KRYPTOGRAFIAN ALKEET

6. LASKUHARJOITUKSET

Koska nämä laskarit ovat viimeiset kurssilla, niin käytetään näitä paitsi elliptisiin käyriin, myös kertaamiseen.

(1) Seuraavat tehtävät ovat vaihtoehtoisia. Niissä molemmissa lasketaan kertalukuja. Huomaa, että jos pisteen P kertaluku on n, niin pisteen jP kertaluku on myös n, jos $\text{syt}(n, j) = 1$, ja muutoin $\frac{n}{\text{syt}(n,j)}$.
   (a) Edellisissä laskareissa vaihtoehtotehtävässä 5a) seikkaili käyrä $y^2 = x^3 + 200x + 192$. Sen pisteet myös listattiin. Laske nyt tietokoneella kaikkien käyrän pisteiden kertaluvut.
   (b) Laske käyrän $y^2 = x^3 - 5x$ pisteiden kertaluvut modulo 7.

(2) Elliptisellä käyrällä $y^2 = x^3 + 9x + 17$ on pisteen $P = (16, 5)$ kertaluku 32. Päättele tästä, että piste P on käyrän generaattori (eli, että sen monikertoina saadaan kaikki pisteet).

(3) Ohessa on käyrän $y^2 = x^3 + 9x + 17$ pisteen $P = (16, 5)$ monikertojen lista:

$P = (16, 5)$	$2P = (20, 20)$	$3P = (14, 14)$	$4P = (19, 20)$
$5P = (13, 10)$	$6P = (7, 3)$	$7P = (8, 7)$	$8P = (12, 17)$
$9P = (4, 5)$	$10P = (3, 18)$	$11P = (5, 7)$	$12P = (18, 10)$
$13P = (1, 21)$	$14P = (10, 7)$	$15P(15, 10)$	$16P = (17, 0)$
$17P = (15, 13)$	$18P = (10, 16)$	$19P = (1, 2)$	$20P = (18, 13)$
$21P = (5, 16)$	$22P = (3, 5)$	$23P = (4, 18)$	$24P = (12, 6)$
$25P = (8, 16)$	$26P = (7, 20)$	$27P = (13, 13)$	$28P = (19, 3)$
$29P = (14, 9)$	$30P = (20, 3)$	$31P = (16, 18)$	$32P = O$

   Oletetaan, että Alice haluaa ottaa vastaan ElGamalin järjestelmällä kryptattuja viestejä käyttäen avainta $(23, (16, 5), (1, 2))$. Hyödyntäen ylläolevaa listaa, lähetä hänelle viesti $(12, 17)$.

(4) Alice ja Bob haluavat yhteisen salasanan. He päättävät käyttää Diffie-Hellmannin avaimenvaihtoprotokollaa elliptisellä käyrällä $y^2 = x^3 + 9x + 17 \pmod{23}$ (ks. tehtävä 3). Alice valitsee luvun 7 ja Bob valitsee luvun 5. Mikä tulee olemaan yhteinen salasana?

(5) Valitse alkuluku p, jokin elliptinen käyrä, ja generoi itsellesi julkinen avain ElGamalin järjestelmän mukaan.

(6) Käytetään Hillin kryptojärjestelmää 26-merkkisessä aakkostossa matriisillä

$$\begin{pmatrix} 5 & 2 \\ 11 & 5 \end{pmatrix}.$$

Määritä kryptauksen purkamiseen tarvittava matriisi (muista, että operaatiot suoritetaan modulossa 26!) ja testaa ensin kryptaamalla sana "sana"ja sitten purkamalla kryptaus.

(7) Valitse tarpeelliset parametrit, ja laske RSA:n julkinen ja salainen avain.