Tik-79.159 Tiedon salaus ja suojaus
Tentti 3 / kevät '98 — 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) diffuusio (1p)
   (c) differentiaalinen virheanalyysi (1p)
   (d) törmäyksettömyys (1p)
   (e) kryptografinen hajautusfunktio (1p)
   (f) sertifikaatti (1p)

2. Selitä, mistä seuraavat asiat johtuvat:
   (a) *One-time-pad* -salauksen avainta ei pidä generoida vahvalla pseudosatunnaislukugeneraattorilla eikä samaa avainta pidä käyttää kahdesti. (2p)
   (b) Heikko törmäyksettömyys ei riitä allekirjoituksissa vaan tarvitaan vahvaa törmäyksettömyyttä. (2p)
   (c) Allekirjoitettaessa sanomaan yleensä lisätään redundanssia jossain muodossa. Anna myös esimerkki, miten redundanssia lisätään. (2p)

3. Diffie–Hellman-parametrien arvoiksi on sovittu $n = 2111$ ja $g = 7$. Vastaanotat A:lta sähköpostitse **asianmukaisesti allekirjoitetussa** sanomassa hänen julkisen DH-avaimensa $X = 360$. Arvot omaksi salaiseksi avaimeksesi $y = 21$.
   (a) Millä sanomilla avaintenvaihtoprotokolla jatkuu? (2p)
   (b) Mikä tulee yhteiseksi salaiseksi avainmateriaaliksi? (2p)
   (c) Miksi sanomat pitää allekirjoittaa? (2p)

4. Yksisuuntainen X.509-autentikointi tapahtuu seuraavasti:

$$\boxed{\begin{array}{lll} 1. & A \to B: & T_A, N_A, B, E_B[\mathit{salaisuus}], \\ & & S_A[T_A, N_A, B, E_B[\mathit{salaisuus}]] \end{array}}$$

   (a) Mitä ovat T_A, N_A, B ja *salaisuus* ja mistä A saa ne? (1p)
   (b) Anna esimerkki algoritmeista, joilla funktiot S ja E voitaisiin toteuttaa. (1p)
   (c) Selitä yksityiskohtaisesti, kuinka B voi tarkistaa sanoman 1 tuoreuden. (2p)
   (d) Miksi $SHA(A, B, \mathit{salaisuus})$ on parempi istuntoavain kuin *salaisuus*? (1p)
   (e) Onko autentikointi protokollassa implisiittinen vai eksplisiittinen? (1p)

5. 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)

6. RSA. (6p)

Tik-79.159 Cryptography and data security Examination 3 / spring '98 — 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) diffusion (1p)
   (c) differential fault analysis (1p)
   (d) collision resistance (1p)
   (e) cryptographic hash function (1p)
   (f) certificate (1p)

2. Explain, why the following claims are true:
   (a) The keys of one-time-pad encryption cannot be generated with a strong pseudo-random number generator, nor can they be reused. (2p)
   (b) Weak collision resistance is not enough for signatures. They require strong collision resistance. (2p)
   (c) Redundancy must usually be added to a message that will be signed. Give also an example of how redundancy can be added. (2p)

3. You have agreed with secret agent A to use Diffie–Hellman key exchange with parameters $n = 2111$ and $g = 7$. You receive in a **properly signed** message from A her public DH key $X = 360$. You randomly choose your own private key to be $y = 21$.
   (a) With which messages does the key exchange protocol continue? (2p)
   (b) What will be the shared secret key? (2p)
   (c) Why must the messages be signed? (2p)

4. The one-way X.509 authentication protocol:

$$\boxed{\begin{array}{lll} 1. & A \rightarrow B: & T_A, N_A, B, E_B[\mathit{secret}], \\ & & S_A[T_A, N_A, B, E_B[\mathit{secret}]] \end{array}}$$

   (a) What are T_A, N_A, B and *secret* and where does A get them from? (1p)
   (b) Give an example of algorithms with which the encryption function E could be implemented. (1p)
   (c) Explain in detail, how B can check the freshness of Message 1. (2p)
   (d) Why is it better to use $SHA(A, B, \mathit{secret})$ than *secret* as a session key? (1p)
   (e) Is the authentication in this protocol implicit or explicit? (1p)

5. Create a $(3, 5)$-threshold 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)

6. RSA. (6p)