Trabalho 2

Thiago Tokarski
190096063

Julho 2023

1 Introdução

Este é um relatório sobre o trabalho 2 de segurança computacional. Dos pontos propostos pelo professor, apenas 2 foram implementados com sucesso, são eles: Cifração e decifração AES, chave 128 bits e Geração de chaves e cifra RSA.

2 Implementação

A linguagem *rust* foi escolhida para a implementação. O código foi dividido em módulos, uma para ao AES e um para o RSA-OAEP.

2.1 Aritmética

Acredito que essa seja a única parte do trabalho que valha a pena comentar. Ela só foi possível devido a grande ajuda do seguinte artigo: https://glitchcomet.com/articles/1024-bit-primes/.

Um detalhe importante é que visando facilitar o código da aritmética de números grandes, é utilizada a forma little-endian de armazenar os bytes.

2.2 Execução

Para executar os programs são utilizados os seguintes comandos:

- *cargo run – generate_aes_key*
- *cargo run – aes_encode*
- *cargo run – aes_decode*
- *cargo run – generate_rsa_key*

- *cargo run – rsa_oaep_encode*

- *cargo run – rsa_oaep_decode*

Os resultados de cada comando podem ser verificados na pasta results.

3 Conclusão

A parte mais desafiadora deste trabalho foi definitivamente a aritmética de números grandes.