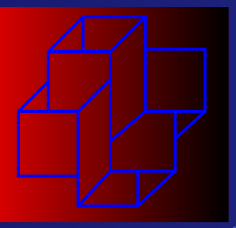
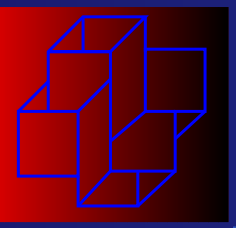


Motivando o Estudo da Matemática através da Criptografia

I Encontro Acadêmico de Modelagem Computacional do LNCC - Mar/08

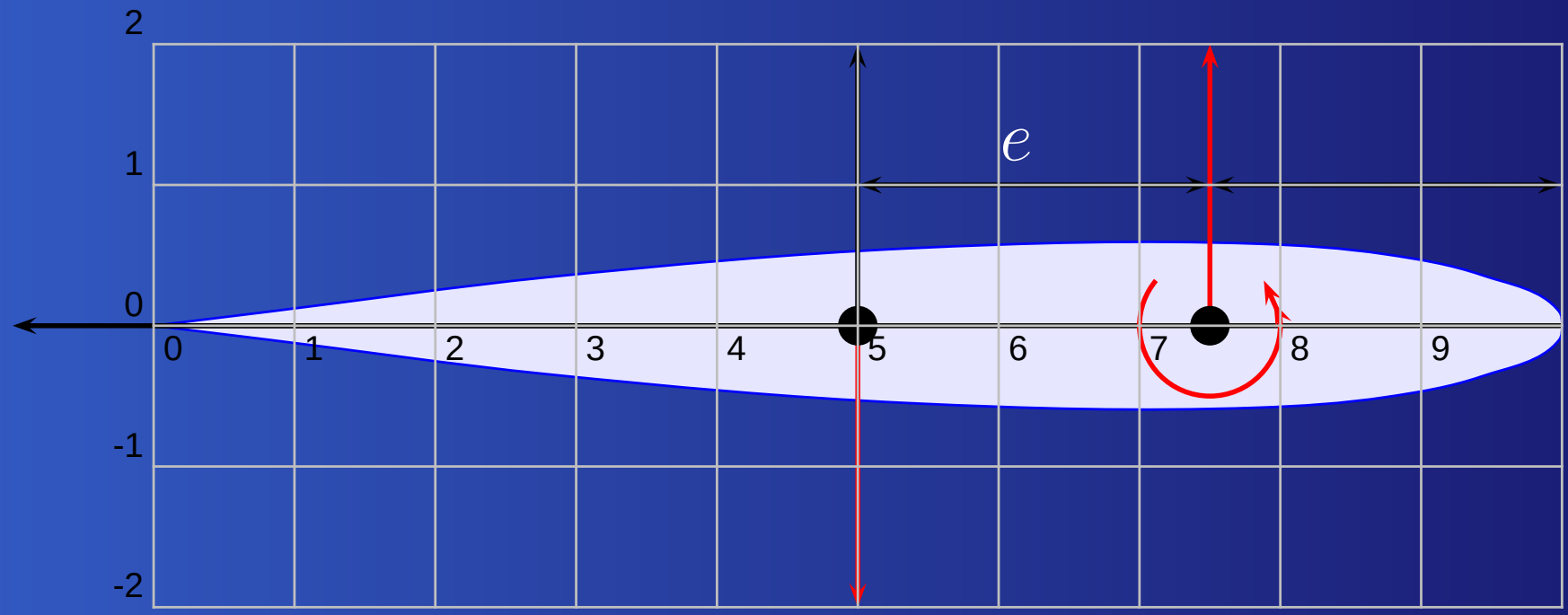
Fábio Borges - LNCC

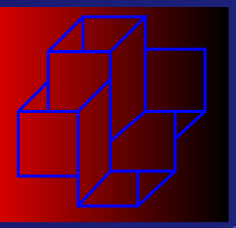


Problema

- Motivação
  - Atenção
    - Abstração
    - Generalização
    - Sutileza
  - Belas aplicações requerem muito conteúdo
  - Aplicações envolvem pouco sentimento

Aerofólio em $\mathbb{C}$

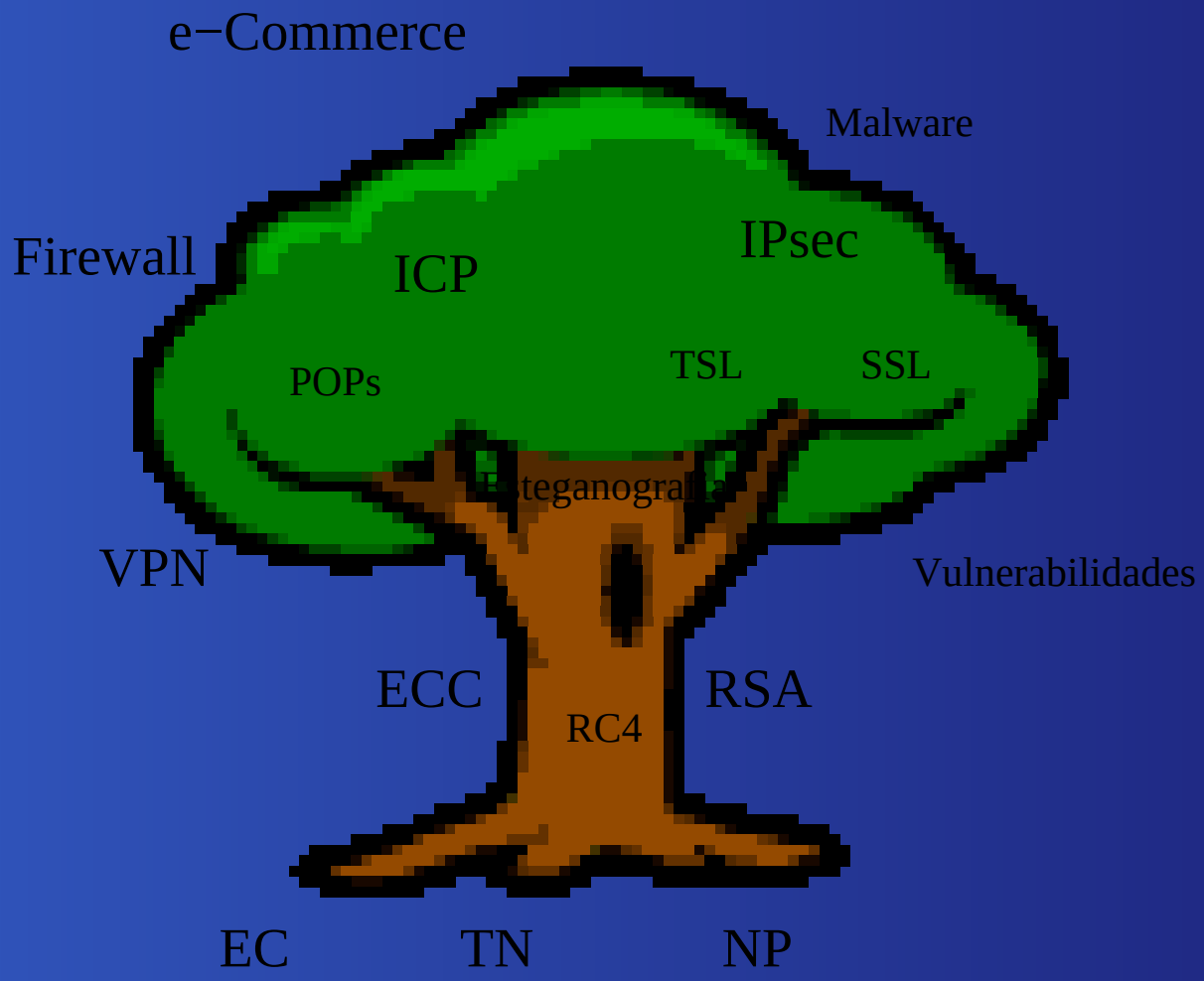


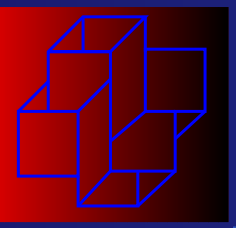


Objetivo da Criptografia

O objetivo básico da Criptografia é transmitir uma mensagem a um destinatário sem que outra pessoa possa compreender seu conteúdo.

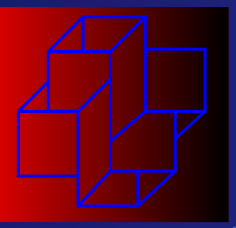
Árvore da Segurança





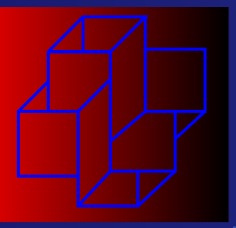
Chamada do SBSeg 2008

"é notável o interesse renovado por áreas que até há algumas décadas eram consideradas aparentemente etéreas como a Teoria dos Números, base na qual reside grande parte da criptografia moderna, ferramenta indispensável no repertório das soluções de segurança."



Início

- Métodos por substituição
  - Celular
  - Diário
- $M + K \mod 27$
- $M \times K \mod 27$

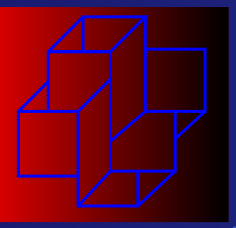


Pós-doutorando

A Hipótese de Riemann afirma que as raízes interessantes de

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

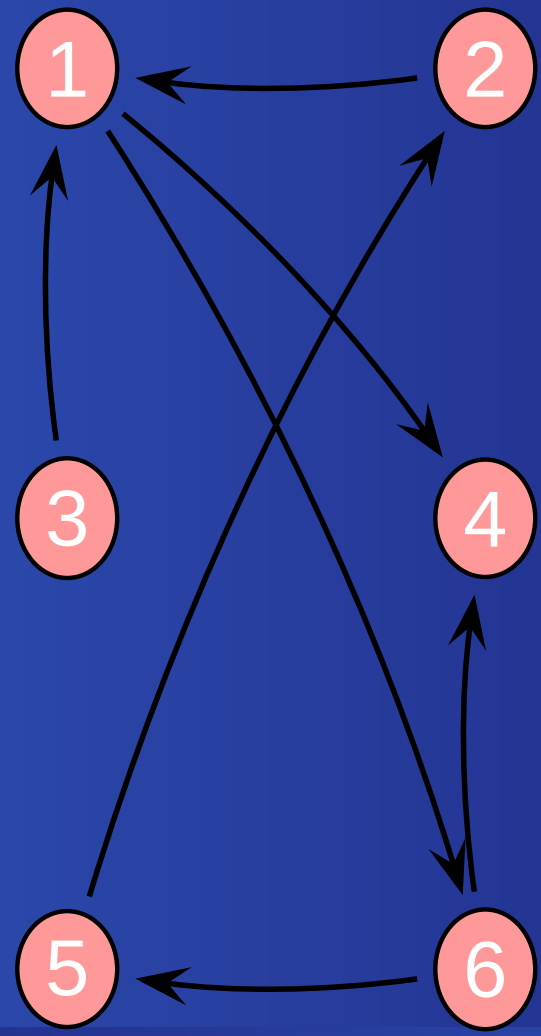
estão em $\mathcal{R}(s) = 1/2$

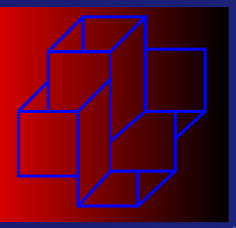


Fatoração

- $xy = 15$
- $xy = 1313$
- RSA amplamente usado na Internet
- Fácil de entender, difícil de solucionar

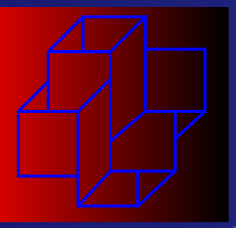
Círculo Hamiltoniano





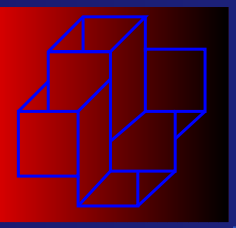
Círculo Hamiltoniano

- Complexidade computacional
- P $\times$ NP
- NP-completo
- Fácil de entender, difícil de solucionar



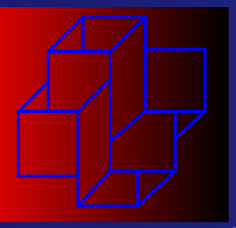
Estatística: Ataques por Domínio

.com	40.9%
.net	6.9%
.de	6.7%
.br	5.1%
.org	4.8%
.it	3.5%
.uk	3.1%



Conclusão

O ensino da Criptografia tem demonstrado ser um facilitador da compreensão da Matemática em virtude das aplicações em segurança da informação.



Último Slide

- Obrigado.
- Quaisquer sugestões serão bem-vindas.