Tik-79.159 Tiedon salaus ja suojaus	
Tentti 2 / kevät '98 (10.8.1998)	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) OFB-moodi (*Output FeedBack*) (1p)
   (b) Kerckhoffsin periaate (1p)
   (c) Feistel-salaus (1p)
   (d) informaatioteoreettisesti turvallinen salaus (1p)
   (e) steganografia (1p)
   (f) *one-time pad* (1p)
2. Selitä, mistä seuraavat asiat johtuvat:
   (a) *One-time-pad* -salausta on mahdoton murtaa. (2p)
   (b) Jos lohkosalakirjoitus on ryhmä, ei moninkertaisesta salauksesta ole hyötyä. (2p)
   (c) Kryptografiaa käyttäen kahden turvattoman kanavan yli kommunikoivan osapuolen on mahdollista luoda uusi yhteinen salaisuus ilman kolmannen osapuolen apua, vaikkei heillä ennestään olisi yhteistä salaisuutta. (Mitä kuintenkin vaaditaan?) (2p)
3. Julkinen RSA-allekirjoitusavaimesi on $(17, 1739)$.
   (a) Modulin 1739 salaiset tekijät ovat $37 \cdot 47$. Mikä on yksityinen allekirjoitusavaimesi? (2p)
   (b) Sanoman "Moi, mitä kuuluu?" sormenjälki sovitulla yksisuuntaisella hajautusfunktiolla laskettuna on 32. Allekirjoita sanoma. (Tee potenssiinkorotus paperilla. Käytä laskinta vain kertolaskuun.) (2p)
   (c) Mitä suuruusluokkaa lukujen 17, 1739 ja 32 oikeasti pitäisi olla? Vastaukseksi riittää antaa esimerkki sopivasta bittimäärästä kullekin. (2p)
4. Wide-mouth-frog -protokolla:

1.	$A \to T:$	$A, E_A(T_A, B, K_{SES})$
2.	$T \to B:$	$E_B(T_T, A, K_{SES})$

   (a) Mikä on T:n rooli protokollassa? (1p)
   (b) Anna esimerkki algoritmeista, joilla funktio E voitaisiin toteuttaa. (1p)
   (c) Mikä vakava hyökkäys protokollaa vastaan on mahdollinen? (2p)
   (d) Miten protokollan voi korjata? (1p)
   (e) Onko autentikointi korjatussa protokollassa implisiittinen vai eksplisiittinen? (1p)
5. LaGrange-kynnysrakenne:
   (a) $(3, 7)$-kynnysrakenteesta (mod $2^{16}+1 = 65537$) tunnetaan varjot (1,17730),(3,15649),(4,63373) ja (7,8381). Laske salainen sanoma. (3p)
   (b) Lisää kynnysrakenteeseen uusi varjo. (1p)
   (c) Mitä mahdollisia sovelluksia kynnysrakenteille on? (2p)
6. Diffie-Hellman -avaintenvaihto (6p)

Tik-79.159 Cryptography and data security	
Examination 2 / spring '98 (August 10, 1998)	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) OFB mode (*Output FeedBack*) (1p)
   (b) Kerckhoffs's principle (i.e. assumption) (1p)
   (c) Feistel cipher (1p)
   (d) information-theoretically secure encryption (1p)
   (e) steganography (1p)
   (f) one-time pad (1p)

2. Explain, why the following claims are true:
   (a) One-time-pad encryption cannot be broken. (2p)
   (b) If a block cipher is a group, multiple encryption is useless. (2p)
   (c) With cryptography, it is possible for two parties communicating over an insecure channel to create a new shared secret even if they do not have any previous shared secrets. (What is, however, needed?) (2p)

3. Your public RSA signature key is $(17, 1739)$.
   (a) The secret factors of the modulus 1739 are $37 \cdot 47$. What is your private signature key? (2p)
   (b) Message "Hello, how are you?" has fingerprint 32, as given by the agreed-on one-way hash function. Sign the message. (Do calculations for the exponentiation on paper. Use a pocket calculator only for the multiplications.) (2p)
   (c) In reality, what approximate size should the numbers 17, 1739 and 32 have? It suffices to give an example of a suitable number of bits for each of the parameters. (2p)

4. The Wide-mouth-frog protocol:

1.	$A \to T:$	$A, E_A(T_A, B, K_{SES})$
2.	$T \to B:$	$E_B(T_T, A, K_{SES})$

   (a) What is the role of T in this protocol?
   (b) Give an example of algorithms with which the function E could be implemented. (1p)
   (c) Describe a serious attack against the protocol. (2p)
   (d) How can the protocol be repaired? (1p)
   (e) Is the authentication in the repaired protocol implicit or explicit? (1p)

5. LaGrange threshold scheme:
   (a) Four shadows of a $(3, 7)$ threshold scheme (mod $2^{16} + 1 = 65537$) are known. The shadows are (1,17730),(3,15649),(4,63373) and (7,8381). What is the secret message? (3p)
   (b) Add a new shadow to the threshold scheme. (1p)
   (c) What possible applications do threshold schemes have? (2p)

6. Diffie-Hellman key exchange (6p)