Indledning:

Opgaven omhandler kryptering under 2. verdenskrig. Der bliver primært taget udgangspunkt i de sidste faser af krigen, både men hensyn til de militære strategier, men også ved hvilken indflydelse det havde for England at Enigma blev brudt, da det er her det kan ses tydeligst. I opgaven kommes ind på de militære strategier under krigen og hvordan tyskerne gjorde brug af Enigma. Til at forklare dette benytter jeg konkrete eksempler, jeg har udvalgt episoder som jeg mener, understøtter og viser udførelsen af militære handlinger, og derfor strategier. Samtidig med det bliver der redegjort for klassiske krypteringsmetoder, for at kunne se hvilken stor forbedring Enigma var. Jeg inddrager det udleverede bilag i hvor jeg skal dekryptere en tekst, under redegørelsen af det additive kryptosystem, herunder det monoalfabetiske. Der bliver i opgaven også beskrevet hvordan tyskerne gjorde brug af denne Enigma-maskine. Til sidst vurderes det, hvilken indflydelse det havde på den engelske militære strategi, at man brød det tyske krypteringssystem, Enigma. Her diskuteres det hvilke fordele der var for de allierede at koden blev brudt, og hvilken indflydelse det havde på slaget ved Atlanten. Havde England kunne vinde kampene på Atlanterhavet, hvis ikke man kendte til tyskernes placering.

Den militære strategi:

Der var mange forskellige strategier under 2. verdenskrig. De mange forskellige afhang af formålet og omstændighederne. Der kommer forskellige eksempler på brugen af forskellige strategier. Samtidig med dette betegnes Enigma også for en form for militær strategi, da blev benyttet til at kommunikere med sine allierede og sine egne. Fordelen ved brug af koder var at fjenden ikke kunne forstå indholdet. På grund af at fjenden ikke kendte indholdet af de krypterede meddelelser, kunne de benyttes til at udføre forskellige former for strategier. Her vælger jeg at fokusere på de allierede, altså England og USA, da især England er så stor et fokus punkt hele opgaven.

Sir Arthur Harris som var øverstkommanderende for RAF's bomberkommando, var hovedtalsmand for fladebombning. Det vil sige at det er en strategi hvor store flåder af bombefly koncentrerede deres natlige angreb mod fjendens byområder. Sir Arthur Harris

blev udnævnt til næstkommanderende, på grund af resultatet som forekom, da RAF benyttede præcisionsbombninger. Eksperimentet med præcisionsbombningerne var skuffende, det viste sig at kun én ud af tre bomber slog ned inden for en afstand af 8 km eller mindre af deres mål. Samtidig med det havde kun én ud af ti påståede træffere under et angreb noget på sig. I praksis betød dette at man hos RAF var nødsaget til at gå over til fladbombning eller helt at opgive bombeoffensiven. Men man så fladbombning som den eneste mulighed. Harris havde tidligere benyttet denne metode, i kampene mod oprørere i Irak, her blev hele landsbyer jævnet med jorden, og han havde sågar selv set hvordan krigsfly påførte civilbefolkningen død og markante skader. Sir Arthur Harris har sågar udtalt: "Det eneste Arabere forstår, er en hård hånd." I dette tilfælde var araberne blot blevet udskiftet med tyskerne.[1] Bombeoffensiven tog for alvor fart i 1942, produktionen af bombefly øgedes og antallet af fladbombninger steg. Amerikanerne der hjalp briterne, bombede om dagen. Målet med dette var officielt at tilintetgøre legitime mål, dette var ikke målet i praksis. Her blev der ikke lagt skjult på, at formålet var at antænde storbrænde, som ikke kunne slukkes. Storbrandenes formål var at "knække den civile kampgejst". I dette eksempel ændres strategien for at få at optimere det og derved gøre det nemmere at udføre.

Den. 5. juni 1944 var datoen hvorpå Debarkation day, også kaldet D-dag skulle finde sted. Dette blev dog udskudt 24 timer, grundet det dårlige vejr. D-dagen bliver af de fleste britiske og amerikanske historikere, set for at den afgørende militære begivenhed under 2. verdenskrig. Det skyldes til dels deres egen deltagelse, men også fordi hvis det slog fejl ville chancen for at få et forsøg som dette igen, være lille. Amerikanernes og englændernes armada på 1200 skibe, kunne krydse Kanalen i sikkerhed, luftdækket med 260 fly kunne med succes i den indledende landing på Pegasus-broen og det samme kunne siges om faldskærmsudspring ved Sainte-Mère-Eglise. I alt blev 156.000 soldater landsat, efterfølgende viste tabstallene at kun 1,6% var faldet, dette var historisk lave. Efterfølgende kunne man sige at "den anden front var åbnet".[2] Men efter et par dage opstod et afgørende problem for briterne og amerikanerne. De havde ikke de nødvendige våben, uddannelse og ledere som skulle til for at besejre tyskerne. Til trods for deres overlegenhed på kampvognsområdet på 20 til en og på flyområdet 25 til en, kunne de ikke udnytte det og var derfor nødsages til at få støtte fra fly. Med hjælp fra fly blev tyskernes panserstillinger

[1] Davies, Norman, Europa i krig, Gads 2009(s. 114)
[2] Davies, Norman, Europa i krig, Gads 2009(s. 130)

ødelagt med raketter og bombeflyene smadrede de tyske forsvarspositioner. Problemet gjorde også at amerikanerne først efter syv uger, kunne fortage et udfald i stedet for ved to uger. I dette eksempel ændres strategien, da man opdager at det man forventede ikke fungerede. Dette viser igen fleksibiliteten omkring strategier, at de kan optimeres undervejs, ligesom i tidligere eksempel. Ved D-dagen spillede bruddet på Enigma også et stor rolle. Bletchley sørgede i månederne op til dagen at komme med et detaljeret billede af den tyske troppekoncentration, langs den franske kyst.

I januar 1945 rykkede de vestlige armeer forsigtigt frem mod Tyskland, imens lagde sovjet planer om en offensiv, der ville blive større end set før. Her blev der i alt sat 3,8 millioner soldater til rådighed for at kunne fuldføre fremrykningen. Denne fremrykning skulle ske fra Vistula til Oder på 15 dage, og efterfølgende fra Oder til Elbe. Den Røde Hær ville de kritiske steder, være i så markant overtal at det ikke ville være den store udfordring. Ingen anden militær styrke havde før haft denne størrelse. Deres talmæssige fordel lå i forholdet 10:1. Oven i købet led Tyskland under mangel på rekrutter og brændstof. Her satsede man på at overmande fjenden og på den måde drage fordel af den situation modstanderen står i.

Fælles for disse eksempler er denne fleksibilitet der er omkring strategierne. Med det menes at man var klar til at ændre den oprindelige plan eller blot vente til tiden var bedre. Dette da man valgte at benytte fladbomberne, da man på grund af et forsøg fandt ud af at den tidligere metode ikke var optimal. Derfor ændrede man det. Denne holdning og vilje til at optimere strategierne gjorde at udfaldet ofte blev bedre, set fra deres øjne, end hvis ingen ændring var sket. Viljen til også at vente til timingen passede bedre var der også. Udsættelsen kunne skyldes forskellige ting som gjorde at angrebet ikke kunne være udført ideelt. Samtidig med dette kan et andet hovedtræk være brugen af den fremskredne teknologi, da der blev brugt fly af forskellig art, til forskellige formål. Med teknologien som støtte kunne det gøre udførelsen af disse strategier væsentlig nemmere. Samtidig med det kan man sige at brugen af Enigma-maskinen fra Tysklands side, var en del af den militære strategi. Man kan senere i opgaven læse om hvordan Tyskland benyttede Enigma. England og de allieredes forsøg på at bryde dette kryptosystem, kan også siges at være en del af deres strategi. Da man ved at bryde denne kode kunne tilrettelægge nye militære strategier.

Enigma:

I 1918 gik den tyske opfinder Arthur Scherbius og han ven Richard Ritter sammen og dannede ingeniørfirmaet Scherbius & Ritter, dette firma kastede sig over mange forskellige ting, alt fra varmepuder til turbiner. Dog var Arthur Scherbius' ynglings projekt at forbedre de utilstrækkelige kryptografiske systemer som blev benyttet tidligere. Man har i tidligere krige også benyttet sig af kryptering, dog i nogle simplere udgaver. Man benyttede sig af cifferskiven under den amerikanske borgerkrig. Brugen af koder under krigsførelse går endnu længere tilbage, allerede i 58-50 f.Kr. brugte Julius Cæsar det monoalfabetiske kryptosystem.

Arthur Scherbius' Enigma-maskine var en udvikling fra kryptografiske systemer som foregik med blyant og papir, til en form for kryptering hvorpå der blev udnyttet den teknologiske fordel i det tyvende århundrede. Man kan sige at Enigma-maskinen er en videreudvikling af Albertis cifferskive. Cifferskiven kan man opfatte som en scrambler, det vil sige at den hvert bogstav i klarteksten og omdanner det til noget andet.[3] Denne måde at benytte den på gør at koden er forholdsvis triviel at bruge, ligesom det monoalfabetiske kryptosystem som senere bliver forklaret. Derfor mente opfinderen af cifferskiven, nemlig Alberti, at man kunne ændre skiverne i løbet af meddelelsen. Derfra kunne den gå fra at være monoalfabetisk til at være polyalfabetisk, det skete altså ved ændringen af skivens indstilling.

I Enigma benyttes samme princip som med cifferskiven, nemlig scrambleren. Scherbius' Enigma-maskine bestod af flere forskelige specialkomponenter. Brydes maskinen ned i komponenter og genopbygges trinvis, kan principperne bagved fremgå. Enigma-maskinen består af elementer som er forbundet via ledninger. Der er et tastatur hvor man indtaster hvert bogstav i klarteksten, efterfulgt af en scrambler som krypterer hvert af klartekstens bogstaver til et tilsvarende bogstav i kodeteksten, og et displaybræt bestående af forskellige lamper til at angive kodetekstens bogstaver.[4] Når et klartekstbogstav skal krypteres, indtaster operatøren det på tastaturet, hvorefter der sendes en elektrisk impuls gennem scramblingsenheden og ud på den anden side, hvor det tilsvarende bogstav i kodeteksten oplyses på lampepladen. Den vigtigste del af Enigma-maskinen er scrambleren, det er en

[3] Singh, Simon, Kode bogen, Gyldendal, 1999 (s. 140)
[4] Singh, Simon, Kode bogen, Gyldendal, 1999 (s. 141)

tyk gummiskive som er overtrukket med ledninger. Disse ledninger kommer fra tastaturet og kommer ind i scrambleren. Her vrider og drejer ledningerne sig en del gange, hvorefter de kommer ud på den anden side. Den interne ledningsføring i scrambleren afgøre hvordan klartekstens bogstaver krypteres. Denne enkelte opsætning kan maskinen opfattes som en mekanisk, sågar, en elektronisk udgave af en monoalfabetisk substitutionskode.

Men Arthur Scherbius' ide var at scramblerskiven skulle rotere automatisk, det vil sige den skulle rotere en seksogtyvendedel af en omgang. Dette er dog kun gældende hvis det er et fuldstændigt alfabet på 26 bogstaver. Det vil sige at scrambleren straks efter indtastningen af et bogstav, rotere en seksogtyvendedel. Det betyder at hvis det samme bogstav som tidligere indtastet, vil det krypterede bogstav ikke være det samme som tidligere. Dette fortsætter således. Derfor kan man taste det samme bogstav for eksempel seks gange i træk, uden at det krypterede bogstav er det samme. Kodealfabetet ændrer sig derfor efter hver kryptering, det vil sige at krypteringen af det samme bogstav som tidligere nævnt, skifter hele tiden. Denne rotation definerer scrambleren mange kodealfabeter, og derfor kan maskinen bruges til implementering af en polyalfabetisk kode.

Det vigtigste træk ved Arthur Scherbius' maskine er denne rotation af scramblerne. Rotationen skaber dog også en oplagt svaghed, tastes det samme bogstav nok gange(i dette tilfælde 26 gange), vender scrambleren tilbage til sin oprindelige position, og hvis bogstavet tastes igen og igen, gentages dette krypteringsmønster. Og eftersom regelmæssighed og struktur i et kodeteksten er tegn på en svag kode, vil man selvfølgelig undgå dette. Det kan løses ved at der indsættes en ekstra scramblerskive. Det vil sige at hver gang et bogstav krypteres, roterer den første scrambler ét "hak", hvilke vil sige at hver forbindelse forskydes én plads nedad.[5] Den anden scramblerskive forbliver derimod på den samme placering det meste af tiden. Den bevæger sig nemlig kun når den første skive har roteret en hel omgang. Det kan samlingens med kilometertælleren i en bil, den rotor som viser de enkelte kilometer, rotere ofte. Når den er færdig med en omgang, det vil sige at den når tallet 9 skubber den til den næste rotor til 10'erne, en position fremad. Tilføjelsen af en ekstra scrambler har den fordel af krypteringsmønsteret ikke gentages, før den anden scrambler er tilbage til udgangspositionen. Hvilke med et fuldt alfabet på 26 betyder at det kræver 26 komplette omdrejninger af den første rotor eller en kryptering af 26*26

[5] Singh, Simon, Kode bogen, Gyldendal, 1999 (s. 144)

bogstaver i alt. Dette betyder at der er 676 kodealfabeter. Afsenderen af beskeden indtaster et bestemt bogstav, dette krypteres så efter et ud af hunderede kodealfabeter, og det næste bogstav der indtastet krypteres efter et nyt kodealfabet. Og på grund af at Enigma er en elektrisk maskine kan dette foregår yderst effektivt, grundet scramblerens automatiske bevægelse og elektricitetens hastighed.[6]

I bilaget ses den standard krypteringsmaskine som Scherbius designede. Her er der tilføjet en ekstra rotor(også kaldet scrambler), den tilføjelse gjorde at maskinen opnåede mere kompleksitet. Det gjorde samtidig også at der var endnu flere scamblerindstillinger, nemlig 26*26*26 eller 17.576. Oven i det er der tilføjet en reflektor, den minder om den måde at det er en gummiskive med ledninger indvendig, dog roterer den ikke og ledningerne kommer ud fra samme side som de kom ind. Reflektoren har den funktion at når afsenderen indtaster et bogstav, som sender et elektrisk signal gennem scramblerne, og når reflektoren modtager signalet sender den det tilbage gennem de tre samme scramblere bare med en anden rute. Samtidig med det blev der også tilføjet en koblingstavle, den vises dog ikke i bilaget men det er mellem tastaturet og den første scrambler. Koblingstavlen kan gøre at afsenderen indsætter ledninger, hvis virkning er at nogle bogstaver byttet rundt inden det når den første rotor.

Ud fra alle ovenstående oplysninger kan regne på hvor mange mulige nøgler der er:

Scramblerorienteringer. Hver af de tre scramblere kan sættes i én ud af 26 stillinger, det er derfor 26*26*26 indstillinger:	17.576
Scramblernes rækkefølge. De tre scramblere (1, 2 og 3) kan anbringes i hvilken som helst af følgende seks placeringer: 123, 132, 213, 231, 312 og 321:	6
Koblingstavle. Antallet af måder hvorpå man kan, og derved ombytte, aeks par af bogstaver ud af 26:	100.391.791.500
I alt. Det samlede antal nøgler er produktet af disse tre tal: 17.576*6*100.391.791'500≈	10.000.000.000.000.000

[7]

[6] Singh, Simon, Kode bogen, Gyldendal, 1999 (s. 146)
[7] Tal til tabellen er fra: Singh, Simon, Kode bogen, Gyldendal, 1999 (s. 150)

Rækkefølgen af hver enkel rotor, og deres respektive orienteringer og ledningsføringen i koblingstavlen bliver tilsammen, den nøgle som skal bruges til at dekryptere beskeden. Det er dette tal som gjorde at man mente at Enigma var ubrydelig. For modtageren af den krypterede besked, var det simpelt at dekryptere den, da man havde kendskab til nøglen. Men for den fjende som ønskede at dekryptere teksten, var der altså 10.000.000.000.000.000 forskellige nøgler, der skulle afprøves. Det var samtidig også en forbedring fra tidligere benyttede systemer, fordi dette var en elektrisk maskine så den arbejdede væsentligt hurtigere end tidligere. Førhen brugte man papir og blyant til at kryptere nu brugte man en maskine, så Scherbius' ide om at forbedre tidligere måder at kryptere på lykkedes.

Enigma havde også svagheder, det var dog ikke maskinen i sig selv. Det var brugen af den som gav den sine svagheder. Folkene som udarbejdede kodebøgerne forsøgte at sikre scramblerindstillingerne ved at gøre dem uforudsigelige. Scramblerne måtte derfor ikke have den samme position to dage i træk. Scramblerne kunne for eksempel have numrene 1, 2, 3, 4 og 5, første dag er rækkefølgen 134, på anden dagen kunne det være 215 men ikke 214, da rotor nr. 4 ikke må være på samme plads som dagen før. Dette gjorde det lettere for kryptoanalytikerne at dekryptere, da afsenderen eller kodebogens ophavsmand indskrænkede antallet af mulige til halvdelen. [8]

Monoalfabetisk kryptosystem, additive kryptosystemer:

Det monoalfabetiske kryptosystem er den af de mest simple måder at kryptere på, også en af de første. Denne måde af kryptering benyttede Julius Cæsar i De galliske Krige (58-50 f.Kr.). Her valgte Julius Cæsar at bruge en meget simpel nøgle, han valgte at erstatte bogstaverne fra klarteksten med bogstaver som stod tre pladser længere fremme i alfabetet. Dette kunne for et eksempel se sådan ud:

Klartekst	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å
Kryptotekst	D E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C

[8] Singh, Simon, Kode bogen, Gyldendal, 1999 (s. 179)

Her er alfabetet blevet parallelforskudt med tre. Det ses også her at når alfabetet slutter, startes der blot forfra. Det ovenstående er altså Cæsars substitutionsalfabet. Det følgende eksempel viser brugen af det monoalfabetiske additive kryptosystem:

Klartekst	JULIUS CÆSAR
Kryptotekst	MXOLXV FAVDU

Denne parallelforskydning som i dette tilfælde er sket med tre, kan også beskrives med k. Med det menes at hvis k=29 vil klartekst alfabetet og kryptoalfabetet være identiske. Vælger man i stedet at k=30, vil kryptoalfabetet være det samme som når k=1.[9] Ud fra dette kan man konkludere at man på denne måde, får 29 forskellige kryptosystemer. Hvoraf den ene, altså K=0 er triviel. Disse kryptosystemer er kaldet additive kryptosystemer, hvor tallet k er kryptosystemets skift. Julius Cæsar benyttede altså sådanne et system med et skift på 3, altså k=3.

Det er dog ikke altid man har kendskab til nøglen. Her bliver man derfor nødsages til at lave en kryptoanalyse af et monoalfabetisk kryptosystem. Når man læser danske tekster, kan man erfare at bogstaverne E, T, N og R forekommer hyppigt. Hvorimod bogstaverne X, W, Z og Q forekommer sjældent. Ud fra en forskellig samling danske tekster, med sammenlagt 50.000 bogstaver er man kommet frem til en frekvens fordeling, som ses i bilag. Disse frekvenser kan være med til at løse en kryptotekst hvor man ikke kender nøglen.

For teksten oplyses det at klarteksten er på dansk og krypteringen er foretaget via et monoalfabetisk kryptosystem:

VOFGHU ØQDZHUÅ TUF YQBTÅUF CA ACFHUB GØCJAIG CX

YQBG XCTU JUB ØÅQFUAIG CX CA ØQXU ÅZÅÅU ACFHUB

GØCJAIG JQF TUN AZBTGHU QV JCFUG GAP JUBBUF Z

YQØØURQØØUGØCJUB

[9] Landrock, Peter, Kryptologi, Abacus, 1990 (s. 9)

Antallet af de forskellige bogstaver tælles, ses i bilag. Hvorefter man ud fra hvor ofte de forskellige bogstaver forekommer, kan finde e. Bogstavet er det det nemmeste at finde, da det er det bogstav som benyttes mest når der skrives på dansk. Samtidig med det kan i findes, da det ligesom e forekommer hyppigt, dog ikke så ofte som e. I er samtidig det et af de få bogstaver, som kan stå alene og samtidig danne et ord. Det bogstav som er brugt mest i ovenstående kryptotekst er u, derfor må dette være vores e, altså U→e. Samtidig med det er det eneste bogstav som står alene z, derfor må Z→i. Man kan nu blot med disse oplysninger lave et substitutionsalfabet, ligesom Cæsar.

Klartekst	A B C D E F G H I J K L M N O P Q R S T U V X Y Z Æ Ø Å
Kryptotekst	Q R S T U V X Y Z Æ Ø Å A B C D E F G H I J K L M N O P

Her er der gjort det samme som med eksemplet med Cæsar, alfabetet er blevet parallelforskudt. Her er skiftet på 15, hvorimod Cæsars var 3. Når kryptoalfabetet er fundet, kan teksten løses, ved blot at aflæse fra ovenstående skema. Så når teksten bliver dekrypteret står der:

FØRSTE KAPITEL DER HANDLER OM MORTEN SKOVMUS OG

HANS GODE VEN KLATREMUS OG OM EN KAGE PIPPE MORTEN

SKOVMUS VAR DEÆ MINDSTE AF VORES SMÅ VENNER I

HAKKEBAKKESKOVEN

Der er dog en enkelt fejl i denne tekst, i tredje linje, ordet ”deæ” findes ikke. Derfor formoder jeg at afsenderen af denne kryptotekst har lavet en fejl. Dette kunne skyldes at der rigtig skulle have stået ”den”, og at der derfor benyttes n som det sidste bogstav. Dog har det ikke den større indflydelse på forståelsen af teksten, da det som det eneste ord, ikke giver mening.

Denne krypteringsmetode er en simpelmåde at kryptere på, derfor kunne den ikke benyttes under 2. verdenskrig. Da den var for simpel, og derfor for nem for fjenden at bryde. Grunden til at den var så simpel, var at det monoalfabetisk. Altså en hver forekomst af bogstavet Q i kryptoteksten svarer til et og samme bogstav i klartekst alfabetet. Det er

grunden til at denne måde at kryptere på er så følsom, da det kan løses nemt med noget simpel statistik.

Polyalfabetiske kryptosystemer:

Den polyalfabetiske mode at kryptere på, er sikret mod de statiske indgreb da et bogstav fra kryptoteksten, kan repræsentere mere end et bogstav fra klartekst alfabetet. Blaise de Vigenère dannede sådan et kryptosystem. Det system han designede bruger flere monoalfabetiske kryptosystemer til at kryptere. Antallet af monoalfabetiske kryptosystemer og hvilke af dem, afgøres af et "repeterende" nøgleord.

Vigenères tableaut bruges når man krypterer efter det polyalfabetiske kryptosystem, denne tabel ses i bilag. Det er svarer lidt til samme skema som kan bruges til monoalfabetiske krypteringssystemer, det har jeg dog ikke valgt at have med i min forklaring af de monoalfabetiske systemer, da det ikke var relevant for den dekrypterings opgave jeg havde fået. Men Vigenères skema har dog en lille modifikation, at skiftene i venstre side er blevet erstattet af klartekst alfabetet.[10] Et eksempel kan være hvis ordet "POLY" vælges som nøgle og ordet "KRYPTOSYSTEMER" som det som krypteres. Her skrives nøglen over klarteksten, og hvis klarteksten er længere end nøglen, gentages nøglen blot:

Nøgle	P O L Y P O L Y P O L Y P O
Klartekst	K R Y P T O S Y S T E M E R

Dette er anderledes fra den monoalfabetiske hvor klarteksten stod øverst. I ovenstående tabel er det bogstav som står over klarteksten et P. Herefter benyttes Vigenère tableauet hvor man vælger den række hvor P er bestemt. Denne række fastlægger nu et monoalfabetisk kryptosystem, som kan benyttes til at kryptere K. Derfor krypteres K til Z. Lignende finder vi over klarteksten R er bogstavet O fra nøglen. Her bruges rækken som er bestemt ved O til at kryptere R til C. Det vil sige at når man krypterer med denne tabel, er bogstaverne fra nøglen den øverste række i tabellen hvorpå rækken til venstre er klarteksten.(Denne forklaring, kræver at man sidder med Vigenères tableaut, som er i blag)

[10] Landrock, Peter, Kryptologi, Abacus, 1990 (s. 14)

Og ved at se hvor de "støder" sammen, får det bogstav krypteret. Forstsætter vi denne metode ender vi med:

Nøgle	P O L Y P O L Y P O L Y P O
Klartekst	K R Y P T O S Y S T E M E R
Kryptotekst	Z C G K F Å A T E E P H T C

[11]

Det vigtige ved dette eksempel er at bemærke at både E og Y krypteres til T, og S og T krypteres til E. Det er nemlig det som gør at det er et polyalfabetisk kryptosystem, da der er blevet brugt flere forskellige alfabeter til at kryptere med. I eksemplet er det blevet brugt fire forskellige alfabeter til krypteringen, altså P, O, L og Y-alfabeterne, da det var nøglen. Kryptosystemets periode er antallet af alfabeter.[12]

Hvis tekst skal dekrypteres ifølge Vigenères tableaut, skrives nøglen over kryptoteksten, her gentages nøglen hvis klarteksten er længere:

Nøgle	P O L Y P O L Y
Kryptotekst	D M O Q X Ø P I
Klartekst	R Ø D V I N E N

For at dekryptere denne tekst finder man alfabetet ved P, derefter man finder bogstavet i den krypterede tekst, i dette tilfælde D. Man aflæser så ude på aksen ude til venstre hvad klarteksten bogstav er, derfor bliver D til R. Denne fremgangsmåde bruger man med hele ordet, selvfølgelig så med det alfabet som at høre til. Her skrives klarteksten nederst. Der er to er samme bogstav i klarteksten, nemlig N, men ikke to ens bogstaver i kryptoteksten. Dette viser igen hvordan det polyalfabetiske kryptosystem virker. At brugen af de forskellige alfabeter, gør at to ens bogstaver ikke krypteres ens, og ligeledes at to ens krypterede bogstaver ikke nødvendigvis er det samme. Dette er derfor væsentlig mere sikkert end det additive monoalfabetiske kryptosystem. Fordi man her har brug for en nøgle og samtidig med det er der flere alfabeter.

[11] Eksemplet er fra: Landrock, Peter, Kryptologi, Abacus, 1990 (s. 15)
[12] Jf. Landrock, Peter, Kryptologi, Abacus, 1990 (s. 15)

Svagheden ved dette krypteringssystem er blandet andet, tiden det tog at kryptere. Det er en forholdsvis tidkrævende proces i forhold til at benytte en Enigma-maskine. Derfor var Enigma-maskinen en forbedring. At bryde en polyalfabetisk krypteret besked, er markant sværere end at bryde en monoalfabetisk. Det skyldes grundende som er beskrevet tidligere. Det er dog ikke umuligt, ved hjælp af kryptoanalyse kan det lade sig gøre. **Mere?**

Tysklands brug af Enigma:

Tyskernes brug af Enigma var meget central når det kom til ubåde. Kommunikationen mellem ubådene kunne ændre udfaldet af en given situation. Tyskerne "jagtede" enkelte konvojer tilhørende de allierede. Målet med at jagte disse både med forsyninger, var at sænke dem, så briterne og amerikanerne ikke kunne komme frem med forsyningerne. Man ville efter at have fundet placeringen på en af de allieredes konvoj, bruge man Enigma til at kommunikere med de andre ubåde. Hvor man ville afsløre deres placering, og derfor få flere ubåde til at hjælpe med at synke konvojen. Dette skete ved et koordineret angreb. Udover at bruge Enigma til at rapportere og kontrollere placering af ubåde i Atlanterhavet, brugte man den også til at videregive oplysninger om bombeoffensiver, flytning af militære enheder og hvor lastninger af militære forsyninger foregik. Derfor var det jo en del af den tyske militære strategi at benytte Enigma-maskinen, da den var med til at videregive vigtige oplysninger og derfor bidrog til måden Tyskland førte krig på.

Som tidligere skrevet har Enigma-maskinen i sig selv, ingen svagheder. Men hvordan den tyskerne brugte den, skabte dens svagheder. Alan Turning som arbejde ved Bletchley Park, bemærkede et vis mønster i de meddelelser som Bletchley Park oplagret. Ud fra det mønster der var, mente Alan Turning at man via afsendelsestidspunktet kunne forudsige indholdet af en given meddelelse. Hans erfaring viste at tyskerne sendte en krypteret vejrudsigt, hver morgen klokken seks. Så de meddelelser som man hos Bletchley opsnappede lidt efter seks, ville højst sandsynlig eller næsten helt sikkert inde holde ordet wetter. Dette gav folk som var interesseret i at dekryptere deres beskeder, chancen for lettere at lykkedes med det.

Hvordan brydes Enigma:

Det var i Polen man begyndte at forsøge at brude Enigma. Dette skyldes at Polen var mistænksom da det kom til Tyskland hensigter, efter 1. verdenskrig. Derfor da tyskerne i 1920'erne startede med at bruge denne maskine, gjorde Polen sit for at knække koden. Her valgte man matematikere fra den vestlige del af landet, som havde været en del af Tyskland indtil 1918. Derfor kunne de tale flydende tysk. Den mest bemærkelsesværdige af disse matematikere var Marian Rejewski, hans anslag mod Enigma var fokuseret på gentagelse, og gentagelse fører til mønstre. De fik også hjælp fra Frankrig, som ikke selv mente oplysningerne var noget værd, de fik nemlig kodebøger. Disse kodebøger modtog franskmændene fra en tysk spion, Schmidt. Det skal dog siges at Rejewski og hans kollegaer, ikke fik gavn af disse bøger, da man fra højere stillinger mente at, ved ikke at fortælle om kodebøgerne kunne forberede sig på tiderne hvor man ikke længere fik kodebøger. Rejewski måtte opgive i 1938, da tyskerne valgte at optimere Enigma-maskinen, ved at sætte to ekstra scramblere på. Polen var på den måde forud for deres tid, da man i England og Frankrig havde set Enigma for at være ubrydelig. Men med det nye håb startede kryptoanalysen for alvor i England. I England foregik kryptoanalyserne i Bletchley Park, her oprettede de et stort opsnapningsnetværk som skulle indsamle den krypterede trafik til kodebryderne på Bletchley. De informationer man ved Bletchly Park skaffede, blev med tiden kaldt Ultra.

Umuligt for england at vinde på havet uden kode, se link

Engelsk krigsstrategi efter bruddet på Enigma:

Jeg har i besvarelsen af betydningen for den engelske krigsstrategi, valgt at fokusere på den britiske flåde. Da jeg mener at det giver et udmærket billede af hvilken betydning det havde. Destroyeren HMS Petards tilhørte den engelske flåde, kampstatistikken for den var meget enestående, med det menes at det var eneste allierede skib som sænkede hver af de tredje fjendtlige flåder.[13] Det afgørende for nedkæmpelsen af de tyske ubåde, var fundet af det vigtige materiale til en forandret tysk Enigma-maskine, som havde modstået alle engelske forsøg på afkodning. Den tyske efterretningstjeneste fandt aldrig ud af, at to

[13] Harper, Stephen, Enigma, Broe 2011 (s. 7)

britiske sømænd fra destroyeren gav nøglen til at bryde tyskernes tophemmelige kodemaskine, Enigma.

Det tyske ubådshovedkvarter i Lorient i Frankrig, ledte de tyske ubåde ved hjælp ad radioforbindelser mellem de enkelte ubåde og hovedkvarteret. Dette foregik i kode, skrevet i Enigma. I maj 1941 lykkedes det at erobre en Enigma-maskine. Denne maskine gjorde at den britiske flåde kunne følge korrespondancen mellem henholdsvis hovedkvarteret og ubådene. Dette gjorde at briterne kunne danne klarhed over antallet af ubåde, hvor de befandt og hvor tyskerne planlagde et angreb. Dette er en klar fordel for briterne, og dette var blandt andet med til at sørge for sejren ved Atlanterhavet.

Et eksempel på hvordan den engelske krigsstrategi ændrede sig, kunne være dette: Den første bombe med fire roterer kom i drift i juni 1943, kunne man ved Bletchly Park med succes aflæse Triton-trafikken. Grunden til den tyskernes nye Enigma-maskine fik navnet Triton, var på grund af at den blev opkaldt efter den græske halvgud, Triton. Denne græske halvgud skabte store storme ved at blæse i en konkylie. Englænderne kaldte den dog Shark. Den vigtigste nøgle til de første afkodninger af signalerne fra Shark, blev fundet søndag den 13 december. Dette var kun seks uger efter sænkningen af U-559. Seksuger tidligere havde man erobret dokumenter og koder som skulle hjælpe folkene i Bletchley Park med at bryde koderne. Dette skete dog efter ti kritiske måneder, hvorpå englænderne ikke havde haft mulighed aflæse de tyske ubådes trafiksignaler.[14] Senere på dagen d. 13. december, begyndte løsningerne på Enigma-meddelelserne at vise sig, dette var meddelelserne mellem ubåde og hovedkvarteret. En time efter afkodningerne sendtes, opsnappede meldinger til Admiralitetets ubådsporingslokale, de afslørede positioner på femten ubåde. På grund af disse afsløringer kunne amerikanske konvojer kunne komme med forsyninger til Nordafrika, uden tab. Dette lykkedes kun på baggrund af Ultras afsløringer, da man kunne undgå ubådskobler da deres position ikke længere var ukendt. Grunden til at dette eksempel kunne bruges var at amerikanerne var blandt Englands allierede. På baggrund af afsløringerne fra Ultra, var amerikanerne i stand til at undgå disse ubådskobler. Dette viser hvordan dekrypteringen af Enigma, var med til at hjælpe og ændre den engelske strategi, da man ud fra de kendte positioner kunne omlægge ruter for at undgå dem eller angribe dem.

[14] Jf. Harper, Stephen, Enigma, Broe 2011 (s. 82)

Samtidig i Nordafrika fik Bernard Montgomery den 8. Armé. Bernard Montgomery var en forsigtig taktiker men god taktiker, som passede godt på sine mænd. Han kunne takket være efterretninger fra Ultra, maksimere fordelen han havde. Han kommanderede lige under 200.000 mænd, over 100 kampvogne og umådelige reserver af benzin og ammunition. Den 23. oktober i 1942 slog Montgomery så til ved el-Alamein. Her tilintetgjorde han fjendens frontlinjer, i de efterfølgende nærkampe gjorde det overtal af briterne udfaldet. Dette betød at kampvognene som tilhørte Bernard Montgomery fik så god fremdrift, at de ikke kunne standses.[15]

Et eksempel hvor man angriber i stedet for at undvige var under den konstante atlantiske kamp, hvor fordelen for begge grupper lå i at placere sig i et område midt i Atlanterhavet. Grunden til dette var at de var udenfor luftfartstøjers rækkevidde. Derfor mente Sir Arthur Harris, at en bedste måde at angribe ubåde på, var ved at bombardere deres baser og værfter, som de blev bygget på. Det viste sig så at denne form for angreb ikke kunne betale sig, da ingen ubåde tog skade. Men det derimod var luftvåbnet som led store tab.

D-day: se strategier

Det stod fra starten klart for England, at det måtte forhindres at tyskerne opdagede at Enigma var blevet brudt. Gik det op for den tyske ledelse at Enigma ikke længere var sikker, ville de sandsynligvis bare ændre på maskinen, ved at tilsætte en ekstra scrambler eller gøre brug af en anden krypteringsmetode. Hvilke ville gøre alt arbejdet både fra de allieredes side, men så sandelig også fra polakkernes side, overflødig. Når det var sagt skulle de allierede jo heller ikke lade så stor en fordel, gå til spilde.

”Jeg kan ikke forestille mig, at der siden oldtiden, om nogensinde, har været udkæmpet krig, hvor den ene side konsekvent har kunnet aflæse de vigtigste militær- og flådeefterretninger hos den anden.”[16] Har tidligere kryptoanalytiker Stuart Milner-Barry udtalt sig. Denne udtalelse viser hvor meget Enigma og bruddet af den betød. Det gav de allierede en markant fordel, da man kendte til tyske operationer og tyske placeringer. Derfor kunne de allierede planlægge ud fra hvad de vidste om fjenden, tyskerne. Dette er jo en stor fordel da, de efter at havde knækket Enigma kunne ’’overvåge’’ tyskerne, uden at de var klar over det. I en amerikansk rapport stod der: ”(…) Følelsen af at kende sin fjende er

[15] Davies, Norman, Europa i krig, Gads 2009 (s. 116)
[16] Singh, Simon, Kode bogen, Gyldendal, 1999 (s. 200)

enormt betrykkende. Den vokser umærkeligt som tiden går, hvis man regelmæssigt og tæt har indblik i hans tanker og veje og vaner og handlinger. Denne slags viden gør ens egen planlægning mindre foreløbig og mere selvsikker, mindre sindsoprivende og mere ukuelig."[17] Dette viser igen at man på grund af bruddet af Enigma, kunne planlægge meget bedre og blev mere sikker i sin planlægning. Bruddet på Enigma koden fik stor betydning for krigsførelsen. Den engelske flåde brugte det blandt som tidligere sagt, til at finde fjendens placering. Når man kendte til placeringen af fjenden kunne man undgå dem og planlægge ruter ud fra dem. Samtidig var det ikke kun England alene som fik gavn af det, også deres allierede, USA, fik gavn af dette. De kunne nemlig som tidligere nævnt fragte deres forsyninger til Nordafrika, uden tab. Samtidig med dette var det med at gøre udfaldet for kampene på Atlanterhavet. Det var selvfølgelige ikke bruddet på Enigma, der var den eneste faktor som gjorde udfaldet af disse kampe. Men afsløringen gjorde at det blev nemmere at planlægge og tilrettelægge i forhold til tyskerne. Selvom tyskerne havde prøvet at gøre den ellers ubrydelige kode, endnu sværere at bryde ved at modificere Enigma-maskinen. Slaget på Atlanterhavet startede til tyskernes side, men ved hjælp fra Ultra vendte England det 180 grader. Takket være Ultras afsløring af tyske ubådes placeringen gjorde de det mulig for de allierede at sænke disse ubåde, således også konvojerne. Samtidig havde man også succes ved de tyske forsyningslinjer i Middelhavet til Afrika. Informationerne fra Ultra gjorde at det tyske tab af ubåde steg og steg, dette gjorde at man valgte at trække ubådene tilbage fra Nordatlanten i maj 1943. Konvojslaget dét var vundet. Dette ville ikke være sket uden hjælp fra Ultra, man havde ikke kendt tyskernes placeringer. Kendskabet til deres placeringer gjorde at man som tidligere nævnt, kunne planlægge ruter som undgik dem, og derfor komme frem med forsyningerne. Man planlagde dog ikke kun ruter væk fra fjenden, men sørgede også for at angribe dem. Så disse oplysninger var både med at hjælpe på den defensive plan, men også den offensive. Jeg mener ikke at man uden bruddet på Enigma ville have vundet kampen på Atlanterhavet. Alene det at de vandt kampene på Atlanterhavet mener jeg viser, hvor stor en indflydelse det havde på måden udfaldet var. Havde de englænderne ikke brudt Enigma, havde Tyskland fortsat den markante fordel på havet. **Mere?**

Konklusion:

[17] Singh, Simon, Kode bogen, Gyldendal, 1999 (s. 201)

Scherbius mål: forbedre lykkedes, udgangspunkt i cifferskiven monoalfabtisk

Indflydelsen det fik, vurder