Salausmenetelmät (801346A, 4 op)

Loppukoe 10.1.2011

EI-OHJELMOITAVAT LASKIMET SALLITTU.

1. a) Joukossa $\mathbb{Z}_{26}$ käytettävän affiinin järjestelmän salausfunktio on $E(x) = 9x$. Määrää avausfunktio.

   b) Mikä on luvun 11^{1324} viimeinen numero 26-kantaisessa esityksessä?

2. Asetetaan suomenkielisen aakkoston kirjaimet vastaamaan joukon $\mathbb{Z}_{27}$ alkioita niin, että A=$\overline{0}$, B=$\overline{1}$, ..., Ö=$\overline{26}$. Tiedetään, että matriisisalauksen salausfunktio on muotoa $E(X) = AX$ ja että viestin TOIMII salaus on MIIAHF. Määrää salaus- ja avausfunktio.

3. Määrittele primitiivijuuri modulo n. Määrää jokin primitiivijuuri modulo 17 ja laske alkion 15 diskreetti logaritmi löytämäsi juuren suhteen.

4. Käyttäjän A antama julkinen RSA-avain on $(n, e) = (187, 23)$. Avaa hänen vastaanottamansa viesti 150, 162, 113, 53, kun englanninkielisen aakkoston kirjaimet vastaavat joukon $\mathbb{Z}_{187}$ alkioita niin, että A = $\overline{2}$, B = $\overline{3}$, ..., Z = $\overline{27}$.

5. a) Esitä ja todista menettely, jolla selkäreppujärjestelmässä julkista avainta ja lähetettyä viestiä vastaava selkäreppuongelma muunnetaan superkasvavaan muotoon.

   b) Käyttäjän U julkinen avain selkäreppujärjestelmässä on 9, 27, 2, 22, 17, jonka muodostamisessa hän on käyttänyt lukuja $n_U = 61$ ja $a_U = 9$. Avaa hänelle tullut viesti 33, 41, 36 (esitä myös välivaiheet, pelkkä kokeilu ei riitä). Englanninkieliset kirjaimet vastaavat lukuja seuraavasti: A=0, B=1, ..., Z=25.