Tik-79.159 Tiedon salaus ja suojaus Tentti 1 / kevät '98 (18.5.1998) 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) CBC-moodi (*Cipher-Block Chaining*) (1p)
   (b) redundanssi (1p)
   (c) differentiaalinen kryptoanalyysi (1p)
   (d) syntymäpäivähyökkäys (tai -paradoksi) (1p)
   (e) *forward search attack* (1p)
   (f) *brute-force* -hyökkäys (1p)

2. Selitä, mistä seuraavat asiat johtuvat:
   (a) Pitkä avain ei takaa salauksen luotettavuutta. (2p)
   (b) Allekirjoitus kannattaa yleensä tehdä ennen salausta eikä sen jälkeen. (2p)
   (c) MD5 on yhä turvallinen aikaleimauksessa, vaikki sille voitaisiin löytää törmäyksiä. (2p)

3. Julkinen RSA-avaimesi on $(733, 2747)$. $(2747 = 41 \cdot 67)$
   (a) Mikä on yksityinen RSA-avaimesi? (2p)
   (b) Vastaanotat julkisella avaimellasi salatun sanoman 2526. Mikä on selväkielinen sanoma? (2p)
   (c) Mitä suuruusluokkaa lukujen 733 ja 2747 oikeasti pitäisi olla? Vastaukseksi riittää antaa esimerkki sopivasta bittimäärästä kullekin. (1p)
   (d) Mikä ongelma syntyy, jos julkisella avaimellasi halutaan salata pitkä sanoma 7453985234? Miten ongelma voidaan ratkaista? (1p)

4. Denning-Sacco -protokolla:

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

   (a) Mitä tässä protokollassa kutsutaan *sertifikaattiksi*? (1p)
   (b) Mikä ongelma liittyy sertifikaattien tuoreuteen ja miten se voitaisiin korjata? (1p)
   (c) Mikä vakava hyökkäys protokollaa vastaan on mahdollinen (vaikka sertifikaaattien tiedettäisiin olevan tuoreita)? (2p)
   (d) Miten protokollan voi korjata? (1p)
   (e) Onko autentikointi korjatussa protokollassa implisiittinen vai eksplisiittinen? (1p)

5. Vertaa kolminkertaisen EDE-moodissa suoritetun 2 avaimen salauksen (1. ja 3. avain samoja) vahvuutta kaksinkertaiseen salaukseen. (6p)

6. Kryptografia tietokoneen käyttäjän tunnistamisessa. (6p)

Tik-79.159 Cryptography and data security	
Examination 1 / spring '98 (May 18, 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) CBC mode (*Cipher-Block Chaining*) (1p)
   (b) redundancy (1p)
   (c) differential cryptanalysis (1p)
   (d) birthday attack (or birthday paradox) (1p)
   (e) forward search attack (1p)
   (f) brute-force attack (1p)
2. Explain, why the following claims are true:
   (a) A long key does not guarantee the security of encryption. (2p)
   (b) It is usually better to sign before, not after, encrypting. (2p)
   (c) MD5 is still secure in timestamping even if collisions can be found. (2p)
3. Your public RSA key is $(733, 2747)$. $(2747 = 41 \cdot 67)$
   (a) What is your private RSA key? (2p)
   (b) You receive the message 2526 that has been encrypted with your public key. What is the plaintext? (2p)
   (c) In reality, what approximate sizes should the numbers 733 and 2747 have? It suffices to give an example of a suitable number of bits for each of the parameters. (1p)
   (d) What problem arises if one wants to encrypt the long message 7453985234 with your public key? How can the problem be solved? (1p)
4. Denning-Sacco protocol:

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.	$A \rightarrow B:$	$E_B(T_A, K_{SES}, S_A(T_A, K_{SES})),$ $B, K_B, S_T(B, K_B),\ A, K_A, S_T(A, K_A)$

   (a) What in this protocol is called *a certificate*? (1p)
   (b) What problem is there with the freshness of the certificates and how could it be fixed? (1p)
   (c) Describe a serious attack against the protocol (assuming the certificates are known to be fresh). (2p)
   (d) How can the protocol be repaired? (1p)
   (e) Is the authentication in the repaired protocol implicit or explicit? (1p)
5. Compare the strength of 2-key EDE-mode triple encryption (the 1st and 3rd keys are equal) to double encryption. (6p)
6. Cryptography in computer user authentication. (6p)