802336A, Salausmenetelmät, 5 op

Tentti 16.12.2022

Tehtävissä 1-3 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

1. Salaa viesti

   xmas

   a) Vigenèren salauksella avainsanalla eve.
   b) Affiinilla kuvauksella $E : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, $E(x) = 3x + 7$.

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

$$A = \begin{bmatrix} 2 & 5 \\ 1 & 2 \end{bmatrix} \quad \text{ja} \quad B = \begin{bmatrix} 8 \\ 3 \end{bmatrix}.$$

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

3. a) Esitä selväkielinen teksti we 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 we edellisen kohdan binääriesityksen avulla selkäreppumenetelmällä lähetettäväksi U:lle, jonka julkinen avainjono

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

4. Käyttäjät A ja B käyttävät RSA-salausjärjestelmää julkisilla avaimilla $(n_A, e_A) = (51, 11)$ ja $(n_B, e_B) = (65, 7)$. Käyttäjä A lähettää allekirjoitetun salatun viestin $(c, r) = (63, 57)$ käyttäjälle B. Määrää käyttäjän B avauseksponentti d_B (murra järjestelmä) ja suorita käyttäjän B tekemä viestin avaus ja varmennus, että viesti on käyttäjältä A.

5. a) Selitä, miten toimii Diffie-Hellman avaimenvaihto äärellisessä syklisessä ryhmässä $H = \langle \beta \rangle$.
   b) Käytetään Elgamal-salausta ryhmässä $\mathbb{Z}_{29}^* = \langle 3 \rangle$. Käyttäjän A salainen eksponentti on $a = 5$. Suorita avaus, kun käyttäjä A saa käyttäjältä B viestin $(k_B, c) = (7, 9)$.

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