| | |
|---|---|
| Tik-79.159 Tiedon salaus ja suojaus | |
| Tentti 19.11.1996 | 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) heikko avain (1p)
   (c) *brute-force* -hyökkäys (1p)
   (d) konfuusio (1p)
   (e) diffuusio (1p)
   (f) Message Authentication Code MAC (1p)

2. Julkinen RSA-allekirjoitusavaimesi on $(17, 1189)$.
   (a) Modulin 1189 salaiset tekijät ovat $29 \cdot 41$. Mikä on salainen allekirjoitusavaimesi? (2p)
   (b) Sanoman "Moi, mitä kuuluu?" sormenjälki sovitulla yksisuuntaisella hajautusfunktiolla laskettuna on 321. Allekirjoita sanoma. Tee potenssiinkorotus paperilla. (2p)
   (c) Mitä suuruusluokkaa lukujen 17, 1189 ja 321 oikeasti pitäisi olla? Vastaukseksi riittää antaa esimerkki sopivasta bittimäärästä kullekin. (2p)

3. Yksisuuntainen X.509-autentikointi tapahtuu seuraavasti:

   $$\boxed{1. \quad A \rightarrow B: \quad S_A[T_A, N_A, B, E_B[K_{AB}]]}$$

   (a) Selitä yksityiskohtaisesti, kuinka B voi tarkistaa sanoman 1 tuoreuden. (2p)
   (b) Mitä B:n täytyy olettaa ennen kuin hän voi uskoa istuntoavaimen tuoreuteen? (2p)
   (c) Mikä merkitys on protokollan turvallisuudelle on sanoman 1 kolmannella osalla $B$? (2p)

4. Lagrange-$(2, 10)$-kynnysrakenteesta tunnetaan varjot (2,19535), (4,1582). Moduuli on 37813. Laske salainen sanoma. (6p)

5. Diffie–Hellman-avaintenvaihto (6p)

6. Nollatietotodistukset. (4p) Voisitko antaa tässä esimerkin, jos paperia ja aikaa riittäisi? Syyt? (2p)

| | |
|---|---|
| Tik-79.159 Cryptography and data security | |
| Examination November 19, 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) weak key (1p)
   (c) brute-force attack (1p)
   (d) confusion (1p)
   (e) diffusion (1p)
   (f) Message Authentication Code MAC (1p)

2. Your public RSA signature key is $(17, 1189)$.
   (a) The secret factors of the modulus 1189 are $29 \cdot 41$. What is your secret signature key? (2p)
   (b) Message "Hello, how are you?" has fingerprint 321, as given by the agreed-on one-way hash function. Sign the message. Do calculations for the exponentiation on paper. (2p)
   (c) In reality, what approximate size should the numbers 17, 1189 and 321 have? It suffices to give an example of a suitable number of bits for each of the parameters. (2p)

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

$$\boxed{1. \quad A \to B: \quad S_A[T_A, N_A, B, E_B[K_{AB}]]}$$

   (a) Explain in detail, how B can check the freshness of Message 1. (2p)
   (b) What assumptions does B have to make before he can believe in the freshness of the session key? (2p)
   (c) What is the significance of the third part of Message 1, $B$, for the security of the protocol?

4. Two shadows are known from a Lagrange (2,10)-threshold structure: (2,19535), (4,1582). The modulus is 37813. What is the secret message? (6p)

5. Diffie-Hellman key exchange (6p)

6. Zero-knowledge proofs. (4p) Could you give here an example if you had sufficient amount of time and paper? Explain. (2p)