Tik-79.159 Tiedon salaus ja suojaus	kevät 98
Laskuharjoitus 10, viikko 15	Tuomas Aura, Antti Huima

1. On ehdotettu 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: $m = c^d \bmod p$.

2. Korjaa seuraavien protokollien keskeiset viat:

   (a) Wide-mouth-frog

   (b) salaisen avaimen Needham-Schröder

   (c) Denning-Sacco

   (d) julkisen avaimen Needham-Schröder

3. Onko autentikointi tehtävän 2 protokollissa (korjatuissa versioissa) eksplisiittinen vai implisiittinen eli varmistuvatko osapuolet siitä, että toisella todella on salainen avain hallussaan, vai selviääkö se vasta kommunikoinnin alkaessa?

4. Vertaa tehtävan 2 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?

5. Schneier (s. 515 alalaita) esittää Diffie–Hellman-protokollasta myös version, jossa käyttäjien julkiset DH-avaimet ovat allekirjoitettuina julkisessa hakemistossa. Istuntoavain kahden käyttäjän välille luodaan joka kerta näitä samoja DH-avaimia käyttäen.

   (a) Mitä ongelmia aiheutuu avaimen tuoreudelle?

   (b) Miten tuoreusongelma on ratkaistavissa? Salliiko protokolla edelleen lähettäjän aloittaa salauksen ennen avaintenvaihtoa?

6. Onko Otway–Rees-protokollan (Schneier s. 59) autentikointi implisiittinen vai eksplisiittinen (erikseen kumpaankin suuntaan)? (Vihje: protokolla ei ole aivan niin luotettava kuin Schneier antaa ymmärtää. Parantaisiko sarjanumeron korvaaminen satunnaisluvulla tilannetta?)