T-01
KRYPTERING

1) Hva er kryptering

Kryptering er den viktigste teknikken for å gjennomføre retningslinjene for å sikre systemet. Kryptering kan forklares som en matematisk metode som sørger for konfidensialitet ved at informasjon ikke kan leses/forstås av uvedkommende

2) Hva er substitusjonschiffer

Å bytte ut tegn med ett annet. For eksempel så kan man forskyve hele alfabete slik at bokstaven «A» blir bokstaven «N», «B» blir «O» osv...

3) Kan man bruke subsitusjon på binærtall?

- Ja
- Nei

4) Hva er «One-Time pads» og er dette sikkert?

One-time pads er en type kryptering der man benytter en tabell med shift-nøkler. One-time pads skal i prinsippet være umulig å knekke, men svakheten for denne typen er at nøkkelen må være like lang som klarteksten det vil si at skal du kryptere en bok så må nøkkelen være like lang som boken. En annen ting som også er viktig er at nøkkelen **ALDRI må gjenbrukes!** Brukes nøkklene omigjen så er dette ikke sikkert!

5) Hva står «AES» for?

- Advanced Encryption Standard
- Advanced Encryption Substitusjon
- Artifact Encounter Selection

6) Hvilke av disse er «AES» versjoner?

- AES-128
- AES-156
- AES-192
- AES-124
- AES-256
- AES-520

7) Er «AES» 100% sikkert?

Vi kan si at selve krypteringen er sikker, men vi kan ikke si at AES er 100% sikker uten å vite hvordan nøkkelen er delt. Så for å kunne snakke med hverandre sikkert må man bruke en nøkkel som er sikker, den nøkkelen er som oftest sendt med RSA som er «sikker» men krevere flere ressurser enn AES. Poenget ender med at AES ikke er sikkert så lenge man ikke vet om nøkkelen er delt på en sikker måte.

På dette spørsmålet kan man både argumentere for ja og nei og hva som blir riktig vil være avhangig av hvordan du begrunner svaret dit.

8) Hva er asymetrisk kryptering (public key kryptering)

Bob har to nøkler en privat nøkkel som må holdes hemmelig og en offentlig nøkkel som gis ut til «alle». Så når for eksempel Alice skal sende en meling til Bob så trenger hun Bob sin offentlige nøkkel som hun krypterer meldingen med og sender den til Bob dermed er det bare Bob sin private nøkkel som kan dekryptere meldingen og lese hva som står.

9) Hva er Symetrisk kryptering?

Alice og Bob deler en hemmelig nøkkel som brukes både til kryptering og dekryptering. Altså her må begge vite/ha nøkkelen for å lese meldingene

10) Er «RSA» Symetrisk eller asymetrisk?

- Symetrisk
- Asymetrisk

11) Er «AES» Symetrisk eller asymetrisk?

- Symetrisk
- Asymetrisk

12) 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»?

For at samtalen skal være sikker så må den krypteres og vi vet at for å kunne kommunisere over AES så må man dele en nøkkel, nøkkelen må deles på en sikker måte som nevnt i spm 7. Så for at nøkkelen skal deles sikkert brukes RSA. RSA algoritmen er ressurs tung i forhold til AES og vi ønsker dermed ikke å bruke denne mer enn nødvendig, dermed byttes det over til AES når den hemmelige nøkkelen er delt og resten av kommunikasjonen fortsetter med AES.

13) Hva er en kryptografisk nøkkel?

En kryptografisk nøkkel er en nøkkel/parameter som avgjør hvilke resultat den kryptere informasjonen vil vise. Har man korrekt nøkkel så vil man kunne se den rette informasjonen, er nøkkelen feil så vil man mest sannsynelig ikke forstå noe av informasjonen.

14) Forklar hva SHA-256 er?

SHA-256 står for Secure Hash Algorithm – 256 bit og er en type hash funksjon som regnes som sikker.