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

(Requisito: Windows 10)

O programa possibilita a execução das seguintes quatro funcionalidades:

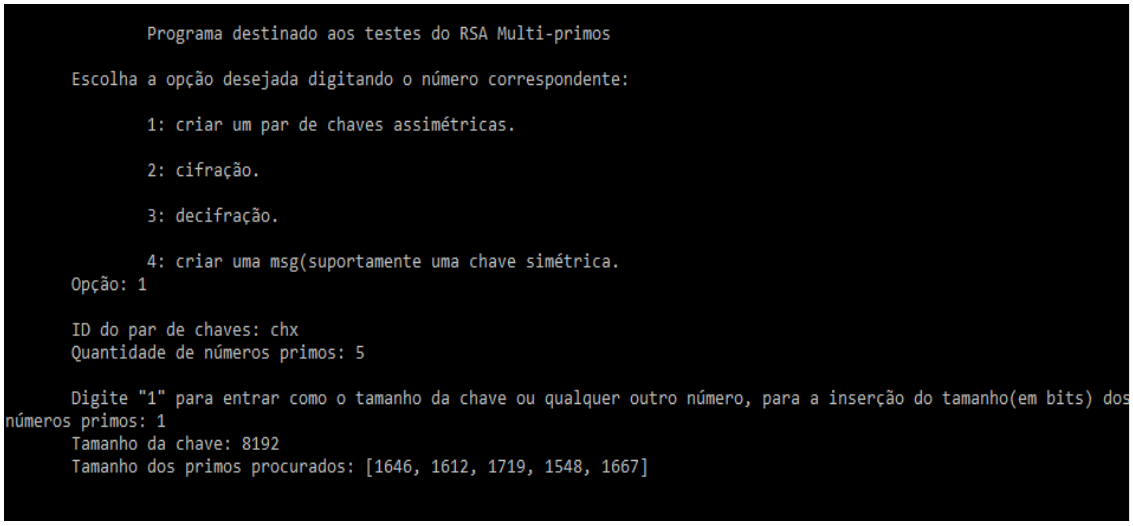
- Criação de pares de chaves assimétricas;
- Cifração;
- Decifração e
- Geração de uma mensagem.

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 o cálculo seja realizado em tempo razoável. Por exemplo: para uma chave de 32768, se forem escolhidos apenas dois números primos, o tempo do cálculo será de algumas horas.

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

   Ao criar um par de chaves insere-se a quantidade de números primos e escolhe-se uma das opções: inserir o tamanho da chave ou escolher o tamanho (em bits) dos primos, conforme mostrado na tela-1.



Tela-1.

Obs.

- Esta tela mostra a escolha da opção-1 "criar um par de chaves".
- São criados dois arquivo em função do "ID do para de chaves". As extensões: -Pub, -Priv são acrescentadas:
  - chx-priv: arquivo contendo a chave privada e
  - chx-pub: arquivo contendo a chave pública
- Foram escolhidos: quantidade de primos = 5 e tamanho da chave = 8192.

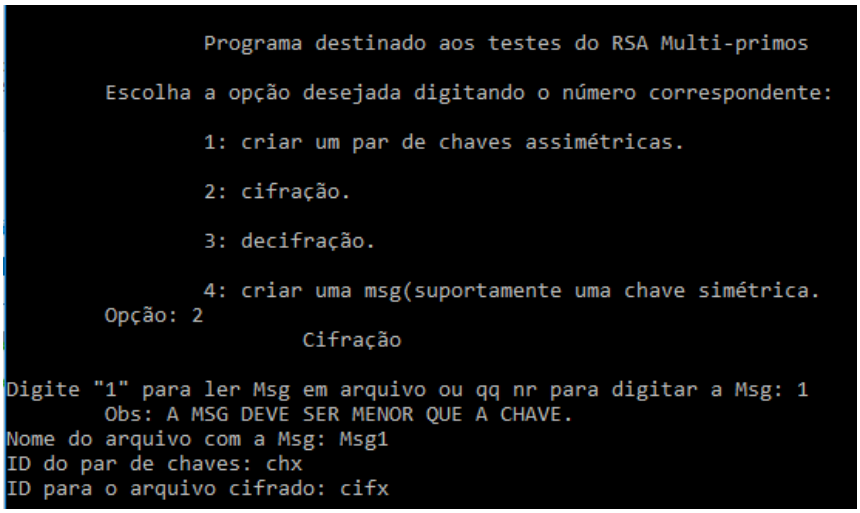
O programa mostra tamanho dos cinco de números primos a serem procurados, em função do tamanho da chave.

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

- Na opção Digite "1" *para entrar como o tamanho da chave ou qualquer outro número, para a inserção do tamanho (em bits) dos números primos,* se for digitado um número diferente de "1", o programa não solicitará o tamanho da chave. Solicitará o tamanho dos números e calculará o tamanho da chave.
- 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. A execução da cifração está mostrada na tela-2.

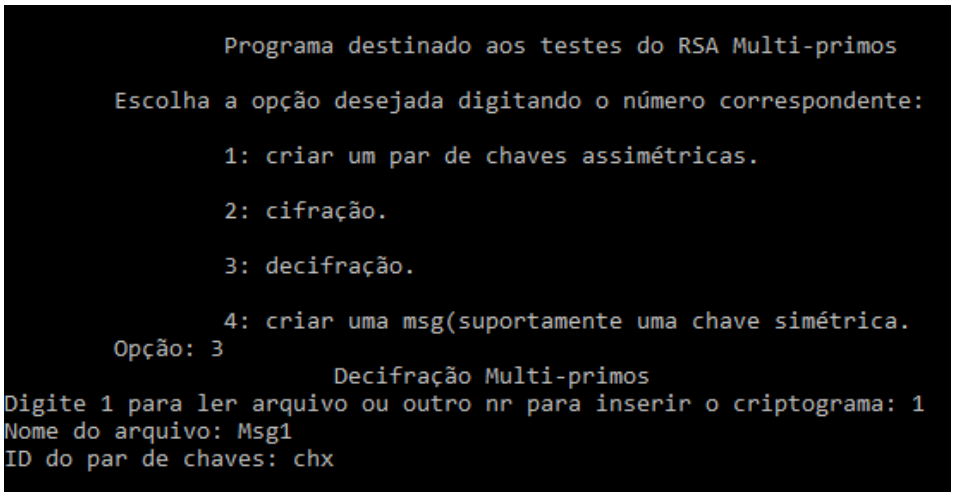


Tela-2.

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).
- 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 e
- Ao final da execução, a msg cifrada é mostrada na tela, além ser gravada no respectivo arquivo.

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



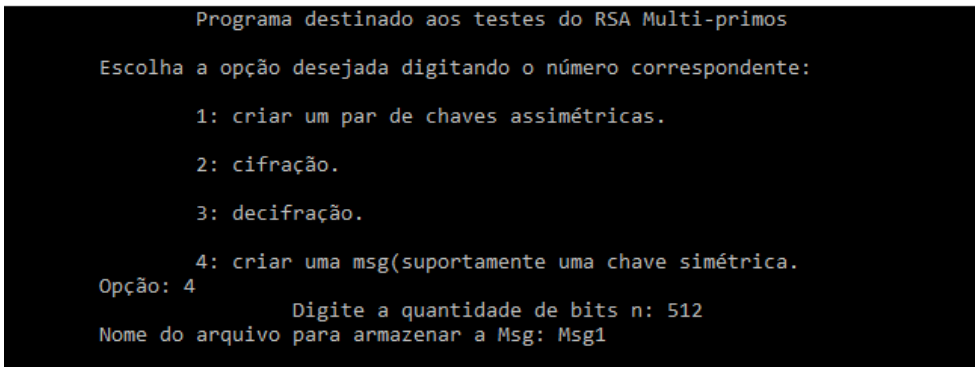
Tela-3.

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-4.

Prof. Rael
jbrael@uol.com.br