Tik-79.159 Tiedon salaus ja suojaus	
Tentti 12.5.1997	Tuomas Aura

Kirjoita vastauspaperiin opintojakson numero ja nimi, päivämäärä, nimesi, opintokirjan numero, osasto ja vuosikurssi.

Vastaa enintään **viiteen** (5) alle olevasta kuudesta tehtävästä. (Muuten tehtävä 6. jätetään arvostelematta.)

1. Määrittele tai selitä seuraavat käsitteet:
   (a) autentikointilogiikka (1p)
   (b) konfuusio (1p)
   (c) subliminaalinen kanava (1p)
   (d) CBC-moodi (Cipher Block Chaining) (1p)
   (e) sertifikaatti (1p)
   (f) nollatietotodistus (1p)

2. Selitä, mistä seuraavat asiat johtuvat:
   (a) *One-time-pad* -salausta on mahdoton murtaa. (2p)
   (b) Hybridisalaus on immuuni *forward search* -hyökkäykselle. (2p)
   (c) Jos jonain päivänä on mahdollista laskea ja tallettaa 2^{64} eri sanomille laskettua kryptografisen hajautusfunktion arvoa massamuistiin, 128-bittinen hajautusarvo ei enää ole riittävän pitkä kaikkiin tarkoituksiin. (2p)

3. Julkinen RSA-avaimesi on $(3, 1927)$. $(1927 = 41 \cdot 47)$
   (a) Mikä on yksityinen RSA-avaimesi? (3p)
   (b) Luet sanoman, johon on liitetty allekirjoitus 1732. Sanoman kryptografinen sormenjälki on 221. Onko sanoma sinun allekirjoittamasi? (3p)

4. Laadi $(3, 5)$-kynnysrakenne, jossa salaisuus on 1997. Selitä myös,miten salaisuus ratkaistaan varjoista, miten varjoja voidaan lisätä myöhemmin ja miten Jaskalle ja Reiskalle voitaisiin antaa oikeus yhdessä avata salaisen sanoma, vaikka muuten vaaditaan kolmen henkilön yhteistoimintaa. (6p)

5. Denning-Sacco:

1.	$A \to T:$	A, B
2.	$T \to A:$	$B, K_B, S_T(B, K_B),\ A, K_A, S_T(A, K_A)$
3.	$A \to B:$	$E_B(T_A, K_{SES}, S_A(T_A, K_{SES})),$
		$B, K_B, S_T(B, K_B),\ A, K_A, S_T(A, K_A)$

   (a) Miten sertifikaattien tuoreudesta voitaisiin varmistua? (1p)
   (b) Mikä vakava hyökkäys protokollaa vastaan on silti mahdollinen? (2p)
   (c) Miten protokollan voi korjata? (1p)
   (d) Mitä yleistä suunnitteluperiaatetta noudattamalla vika olisi voitu välttää? (1p)
   (e) Onko autentikointi korjatussa protokollassa implisiittinen vai eksplisiittinen? (1p)

6. Unix-salasanajärjestelmä (perinteinen `/etc/passwd`). Kerro myös, kuinka samat ideat voitaisiin toteuttaa paremmin esim. SHA-hajautusfuktion avulla. (6p)

Tik-79.159 Cryptography and data security Examination, May 12, 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) of the following six questions. (If you answer them all, question 6 will not be graded.)

1. Define or explain the following terms:
   (a) authentication logic (1p)
   (b) confusion (1p)
   (c) subliminal channel (1p)
   (d) CBC mode (*Cipher Block Chaining*) (1p)
   (e) certificate (1p)
   (f) zero-knowledge proof (1p)

2. Explain, why the following claims are true:
   (a) It is impossible to break one-time-pad encryption. (2p)
   (b) Hybrid encryption is immune to the forward search attack. (2p)
   (c) If one day it would be possible to compute and save 2^{64} different values of a cryptographic hash function to a mass memory, a 128-bit hash value would not any more be sufficiently long for all uses. (2p)

3. Your public RSA key is $(3, 1927)$. $(1927 = 41 \cdot 47)$
   (a) What is your private RSA key? (3p)
   (b) You read a message with attached signature 1732. The cryptographic fingerprint of the message is 221. Has this message been signed by yourself? (3p)

4. Create a $(3, 5)$ threshhold structure where the secret is 1997. Explain how the secret can be determined from the shadows, how more shadows could be added later, and how Jack and Jim could be given the right to recover the secret message together even if otherwise three persons are needed. (6p)

5. Denning-Sacco:

$$
\begin{array}{lll}
1. & A \rightarrow T: & A, B \\
2. & T \rightarrow A: & B, K_B, S_T(B, K_B),\ A, K_A, S_T(A, K_A) \\
3. & A \rightarrow B: & E_B(T_A, K_{SES}, S_A(T_A, K_{SES})), \\
 & & \quad B, K_B, S_T(B, K_B),\ A, K_A, S_T(A, K_A)
\end{array}
$$

   (a) How could the freshness of the certificates be ensured? (1p)
   (b) Describe a serious attack that would still be possible against the protocol. (2p)
   (c) How can the protocol be repaired? (1p)
   (d) Which common design principle would have helped in avoiding the flaw? (1p)
   (e) Is the authentication in the repaired protocol implicit or explicit? (1p)

6. Unix password system (traditional `/etc/passwd`). Explain also how the same ideas could be better implemented with, for example, the SHA hash function. (6p)