Tik-79.159 Tiedon salaus ja suojaus	
Tentti 4 / 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) ECB-moodi (*Electronic CodeBook*) (1p)
   (b) entropia (1p)
   (c) bittivirtasalaus (1p)
   (d) **vahva** salaus (1p)
   (e) ajoitushyökkäys (*timing attack*) (1p)
   (f) kiistämättömyys (1p)

2. Selitä, mistä seuraavat asiat johtuvat:
   (a) Hybridisalaus on immuuni *forward search* -hyökkäykselle. (2p)
   (b) Kolminkertainen salaus 2 avaimella EDE-moodissa on paljon parempi kuin kaksinkertainen salaus 2 avaimella. (2p)
   (c) Diffie-Hellman -avaintenvaihdon sanomat pitää allekirjoittaa. (2p)

3. Julkinen RSA-allekirjoitusavaimesi on $(3, 2173)$.
   (a) Modulin 2173 salaiset tekijät ovat $53 \cdot 41$. Mikä on yksityinen allekirjoitusavaimesi? (2p)
   (b) Luet luultavasti itse allekirjoittamasi sanoman $(1998, 1183)$, missä 1998 on sanoma ja 1183 allekirjoitus. Tarkista julkisen avaimen avulla, onko allekirjoitus aito. (2p)
   (c) Mitä suuruusluokkaa lukujen 3 ja 2173 oikeasti pitäisi olla? Vastaukseksi riittää antaa esimerkki sopivasta bittimäärästä kullekin. (1p)
   (d) Mikä ongelma syntyy, jos haluat allekirjoittaa pitkän sanoman 7453985234? Miten ongelma voidaan ratkaista? (1p)

4. (Korjattu) kolmisuuntainen X.509-autentikointi tapahtuu seuraavasti:

1.	$A \to B:$	$0, N_A, B, E_B[\mathit{salaisuus}_A],\ S_A[0, N_A, B, E_B[\mathit{salaisuus}_A]]$
2.	$B \to A:$	$0, N_B, A, N_A, E_A[\mathit{salaisuus}_B],\ S_B[0, N_B, A, N_A, E_A[\mathit{salaisuus}_B]]$
3.	$A \to B:$	$N_B, A,\ S_A[N_B, A]$

   (Aikaleimoja ei käytetä, joten niiden arvo on 0.)

   (a) Mitä ovat 1. sanoman osat T_A, N_A, B ja $\mathit{salaisuus}_A$ ja mistä A saa ne? (1p)
   (b) Anna esimerkki algoritmeista, joilla funktiot S ja E voitaisiin toteuttaa. (1p)
   (c) Selitä yksityiskohtaisesti, kuinka vastaanotettujen sanomien tuoreus voidaan tarkistaa. (2p)
   (d) Mihin arvoja $\mathit{salaisuus}_A$ ja $\mathit{salaisuus}_B$ voidaan käyttää? (1p)
   (e) Onko autentikointi korjatussa protokollassa implisiittinen vai eksplisiittinen? (perustele) (1p)

5. Selitä, mitä ongelmia aiheutuu (4p) ja miten ne vältetään (2p), jos RSA-salauksessa
   (a) yksityinen eksponentti tai moduli on pieni
   (b) julkinen salauseksponentti on pieni (esim. $e = 3$)
   (c) selväkielinen sanoma-avaruus on pieni
   (d) sanoma on kahden aikaisemman tulo.

6. Anonyymi sähköinen raha (6p)

Tik-79.159 Cryptography and data security Examination 4 / spring '98 (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) ECB mode (Electronic CodeBook) (1p)
   (b) entropy (1p)
   (c) stream cipher (1p)
   (d) **strong** encryption (1p)
   (e) timing attack (1p)
   (f) non-repudiation (1p)

2. Explain, why the following claims are true:
   (a) Hybrid encryption is immune to the forward-search attack. (2p)
   (b) Triple encryption in EDE mode with 2 keys is much better than double encryption with 2 keys. (2p)
   (c) The messages in a Diffie-Hellman key exchange must be signed. (2p)

3. Your public RSA signature key is $(3, 2173)$.
   (a) The secret factors of the modulus 2173 are $53 \cdot 41$. What is your private signature key? (2p)
   (b) You read the message $(1998, 1183)$, presumably signed by you. The message is 1998 and the signature 1183. Check the validity of the signature with the public key. (2p)
   (c) In reality, what approximate size should the numbers 3 and 2173 have? It suffices to give an example of a suitable number of bits for each of the parameters. (1p)
   (d) What problem arises if you want to sign the long message 7453985234? How can the problem be solved? (1p)

4. The (fixed) three-way X.509 authentication protocol:

1.	$A \to B:$	$0, N_A, B, E_B[secret_A],\ S_A[0, N_A, B, E_B[secret_A]]$
2.	$B \to A:$	$0, N_B, A, N_A, E_A[secret_B],\ S_B[0, N_B, A, N_A, E_A[secret_B]]$
3.	$A \to B:$	$N_B, A,\ S_A[N_B, A]$

   (Time stamps are not used. They have value 0.)

   (a) What are T_A, N_A, B and $secret_A$ in message 1 and where does A get them from? (1p)
   (b) Give an example of algorithms with which the functions S and E could be implemented. (1p)
   (c) Explain in detail how the freshness of the received messages can be checked. (2p)
   (d) What can the values $secret_A$ and $secret_B$ be used for?
   (e) Is the authentication in the repaired protocol implicit or explicit? (explain why) (1p)

5. Explain what problems are caused (4p) and how they can be avoided (2p) if in RSA encryption,
   (a) the private exponent or modulus is small
   (b) the public encryption exponent is small (e.g. $e = 3$)
   (c) the plaintext message space is small
   (d) a message is the product of two previous ones.

6. Anonymous digital cash (6p)