Algoritmos e Estruturas de Dados III

# Trabalho de criptografia RSA e AES


Fernando Ribeiro Ollé

Centro de Desenvolvimento Tecnológico – UFPEL

Pelotas – RS, 2021

## 1. Resumo

Este trabalho tem como objetivo documentar o processo de descriptografia de uma conteúdo cifrado com o algoritmo AES de 25 Bits que por sua vez tem sua chave cifrada com a criptografia RSA.

Será apresentado o método que foi utilizado para obter o conteúdo da mensagem que foi protegida com o algoritmo AES e logo em seguida demonstrado os resultado obtidos neste processo.

## 2. Passo a passo da desencriptação

A criptografia RSA se dá seguinte forma :

- Definição de dois números primos grandes, *P* e *Q*
- Cálculo de *n, n = p*q*
- Cálculo da função *totiente, n: phi(n) = (p -1) *(q -1)*
- Definição de um inteiro, *e* tal que *1 < e < phi(n)*
- Cálculo de *d, de === 1 (mod phi(n)),*

Então, a partir da chave pública disponibilizada para a realização da tarefa é possível obter o valor do módulo *(n)* e do expoente público *(e)* utilizando a chave pública *(pub.key)* e conjunto com o comando do programa openssl:

- *openssl rsa -pubin -in pub.key -text -noout*

Em posse destas informações podemos executar um algoritmo modular inverso (posteriormente demonstrado em Python) para obtermos nosso '*d'.*

```python
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    g, y, x = egcd(b%a,a)
    return (g, x - (b//a) * y, y)
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
       raise Exception('No modular inverse')
    return x%m
d = modinv(e, phi)
```

Agora temos todas as informações necessárias para podermos utilizar a biblioteca *Crypto.PublicKey.* Precisaremos importar o módulo *RSA*, que por sua vez possui o método chamado '*construct'* passando nossos valores (*n, e, d, p, q*) que então nos retornará a chave pública para a mensagem AES.

Então utilizaremos mais um comando do software openssl, primeiramente para obtermos a senha para a arquivo AES :

- *openssl rsautl -decrypt -in key.cipher -out key.txt -inkey pk.key*

Onde '*key.cipher'* é a senha cifrada, '*key.txt'* é o nome do arquivo onde obteremos a senha e '*pk.key*' é o arquivo que possui a chave pública para a mensagem.

Por fim, o comando :

- *openssl aes-256-cbc -md md5 -a -d -in ciphertext.enc -out message.txt*

Nos revela a mensagem assim que conseguirmos entrar corretamente a senha previamente obtida!

## 3. Conclusão

O trabalho de criptografia da cadeira de Algoritmos e Estruturas de Dados III foi deveras muito interessante, apresentando-se como um desafio empolgante e muito satisfatório de ser encarado. Porém deve ser ressaltado que o software *openssl,* simples pelo fato de não exibir a senha que está sendo inserida, pode tornar a experiência em um grande pesadelo.

Porém, mesmo com todas as dificuldades enfrentadas ao longo do desenvolvimento do projeto, podemos afirmar que este trabalho foi concluido com êxito!

( Abaixo (Capítulo 4) encontra-se as informações coletadas durante o processo )

## 4. Resultados Obtidos

### 4.1. Chave privada para a chave criptografada em RSA:

-----BEGIN RSA PRIVATE KEY-----
MIHBAgEAAiYOWxON4VVOCjgECz38THnFRTqJY2gENjwnu266/sg0
yYw6BiggVQIDAQABAiYKAICuQInrtojyoFaOm0XYIPS4gdMeNj3C5u
Wo2lfKGNERZ8+4AQITO8QkAkcydrUiO+qEJlMfWe2aVQITPX2sM0jD
hgm4ndB+ijBfokJuAQITL1bOxtcqC4ixkw/QmKKiZJKk+QITFVxIq3AFa
9SIq1m3+20ea5FEAQITN/40BShNq1ObmZYjs4c09WgfqQ==
-----END RSA PRIVATE KEY-----

### 4.2. Senha para a mensagem:

6AYwFJffIFVVpYkCUFf4Jw==

### 4.3. A mensagem:

We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace.

Signed, ZIMMERMANN.