Kryptering i sjøforsvaret

Sondre Granlund Moen

27.06.17

Innhold

MERKNAD: dette dokumentet er ugradert. Det vil gjøre at mye av det som ble sagt på fremføringen vil du ikke finne igjen her. Dette gjør også at mye av informasjonen er forkortet ned.

Hva er kryptering?

Ordet kryptografi kommer fra gresk og betyr «skjult tekst». Kryptering innebærer at man koder informasjon på en slik Måte at kun den som kjenner koden kan lese informasjonen. Kryptering benyttes også for å autentisere (verferisere) Informasjon. For eksempel kan man benytte digitale signaturer for å bekrefte identiteten til en avsender av en e-post. Det kan også defineres som en matematisk metode som sørger for konfidensialitet ved at informasjon ikke kan leses av uvedkommende. Informasjonen «låses ned» med en nøkkel og kan ikke leses før man har låst den opp igjen med riktig nøkkel. Nøkkelen som brukes til å låse opp trenger ikke være den samme som ble brukt til å låse ned informasjonen.

Symmetrisk kryptering

Symmetrisk kryptering innebærer at det benyttes samme nøkkel til å låse ned og låse opp informasjon. Denne nøkkelen må utveksles mellom avsender og mottaker på en sikker måte. Cæsar- siffer er et eksempel på symmetrisk kryptering. Det er også dette papirnøklene tar utgangspunkt i.

Asymmetrisk kryptering

Asymmetrisk kryptering kalles også offentlig nøkkelkryptering (public key). Man benytter et nøkkelpar: en privat og en offentlig nøkkel, som er matematisk relatert til hverandre. Den offentlige nøkkelen kan gjøres tilgjengelig for hvem som helst, og den private er kun kjent av nøkkelens eier. Selv om det er en matematisk sammenheng mellom de to nøklene, så kan ikke den ene utledes av den andre. Den offentlige nøkkelen kan fritt distribueres. Gyldighet og ekthet på den offentlige nøkkelen må imidlertid kontrolleres og administreres.

Kravet til nøkkellengde er forskjellig ved bruk av disse metodene.

Historie:

Egypterne

Den tidligste kjente form for kryptering var egyptiske skribenter som ca 1900f.kr byttet ut hieroglyfene med andre. Alstå endret på figurene slik at du leste feil.

Cæsar- siffer (alfabetet)

En annen tidlig krypteringsmetode var Cæsar-metoden som ble brukt ca 50 år f.kr. Den gikk ut på å forflytte alle bokstavene i alfabetet et visst antall plasser. Det vil si om nøkkelen er 3, så vil bokstaven «a» bli erstattet med «d». Denne metoden brukte Cæsar for å sende meldinger til sine generaler.

Marconi- radiobølger

Etter dette kom Radiobølger som var en stor endring. Dette gjorde det lettere å kommunisere lengre unna. Men problemet med krypteringen her var når fienden tokk opp frekvensen din så kunne dem tyde hva du snakket om i kodespråk.

Første verdenskrig

I 1914 klarte britene å knekke koden til tyskerne. Noe som gjorde at mange av angrepene til tyskerne ble sabotert

I 1917 klarte britene å dekode en melding som ble sendt bra Zimmerman som var en offisert høyt oppe i det tyske systemet.

I denne meldingen så sendte Zimmerman er forespørsel til Mexico, hvor han ba dem angripe USA som var nøytral i krigen foreløpig.

Men etter at britene lekket denne informasjonen til USA så ble de med i krigen.

Andre verdenskrig

Mekanisering av kryptering under andre verdenskrig.enigma sinn modell 19:13 minutter

Polakkene var de første til å knekke enigma. Dette gjorde dem uten å ha sett en enigma selv. Men de hadde et par problemer som de sleit med.

Det ene var hvordan tastaturet fungeret og det andre var at tyskerne byttet kode daglig.

Så de måtte spørre britene om hjelp. Britene var som sagt veldig dedikerte til å knekke krypterte koder og hadde en egen avdeling som bare skulle knekke koder.

Denne avdelingen med Allen Turan i spissen klarte til slutt og knekke enigma. Noe som var veldig viktig for å få slutt på krigen

Dagens kryptering går mye inne i data med bruk av det binære systemet.

Kryptering i sjøforsvaret

Forteller hvor vi setter krypto på fregatten og at det er likt på de andre fartøyene.

Så forteller jeg litt om nato changeling call sign:

NCCS er kallesignalene til fartøyene til nato som blir brukt på plain linjer. Dette for at vi skal kunne snakke med hverandre uten krypering.

Dette består da av 2 bokstaver og et tall. Disse blir byttet hver dag ved 00:00Z. Eller etter bestemte tidspunkter under en øvels

Landstasjoner 3 bokstaver: LBJ

Plain linje er en linje som er uten krypto, mens secure er linje med krypto

Kanister: den grå greia til høyre er en kanister med viss antall krypto-nøkler inni seg. Dette er den papirkryptoen som blir brukt i forsvaret pr dags dato.

Men det er inne i en digitaliseringsperiode, hvor Raskl og digitale nøkler er på vei inn.

Vernman-metoden er den nærmeste metoden jeg fant ut av som lignet på den metoden som blir bruk på fartøyene men kan ikke si med helt sikkerhet på grunn Av gradering.

Krypteringsutstyr

Her forteller jeg kort om hva slags instrumenter som blir brukt for at det skal være en slags linje for videre delen av fremføringen min

Her snakker jeg litt om hva som blir brukt til å laste inn nøklene på krypteringsinstrumentene

KYK-13

kan ha lastet inn opptil 6 nøkler omgangen. Bruker en Koi-18 for å laste nøklene inn på den. Mye brukt når du skal sette flere nøkler samtidig.

Koi-18

kan kun laste en nøkkel om gangen. Den kan heller ikke lagre nøkler på seg og kan ha problemer med å lese nøkkelen.

RASKL

Kan ha over 40 nøkler lastet inn samtidig. Er det nyeste innen for kryptolasting og er framtiden til krypto. Denne er akkurat på vei inn i sjøforsvaret.

KW-46/ KWR

Denne blir brukt til å kryptere og dekryptere signaler som kommer til fartøyet. KWR er noe av det viktigste vi har når det kommer til samband i sjøforsvaret. Noe som ligner er XOMAIL

Dette på grunn av det er denne som gjør det mulig for oss å motta alle meldingene som sendes til oss på Kringkasteren.

Kringkasteren er en slags TV-kanal som du setter på (en viss frekvens). Denne mottar da alle signalene som blir sendt i nordområde som er på denne kringkasteren. Disse blir først sendt via FOH også sender de det videre inn på kringkasteren.

Du lytter alltid på denne. Det er altså lytteplikt når du drar fra kai på denne. Får en landkanal til å ta inn signalene når du ligger til kai.

Det finnes mange forskjellige kringkaster kanaler rundt omkring i verden. Her i Norge har vi hovedsakelig to kanaler, men kun den ene som blir brukt hele tiden.

Når du skal få denne KWR til å funke må man laste inn 3 forskjellige nøkler og taste inn mange forskjellige kodesystemer for å få den opp å gå. Er en misfornøyd så begynner den å pipe som faen.

Hvis denne havner ute av sync. Altså mister signalet på grunn av fjell, nordlys osv så kommer det en forferdelig pipe lyd som egentlig er skadelig høy.

Da må du så kjapt som mulig komme i sync innen 30 minutter. Hvis ikke det er mulig så må du sende melding til FOH at du er ute av sync.

VOICE-kryptering

Klar tekst går inn i en analog til digital konverter og blir til data tekst.

Datateksten blir så kryptert ved hjelp av en CIK også går den via et moden som også er kryptert. Dette gjelder spesielt datakryptert voice.

Dette er ikke den som finnes på norske fartøy men er kun en boks for å vise poenget.

TCE-621

Dette er da boksene som blir brukt på skolen for å drifte fis Basis. Disse krypterer da IP-adressene til pcene som er koblet til nettverket

Det vil si at du må ha en slik boks med samme type krypto for å da få opp fis Basis.

Bruker en CIK som ligner på et helt vanlig kort. Også bruker den papirnøkkel.