802336A, Salausmenetelmät, 5 op

Tentti 18.12.2019

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

   `christmas`

   a) Caesarin yhteenlaskumenetelmällä avaimella $k = 12$.
   b) Vigenéren salauksella avainsanalla `star`.

2. Oletetaan, että englanninkielisen aakkoston kirjaimet vastaavat $\mathbb{Z}_{26}$:n alkioita. Käytetään matriisisalausta $E(X) = AX$, missä

   $$A = \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix}.$$

   Määrää avausfunktio $D(Y)$ ja avaa salaus `KYEVGFED`.

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

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

4. a) Selitä, miten toimii Diffie-Hellman avaimenvaihto äärellisessä syklisessä ryhmässä $H = \langle \beta \rangle$.
   b) Käytetään ElGamal-salausta ryhmässä $\mathbb{Z}_{26}^* = \langle 11 \rangle$. Käyttäjän A salainen eksponentti $a = 10$. Käyttäjä A salaa viestin 5 ja lähettää sen käyttäjälle B, kun käyttäjän B julkinen avain $k_B = 7$. Määrää A:n lähettämä viesti (k_A, v_A).

5. 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.

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