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.

```
Programa destinado aos testes do RSA Multi-primos

Escolha a opção desejada digitando o número correspondente:

1: criar um par de chaves assimétricas.

2: cifração.

3: decifração.

4: criar uma msg(suportamente uma chave simétrica.

Opção:
```

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

```
Programa destinado aos testes do RSA Multi-primos

Escolha a opção desejada digitando o número correspondente:

1: criar um par de chaves assimétricas.

2: cifração.

3: decifração.

4: criar uma msg(suportamente uma chave simétrica.

Opção: 1

ID do par de chaves: chave-1

O PADRÃO DE CHAVES, nesta implemantação, é de 6400 bits, gerada por três primos

Para gerar a chave no PADRÃO, digite "1". Para outra chave, digite outro número:
```

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.

```
Programa destinado aos testes do RSA Multi-primos

Escolha a opção desejada digitando o número correspondente:

1: criar um par de chaves assimétricas.

2: cifração.

3: decifração.

4: criar uma msg(suportamente uma chave simétrica.
Opção: 1

ID do par de chaves: chave-2

O PADRÃO DE CHAVES, nesta implemantação, é de 6400 bits, gerada por três primos

Para gerar a chave no PADRÃO, digite "1". Para outra chave, digite outro número: 2

Quantidade de números primos: 7

Digite "1" para entrar como o tamanho da chave ou qualquer outro número para a inserção do tamanho(em bits) dos primos: 1

Tamanho da chave: 16384

Tamanho dos primos procurados: [2349, 2271, 2461, 2311, 2220, 2505, 2267]
```

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.

```
Programa destinado aos testes do RSA Multi-primos
        Escolha a opção desejada digitando o número correspondente:
                  1: criar um par de chaves assimétricas.
                  2: cifração.
                  3: decifração.
                  4: criar uma msg(suportamente uma chave simétrica.
                           Cifração
        "1" para ler Msg em arquivo ou qq nr para digitar a Msg: 2
Obs: A MSG DEVE SER MENOR QUE A CHAVE.
para o arquivo cifrado: cifx
           5835824402856815225439657153895110761487976016249791236980938202412871808472809341727908620431105695628533832107
1484476372023178358699460434504253019502802028808113427273781075457720540289719822185320475395946575435542196582
3618172808390210177161875228645358312844316839303392344797592805731458242815943062420266988821293679293761657499
113124287302635414392855527182486978977961074858587592618842914362702591389696736869398239403234184885233625396
120781590037923987101899368643274564743178469284352517316607469285929398466284189714149816615127172868453734725
.1670645461950265512924391694875483166382729701476126008641446856145361791087778133050017875407639231842792356
.0365313455375760226740067179817387788782664367669795996646796518449024835167049188783712439506130379152005887
.0137432571774500761454587579770972949454523388142235190748507037244140161199667013120066969964820989758356001
600042636002486808625969970243745790157837201356157308199235597383682040618536207444189269460211866609573354092
968568329438108798100232172908593940569786856532500562374673984450203097154451670425255295830994654107428930450
520016466794911881160175016754298963535128373236551548850251405403362790234619620097967757012462973736664477941
609557541085319302983299059504987028313560902896204350845474452710045019058818651563147670313745961216060306881
        Tempo de processamento: 0.015
```

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. Se 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'.
- 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.

```
Programa destinado aos testes do RSA Multi-primos

Escolha a opção desejada digitando o número correspondente:

1: criar um par de chaves assimétricas.

2: cifração.

3: decifração.

4: criar uma msg(suportamente uma chave simétrica.

Opção: 3

Decifração Multi-primos

Digite 1 para ler arquivo ou outro nr para inserir o criptograma: 1

Nome do arquivo: Msg1

ID do par de chaves: chx
```

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. Se 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.

```
Programa destinado aos testes do RSA Multi-primos

Escolha a opção desejada digitando o número correspondente:

1: criar um par de chaves assimétricas.

2: cifração.

3: decifração.

4: criar uma msg(suportamente uma chave simétrica.

Opção: 4

Digite a quantidade de bits n: 512

Nome do arquivo para armazenar a Msg: Msg1
```

Tela-6.