UNIVERSIDADE FEDERAL DE PELOTAS
CURSO DE CIÊNCIA DA COMPUTAÇÃO
ALGORITMOS E ESTRUTURA DE DADOS III

Relatório sobre criptografia RSA e AES

1→ Encontrando chave privada e decriptando RSA

Optei por não utilizar o openssl nesta primeira etapa pois eu já possuía um código em Python que encontra o valor de N e E pela chave publica RSA (O algoritmo em python está na pasta junto com este relatório).

Tendo o valor de N e E em mãos, o próximo passo era encontrar o valor de P e Q, para isso eu deveria fatorar o numero N, onde eu utilizei o programa MSIEVE. Passando o valor de N como entrada para o programa, eu obtive o valor P e Q respectivos:
p: 887015894239637
q:
5568933029697020901913868071965413516265796238726 33

O programa demorou por volta de 30 minutos para encontrar os valores da fatoração.

Após isto, eu utilizei o mesmo algoritmo em python para encontrar a chave privada, utilizando a tripla P,Q,E onde o valor de E é **65537** e o N:
18277008811800209610875687687880247478375528987118320666330121706177313962836655487388304 21.

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

-----END RSA PRIVATE KEY-----

Após isto, salvei em um arquivo .txt com o nome private.txt e utilizei um comando openssl para transformar o arquivo .txt em um arquivo .pem, esse arquivo .pem funciona para abrir o arquivo RSA utilizando o openssl. O comando foi:
openssl rsa -in private.txt -outform pem -out pvt-key.pem

Tendo a senha em mãos, pude abrir o RSA com a linha de comando a seguir, mas antes eu alterei o nome do arquivo "key.cipher" para "key.enc":
openssl rsautl -decrypt -inkey pvt-key.pem -in key.enc -out out.txt

Então eu obtive a chave AES:
6AYwFJffIFVVpYkCUFf4Jw==

2→ Decriptando AES

Eu tive bastante dificuldade para utilizar o Openssl no ubunto para decriptar o AES, eu estava utilizando uma versão mais recente do Openssl, a qual ao tentar decriptar o arquivo me retornava os dados em um formato incorreto, não podendo assim ler o texto.
Buscando na internet, vi que a solução era ir para uma versão anterior, logo, tentei fazer o downgrade mas não consegui, então resolvi ir para o windows onde finalmente consegui instalar a versão correta para o Openssl e decriptar o arquivo.
Utilizei o comando em Openssl para decriptar o AES:

Esse é o comando: aes-256-cbc -salt -a -d -in ciphertext.enc -out texto.txt

e digitei a chave, onde obtive o texto seguinte:

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.