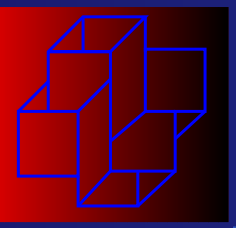


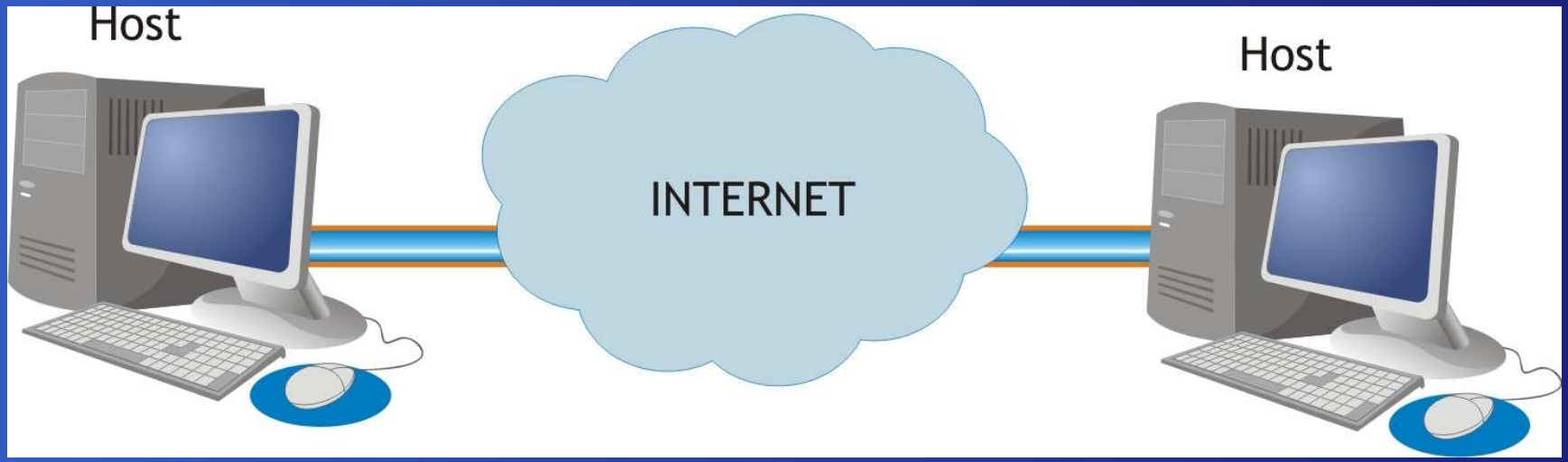
Falando um segredo em público a um estranho e mantendo o segredo

UEL - Out/2007

Fábio Borges de Oliveira

LNCC

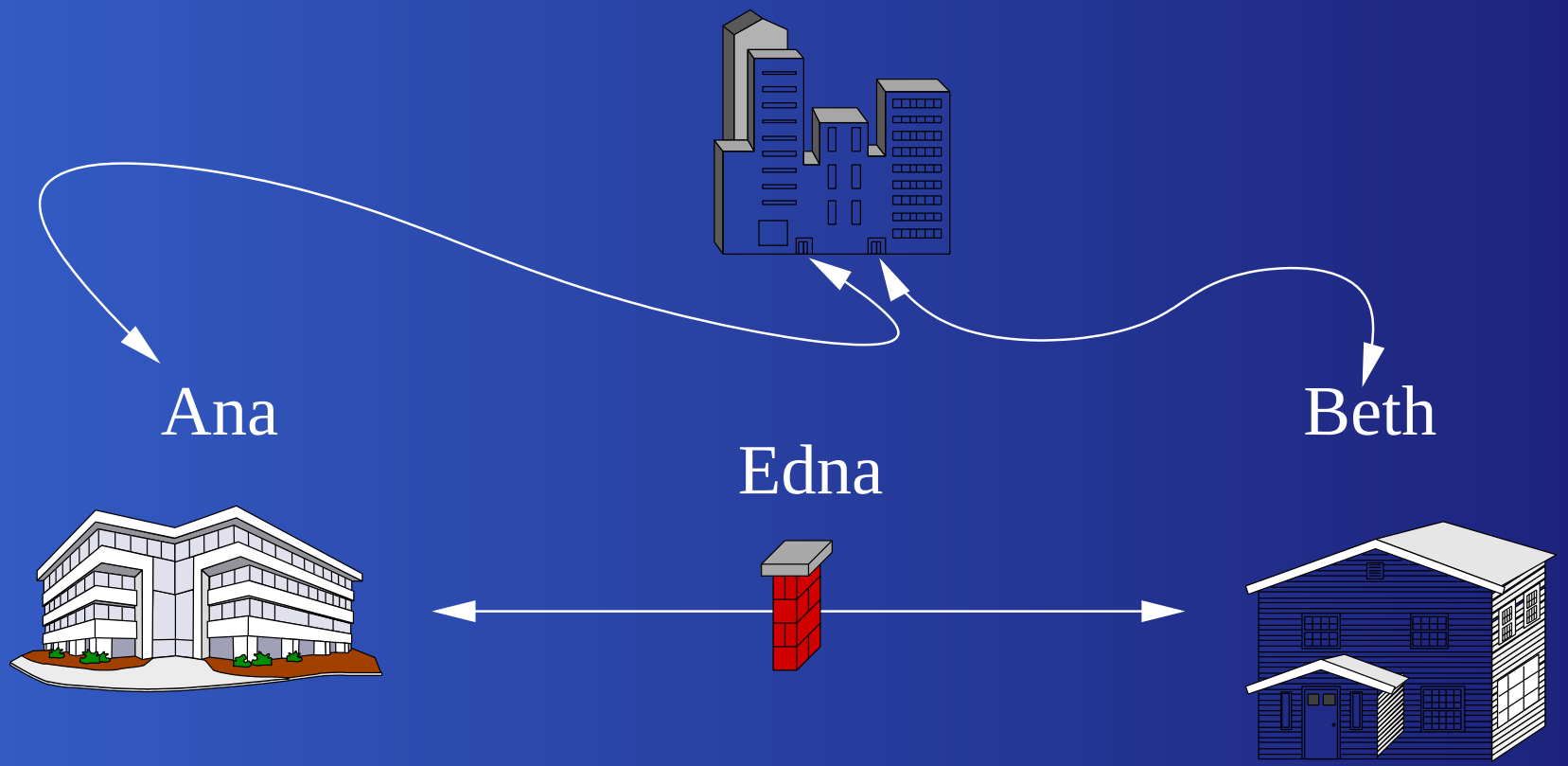
Origem do problema

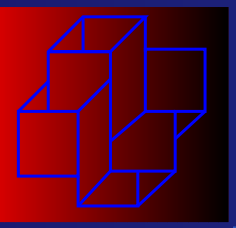


- Falando significa transmitindo
- Meio público significa canal inseguro
- Estranho significa não credenciado
- Manter o segredo significa mensagem cifrada

Simétrica

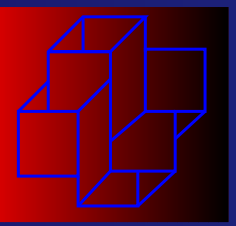
Assimétrica





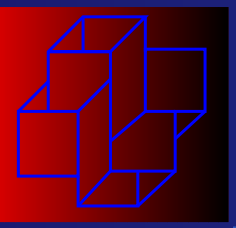
Entre outras Matemáticas

- Simétrica
  - César – Estatística
  - Hill – Matrizes Involutórias
  - AES – Corpos de Galois – $GF(2^8)$
- Assimétrica
  - RSA – PFI
  - ECC – Curvas Elípticas
  - Diffie-Hellman – índice ou PLD
  - ElGamal – Grupo
  - Menezes-Vanstone – Escalar – $k \cdot P$



Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$
  - $D_k(C) = M$
  - $D_k(E_k(M)) = M$
  - $D_r(E_k(M)) = S$
- Assimétrica
  - $E_a(M) = C$
  - $D_b(C) = M$
  - $D_a(E_b(M)) = M$
  - $D_r(E_a(M)) = S$



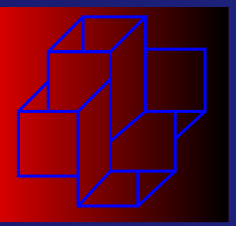
Quantas chaves são necessárias?

- Criptografia Simétrica

$$\#k = \frac{n(n-1)}{2}$$

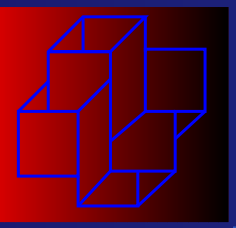
- Criptografia Assimétrica

$$\#k = 2n$$



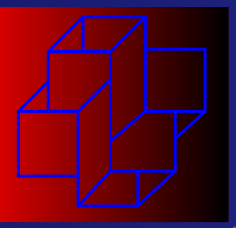
Diffie-Hellman

1. A escolhe dois primos p e q, faz $R = \mathbb{Z}_{pq}$
2. A escolhe $1 < k \in R$ tal que $(k, pq) = 1$ e envia k e R para B
3. A escolhe $1 < r \in R$, calcula k^r e envia o resultado para B mantendo r em segredo
4. B escolhe $1 < s \in R$, calcula k^s e envia o resultado para A mantendo s em segredo
5. Ambos calculam $a = (k^r)^s = (k^s)^r$



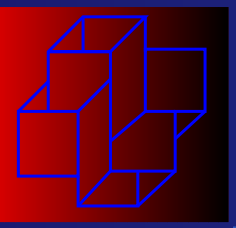
ElGamal

1. B escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$
2. B calcula $b = a^n$ e envia a, b e G, escondendo n
3. A aplica $\alpha : m \longrightarrow w \in G$, escolhe $k \in \mathbb{N}^*$, calcula $y = a^k$ e $z = wb^k \in G$, depois envia y e z
4. Somente B calcula $zy^{-n} = wb^k(a^k)^{-n} = w(ba^{-n})^k = w(1)^k = w$



Número de bits recomendado

ECC	RSA	Razão
163	1024	1/6
256	3072	1/12
384	7680	1/20
512	15360	1/30



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.

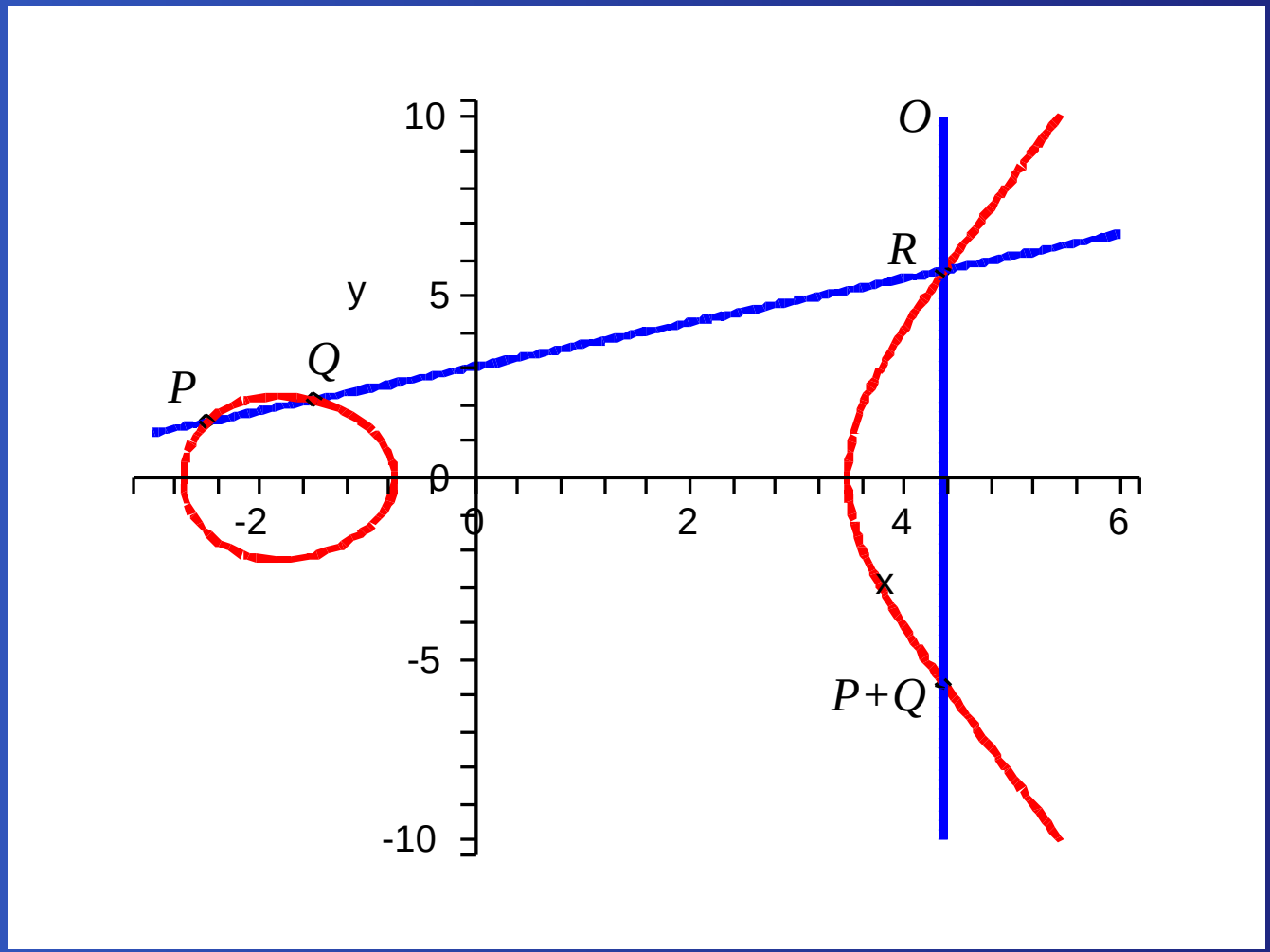
$$4c^3 + 27d^2 \neq 27$$

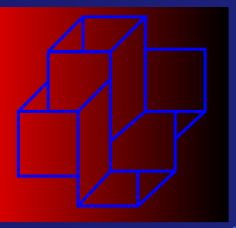
então o conj. dos pontos $(x, y) \in \mathbb{F} \times \mathbb{F}$ que são soluções de

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

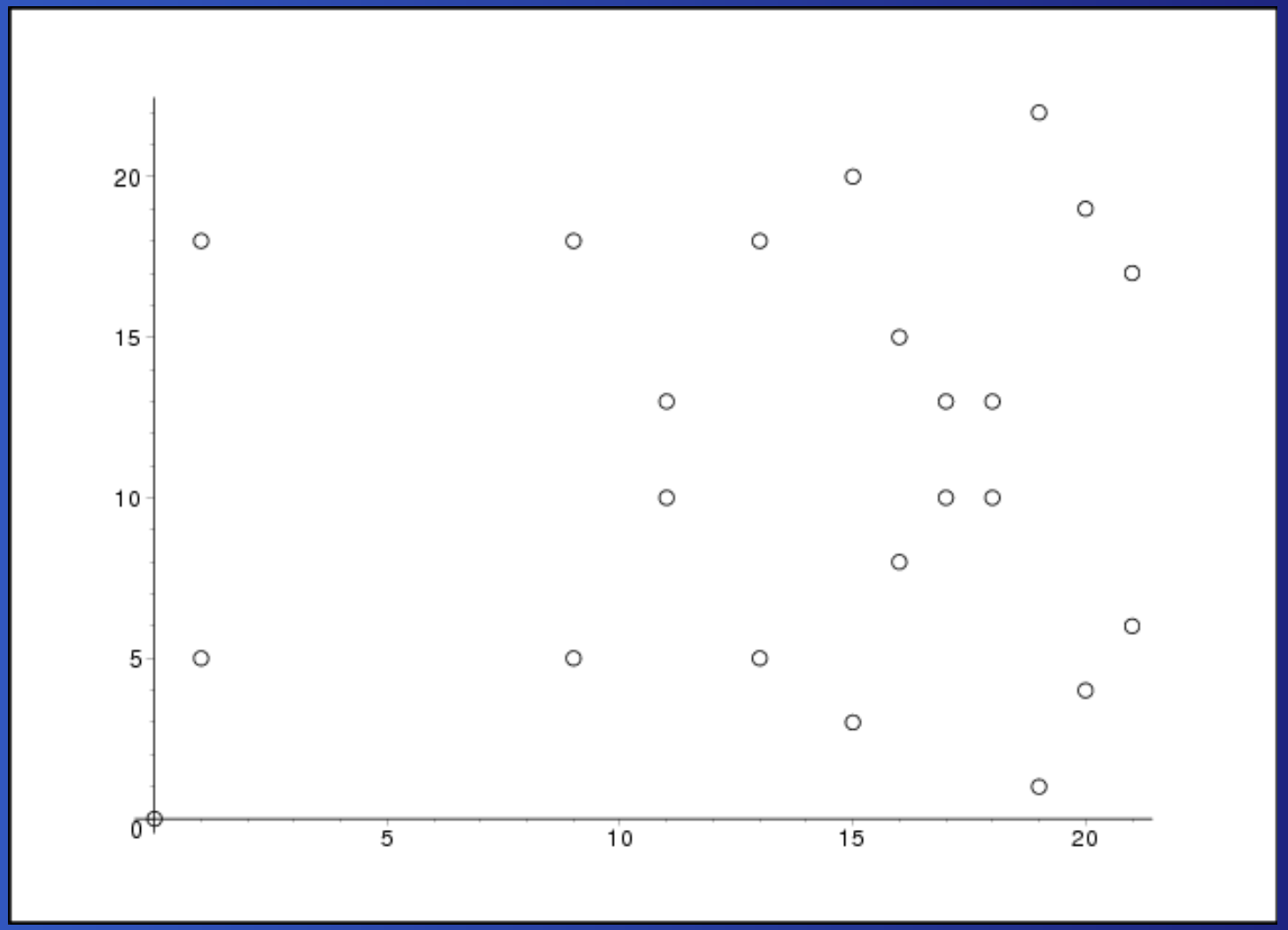
junto com um elemento neutro chamado ponto no infinito $\mathcal{O}$ é uma Curva Elíptica

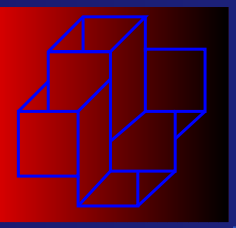
$P + Q = -R$





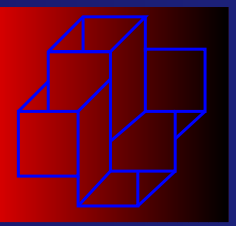
$$y = x^3 + x$$





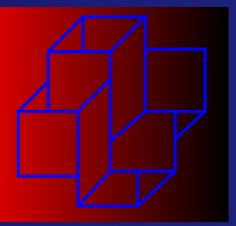
ElGamal – ECC

1. B escolhe um primo p grande, c e d
2. Se $4c^3 + 27d^2 \equiv 0 \mod p$ então volta ao passo anterior
3. B escolhe $a \in E$ com ordem grande e n
4. B calcula $b = na$ e envia p, c, d, a e b
5. A aplica $\alpha : m \longrightarrow w \in E$ escolhe k, calcula $y = ka$ e $z = w + kb \in E$, envia y e z
6. Somente B pode ler calculando $z - ny = w + kb - nka = w + kb - kb = w$



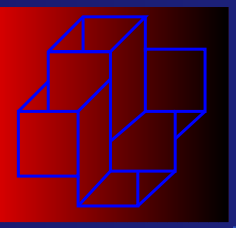
Menezes-Vanstone

1. B escolhe um primo p grande, c e d
2. Verifica se $4c^3 + 27d^2 \equiv 0 \mod p$
3. B escolhe $a \in E$ com ordem grande e $n \in \mathbb{N}^*$, calcula $b = na$ e envia p, c, d, e $a, b \in E$
4. A aplica $\alpha : m \rightarrow w \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$
5. A escolhe $k \in \mathbb{N}^*$, 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
6. Somente B calcula $ny = nka = kna = kb$ e $\left(c_1^{-1} z_1 \mod p, c_2^{-1} z_2 \mod p\right) =$ $\left(c_1^{-1} c_1 w_1 \mod p, c_2^{-1} c_2 w_2 \mod p\right) = w$



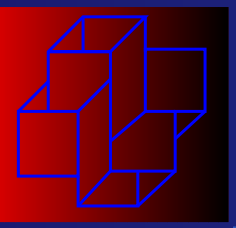
Exemplo Menezes-Vanstone

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



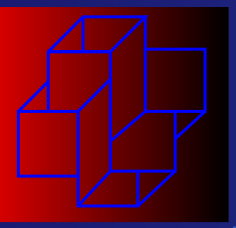
Comparação de Mensagens

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



Conclusão

Neste trabalho apresentamos uma forma atrativa e interdisciplinar de aprender Matemática. A criptografia é um assunto interessante que proporciona motivação para o estudo de Matemática Pura. Recomendamos o uso de algoritmos criptográficos no conteúdo das disciplinas.



Último Slide

- Obrigado.
- Quaisquer sugestões serão bem-vindas.

www.lncc.br/borges

Fábio Borges de Oliveira