1. RSA-salaus on kommutatiivinen, jos käytetään yhteistä modulia. Schneier ehdottaa tällaisen RSA:n käyttöä lantinheittoprotokollassa (Schneier s.90). Onko yhteisen RSA-modulin käytöstä tässä haittaa? Mistä osapuolet saavat avainparinsa?

2. On myös ehdottettu kommutatiivisen salauksen käyttöä avaintenjakeluun. Alicella ja Bobilla on kommallakin oma salainen avain tai avainpari. Alice lähettää Bobille generoimansa istuntoavaimen seuraavasti: (E_A tarkoittaa salausta Alicen salaisella salausavaimella, D_A avausta Alicen salaisella avausavaimella.)

1.	$A \longrightarrow B$	$E_A(K_{SES})$
2.	$B \longrightarrow A$	$E_B(E_A(K_{SES})) = E_A(E_B(K_{SES}))$
3.	$A \longrightarrow B$	$D_A(E_A(E_B(K_{SES}))) = E_B(K_{SES})$

   Onko tämä avaintenjakeluprotokolla turvallinen tai voidaanko siitä muokata turvallinen, jos kommutatiivisena salauksena on

   (a) RSA yhteisellä modulilla

   (b) bittivirtasalaus

   (c) potenssiinkorotus modulo p, missä p on julkinen alkuluku, salausavain e on salainen satunnaisluku ja avausavain on salainen ratkaisu yhtälölle $ed = 1 \pmod{p-1}$. Salaus: $c = m^e \bmod p$. Avaus: $m = c^d \bmod p$.

3. Kuinka kaksi henkeä voi heittää noppaa sähköisten sanomien välityksellä niin, että toisen huomaamatta ei pysty huijaamaan? (Ulkopuolisia uhkia ei tarvitse huomioida.) Entä n henkeä?

4. Korjaa seuraavien protokollien keskeiset viat:

   (a) Wide-mouth-frog

   (b) salaisen avaimen Needham-Schröder

   (c) Denning-Sacco

   (d) julkisen avaimen Needham-Schröder

5. Onko autentikointi tehtävän 4 protokollissa (korjatuissa versioissa) eksplisiittinen vai implisiittinen eli varmistuvatko osapuolet siitä, että toisella todella on salainen avain hallussaan, vai selviääkö se vasta kommunikoinnin alkaessa?

6. Vertaa tehtävan 4 protokollien kustannuksia: yhteyksien määrää sekä sanomien määrää ja pituutta ja laskennan vaativuutta. Voidaanko laskentaa suorittaa *off-line*? Kuinka raskas on luotetujen osapuolien tehtävä? Tarvittaanko kelloja? Kuka generoi satunnaislukuja?