802336A, Salausmenetelmät, 5 op

Tentti 13.3.2020

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

   `light`

   a) Vigenéren salauksella avainsanalla `sun`.
   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 $E(X) = AX + B$, missä

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

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

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. Käyttäjä A lähettää RSA-salausjärjestelmää käyttäen allekirjoitetun viestin käyttäjälle B ja B avaa tämän viestin alla olevan taulukon mukaisesti. Kerro yksityiskohtaisesti, mitä valintoja A ja B ovat tehneet ja mitä he ovat laskeneet ja millä tavalla. Kerro myös, mitä viestin salauksessa, lähettämisessä ja avaamisessa tapahtuu ja mistä B tietää, että lähettäjä on A.

A	Public channel	B
Secret data		Secret data
$j = 2 \in \mathbb{Z}_{143}$	$(n_A, e_A) = (119, 5)$	
	$(n_b, e_B) = (143, 7)$	
$E_B(j) = j^{e_B} = 2^7$		$D_B(c) = c^{d_B}$
$= 128 = c \in \mathbb{Z}_{143}$	(c, r)	$= 128^{103} = 2 = j$
	$= (128, 98) \rightarrow$ B	
$j \in \mathbb{Z}_{119}$: $D_A(j) = j^{d_A}$		
$= 2^{77} = 32 = s$		
		$E_A(D_B(r))$
$s \in \mathbb{Z}_{143}$:		$= E_A(r^{d_B})$
$E_B(s) = s^{e_B} = 32^7$		$E_A(98^{103}) = E_A(32)$
$= 98 = r \in \mathbb{Z}_{143}$		$32^5 = 2 = j$.

5. (a) 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 $0, 1, \ldots, 24, 25$.

   (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.