KRYPTOGRAFIAN ALKEET

2. LASKUHARJOITUKSET

Ensimmäisten tehtävien idea on tutustua DES-järjestelmän koukeroihin, viimeisissä tehtävissä puolestaan palautetaan lukuteorian alkeita mieleen kurssin jatkoa ajatellen.

Lukuteorian materiaalia löytyy verkosta useammastakin paikasta. Yksi mahdollisuus on vilkaista viime kevään kurssini (Lukuteorian alkeet, kevät 2013) kotisivuilta löytyvää monistetta. Kotisivut ovat osoitteessa:

`http://wiki.helsinki.fi/pages/viewpage.action?pageId=96704211`

(1) Olkoon

$$w = 00000001\ 00100011\ 01000101\ 01100111\ 10001001\ 10101011\ 11001101\ 11101111.$$

Tämä tahdotaan salata DES-järjestelmällä. Suorita ensimmäinen permutaatio, ja jako blokkeihin L_0 ja R_0.

(2) Olkoon DES-järjestelmän salainen avain

$$K = 000100100011010001010110011111000100110101011110011011110.$$

Laske tarkistusbitit. Määritä lisäksi blokit C_0, D_0, C_1, D_1, muodosta näiden avulla avain K_1 ja käytä sitä laskeaksesi blokit L_1 ja R_1.

(3) Milloin kahden muuttujan ensimmäisen asteen Diofantoksen yhtälöllä on ratkaisu? Ratkaise Diofantoksen yhtälö

$$8x + 5y = 3$$

(4) Muistele, mikä on Fermat'n pieni lause. Laske $3^{58} \pmod{59}$.

(5) Mikä onkaan primitiivinen juuri? Entä kertaluku? Määritä primitiiviset juuret modulo 7 sekä redusoidun jäännössysteemin kaikkien jäsenten kertaluvut.

(6) Mikä on Eulerin φ-funktio? Laske

$$\varphi(29),\ \varphi(30),\ \varphi(16).$$

(7) Mitä kertookaan Eulerin lause? Laske $7^{25} \pmod{30}$.