T-F01

**KRYPTERING**

Notater:

* Brukere og prosseser trenger adgang til ressurser
* Nøkkel brukes til lagring av konfidensiell data
* Angriperen kan ha en samling av kryptogram, klartekst/kryptogram(known plain attack), (chosen plain text attack) angriper kan velge hvilke klartekst fra samlingen av kryptogram. Chosen ciphertext attack er når samlingen av kryptogram/klartekst par for kryptering valgt av angriper. Denne er veldig sårbar.
* Brute Force er når man prøver alle nøkler K og sjekke om Dk(C) ser ut som en sannsynlig klartekst
* E har høyest frekvens (frekvensanalyse) som betyr av hvis en tekst har en høy frekvens består den mest sannsynlig av en E bokstav
* Substitusjon kan gjøres med binære tall og kan unngå å erstatte hele bokstaver, denne gjør frekvensanalyse vanskeligere.
* One Time Pads er umulig å knekke , benytter en tabell med shift nøkler
* 3DES kan krypteres av og DES kan krypteres av angripere.
* Advanced Encrypted Standard
* CBC er en kjede med krypterings blokker som er avhengig av hverandre og hvis man mister en blokk mister du alle krypteringsblokker.
* Windows Encrypted File Systems (EFS) er det innebygd kryptering og bruker AES som default (kan bruke 3DES og DESX) . Beskytter ikke hvis et program er logget inn med rettigheter til å lese
* Stream cypher krypterer en og en bit data og er sårbar
* Ikke mulig å få tilbake 65 siden informasjon ble borde når man regnet og dermed er enveis og ikke kan komme tilbake.
* En OpenSSL bibliotek er anbefalt for kryptering for det er lett å snuble i krypteringen (manuelt).

1. **Hva er kryptering**

Kryptering er når to parter kan kommunisere med hverandre over eller via en usikker kanal som kan overvåkes (eve) eller avlyttes . Hvis man har blitt enige om en symmetrisk krypteringsmetode og en hemmelig nøkkel så kan meldingen sendes kryptert (nøkkel Dk(C)) så kan mottakeren dekryptere

meldingen og lese den.

Hvis informasjonen er kryptert er den dermed sikker. Hvis informasjonen er kryptert og man ikke vet hvordan den er kryptert er den ikke sikker, og dette er en indikasjon på at den er dårlig designet.

Kryptering er den viktigste teknikken for å gjennomføre retningslinjer for å sikre systemet.

Viktig at det er en til en relasjon mellom antall bits i arrayet

1. **Hva er substitusjonschiffer**

Bytte ut et tegn med et annet tegn, Hver bokstav erstattes med en annen

A erstattes med N for eksempel. Substitusjon kan gjøres med binære tall og kan unngå å erstatte hele bokstaver, denne gjør frekvensanalyse vanskeligere.

Kryptering AL1 er en enkel form for koding (teknisk sett ikke kryptering)

1. **Kan man bruke subsitusjon på binærtall?**
   * **Ja**
   * Nei
2. **Hva er «One-Time pads» og er dette sikkert?**

One Time Pads eller engangsblokker praktisk sett umulig å knekke. benytter seg av en tabell med shift nøkler til å kryptere en ren tekst

Nøkkelen må være like lang som klarteksten Nøkler må aldri gjenbrukes

1. **Hva står «AES» for?**
   * **Advanced Encryption Standard**
   * Advanced Encryption Substitusjon
   * Artifact Encounter Selection
2. **Hvilke av disse er «AES» versjoner?**
   * **AES-128**
   * AES-156
   * **AES-192**
   * AES-124
   * AES-128
   * **AES-256**
   * AES-520
3. **Er «AES» 100% sikkert?**

AES har ingen kjente svakheter den må knekkes med et brute force angrep og for å kontrollere utfall av brute force må man lagre det

AES kan dermed ikke krypteres lett den eneste måten er å få tak i nøkkelen. Brukerens passord er det eneste svakeste leddet.

Trenger mye elektrisitet (all elektrisitet på jorda) for å brute force(utføre dekryptering) (knekkes) AES 256 versjonen.

AES klarer ikke å krypteres av stater fordi arbeidsmengden er for stor, dermed er AES generelt sett ganske sikkert.

AES har en input:128 bit , output : 128 bit

Nøkkel:128,192,256 bit.

Krypterer en og en blokk (Blokkchiffer) , dette er en kompleks krypteringmetode som er designet for datamaskiner.

1. **Hva er asymetrisk kryptering (public key kryptering)**

Asymmetrisk kryptering tar i bruk en offentlig nøkkel og en privatnøkkel. Den ene brukes for kryptering mens den andre brukes for dekryptering.

Alice sender en krypter melding til bob med sin offentlige nøkkel og beholder den private nøkkelen for seg selv, og Bob dekrypterer meldingen ved hjelp av sin private nøkkel. Krypterer melding altså med den offentlige nøkkelen og dekrypterer med den private.

RSA og ECC er eksempeler på det , ECC brukes mest i dag.

Dette er en krypteringsmetode som bygger på noen egenskaper ved primtall det er vannskelig, Det er kostbart og tidskrevende å faktorisere store tall .

4 M primrall under 10 G(millioner( blir ofte sjeldenere)

1. **Hva er Symmetrisk kryptering?**

Symmetrisk kryptering er når det brukes en nøkkel til å kryptere og dekryptere informasjonen. Eksempel er når Alice sender en Klartekst til Bob via en kommunikasjonskanalen som er overvåket eller avlyttet av Eve. Da blir Alice og Bob enige om en felles nøkkel K som brukes både for å kryptere og dekryptere meldingen.

fordi den bruker én nøkkel til å kryptere og dekryptere informasjon, mens dens motstykke, asymmetrisk kryptering, bruker en offentlig nøkkel og en privat nøkkel

Symmetrisk kryptering

1. **Er «RSA» Symetrisk eller asymetrisk?**
   * Symetrisk
   * **Asymetrisk**
2. **Er «AES» Symetrisk eller asymetrisk?**
   * **Symetrisk**
   * Asymetrisk
3. **Forklar hvordan en person ville startet en samtale med «RSA», men senere byttet til «AES» like etter. Hvorfor ikke bruke «AES» hele tiden? Eller hvorfor ikke bare bruke «RSA»?**

RSA er ikke en kvantesikker metode, men det er AES . Hvis en person starter en samtale med RSA vil både dekrypteringsnøkkelen fra krypter

1. **Hva er en kryptografisk nøkkel?**

En kryptografisk nøkkel består av en rekke /lengde med bits som tas i bruk av en kryptografisk algoritme for å transportere ren tekst til chiffertekst eller motsatt. Nøkkelen kan vare symmetriske eller asymmetriske og brukes til å kryptere eller dekryptere informasjon avhengig av om den er symmetrisk eller asymmetrisk. Det brukes også i meldingsautentisering ,nøkkel transport og innpakning osv. Jo lengere nøkkelen er desto vanskeligere er det å kryptere dataen som kan være tidskrevende. En sender og en mottaker har både en privat og en offentlig nøkkel i asymmetrisk kryptering og i symmetrisk er det en fellesnøkkel som partene blir enige om. Denne brukes til både kryptering og dekyptering.

1. **Forklar hva SHA-256 er?**

Secure hash algorithm er utviklet av NSA og godkjent av NIST

SHA-256 er 256 bit og er hash algoritmen som er sikre selv om det er publisert angreps teknikker mot dem. Denne er den andre utgivelsen av SHA som kom ut i 2002 og det finnes også i 512 bit (SHA-512) .Etter SHA-2 ble det utviklet SHA-3 ,men den brukes ikke mye i dag.

Det er en hash funksjon h tranformerer en klartext P til en verdi x=h(P)

Kryptografisk hash funksjon skal være enveis.

Dette brukes for å sikre fil/melding som ikke er endret.