Segurança Computacional
Advanced Encryption Standard

Pedro Henrique de Brito Agnes, 18/0026305
Pedro Pessoa Ramos, 18/0026488

Dep. Ciência da Computação - Universidade de Brasília (UnB)

1 Geração e Verificação de Assinatura Digital

1.1 Implementação

Foi desenvolvido um algoritmo em python na versão 3.8 ou acima que recebe um arquivo e gera a assinatura digital para ele ou verifica a assinatura. Para executar passando o documento `message.txt`, pode-se usar o comando abaixo:

```
1 python src/rsa.py sample/message.txt
```

Pode ser passado o argumento `-h` para o programa para a listagem de opções disponíveis conforme mostrado abaixo:

- ...

1.2 RSA

1.2.1 Geração de Chaves

Para a geração de chaves, inicialmente foram gerados 2 números primos aleatórios `p` e `q` de 1024 bits cada. Para obter estes números, foi inicialmente gerado um número qualquer do tamanho especificado, em seguida, sua primalidade foi testada para cada um dos primos até 1000, que foram computados uma vez pelo crivo de Erastótenes e dispostos em um array. Em seguida, é realizado o teste de primalidade probabilístico de Miller Rabin, executado 20 vezes.