T-79.4501 Cryptography and Data Security
Tentti
28.10.2008

1. Tarkastellaan Hillin salausmenetelmää Galois'n kunnassa $GF(2^4)$ polynomilla x^4+x+1. Salausavain on 2×2-matriisi

$$\begin{pmatrix} x^2 & 1 \\ 1 & x+1 \end{pmatrix}, \text{ eli bittijonomerkintää käyttäen } \begin{pmatrix} 0100 & 0001 \\ 0001 & 0011 \end{pmatrix}.$$

   a) (3 pts) Salaa sana $(x^2, x+1) = (0100, 0011)$.

   b) (3 pts) Laske tulkinta-avainmatriisi.

2. Alice ja Bob käyttävät CBC salausta. Selväkieli on jono lohkoja $P_1, P_2, \ldots, P_t$ ja vastaavat salakielilohkot, jotka Alice lähettää Bobille, ovat $C_1, C_2, \ldots, C_t$. Bob vastaanottaa salakielilohkot $C'_1, C'_2, \ldots, C'_t$, joista täsmälleen yhdessä lohkossa C'_j, missä $1 \leq j < t$, on virhe. Siten $C'_i = C_i$ kaikilla $i = 1, 2, \ldots, t$, paitsi kun $i \neq j$, jolloin $C'_j \neq C_j$.

   a) (3 pts) Osoita että tulkinnan jälkeen Bobin selväkielilohkoista täsmälleen kaksi on virheellistä. Mitkä ovat virheellisten salakielilohkojen indeksit?

   b) (3 pts) Kuinka virheelliset selväkielilohkot eroavat alkuperäisistä?

3. Sun Tsu oli kiinalainen matemaatikko, joskus kolmannen ja viiden vuosisadan välillä jälkeen Kristuksen. Keksimänsä Kiinalaisen Jäännöslauseen havainnollistamiseksi hän käytti esimerkkiä

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7. \end{aligned}$$

   a) (3 pts) Ratkaise x mod 105.

   b) (3 pts) RSA voidaan määritellä myös moduulille n joka on kolmen erisuuren alkuluvun tulo. Samoin kuin tavallisen RSA:n tapauksessa salauseksponentin e ja tulkintaeksponentin d täytyy toteuttaa kongruenssi

$$ed \equiv 1 \pmod{\phi(n)}$$

   Kun $n = 105$ ja $e = 7$, laske d.

4. (6 pts) Esitä Man-in-the-Middle hyökkäys tavallista (autentikoimatonta) Diffie-Hellman avaintenvaihtoprotokollaa vastaan.

5. (6 pts) Oletetaan että on annettu kaksi lukugeneraattoria mustina laatikkoina, eli päältäpäin ne näyttävät aivan samoilta, ja voimme ainoastaan tarkastella niiden tuottamia lukujonoja. Molemmat generaattorit tuottavat 64-bittisiä lukuja. Edelleen on annettu että toinen laatikko sisältää laskurigeneraattorin, joka käyttää Triple-DES salausta ja 64-bittistä laskuria. Toinen laatikko sisältää todellisen satunnaislukugeneraattorin. Tehtävänä on erottaa nämä laatikot toisistaan. Kun molemmat generaattorit ovat tuottaneet noin 2^{32} lukua, on noin 50% todennäköisyys, että generaattorit pystytään erottamaan. Mihin tämä perustuu?

Laskimen käyttö tentissä. Tavallinen, ei ohjelmoitava, funktiolaskin on sallittu.