Tik-79.159 Tiedon salaus ja suojaus	
Tentti 20.5.1996	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) EDE-moodi (1p)
   (c) informaatioteoreettinen salausmenetelmä (1p)
   (d) **vahva** autentikointi (1p)
   (e) BAN-logiikka (1p)
   (f) Message Authentication Code MAC (1p).

2. Julkinen RSA-avaimesi on $(3, 4897)$ ja salainen $(3171, 4897)$.
   (a) Luet luultavasti itse allekirjoittamasi sanoman $2345, 689$, missä 2345 on sanoma ja 689 allekirjoitus. Tarkista julkisen avaimen avulla, onko allekirjoitus aito. (3p)
   (b) Allekirjoita sanoma 4321. Tee potenssiinkorotus paperilla. (3p)

3. Kaksisuuntainen X.509-autentikointi tapahtuu seuraavasti:

$$\boxed{\begin{array}{lll} 1. & A \to B: & S_A[T_A, N_A, B, E_B[K_{AB}]] \\ 2. & B \to A: & S_B[T_B, N_B, A, N_A, E_A[K_{BA}]] \end{array}}$$

   (a) Selitä yksityiskohtaisesti, mikä merkitys sanomissa istuntoavainten lisäksi olevilla osilla $(T_A, T_B, N_A, N_B, A, B)$ on protokollan turvallisuuden kannalta. (4p)
   (b) Mitä protokolla osapuolet tietävät protokollan onnistuneen suorituksen jälkeen, eli mikä protokollan lopputulos täsmälleen on? (2p)

4. Salataan sanoma DES-algoritmilla ensin 64 bitin CFB-moodissa (Cipher FeedBack mode (*painovirhe korjattu*)) ja sitten uudelleen ECB-moodissa (Electronic Code Book mode) käyttäen samaa avainta. Millainen moodi saadaan? Kuinka hyödyllinen tällainen kaksinkertainen salaus on? (6p)

5. Diffie–Hellman-avaintenvaihto (6p)

6. Anonyymin sähköisen rahan toimintaperiaate (6p)

Tik-79.159 Cryptography and data security	
Examination May 20, 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) EDE mode (1p)
   (c) information-theoretic encryption method (1p)
   (d) **strong** authentication (1p)
   (e) BAN logic (1p)
   (f) Message Authentication Code MAC (1p).

2. Your public RSA key is $(3, 4897)$ and your secret key is $(3171, 4897)$.
   (a) You read the message $2345, 689$, psesumably signed by you. The message is 2345 and the signature 689. Chech the validity of the signature. (3p)
   (b) Sign the message 4321. Do the exponentiation on paper. (3p)

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

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

   (a) Explain in detail, what kind of importance the parts of the messages besides the session key (i.e. T_A, T_B, N_A, N_B, A, B) have for the protocol security. (4p)
   (b) What do the protocol principals know after a successful execution of the protocol? That is, what exactly is the result of the protocol? (2p)

4. A message is enciphered with the DES algorithm, first in 64-bit CFB mode (Cipher FeeBack mode (*misprint coorected*)) and then again in ECB mode (Electronic Code Book mode) using the same key. What kind of mode do we get? How useful is this kind of double encryption? (6p)

5. Diffie–Hellman key exchange (6p)

6. How does anonymous digital cash work? (6p)