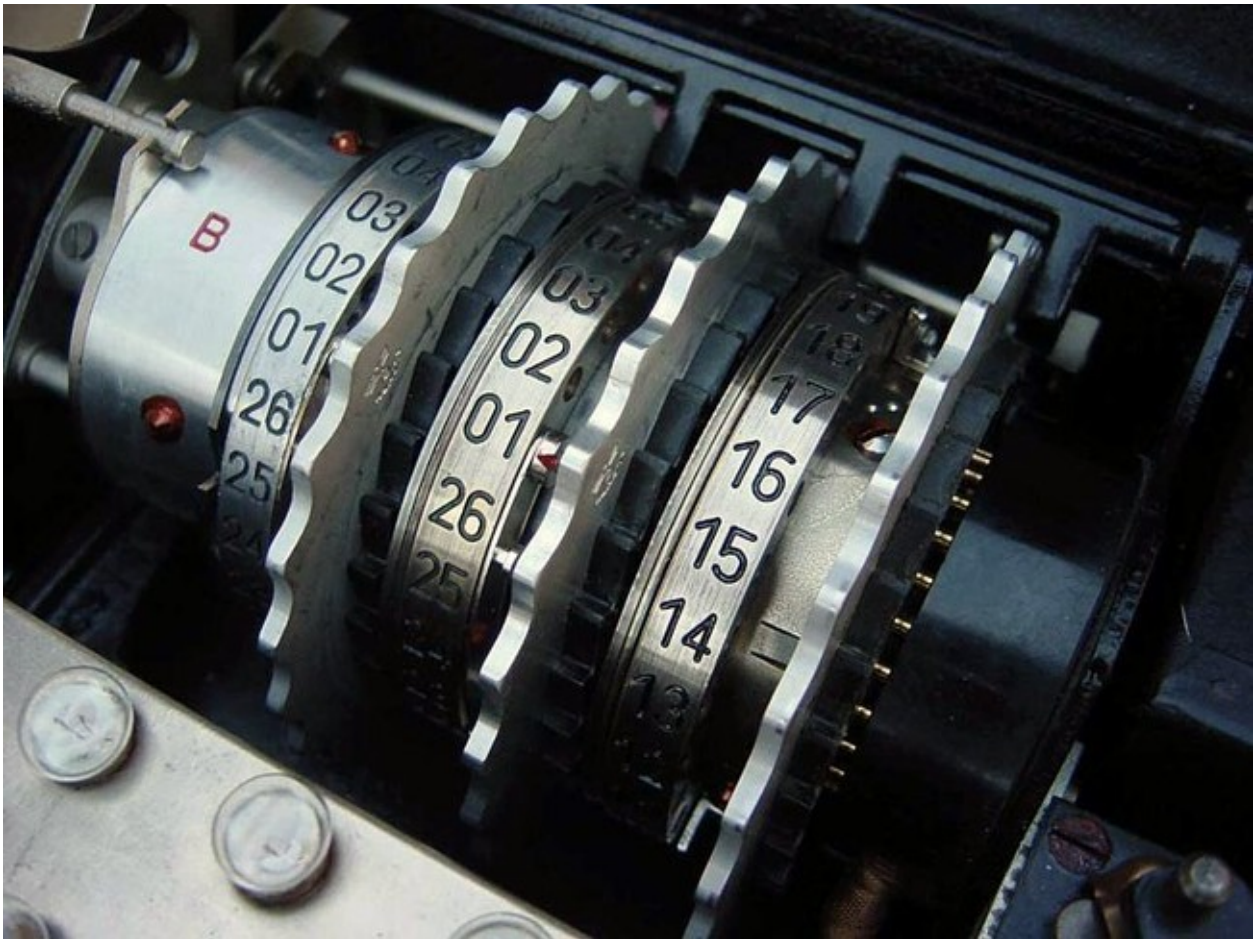
Bilag 5 - Der fremgår på billaget en beskrivelse på fakultetsfunktionen - Selvlavet.

bilag 6 er nedestående
Eks:
Der er 5 ledninger tilkoblet koblingstavlen, derfor vil antallet af mulige kombinationer være følgende:

$$\frac{26!}{(26-2\cdot 5)!\cdot 5!\cdot 2^5} = 5.019.589.575$$

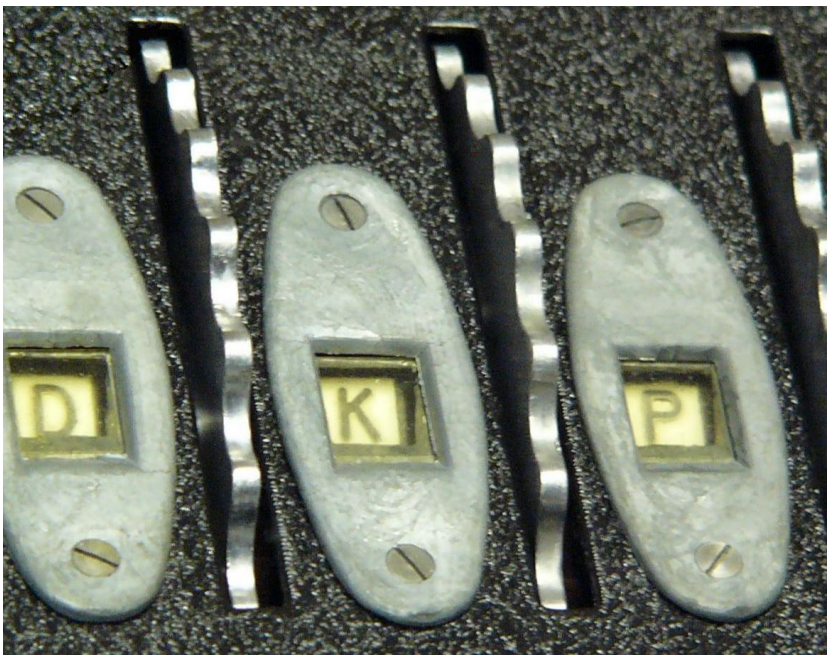
Antal ledninger (n)	Mulige kombinationer
0	1
1	325
2	44.850
3	3.453.450
4	164.038.875
5	5.019.589.575
6	100.391.791.500
7	1.305.093.289.500
8	10.767.019.638.375
9	53.835.098.191.875
10	150.738.274.937.250
11	**205.552.193.096.250**
12	102.776.096.548.125
13	7.905.853.580.625

Bilag 6 - En tabel over mulige kombinationer med n antal ledninger - selvlavet



Bilag 7 - et billede af scramblerenheden - Kilde: https://www.google.dk/search?q=enigma+tastatur&espv=2&biw=1177&bih=630&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjCm9euu_TQAhVDjywKHdB7DxMQ_AUIBigB#imgrc=_rlc-LVniRafMM%3A

Bilag 8 - en simplificeret tegning af ledningsnettet inden i en rotor - Kilde: https://www.google.dk/search?q=enigma+rotor&espv=2&biw=1177&bih=630&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjXoMrBzfTQAhWKkCwKHabzD-UQ_AUIBigB#imgrc=-eKwfH5t5D_SzM%3A



Bilag 9 - Billedet viser at rotorerne er indstillet på DKP - Kilde: https://www.google.dk/search?q=enigma+srp&espv=2&biw=1177&bih=630&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj8lOiW8vXQAhVBXCwKHZAXC7cQ_AUIBigB#tbm=isch&q=enigma+rotor&imgrc=64lktxB-NxupWM%3A

Bilag 10 - Reflektor åben, så man kan se ledningsnettet - Kilde: https://www.google.dk/search?q=enigma+reflektor&espv=2&biw=1177&bih=630&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjR5Myf5PjQAhVDCSwKHdXfAK4Q_AUIBigB#q=enigma+reflektor+open&tbm=isch&tbs=rimg:Cafh1PCd0QtQIjjhabBY98GxrzrgOtROyNuxBZms7S0z230jVTmSXmK4_1qesqXz89fP18neiLfD8zrjTiK7lr6eEnyoSCeFpsFj3wbGvEVR5H3ZXUT47KhIJOuA61E7I27ERr-2YUyMlda8qEgkFmaztLTPbfRGMqczpqnAU8ioSCSNVOZJeYrj-EX_1_1cJYbFBJGKhIJp6ypfPz18_1URN2xG7Lx4u6kqEgnyd6It8PzOuBGv7ZhTIyV1ryoSCdOIruWvp4SfEYypzOmqcBTy&imgrc=p-HU8J3RC1DkkM%3A

Bilag 11 - Viser et i blive krypteret til et u- Kilde:
https://www.google.dk/search?q=Enigma+lampeplade&espv=2&biw=1177&bih=630&source=lnms&tbm=isch&sa=X&ved=0ahUKEwja5pq9i_nQAhXJ6CwKHeZKCqMQ_AUIBigB#tbm=isch&q=enigma+lamp+panel&imgrc=MyQN7_lpYUan5M%3A

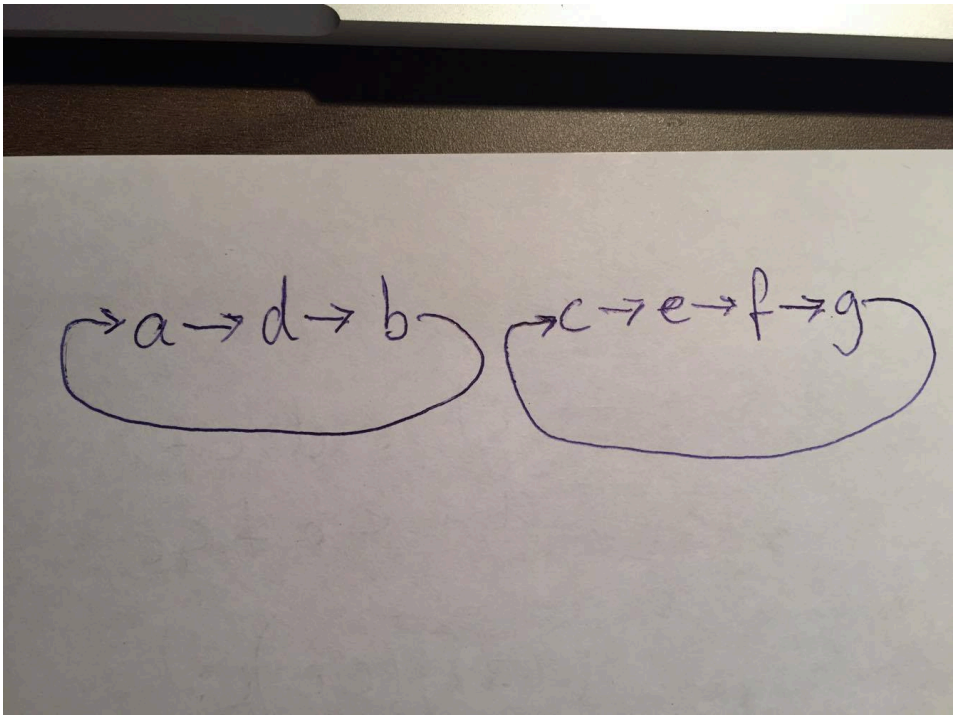
Geheime Kommandosache!
Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. X
für Juni 1943

	Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
St	30.	V I III	22 04 16	TU RQ PL SI NF XW DZ GA YV MB	oab hvs ilg wtm
St	29.	I III II	02 18 05	AR DQ LP MF ES KT YZ HW CO UG	hax oqa kpa yyt
St	28.	II III IV	14 25 11	BI XC OF RT MG DV SK JE HL UW	nal clo xaz bab
St	27.	V II I	17 23 08	ZA TD WI VR OX PQ FS CM HY BU	kwq rsu uvt rmw

fiktive værdier!

Bilag 12 - kodebogen med fiktive nøgler til Enigma-maskinen - Kilde:
http://www.matematiksider.dk/enigma.html#how_enigma_works



bilag 13 - Viser hvordan en permutation cykel virker - selvlavet

Bilag 14- et eksempel på at finde en crib - Kilde: http://www.matematiksider.dk/enigma.html