Criptografia com Maple

LNCC - Verão/2005

Fábio Borges & Renato Portugal

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus),\ a \in G$ e $n \in \mathbb{N}^*$
- calcula $b = a^n$ e envia a e b

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$
- calcula $b = a^n$ e envia a e b
- Ana $\alpha : \mathrm{msg} \to w \in G$ escolhe $k \in \mathbb{N}^*$ e calcula $y = a^k$ e $z = wb^k \in G$ e envia y e z

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus),\ a \in G$ e $n \in \mathbb{N}^*$
- calcula $b = a^n$ e envia a e b
- Ana $\alpha : \mathrm{msg} \to w \in G$ escolhe $k \in \mathbb{N}^*$ e calcula $y = a^k$ e $z = wb^k \in G$ e envia y e z
- Beth calcula
  $zy^{-n} = wb^k(a^k)^{-n} = w(ba^{-n})^k = w(1)^k = w$

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$
- calcula $b = a^n$ e envia a e b
- Ana $\alpha : \mathrm{msg} \to w \in G$ escolhe $k \in \mathbb{N}^*$ e calcula $y = a^k$ e $z = wb^k \in G$ e envia y e z
- Beth calcula $zy^{-n} = wb^k(a^k)^{-n} = w(ba^{-n})^k = w(1)^k = w$
- Se $|a| = m$ ou $|G| = m$ então $y^{-n} = y^{m-n}$

Exemplo ElGamal

- Ana quer mandar uma mensagem para Beth

Exemplo ElGamal

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $p = 1000000007$, $a = 419666093$, $n = 110691024$ e calcula $b = a^n \mod p = 215094385$ e envia $p,\ a$ e b

Exemplo ElGamal

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $p = 1000000007$, $a = 419666093$, $n = 110691024$ e calcula $b = a^n \mod p = 215094385$ e envia $p,\ a$ e b
- Ana: $\alpha : \mathrm{msg} \rightarrow w = 12140303$ escolhe $k = 633071297$ e calcula $y = a^k \mod p = 295903670$ e $z = wb^k \mod p = 763646857$

Exemplo ElGamal

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $p = 1000000007$, $a = 419666093$, $n = 110691024$ e calcula $b = a^n \mod p = 215094385$ e envia $p,\ a$ e b
- Ana: $\alpha : \mathrm{msg} \rightarrow w = 12140303$ escolhe $k = 633071297$ e calcula $y = a^k \mod p = 295903670$ e $z = wb^k \mod p = 763646857$
- Beth lê calculando $zy^{-n} \mod p = 12140303$

Exemplo II - ElGamal

- Ana quer mandar uma mensagem para Beth

Exemplo II - ElGamal

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $a = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $n = 5$ calcula

$b = a^5 = \begin{bmatrix} 25 & 21 \\ 17 & 13 \end{bmatrix}$, sobre $\mathbb{Z}_{27}$ esconde o n

Exemplo II - ElGamal

- Ana faz $w = \begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix}$, escolhe $k = 3$ e calcula

$$y = a^k = \begin{bmatrix} 37 & 54 \\ 81 & 118 \end{bmatrix} \text{ e } z = wb^k = \begin{bmatrix} 15 & 4 \\ 22 & 7 \end{bmatrix}$$

Exemplo II - ElGamal

- Ana faz $w = \begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix}$, escolhe $k = 3$ e calcula

$$y = a^k = \begin{bmatrix} 37 & 54 \\ 81 & 118 \end{bmatrix} \text{ e } z = wb^k = \begin{bmatrix} 15 & 4 \\ 22 & 7 \end{bmatrix}$$

- Ana lê calculando $zy^{-n} = \begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix}$

Curvas Elípticas

Seja $\mathbb{F}$ um corpo de característica diferente de 2 ou 3 e $c, d \in \mathbb{F}$ t.q. $x^3 + cx + d$ seja livre de raiz, i.e.

$$4c^3 + 27d^2 \neq 27$$

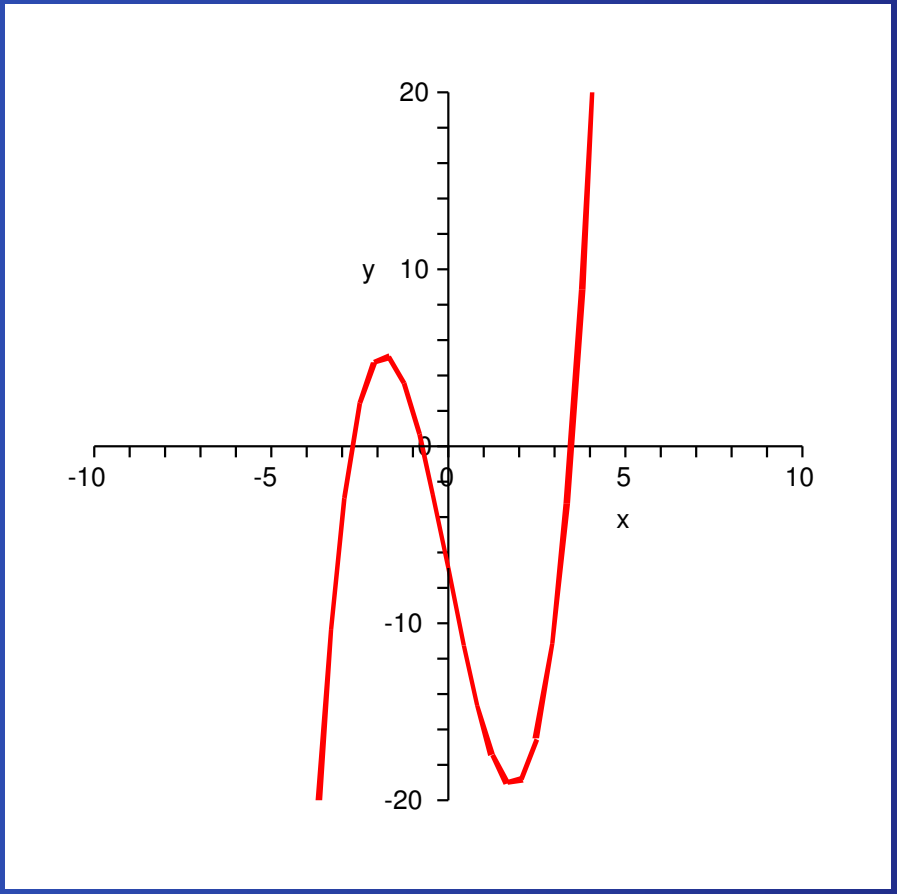
então o conj. dos pontos $(x, y) \in \mathbb{F} \times \mathbb{F}$ que são soluções de

$$y^2 = x^3 + cx + d$$

junto com um elemento neutro chamado ponto no infinito $\overline{O}$ é uma Curva Elíptica

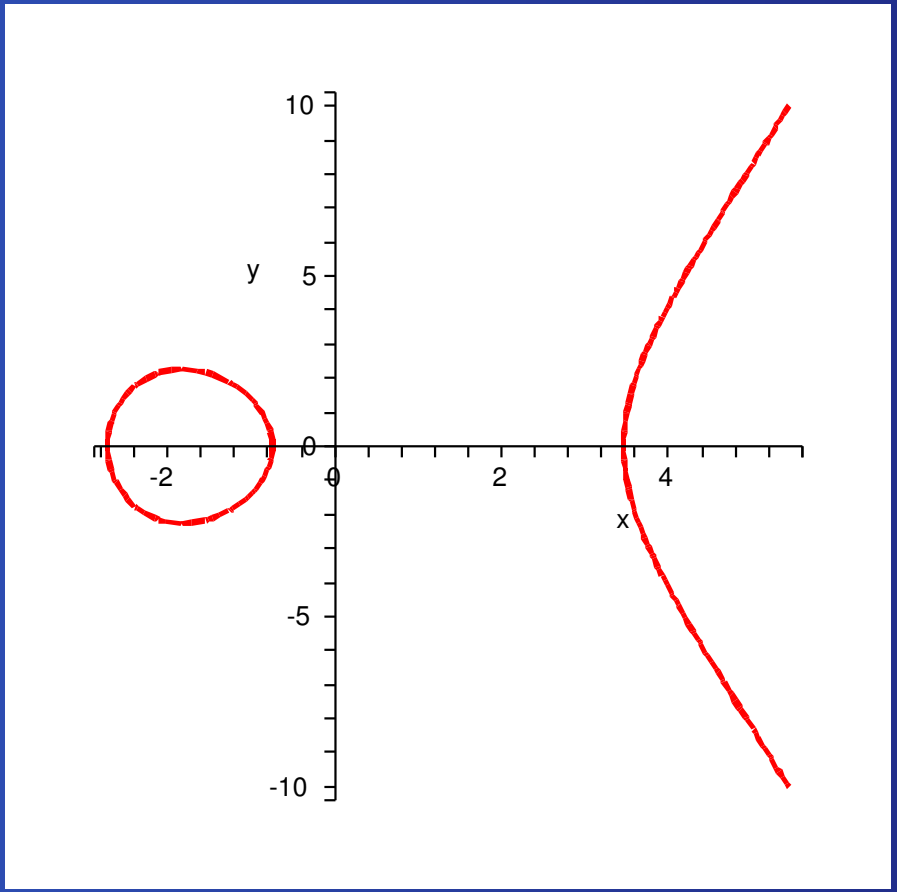
Gráfico

$$y = x^3 - 10x - 7$$



Gráfico

$$y^2 = x^3 - 10x - 7$$



Operação

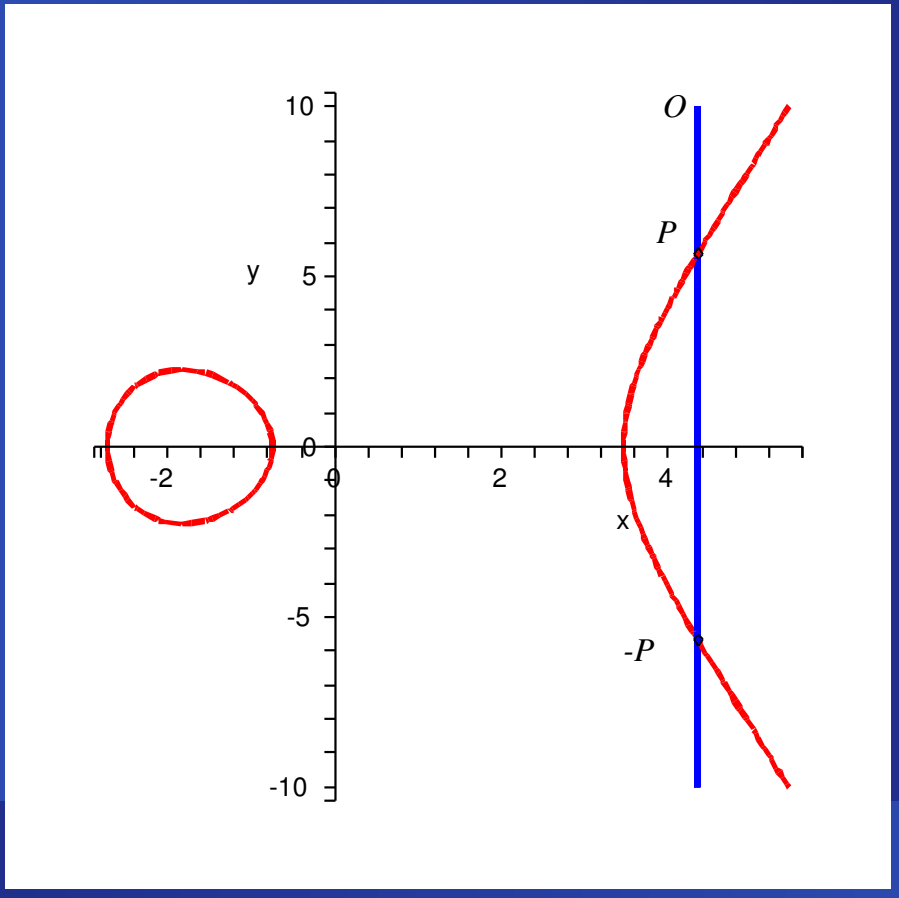
- $P + \overline{O} = P \qquad \forall P \in E$

Operação

- $P + \overline{O} = P \qquad \forall P \in E$
- $P = (x, y)$ definimos $-P = (x, -y)$

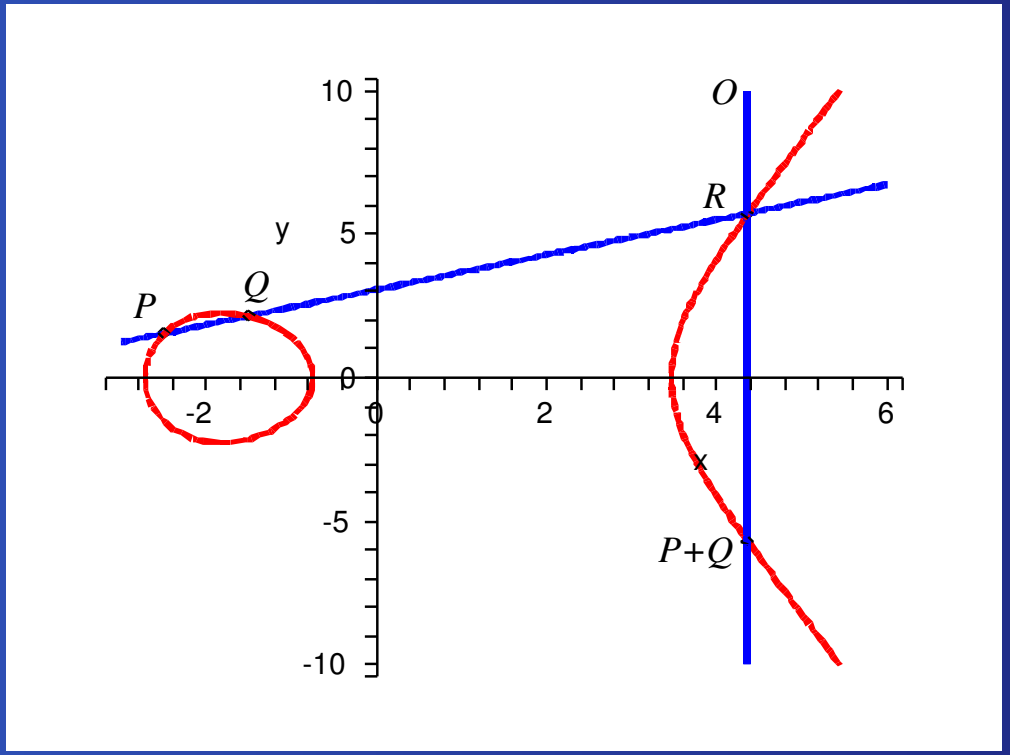
Operação

- $P + \overline{O} = P \qquad \forall P \in E$
- $P = (x, y)$ definimos $-P = (x, -y)$



Operação (I cont.)

Se $P, Q \in E$ e $P \neq \pm Q$ e a reta $\overline{PQ}$ não é tangente a P ou Q então a reta vai interceptar um ponto R. Definimos $P + Q = -R$



Operação (II cont.)

- Se $P \neq \pm Q$ e $\overline{PQ}$ é tangente a P definimos $P + Q = -P$

Operação (II cont.)

- Se $P \neq \pm Q$ e $\overline{PQ}$ é tangente a P definimos $P + Q = -P$
- Se P não é ponto de inflexão, definimos $P + P = -R$

Operação (II cont.)

- Se $P \neq \pm Q$ e $\overline{PQ}$ é tangente a P definimos $P + Q = -P$
- Se P não é ponto de inflexão, definimos $P + P = -R$
- Se P é ponto de inflexão $P + P = -P$

Discreto

Se $P = Q$ definimos:

$$x_3 = \left(\frac{3x_1^2+c}{2y_1}\right)^2 - 2x_1 \mod p$$

$$y_3 = \left(\frac{3x_1^2+c}{2y_1}\right)(x_1 - x_3) - y_1 \mod p$$

Discreto

Se $P \neq \pm Q$ definimos:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \mod p$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \mod p$$

Curva Elíptica em $\mathbb{Z}_{23}$

Se $a = 1$ e $b = 0$ temos

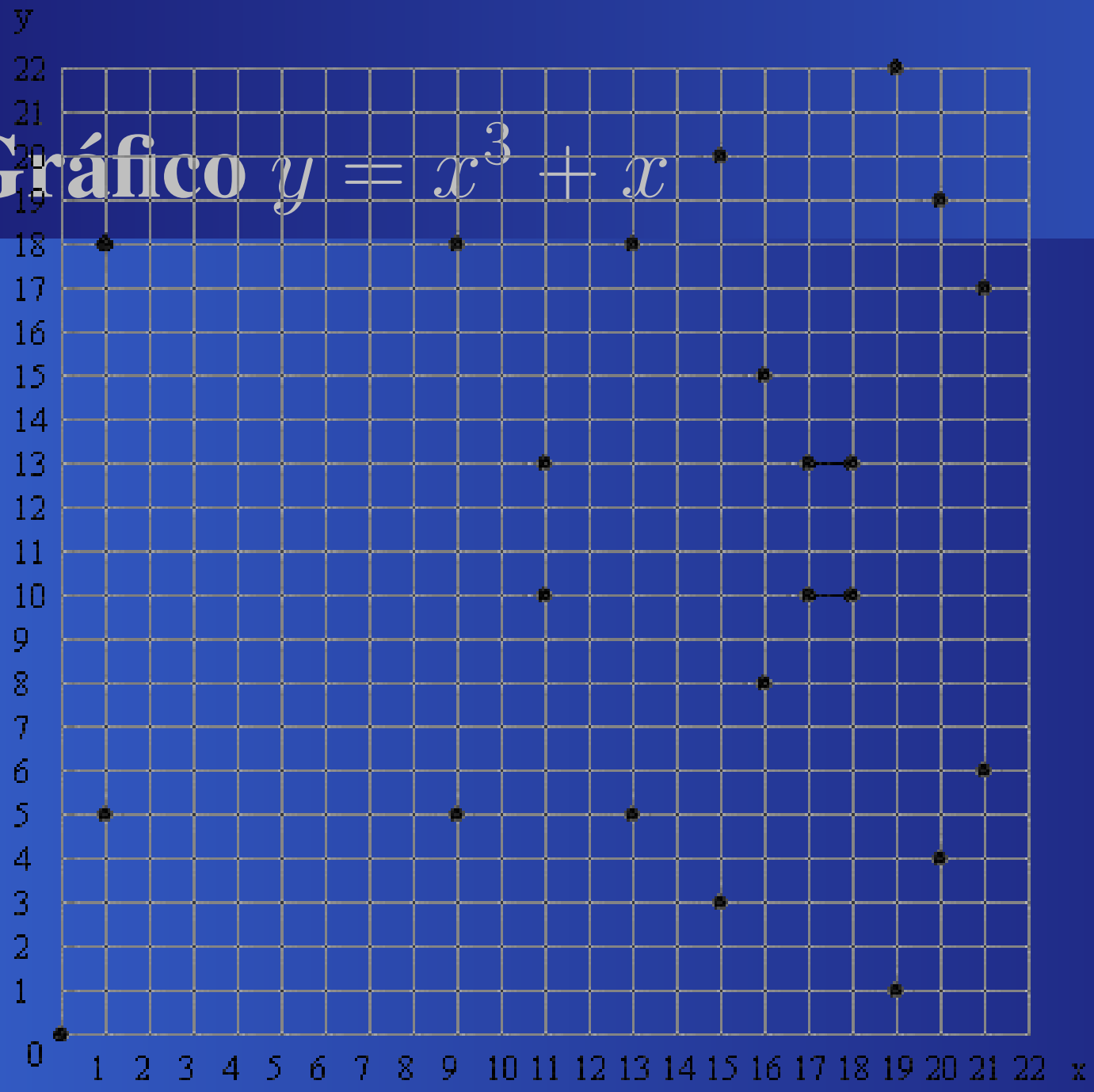
$$y^2 = x^3 + x$$

O ponto (9,5) satisfaz a equação:

$$\begin{aligned} y^2 &= x^3 + x \\ 5^2 &= 729 + 9 \\ 25 &= 738 \\ 2 &= 2 \end{aligned}$$

Existem 23 pontos que satisfazem esta equação

Gráfico $y == x^3 + x$



Tamanho do Conjunto

Se E é uma Curva Elíptica sobre $\mathbb{Z}_p$

$$p + 1 - 2\sqrt{p} \leqslant |E| \leqslant p + 1 + 2\sqrt{p}$$

Criptografando

- Ana quer mandar uma mensagem para Beth

Criptografando

- Ana quer mandar uma mensagem para Beth
- Beth escolhe um primo p grande, c e d t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a \in E$ com ordem grande e n, calcula $b = na$ e envia p, c, d, a e b

Criptografando

- Ana quer mandar uma mensagem para Beth
- Beth escolhe um primo p grande, c e d t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a \in E$ com ordem grande e n, calcula $b = na$ e envia p, c, d, a e b
- Ana $\alpha : \mathrm{msg} \rightarrow w \in E$ escolhe k, calcula $y = ka$ e $z = w + kb \in E$, envia y e z

Criptografando

- Ana quer mandar uma mensagem para Beth
- Beth escolhe um primo p grande, c e d t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a \in E$ com ordem grande e n, calcula $b = na$ e envia p, c, d, a e b
- Ana $\alpha : \mathrm{msg} \rightarrow w \in E$ escolhe k, calcula $y = ka$ e $z = w + kb \in E$, envia y e z
- Beth pode ler calculando $z - ny = w + kb - nka = w + kb - kb = w$

Ex. Criptografando

- Beth escolhe um primo $p = 19$ grande, $c = 1$ e $d = 6$ t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a = (0, 5)$ com ordem grande e $n = 4$, calcula $b = na = 4(0, 5) = (3, 6)$ e envia p, c, d, a e b

Ex. Criptografando

- Beth escolhe um primo $p = 19$ grande, $c = 1$ e $d = 6$ t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a = (0, 5)$ com ordem grande e $n = 4$, calcula $b = na = 4(0, 5) = (3, 6)$ e envia p, c, d, a e b
- Ana $\alpha : \text{msg} \longrightarrow w = (18, 17)$ escolhe $k = 3$, calcula $y = ka = 3(0, 5) = (2, 4)$ e $z = w + kb = (18, 17) + 3(3, 6) = (14, 3)$, envia y e z

Ex. Criptografando

- Beth escolhe um primo $p = 19$ grande, $c = 1$ e $d = 6$ t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a = (0, 5)$ com ordem grande e $n = 4$, calcula $b = na = 4(0, 5) = (3, 6)$ e envia p, c, d, a e b
- Ana $\alpha : \text{msg} \rightarrow w = (18, 17)$ escolhe $k = 3$, calcula $y = ka = 3(0, 5) = (2, 4)$ e $z = w + kb = (18, 17) + 3(3, 6) = (14, 3)$, envia y e z
- Beth pode ler calculando $z - ny = (14, 3) - 4(2, 4) = (14, 3) - (12, 6) = (14, 3) + (12, 13) = (18, 17)$

Menezes-Vanstone

- Beth escolhe um primo p grande, c e d t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a \in E$ com ordem grande e n, calcula $b = na$ e envia p, c, d, a e b

Menezes-Vanstone

- Beth escolhe um primo p grande, c e d t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a \in E$ com ordem grande e n, calcula $b = na$ e envia p, c, d, a e b
- Ana $\alpha : \text{msg} \rightarrow w \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ escolhe k, calcula $y = ka$, $kb = (c_1, c_2) \in E$ e $z = (z_1, z_2) = (c_1 w_1 \mod p, c_2 w_2 \mod p)$, envia y e z

Menezes-Vanstone

- Beth escolhe um primo p grande, c e d t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a \in E$ com ordem grande e n, calcula $b = na$ e envia p, c, d, a e b
- Ana $\alpha : \text{msg} \rightarrow w \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ escolhe k, calcula $y = ka$, $kb = (c_1, c_2) \in E$ e $z = (z_1, z_2) = (c_1 w_1 \mod p, c_2 w_2 \mod p)$, envia y e z
- Beth calcula $ny = nka = kna = kb$ depois $\left(c_1^{-1} z_1 \mod p, c_2^{-1} z_2 \mod p\right) =$ $\left(c_1^{-1} c_1 w_1 \mod p, c_2^{-1} c_2 w_2 \mod p\right) = w$

Ex. Menezes-Vanstone

- Beth escolhe $p = 19$, $c = 1$ e $d = 6$ t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a = (0, 5)$ e $n = 4$, calcula $b = na = (3, 6)$ e envia p, c, d, a e b

Ex. Menezes-Vanstone

- Beth escolhe $p = 19$, $c = 1$ e $d = 6$ t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a = (0, 5)$ e $n = 4$, calcula $b = na = (3, 6)$ e envia p, c, d, a e b
- Ana $\alpha : \text{msg} \rightarrow w = (5, 13) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ escolhe $k = 3$, calcula $y = ka = (2, 4)$, $kb = (12, 6) \in E$ e $z = ((12)(5) \mod p, (6)(13) \mod p) = (3, 2)$, envia y e z

Ex. Menezes-Vanstone

- Beth escolhe $p = 19$, $c = 1$ e $d = 6$ t.q. $4c^3 + 27d^2 \neq 0 \mod p$, $a = (0, 5)$ e $n = 4$, calcula $b = na = (3, 6)$ e envia p, c, d, a e b
- Ana $\alpha : \text{msg} \rightarrow w = (5, 13) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ escolhe $k = 3$, calcula $y = ka = (2, 4)$, $kb = (12, 6) \in E$ e $z = ((12)(5) \mod p, (6)(13) \mod p) = (3, 2)$, envia y e z
- Beth calcula $ny = (12, 6)$ depois $\left((12)^{-1}(3) \mod p, (6)^{-1}(2) \mod p\right) = ((8)(3) \mod p, (16)(2) \mod p) = (5, 13)$

Comparação de Mensagens

- Com E sobre $\mathbb{Z}_{19}$

Comparação de Mensagens

- Com E sobre $\mathbb{Z}_{19}$
- ElGamal usual temos $|E| = 18$

Comparação de Mensagens

- Com E sobre $\mathbb{Z}_{19}$
- ElGamal usual temos $|E| = 18$
- Menezes-Vanstone temos $|\mathbb{Z}_{19}^*|^2 = 324$

Último Slide

- Obrigado.
- Quaisquer sugestões serão bem-vindas.

www.lncc.br/borges