Algoritmos e Estruturas de Dados III

Trabalho de criptografia RSA e AES

Integrantes

Alejandro da Silva Pereira
Centro de Desenvolvimento Tecnológico – UFPEL
Universidade Federal de Pelotas - http://www.ufpel.edu.br/

Amaral Ferrador – RS, 2021

1. Resumo

Nesse trabalho irei detalhar todos os procedimentos adotados para obter uma mensagem cifrada, criptografada com AES 256 bits, cuja chave foi criptografada utilizando uma chave pública RSA nas quais temos acesso, e que se sabe que provavelmente foi utilizado o programa **openssl** para realizar ambas as encriptações, e por fim mostrar a senha obtida e a mensagem original.

2. Procedimentos adotados

1º passo: Fazer o download e a instalação do programa openssl.

2º passo: Obter o valor do módulo (n) e do expoente público (e) a partir da chave pública que foi dada, executando o comando: **openssl rsa -pubin -in pub.key -text -noout,** o openssl vai fornecer o módulo (n) em hexadecimal, então usei o site https://www.binaryhexconverter.com/hex-to-decimal-converter para fazer a conversão para decimal, como resultado obtive
n = 18277008811800209610875687687880247478375528987118320666330121706177313962836655487388304 21 e **e = 65537**.

3º passo: Colocar o módulo (n) no site https://www.alpertron.com.ar/ECM.HTM , para fatorar ele e assim consegui descobrir p e q, esse procedimento pode demorar um pouco, como resultado obtive **p = 133283022794927352146536731923427727943962478 9** e **q = 137129308958738729218048129378403679307683788 9**.

4º passo: Com o valor de p e q calculei fi(n) pela fórmula fi (n) = (p – 1) * (q – 1), como resultado obtive **fi (n) = 127339746914812910423454655464287346096114412903562856390265802997838075845216005852861030 5**.

5º passo: Calcular o expoente privado (d), pela fórmula d = e^–1 mod fi(n), para calcular de uma forma mais simplificada usei esse site, ele possui a função modinv, que é bastante útil para esse cálculo, como resultado obtive **d = 121846725412001397405837917919201649855836859733847249939756757131458852176900984148245163**.

6º passo: Calcular o coeficiente (c), pela fórmula c = q^-1 mod p, para calcular de uma forma mais simplificada também usei o site, como resultado obtive **c = 124868520808433843692941526730146403196338986 5**.

7º passo: Calcular os demais expoentes e1 e e2, que são calculados pelas seguintes formulas: e1 = d mod (p - 1) e e2 = d mod (q - 1), ambos cálculos usei um programa em phyton para calcular esses números grandes, como resultado obtive **e1 = 105569704339299614720336935687399932491736313** e **e2 = 476354707684917818847076264313096138535289857**.

8º passo: Criar uma estrutura ASN.1 da chave privada usando todos os números que foram calculados, da seguinte forma:
asn1=SEQUENCE:rsa_key

[rsa_key]
version=INTEGER:0
modulus=INTEGER:18277008811800209610875687687880247478375528987118320666330121706177313962836655487388304 21
pubExp=INTEGER:65537
privExp=INTEGER:12733974691481291042345465546428734609611441290356285639026580299783807584521600585286103 05
p=INTEGER:133283022794927352146536731923427727943962478 9
q=INTEGER:137129308958738729218048129378403679307683788 9
e1=INTEGER:105569704339299614720336935687399932491736313
e2=INTEGER:476354707684917818847076264313096138535289857
coeff=INTEGER:124868520808433843692941526730146403196338986 5

9º passo: Usar a estrutura asn.1 para gerar a chave privada com o seguinte comando **openssl asn1parse -genconf asn.1 -out private.der**, após isso converter a chave privada gerada para .pem com o seguinte comando **openssl rsa -in private.der -inform der -out private.pem -outform pem**.

10º passo: Verificar se a chave privada criada corresponde a chave publica que foi dada no trabalho com o seguinte comando **openssl rsa -in private.pem -pubout**, verifica-se assim que a chave privada está correta.

11º passo: Descriptografar a chave key.cipher usando a chave privada que geramos com o seguinte comando **openssl rsautl -decrypt -inkey private.pem -in key.cipher -out senha.txt**, como resultado obtemos dentro do arquivo texto gerado a senha para descriptografar a mensagem cifrada.

12º passo: Por fim descriptografei a mensagem cifrada ciphertext.enc com o seguinte comando **openssl aes-256-cbc -md md5 -a -d -in ciphertext.enc -out mensagem.txt,** após isso colamos a senha obtida no arquivo senha.txt, então a mensagem original vai ser gerada no arquivo mensagem.txt**.**

3. Resultados

Chave privada para a chave criptografada em RSA:

-----BEGIN RSA PRIVATE KEY-----
MIHBAgEAAiYOWxON4VVOCjgECz38THnFRTqJY2gENjwnu266/sg0yYw6BiggVQID
AQABAiYKAICuQInrtojyoFaOm0XYIPS4gdMeNj3C5uWo2IfKGNERZ8+4AQITO8Qk
AkcydrUiO+qEJlMfWe2aVQITPX2sM0jDhgm4ndB+ijBfokJuAQITL1bOxtcqC4ix
kw/QmKKiZJKk+QITFVxIq3AFa9SIq1m3+20ea5FEAQITN/40BShNq1ObmZYjs4c0
9WgfqQ==
-----END RSA PRIVATE KEY-----

Senha para a mensagem cifrada em AES:

6AYwFJffIFVVpYkCUFf4Jw==

Mensagem original:

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.