802336A, Salausmenetelmät, 5 op

Tentti 1.9.2023 (5 tehtävää)

Tehtävissä 1, 2 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 10111213141516171819202122232425
```

1. Salaa viesti

   `rain`

   a) Vigenéren salauksella avainsanalla `day`.
   b) affiinilla kuvauksella $E : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, $E(x) = 5x + 3$.

2. Tässä tehtävässä matriisien ja vektoreiden alkiot kuuluvat joukkoon $\mathbb{Z}_{26}$. Tarkastellaan matriisisalausta, jonka salausfunktio on $E(X) = AX$, missä A on 2×2-matriisi. Tiedetään, että selväkieliset viestit $P_1 = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$ ja $P_2 = \begin{bmatrix} 9 \\ 0 \end{bmatrix}$ salautuvat viesteiksi $C_1 = \begin{bmatrix} 13 \\ 12 \end{bmatrix}$ ja $C_2 = \begin{bmatrix} 19 \\ 1 \end{bmatrix}$. Avaa salakirjoitettu englanninkielinen viesti `TBUA`.

3. a) Merkitään RSA-salausjärjestelmässä käyttäjän U julkista avainta (n_U, e_U). Mitkä oletukset vaaditaan luvuilta n_U ja e_U? Miten käyttäjä A salaa käyttäjälle U tarkoitetun viestin j?
   b) Käyttäjän A julkinen RSA-avain on $(n_A, e_A) = (209, 103)$, missä $n_A = 11 \cdot 19$. Käyttäjä A saa viestin $129, 192$. Avaa tämä kaksikirjaiminen viesti, kun tiedetään, että englanninkielisen aakkoston kirjaimet `a-z` vastaavat joukon $\mathbb{Z}_{209}$ alkioita $0, 1, \ldots, 24, 25$.

4. a) Esitä selväkielinen teksti `he` kantamenetelmän avulla ryhmän $\mathbb{Z}_{2173}$ alkiona.
   b) Muodosta kokonaisluvulle (väliltä $[0, 2173[$), joka määrää edellisen kohdan ratkaisuna olevan jäännösluokan, binääriesitys (2-kantainen esitys).
   c) Salaa sana `he` edellisen kohdan binääriesityksen avulla selkäreppumenetelmällä lähetettäväksi U:lle, jonka julkinen avainjono

   $$K_U = \{43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523\}.$$

5. a) Osoita, että 7 on ryhmän $\mathbb{Z}_{26}^*$ generaattori (toisin sanoen osoita, että $\mathbb{Z}_{26}^* = \langle 7 \rangle$).
   b) Käytetään ElGamal-salausta ryhmässä $\mathbb{Z}_{26}^* = \langle 7 \rangle$. Käyttäjän A salainen eksponentti on $a = 5$. Suorita avaus, kun käyttäjä A saa käyttäjältä B viestin $(K_B, c) = (11, 3)$.

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