Tik-79.159 Tiedon salaus ja suojaus
Tentti 16.1.1997 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) heikko avain (1p)
   (b) diffuusio (1p)
   (c) Message Authentication Code MAC (1p)
   (d) informaatioteoreettinen salausmenetelmä (1p)
   (e) bittivirtasalaus (stream cipher) (1p)
   (f) subliminaalinen kanava (1p).

2. Julkinen RSA-allekirjoitusavaimesi on $(33, 1333)$. **Huom. Tehtävän (a)- ja (b)-kohdat ovat virheellisiä, eikä niitä kannata yrittää ratkaista. Ks. 19.11.-96 tentti.**
   (a) Modulin 1189 salaiset tekijät ovat $31 \cdot 43$. Mikä on salainen allekirjoitusavaimesi? (2p)
   (b) Sanoman "Moi, mitä kuuluu?" sormenjälki sovitulla yksisuuntaisella hajautusfunktiolla laskettuna on 1234. Allekirjoita sanoma. Tee potenssiinkorotus paperilla. (2p)
   (c) Mitä suuruusluokkaa lukujen 33, 1333 ja 1234 oikeasti pitäisi olla? Vastaukseksi riittää antaa esimerkki sopivasta bittimäärästä kullekin. (2p)

3. (a) Allekirjoituksissa käytettävän kryptografisen hajautusfunktion tuottaman arvon bittien määrä (esim. 128 bittiä) on yleensä noin noin kaksinkertainen lohkosalauksen salauslohkon pituuteen nähden (esim. 64 bittiä). Selitä, miten sopivat pituudet määräytyvät? (3p)
   (b) Millaiset hyökkäykset lohkosalakirjoitusta vastaan tulevat mahdollisiksi, jos muistia on käytettävissä rajattomasti? (3p)

4. Esitä protokolla, jolla kaksi henkilöä voi heittää lanttia kommunikoidessaan tietoverkon yli. (Oletetaan, etteivät ulkopuoliset häiritse protokollaa. Ulkopuolisia ei myöskään tarvitse vakuuttaa tuloksen reiluudesta.) (6p)

5. Vertaa kolminkertaisen salauksen (1. ja 3. avain samoja) vahvuutta kaksinkertaiseen salaukseen. (6p)

6. Diffie–Hellman-avaintenvaihto (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 **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) weak key (1p)
   (b) diffusion (1p)
   (c) Message Authentication Code MAC (1p)
   (d) informaatioteoreettinen salausmenetelmä (1p)
   (e) stream cipher (1p)
   (f) subliminal channel (1p).

2. **Note: This problem was erroneous. Don't try to solve it. See a similar problem in the examination on November 19th, 1996.**

   Your public RSA signature key is $(33, 1333)$.

   (a) The secret factors of the modulus 1189 are $31 \cdot 43$. What is your secret signature key? (2p)
   (b) Message "Hello, how are you?" has fingerprint 1234, 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 33, 1333 and 1234 have? It suffices to give an example of a suitable number of bits for each of the parameters. (2p)

3. (a) Cryptographic hash functions that are used in digital signatures produce usually approximately twice as long values (128 bits, for example) as the block length is in a typical block cipher (64 bits). Explain how the suitable lengths have been determined? (3p)
   (b) What kinds of attacks against block ciphers become possible if the attacker has unlimited memory capacity? (3p)

4. Describe a protocol for fair coin-flipping between two parties over a communication line. (Assume that outsiders do not interfere with the protocol. It is also not necessary to convince any outsiders of the fairness of the result.) (6p)

5. Compare the strength of triple encryption (where the 1st and 3rd keys are equal) to double encryption. (6p)

6. Diffie-Hellman key exchange (6p)