

# **T-01**

## **KRYPTERING**

**1) Hva er kryptering**

**2) Hva er substitusjonschiffer**

**3) Kan man bruke substitusjon på binærtall?**

- Ja
- Nei

**4) Hva er «One-Time pads» og er dette 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-128
- AES-256
- AES-520

**7) Er «AES» 100% sikkert?**

**8) Hva er asymmetrisk kryptering (public key kryptering)**

**9) Hva er Symetrisk kryptering?**

**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»?**

**13) Hva er en kryptografisk nøkkel?**

**14) Forklar hva SHA-256 er?**