Tik-79.159 Tiedon salaus ja suojaus	
Tentti 8.8.1996	Tuomas Aura

Kirjoita vastauspaperiin opintojakson numero ja nimi, päivämäärä, nimesi, opintokirjan numero, osasto ja vuosikurssi.

Vastaa **viiteen** (5) alle olevasta kuudesta tehtävästä. (Jos vastaat kaikkiin, jätetään tehtävä 6. arvostelematta.)

1. Selitä lyhyesti (1–2 riviä riittää)
   - (a) hybridisalaus (1p)
   - (b) CBC-moodi (1p)
   - (c) yksisuuntainen hajautusfunktio (1p)
   - (d) **vahva** kryptografinen algoritmi (1p)
   - (e) bittivirtasalaus (stream cipher) (1p)
   - (f) subliminaalinen kanava (1p).

2. Olet sopinut käyttäväsi salaisen asiamiehen A kanssa Diffie–Hellman-avaintenvaihtoprotokollaa moduulin arvolla $n = 1997$ (oikeasti luku olisi huomattavasti suurempi) ja kantaluvun arvolla $g = 999$. Vastaanotat A:lta sähköpostitse sanoman: "Julkinen Diffie–Hellman-avaimeni on $X = 1872$." Valitset omaksi salaiseksi avaimeksesi $y = 521$.
   - (a) Millä sanomilla avaintenvaihtoprotokolla jatkuu? Mikä tulee yhteiseksi salaiseksi avaimeksi?
   - (b) Mikä ratkaiseva asia jäi protokollassa huomioimatta?

3. Kolmisuuntainen X.509-autentikointi tapahtuu seuraavasti:

1.	$A \to B$:	$S_A[T_A, N_A, B, E_B[K_{AB}]]$
2.	$B \to A$:	$S_B[T_B, N_B, A, N_A, E_A[K_{BA}]]$
3.	$A \to B$:	$S_A[N_B]$

   - (a) Selitä yksityiskohtaisesti, kuinka vastaanotettujen sanomien tuoreus voidaan tarkistaa. (3p)
   - (b) Miksi istuntoavaimia on kaksi: K_{AB} ja K_{BA}? (1p)
   - (c) Kaksisuuntaisessa X.509-autentikoinnissa lähetetään vain kaksi ensimmäistä sanomaa. Miten kaksi ja kolmisuuntainen autentikointi eroavat toisistaan, eli mikä on kolmannen sanoman tehtävä? (2p)

4. Lagrange-$(2, 10)$-kynnysrakenteesta tunnetaan varjot (2,19535), (4,1583). Moduuli on 37813. Laske salainen sanoma.

5. RSA. (6p)

6. Kryptografia tietokoneen käyttäjän tunnistamisessa.

Huom. Arvostelen tentin kesäloman jälkeen, 1.9. mennessä.

Tik-79.194 Tietojenkäsittelyteorian seminaari (2 ov)
Opetusohjelmasta poiketen kurssi järjestetään myös syksyllä 1996. Aiheena on **Tietoturvajärjestelmien formaalit mallit**. Kokoontuminen tiistaisin 17-20. Lisätietoja: Tuomas Aura tai Pekka Nikander. Seuraa ilmoittelua.

Tik-79.159 Cryptography and data security	
Examination August 8, 1996	Tuomas Aura

Write on the answer sheet the number and name of the course, today's date, your name, student number, department and class number.

Answer **five** (5) of the following six questions. (If you answer them all, question 6 will not be graded.)

1. Explain in short (1 or 2 lines of text is enough)
   (a) hybrid cipher (1p)
   (b) CBC mode (1p)
   (c) one-way hash function (1p)
   (d) **strong** cryptographic algorithm (1p)
   (e) stream cipher (1p)
   (f) subliminal channel (1p).

2. You have agreed with secret agent A to use Diffie–Hellman key exchange with modulus $n = 1997$ (in reality, the number would be much larger) and with base $g = 999$. You receive an email message from A: "My public Diffie-Hellman key is $X = 1872$." You choose number $y = 521$ for you own secret key.
   (a) With which messages does the key exchange protocol continue? What will be the shared secret key?
   (b) What major question was forgotten in the protocol?

3. The three-way X.509 authentication protocol:

1.	$A \to B:$	$S_A[T_A, N_A, B, E_B[K_{AB}]]$
2.	$B \to A:$	$S_B[T_B, N_B, A, N_A, E_A[K_{BA}]]$
3.	$A \to B:$	$S_A[N_B]$

   (a) Explain in detail, how freshness of received messages can be checked. (3p)
   (b) Why are there two session keys: K_{AB} and K_{BA}? (1p)
   (c) In two-way authentication, only the two first messages are sent. How do the three-way and two way authentications differ, i.e. what is the purpose of the third message?

4. Two shadows are known from a Lagrange (2,10)-threshold stucture: (2,19535), (4,1583). The modulus is 37813. What is the secret message? (6p)

5. RSA. (6p)

6. Cryptography in computer user authentication.