IN2120 – Informasjonssikkerhet: Workshop uke 2: Kryptografi

Oppgave 1

1. **For hvilke informasjonstilstander (lagring, overføring, behandling) kan kryptografi brukes til å beskytte informasjon?**

Kryptografi kan brukes til å beskytte informasjon når den overføres via ubeskyttede nettverk eller lagres på steder med utilstrekkelig fysisk eller logisk tilgangskontroll. Såkalt homomorf kryptografi kan brukes til å beskytte data under prosessering i en mikroprosessor, dvs. at data holdes kryptert hele tiden. Problemet med homomorf kryptografi er at det bruker svært mye prosesseringskraft.

1. **Hvilke sikkerhetstjenester kan støttes av kryptografi?**

Kryptografi kan gi konfidensialitet, integritet og autentisitet (inkludert uavviselighet) av informasjon.

Oppgave 2