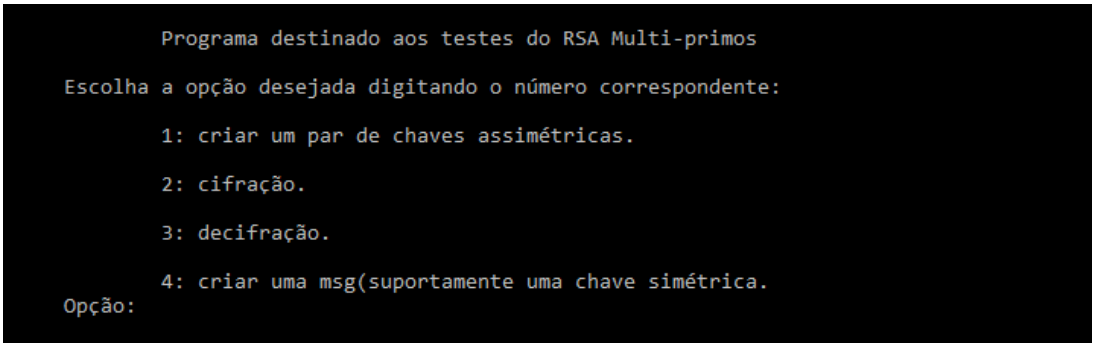
Instruções sobre o uso do programa "Sistema Assimétrico Multi-primos"

(Requisito: Windows 10)

O programa possibilita a execução das seguintes quatro funcionalidades, [Tela-1]:

- Criação de pares de chaves assimétricas;
- Cifração;
- Decifração e
- Geração de uma mensagem, para testes.



Tela-1

1. Criação de chaves.

   Esta funcionalidade é usada para a criação de chaves. As chaves poderão ser qualquer tamanho. Não se detectou um limite. Porém, quanto maior for à chave, maior deve ser a quantidade de primos, para cálculos realizados em tempo razoável. Por exemplo: para uma chave de 32768, se forem escolhidos apenas dois números primos, o tempo do cálculo poderá chegar a algumas horas.

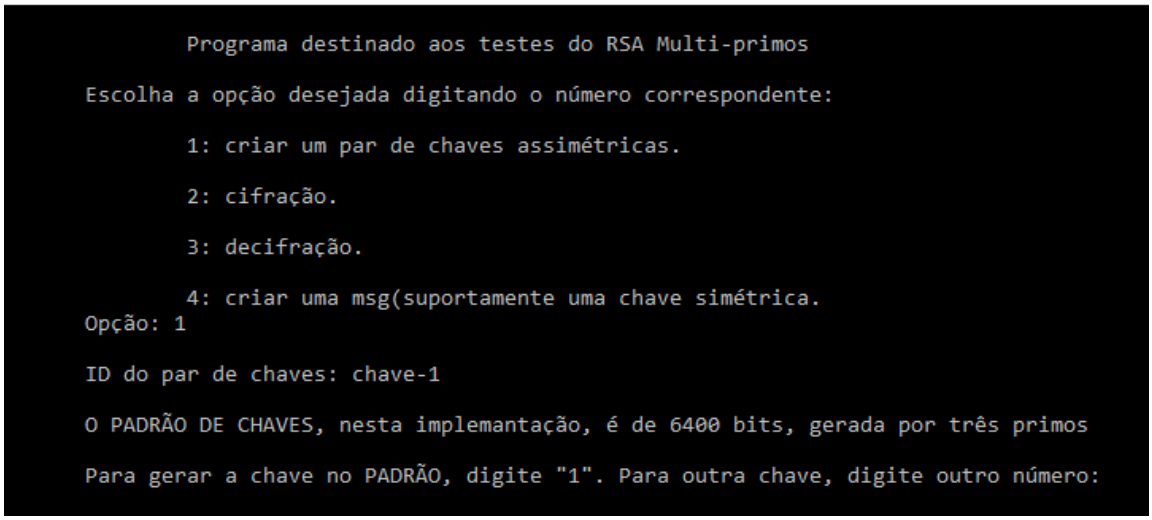
   O programa funciona com qualquer quantidade de números primos. Evidentemente a quantidade (maior ou igual a dois) deve ser adequada ao tamanho de chave, para que esta não se torne vulnerável.

   Na atual implementação, sugere-se como tamanho padrão 6400 bits formado por três primos.

   Ao criar um par de chaves insere-se o ID da chave (Ex: chave-1) e pode-se optar ou não pelo tamanho padrão, [Tela-2]:

   Em função do "ID do para de chaves" são criados dois arquivos e as extensões -Pub, -Priv são acrescentadas:

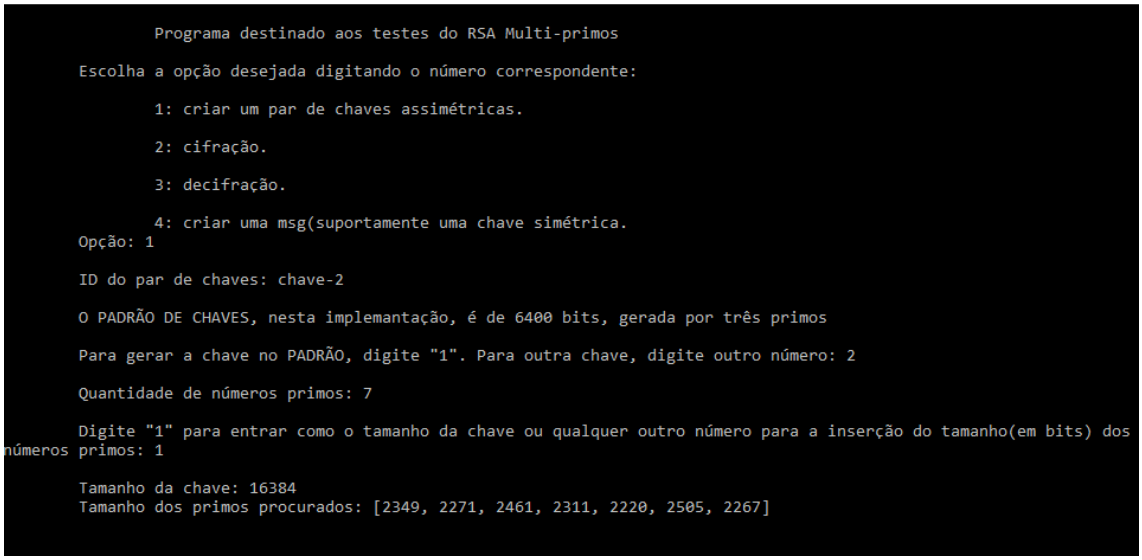
   - chave-1-priv: arquivo contendo a chave privada e
   - chave-1-pub: arquivo contendo a chave pública



Tela-2.

Para criar chaves com tamanhos diferentes do padrão citado, as opções além da quantidade de primos são: escolher o tamanho da chave ou escolher o tamanho dos primos.

Na Tela-3 é mostrado o procedimento para a criação de uma chave formada por sete primos, inserindo-se o tamanho da chave = 16384 [Tela-3]. O tamanho dos primos é determinado em função do tamanho da chave e da quantidade de primos.



Tela-3.

Obs.

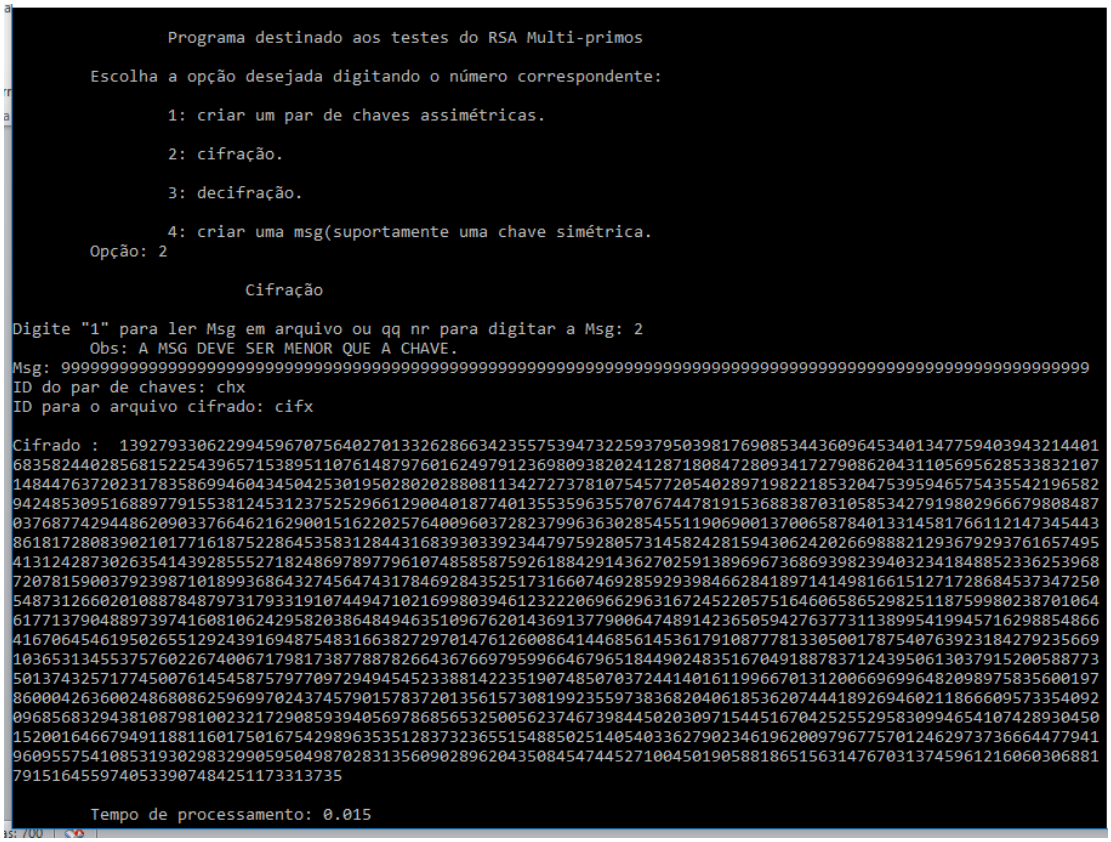
- Esta tela mostra a escolha da opção-1 “criar um par de chaves”.
- Chave-2, para a identificação das chaves.
- Digitado o ‘2’ para chaves diferente do padrão citado.
- Foram escolhidos: quantidade de primos = 7 e tamanho da chave = 16384.
  O programa mostra tamanho dos sete de números primos a serem procurados, em função do tamanho da chave.

O tamanho calculado da chave pode diferir por alguns bits do tamanho digitado, devido à varredura realizada para encontrar os números primos.

- Ao final da execução, as chaves são mostradas na tela as chaves, além serem gravadas nos respectivos arquivos:

2. Cifração.

Com a opção cifração pode-se cifrar mensagem lida de arquivo ou inserida pelo teclado. A limitação desta implementação é a normal para a maioria dos empregos do RSA, isto é, a mensagem ter tamanho inferior ao tamanho da chave. Um exemplo de execução da cifração está mostrado na tela-4.

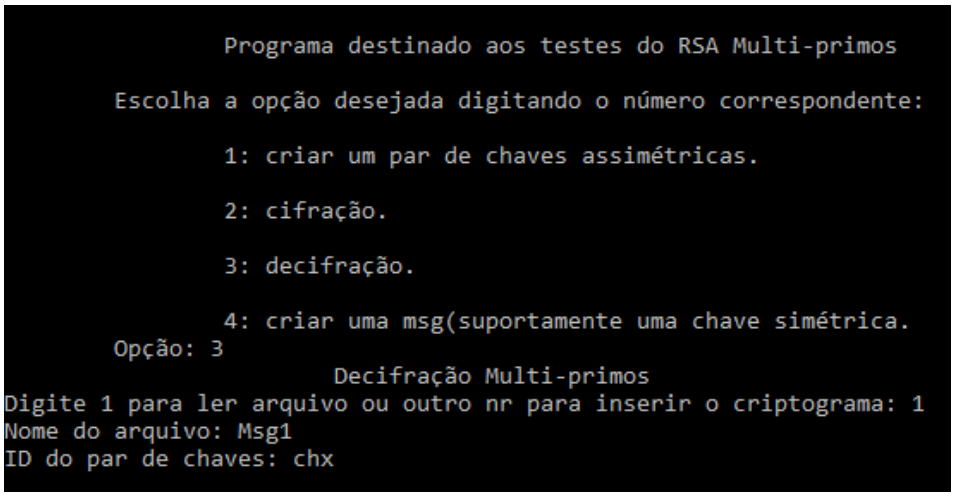


Tela-4

Obs.

- A tela mostra a escolha da opção-2 “cifração.”.
- Na opção Digite "1" *para ler Msg em arquivo ou qq nr para digitar a Msg. S*e for digitado um número “1”, o programa solicitará o nome do arquivo que contém a mensagem. Caso contrário, deverá ser digitada a mensagem (pode ser qualquer número menor que a chave). No exemplo foi digitado ‘2’.
- Msg digitada: 999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
- Entrar com o ID da chave, que é parte da chave que antecede “-pub”.
- O ID do arquivo cifrado é o nome do arquivo em que a msg. cifrada será gravada.
- Ao final da execução, a msg cifrada é mostrada na tela, além ser gravada no respectivo arquivo [cifx].

3. Decifração.
   Com a opção decifração pode-se decifrar mensagem lida de arquivo ou inserida pelo teclado.



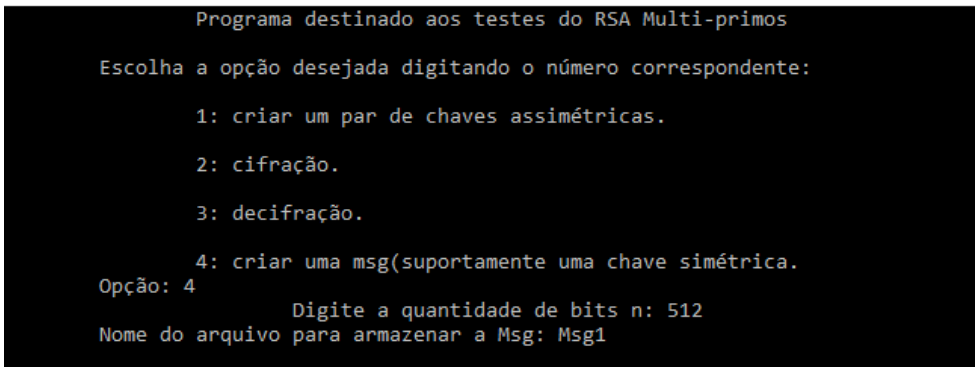
Tela-5.

Obs.

- A tela mostra a escolha da opção-3 “decifração.”.
- Na opção Digite "1" *para ler arquivo ou outro nr inserir o criptograma. S*e for digitado um número “1”, o programa solicitará o nome do arquivo que contém a mensagem cifrada. Caso contrário, deverá ser digitada a mensagem cifrada.
- Entrar com o ID do par de chaves, que é parte da chave que antecede “-priv” e
- Ao final da execução, a mensagem decifrada é mostrada na tela.

4. Criar uma mensagem.

- Esta opção destina-se a criação de uma mensagem, com o tamanho desejado, para facilitar a realização de testes. A mensagem é composta por um número, supostamente uma chave simétrica. Precisa-se inserir a quantidade de bits da mensagem e o nome do arquivo em que a mensagem será gravada.



Tela-6.

Prof. Rael
jbrael@uol.com.br