Salausmenetelmät (801346A, 4 op)

Loppukoe 11.4.2011

EI-OHJELMOITAVAT LASKIMET SALLITTU.

1. Joukossa $\mathbb{Z}_{27}$ käytettävän affiinin järjestelmän salausfunktio on $E(x) = 11x + 21$. Avaa salakirjoitus `VHYÄ`, kun suomenkielisen aakkoston kirjaimet vastaavat joukon $\mathbb{Z}_{27}$ alkioita seuraavasti: `A`=$\overline{0}$, `B`=$\overline{1}$, ..., `Ö`=$\overline{26}$.

2. Suomenkielisen aakkoston kirjaimet ja tyhjä väli vastaavat joukon $\mathbb{Z}_{28}$ alkioita seuraavasti: `A`=$\overline{0}$, `B`=$\overline{1}$, ..., `Ö`=$\overline{26}$, ␣=$\overline{27}$. Salaa Vigenéren järjestelmällä ja salasanalla `JEP` viesti `KEVÄTILMA`. Avaa samalla järjestelmällä ja salasanalla tehty salaus `ZSHAE`.

3. Käytetään kirjaimille ja välille samoja numerovastineita kuin edellisessä tehtävässä. Käytetään matriisisalausta joukossa $\mathbb{Z}_{28}$ salausfunktiolla $E(X) = AX$. Tiedetään, että viestin `NÄINKÖ` salaus on ␣`JUNXC`. Määrää salausfunktio ja salaa vastaukseksi `EI`.

4. Käytetään Elgamal-salausta joukossa $\mathbb{Z}_{37}$ ja primitiivialkiota 2. Käyttäjän U julkinen avain on 35. Sieppaat hänelle tulevan viestin $(13, 3)$, $(13, 33)$. Murra salaus ja avaa viesti, kun suomenkielisen aakkoston kirjaimet vastaavat joukon $\mathbb{Z}_{37}$ alkioita seuraavasti: `A`=$\overline{2}$, `B`=$\overline{3}$, ..., `Ö`=$\overline{28}$.

5. Määrittele Eulerin φ-funktio ja esitä Eulerin lause. Miten Eulerin lausetta hyödynnetään RSA-menetelmässä?