Tik-79.159 Tiedon salaus ja suojaus	
Tentti 2.9.1997	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) diffuusio (1p)
   (b) karakteristinen differenssi (1p)
   (c) törmäyksettömyys (1p)
   (d) OFB-moodi (*output feedback*) (1p)
   (e) Kerckhoffsin periaate (1p)
   (f) eksplisiittinen autentikointi (1p)

2. Selitä, mistä seuraavat asiat johtuvat:
   (a) Lohkosalaus CBC-moodissa ei suojaa sanomien eheyttä. (Anna esimerkki hyökkäyksestä.) (2p)
   (b) Salattavaan sanomaan pitää yleensä lisätä satunnaisuutta jossain muodossa. Kerro myös, miten satunaisuutta voidaan lisätä lohkosalauksessa ja RSA:ssa. (2p)
   (c) RSA:ssa pidä käyttää samaa modulia n useammassa avainparissa. (Entä jos yksityiset avaimet ovat saman henkilön hallussa?) (2p)

3. Diffie–Hellman-parametrien arvoiksi on sovittu $n = 1949$ ja $g = 7$. (Varoitus: lukuarvot ovat todellisuutta ajatellen liian pieniä.) Vastaanotat A:lta sähköpostitse **asianmukaisesti allekirjoitetussa** sanomassa hänen julkisen DH-avaimensa $X = 1172$.
   (a) Miten Diffie-Hellman avaintenvaihtoprotokolla jatkuu?
   (b) Mikä tulee yhteiseksi salaiseksi avainmateriaaliksi?

   Tee potenssiinkorotukset paperilla.

4. LaGrange-kynnysrakenne:
   (a) $(3,7)$-kynnysrakenteesta $(\mathrm{mod}\ 2^{16}+1)$ tunnetaan varjot (1,1123),(3,9322),(4,16678). Laske salainen sanoma. (4p)
   (b) Lisää kynnysrakenteeseen uusi varjo. (2p)

5. Wide-mouth-frog -protokolla:

   $$\boxed{\begin{array}{lll} 1. & A \to T: & A, E_A(T_A, B, K_{SES}) \\ 2. & T \to B: & E_B(T_T, A, K_{SES}) \end{array}}$$

   (a) Mitä ominaisuuksia vaaditaan salausfunktiolta E? (1p)
   (b) Mikä vakava hyökkäys protokollaa vastaan on mahdollinen? (2p)
   (c) Miten protokollan voi korjata? (1p)
   (d) Mitä yleistä suunnitteluperiaatetta noudattamalla vika olisi voitu välttää? (1p)
   (e) Onko autentikointi korjatussa protokollassa implisiittinen vai eksplisiittinen? (1p)

6. Anonyymi sähköinen raha (6p)

Tik-79.159 Cryptography and data security	
Examination, September 2 , 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) diffusion (1p)
   (b) characteristic difference (1p)
   (c) collision resistance (1p)
   (d) OFB mode (*output feedback*) (1p)
   (e) Kerckhoffs's principle (or assumption) (1p)
   (f) explicit authentication (1p)

2. Explain, why the following claims are true:
   (a) Block cipher in CBC mode does not protect the integrity of the messages. (Give an example of an attack.) (2p)
   (b) Usually randomness should be added to messages before encryption. Describe also how randoness can be added in a block cipher and in RSA. (2p)
   (c) One must not use the same modulus for several key pairs in RSA. (What if the private keys belong to the same entity?) (2p)

3. It has been agreed that the Diffie-Hellman parameters are $n = 1949$ and $g = 7$. (Warning: these values are far too small for real systems.) You receive A's public DH key $X = 1172$ in a **properly signed** email.
   (a) How does the Diffie–Hellman key-exchange protocol continue?
   (b) What will be the shared secret key material?

4. LaGrange threshold scheme:
   (a) Three shadows of a $(3, 7)$ thereshold scheme (mod $2^{16}+1$) are known. The shadows are (1,1123),(3,9322),(4,16678). What is the secret message. (4p)
   (b) Add a new shadow to the threshold scheme. (2p)

   Do the exponentiation by hand.

5. The Wide-mouth-frog protocol:

   $$\begin{array}{|lll|} 1. & A \to T: & A, E_A(T_A, B, K_{SES}) \\ 2. & T \to B: & E_B(T_T, A, K_{SES}) \end{array}$$

   (a) What requirements must the encryption function fulfill? (1p)
   (b) Describe a serious attack against the protocol. (2p)
   (c) How can the protocol be repaired? (1p)
   (d) Which common design principle would have helped in avoiding the flaw? (1p)
   (e) Is the authentication in the repaired protocol implicit or explicit? (1p)

6. Anonymous digital cash (6p)