Tik-79.159 Tiedon salaus ja suojaus	
Tentti 16.1.1998	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) CBC-moodi (*cipher-block chaining*) (1p)

   (b) Kerckhoffsin periaate (1p)

   (c) syntymäpäivähyökkäys (tai -paradoksi) (1p)

   (d) subliminaalinen kanava (1p)

   (e) informaatioteoreettinen turvallisuus (1p)

   (f) *Message Authentication Code* (MAC) (1p)

2. Selitä, mistä seuraavat asiat johtuvat:

   (a) MD5 on yhä turvallinen aikaleimauksessa, vaikki sille voitaisiin löytää törmäyksiä. (2p)

   (b) Allekirjoitettaessa sanomaan yleensä pitää lisätä redundanssia jossain muodossa. Mainitse myös tavallisia tapoja lisätä redundanssia. (2p)

   (c) Kaksinkertainen salaus ei ole kovin paljon yksinkertaista parempi. (2p)

3. Julkinen RSA-allekirjoitusavaimesi on $(17, 1927)$.

   (a) Modulin 1927 salaiset tekijät ovat $47 \cdot 41$. Mikä on salainen allekirjoitusavaimesi? (3p)

   (b) Sanoman "Moi, mitä kuuluu?" sormenjälki sovitulla yksisuuntaisella hajautusfunktiolla laskettuna on 123. Esitä allekirjoitettu sanoma kokonaisuudessaan. (3p)

   Tee potenssiinkorotukset paperilla.

4. Laadi $(3, 5)$-kynnysrakenne, jossa salaisuus on 1998. Kerro, miten kaikki käyttämäsi parametrit on valittu. Selitä myös, miten salaisuus ratkaistaan varjoista, miten varjoja voidaan lisätä myöhemmin ja miten Alicelle ja Bobille voitaisiin antaa oikeus yhdessä avata salaisen sanoma, vaikka muuten vaaditaan kolmen henkilön yhteistoimintaa. (6p)

5. Sanoman eheys ja alkuperä varmistetaan allekirjoituksella:

   $$\boxed{1. \quad A \longrightarrow B \quad \text{data}, B,\ S_A(\text{data}, B).}$$

   (a) Mikä merkitys sanomassa on vastaanottajan nimellä B? (1p)

   (b) Oletetaan, että osapuolilla on luotettavat kellot. Miten lisäisit protokollaan sanomien tuoreuden varmistuksen? (2p)

   (c) Mitä kelloja käyttävässä protokollassa tapahtuu, jos jomman kumman osapuolen kello on väliaikaisesti väärässä ajassa. (2p)

   (d) Kuinka sanoman tuoreudesta voitaisiin varmistua, jos kelloihin ei luoteta? (1p)

   Kirjoita kohtien (b) ja (d) vastauksiin kokonaiset sanomat.

6. Suunniteltaessa uutta (esim. Feistel-tyyppistä) lohkosalakirjoitusta, jonka tulisi olla luotettava seuraavat 30–60 vuotta, valitaan 128-bittiset lohkot ja 128–256-bittinen avain. Mitkä tekijät vaikuttavat valintoihin? (6p)

Tik-79.159 Cryptography and data security Examination, January 16, 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) CBC mode (*cipher-block chaining*) (1p)
   (b) Kerckhoffs's principle (i.e. assumption) (1p)
   (c) birthday attack (or birthday paradox) (1p)
   (d) subliminal channel (1p)
   (e) information-theoretically secure (1p)
   (f) Message Authentication Code (MAC) (1p)

2. Explain, why the following claims are true:
   (a) MD5 is still secure in timestamping even if collisions can be found. (2p)
   (b) Redundancy must usually be added to a message that will be signed. Mention also common ways of adding redundancy. (2p)
   (c) Double encryption is not terribly much more secure than single encryption. (2p)

3. Your public RSA key is $(17, 1927)$.
   (a) The secret factors of the modulus 1927 are $47 \cdot 41$. What is your private RSA key? (3p)
   (b) You want to sign the message "Hello! How are you?" The fingerprint computed by a one-way hash function for this message is 123. What is the signed message? (3p)

   Do the exponentiations on paper.

4. Create a $(3, 5)$ threshhold structure where the secret is 1998. Explain how you have selected all the necessary parameters. Explain how the secret can be determined from the shadows, how more shadows could be added later, and how Alice and Bob could be given the right to recover the secret message together even if otherwise three persons are needed. (6p)

5. The integrity and authenticity of a message can be ensured with a signature:

   $$\boxed{1. \quad A \longrightarrow B \quad \text{data}, B,\ S_A(\text{data}, B).}$$

   (a) What is the purpose of the receiver name B in the message? (1p)
   (b) Assume that the communicating parties have accurate clocks. How could a freshness-check be added to the message? (2p)
   (c) What happens in the clock-based protocol if the clock of the sender or the receiver temporarily shows a wrong time? (2p)
   (d) How could the freshness of the messages be ensured if the clocks cannot be trusted? (1p)

   In answering parts (b) and (d), give the complete messages.

6. In designing a new block cipher (for example, a Feistel-type algorithm) that should be secure for the next 30 to 60 years, the block length is chosen to be 128 bits and the keylength 128–256 bits. What factors affect these choices? (6p)