

Hướng dẫn sử dụng

Phần mềm Mã hóa

(Dành cho end-user)

Thực hiện: Phùng Minh Đạt

<Version: 1.0>

I. Giới thiệu.

1. Mục đích.

- Tài liệu hướng dẫn sử dụng này giúp cho người dùng có thể tra cứu nhanh cách sử dụng các chức năng trong phần mềm.
- Bạn có thể sử dụng tài liệu này trong khi đang sử dụng phần mềm hoặc trước khi sử dụng phần mềm.

2. Yêu cầu của phần mềm.

- Máy tính đã có môi trường JRE (Java Runtime Environment) phiên bản 1.8 trở lên.
- Nếu không có, cài JRE1.8 tại <https://www.java.com/download/>

3. Cài đặt phần mềm.

- Download phần mềm và click vào file .jar hoặc chạy cmd “java -jar filepath”

II. Sử dụng chức năng của phần mềm.

1. Mã hóa, Giải mã và phát sinh khóa (Mã hóa đối xứng).

The screenshot shows the 'Cryptography' application window. The 'Symmetric' tab is selected. The 'Input' field contains the text 'Phùng Minh Đạt'. The 'Key' field contains the text 'AvRUBLyoPjQ='. The 'Output' field contains the text 'kMuovd4Y0COjXs+BM3K7S0u7fZJGfgk'. The 'Select' panel on the right shows 'Encrypt' selected, 'DES' as the algorithm, '56' as the key size, 'None' as the mode, and 'NoPadding' as the padding. The 'Auto generate key' checkbox is checked. The 'Start' button is highlighted in green.

Cryptography

Symmetric Asymmetric Genkey pair Hash

Input
Phùng Minh Đạt

Input file **Open file**

Key
AvRUBLyoPjQ=

Key file **Save file**

Output
kMuovd4Y0COjXs+BM3K7S0u7fZJGfgk

Output file **Save file**

Select

☒ Encrypt ☐ Decrypt

properties

Algorithms **DES**

Key size **56**

Option

Mode **None**

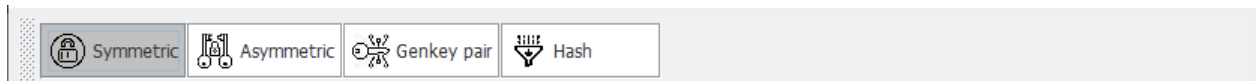
Padding **NoPadding**

☒ Auto generate key

Start

Generate Key

Bước 1: Nhấn vào button “Symmetric” trên thanh công cụ.



Bước 2: Chọn các tùy chọn cho quá trình Mã hóa, Giải mã.

A screenshot of a 'Select' dialog box. At the top, there are two radio buttons: 'Encrypt' (selected) and 'Decrypt'. Below this is a section titled 'properties' containing two dropdown menus: 'Algorithms' set to 'DES' and 'Key size' set to '56'. Below the 'properties' section is another section titled 'Option' containing two dropdown menus: 'Mode' set to 'None' and 'Padding' set to 'NoPadding'. At the bottom of the dialog is a checkbox labeled 'Auto generate key' which is checked.

- Chọn button “encrypt” cho quá trình Mã hóa hoặc “decrypt” cho quá trình Giải mã.
- Chọn “Algorithms” cho thuật toán bạn muốn thực hiện.
- Chọn “Key size” cho độ dài của Khóa.
- Chọn “Mode” để giải thuật thực hiện trên các khối block. Nếu không, bỏ qua lựa chọn này.
- Chọn “Padding” cho “Mode”
- Chọn “Auto generate key” để lựa chọn tự động phát sinh khóa khi Mã hóa hoặc nhập khóa từ bạn

Bước 3: Nhập dữ liệu Đầu vào.

A screenshot of an 'Input' dialog box. It features a large, empty rectangular text area for entering data. Below the text area, there is a label 'Input file' followed by a small text input field. To the right of this field is a button labeled 'Open file'.

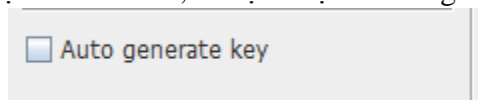
- Nhập dữ liệu Đầu vào của bạn (plain text cho quá trình Mã hóa, cipher text cho quá trình Giải mã).

- Bạn có thể đưa dữ liệu Đầu vào bằng cách mở file từ button “Open file”

Bước 4: Nhập khóa.

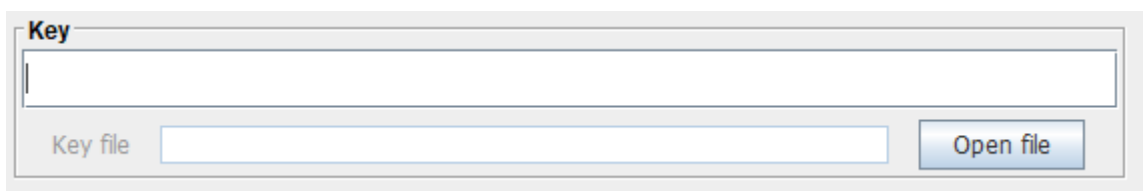
* Mã hóa.

- Nếu bạn đã có khóa, bỏ lựa chọn “Auto generate key” ở Bước 2.



☐ Auto generate key

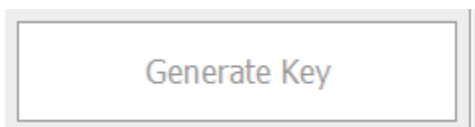
+ Sau đó bạn nhập khóa đã có khóa chọn “Open file” để nhập khóa từ file.



Key

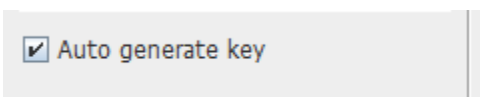
Key file

- Nếu bạn chỉ muốn phát sinh một khóa, bỏ lựa chọn “Auto generate key” ở Bước 2, sau đó nhấn button “Generate key”.



Generate Key

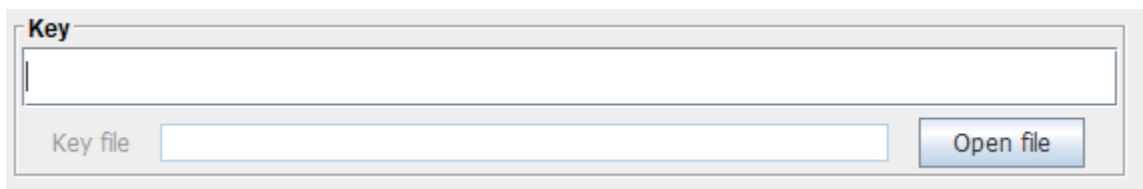
- Lựa chọn “Auto generate key” ở bước 2 để tự động phát sinh khóa trong quá trình Mã hóa.



☒ Auto generate key

* Giải mã.

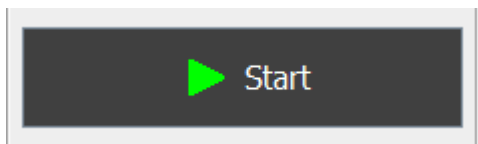
- Nhập khóa vào trường dữ liệu hoặc chọn “Open file” để nhập khóa từ file.



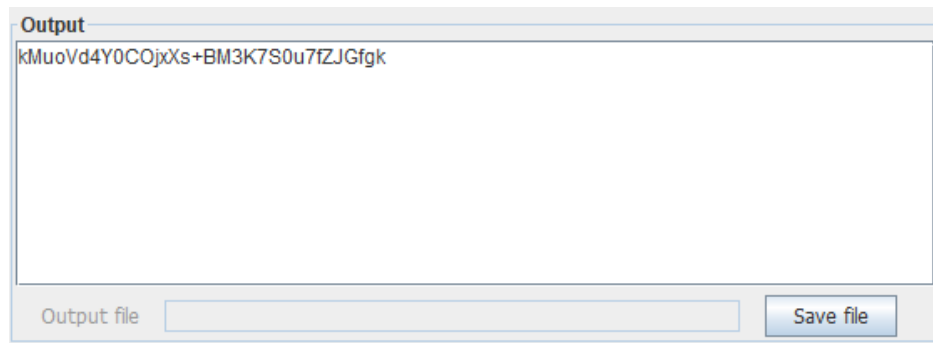
Key

Key file

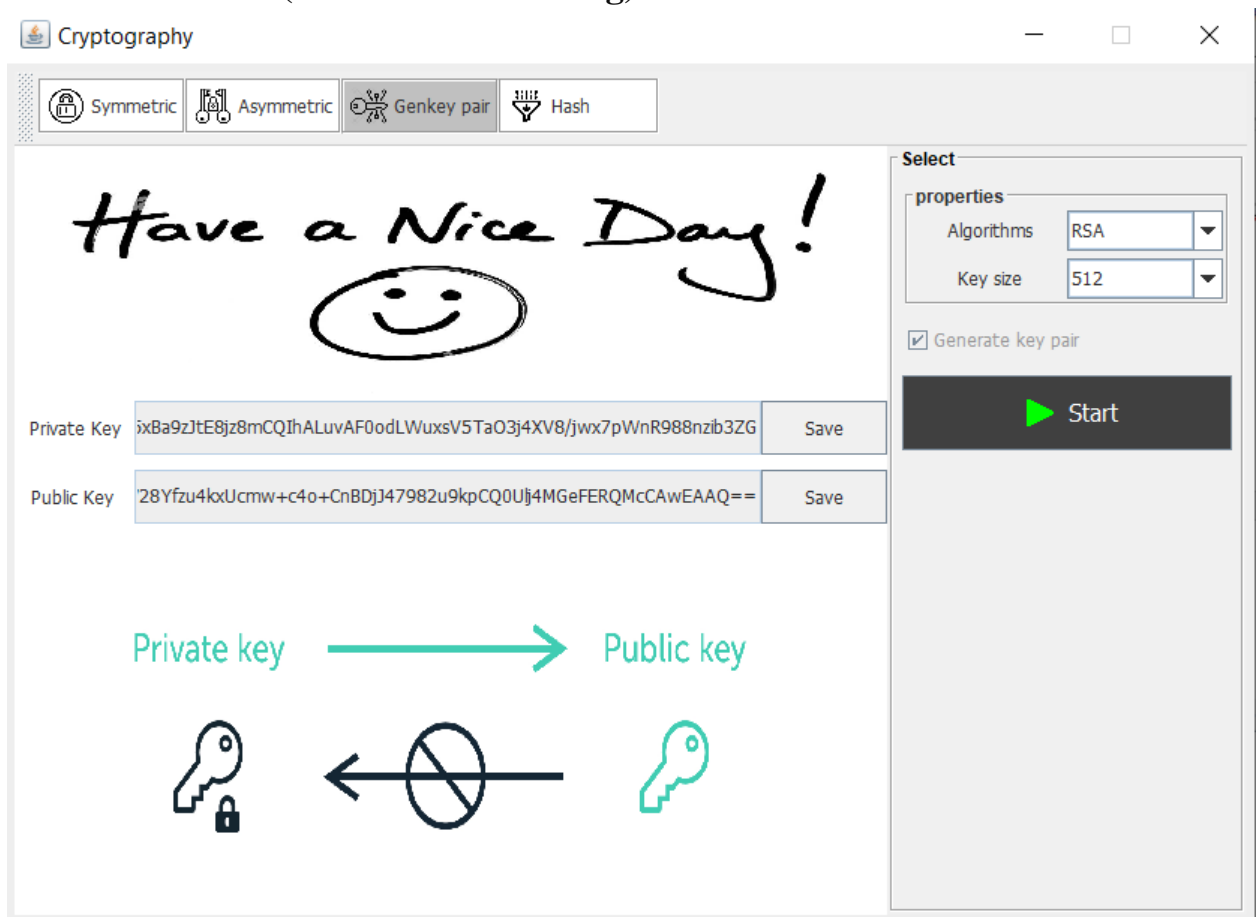
Bước 5: Nhấn vào button để thực hiện quá trình Mã hóa (Giải mã).



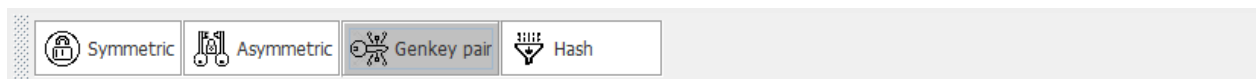
Bước 6: Nhấn vào button “Save file” để lưu dữ liệu Đầu ra (nếu muốn).



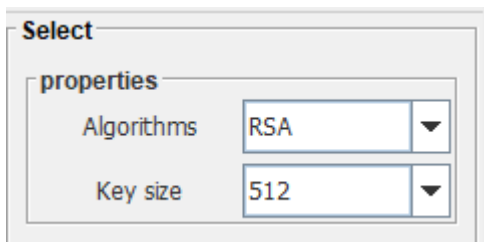
2. Phát sinh khóa (Mã hóa bất đối xứng).



Bước 1: Chọn button “Genkey Pair ” trên thanh công cụ.



Bước 2: Chọn thuật toán (Algorithms) và độ dài của khóa (Key size).



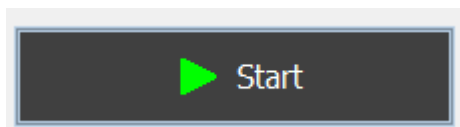
Select

properties

Algorithms RSA

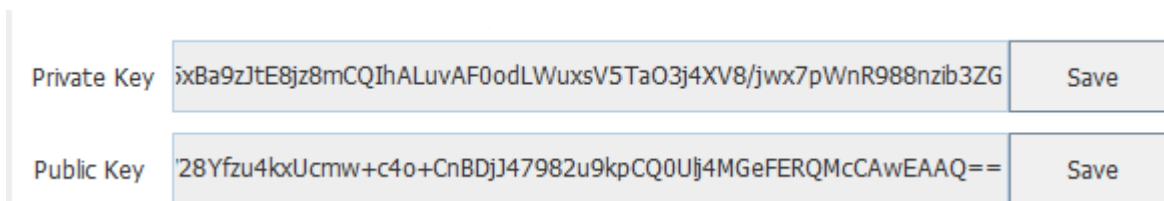
Key size 512

Bước 3: Nhấn button “Start” để phát sinh khóa.



Start

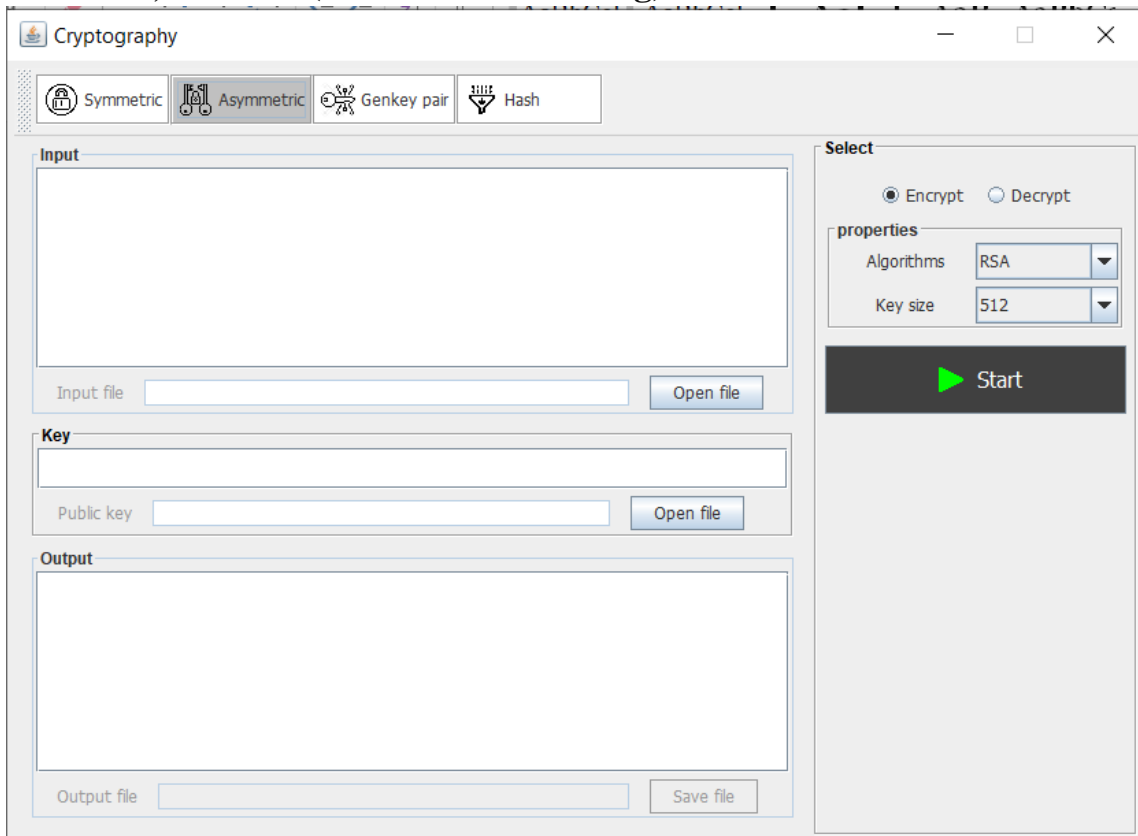
Bước 4: Nhấn vào button “Save” để lưu khóa vào file (nếu muốn).



Private Key ixBa9zJtE8jz8mCQIhALuvAF0odLWuxsV5TaO3j4XV8/jwx7pWnR988nzib3ZG Save

Public Key 28Yfzu4kxUcmw+c4o+CnBDjJ47982u9kpCQ0Uj4MGeFERQMCCAWEAAQ== Save

3. Mã hóa, Giải mã (Mã hóa bất đối xứng).



Cryptography

Symmetric Asymmetric Genkey pair Hash

Input

Input file Open file

Key

Public key Open file

Output

Output file Save file

Select

Encrypt Decrypt

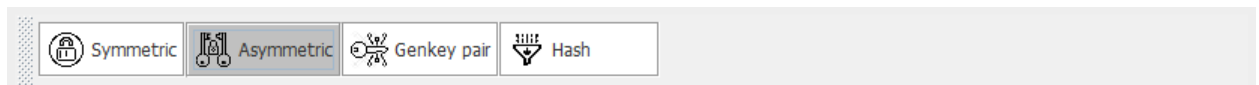
properties

Algorithms RSA

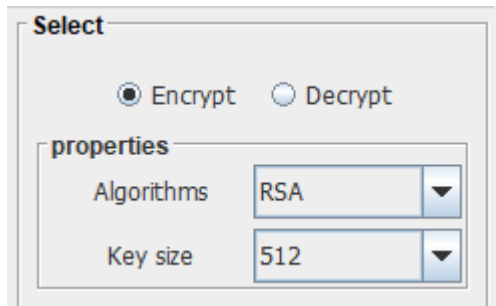
Key size 512

Start

Bước 1: Chọn button “Asymmetric” trên thanh công cụ.

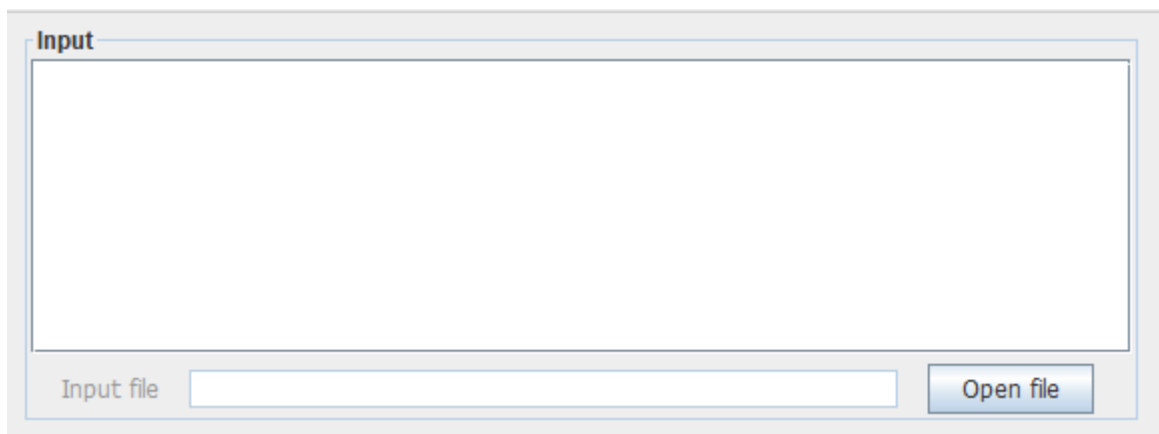


Bước 2: Tùy chọn

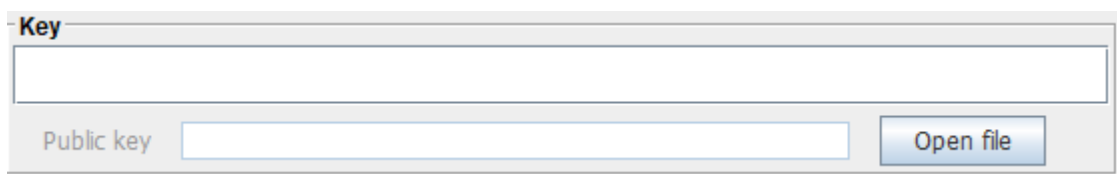


- Chọn button “Encrypt” để thực hiện quá trình Mã hóa, “Decrypt” cho quá trình Giải mã.
- Chọn giải thuật (algorithms) để thực hiện Mã hóa.
- Chọn độ dài khóa (key size) cho thuật toán.

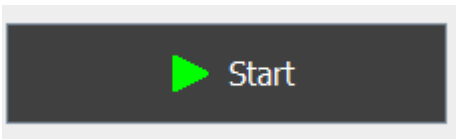
Bước 3: Nhập dữ liệu Đầu vào vào trường dữ liệu hoặc chọn button “Open file” để nhập dữ liệu từ file.



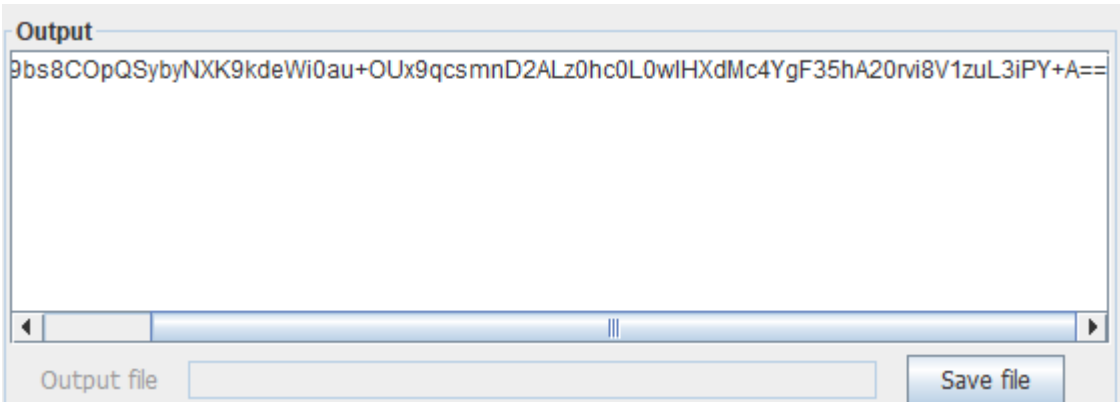
Bước 4: Nhập khóa(private key cho Giải mã && public key cho Mã hóa) vào trường dữ liệu hoặc chọn button “Open file” để nhập khóa từ file.



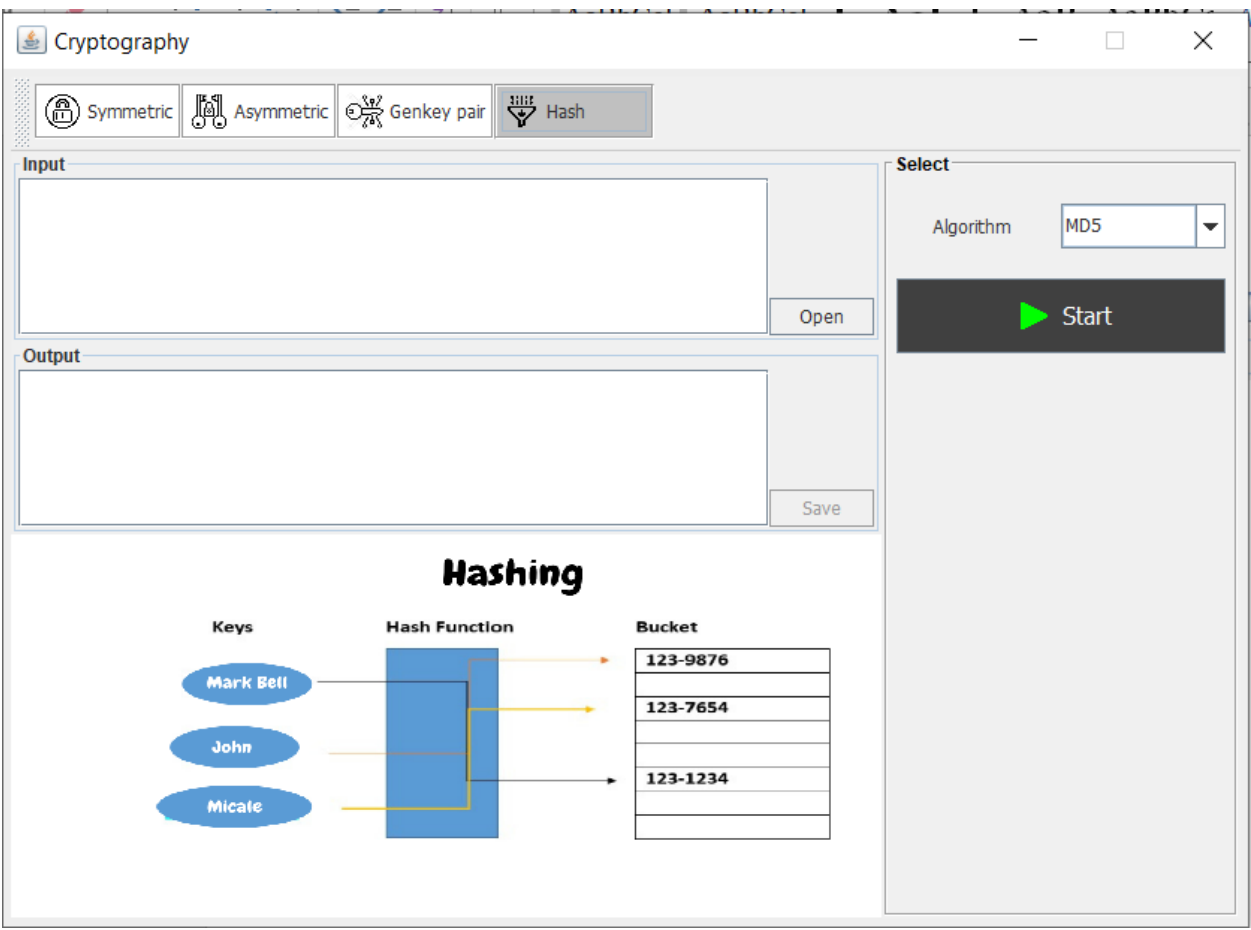
Bước 5: Nhấn vào button “Start” để Mã hóa (Giải mã).



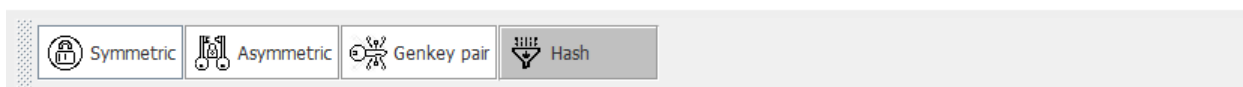
Bước 6: Chọn button “Save” để lưu dữ liệu Đầu ra đến file (nếu muốn).



4. Hàm băm.



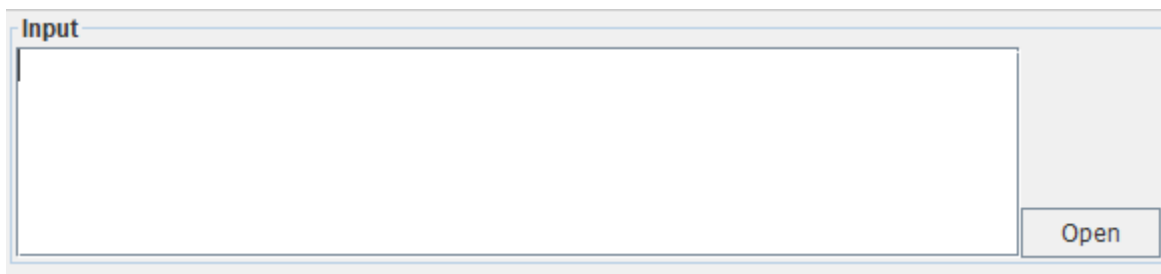
Bước 1: Chọn “Hash” trên thanh công cụ.



Bước 2: Chọn thuật toán cho hàm băm.



Bước 3: Nhập dữ liệu Đầu vào vào trường hoặc nhấn button “Open” để nhập từ file.



Bước 4: Nhấn “Start” để băm.



Bước 5: Nhấn “Save” để lưu Đầu ra vào file (nếu muốn).