

Salausmenetelmät 801346A

Loppukoe 18.6.2012

EI-OHJELMOITAVAT LASKIMET SALLITTU.

Tehtävissä englanninkielisen aakkoston kirjaimet vastaavat joukon $\mathbb{Z}_n$ alkioita seuraavasti: $A=\bar{0}$, $B=\bar{1}$, ..., $Z=\bar{25}$. Viesti on englantia tai suomea ja n ilmoitetaan tehtävässä.

1. Esitä Eulerin lause. Laske sen avulla $\bar{6}^{1691}$ joukossa $\mathbb{Z}_{563}$, kun tiedetään, että 563 on alkuluku.
2. Käytetään joukkoa $\mathbb{Z}_{27}$. Salaa viesti **OIKEA**
 - a) Vigenéren järjestelmällä ja salasanalla **ISO**
 - b) matriisisalakirjoituksella, kun

$$A = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}, \quad B = \begin{bmatrix} 8 \\ 13 \end{bmatrix}.$$

3. Olkoon $n = 27$. Saat affiinilla järjestelmällä salatun viestin **KMFOMTVQ** ja tiedät, että sen kaksi viimeistä merkkiä ovat **SU**. Määrää salausfunktio ja selkokielinen viesti.
4. Käyttäjän A julkinen RSA-avain on $(n, e) = (209, 103)$. Hän on lähettänyt viestin "Onko kaikki valmista?", johon saapui vastaus 192, 129. Avaa tämä viesti.
5. Oletetaan, että g on primitiivijuuri modulo n . Määrittele diskreetti logaritmi kannan g suhteen. Osoita, että jos $x, y \in \mathbb{Z}_n^*$, niin

$$\log_g(xy) \equiv \log_g x + \log_g y \pmod{\varphi(n)}$$

ja anna esimerkki tilanteesta, jossa $\log_g(xy) \neq \log_g x + \log_g y$.