Curso Criptografia

UFAL, Agosto – Dezembro 2017

Enno Nagel

2 de agosto de 2017

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 codificar e descodificar é a mesma: a *codificação simétrica*. Nos anos 70, surgiu a *codificação assimétrica*, na qual as chaves para codificar (*a chave pública*) e descodificar (*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 codificação 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, historicamente mais importante que matematicamente, introduzimos as ferramentas básicas para abordar a criptográfica assimétrica, que é matematicamente mais rica. Trataremos:

1. Criptografia simétrica
2. Introdução matemática
    a. Divisor Comum
    b. Aritmética Modular
    c. Corpos Finitos
3. 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