T-79.159 Tiedon salaus ja suojaus
2005 / Tentti
15.8.2005

1. (6 pist) Seuraava salakieliteksti on tuotettu Vigenèren salaamismenetelmää käyttäen. Määritä periodi Kasiskin menetelmän avulla.

   ```
   VKMHG QFVMO IJOII OHNSN IZXSS CSZEA WWEXU
   LIOZB AGEKQ UHRDH IKHWE OBNSQ RVIES LISYK
   BIOVF IEWEO BQXIE UUIXK EKTUH NSZIB SWJIZ
   BSKFK YWSXS EIDSQ INTBD RKOZD QELUM AAAEV
   MIDMD GKJXR UKTUH TSBGI EQRVF XBAYG UBTCS
   XTBDR SLYKW AFHMM TYCKU JHBWV TUHRQ XYHWM
   IJBXS LSXUB BAYDI OFLPO XBULU OZAHE JOBDT
   ATOUT GLPKO FHNSO KBHMW XKTWX SX
   ```

2. (a) (2 pist) Anna esimerkki salaamismenetelmästä, joka on täydellisesti salaava.
   (b) (2 pist) Voidaanko täydellisesti salaavassa menetelmässä tunnetun salakielen perusteella ratkaista avainta ja/tai selvkieltä?
   (c) (2 pist) Voidaanko täydellisesti salaavassa menetelmässä tunnetun selväkielen perusteella ratkaista käytettyä avainta?

3. (6 pist) DESX on Ron Rivestin esittämä tapa, jolla DES salaamismenetelmä voidaan suojata kaikkien avainten läpikäymistä vastaan. DESX:ssä on 64-bittinen salainen avain W, jolla data häivytetään ennen ja jälkeen salauksen. Lisäksi siinä on tavallinen 56-bittinen DES avain K, ja salausoperaatio toimii seuravasti:

   $$C = W \oplus E_K(P \oplus W)$$

   Osoita että samanlainen konstruktio

   $$C = E_K(P \oplus W)$$

   josta salauksen jälkeinen häivyttäminen on jätetty pois, ei paranna DESin turvallisuutta ja voidaan murtaa ratkaisulla jonka kompleksisuus on 2^{56}.

4. (6 pist) Kuvaa *Polynomial MAC* autentikointikoodin toimintaperiaate.

5. (6 pist) Alice ja Bob käyttävät Diffie-Hellman avaintenvaihtomenetelmää kertaluvun 18 syklisessä ryhmässä, jonka generoi alkio $g = 2$ modulo 19 aritmetiikassa. Alicen salainen eksponentti on $a = 7$ ja Bobin salainen eksponentti on $b = 5$. Laske Diffie-Hellman avain K.