802336A, Salausmenetelmät, 5 op

Tentti 7.11.2019

Tehtävissä 1, 3 ja 4 käytetään englanninkielistä aakkostoa ja kirjaimet vastaavat joko kokonaislukuja tai ryhmän $\mathbb{Z}_{26}$ alkioita seuraavasti:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
```

Tehtävässä 2 käytetään suomenkielistä aakkostoa ja kirjaimet vastavaat ryhmän $\mathbb{Z}_{29}$ alkioita samalla tavalla kuin edellä, mutta lisäksi

```
å ä ö
26 27 28
```

1. Salaa viesti

   `autumn`

   a) avainsana-Caesarilla avaimella $(7, \texttt{november})$.
   b) Vigenéren salauksella avainsanalla `snow`.

2. Suomenkielinen viesti

   `IDÅVN`

   on salattu affiinilla salausfunktiolla $E(x) = ax + b$, missä $a \in \mathbb{Z}_{29}^*$ ja $b \in \mathbb{Z}_{29}$. Tiedät, että selkokielinen viesti alkaa `ka`. Avaa viesti.

3. Tässä tehtävässä matriisien ja vektoreiden alkiot kuuluvat joukkoon $\mathbb{Z}_{26}$. Tarkastellaan matriisisalausta, jonka salausfunktio on $E(X) = AX + B$, missä

   $$A = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} \quad \text{ja} \quad B = \begin{bmatrix} 10 \\ 3 \end{bmatrix}.$$

   a) Salaa viesti `base`.
   b) Määrää avausfunktio $D = E^{-1}$.

4. a) Esitä selväkielinen teksti `is` kantamenetelmän avulla ryhmän $\mathbb{Z}_{2173}$ alkiona.
   b) Käytetään RSA-salausta. Tiedät, että käyttäjän A julkinen avain $(n_A, e_A) = (2173, 11)$. Käytä tätä tietoa, kun salaat sanan `is`, jonka aiot lähettää käyttäjälle A (Salaa a)-kohdan vastaus).
   c) Mikä on käyttäjän A avausfunktio, kun tiedetään, että luku $2173 = 41 \cdot 53$?

5. a) Selitä, miten toimii Diffie-Hellman avaimenvaihto äärellisessä syklisessä ryhmässä $H = \langle \beta \rangle$.
   b) Käytetään ElGamal-salausta ryhmässä $\mathbb{Z}_{37}^* = \langle 2 \rangle$. Käyttäjä A on antanut julkisen avaimen $k_A = 35$. Sieppaat käyttäjälle A lähetetyn viestin $(13, 3), (13, 33)$. Murra salaus, kun tiedät, että kaksikirjaimisen viestin 1. kirjain on `m` ja englanninkielisen aakkoston kirjaimet `a-z` vastaavat joukon $\mathbb{Z}_{37}^*$ alkioita $2, 3, \ldots, 26, 27$.

Perustele ratkaisusi hyvin! Laskut näkyviin, pelkkä vastaus ei riitä.