Tik-79.159 Tiedon salaus ja suojaus	
Tentti 18.11.1997	Tuomas Aura

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

Vastaa enintään **viiteen** (5) tehtävään. (Muuten tehtävä 6. jätetään arvostelematta.)

1. Määrittele tai selitä seuraavat käsitteet:
   (a) konfuusio (1p)
   (b) steganografia (1p)
   (c) ECB-moodi (*electronic codebook*) (1p)
   (d) sertifikaattipolku (1p)
   (e) vahva pseudosatunnaisluku (1p)
   (f) hybridisalaus (1p)

2. Selitä, mistä seuraavat asiat johtuvat:
   (a) *One-time-pad* -salausta on mahdoton murtaa. (2p)
   (b) Kahden kierroksen Feistel-salaus ei ole turvallinen. (2p)
   (c) Heikko törmäyksettömyys ei riitä allekirjoituksissa vaan tarvitaan vahvaa törmäyksettömyyttä. (2p)

3. Julkinen RSA-avaimesi on $(17, 2183)$. $(2183 = 59 \cdot 37)$
   (a) Mikä on yksityinen RSA-avaimesi? (3p)
   (b) Vastaanotat julkisella avaimellasi salatun sanoman 406. Mikä on selväkielinen sanoma? (3p)

4. Selitä, mitä ongelmia aiheutuu (4p) ja miten ne vältetään (2p), jos RSA-salauksessa
   (a) yksityinen eksponentti tai moduli on pieni
   (b) julkinen salauseksponentti on pieni (esim. $e = 3$)
   (c) selväkielinen sanoma-avaruus on pieni
   (d) sanoma on kahden aikaisemman tulo.

5. Julkisen avaimen Needham-Schröder (oletetaan, että osapuolet jo tuntevat toistensa julkiset avaimet):

1.	$A \longrightarrow B$	$E_B(N_A, A)$
2.	$B \longrightarrow A$	$E_A(N_A, N_B)$
3.	$A \longrightarrow B$	$E_B(N_B)$

   (a) Mitä ominaisuuksia vaaditaan salaukselta E? (2p)
   (b) Mikä vakava hyökkäys protokollaa vastaan on mahdollinen? (Vihje: kun A ottaa yhteyden B:hen, B voi esiintyä C:lle A:na. Esitä hyökkäyksen kulku yksityiskohtaisesti.) (2p)
   (c) Miten protokollan voi korjata? (1p)
   (d) Onko autentikointi korjatussa protokollassa implisiittinen vai eksplisiittinen? (perustele) (1p)

6. Moninkertainen salaus (6p)

Tik-79.159 Cryptography and data security	
Examination, November 18, 1997	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 at most **five** (5) questions. (Otherwise, question 6 will not be graded.)

1. Define or explain the following terms:
   (a) confusion (1p)
   (b) steganography (1p)
   (c) ECB mode (electronic codebook) (1p)
   (d) certificate path (1p)
   (e) strong pseudorandom number (1p)
   (f) hybrid encryption (1p)

2. Explain, why the following claims are true:
   (a) One-time-pad encryption cannot be broken. (2p)
   (b) Two-round Feistel encryption is not secure. (2p)
   (c) Weak collision resistance is not enough for signatures. They require strong collision resistance. (2p)

3. Your public RSA key is $(17, 2183)$. $(2183 = 59 \cdot 37)$
   (a) What is your private RSA key? (3p)
   (b) You receive a message 406 that has been encrypted with your public key. What is the plaintext? (3p)

4. Explain what problems are caused (4p) and how they can be avoided (2p) if in RSA encryption,
   (a) the private exponent or modulus is small
   (b) the public encryption exponent is small (e.g. $e = 3$)
   (c) the plaintext message space is small
   (d) a message is the product of two previous ones.

5. Public-key Needham-Schröder (we assume that the parties know each other's public keys):

1.	$A \longrightarrow B$	$E_B(N_A, A)$
2.	$B \longrightarrow A$	$E_A(N_A, N_B)$
3.	$A \longrightarrow B$	$E_B(N_B)$

   (a) What properties must the encryption E have? (2p)
   (b) What serious attack is possible against the protocol? (Hint: when A contacts B, B can pose as A to C. Present details of the attack.) (2p)
   (c) How can the protocol be repaired (1p)
   (d) Is the authentication in the repaired protocol implicit or explicit? (explain why) (1p)

6. Multiple encryption (6p)