ALGORITMOS E ESTRUTURAS DE DADOS III

RSA e AES

Nome: Ronei Ângelo Zanol Júnior

- ## Introdução

O Trabalho consiste em quebrar a chave pública RSA (**pub.key**) por fatoração de inteiros, gerar a chave privada RSA e obter a chave AES para decriptar a mensagem final. Primeiro fatoramos a variável **n** que está na chave pública, gerando 2 outras variáveis usadas na construção da chave privada, **p** e **q**. A chave privada é então usada para decriptar a mensagem encriptada com RSA, contida em **key.cipher**. A mensagem decriptada é a chave AES para decriptar outra mensagem, contida em **ciphertext.enc**. Com isso, é então usada essa chave para decriptar e obter a mensagem final.

- **Métodos usados**
  - **Decriptação do RSA**
    1. Para obter a variável **n** contida na chave pública, foi usado o programa:

       aesdec.exe getpublickeys

       Com a saída do programa, obtemos:

       n = 18277008811800209610875687687880247478375528987118320666330121706177313962836655487388304021

    2. Fatoramos esse número com outro programa chamado **Yafu**:

       yafu-x64.exe factor(18277008811800209610875687687880247478375528987118320666330121706177313962836655487388304021)

       O tempo para fatorar levou 1677.1774 segundos. E resultou nos fatores:

       p = 137129308958738729218048129378403679307683788 9
       q = 133283022794927352146536731923427727943962478 9

    3. Com isso usamos novamente o programa **aesdec** para obter a chave privada RSA e decriptar o arquivo **key.cipher**:

       aesdec.exe

       A saída gerada é a **chave AES** para decriptar a mensagem final:

       6AYwFJffIFVVpYkCUFf4Jw==

- **Decriptação do AES**

    1. Com a chave AES, usamos o programa **openssl** para decriptar a mensagem final:

```
opensslMD aes-256-cbc -d -a -k 6AYwFJffIFVVpYkCUFf4Jw== -in ciphertext.enc -out decrypted_text.txt
```

    2. Obtemos então a mensagem final no arquivo **decrypted_text.txt**:

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.

- **Programas utilizados**

    - Yafu: https://sourceforge.net/projects/yafu/
    - openssl: http://www.npcglib.org/~stathis/blog/precompiled-openssl