UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Disciplina: Números Inteiros e Criptografia
Professor: Luis Menasché
Aluno: Breno Ferreira Rocha

Trabalho Final

Manual do Usuário

Pré-Requisitos:

- O usuário precisa estar utilizando uma das distribuições do **Linux**. Uma das versões mais utilizadas do Linux e o **Ubuntu**. Abaixo estão links de download e de um tutorial de instalação do sistema operacional.

Download do **Ubuntu**: https://www.ubuntu.com/download
Manual de Instalação do **Ubuntu**:
http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2016/01/como-instalar-o-ubuntu.html

- Após a instalação do **Ubuntu**, o usuário deverá fazer o download do programa a partir da plataforma **Chalkup** ou **Github**.

Passo a passo:

- Depois de fazer download do programa, o terminal deverá ser aberto na pasta onde o programa se encontra.

- Após a abertura do terminal o usuário deverá digitar “python 117079354.py” (sem as aspas) e pressionar a tecla “enter” para confirmar.

- Após a confirmação do comando, o usuário será apresentado à um menu do programa. Para fazer a escolha dos modos, o usuário deverá digitar um número de 1 à 7 no terminal e pressionar “enter” para confirmar. O programa oferece os seguintes modos que serão descritos abaixo:

  1 - Ao escolher esta opção, o usuário terá acesso ao modo de geração de chaves, onde o mesmo deverá escolher digitando “Assinatura Digital” (sem as aspas) ou “Criptografia” (sem as aspas) e pressionando o enter para confirmar. Ao digitar “Assinatura Digital” (sem as aspas) o programa gerará chaves de assinatura digital. Ao digitar “Criptografia”(sem as aspas) o programa levará o usuário ao menu de escolha do tipo de chave de criptografia que se deseja gerar.

    1.1 - Ao digitar “Assinatura Digital”, o programa começará a gerar chaves para o método de assinatura digital, após a geração das chaves o programa oferecerá opções para salvar as chaves geradas em novos arquivos ou exibir as chaves geradas. Para escolher basta digitar “Salvar” (sem as aspas) ou “Exibir” (sem as aspas).

      1.1.1 - Ao escolher “Salvar”, o programa perguntará ao usuário qual nome deseja dar ao arquivo que guardará a chave pública e qual nome deseja dar ao arquivo que guardará a chave privada (nesta ordem).

      OBS: O nome escolhido para os arquivos deverá ser diferente do nome de qualquer outro arquivo na mesma pasta, caso o contrário, o arquivo já existente de mesmo tamanho será substituído pelo novo arquivo.

      1.1.2 - Ao escolher “Exibir”, o programa imprimirá no terminal os componentes da chave gerada separados por quebra de linha.

1.2 - Ao digitar “Criptografia”, o programa perguntará ao usuário qual tipo de chave ele deseja gerar e o usuário poderá escolher entre gerar chaves do método “El Gamal” ou do método “RSA”. Para fazer a escolha basta que o usuário digite “El Gamal” (sem as aspas) ou “RSA” (sem as aspas) e pressione “enter” para confirmar.

1.2.1 - Ao escolher “RSA”, o programa gerará chaves e componentes do método RSA. Após a geração das chaves o programa oferecerá opções para salvar as chaves geradas em novos arquivos ou exibir as chaves geradas. Para escolher basta digitar “Salvar” (sem as aspas) ou “Exibir” (sem as aspas).

1.2.1.1 - Ao escolher “Salvar”, o programa perguntará ao usuário qual nome deseja dar ao arquivo que guardará a chave pública e qual nome deseja dar ao arquivo que guardará a chave privada (nesta ordem).

OBS: O nome escolhido para os arquivos deverá ser diferente do nome de qualquer outro arquivo na mesma pasta, caso o contrário, o arquivo já existente de mesmo tamanho será substituído pelo novo arquivo.

1.2.1.2 - Ao escolher “Exibir”, o programa imprimirá no terminal os componentes da chave gerada separados por quebra de linha.

1.2.2 - Ao escolher “El Gamal”, o programa gerará chaves e componentes do método El Gamal. Após a geração das chaves o programa oferecerá opções para salvar as chaves geradas em novos arquivos ou exibir as chaves geradas. Para escolher basta digitar “Salvar” (sem as aspas) ou “Exibir” (sem as aspas).

1.2.1.1 - Ao escolher “Salvar”, o programa perguntará ao usuário qual nome deseja dar ao arquivo que guardará a chave pública e qual nome deseja dar ao arquivo que guardará a chave privada (nesta ordem).

OBS: O nome escolhido para os arquivos deverá ser diferente do nome de qualquer outro arquivo na mesma pasta, caso o contrário, o arquivo já existente de mesmo tamanho será substituído pelo novo arquivo.

1.2.1.2 - Ao escolher “Exibir”, o programa imprimirá no terminal os componentes da chave gerada separados por quebra de linha.

2 - Ao escolher esta opção, o usuário terá acesso ao modo de encriptação (pura), onde o mesmo deverá escolher digitando “RSA” (sem as aspas) para encriptar utilizando o método RSA ou “El Gamal” (sem as aspas) para encriptar utilizando o método El Gamal e pressionando o enter para confirmar.

2.1 - Após a escolha do método de encriptação o programa perguntará o nome do arquivo que se deseja encriptar. O usuário deverá digitar o nome do arquivo (que precisa estar na mesma pasta do programa) que se deseja encriptar.

2.1.1 - Após a digitação do nome do arquivo que se deseja encriptar, o programa deverá pedir a chave pública de encriptação. O usuário terá a opção de digitar ou de ler de um arquivo a chave pública. Para escolher basta escrever “Digitar” (sem as aspas) ou “Leia” (sem as aspas).

2.1.2 - Ao escolher digitar a chave pública, o usuário deverá digitar a chave pública obtida através do método de geração de chaves respeitando a quebra de linha. Para isso, o usuário deverá pressionar a tecla “enter” sempre que acabar de digitar uma linha da chave pública.

2.1.3 - Ao escolher ler a chave pública, o usuário deverá digitar o nome do arquivo que contém a chave pública e confirmar pressionando “enter”.

2.2 - Por fim, o usuário deverá escolher o nome com o qual deseja salvar o arquivo encriptado.
OBS: O nome escolhido para o arquivo deverá ser diferente do nome de qualquer outro arquivo na mesma pasta, caso o contrário, o arquivo já existente de mesmo tamanho será substituído pelo novo arquivo.

3 - Ao escolher esta opção, o usuário terá acesso ao modo de decriptografia (pura), onde o mesmo deverá escolher digitando “RSA” (sem as aspas) para decriptar utilizando o método RSA ou “El Gamal” (sem as aspas) para decriptar utilizando o método El Gamal e pressionando o enter para confirmar.

3.1 - Após a escolha do método de decriptografia o programa perguntará o nome do arquivo que se deseja decriptar. O usuário deverá digitar o nome do arquivo (que precisa estar na mesma pasta do programa) que se deseja decriptar.

3.1.1 - Após a digitação do nome do arquivo que se deseja decriptar, o programa deverá pedir a chave privada de decriptografia. O usuário terá a opção de digitar ou de ler de um arquivo a chave privada. Para escolher basta escrever “Digitar” (sem as aspas) ou “Leia” (sem as aspas).

3.1.2 - Ao escolher digitar a chave privada, o usuário deverá digitar a chave privada obtida através do método de geração de chaves respeitando a quebra de linha. Para isso, o usuário deverá pressionar a tecla “enter” sempre que acabar de digitar uma linha da chave privada.

3.1.3 - Ao escolher ler a chave privada, o usuário deverá digitar o nome do arquivo que contém a chave privada e confirmar pressionando “enter”.

3.2 - Por fim, o usuário deverá escolher o nome com o qual deseja salvar o arquivo descriptografado.

OBS: O nome escolhido para o arquivo deverá ser diferente do nome de qualquer outro arquivo na mesma pasta, caso o contrário, o arquivo já existente de mesmo tamanho será substituído pelo novo arquivo.

4 - Ao escolher esta opção, o usuário terá acesso ao modo de assinatura digital (pura), onde o mesmo deverá escolher o arquivo que deseja assinar digitalmente digitando o nome do arquivo (que precisa estar na mesma pasta do programa) e pressionando o enter para confirmar.

4.1 - Após a digitação do nome do arquivo que se deseja assinar, o programa deverá pedir a chave privada de assinatura. O usuário terá a opção de digitar ou de ler de um arquivo a chave privada. Para escolher basta escrever “Digitar” (sem as aspas) ou “Leia” (sem as aspas).

4.1.1 - Ao escolher digitar a chave privada, o usuário deverá digitar a chave privada obtida através do método de geração de chaves respeitando a quebra de linha. Para isso, o usuário deverá pressionar a tecla “enter” sempre que acabar de digitar uma linha da chave privada.

4.1.2 - Ao escolher ler a chave privada, o usuário deverá digitar o nome do arquivo que contém a chave privada e confirmar pressionando “enter”.

4.2 - Por fim, o usuário deverá escolher o nome com o qual deseja salvar o arquivo que contém a assinatura do arquivo primeiramente escolhido pelo usuário.

OBS: O nome escolhido para o arquivo deverá ser diferente do nome de qualquer outro arquivo na mesma pasta, caso o contrário, o arquivo já existente de mesmo tamanho será substituído pelo novo arquivo.

5 - Ao escolher esta opção, o usuário terá acesso ao modo de verificação assinatura digital (pura), onde o mesmo deverá escolher o arquivo original que foi assinado digitando o nome do arquivo (que precisa estar na mesma pasta do programa) e pressionando o enter para confirmar. Depois o usuário precisará fornecer o nome do arquivo que contém a assinatura que se deseja verificar digitando o nome do arquivo (que precisa estar na mesma pasta do programa) e pressionando o enter para confirmar.

5.1 - Após a digitação do nome do arquivo que se deseja assinar, o programa deverá pedir a chave pública de assinatura. O usuário terá a opção de digitar ou de ler de um arquivo a chave pública. Para escolher basta escrever “Digitar” (sem as aspas) ou “Leia” (sem as aspas).

5.1.1 - Ao escolher digitar a chave pública, o usuário deverá digitar a chave pública obtida através do método de geração de chaves respeitando a quebra de linha. Para isso, o usuário deverá pressionar a tecla “enter” sempre que acabar de digitar uma linha da chave privada.

5.1.2 - Ao escolher ler a chave pública, o usuário deverá digitar o nome do arquivo que contém a chave pública e confirmar pressionando “enter”.

5.2 - Por fim, o programa imprimirá o resultado da verificação informando se a assinatura é válida ou inválida.

6 - Ao escolher esta opção, o usuário terá acesso ao modo de assinatura digital e encriptação, onde o mesmo deverá escolher o arquivo que deseja encriptar e assinar digitalmente digitando o nome do arquivo (que precisa estar na mesma pasta do programa) e pressionando o enter para confirmar.

6.1 - Após a digitação do nome do arquivo que se deseja assinar e encriptar, o programa deverá pedir a chave privada de assinatura. O usuário terá a opção de digitar ou de ler de um arquivo a chave privada. Para escolher basta escrever “Digitar” (sem as aspas) ou “Leia” (sem as aspas).

6.1.1 - Ao escolher digitar a chave privada, o usuário deverá digitar a chave privada obtida através do método de geração de chaves respeitando a quebra de linha. Para isso, o usuário deverá pressionar a tecla “enter” sempre que acabar de digitar uma linha da chave privada.

6.1.2 - Ao escolher ler a chave privada, o usuário deverá digitar o nome do arquivo que contém a chave privada e confirmar pressionando “enter”.

6.2 - O programa deverá perguntar o método de encriptação que se deseja utilizar, onde o usuário deverá escolher digitando “RSA” (sem as aspas) para encriptar utilizando o método RSA ou “El Gamal” (sem as aspas) para encriptar utilizando o método El Gamal e pressionando o enter para confirmar.

6.2.1 - Após a digitação do método de encriptação que se deseja utilizar, o programa deverá pedir a chave pública de encriptação. O usuário terá a opção de digitar ou de ler de um arquivo a chave pública. Para escolher basta escrever “Digitar” (sem as aspas) ou “Leia” (sem as aspas).

6.2.2 - Ao escolher digitar a chave pública, o usuário deverá digitar a chave pública obtida através do método de geração de chaves respeitando a quebra de linha. Para isso, o usuário deverá pressionar a tecla “enter” sempre que acabar de digitar uma linha da chave pública.

6.2.3 - Ao escolher ler a chave pública, o usuário deverá digitar o nome do arquivo que contém a chave pública e confirmar pressionando “enter”.

6.3 - Por fim, o usuário deverá escolher o nome com o qual deseja salvar o arquivo encriptado e assinado.

OBS: O nome escolhido para o arquivo deverá ser diferente do nome de qualquer outro arquivo na mesma pasta, caso o contrário, o arquivo já existente de mesmo tamanho será substituído pelo novo arquivo.

7 - Ao escolher esta opção, o usuário terá acesso ao modo de verificação de assinatura digital e decriptografia, onde o mesmo deverá escolher o arquivo que deseja decriptar e verificar a assinatura digital digitando o nome do arquivo (que precisa estar na mesma pasta do programa) e pressionando o enter para confirmar.

7.1 - Após a digitação do nome do arquivo que se deseja decriptar e verificar assinatura digital, o usuário deverá escolher digitando “RSA” (sem as aspas) para decriptar utilizando o método RSA ou “El Gamal” (sem as aspas) para decriptar utilizando o método El Gamal e pressionando o enter para confirmar.

7.1.1 - O programa deverá pedir a chave privada de decriptografia. O usuário terá a opção de digitar ou de ler de um arquivo a chave privada. Para escolher basta escrever “Digitar” (sem as aspas) ou “Leia” (sem as aspas).

7.1.2 - Ao escolher digitar a chave privada, o usuário deverá digitar a chave privada obtida através do método de geração de chaves respeitando a quebra de linha. Para isso, o usuário deverá pressionar a tecla “enter” sempre que acabar de digitar uma linha da chave privada.

7.1.3 - Ao escolher ler a chave privada, o usuário deverá digitar o nome do arquivo que contém a chave privada e confirmar pressionando “enter”.

7.1.4 - Por fim, o usuário deverá escolher o nome com o qual deseja salvar o arquivo descriptografado.

OBS: O nome escolhido para o arquivo deverá ser diferente do nome de qualquer outro arquivo na mesma pasta, caso o contrário, o arquivo já existente de mesmo tamanho será substituído pelo novo arquivo.

7.2 - O programa deverá pedir a chave pública de assinatura. O usuário terá a opção de digitar ou de ler de um arquivo a chave pública. Para escolher basta escrever “Digitar” (sem as aspas) ou “Leia” (sem as aspas).

7.2.1 - Ao escolher digitar a chave pública, o usuário deverá digitar a chave pública obtida através do método de geração de chaves respeitando a quebra de linha. Para isso, o usuário deverá pressionar a tecla “enter” sempre que acabar de digitar uma linha da chave privada.

7.2.2 - Ao escolher ler a chave pública, o usuário deverá digitar o nome do arquivo que contém a chave pública e confirmar pressionando “enter”.

7.2.3 - O usuário deverá escolher o nome com o qual deseja salvar o arquivo que contém a assinatura do arquivo primeiramente escolhido pelo usuário.

OBS: O nome escolhido para o arquivo deverá ser diferente do nome de qualquer outro arquivo na mesma pasta, caso o contrário, o arquivo já existente de mesmo tamanho será substituído pelo novo arquivo.

7.3 - Por fim, o programa imprimirá o resultado da verificação informando se a assinatura é válida ou inválida.

Universidade Federal do Rio de Janeiro

Disciplina: Números Inteiros e Criptografia
Professor: Luis Menasché

Aluno: Breno Ferreira Rocha
