Curso: Introdução à Criptografia para leigos

A partir de 4 de Outubro 2017

Cada quarta-feira às 10 h na Sala da Pós no IM Velho (primeiro andar)

Enno Nagel

Resumo

A criptografia estuda a transformação de textos inteligíveis em textos ininteligíveis, tal que só uma informação adicional secreta, a *chave*, permite desfazê-la.

Historicamente, a chave para cifrar e descifrar é a mesma: a *cifragem simétrica*. Nos anos 70, surgiu a *cifragem assimétrica*, na qual as chaves para cifrar (*a chave pública*) e descifrar (*a chave secreta*) são diferentes. Matematicamente, ela baseia-se em uma *função alçapão*, uma função invertível que é facilmente computável, mas cujo inverso é computacionalmente inviável.

Hoje em dia os algoritmos de cifragem assimétrica têm altíssimo valor comercial: Toda hora, seguram e certificam milhões de transações financeiras na internet; quanto mais seguros os algoritmos, tanto mais as transações.

Cronograma

Contentamo-nos com os conhecimentos algébricos do ensino médio. Orientamo-nos ao livro “An Introduction to Mathematical Crytography” por Hoffstein, Pipher e Silverman ([1]).

Após uma revista da criptografia simétrica, que é historicamente fascinante, mas sobretudo artesanal e com pouco fundamento matemático, introduzimos as ferramentas básicas para abordar a criptográfica assimétrica, que é matematicamente mais rica. Trataremos:

1. Criptografia simétrica
    a. Substituição
    b. Transposição
2. Criptografia assimétrica:
    a. usos da chave pública e privada
    b. o problema da confiança na chave pública
3. Introdução matemática
    a. Divisor Comum
    b. Aritmética Modular
    c. Corpos Finitos
4. Aplicação à Criptografia Assimétrica:
    a. o Logaritmo Discreto e Chaves Públicas segundo Diffie-Hellman
    b. Fatoração Inteira e o Algoritmo RSA

---

1 An introduction to mathematical cryptography; Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman; 2008; Springer