Syventävää materiaalia

- Diskreetin matematiikan kertausta
- Ryhmän määritelmä
- Syklinen ryhmä laskutoimituksena kertolasku mod n
- Diffie- Hellman ja ElGamal algoritmit
- Elliptiset käyrät
- Sykliset ryhmä elliptisillä käyrillä
- ECDHE ja EC-Elgamal analogia

Peruskäsitteiden kertaus

Merkintöjä:

Kokonaislukujen joukko Z = { …,-2, -1, 0, 1, 2, ,,,, }

Äärellinen Z:n osajoukko Z_n = { 0, 1, 2, ..., n – 1}

Alkuluvut (prime numbers) ja **yhdistetyt luvut** (composite numbers):
Positiivinen kokonaisluku on alkuluku, jos se on jaollinen vain itsellään ja 1:llä.
Jos positiivinen kokonaisluku ei ole alkuluku, se on yhdistetty luku.

Esim. Mitkä seuraavista ovat alkulukuja, mitkä yhdistettyjä?
a) 31
b) 59
c) 177
d) 8674317

JAKOALGORITMI, osamäärä ja jakojäännös:
(division algorithm, quotient , remainder)
Jos a ja b ovat kokonaislukuja, on olemassa yksikäsitteiset kokonaisluvut q ja r siten, että $a = q\,b + r$

Esim. Luku 1321 jaetaan 521:llä . Laske osamäärä ja jakojäännös.

$1321 = 2*521 + 279$
Osamäärä on 2, jakojäännös 279

DIVISORI ELI JAKAJA: b on luvun n jakaja, jos jakojäännös jaettaessa luku n b:llä on 0. Sanomme tällöin myös, että ”luku b jakaa luvun n”.

Määritä luvun a) 45 ja b) 23 divisorit

a) Tuloesitys: $45 = 1*3*3*5$
Divisorit: 1, 45, 3, 5, 9, 15
b) Tuloesitys : $23 = 1*23$
Divisorit: 1 ja 23

KOKONAISLUKUJEN YKSIKÄSITTEINEN ALKULUKUESITYS

Jokainen kokonaisluku voidaan esittää yksikäsitteisesti alkulukutekijöidensä tulona
Esitä kokonaisluvut a) 45 ja b) 20 alkutekijöidensä tulona.

a) Tuloesitys: $45 = 3*3*5$
b) Tuloesitys : $20 = 2^2*5$

Jakojäännösaritmetiikka

Joukossa Z_n = { 0, 1, 2, ..., n- 1} voidaan määritellä yhteen- , vähennys- , kerto- ja potenssilasku jakojäännöksiä mod n

Esim. Laske joukossa Z_{13} , jossa yhteen- ja kertolasku on määritelty mod 13
*a) 7 + 9 b) 7 – 13 c) 4*12 d) 3^4*

a) 7 + 9 mod 13 = 16 mod 13 = 3
b) 7 – 13 mod 15 = -6 mod 15 = 15 -6 = mod 9 = 9
c) 4*12 mod 13 = 48 mod 13 = 9
d) 3^4 mod 11 = 81 mod 11 = 4

Kysymys: Voidaanko jakojäännösaritmetiikassa määritellä myös jakolasku a/b ?
Tähän vastaaminen onnistuu parhaiten ottamalla käyttöön ryhmän käsite.

Ryhmä (Group)

Olkoon G joukko jossa on määritelty laskutoimitus * . Tällöin G:tä sanotaan ryhmäksi , jos laskutoimituksella on seuraavat ominaisuudet

G1: a*b kuuluu G:hen aina kun $a,b \in G$

G2: $(a*b)*c = a*(b*c)$ kaikille $a,b,c \in G$

G3 Joukossa G on olemassa neutraalialkio e (vrt. luku 1), jolle
$e*a = a*e = a$ kaikille $a \in G$

G4 Jokaisella G:n alkiolla a on olemassa käänteisalkio a^{-1}, jolle
$a^{-1} * a = a * a^{-1} = e$

Ryhmää sanotaan Abelin ryhmäksi, jos edellisten lisäksi on voimassa

G5: $a*b = b*a$ kaikille $a,b \in G$

Esimerkkejä ryhmistä

a) Kokonaisluvut Z muodostavat selvästikin ryhmän yhteenlaskun a + b suhteen. Neutraalialkiona on selvästikin luku 0: $a + 0 = 0 + a = a$
Jokaisella kokonaisluvulla on käänteisalkiona sen vastaluku:
$$a + (-a) = -a + a = 0$$

b) Kokonaisluvut Z eivät muodosta ryhmää kertolaskun a * b suhteen. Neutraalialkio kyllä löytyy: luku 1: $a*1 = 1*a = a$, mutta kokonaisluvuilla ei ole käänteislukua kokonaislukujen joukossa.

esim. Luvun 2 käänteisalkio ½ ei ole kokonaisluku

Murtoluvut $Q \setminus \{0\}$ sen sijaan muodostavat ryhmän kertolaskun suhteen, kun luku 0 on ensin poistettu joukosta. Luku 0 pitää poistaa, koska sillä ei ole käänteislukua. (1/ 0 ei ole määritelty)

Äärelliset ryhmät

Salausmenetelmissä käytetään äärellisiä ryhmiä.

Äärellisen ryhmän kertotaulussa
1) jokainen rivi ja sarake sisältää ryhmän alkiot uudessa järjestyksessä eli jokainen rivi ja sarake on ryhmän alkioiden permutaatio.

2) Ryhmän alkio voi olla vain yhdellä rivillä ja yhdessä sarakkeessa kertotaulussa.

Esim. Täydennä seuraava 4:n alkion e, a, b, c Abelin ryhmän kertotaulu, missä e on neutraalialkio.

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Eulerin lause

Olkoon äärellisen Abelin ryhmän G alkioiden lukumäärä n. Tällöin ryhmän mielivaltaiselle alkiolle a on voimassa $a^n = 1$, jos neutraalialkiota merkitään 1:llä

Todistus: Kertotaulun 1. rivi $g_1, g_2, ..., g_n$. Kertotaulun eräällä rivillä on 1. rivin alkiot kerrottuna luvulla a. Koska molemmat rivit sisältävät samat alkiot eri järjestyksessä, on oltava:

$$g_1 * g_2 * ... g_n = (a\, g_1) * (a\, g_2) * ... * (a\, g_n) = a^n (g_1 * g_2 * .... g_n)$$

Tulo $(g_1 * g_2 * .... g_n)$ on ryhmän alkio, joten sillä on käänteisalkio. Kertomalla yhtälö puolittain tuolla käänteisalkiolla saadaan
$1 = a^n$
Ts. $a^n = 1$

Kertolaskuryhmä Z_n^*

Julkisen avaimen salauksen tämänhetkiset salausstandardit, RSA ja Diskreetin logaritmin ongelmaan perustuvat järjestelmät kuten Diffie Hellman avaimesta sopiminen ja Elgamal perustuvat jakojäännösaritmetiikkaan kertolaskuryhmässä Z_n^*

Tutkitaan tätä kertolaskuryhmää tarkemmin.

Tapaus1: n on alkuluku, esim Z_{11}*

	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Kertotaulu, jossa on laskettu kaikki tulot a*b mod 11, esim. 7*5 mod 11 = 35 mod 11 = 2

Havainto: neutraalialkio = 1, kaikilla luvuilla paitsi luvulla 0 on käänteisluku. Kun se jätetään pois, saadaan ryhmän alkioiksi
Z_{11}* = [1. 2. ,,, , 10} , yhteensä 11 – 1 eli 10 alkiota

YLEISESTI: Kun p on alkuluku, kertolaskuryhmä Z_p* = {1,2,..., p – 1)

Eulerin lauseesta Abelin ryhmille seuraa Fermat'n lause:
Kun p on alkuluku, a^{p-1} mod p = 1 kaikille $1 \leq a \leq p-1$

Z_{11}*n kertotaulu on siten seuraava

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Alkioiden määrä
$\Phi(11) = 10$ kpl

Tapaus2: n yhdistetty luku, esim Z_{10}^*

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Kertotaulu, jossa on laskettu a*b mod 10, esim. 4*4 mod 10 = 16 mod 10 = 6

Vain luvuilla 1, 3, 7 ja 9 on käänteisluvut. Ne ovat ainoat luvut välillä 0 - 9, joille GCD(a, 10) = 1. Niiden lukumäärä on $\varphi(10) = \varphi(2*5) = 1*4 = 4$ kpl.
Siten kertolaskuryhmä $Z_{10}^* = \{1,3,7,9]$

YLEISESTI: Kertolaskuryhmä Z_n^* koostuu niistä luvuista a välillä 1 ... n-1, joille GCD(a, n) = 1. Niiden lukumäärä on $\varphi(n)$

Eulerin lause:
$a^{\varphi(n)} \bmod n = 1$ kaikille kertolaskuryhmän Z_n^* alkioile a.

Z_{10}*n kertotaulu

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Alkioiden määrä
$\Phi(10) = 4$ kpl

Eulerin funktion ominaisuuksia

$\Phi(n)$ antaa niiden kokonaislukujen a lukumäärän välillä 1 ... n-1, joilla ei ole yhteisiä tekijöitä luvun n kanssa, ts. joille GCD(a,n) = 1.
Luvuilla a on tällöin kertolaskun suhteen käänteisluku mod n.
$\Phi(n)$ on samalla kertolaskuryhmän Z_n^* alkioiden lukumäärä.

Eulerin funktion laskeminen:

1) $\Phi(p) = p - 1$, kun p on alkuluku

2) $\Phi(n) = (p-1)(q-1)$, kun $n = p*q$ missä p,q ovat alkulukuja

3) $\Phi(n) = n\,(1- 1/p_1)\,/1- 1/p_2),,,$
Missä p_1, p_2, ... ovat luvun n eri alkulukutekijöitä

Esimerkkejä Φ(n):n laskemisesta

Laske a) Φ(29) b) Φ(35) c) Φ(36):

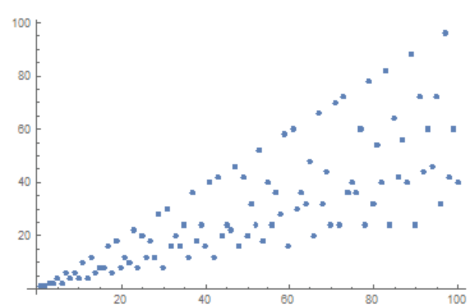
a) 29 on alkuluku => Φ(29) = 29 – 1 = 28

b) 35 on 7*5 (kahden alkuluvun tulo)=> Φ(35) = 6*4 = 24

c) $36 = 2^2 * 3^2$ => Φ(36) = 36 (1- ½)(1- 1/3) = 12

Φ(n) kuvaaja kun n ≤ 100

Yläreunan pisteet kuuluvat alkuluvuille. Alimmat pisteet kuuluvt luvuille, joilla on paljon pieniä tekijöitä.



Sykliset ryhmät

Aliryhmän määritelmä:

A**liryhmä (subgroup)**:
H on ryhmän G aliryhmä jos

1) H sisältyy G:hen
2) H on itsekin ryhmä (toteuttaa ryhmän aksioomat)
3) Laskutoimitus * on sama H:ssa ja G:ssä

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Ryhmän Z_{10}* aliryhmä on esim. {1,9}

Syklinen ryhmä

Ryhmä G on syklinen, jos siinä on alkio, jonka potenssit generoivat ryhmän kaikki alkiot, ts. Jos on olemassa g ϵ G , jolle

$G = g, g^2, g^3, ..., g^n = e$, miss n on G:n alkioiden lukumäärä

Alkiota g, jonka potenssit antavat kaikki ryhmän alkiot, sanotaan ryhmän G **generoivaksi alkioksi** (group generator) eli ***primitiivijuureksi*.**

Muut kuin generoivat alkiot generoivat ryhmän aliryhmiä. Aliryhmän koko on aina ryhmän koon divisori. Alkion **g kertaluvulla , Ord(g)** tarkoitetaan sen generoiman aliryhmän kokoa.

Kertolaskuryhmät Z_n* ovat syklisiä, ts. Niistä löytyy generoivia alkioita, mikäli modulus n on muotoa 2, 4, p , p^k, $2p^k$, missä p on alkuluku

G:n alkioiden virittämien aliryhmien kokoja koskeva kaunis tulos:
Olkoon ryhmän G koko n. Kaikille n:n divisoreille d on olemassa φ(d) G:n alkioita, joiden virittämän aliryhmän koko on juuri d.

Z_p^*:n potenssitaulu (p alkuluku)

Esim. Z_{11}^*

		powers 1,2, ..., 10 of elements											
		1	2	3	4	5	6	7	8	9	10	Order of elemen	
e	1	1	1	1	1	1	1	1	1	1	1	1	
l	2	2	4	8	5	10	9	7	3	6	1	10	generator
e	3	3	9	5	4	1	3	9	5	4	1	5	
m	4	4	5	9	3	1	4	5	9	3	1	5	
e	5	5	3	4	9	1	5	3	4	9	1	5	
n	6	6	3	7	9	10	5	8	4	2	1	10	generator
t	7	7	5	2	3	10	4	6	9	8	1	10	generator
s	8	8	9	6	4	10	3	2	5	7	1	10	generator
	9	9	4	3	5	1	9	4	3	5	1	5	
	10	10	1	10	1	10	1	10	1	10	1	2	

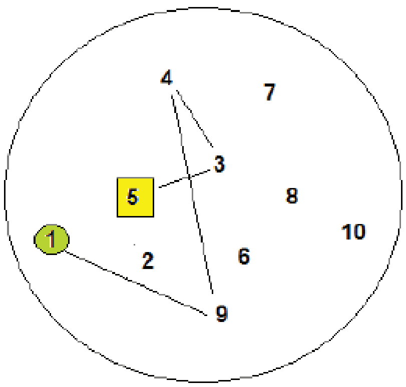
Generaattoreita on 4 kpl : 2, 6, 7 ja 8 — $\varphi(10) = 4$
Aliryhmän, jonka koko on 5 , virittävät 3,4,5 ja 9 — $\varphi(5) = 4$
Aliryhmän , jonka koko on 2 virittää alkio 10 — $\varphi(2) = 1$
Neutraalialkio 1 virittää pienimmän aliryhmän, jonka koko on 1. — $\varphi(1) = 1$

Esimerkki kertolaskuryhmästä, jossa ei ole generoivaa alkiota Z_{15}^*

potenssi

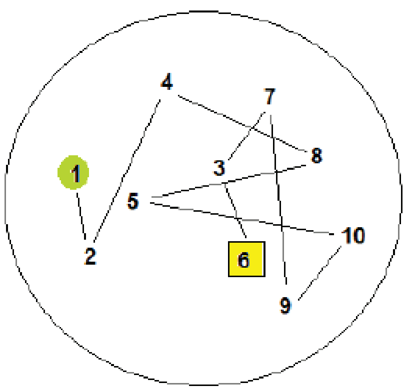
ALKIO	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	2	4	8	1	2	4	8	1
4	4	1	4	1	4	1	4	1
7	7	4	13	1	7	4	13	1
8	8	4	2	1	8	4	2	1
11	11	1	11	1	11	1	11	1
13	13	4	7	1	13	4	7	1
14	14	1	14	1	14	1	14	1

Kertolaskuryhmistä Z_n^* löytyy generoivia alkioita, mikäli modulus n on muotoa 2, 4, p , p^k, $2p^k$, missä p on alkuluku. Luku 15 ei ole em. muotoa, joten ryhmä ei ole syklinen. Alkoiden kertaluvut jäävät enintään neljään.



Kuvissa näkyy alkioiden potenssien muodostamia aliryhmiä graafeina.

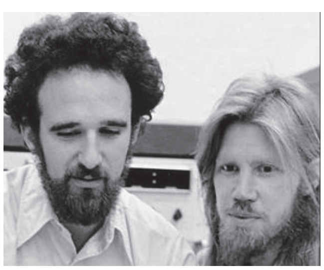
Alkio 5 virittää aliryhmän {5,3,4,9, 1}. Se ei siis ole generoiva alkio.



Alkio 6 virittää koko ryhmän Z_{11}^{*} = {6,3,7,9,10,5,8,4,2,1}
Siten 6 on ryhmän generaattori.

Sovellus: Diffie Hellman key exhange -protokolla

- Menetelmä, jolla yhteyden osapuolet voivat sopia symmetrisestä salausavaimesta.
- Algoritmi esitettiin 1977 kuuluisassa konferenssipuheessa, jossa Diffie ja Hellman ensimmäistä kertaa esittivät julkisen avaimen salauksen perusperiaatteen.
- Puheessaan he esittivät metodin, jolla voidaan turvallisesti sopia esim. AES avaimesta ennen istuntoa
- DH – menetelmä on yleisesti käytössä esim. AES:lla salatuissa videoneuvotteluyhteyksissä.



Kryptologit
Diffie ja Hellman
1980- luvun alussa

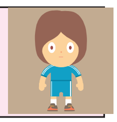
Diffie – Hellman avaimesta sopiminen

Järjestelmäparametrit alkuluku p ja Z_p^* :n generaattori g on annettu.

Turvallinen koko modulukselle p on 2048 bittiä.

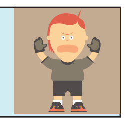
Alice valitsee

luvun a



Bob valitsee

luvun b



$\mathbf{y_a = g^{\,a} \bmod p}$

$\mathbf{y_b = g^{\,b} \bmod p}$

* A ja B laskevat ja lähettävät toisilleen julkiset avaimensa Ya ja Yb

$K = Y_b^{\,a} \bmod p$

$K = Y_a^{\,b} \bmod p$

A ja B laskevat symmetrisen avaimen K =

g^{ab} mod p

Järjestelmäparametrit p ja g

Alkulukumodulus p luodaan alkulukugeneraattorilla, jollainen löytyy kryptologiaan käytettävistä ohjelmointikielistä.

Generoiva alkio q luodaan seuraavalla algoritmilla:

1. Generoidaan satunnaisluku g väliltä 1 ... (p-1)

2. Testataan sen kertaluku Ord(g) (ts. alkion g virittämän aliryhmän koko) kertolaskuryhmässä Z_p seuraavasti.

a) Etsitään luvun p-1 divisorit eli jakajat d
b) Lasketaan potenssit q^d mod p kaikille p-1:n divisoreille
c) Jos ainoastaan g^{p-1} mod p = 1 , q on generoiva alkio

Toistetaan askelia 1 ja 2, kunnes löydetään generoiva alkio.

Esim. parametrien p ja g luonnista

1. Generoidaan alkuluku p (tässä väliltä 150... 200)

RandomPrime[{150,200}] Komento wolframalphalla

Ans: 173

2. Kertolaskuryhmän $Z_{173}{}^*$ mahdolliset aliryhmien koot ovat p-1:n jakajat:

Divisors[172]

Ans: 1,2,4, 43, 86, 172

3. Valitaan generaattoriehdokas ja testataan, onko sen kertaluku 172 vai pienempi. Ehdokas1: g = 10.

10^{1,2,4,43,86,172} mod 173

Ans: {10, 100, 139, 1, 1, 1}

=> kantaluvun 10 kertaluku = 43 => luku 10 ei ole generoiva alkio

Ehdokas 2: g = 11

10^Divisors[172] mod 173

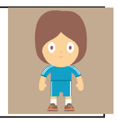
{11, 121, 109, 93, 172, 1]} => 11 on generaattori

Diffie – Hellman esimerkki

Järjestelmäparametrit $p = 173$ ja $g = 11$

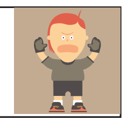
Alice valitsee

luvun $a = 17$



Bob valitsee

luvun $b = 56$



$\mathbf{y_a = 11^{17} \bmod 173}$

$\mathbf{= 69}$

$\mathbf{y_b = 11^{56} \bmod 173}$

$\mathbf{= 43}$

* A ja B laskevat ja lähettävät toisilleen

julkiset avaimensa

$K = 43^{17} \bmod 173$

$= 132$

$K = 69^{56} \bmod 173$

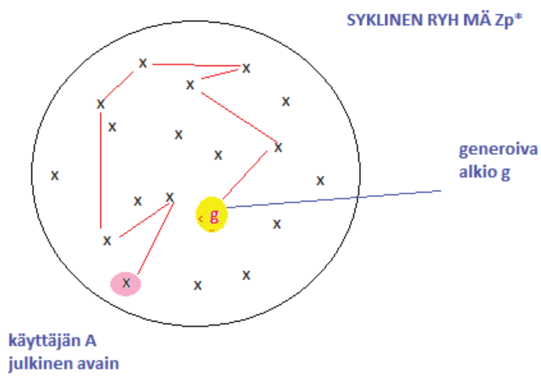
$= 132$

A ja B laskevat symmetrisen avaimen $K =$

$g^{ab} \bmod p$

Sovittu symmetrinen avain on 132.

DH :n turvallisuus, DLP



Murtaakseen DH:n turvallisuuden hyökkääjän tulisi kyetä laskemaan X:n julkisesta avaimesta Yx eksponentti x.

DLP : Ratkaise x yhtälöstä $Y_x = g^x \bmod p$

Tämä on ns. Diskreetin logaritmin ongelma, Discrete Logarithm Problem. Se on yksi lukuteorian ns. kovista ongelmista. Yleisesti katsotaan, että jos modulus p on väh. 2048 bittinen, ei käyttäjän yksityistä avainta x ole mahdollista murtaa tällä hetkellä tiedossa olevilla parhaillakaan algoritmeilla.

On tärkeää selvittää g:n kertaluku aiemmin kuvatulla tavalla. g:n tulisi olla generoiva alkio. Joskus hyväksytään kantaluvuksi muitakin kuin generoivia alkioita, jos aliryhmän koko on lähellä koko ryhmän suuruusluokkaa p – 1.

Alkulukujen generointi

1. Generoi pariton satunnaisluku halutulta väliltä
2. Suorita alkulukutesti. Jos testitulos on negatiivinen, palaa kohtaan 1

Huom. Lukujen kasvaessa alkuluvut harvenevat. Siksi suurten alkulukujen generointi esim. RSA:ta tai DH- algoritmia varten voi olla hidasta.

Vahvat alkuluvut (strong primes)

Vahva alkuluku p on alkuluku, jolle p-1:llä on suuri alkulukutekijä, esim. kun $p - 1 = 2^* r$, missä r on alkuluku

1. Diskreetin logaritmin ongelma DLP on erityisen vaikea ratkaista ryhmässä Z_p, missä p on vahva alkuluku => DH protokolla on tavanomaista turvallisempi.

2. Lisäksi järjestelmäparametrien generoinnissa kantaluvun g kertaluvun selvittäminen on helpompaa kun p on vahva alkuluku.
Jos p on suuri, luvun p- 1 divisoreja ei välttämättä saada selville. Tällöin jos $p - 1 = 2^*r$, missä r olisi alkuluku, p-1:n divisorit ovat 1, 2 , (p-1)/2 ja (p-1) ja kantaluvun g kertaluku selviää korottamalla se em. potensseihin.

Alkulukutestit

Deterministiset alkulukutesti ovat hitaita, niitä ei voi käyttää suurten lukujen testaukseen.

Käytetyt alkulukutestit ovat probabilistisia:

* Jos testi antaa, että luku on yhdistetty luku, tulos on 100% varma.

- Jos testi antaa, että luku on alkuluku, tulos ei ole 100% varma. On vähäinen mahdollisuus, että luku on silti yhdistetty luku. Tämän mahdollisuuden todennäköisyys on hyvissä alkulukutesteissä laskettavissa.

- **1) Fermat'n testi** perustuu Fernat'n lauseeseen. Se ei ole kovin yleisesti käytössä, mutta esim. PGP salausohjelmisto on käyttänyt sitä
- **2) Rabin-Millerin** testi on yleisimmin käytetty alkulukutesti. Se on nopea ja sen erehtymistodennäköisyys tunnetaan ja sitä voidaan säädellä parametrillä.

Fermat’n alkulukutesti

INPUT: testattava alkuluku n
kierrosten lukumäärä k
TOISTA k kertaa
{arvo satunnaisluku **a** väliltä 2 ... (n-1)
Jos a^{n-1} mod n ≠ 1, tulos = FALSE, lopeta testi}

Jos jokaisella kierroksella a^{n-1} mod n = 1, niin
testin tulos = TRUE (n = alkuluku)

Testi perustuu Fermat’n lauseeseen, jonka mukaan a^{n-1} mod n = 1 kaikilla kantaluvuilla a välillä 1...n-1, mikäli n on alkuluku.

Yhtälö voi olla voimassa joillekin kantaluvuille a, vaikka n olisi yhdistetty luku. Erityisesti jos n kuuluu Charmichaelin lukuihin (mm. 561, 1105, ...), alkulukutesti saattaa mennä läpi useilla kantaluvuilla a, joita kutsutaan tällöin nimellä ”Fermat’n liar”. Fermat’n testiä käytettäessä tulee käyttää riittävää määrää kantalukuja a testituloksen varmistamiseksi, mikäli testi menee läpi. Tuloksen luotettavuuden yhteyttä kierrosten määrää ei tunneta.

Rabin Miller -alkulukutesti

1. Valitse satunnainen kantaluku a välilä 2 … (p-1)

2. Erota p-1:stä luvun 2 potenssit =>
Ts. esitä p-1 muodossa $p-1 = 2^s r$, missä r on pariton.

3. Laske jono : 2^{p-1} mod p , $2^{(p-1)/2}$ mod p, $2^{(p-1)/4}$ mod p,…
lukuun a^r mod p saakka. Jonon tulisi alkaa luvulla 1, seuraava luku tulisi olla 1 tai p-1. Pysähdy, jos tulos on p-1. Jos jotain muuta kuin 1 tai p-1 esiintyy jonossa, p ei ole alkuluku.

4. Toista askeleita 1 – 3 k kertaa eri kantaluvuilla a. Jos testi menee läpi joka kerta, todennäköisyys sille, että p on alkuluku $> 1 - 1 / 4^k$.

99% varmuus saavutetaan jo neljällä eri satunnaisesti valitulla kantaluvulla.

Testi perustuu siihen faktaan, että mikäli **p** on alkuluku,
kertolaskuryhmässä luvun 1 neliöjuuri voi olla vain 1 tai -1 eli p- 1

Esim. Alkulukutesti luvulle 561

Kyseessä on ensimmäinen Carmichaelin luku, josta tiedetään, että
Fermat'n testi saattaa antaa useilla kantaluvuilla vääriä tuloksia.

1) Fermat'n testi kantaluvuilla 5, 2, 3
5^{560} mod 561 = 1 testi menee läpi
2^{560} mod 561 = 1 testi menee läpi
3^{560} mod 561 = 375 vasta kantaluku 3 osoittaa, että 561 ei ole alkuluku

1) Rabin Miller -testi kantaluvulla 5
Kirjoitetaan p – 1 = 560 muodossa 560 = 2^5*35

5^{560} mod 561 = 1
5^{280} mod 561 = **67**
Koska tämä ei ole 1 tai 560, päätellään, että 561 ei ole alkuluku

Rabin Miller testiin riitti yksi kantaluku, kun Fermat'n testi antoi oikean tuloksen vasta kolmannella yrityksellä.

Rabin- Miller esimerkki

Onko p = 3 334 141 alkuluku ?

Erotetaan p-1: stä 2:n potenssit :
p - 1= 3 334 140 = $2^2 * 833535$

Testi kantaluvulla a = 7 :

7^{p-1} mod p = $7^{3\,334\,140}$ mod 3 334 141 = 1
$7^{(p-1)/2}$ mod p = $7^{1\,667\,070}$ mod 3 334 140
Viimeinen tulos = p-1 => p läpäisi testin kantaluvulla a = 7

Testi kantaluvulla a = 16 :

16^{p-1} mod p = $16^{3\,334\,140}$ mod 3 334 141 = 1
$16^{(p-1)/2}$ mod p = $16^{1\,667\,070}$ mod 3 334 140 = 1
$16^{(p-1)/4}$ mod p = 16^{833535} mod 3 334 140 = 1
=> p läpäisi testin kantaluvulla a = 16

Kierrosten määrä yo. testissä k = 2 . Luku p on alkuluku
todennäköisyydellä > 1 – $1/4^k$ = 93.7 %

Muita tarvittavia algoritmeja

POWERMOD: NOPEA POTENSSIIN KOROTUS a^b mod n

Algoritmi on nopea, ja tarvitsee muistia enintään n^2 verran.

Example 7^{11} mod 13

7^{11} mod 13	
$= 7^{10} * 7$ mod 13	
$= 49^5 * 7$ mod 13	
$= 10^5 * 7$ mod 13	
$= 10^4 * (7*10)$ mod 13	70 mod 13 = 5
$= 100^2 * 5$ mod 13	100 mod 13 = 9
$= 9^2 * 5$ mod 13	
= 81*5 mod 13	81 mod 13 = 3
= 3*5 mod 13	
= 15 mod 13	
= 2	

1. Jos b on parillinen, puolita se ja neliöi samalla kantaluku mod n
2. Jos b on pariton, kirjoitetaan a^b muodossa $a*a^{b-1}$ ja parilliseen sovelletaan kohdan 1 menettelyä

Muita tarvittavia algoritmeja

SUURIN YHTEINEN TEKIJÄ GCD

Suurin yhteinen tekijä GCD (greatest common divisor) lasketaan Eucleiden algoritmilla soveltaen jakoalgoritmia useita kertoja perättäin.
Esim. Laske GDC(13,5)

13 = 2* **5** + **3**
5 = 1***3** + **2**
3 = 1***2** + **1** < = GDC on viimeinen 0:sta eroava jakojäännös
2 = 2***1** + 0

Algoritmissa edellisen vaiheen jakaja siirtyy jaettavaksi, ja jakojäännös siirtyy jakajaksi.

a:n käänteisluvun laskeminen mod n

GCD(a,n):n laskemisen yhteydessä saatu jakoalgoritmien jono
Käännetään ja esitetään GCD(a,n) = 1 lukujen a ja n
lineaariyhdistelmänä. 1 = k*a + s*n
a:n kerroin k lineaariyhdistelmässä on käänteisluku a^{-1} mod n

Esim. Laske 5^{-1} mod 13 lähtien GCD :n iteraatiosta:
13 = 2* **5** + **3**
5 = 1***3** + **2**
3 = 1***2** + **1** < = **gcd**

Algoritmi käännettynä antaa lineaariyhdistelmän
1 = 3 – 1*2 eliminoidaan 2 käyttäen seur. Yhtälöä
1 = 3 – 1*(5 – 1*3) = 3 – 5 + 3 = 2***3** – **5** eliminoidaan 3
1 = 2*(13 – 2*5) – 5 = 2*13 – 4*5 – 5 = 2***13** – 5***5**

Luvun 5 käänteisluku on sen kerroin lineaariyhdistelmässä
= -5 mod 13 = 13 – 5 = 8.

Tarkistus: 5*8 mod 13 = 40 mod 13 = 1

Satunnaislukujen generointi

Salausavaimet luodaan usein satunnaislukugeneraattorilla. Hyökkäys salausavaimia vastaan on huomattavasti helpompaa, jos jotkut satunnaisluvut ovat todennäköisempiä kuin toiset. Satunnaislukugeneraattori voi olla salausprotokollan heikko kohta, vaikka kaikki muu olisi kunnossa.
Yksi tämän vuosikymmenen skandaaleista oli se, kun Eduard Snowden paljasti, että SSL-yhteyksissä yleinen satunnaislukugeneraattori Dual EC-DRBG sisälsi tietoisen takaportin, joka tarjosi NSA:lle mahdollisuuden murtaa salausavaimia ja kuunnella suojattuja yhteyksiä. On väitetty, että mm. RSA laboratories on auttanut levittämään tätä satunnaisluku- generaattoria tuotteidensa välityksellä.

SATUNNAISLUKUGENERAATTORIN KÄYTTÖ

Haastelukuina autentikoinnissa
Salausavaimina
RSA:n avainten luonnissa
DH:ssa osapuolten yksityisinä avaimina
Kertakäyttösalasanoja generoivissa laitteissa

Kuva laitteesta joka luo minuutin välein uuden 7 -numeroisen salasanan.

Satunnaislukugeneraattorien tuottamien bittijonojen vaatimuksia:

1. **Binäärimuodossa esitettyinä generaattorin tuottamien lukujen tulee sisältää yhtä paljon ykkösiä kuin nollia**

2) Todennäköisyydet 1,2,3 ja 4 pituiselle saman pitin toistolle:
1, 11, 111, 1111, (tai 0, 00, 000, 000) tulisi olla
½, ¼, 1/8 , 1/16, …

3) Kun bittijonoon tehdään määrätyn bittimäärän suuruinen rotaatio, ja lasketaan sen jälkeen alkuperäisen ja uuden jonon bittien samat ja eroavat bitit, niiden määrien pitäisi olla likimain samat: 50%.

Kryptografisia vaatimuksia:
4) Kaikilla satunnaislukugeneraattoreilla on periodi. Tietyn bittimäärän jälkeen ne alkavat tuottaa samoja bittejä alusta. Salauksessa käytettyjen satunnaislukugeneraattorien periodin pitäisi olla riittävän suuri.

5) Jos tunnetaan osajono satunnaislukugeneraatorin tuottamista biteistä, ei saisi olla mahdollista laskea niistä edellisiä ja seuraavia bittejä.

ElGamal -salaus

- Perustuu Diffie-Hellman – avaimenvaihtoprotokollaan. ElGamal algoritmissa sovitaan samassa algoritmissa symmetrinen avain ja käytetään sitä viestien salaamiseen. Lohkosalainta ei tarvita.

Alice salaa viestin **m**

1. Alice hakee serveriltä Bob:n julkiset avaimet

2. Alice generoi oman yksityisen avaimen **a** ja laskee julkisen avaimen Ya = g^a mod p
3. Alice laskee salausavaimen K = Y_b^a mod p
4. Alice laskee salakirjoituksen C = K*M mod p
Ja lähettää Bob:lle parin (Ya, C)

Bob purkaa salauksen

5. Bob laskee avaimen K = Y_a^b mod p
6. Bob laskee avaimen K käänteisluvun K^{-1} mod p
7. Bob purkaa salauksen M = K^{-1}*C mod p

Bob:n yksityinen avain = b

Bob:n julkiset avaimet ovat

p = alkulukumodulus

g = generoiva alkio

$y_b = g^b$ mod p

ElGamal on käytössä GNU Privacy Guard salausohjelmistossa.

Kurssimateriaalin liite 2, jossa on lisätietoa elliptisistä käyristä. Palautettavissa tehtävissä ei ole kysymyksiä tästä liitteestä.

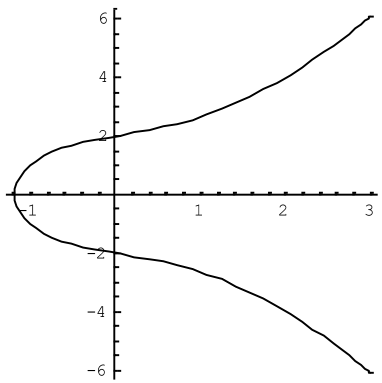
ECC : Elliptisten käyrien salaus

Elliptic curve cryptography

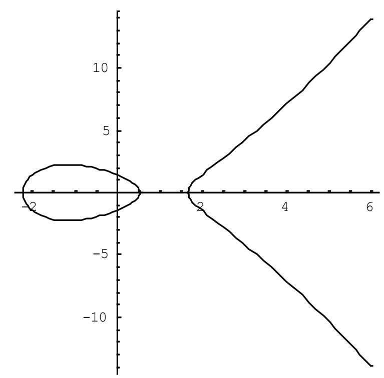
Elliptiset käyrät salauksessa

Salauksessa käytetyt ellptiset käyrät ovat muotoa **$y^2 = x^3 + a\,x^2 + b$**

- Niiden kuvaajien muoto on jompikumpi alla olevista



$y^2 = x^3 + 2x +4$

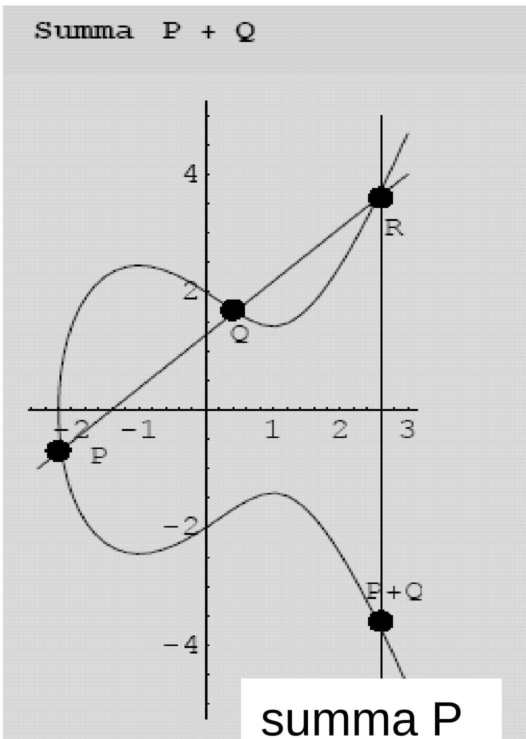


$y^2 = x^3 - 4x +2$

Käyrän pisteiden yhteenlasku

Yli 100 vuotta sitten havaittiin, että käyrän pisteille voidaan määritellä summa, joka muodosta ns. Ryhmärakenteen.

Geometrisesti summa on pisteiden P ja Q kautta piirretyn suoran ja käyrän leikkauspisteen peilikuvapiste



summa P + Q

Algebrallisesti pisteiden

P = (x_1, y_1) ja Q = (x_2, y_2)

summa voidaan laskea kaavoilla

P + Q = (x, y), missä

$$\boxed{x = \lambda^2 - x_1 - x_2}$$

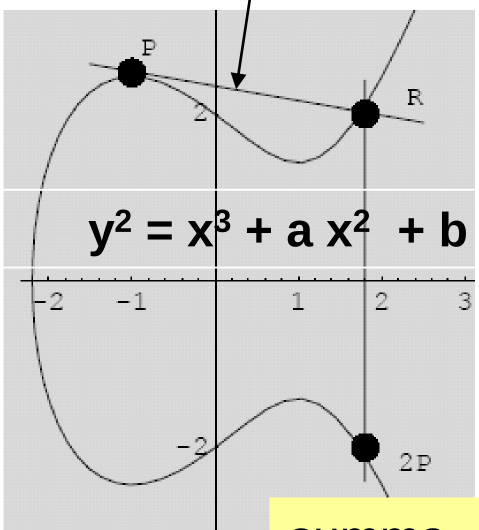
$$\boxed{y = -y_1 + \lambda(x_1 - x)}$$

ja λ (kuvan suoran kulmakerroin)

$$\boxed{\lambda = \frac{y_2 - y_1}{x_2 - x_1}}$$

Pisteen monikerta P + P (= 2P)

Geometrisesti 2P on pisteeseen P piirretyn tangentin ja käyrän leikkauspisteen R peilikuva



summa
P+P

Algebrallinen kaava pisteelle

2P =(x,y), missä P = (x_1, y_1)

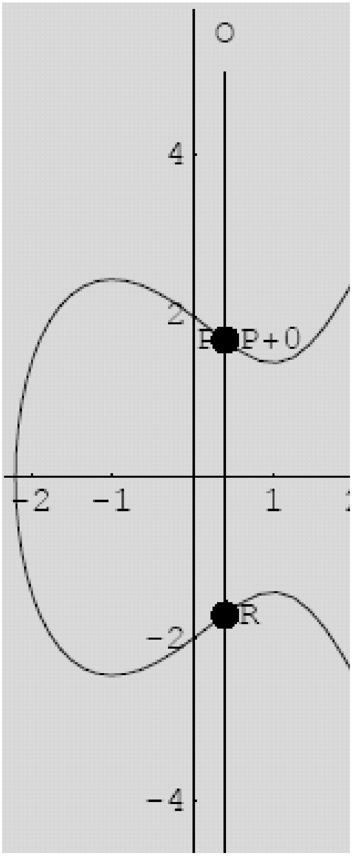
$$\boxed{x = \lambda^2 - 2x_1}$$

$$\boxed{y = -y_1 + \lambda(x_1 - x)}$$

Käyrän tangentin kulmakerroin λ

$$\boxed{\lambda = \frac{3x_1^{\;2} + a}{2y_1}}$$

Ryhmän neutraalialkio *O*

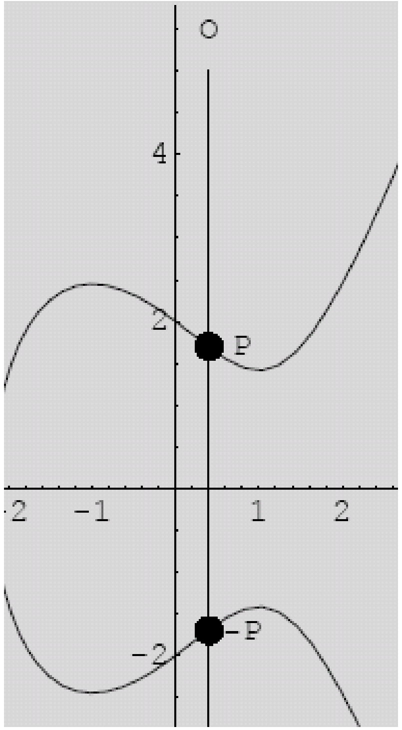


- Ryhmän määritelmän mukaan sillä pitää olla neutraalialkio. Elliptisen käyrän “Luku 0” määritellään pisteeksi O, jonka y –koordinaatti on ääretön.

Pisteelle *O* on voimassa

$$P + O = O + P = P$$

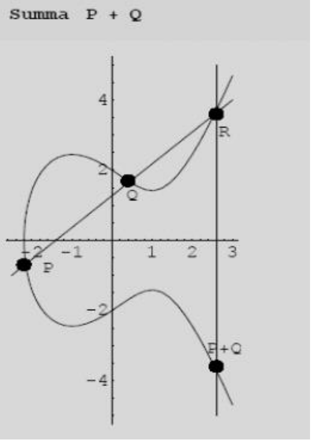
Jokaisella alkiolla P on käänteisalkio -P



Pisteen P käänteisalkiota merkitään –P. Se on pisteen P peilikuvapiste x – akselin toisella puolen

$$P + -P = -P + P = O$$

Muut ryhmäominaisuudet



- Summa P + Q on olemassa kaikille käyrän pisteille

(kahden pisteen kautta kulkeva suora aina leikkaa käyrää kolmannessa pisteessä)

- P+(Q+R) = (P+Q)+R

(usean pisteen summassa yhteenlaskujen suoritusjärjestyksellä ei väliä)

- P + Q = Q + P

(summa on vaihdannainen => ryhmä on Abelin ryhmä)

Diskreetti elliptinen käyrä

Pisteet (x,y) ovat kokonaislukupareja, missä $x,y \in Z_q = \{0,1,\ldots, q-1\}$

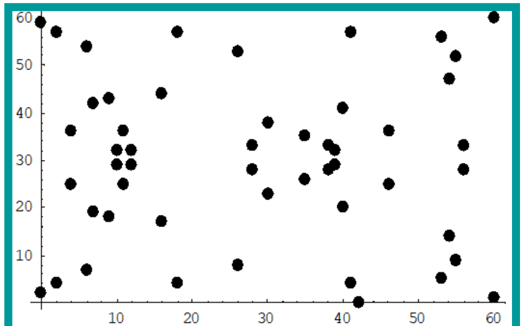
$$y^2 = x^3 + a*x + b \quad (\text{mod } q)$$

Esimerkki: Käyrä $y^2=x^3+2x+4$ joukossa Z_{61}, ts. modulus q = 61

```
In[13]:= curve = {O};
         Do[If[Mod[y^2, 61] == Mod[x^3 + 2*x + 4, 61], curve = Append[curve, {x, y}];], {x, 0, 60}, {y, 0, 60}]
         curve
         Print["Number of points ", Length[curve]]

Out[15]= {O, {0, 2}, {0, 59}, {2, 4}, {2, 57}, {4, 25}, {4, 36}, {6, 7}, {6, 54}, {7, 19}, {7, 42}, {9, 18},
 {9, 43}, {10, 29}, {10, 32}, {11, 25}, {11, 36}, {12, 29}, {12, 32}, {16, 17}, {16, 44}, {18, 4},
 {18, 57}, {26, 8}, {26, 53}, {28, 28}, {28, 33}, {30, 23}, {30, 38}, {35, 26}, {35, 35}, {38, 28},
 {38, 33}, {39, 29}, {39, 32}, {40, 20}, {40, 41}, {41, 4}, {41, 57}, {42, 0}, {46, 25}, {46, 36},
 {53, 5}, {53, 56}, {54, 14}, {54, 47}, {55, 9}, {55, 52}, {56, 28}, {56, 33}, {60, 1}, {60, 60}}

Number of points 52
```



Ryhmässä on 52 alkiota, neutraalialkio O mukaan luettuna.

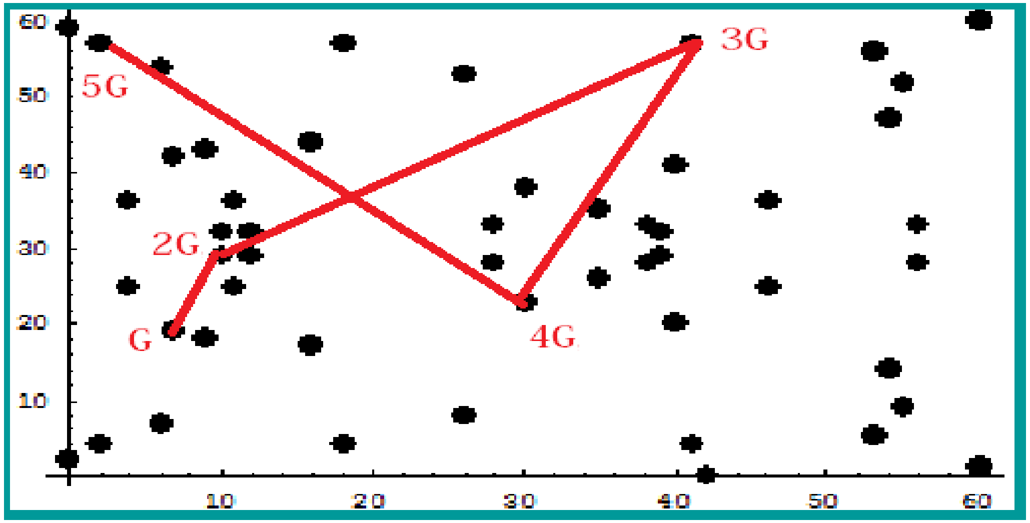
Diskreetti EC muodostaa syklisen ryhmän

Elliptisellä käyrällä on **generoiva alkio G**, joka generoi kaikki käyrän pisteet

Esimerkkikäyrämme $y^2=x^3+2x+4$ joukossa Z_{61} eräs generaattori on (7,19)

Syklinen ryhmä: G = (7,19), 2G = (8,30) , ….., 52 G = O (viimeisenä neutraalialkio) :

{{7, 19}, {8, 30}, {45, 51}, {31, 25}, {4, 58}, {36, 53}, {37, 51}, {26, 38}, {29, 20}, {40, 10},
{5, 47}, {1, 19}, {53, 42}, {47, 22}, {12, 34}, {51, 32}, {42, 58}, {60, 30}, {14, 44}, {54, 31},
{58, 16}, {15, 3}, {43, 53}, {23, 54}, {6, 48}, {35, 0}, {6, 13}, {23, 7}, {43, 8}, {15, 58}, {58, 45},
{54, 30}, {14, 17}, {60, 31}, {42, 3}, {51, 29}, {12, 27}, {47, 39}, {53, 19}, {1, 42}, {5, 14},
{40, 51}, {29, 41}, {26, 23}, {37, 10}, {36, 8}, {4, 3}, {31, 36}, {45, 10}, {8, 31}, {7, 42}, {O}}



syklinen ryhmä esimerkin käyrällä , generaattori (7,19)

EC:n käyttö salauksessa

* Perustuu matemaattiseen ongelmaan nimeltä “Diskreetin logaritmin ongelma elliptisillä käyrillä”, lyh. ECDLP (elliptic curve discrete logarithm problem)

ECDLP:

Jos tunnetaan käyrän mielivaltainen piste Y, joka on generaattorin G jokin monikerta kG , on mahdotonta äärellisessä ajassa ratkaista kerrointa k yhtälöstä

$$Y = kG$$

mikäli käyrän modulus q ja parametrit ovat suuria eli käyrällä on riittävän monta pistettä.

ECDHE key exchange

Järjestelmäparametreina ovat annettu elliptinen käyrä ja sen generaattori G.

Symmetrisestä avaimesta sopiminen tapahtuu alla olevan kaavion mukaan

A valitsee luvun a

B valitsee luvun b

A laskee ja lähettää generoivan pisteen monikerran a*G

$y_a = a\,G$

$y_b = b\,G$

B laskee ja lähettää generoivan pisteen monikerran b*G

$K = a\,(b\,G) = (ab)\,G$

A ja B laskevat symmetrisen avaimen K = abG

$K = b\,(a\,G)$

$= (ab)\,G$

Avain K on käyrän piste (x,y), josta saadaan symmetrinen AES – avain esim. ottamalla sen x –koordinaatista esim. 256 ensimmäistä bittiä.

VIESTIN SALAUS ECC:ssä

Viestien salaus ECC:ssä voidaan toteuttaa monella tavalla. Seuraavassa eräs versio, joka pohjautuu vanhaan ElGamal algoritmiin

Oletetaan , että A ja B ovat sopineet edellisellä kalvolla esitetyllä tavalla salausavaimesta K = (k1,k2)

Viestin salaus

1. A koodaa viestin lukupareiksi M = (m1, m2)

2. Alice salaa viestin tulona C = K*M , **missä**

kertolasku * määritellään $(k_1,k_2)*(m_1,m_2)=(k_1m_1,k_2m_2)$

Salakirjoituksen purku

1. Bob laskee avaimen käänteisalkion $K^{-1} = (k_1^{-1}, k_2^{-1}) \bmod q$

missä q on elliptisen käyrän modulus

3. Bob purkaa salauksen

$K^{-1}*C = (k_1^{-1}k_1m_1, k_2^{-1}k_2m_1) = (m_1,m_2) = M$

Esimerkki standardoidusta Elliptisestä käyrästä : EC192

USA:n standardiviranomainen FIPS on standardoinut joukon elliptisiä käyriä, jotka on todettu soveltuvan käytettäväksi tiedon salauksessa. Eräs niistä on käyrä EC192, jonka yhtälö, modulus q, generoiva alkio G ja yhtälössä esiintyvä vakiotermi b on annettu alla

Käyrä EC192 on $y^2 = x^3 - 3x + b$

Modulus on 192 –bittinen luku q =
6277101735386680763835789423207666416083908700390324961279

Generoiva alkio on piste G =
(602046282375688656758213480587526111916698976636884684818,
174050332293622031404857552280219410364023488927386650641)

Parametri b =
2455155546008943817740293915197451784769108058161191238065

-Kurssimateriaalin liitteenä on seminaariesitys, jossa Mathematica ohjelmaa käyttäen on implementoitu algoritmeja käyrällä EC192