

T-00

INTRODUKSJON

1) Hva er informasjonssikkerhet?

2) I forhold til informasjonsikkerhet hva står «C.I.A» for?

3) Forklar begrepene nedenfor (gi gjerne eksempler på begrepene også):

- **Kryptering**
- **Adgangskontroll**
- **Autentisering**
- **Autorisering**

4) Hva betyr Integritet? Hvordan kan man bevare integriteten til noe?

5) Hva betyr Tilgjengelighet?

6) Hva står begrepet «A.A.A» for? forklar kort hva hver enkelt «A» står for.

7) Er Cæsar Chiper en «sikker» måte å kryptere informasjon på?

- Ja
- Nei

8) Hva slags kryptografiske funksjoner er: «SHA-1» og «SHA-256» eksempler på?

- Dette er ikke kryptografiske funksjoner
- Dette er Hash funksjoner
- Dette kan man ikke svare på uten å vite hvilken algoritme klokkesyklusen på en datamaskin kjører.

9) Hva står «MAC» for?

- Message Authorization Certificate
- Message Authentication Codes
- Message Anonymity Controll
- Ingen av alternativene

10) Hva vil et «DOS» angrep bety?

11) Nevn de 10 prinsippene for sikker design av datasystemer og en kort beskrivelse av hver av de.