Tik-79.159 Tiedon salaus ja suojaus	
Tentin 20.5.1996 ratkaisut	Tuomas Aura

1. Arvostelu: Käsitteet osattiin harmittavan huonosti. Olisi ilmeisesti pitänyt painottaa niitä enemmän. Muiden tehtävien vastauksia olikin sitten ilo lukea.

   (a) Hybridisalauksessa itse sanoma salataan symmetrisellä salausmenetelmällä ja satunnaisella istuntoavaimella. Istuntoavain salataan vastaanottajan julkisella avaimella ja lähetetään vastaanottajalle erikseen tai sanoman mukana.

   Arvostelu: hyvästä esimerkistäkin sai pisteen.

   (b) EDE-moodi on kolminkertainen salaus, jossa ensin salataan, sitten avataan ja taas salataan eri avaimilla. (Usein ensimmäinen ja viimeinen avain ovat samoja.)

   (c) Informaatioteoreettisen salausmenetelmän turvallisuus perustuu siihen, ettei pelkässä salakielisessä sanomassa ole riittävästi tietoa avaamiseen. Sanomaa ei voi avata ilman avainta, vaikka hyökkääjällä olisi käytössä rajaton laskentakapasiteetti.

   (d) Autentikoinnissa varmistutaan sanomien alkuperästä eli kommunikaation vastapuolen henkilöllisyydestä. Vahva kryptografinen menetelmä on nähtävissä olevassa tulevaisuudessa turvallinen kaikkia ajateltavissa olevia hyökkääjiä vastaan, ainakin erittäin suurella todennäköisyydellä.

   Arvostelu: pisteen sai vain, jos oli jonkinmoinen käsitys siitä, millainen mentelmä on **vahva**.

   (e) BAN-logiikka on tietämyslogiikka, jolla tehdään päätelmiä kryptografisten protokollien osapuolten uskomuksista. Sillä voidaan osoittaa protokolla turvalliseksi, jos tietyt perusoletukset ovat voimassa.

   (f) Message Authentication Code MAC on symmetriseen menetelmään perustuva "allekirjoitus". Sanoma allekirjoitetaan ja sen alkuperä tarkistetaaan salaisen avaimen avulla.

   Arvostelu: avain on **salainen**. Hyvästä esimerkistäkin sai pisteen.

2. (a) $689^3 \bmod 4897 = 327082769 \bmod 4897 = 2345$. Ok.

   Arvostelu: Jotkut olivat laskenut 2345^3, missä ei ole mitään mieltä!

   (b) $3171 = 110001100011_{16}$.

$$
\begin{array}{llll}
1 & 4321^{2^0} \bmod 4897 & & = \mathbf{4321} \\
1 & 4321^{2^1} \bmod 4897 & = 4321^2 \bmod 4897 & = \mathbf{3677} \\
0 & 4321^{2^2} \bmod 4897 & = 3677^2 \bmod 4897 & = 4609 \\
0 & 4321^{2^3} \bmod 4897 & = 4609^2 \bmod 4897 & = 4592 \\
0 & 4321^{2^4} \bmod 4897 & = 4592^2 \bmod 4897 & = 4879 \\
1 & 4321^{2^5} \bmod 4897 & = 4879^2 \bmod 4897 & = \mathbf{324} \\
1 & 4321^{2^6} \bmod 4897 & = 324^2 \bmod 4897 & = \mathbf{2139} \\
0 & 4321^{2^7} \bmod 4897 & = 2139^2 \bmod 4897 & = 1523 \\
0 & 4321^{2^8} \bmod 4897 & = 1523^2 \bmod 4897 & = 3248 \\
0 & 4321^{2^9} \bmod 4897 & = 3248^2 \bmod 4897 & = 1366 \\
1 & 4321^{2^{10}} \bmod 4897 & = 1366^2 \bmod 4897 & = \mathbf{199} \\
1 & 4321^{2^{11}} \bmod 4897 & = 199^2 \bmod 4897 & = \mathbf{425}
\end{array}
$$

$$
\begin{array}{ll}
4321 \cdot 3677 \bmod 4897 & = 2449 \\
2449 \cdot 324 \bmod 4897 & = 162 \\
162 \cdot 2139 \bmod 4897 & = 3728 \\
4321 \cdot 199 \bmod 4897 & = 2425 \\
4321 \cdot 425 \bmod 4897 & = \mathbf{2255}
\end{array}
$$

Siis $4321^{3171} \bmod 4897$
$= 4321^{2^0} \cdot 4321^{2^1} \cdot 4321^{2^5} \cdot 4321^{2^6} \cdot 4321^{2^{10}} \cdot 4321^{2^{11}}$
$= 4321 \cdot 3677 \cdot 324 \cdot 2139 \cdot 199 \cdot 425 = 2255.$

Allekirjoitettu sanoma on $4321, 2255$.

(Tarkistus $2255^3 \bmod 4897 = 4321$.)

Arvostelu: Täydet pisteet sai laskuvirheistä huolimatta, jos muuten olisi mennyt oikein.

3. (a) Kaksisuuntaisessa X.509 autentikoinnissa B tarkistaa sanoman 1 tuoreuden aikaleimasta T_A. Yleensä B myös muistaa vanhat nonssit N_A niin kauan kuin niitä vastaava aikaleima on tuore. Näin B voi varmistaa, ettei hän vastaanota samaa sanomaa 1 toista kertaa aikaleiman voimassaoloaikana.

Kaksisuuntaisessa autentikoinnissa A päättelee sanoman 2 tuoreuden nonssista N_A. (Yleensä A myös tarkistaa aikaleiman T_B tuoreuden, mutta se ei ole välttämätöntä. Tällöin A voi myös muistaa vanhat nonssit N_B vastaavan aikaleiman voimassaoloajan, mutta sekään ei ole välttämätöntä. T_B ja N_B ovat periaatteessa tarpeettomia, sillä sanoman 2 tuoreus nähdään pelkästä nonssistakin.)

Vastaanottajan nimi (A tai B) on mainittu sanomissa, koska muuten hyökkääjä voisi ohjata sanoman väärälle vastaanottajalle. Tämä väärä vastaanottaja avaisi salatun istuntoavaimen omalla salaisella avaimellaan ja saisi tulokseksi jotain roskaa. Onneksi hyökkääjä ei tällöinkään saisi tietoonsa samaa istuntoavainta. Enemmän hyötyä nimien sanomassa olosta on, jos allekirjoituksesta ei suoraan näy lähettäjän nimi.

Arvostelu: kolme pistettä sai, jos keksi aikaleimoille, nonsseille ja nimille jotain käyttöä. Neljännen sai huomaamalla, että A ja B tarkistavat tuoreuden eri tavalla. Useimmat keksivät osasille jonkin tarkoituksen, mutta harva ymmärsi, miten niitä juuri tässä protokollassa käytetään.

(b) Protokollan onnistuneen suorituksen jälkeen A ja B tietävät kumpikin molemmat istuntoavaimet. Lisäksi A tietää, että B tietää istuntoavaimen K_{AB}. Jos A ja B luottavat toisiinsa, he luottavat istuntoavainten turvallisuuteen.

4. Tehtäväpaperissa on virhe, joka mainittiin tenttitilaisuudessa. Tehtävässä pitäisi lukea:

   ”Salataan sanoma DES-algoritmilla ensin 64 bitin CFB-moodissa (**Cipher FeedBack mode**) ja sitten uudelleen ECB-moodissa (Electronic Code Book mode) käyttäen samaa avainta.”

   CFB- ja ECB-moodien yhdistelmästä tulee yllättäen CBC moodi (Cipher Block Chaining), joten kaksinkertaisesta salauksesta ei ole yhtään mitään hyötyä. Vastauksen keksii helpoiten piirtämällä kuvan.

   Arvostelu: Tämän piti olla helppo ja hauska tehtävä, mutta kumma kyllä vain muutama oli huomannut yhtäläisyyden CBC-moodiin. Useimmat olivat konstruoineet yhdistelmän väärin, eivätkä osanneet sanoa siitä mitään järkevää. CBC-moodin ominaisuuksista sai pisteitä.

5. Diffie–Hellman-avaintenvaihdosta voi kertoa toimintaperiaatteen lisäksi monenlaisia asioita, joita löytyy oppikirjasta, luennoilta ja laskuharjoituksista sekä kirjallisuudesta.

   Arvostelu: Tarkoituksesta ja toimintaperiaatteesta sai 2 pistettä. Diskreetti logaritmi ja *man-in-the-middle* toivat 2 lisää. Mistä tahansa muista tarkennuksista, huomioista tai laajennuksista sai myös pisteitä. Tarpeettomista lisäehdoista ei tällä kertaa sakotettu.

6. Viimeiseen tehtävään pätee sama kuin edelliseen eli monenlaiset vastaukset voivat olla hyväksyttäviä.

   Arvostelu: Tämä osattiin ällistyttävän hyvin. 1–3 pistettä sai irtonaisilla tiedoilla, mutta 4–6 pisteeseen vaadittiin toimiva protokolla ja ymmärrettävä kokonaisuus.