Marcelo Medeiros de Lima

Matrícula: 2018047030
Curso: Sistemas de Informação 2018/1

Criptografia e Est3g4n0gr4f14 Checkpoint 1

3 de junho de 2018

Visão geral

O primeiro checkpoint do trabalho visa a reprodução do algoritmo de cifragem RSA, um dos mais usados no mundo. O RSA é um sistema de criptografia de chave pública amplamente utilizado em bancos, transações com cartão de crédito, compras online, mensagens de e-mail e muito mais. O método é surpreendentemente simples e extremamente seguro.

O que será apresentado neste checkpoint do trabalho é a codificação e decodificação da mensagem e para tal foi seguido um passo a passo de cálculos a serem aplicados nas fórmulas:

Codificação

c = s^e mod n

Decodificação

s = c^d mod n

Onde:

• s = Mensagem a ser encriptada
• c = Mensagem encriptada
• e = Expoente de cifragem
• d = Expoente de decifragem

• n = Módulo formado pelos dois primos p e q
• φ(n) Função totiente de Euler

A receita para se encontrar cada um desses valores é:

1. Escolhe-se dois números primos p e q.
2. Calculamos n = p.q.
3. Daí calculamos φ(n) = (p – 1)(q - 1), onde φ é a função totiente de Euler.
4. Escolhe-se um e tal que 1 < e < φ(n) e m.d.c.(φ(n), e) = 1.
5. Daí calculamos d de tal forma que d.e ≡ 1 (mod φ(n)).

Observações

- A chave pública é o par de números ***n*** e ***e***
- A chave privada o par de números ***n*** e ***d***

Objetivos

1. **Cifrar a entrada de acordo com a chave pública**
2. **Decifrar a mensagem de acordo com a chave privada**

Instruções

O código deve ser executado em uma máquina com sistema operacional Linux e utilizando-se do makefile presente no zip do projeto. Para executar basta digitar "make". Após a compilação, o makefile criará um arquivo de execução chamado "rsa". Para executá-lo basta digitar no terminal "./rsa". Toda as outras instruções são dadas durante a execução do código.

Observações finais

Todas as funções e detalhes relevantes do código estão comentados. Os comentários de topo de função explicam de forma generalizada o que acontece e quais teoremas matemáticos foram aplicados e os comentários internos explicam partes específicas das funções.