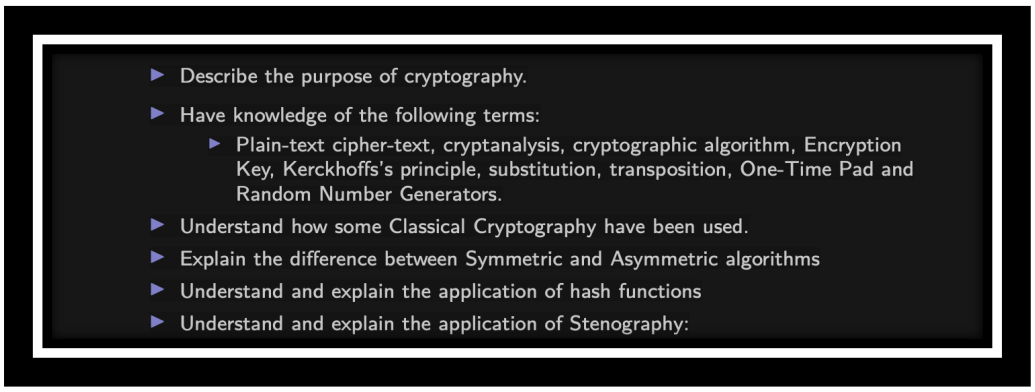
Introduction cryptography

Etter å ha fullført denne ukas presentasjon skal jeg kunne klare:



HVORDAN KAN VI SIKRE VÅRE RESSURSER?

Identify

- Assets – (inventory system, asset management)
- Potential threats – (threat modeling, risk assessment)

Prevent

- Block attacks – (authentication, access control, encryption, firewall)
- Reduce vulnerabilities – (static/dynamic code analysis, software updates, vulnerability penetration testing)

Detect

- When an incident happens or shortly after – (monitoring systems, logs, malware scan, intrusion detection systems, integrity checksums/hashes, digital signatures)

Respond

- Be able to respond to stop attacks and prevent further damage – (intrusion prevention systems, shutting down and rebuilding the system)

Recover

- Correct copy of the data can be reloaded from backup

Vi kan på et vis si at kryptografi kan deles i to deler. Den matematiske vitenskapen som håndterer transformasjon av data for å gjøre dens betydning uforståelig (det vil si å skjule dens semantiske innhold), forhindre uoppdaget endring av den, eller forhindre uautorisert bruk.

CRYPTOANALYSIS: Også har vi den matematiske vitenskapen som handler om analyse av et kryptografisk system for å skaffe kunnskapen som trengs for å bryte eller omgå beskyttelsen som systemet er designet for å gi.

WHAT IS CRYPTOGRAPHY?

It is a Greek word meaning hidden text or writing.
Crypto = hidden
Graphy = writing or text

WHAT IS ENCRYPTION?

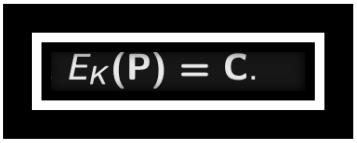
(På norsk er det kryptering)
Kryptering: er den kryptografiske transformasjonen av data (kalt 'klartekst') til en annen form (kalt 'chiffertekst') som skjuler den opprinnelige betydningen til dataen og forhindrer at den opprinnelige formen blir brukt.

DIFFERENT CONCEPTS

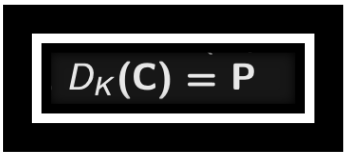
- PLAIN TEXT **P** – tekst som kan leses av alle
- CIPHER TEXT **C** – tekst som er kryptert, ikke leselig for noen utenom de som har nøkkelen til å dekryptere den.
- ENCRYPTION KEY **K** - nøkkelen som brukes til å dekryptere
    - Samme krypteringsnøkkel (K) kan brukes for kryptering og dekryptering (dette kalles symmetric encryption)

- Når ulike nøkler brukes for kryptering og dekryptering kalles det asymmetric encryption

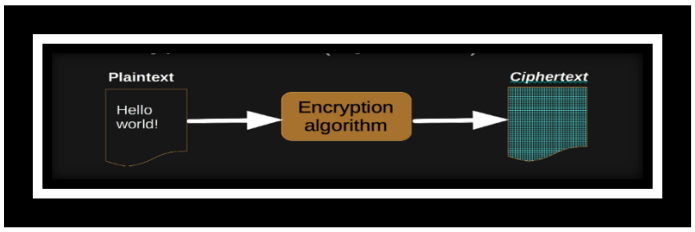
- THE ENCRYPTION FUNCTION **E** – funksjonen som P (vanlig tekst) er sendt gjennom for å få C (cipher tekst)



- THE DECRYPTION FUNCTION **D** – funksjonen som cipher teksten sendes gjennom for å få vanlig tekst



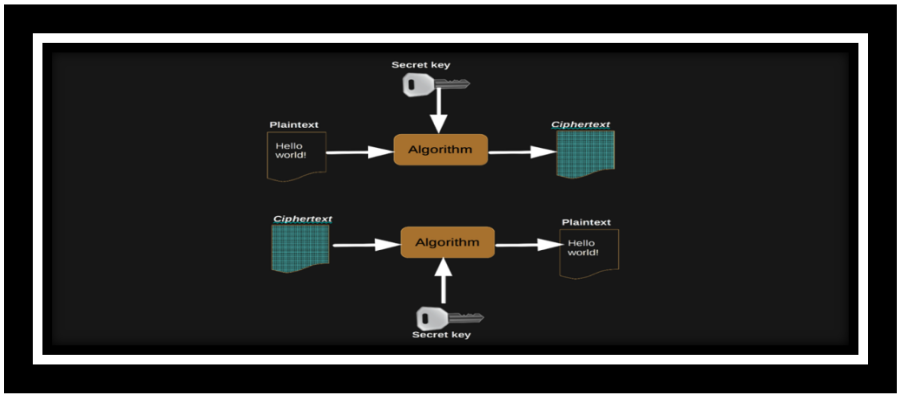
Kryptert tekst (cipher) og algoritmer er to type operasjoner brukt i kryptografi.



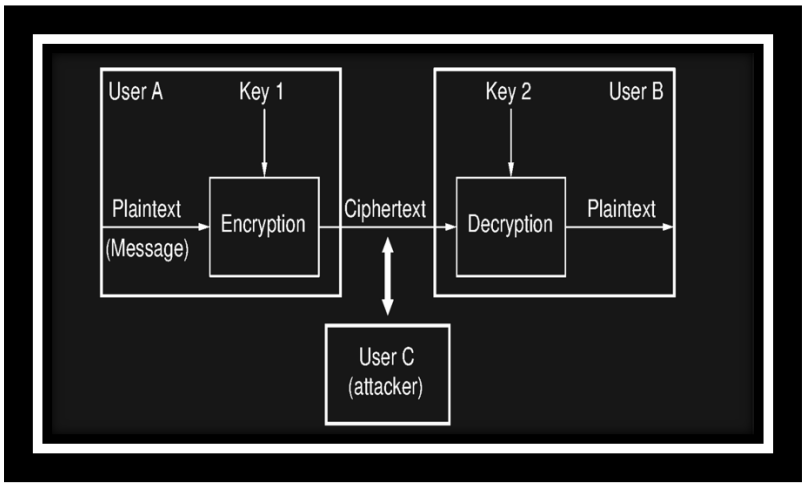
PRINSIPP:

"Kerckhoffs prinsipp: Et kryptografisk system skal være sikkert selv om alt om systemet, bortsett fra nøkkelen, er allment kjent."

Annet tilfelle hvor algoritmen er kjent men en hemmelig nøkkel tilføres til algoritmen:



Hvis noen skal prøve å hacke dette vil dette skje på den hemmelige teksten slik som bildet under viser:

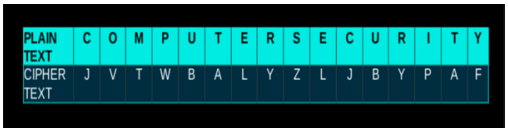


HVORFOR BRUKE KRYPTOGRAFI?

- **Konfidensialitet**: At data ikke blir avslørt for systementiteter med mindre de er autorisert til å kjenne til dataen.
- **Integritet**: At dataen ikke er blitt endret på en uautorisert måte siden den ble opprettet, overført eller lagret.
- **Autentisering**: Prosessen med å verifisere en påstand om at en systementitet eller systemressurs har en bestemt attributtverdi.
- **Autorisasjon**: En godkjenning som gis til en systementitet for å få tilgang til en systemressurs.
- **Non-repudiering**: Sikrer at avsenderen ikke kan nekte for å ha sendt meldingen.

De to grunnleggende byggesteinene i alle krypteringsteknikker er:

- Substitusjon: En metode for kryptering der elementer i klarteksten beholder sin sekvensielle posisjon, men blir erstattet av elementer i chifferteksten.



EKS:

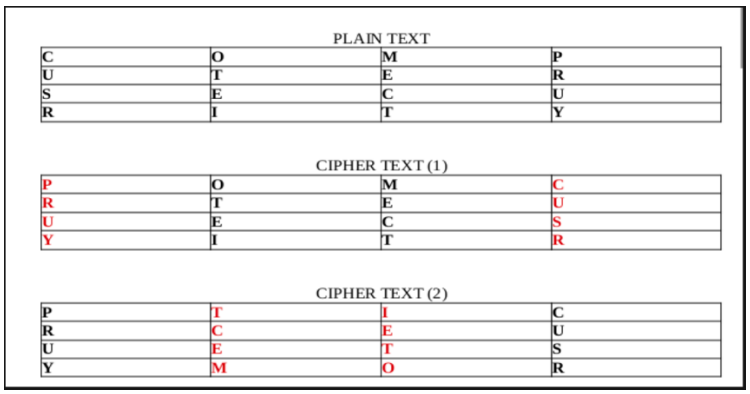
La oss si at vi har følgende klartekst: "HELLO."

I substitusjonskryptering erstatter vi hver bokstav med en annen bokstav i henhold til en bestemt regel. For eksempel kan vi erstatte hver bokstav med bokstaven som kommer etter den i alfabetet. Resultatet vil se slik ut:

Klartekst: H E L L O Chiffertekst: I F M M P

Her har vi beholdt rekkefølgen av bokstavene, men erstattet dem med andre bokstaver for å lage chifferteksten. Dette er et enkelt eksempel på substitusjonskryptering.

- Transposisjon: En metode for kryptering der elementer i klarteksten beholder sin opprinnelige form, men gjennomgår en endring i sin sekvensielle posisjon



PLAIN TEXT

C	O	M	P
U	T	E	R
S	E	C	U
R	I	T	Y

CIPHER TEXT (1)

P	O	M	C
R	T	E	U
U	E	C	S
Y	I	T	R

CIPHER TEXT (2)

P	T	I	C
R	C	E	U
U	E	T	S
Y	M	O	R

La oss si at vi har følgende klartekstsetning: "THE QUICK BROWN FOX."

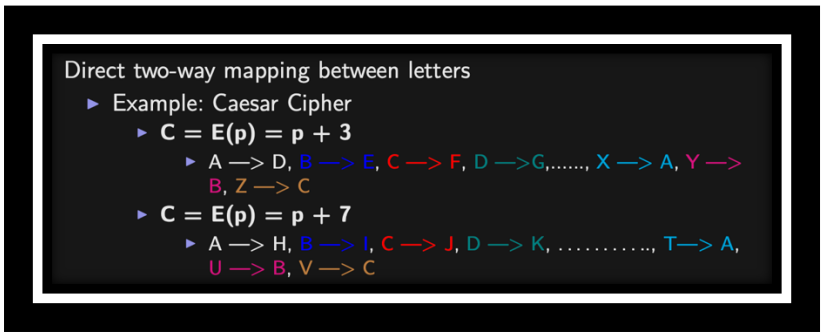
I denne krypteringsteknikken kan vi bare endre rekkefølgen på ordene i setningen, og klarteksten vil fremdeles beholde sin opprinnelige form:

Klartekst: "THE QUICK BROWN FOX." Chiffertekst: "BROWN THE FOX QUICK."

Her ser vi at alle bokstavene og ordene i klarteksten forblir uendret, men rekkefølgen på ordene er endret. Dette er et eksempel på transposisjonskryptering, der klarteksten ikke mister sin opprinnelige form, men sekvensen av elementer er endret for å lage chifferteksten.

CAESAR CIPHER

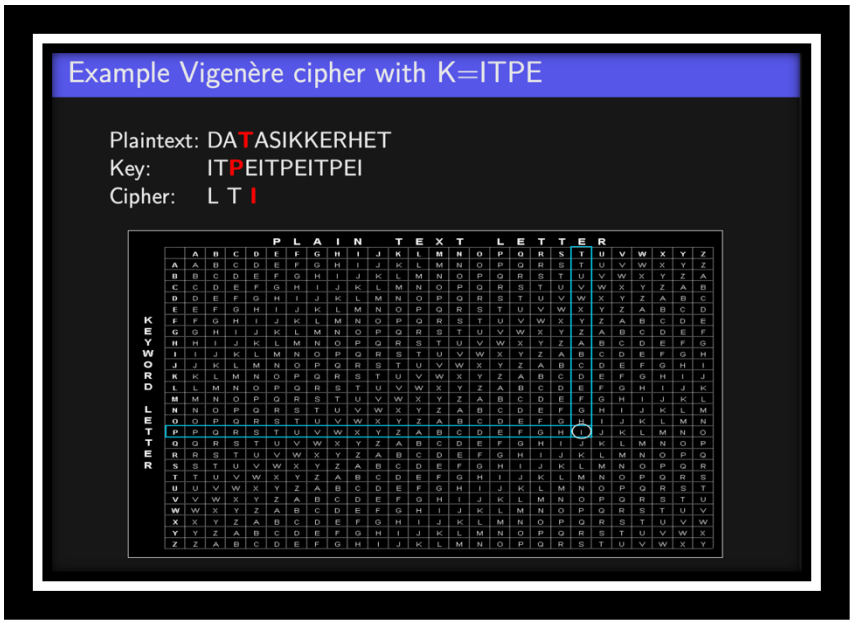
Den tidligste bruken av substutisjon cipher var med caesar cipher. Det involverte at man bytter hver bokstav i alfabetet med en bokstav som kommer tre plasser lenger ned i alfabetet.



Ulempene med denne typen kryptering er at det lett kan knekkes med brute force blant annet.

VIGNERE CIPHER ble designet slik at hver bokstav ikke ble kodet med den samme bokstaven eller tegnet. I stedet for å bruke et alfabet som i caesar, brukes flere. Vi sier at Vignere bruker polyalfabetisk substutisjon (polyalpabetic substituion). Vignere ciphernøkkelen defineres som K og "ITPE" er nøkkelen som brukes for å bestemme skiftverdiene som brukes til å kryptere teksten.

POLYALFABETISK SUBSTUTISJON: en bokstav kan kartlegges til flere bokstaver.



ONE-TIME PAD VERNAM CIPHER

What is a one-time pad (engangsnøkkel)?

En krypteringsalgoritme der nøkkelen er en tilfeldig sekvens av symboler, og hvert symbol brukes bare en gang for kryptering – det vil si, brukes for å kryptere bare ett klartekstsymbol og dermed produserer bare ett krypteringssymbol – og en kopi av nøkkelen brukes tilsvarende for dekryptering.

For å sikre en gangs bruk, blir kopien av nøkkelen som brukes for kryptering, ødelagt etter bruk, slik også kopien som brukes for dekryptering.

En slik one-time pad er en perfekt krypteringsplan fordi den er vurdert uknekkelig dersom den er implementert riktig. Dette var oppfunnet av Gilbert Vernam.

FOR AT ENGANGSNØKKELEN SKAL VURDERES UKNEKKELIG:

- Funnet opp av random verdier
- Brukt kun en gang
- Sikker distribusjon til der til skal
- Sikret hos sender og mottaker sider
- Må være minst like lang som meldingen

Hvorfor engangsnøkler ikke brukes i praksis?
For at en engangsnøkkel (One-Time Pad) skal være sikker, må man opprette en tilfeldig hemmelig nøkkel som er like lang som klarteksten og bruke den kun én gang. Av denne grunnen forlater man begrepet perfekt sikkerhet til fordel for andre mer praktiske kryptografiske algoritmer.

RANDOM NUMBER GENERATOR

En prosess for å generere tilfeldig sekvens av verdier (vanligvis i bits) eller en enkelt tilfeldig verdi.

Hvorfor trenger vi dette i kryptografi?

- Nøkkel generering (Key Derivation Functions (KDFs) er brukt til å generere nøkler som er oppfunnet av tilfeldige verdier)
- Salting (tilfeldige bits ofte brukt av passord hash funksjoner)
    - Hash funksjoner spiller en viktig rolle når det kommer til integritet
- Nonces (tilfeldige biter av string ofte brukt i time-stamping)
    - En nonce står for number used once. Det er en tilfeldig generert bitstreng eller tallverdi som brukes en gang i kryptografisk sammenheng.
      AUTHENTICATOR APPEN

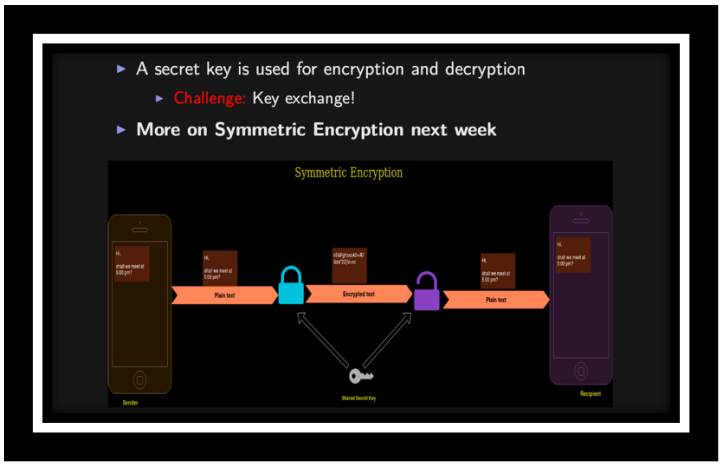
MODERN CRYPTOGRAPHY

Modern cryptography uses advanced mathematical functions to disort the content of documents and messages. There are two different main categories of modern cryptography:

- Symmetrical cryptography
    - Classical cryptography was based solely on symmetric cryptography
- Asymmetric cryptography

SYMMETRIC CRYPTOGRAPHY

Er en bransje innenfor kryptografi I hvilke algoritmen bruker samme nøkkel for begge deler av den kryptografiske operasjonen (kryptering og dekryptering).

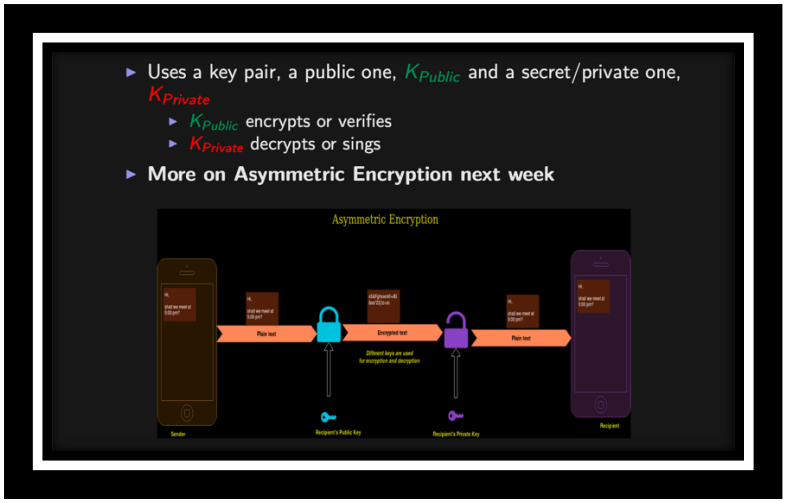


SYMMETRIC CRYPTOGRAPHY

En moderne gren av kryptografi (kjent som offentlig nøkkelkryptografi) der algoritmene bruker et par nøkler (en offentlig nøkkel og en privat nøkkel) og bruker en forskjellig komponent av paret for hver av de to tilhørende kryptografiske operasjonene (for eksempel kryptering og dekryptering, eller opprettelse av signatur og verifisering av signatur).

Offentlig nøkkelkryptografi:

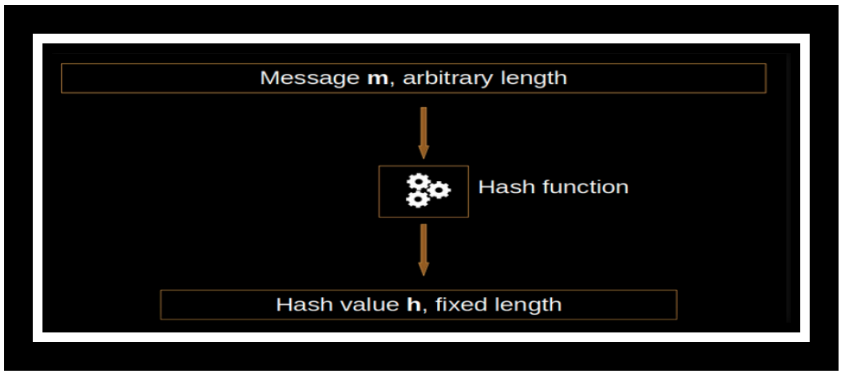
1. **Offentlig nøkkel (Public Key):** Dette er nøkkelen som er kjent for alle og brukes til å kryptere meldinger. Den kan sammenlignes med en postboks der alle kan legge en melding inni, men bare mottakeren med den tilsvarende private nøkkelen kan åpne og lese meldingen.
2. **Privat nøkkel (Private Key):** Dette er nøkkelen som er kjent bare for mottakeren og brukes til å dekryptere meldinger som er kryptert med den offentlige nøkkelen. Den er som en nøkkel til postboksen som lar mottakeren åpne og lese meldingene som er lagt inn der.



En god kryptoalgoritme kjennetegnes av at den er basert på solid matematiske prinsipper, den har blitt analysert av eksperter og funnet safe, den passerer tidens test, som i at ingen har funnet svakheter med den så langt.

HASH FUNKSJONER

Noen ganger er det ønsket å unngå kryptering, men samtidig å holde integritet. En måte å løse dette problemet på er ved å bruke enveis hash funksjon. Denne opererer på inndata av vilkårlig lengde og produserer utdata av fast lengde.



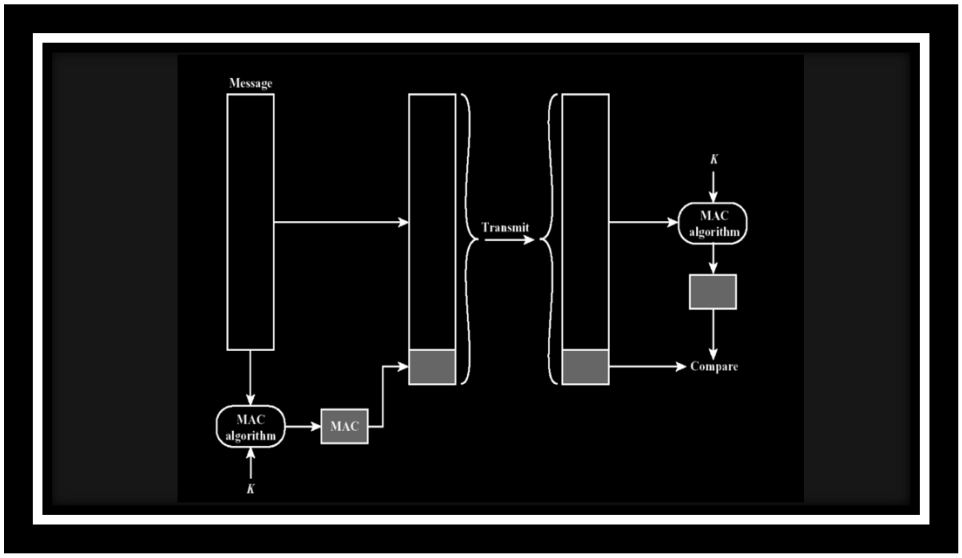
- Gitt en melding m, er det enkelt og raskt å regne en hash-verdi h
- Gitt meldingen m, skal en hash-funksjon alltid produsere den samme hash-verdien h for den samme meldingen m (Deterministisk)
- Gitt en hash-verdi h, er det vanskelig å beregne meldingen m slik at hash-funksjonen H produserer H(m)=h
- Det er vanskelig å beregne et unikt par (x,y) slik at H(x)=H(y) (collision resistance)
    - Collision resistance: krever at hash-funksjonen forhindrer en angriper fra å opprette to ulike dokumenter med samme hash-verdi.

Her er eks på noen kryptografiske hash-funksjoner

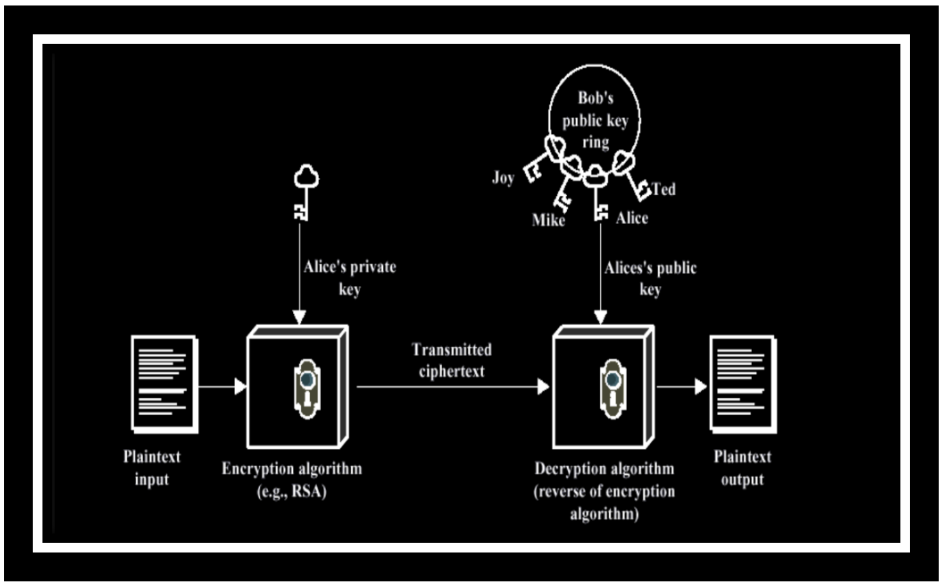
- MD5
    - Utviklet I 1991
    - Ble brukt I programmer for password og fil integritet
    - Anbefales ikke å bruke MD5 fordi det er utsatt for mulige collision attacks
- SHA-1, SH-2 and SHA-3
    - Utviklet I 1993
    - Ansees som utrygg, ikke lenger anbefalt
- BLAKE and BLAKE2

- RIPEMD-160, RIPEMD-256 and RIPEMD-320
- Whirlpool

Vi ønsker å sikre integritet ved å sørge for at innholdet ikke endres underveis.
Dette kan gjøres med en meldingsautentiseringskode (MAC) eller digital signering av meldingen.



Digital signering under:



STEGANOGRAFI

- Gresk ord som betyr å skjule eller dekke tekst eller skriving i annen data
    - Ulik kryptografi som skjuler meningen til en melding, men skjuler ikke meldingen i seg selv

- Å gjemme en representasjon av data i noe annet
    - Et bilde eller en lydfil

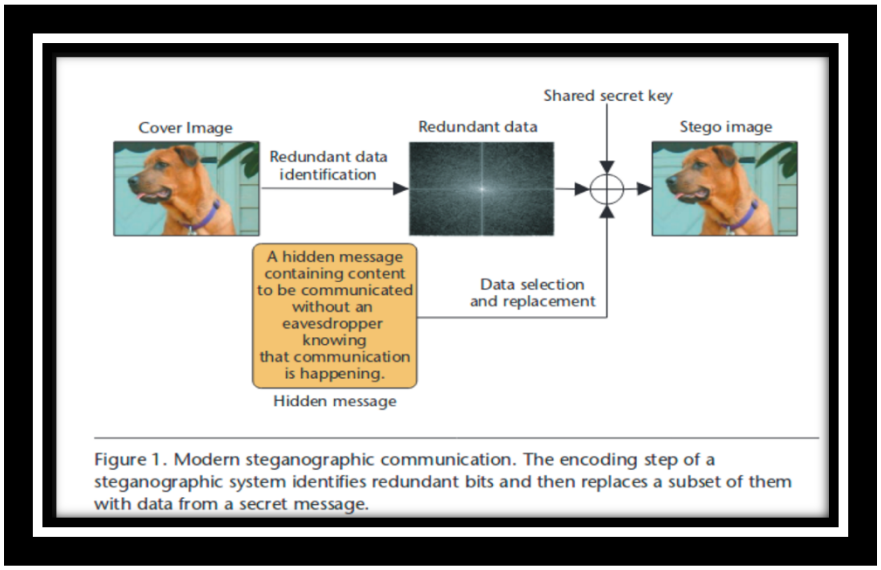


Figure 1. Modern steganographic communication. The encoding step of a steganographic system identifies redundant bits and then replaces a subset of them with data from a secret message.