11174 Datasikkerhet

Øving 5

1. Oluf har en privat nøkkel R, en offentlig nøkkel P, en beskjed M og en hash-algoritme H[]. Forklar hvordan Oluf bruker nøklene for å signere beskjeden M og hvordan en mottaker kan verifisere at meldingen er fra Oluf.

2. Oluf og Lars har begge en identisk kopi av en symmetrisk nøkkel. Kan denne nøkkelen brukes til å autentisere meldinger mellom de to?

3. Gitt at staten påtar seg å opprette et eget nettsted www.offentlig.no med offentlige nøkler til alle innbyggere i Norge. Diskuter i hvilken grad dette ville ha løst nøkkeldistribusjons-problemet for innenlandsk kommunikasjon.

4. På side 177 (figur 6.7) i Stallings presenteres pseudokode for en algoritme som gjør det mulig å beregne a^b mod n. Implementer denne algoritmen i C. (Hvis det er ønskelig, kan oppgaven begrenses til eksponenter <256)