| | |
|---|---|
| Tik-79.159 Tiedon salaus ja suojaus | kevät 98 |
| Laskuharjoitus 5, viikko 10 | Tuomas Aura, Antti Huima |

1. Mitä kryptografisen hajautusfunktion funktion ominaisuuksia tarvitaan seuraavissa käyttötarkoituksissa:

   (a) pseudosatunnaislukujen generointi $(x, H(x), H(H(x)), \ldots)$

   (b) haaste-vastemenettely salaisen avaimen tuntemisen osoittamiseksi paljastamatta avainta ulkopuolisille

   (c) istuntoavaimen generointi yhteisestä salaisuudesta (pääavaimesta) ja muusta datasta (nonsseista)

   (d) digitaalinen allekirjoitus

   (e) ohjelmakoodin muuttumattomuuden osoittava (allekirjoittamaton) sormenjälki

   (f) dokumentin aikaleimaus julkaisemalla funktion arvo sanomalehdessä.

   MD5-hajautusfunktiosta arvellaan lähivuosina löytyvän siinä määrin törmäyksiä, että funktio tulee epäluotettavaksi. Mihin edellä mainitusta tarkoituksista se ei sopisi?

2. 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?

3. CBC-MAC: salataan viesti erillisellä avaimella CBC-moodissa ja hylätään salakielinen teksti paitsi viimeinen lohko, joka liitetään selväkielisen tekstin perään virheentarkistuskoodiksi. Sen jälkeen suoritetaan varsinainen salaus salausavaimella.

   Miksi CBC-salausta ja CBC-MAC-eheystarkistusta ei voida tehdä samalla avaimella?

4. Eräs yritys suojaa maksumääräystensä eheyden 32-bittisellä CRC-virheentarkistuskoodilla (polynomi 1 00000100 11000001 00011101 10110111) ja salaa viestilikenteen RC4-salausalgoritmilla. Sanomien formaatti on seuraava:

   | tavut | sisältö |
   |---|---|
   | 0–15 | saajan tilinumero |
   | 16–19 | rahasumma markkoina (32-bit uint, MSB first) |
   | 20–199 | viitenumero tai viesti saajalle |
   | 200-203 | CRC |

   Tiedät, että yritys on juuri maksamassa sinulle viheliäisen pientä 790 markan palkkiota yhteyskaapelin maahan kaivamisesta. Miten saattaisit toimia, jos moraalisi ei olisi niin korkea?

5. Laske (jos mahdollista):

   (a) $64303^{-1} \bmod (2^{16} + 1)$

   (b) $2397^{-1} \bmod 2679$

6. Laske:

   (a) $1001^{433} \bmod 1927$

   (b) $42^{2^{16}+1} \bmod 1997$

   Mitkä eksponentin ominaisuudet tekevät potenssiin korotuksen nopeaksi?