

Data Security: Public key

- Nyilvános kulcsú rejtjelezés
- RSA rejtjelező
- El-Gamal rejtjelező
- ECC: Elliptikus görbe kriptográfia

Data Security: Public key

RSA

1. Véletlenszerűen választunk két "nagy" prímszámot: p_1, p_2

2. $m = p_1 p_2$ $\phi(m) = (p_1 - 1)(p_2 - 1)$

$e, \quad 1 \leq e < \phi(m) \quad (\phi(m), e) = 1$

3. $d = e^{-1} \pmod{\phi(m)}$

4. $k^p = (m, e) \quad k^s = (d, p_1, p_2)$

Kódolás: $y = x^e \pmod{m} \quad 1 \leq x < m$

Dekódolás: $x = y^d \pmod{m} \quad 1 \leq y < m$

Data Security: Public key

RSA

Diszkrét matematika előismeretek

Maradékos osztás tétele: Tetszőleges a és b , $a > 0$, $b > 0$ egészekre egyértelműen létezik q és r egész, hogy $a = b q + r$, ahol $0 \leq r < b$, $q \geq 0$.

Euklideszi l.n.k.o. algoritmus

l.n.k.o. algoritmus következménye: Tetszőleges b és c egészekre, amelyek közül legalább egyik nem nulla, léteznek s és t egészek, hogy $(b, c) = s b + t c$

Inverz modulo m : A b szám modulo m inverze akkor és csak akkor létezik, ha $(b, m) = 1$. Ha létezik inverz, akkor az egyértelmű az m -nél kisebb pozitív egészek között.

Fermat tétel: Ha a és c egész nem osztható a p prímmel, akkor $c^{p-1} = 1 \pmod{p}$

Fermat-tétel általánosítása: Ha p_1 és p_2 különböző prímek, és az c egészre teljesül, hogy $(c, p_1 p_2) = 1$, akkor $c^{(p_1-1)(p_2-1)} = 1 \pmod{p_1 p_2}$.

Kínai maradékok tétele: Ha az m_1, m_2, \dots, m_r pozitív egészek páronként relatív prímek, és a_1, a_2, \dots, a_r tetszőleges egész számok, akkor az $x = a_i \pmod{m_i}$, $i=1, \dots, r$, rendszernek van közös megoldása. Bármely két megoldás azonos modulo m_1, m_2, \dots, m_r .

Data Security: Public key

RSA

Játék RSA algoritmus:

$$p_1=7, p_2=11$$

$$m=77, \quad \varphi(m)=6*10=60=2*3*5$$

$$e=7$$

$$d = 7^{-1} \pmod{60}$$

Euklideszi algoritmus alkalmazása:

$$60=8*7+4 \quad 1*60-8*7=4$$

$$7=1*4+3 \quad 7=60-8*7+3$$

$$4=1*3+1 \quad -60+9*7=3$$

$$3=3*1+0 \quad 60-8*7=-60+9*3+1$$

$$2*60-17*7=1 \quad \text{--->} \quad (-17)*7=1 \pmod{60} \quad \text{--->} \quad d=7^{-1} = -17 = 43 \pmod{60}$$

Data Security: Public key

RSA

“Ismételt négyzetre emelés és szorzás” algoritmus

Miért előnyös az $e=3$ vagy általában $e=2^t+1$ alakú választás?

$e=2^t+1$: 1 db (moduláris) szorzás és t db négyzetre emelés,
összes szorzási műveletek száma: $t+1$

Pl.

$e=3$: 1 szorzás és 1 négyzetre emelés,

$e=2^{16}+1$: 1 szorzás és 16 négyzetre emelés.

Data Security: Public key

RSA

Primszámkeresés

Mekkora annak P valószínűsége, hogy egy véletlenszerűen választott m bit hosszú n egész ($2^{m-1} < n < 2^m$) prímszám?

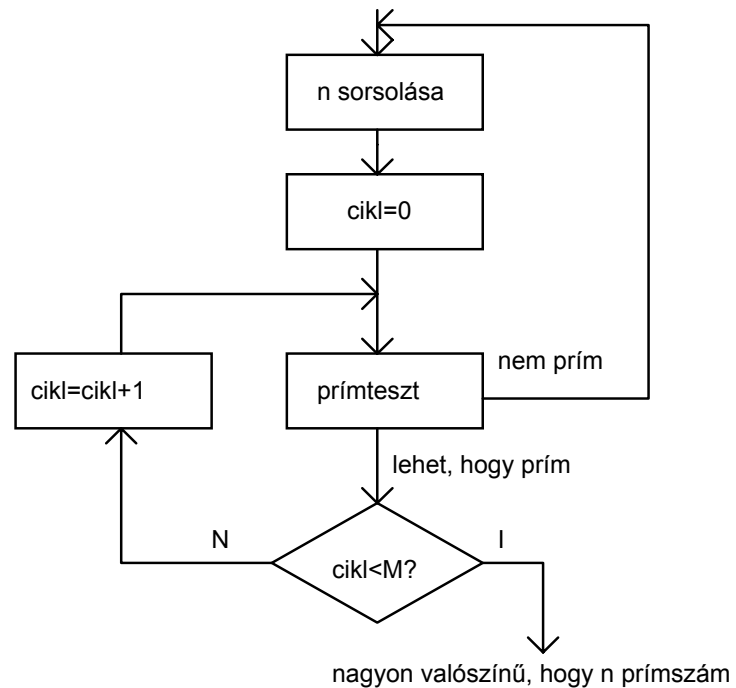
Csebisev számelméleti tétele: $\Pi(n)$ az n pozitív egésznél kisebb primek számának nagyságrendje:

$$\Pi(n) \cong \frac{n}{\ln n}$$

$$P = \frac{\Pi(2^m) - \Pi(2^{m-1})}{2^m - 2^{m-1}} \cong \frac{2^{m-1} \frac{1}{(m-1) \cdot \ln 2}}{2^{m-1}} \cong \frac{1}{(m-1) \ln(2)}$$

Data Security: Public key

RSA



Fermat-teszt: Egy n összetett szám álprím egy b bázisra nézve, ha

$$b^{n-1} = 1 \pmod{n}$$

ahol $b \in Z_n$, $Z_n = \{z : 1 < z < n \text{ és } (z, n) = 1\}$.

Miller-Rabin teszt: Egy n összetett szám *prímgyanús* egy b bázisra, ha

$$n - 1 = 2^v u, \quad u \text{ páratlan esetén}$$

$$b^u = 1 \pmod{n},$$

vagy létezik olyan $0 \leq j < v$, melyre

$$b^{2^j u} = -1 \pmod{n}$$

Data Security: Public key

RSA

$$b^{n-1} = 1 \pmod{n}$$

Fermat álprím-e 33 a $b=2$ bázisra nézve?

Nem: $2^{32} = 4 \cdot (2^5)^6 = 4 \cdot (32)^6 = 4 \cdot (-1)^6 = 4 \neq 1 \pmod{33}$

Fermat álprím-e $p-1$ a $b=p-2$ bázisra nézve, ahol p prim, $p > 3$?

Nem. $(p-2)^{p-2} = (-1)^{p-2} = -1 \pmod{p-1}$, ($p-2$ páratlan).

Data Security: Public key

RSA

Fermat-faktorizáció: $n = ab$, $a, b > 0$.

Legyen $t = (a + b) / 2$, $s = (a - b) / 2 \rightarrow a = t + s$, $b = t - s$.

$$\rightarrow n = t^2 - s^2 = (t + s)(t - s)$$

Ötlet: ha $a - b$ különbség "kicsi", akkor s is "kicsi" $\rightarrow t \approx n^{1/2}$.

Találgatás t -re: $t_1 = \text{int}(n^{1/2}) + 1$, $t_2 = \text{int}(n^{1/2}) + 2$, ...

Ellenőrzés: $t_i^2 - n$ négyzetszám?

Ha igen, akkor $t_i^2 - n = s^2 \rightarrow t, s \rightarrow a, b$.

Példa: $n = 14803$; $\text{int}(n^{1/2}) + 1 = 122 \rightarrow 122^2 - n = 81 = 9^2$,
 $a = 122 + 9 = 131$, $b = 122 - 9 = 113$.

Data Security: Public key

RSA

Kicsi kódoló kulcsok problémája

$$y_1 = x^e \pmod{m_1}$$

$$y_2 = x^e \pmod{m_2}$$

...

$$y_r = x^e \pmod{m_r} \quad r \geq e$$

Ha m_1, m_2, \dots, m_r

modulusok páronként relatív prímek, a kínai maradékok tétele alkalmazható

→ hatékonyan kiszámíthatjuk $z=x^e$ hatványt,

$$x < \min\{m_i\} \quad \rightarrow \quad 0 < x^e < m_1 m_2 \cdots m_r$$

z egész szám e-edik gyökét kiszámítva x nyílt szöveget megkapjuk!

Data Security: Public key

RSA

Közös modulus problémája

$$y_A = x^{e_A} \pmod{m} \quad y_B = x^{e_B} \pmod{m}$$

rejtett szövegek, ahol

$$(e_A, e_B) = 1 \quad \exists t, s: \quad t \cdot e_A + s \cdot e_B = 1$$

ahol $t \cdot s < 0$, mivel $e_A > 0$, $e_B > 0$

$$\text{(wlog)} \quad t < 0 \rightarrow t = -1 \cdot |t|$$

$$\text{(wlog)} \quad (y_A, m) = 1, \quad (y_A, m) = (y_B, m) = 1 \quad \rightarrow \exists \quad y_A^{-1} \pmod{m}$$

$$(y_A^{-1})^{|t|} \cdot (y_B)^s = (x^{e_A})^t \cdot (x^{e_B})^s = x^{te_A + se_B} = x \pmod{m}$$

Data Security: Public key

ElGamal

El-Gamal rejtjelező

G: multiplikatív csoport g generátor elemmel

Kulcspár: $pk=X$, $sk=x$,

ahol $X=g^x$, x véletlen elem $S=\{1,2,\dots,|G|\}$ halmazból

Rejtjelezés:

$m \in S$

$E_{pk}(m)=(Y,b)$,

ahol $Y=g^y$, y véletlen elem S halmazból

$b=Km$, $K=X^y$

Dekódolás:

(Y,b) rejtett szöveg

$D_{sk}(Y,b)=m$, $K=Y^x$, $m=b/K$,

Data Security: Public key

ECC

Elliptikus görbe F test felett:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad a_i \in F$$

$\text{char}(F) \neq 2$, $a_1 = a_3 = 0$ (karakterisztika)

$\text{char}(F) = 2$, szuperszinguláris: $a_1 = 0$ ($y^2 + a_3y = \dots$)

nem-szuperszinguláris: $a_3 = 0$ ($y^2 + a_1xy = \dots$)

$\text{char}(F) \neq 2, 3 \rightarrow y^2 = f(x)$, $f(x)$ harmadfokú polinom

\rightarrow változócsere \rightarrow Weierstrass normál alak: $y^2 = x^3 + ax + b$

(x^2 -es tag eliminálása)

Példa: $y^2 - 2y = x^3 - x^2$

$y \rightarrow y - 1$

$x \rightarrow x - 1/3$

$y^2 = x^3 + 1/3x + 1/27$

Data Security: Public key

ECC

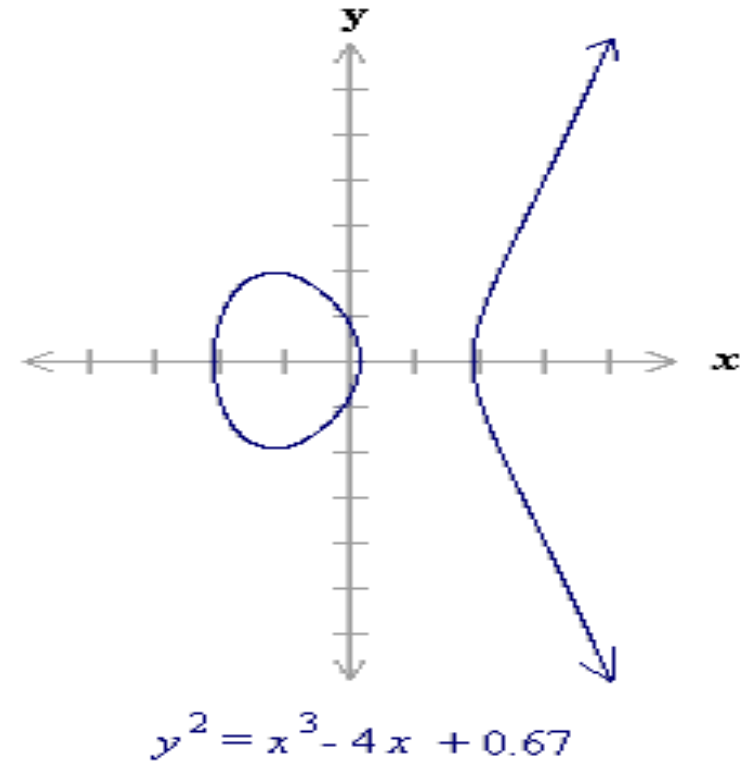
EC valós számtest felett

$E/R = \{(x,y) : y^2 = x^3 + ax + b\}$, ahol x, y, a, b valós

$x^3 + ax + b$ nincs ismételt faktor ($4a^3 + 27b^2 \neq 0$) \rightarrow

$\{E/R \cup O, +\}$ csoport

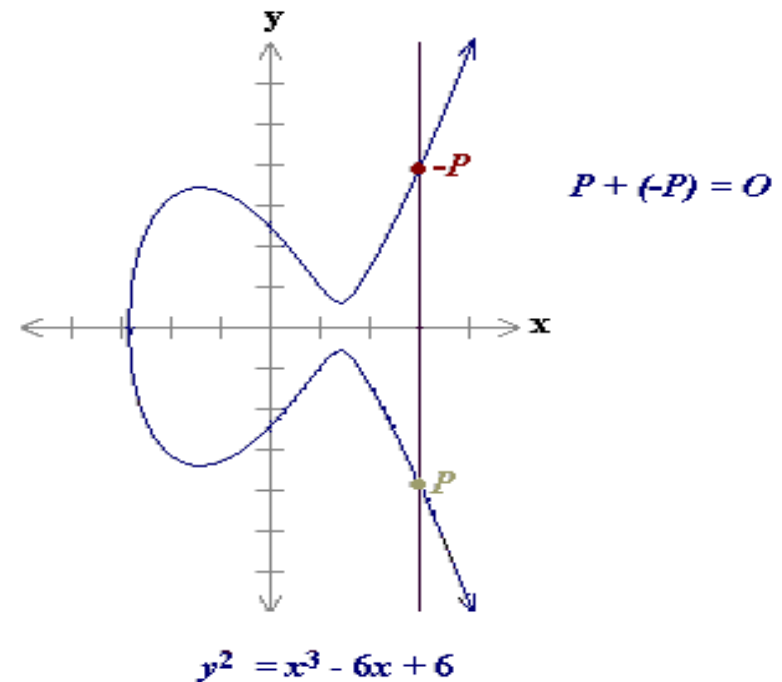
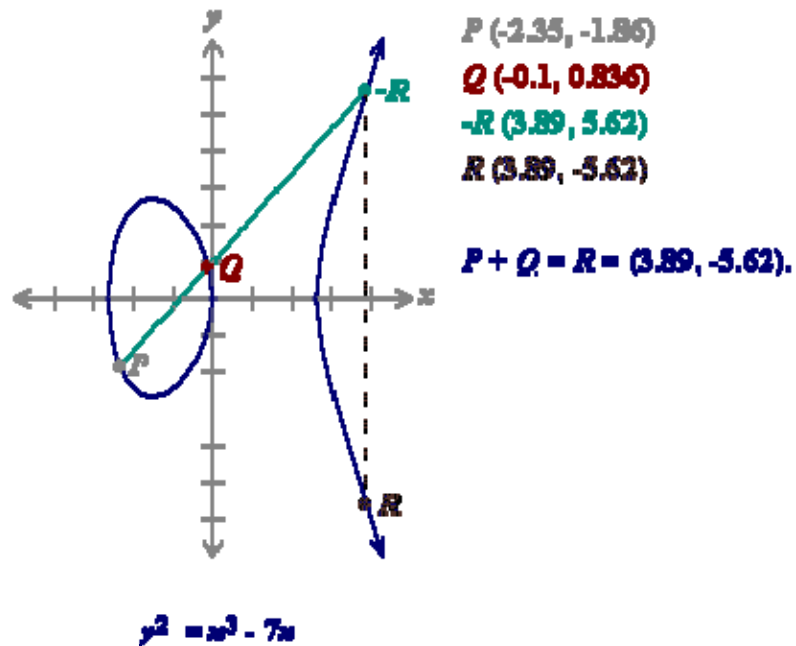
O : végtelenben fekvő pont



Data Security: Public key

ECC

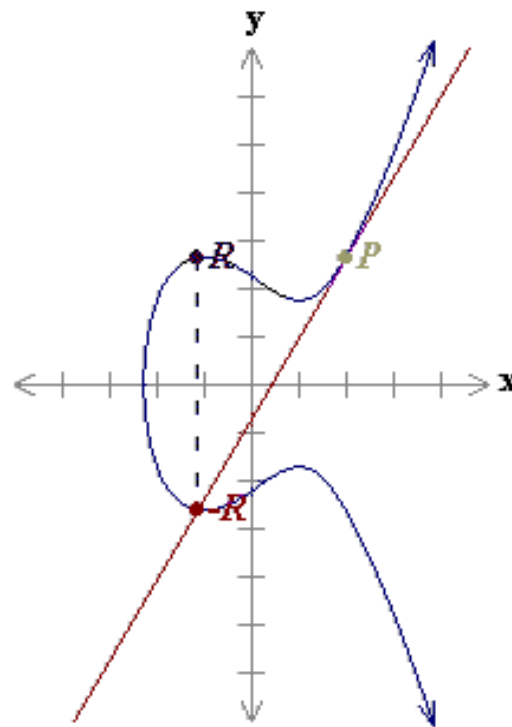
Összeadás művelet: $P+Q=R$



Data Security: Public key

ECC

$$2P = P + P = R$$



$$P (2, 2.65)$$

$$-R (-1.11, -2.64)$$

$$R (-1.11, 2.64)$$

$$2P = R = (-1.11, 2.64).$$

$$y^2 = x^3 - 3x + 5$$

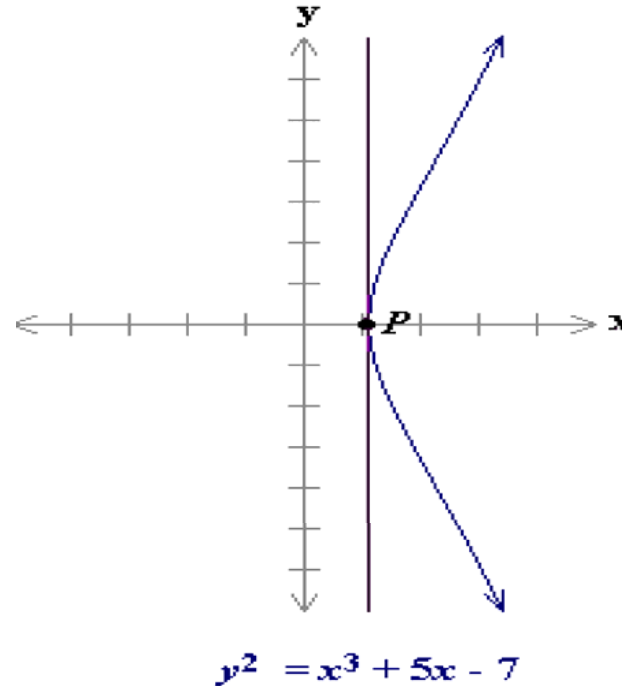
Data Security: Public key

ECC

2P, ha $y_P = 0$

Definició: $2P = O$!

$3P = 2P + P = O + P = P$, $4P = O$, $5P = P$,
 $6P = O$, $7P = P$,...



Data Security: Public key

ECC

P+Q:

$$P=(x_1,y_1), Q=(x_2,y_2), P+Q=(x_3,y_3) \quad (P \neq -Q)$$

$$y=sx+\beta, \quad s=(y_2-y_1)/(x_2-x_1), \quad \beta=y_1-s x_1$$

$$y^2=(sx+\beta)^2=x^3+ax+b \quad : x_1, x_2 \text{ két megoldás}$$

$$x^3 - s^2x^2 + (a-2s\beta)x + (b-\beta^2) = 0 \rightarrow s^2 = x_1 + x_2 + x_3 \rightarrow x_3 = s^2 - x_1 - x_2$$

$$x_3 = [(y_2-y_1)/(x_2-x_1)]^2 - x_1 - x_2$$

$$y_3 = -y_1 + [(y_2-y_1)/(x_2-x_1)](x_1 - x_3)$$

Data Security: Public key ECC

Elliptikus Görbe F_p felett

$$y^2 = x^3 + ax + b \pmod{p}$$

$x^3 + ax + b \pmod{p}$ nincs ismételt faktora ($4a^3 + 27b^2 \neq 0 \pmod{p}$)

$\rightarrow \{E/F_p \cup O, +\}$ csoport

O : végtelenben fekvő pont

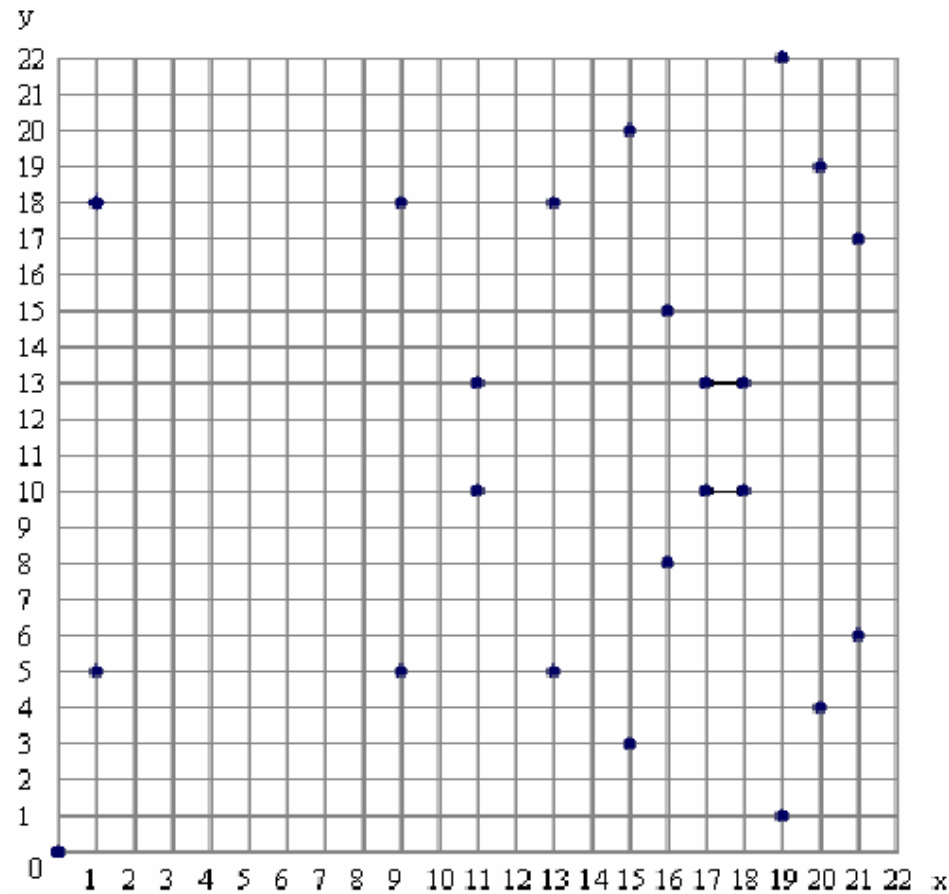
Példa: F_{23} $y^2 = x^3 + x \pmod{23}$.

23 db görbén fekvő pont:

(0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5)
(13,18) (15,3) (15,20) (16,8) (16,15) (17,10) (17,13) (18,10)
(18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17)

Data Security: Public key

ECC



$$y^2 = x^3 + x \pmod{23}$$

Data Security: Public key ECC

Elliptikus Görbe F_2^m felett

$$y^2 + xy = x^3 + ax^2 + b$$

Példa: F_{2^4}

$f(x) = x^4 + x + 1$ (aritmetika polinom)

$g = (0010)$: generátor. G hatványai:

$$\begin{aligned} g^0 &= (0001) & g^1 &= (0010) & g^2 &= (0100) & g^3 &= (1000) & g^4 &= (0011) & g^5 &= (0110) \\ g^6 &= (1100) & g^7 &= (1011) & g^8 &= (0101) & g^9 &= (1010) & g^{10} &= (0111) & g^{11} &= (1110) \\ g^{12} &= (1111) & g^{13} &= (1101) & g^{14} &= (1001) & g^{15} &= (0001) \end{aligned}$$

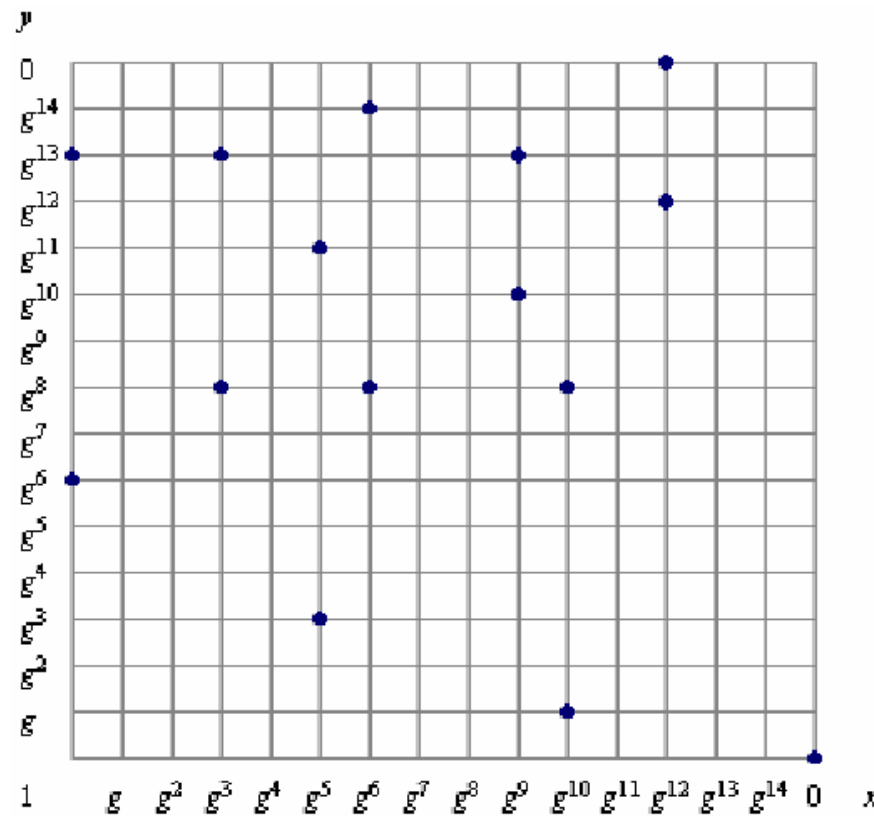
$$y^2 + xy = x^3 + g^4x^2 + 1 \quad (a = g^4, b = g^0 = 1)$$

15 db görbén fekvő pont:

$$\begin{aligned} &(1, g^{13}) (g^3, g^{13}) (g^5, g^{11}) (g^6, g^{14}) (g^9, g^{13}) (g^{10}, g^8) (g^{12}, g^{12}) \\ &(1, g^6) (g^3, g^8) (g^5, g^3) (g^6, g^8) (g^9, g^{10}) (g^{10}, g) (g^{12}, 0) (0, 1) \end{aligned}$$

Data Security: Public key

ECC



$$y^2 + xy = x^3 + g^4x^2 + 1$$

Data Security: Public key ECC

Elliptikus görbék feletti diszkrét logaritmus probléma (ECDLP).

ECDLP: adott a csoport két pontja P és Q , adjuk meg azt a k természetes számot, amelyre $kP = Q$;

k : Q diszkrét logaritmus P bázisra

Példa:

$$y^2 = x^3 + 9x + 17 \text{ over } F_{23},$$

Adjuk meg $Q = (4,5)$ diszkrét logaritmusát $P = (16,5)$ bázisra nézve!

$$P = (16,5) \quad 2P = (20,20) \quad 3P = (14,14) \quad 4P = (19,20) \quad 5P = (13,10) \quad 6P = (7,3) \quad 7P = (8,7) \quad 8P = (12,17) \quad 9P = (4,5)$$

Mivel $9P = (4,5) = Q$, így $k = 9$.

Data Security: Public key ECC

ECC Diffie-Hellman kulcscsere:

$E/GF(q)$

Q: publikus pont $E/GF(q)$ görbén:

1. $A \rightarrow B: k_A Q$
2. $B \rightarrow A: k_B Q$
3. A: $P = k_A(k_B Q)$
B: $P = k_B(k_A Q),$

ahol k_A, k_B véletlen egészek $\{1, 2, \dots, |E|\}$ halmazból.

Passzív támadó ismerete $\{E/GF(q), k_A Q, k_B Q, Q\}$,
célja $P = k_A k_B Q$ kiszámítása.

Data Security: Public key ECC

ECC El-Gamal rejtjelező

$E/\text{GF}(q)$

Q : publikus pont $E/\text{GF}(q)$ görbén

1. $B: k_B Q$

2. $A \rightarrow B: rQ, M+r(k_B Q)$

ahol k_B, r véletlen egészek $\{1, 2, \dots, |E|\}$ halmazból.