**TRƯỜNG ĐẠI HỌC NÔNG LÂM TP. HỒ CHÍ MINH**



**KHOA CÔNG NGHỆ THÔNG TIN**

**----🙣🕮🙡----**

**Logo

Description automatically generated**

**Hướng dẫn sử dụng tool encrypt\_decypt**

**Lớp: Thứ 3 - Ca1**

**Sinh viên thực hiện:**

**21130419-Nguyễn Hoàng Lập**

**TP.HCM, ngày 29 tháng 02 năm 2024**

## 1.Giới thiệu về tool ecrytp\_decrypt:

Tool encrypt\_decrypt là giải pháp hỗ trợ mã hóa và giải mã một số giải thuật cơ bản , đối xứng, bất đối xứng, hỗ trợ tạo chữ kí số dựa trên file người dung cung cấp phục vụ cho người dung có nhu cầu mã hóa/ giải mã, kiểm tra file đồng nhất, tạo chữ kí số, kiểm tra chữ kí số, tính toán mã băm .

Bộ tool bao gồm:

|  |  |  |
| --- | --- | --- |
| TT | Tên File | Mô tả |
| 1 | Encrypt\_decrypt.jar | Đây là file khởi chạy tool trên môi trường java ire17 |
| 2 | Encrypt\_decrypt.exe | Đây là file khởi chạy |

## 2.Hướng dẫn cài đặt:

### 2.1. Hướng dẫn cài đặt:

Mở file encrypt\_decrypt.jar hoặc Encrypt\_decrypt.exe và tiến hành sử dụng. Không cần setup gì them.

### 2.2 Yêu cầu đối với hệ thống sử dụng tool:

Vì tool phát triển trên bộ ngôn ngữ java với sdk 17.0.0 nên bắt buộc thiết bị cần cài bộ môi trường chạy ngôn ngữ này.

Hệ điều hành: windown , linux,…

- Bộ nhớ RAM: trên phiên bản test gần nhất , tool chạy 94.7mb ram.

-- Dung lượng ổ đĩa: Tool không cài vào ổ đĩa nên không có yêu cầu về dung lượng nhưng bạn cần ít nhất 10mb trở lên để thực hiện các tác vụ lưu file output

-Trên máy tính người dùng cần cài đặt **Java SE 17** , bạn có thể tải ở đây<https://www.oracle.com/java/technologies/javase/jdk17-archive-downloads.html>

## 3. Hướng dẫn sử dụng phần mềm:

Khi chạy file jar bạn sẽ vào màn hình tại tab mã hóa truyền thống:

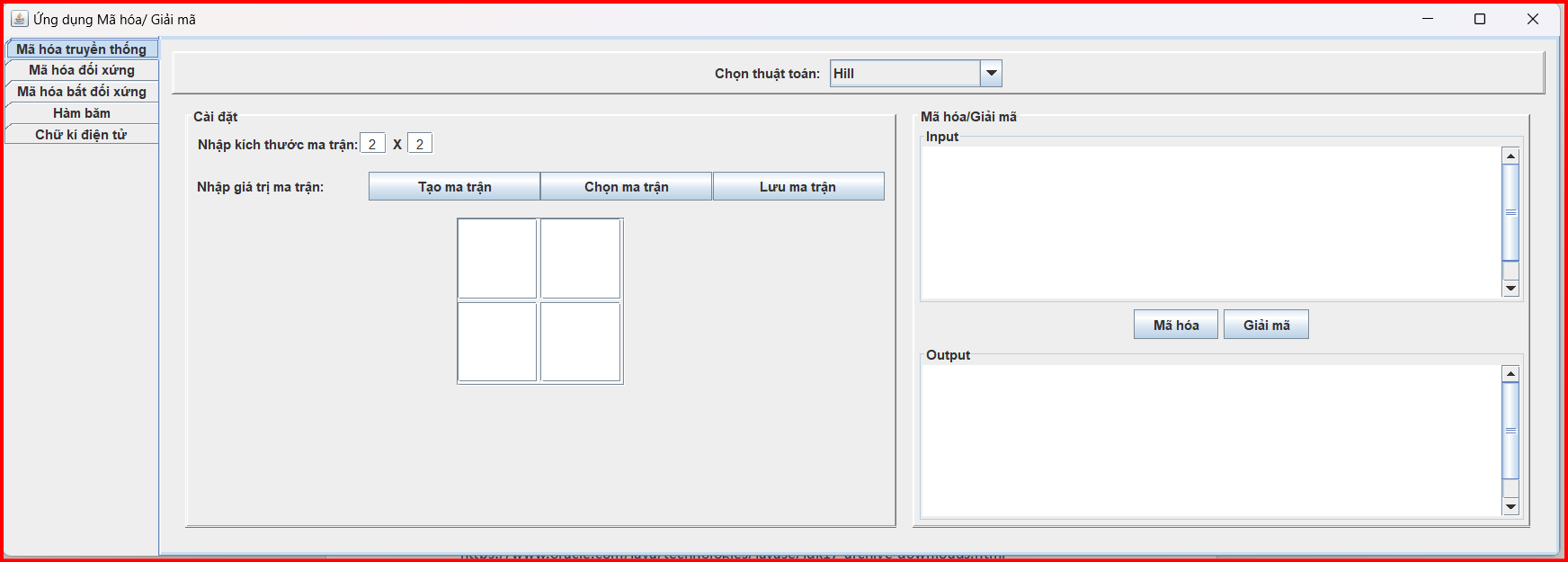
****

Figure :màn hình khởi chạy

Bước 1: người dùng chọn giải thuật theo phân loại

Mã hóa truyền thống : Caesar, substitution , affine, hill, vigenere,

Mã háo đối xứng : AES , DES

Mã hóa bất đối xứng: RSA

Hàm băm : MD5 ,SHA,

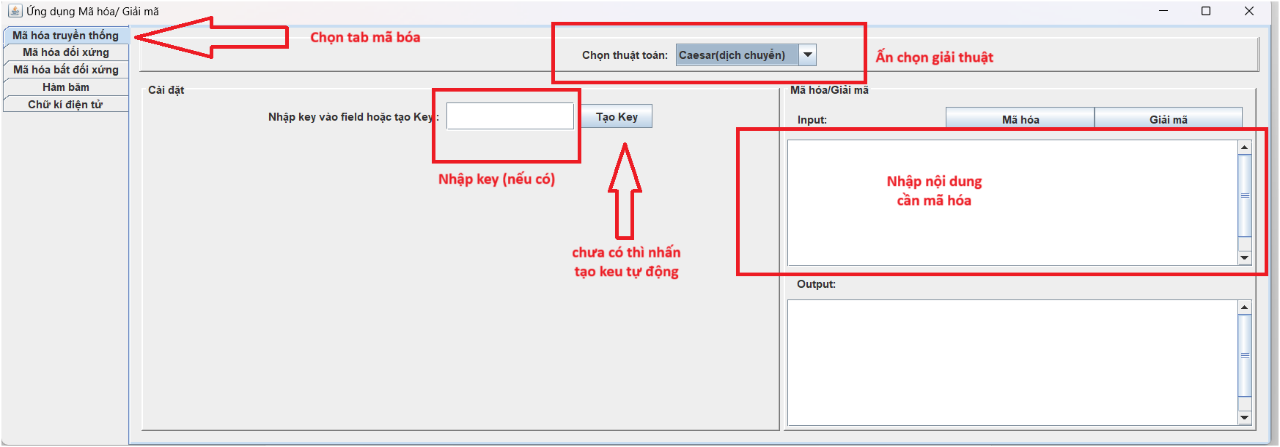
Chữ kí điện tử

### 3.1 Hướng dẫn mã hóa truyền thống:

#### 3.1.1 caesar :

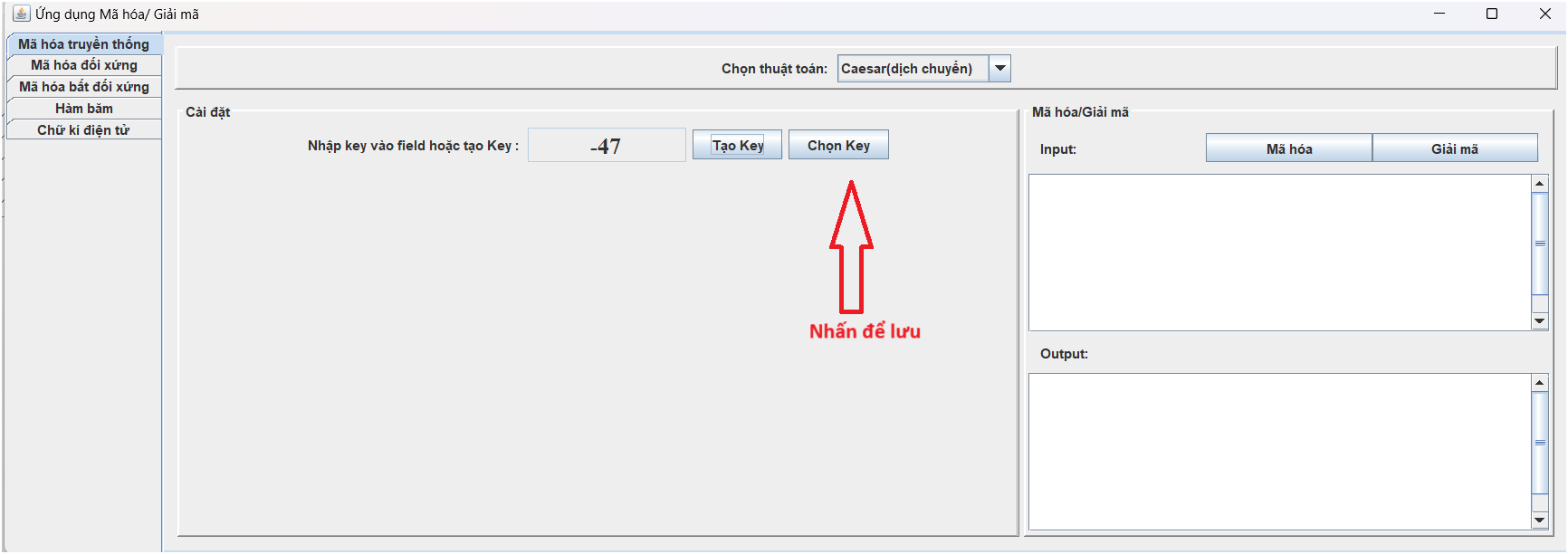
Bước 1: người dùng chọn tab mã hóa truyền thống, sau đó chọn thuật toán Caesar

Bước 2: Nếu người dùng đã có key thì người dùng nhập key vào ô nhập key, nếu chưa có nhấn nút “tạo key” phần mềm sẽ tự động tạo ra 1 key phù hợp với giải thuật

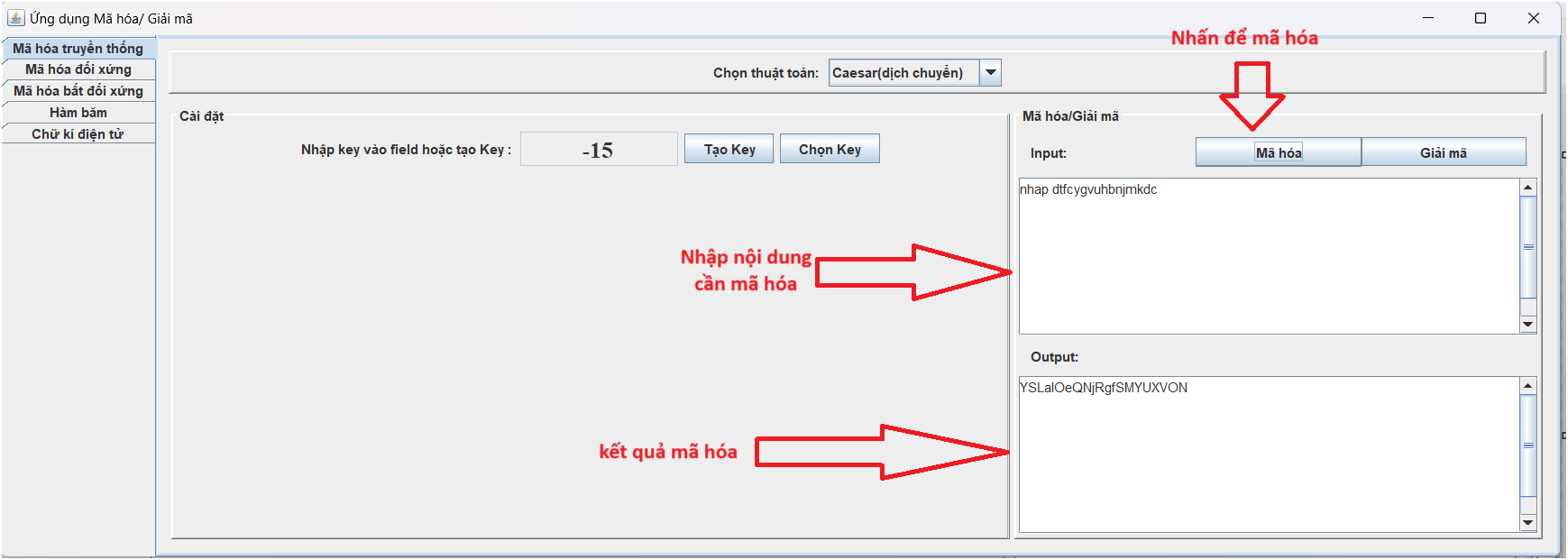


\*Lưu ý: Phần mềm hiện tãi chỉ hỗ trợ nhập key với chuẩn theo số nên nếu key của bạn chưa không phải số thì không sử dụng được

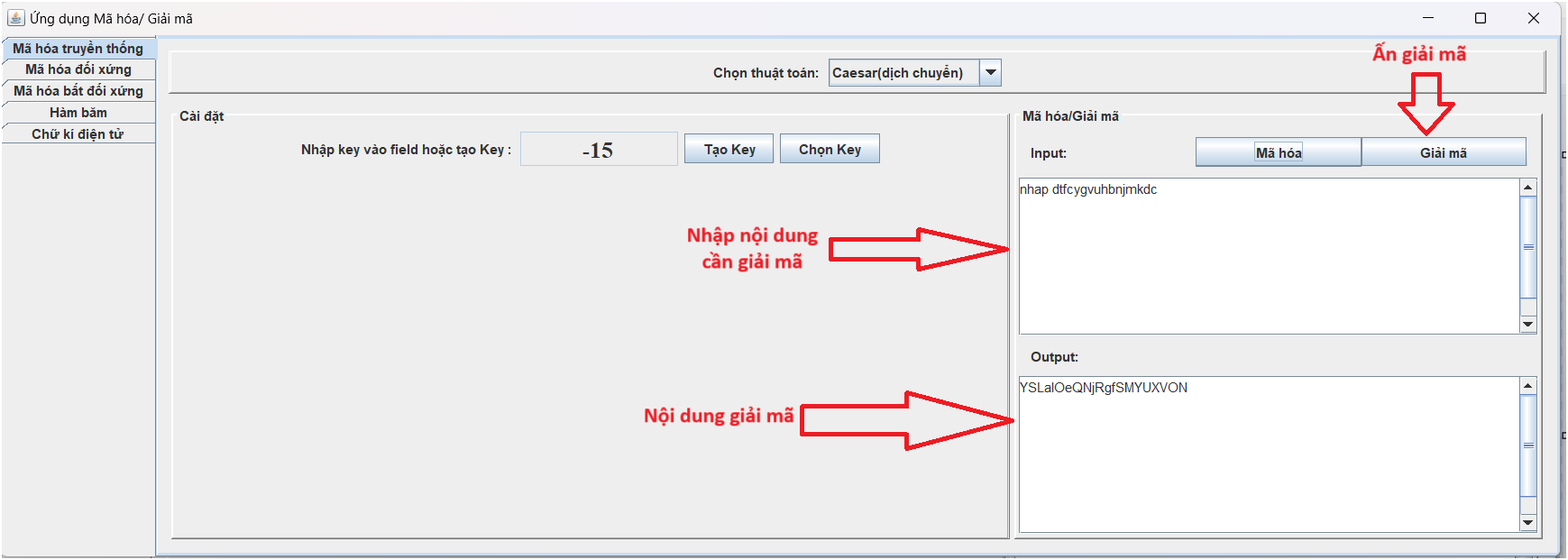
Bước 3: sau khi nhập hoạc tạo key , người dùng cần nhấn “ chọn key” để phần mềm biết quá trình nhập key đã xong. Tiến hành mã hóa/ giải mã.



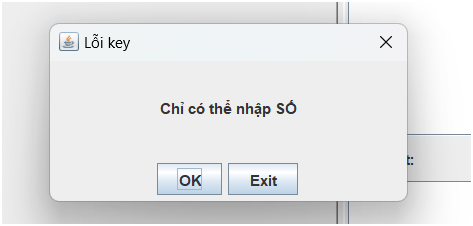
Bước 3.1: sau khi nhập key , người dùng muốn mã hóa thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



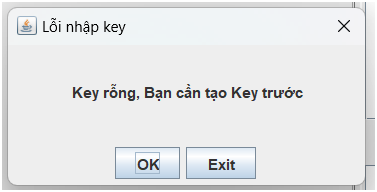
Bước 3.2: sau khi nhập key , người dùng muốn giải mã thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 `sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



* 1 số lỗi khi sử dụng
  + Nhập key là chữ sẽ mở cửa sổ lỗi

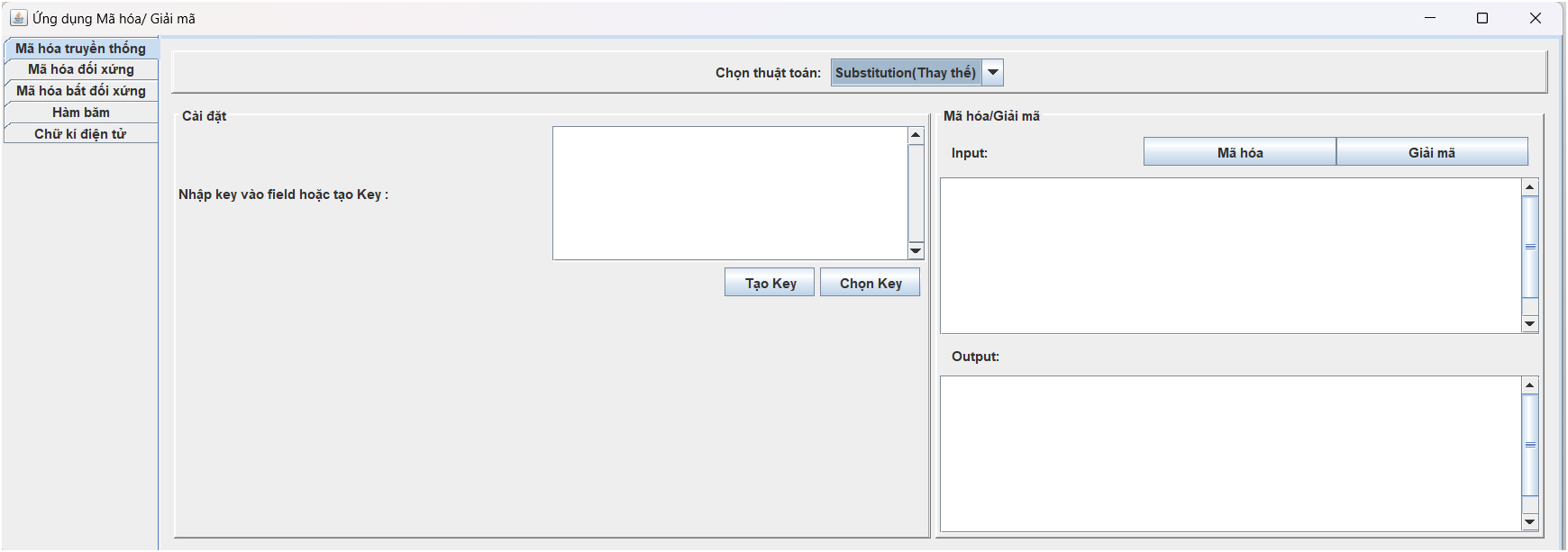
cc

* + Key chưa được chọn

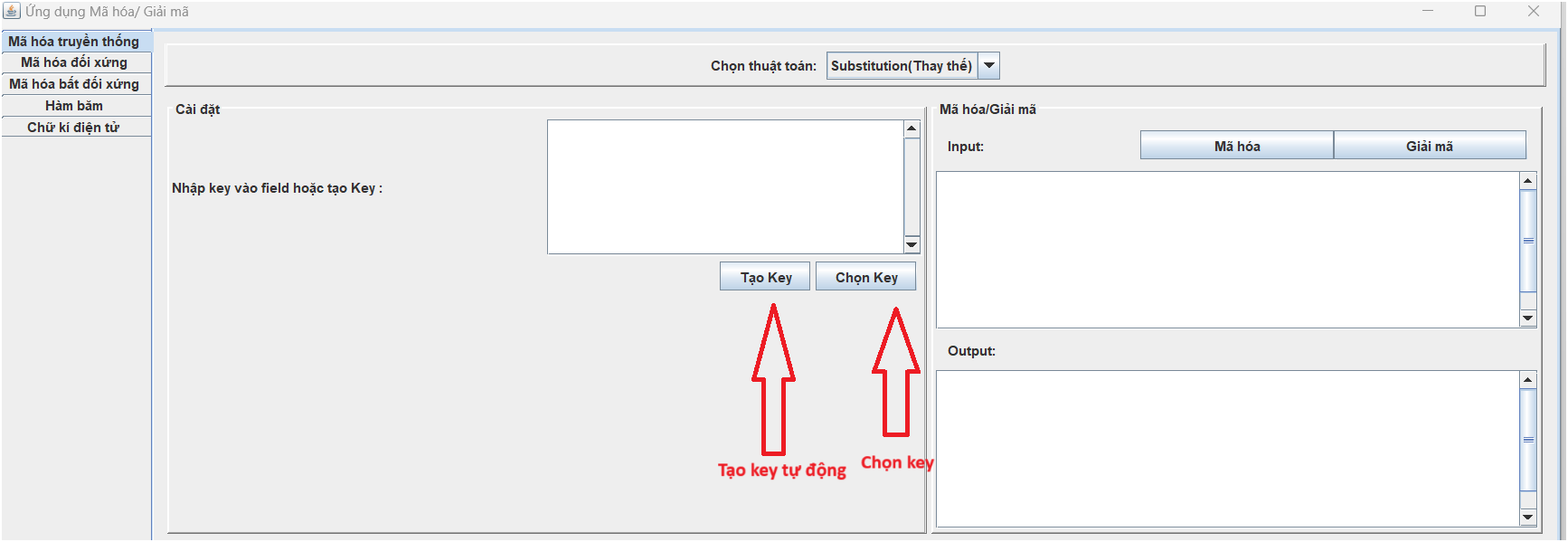


#### 3.1.2: Substitution:

Bước 1: người dùng chọn tab mã hóa truyền thống, sau đó chọn thuật toán Subtitution

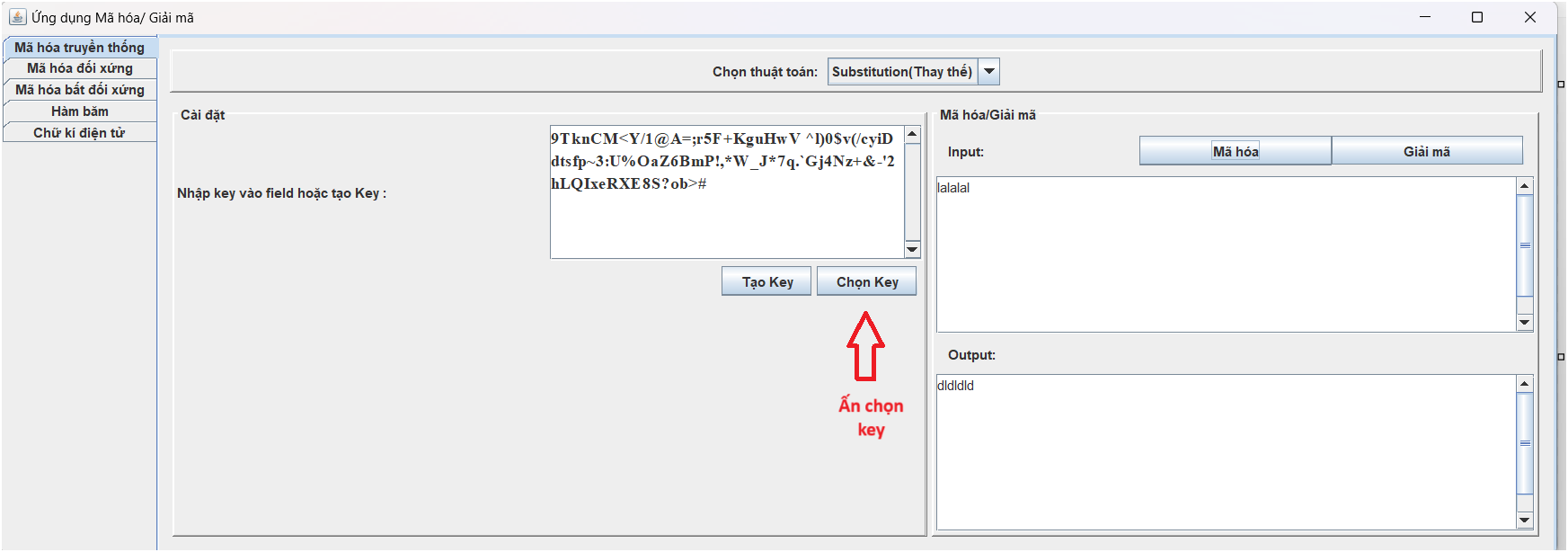


Bước 2: Nếu người dùng đã có key thì người dùng nhập key vào ô nhập key, nếu chưa có nhấn nút “tạo key” phần mềm sẽ tự động tạo ra 1 key phù hợp với giải thuật

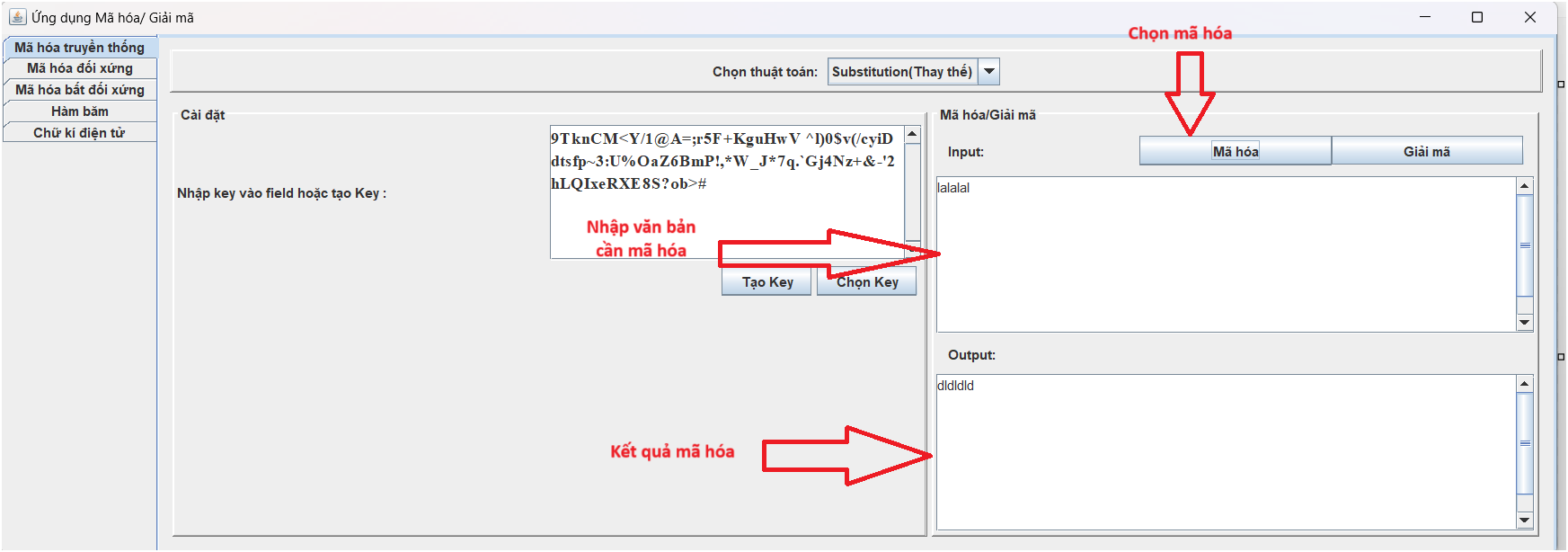


\*Lưu ý: Phần mềm hiện tãi chỉ hỗ trợ nhập key là số nên nếu key của không phải số thì không sử dụng được

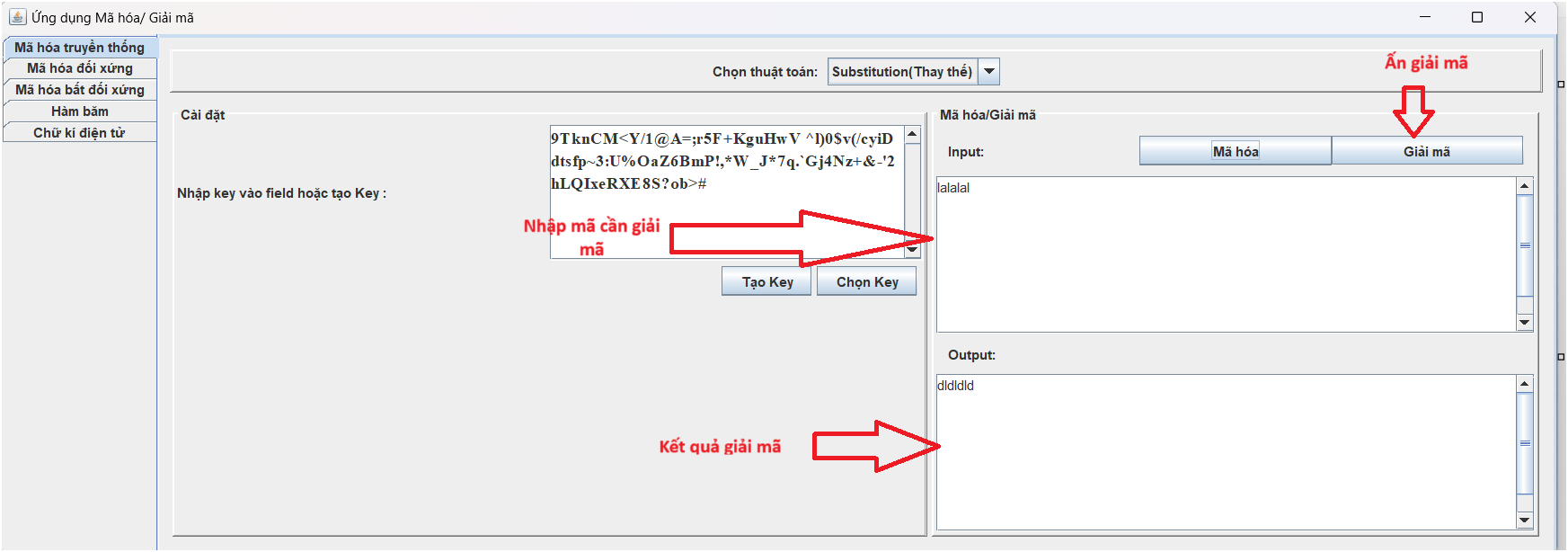
Bước 3: sau khi nhập hoạc tạo key , người dùng cần nhấn “ chọn key” để phần mềm biết quá trình nhập key đã xong. Tiến hành mã hóa/ giải mã



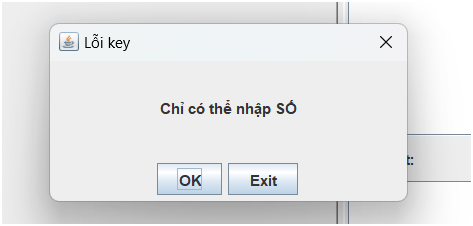
Bước 3.1: sau khi nhập key , người dùng muốn mã hóa thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



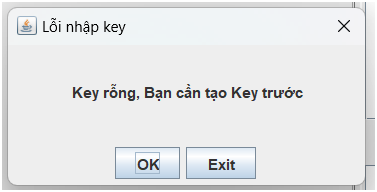
Bước 3.2: sau khi nhập key , người dùng muốn giải mã thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



* 1 số lỗi khi sử dụng
  + Nhập key là chữ

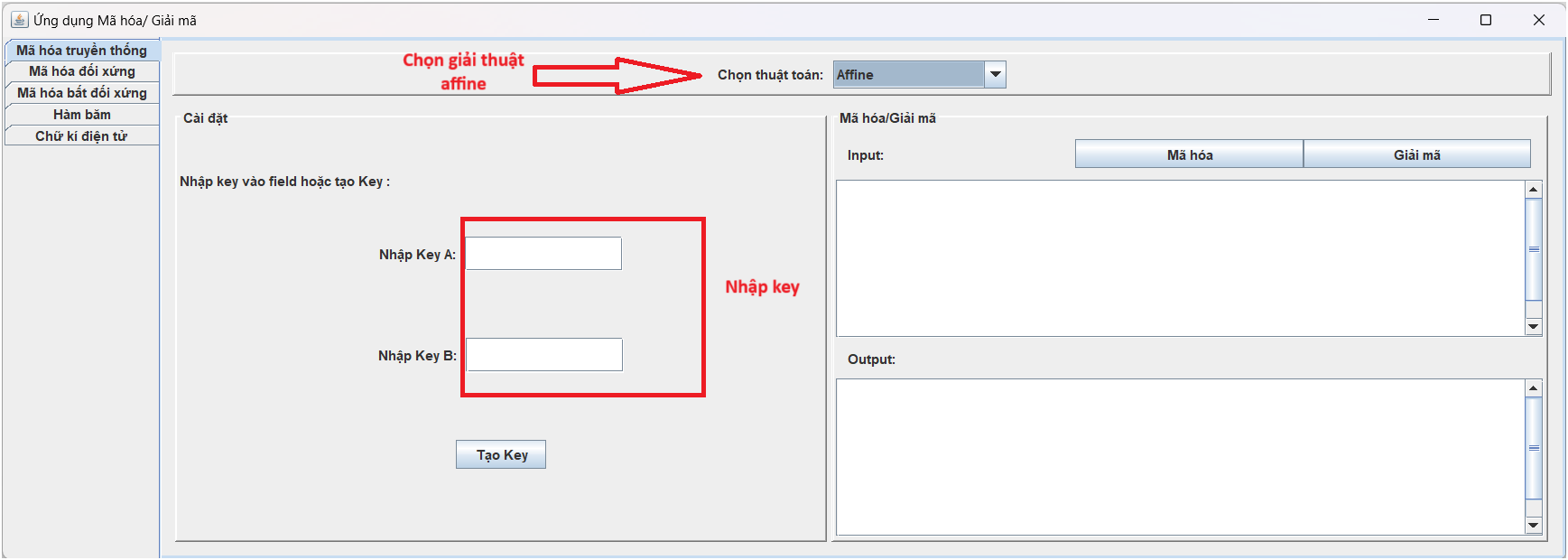


* + Key chưa được chọn

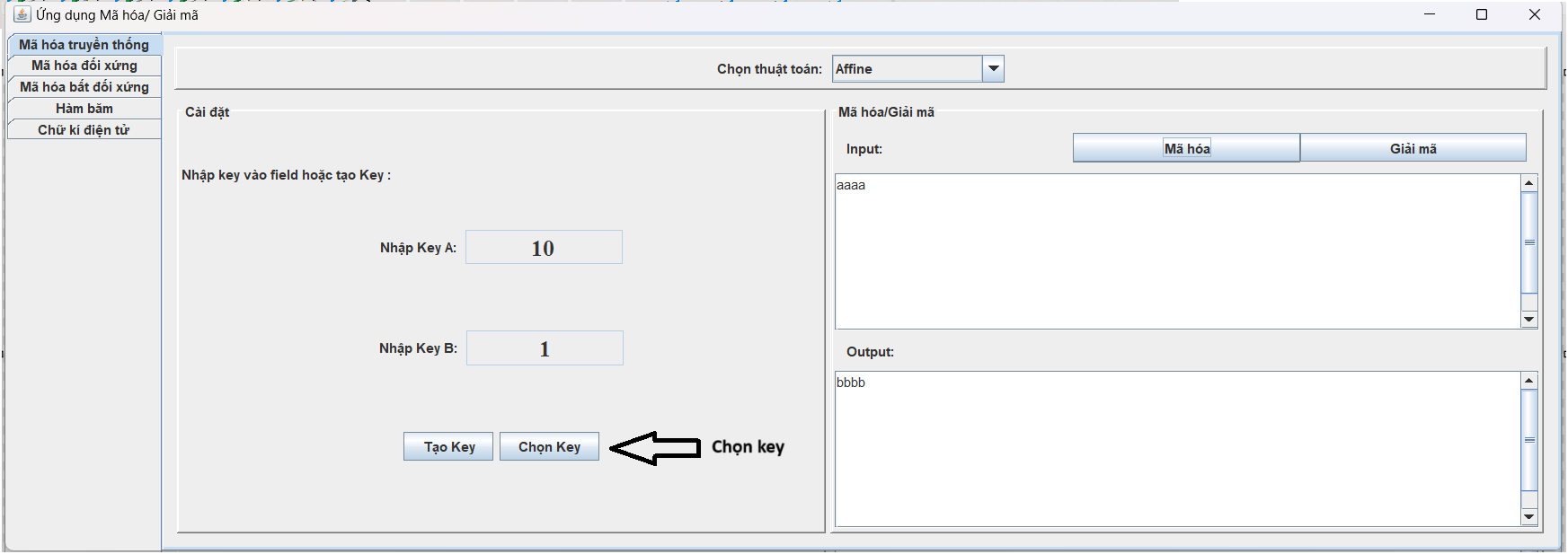


#### 3.1.3 Affine:

Bước 1: người dùng chọn tab mã hóa truyền thống, sau đó chọn thuật toán Affine

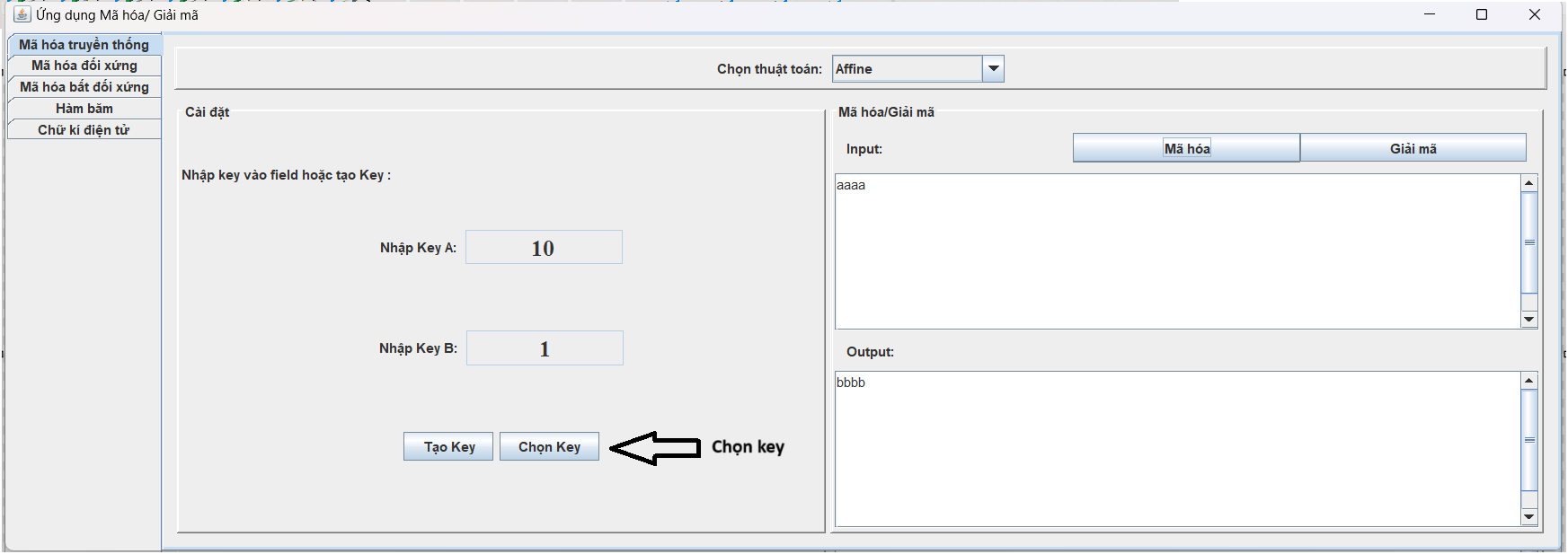


Bước 2: Nếu người dùng đã có key thì người dùng nhập key vào ô nhập key, nếu chưa có nhấn nút “tạo key” phần mềm sẽ tự động tạo ra 1cặp key A B phù hợp với giải thuật

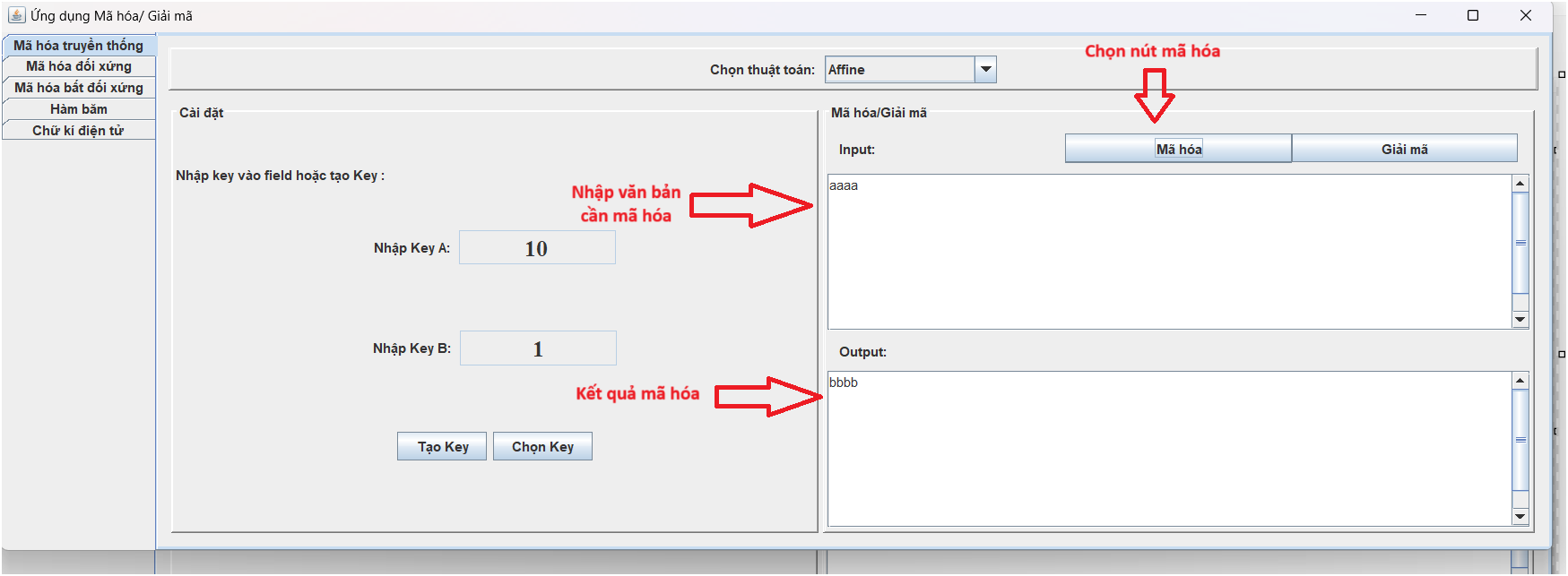


\*Lưu ý: Phần mềm hiện tãi chỉ hỗ trợ nhập key là số nên nếu key của không phải số thì không sử dụng được

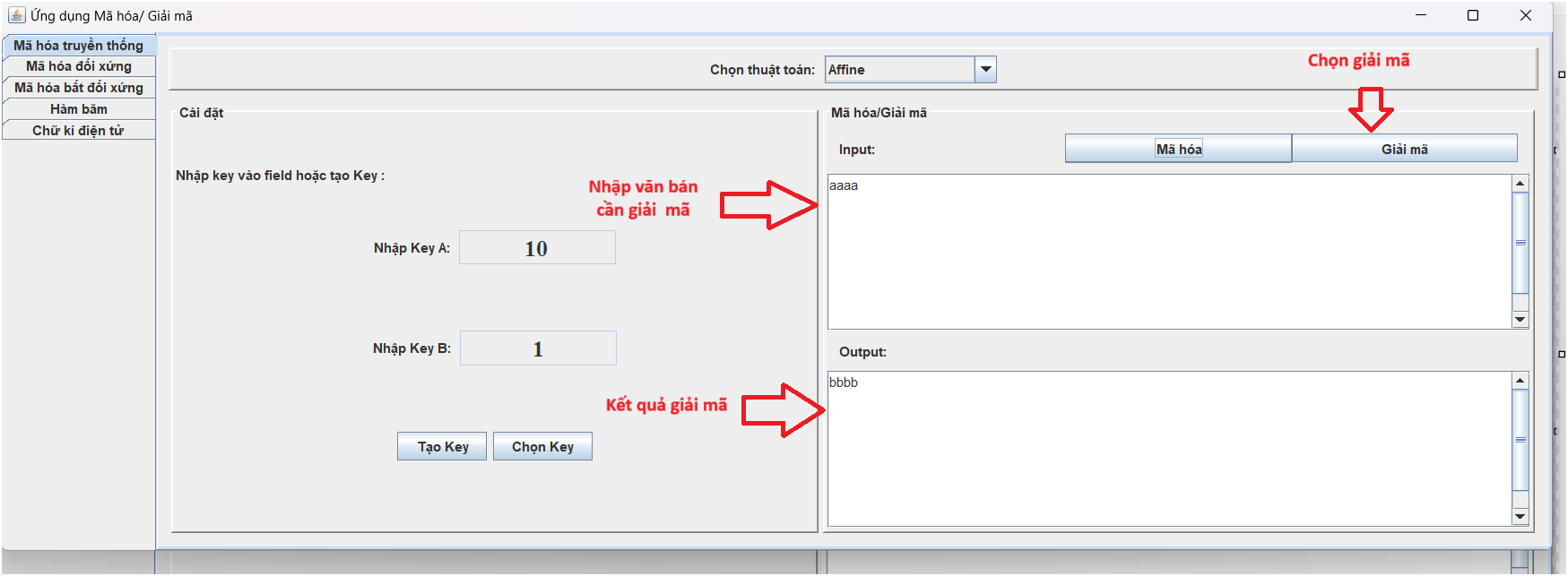
Bước 3: sau khi nhập hoạc tạo key , người dùng cần nhấn “ chọn key” để phần mềm biết quá trình nhập key đã xong. Tiến hành mã hóa/ giải mã.



Bước 3.1: sau khi nhập key , người dùng muốn mã hóa thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



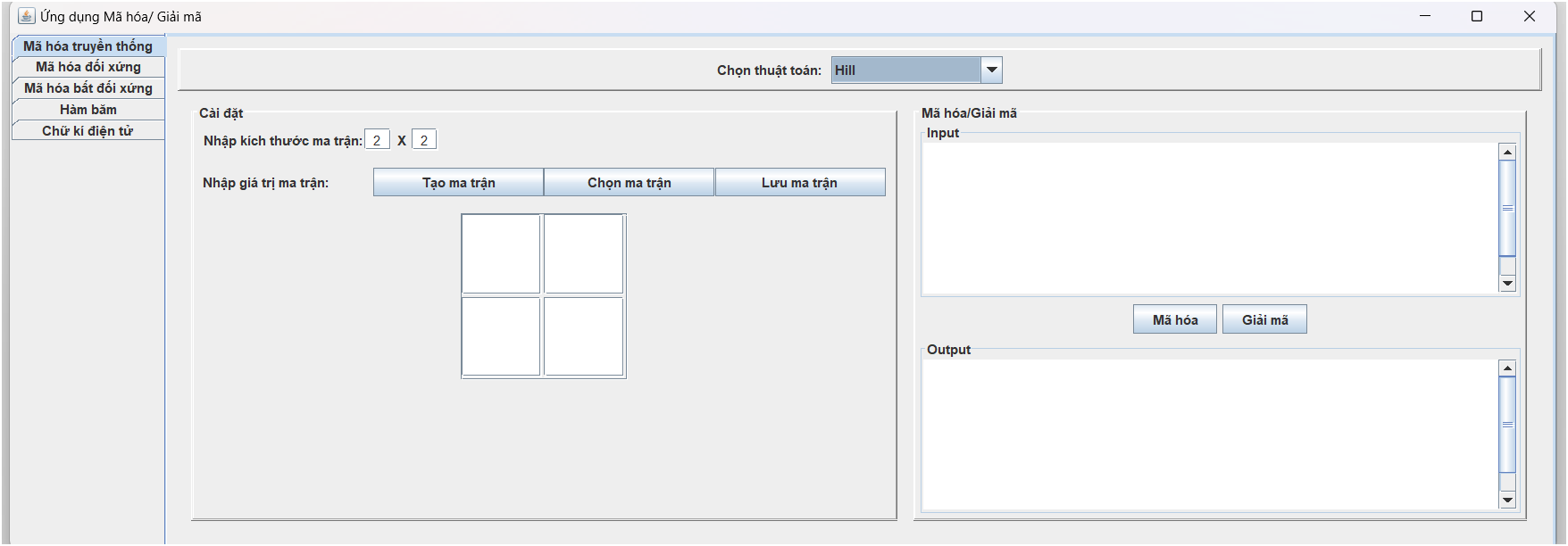
Bước 3.2: sau khi nhập key , người dùng muốn giải mã thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



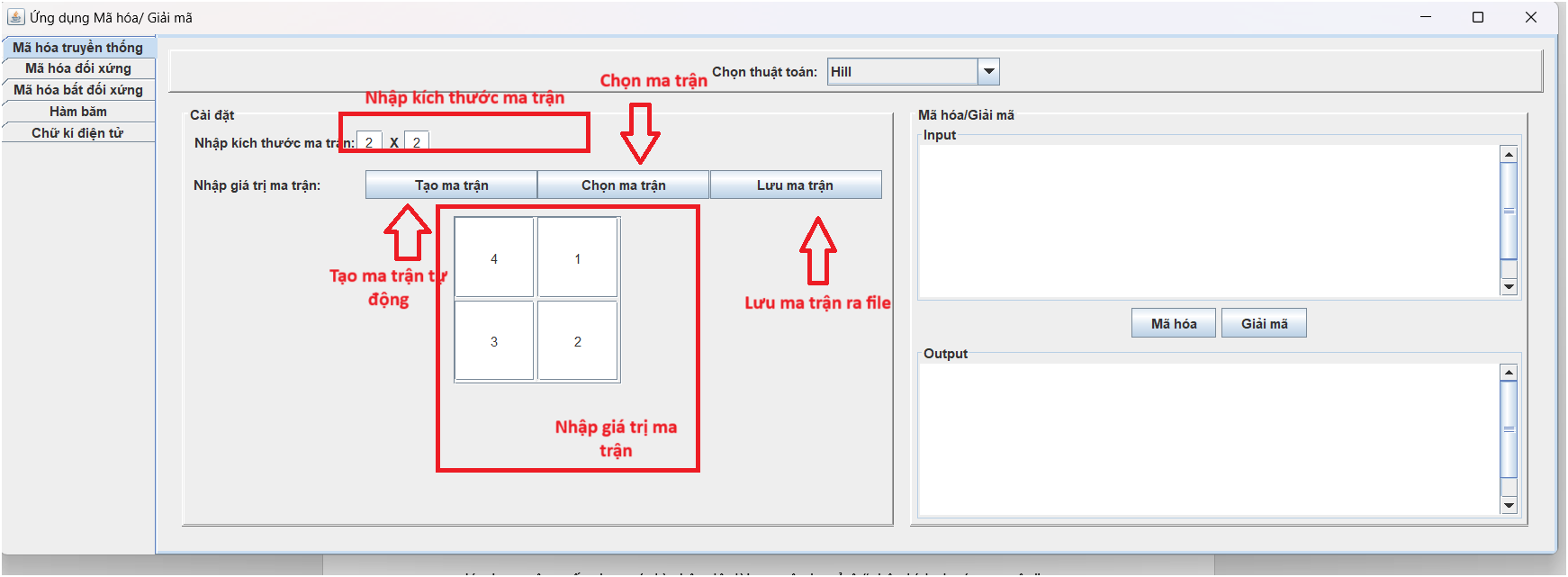
* 1 số lỗi khi sử dụng
  + Nhập key là chữ
  + Key chưa được chọn

#### 3.1.4 Hill:

Bước 1: người dùng chọn tab mã hóa truyền thống, sau đó chọn thuật toán Hill

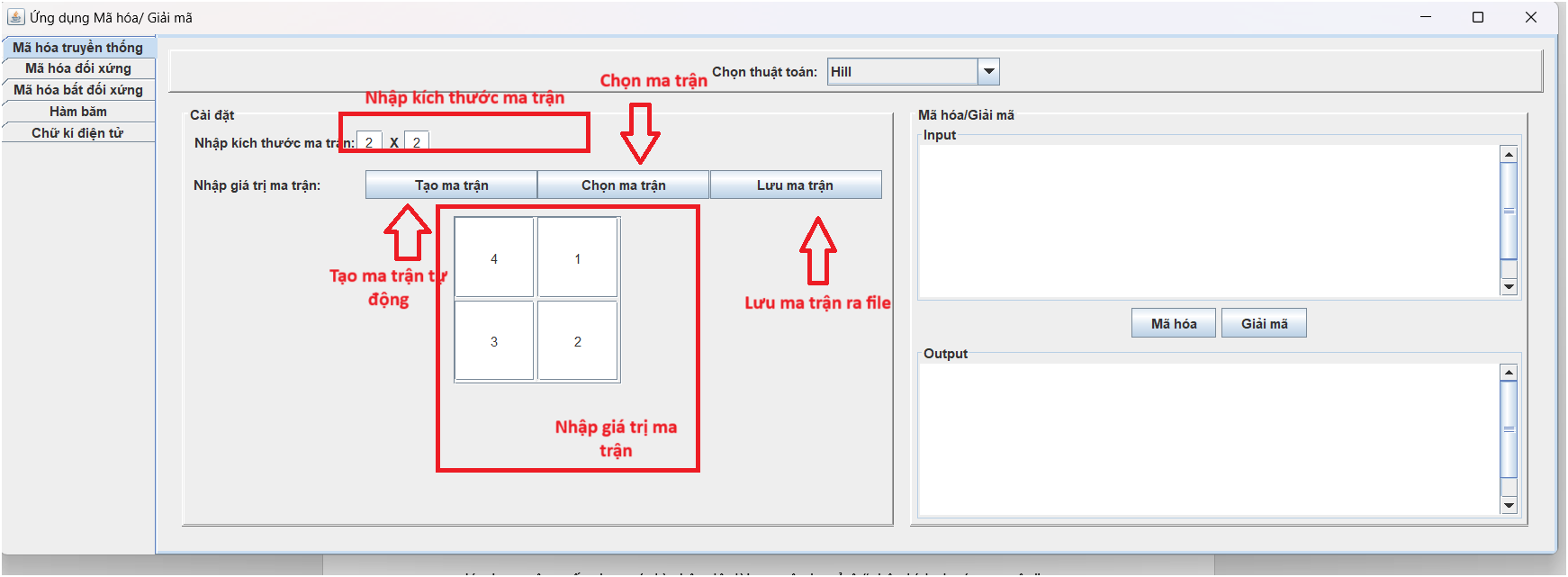


Bước 2: Thuật toán hill nhận vào là 1 ma trận nxn có khả năng đảo ngược như là 1 key nên nếu người dùng đã có key thì người dùng nhập độ dài ma trận key vào ô nhập kích thước, và giá trị ma trận , nếu chưa có thì nhập độ dài ma trận key ở ô “nhập kích thước ma trận” sau đó nhấn nút “tạo key” phần mềm sẽ tự động tạo ra ma trận phù hợp với giải thuật

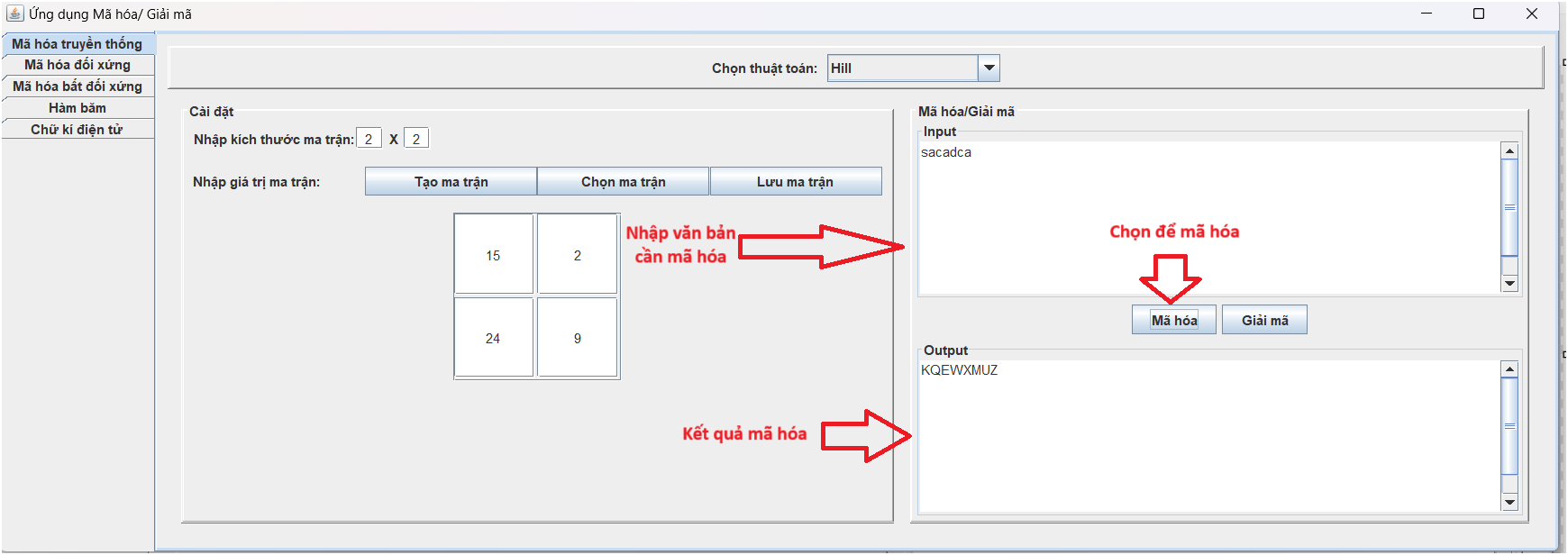


\*Lưu ý: Phần mềm hiện tãi chỉ hỗ trợ nhập key là ma trận nxn đối xứng nên nếu key của không phải đáp ứng được thì không sử dụng được

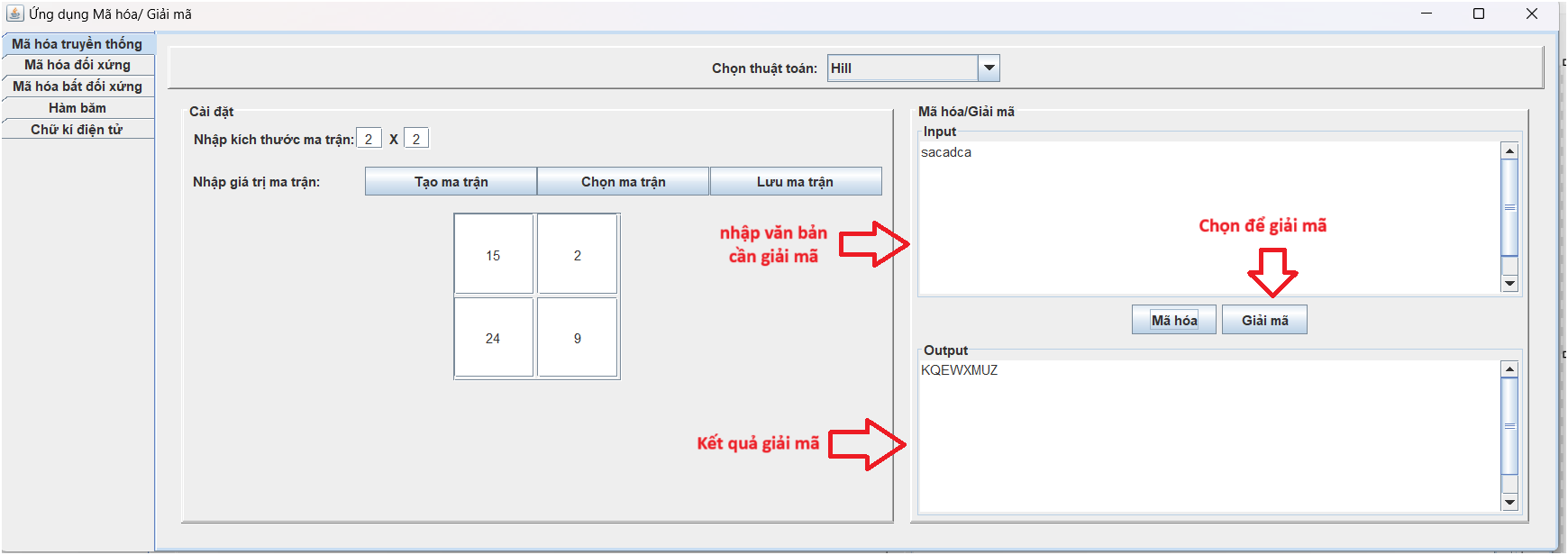
Bước 3: sau khi nhập hoạc tạo key , người dùng cần nhấn “ chọn key” để phần mềm biết quá trình nhập key đã xong. Tiến hành mã hóa/ giải mã.



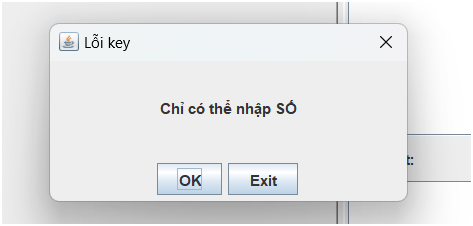
Bước 3.1: sau khi nhập key , người dùng muốn mã hóa thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



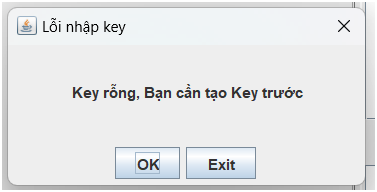
Bước 3.2: sau khi nhập key , người dùng muốn giải mã thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



* 1 số lỗi khi sử dụng
  + Nhập key là chữ

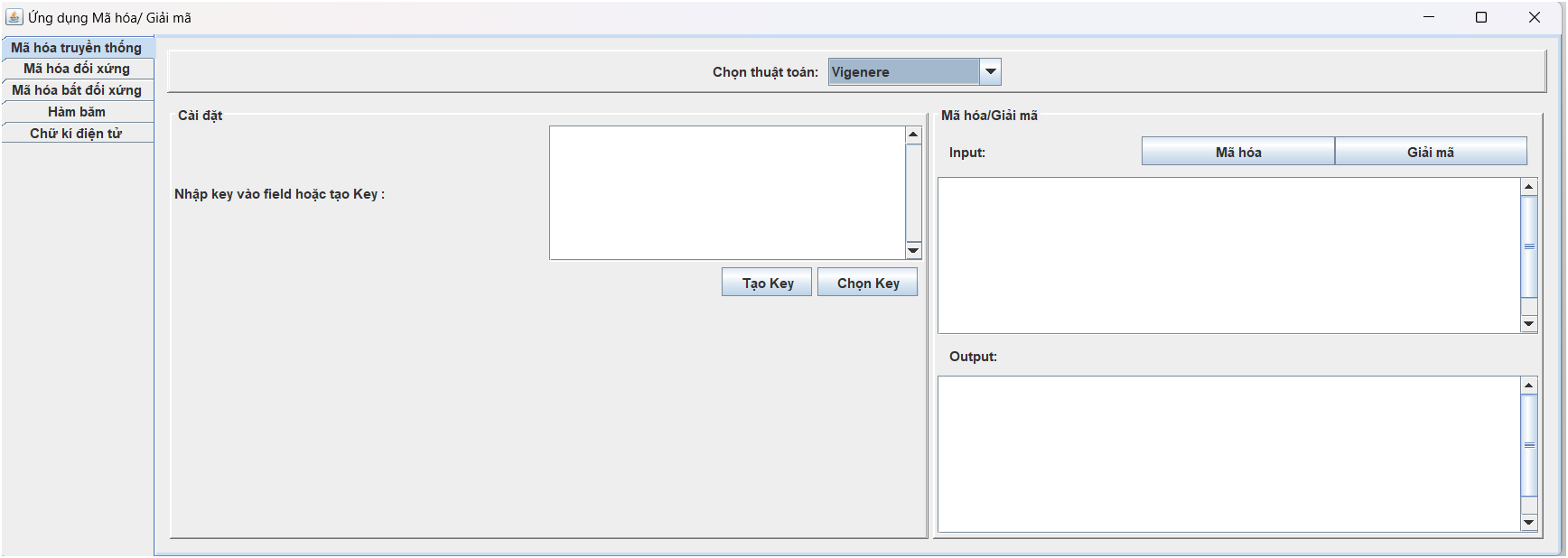


* Key chưa được chọn

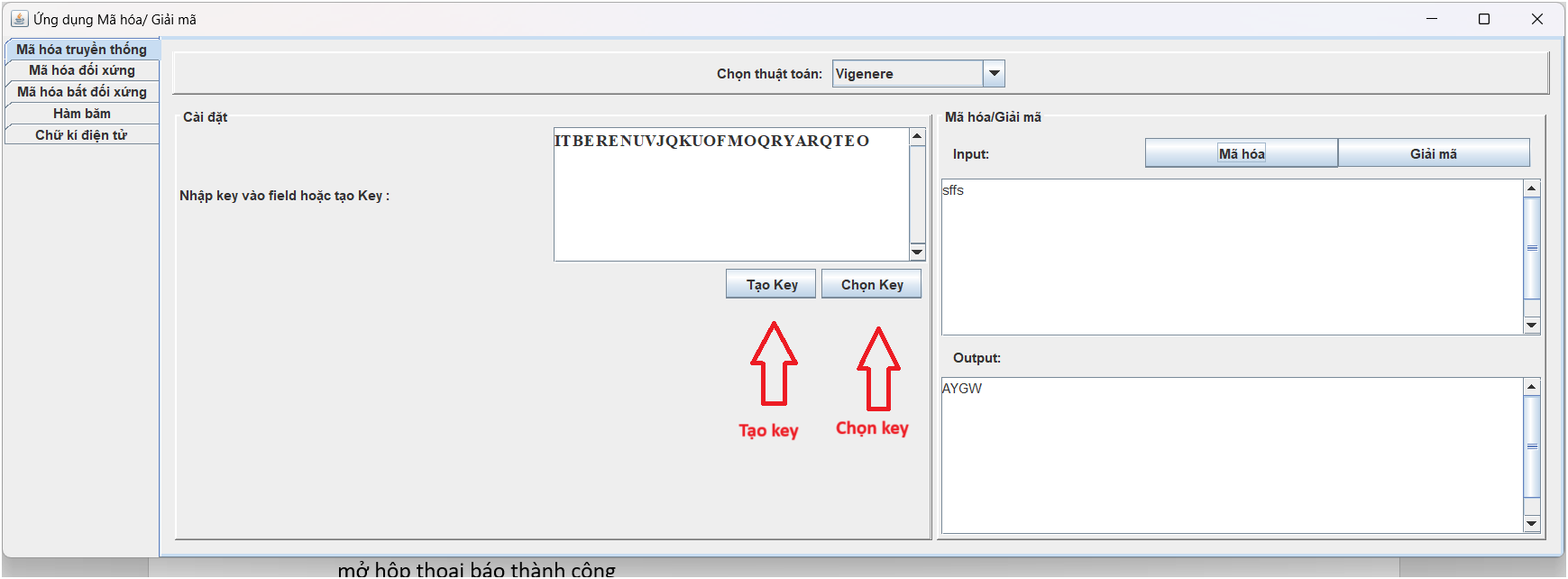


#### 3.1.5 Vigenere:

Bước 1: người dùng chọn tab mã hóa truyền thống, sau đó chọn thuật toán Vigenere

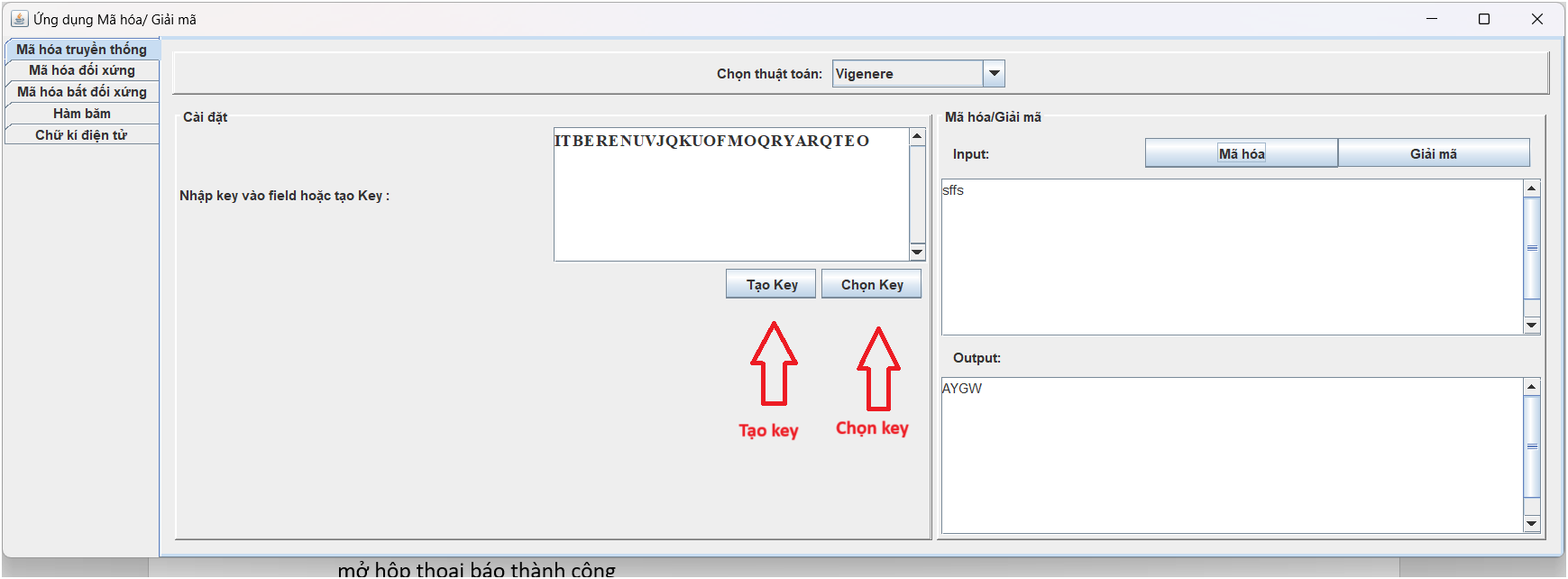


Bước 2: Thuật toán Vigenere nhận vào 1 chuỗi có dộ dài 26 kí nên nếu người dùng đã có key thì người dùng nhập độ dài ma trận key vào ô nhập kích thước, và giá trị ma trận , nếu chưa có thì nhấn nút “tạo key” phần mềm sẽ tự động tạo ra key phù hợp với giải thuật

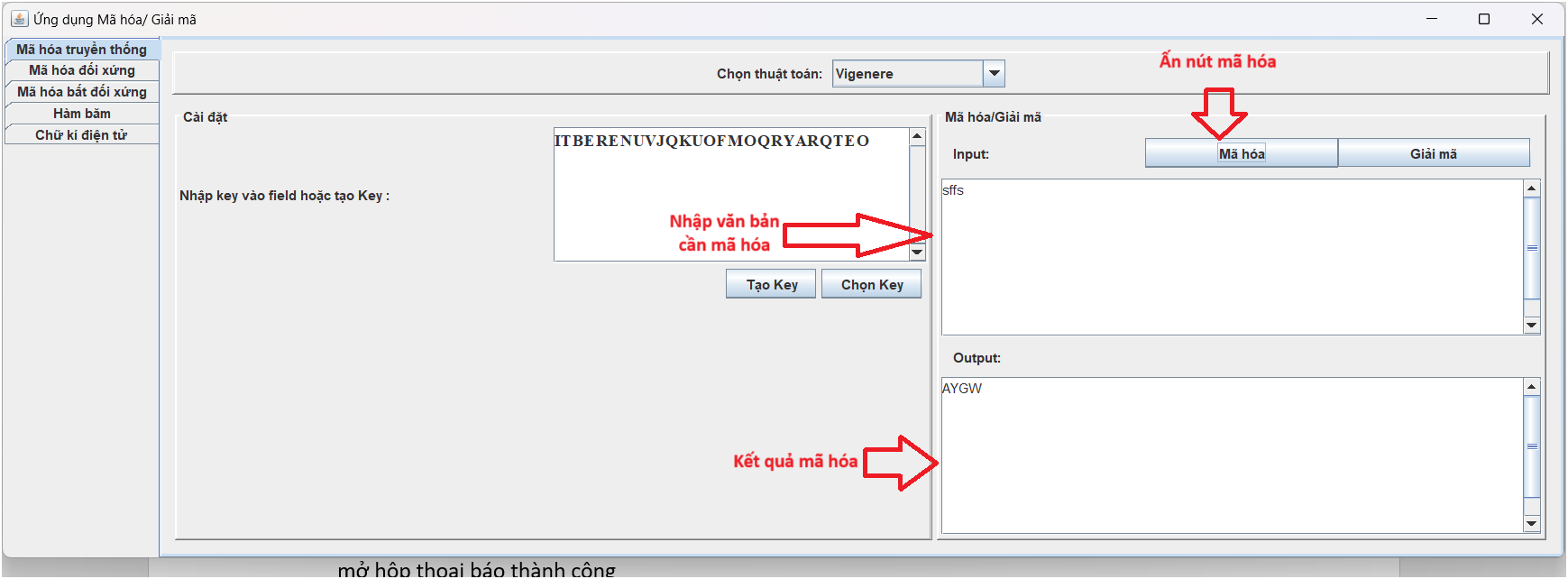


\*Lưu ý: Phần mềm hiện tãi chỉ hỗ trợ nhập key là chuỗi 26 kí tự nên nếu key của không phải đáp ứng được thì không sử dụng được

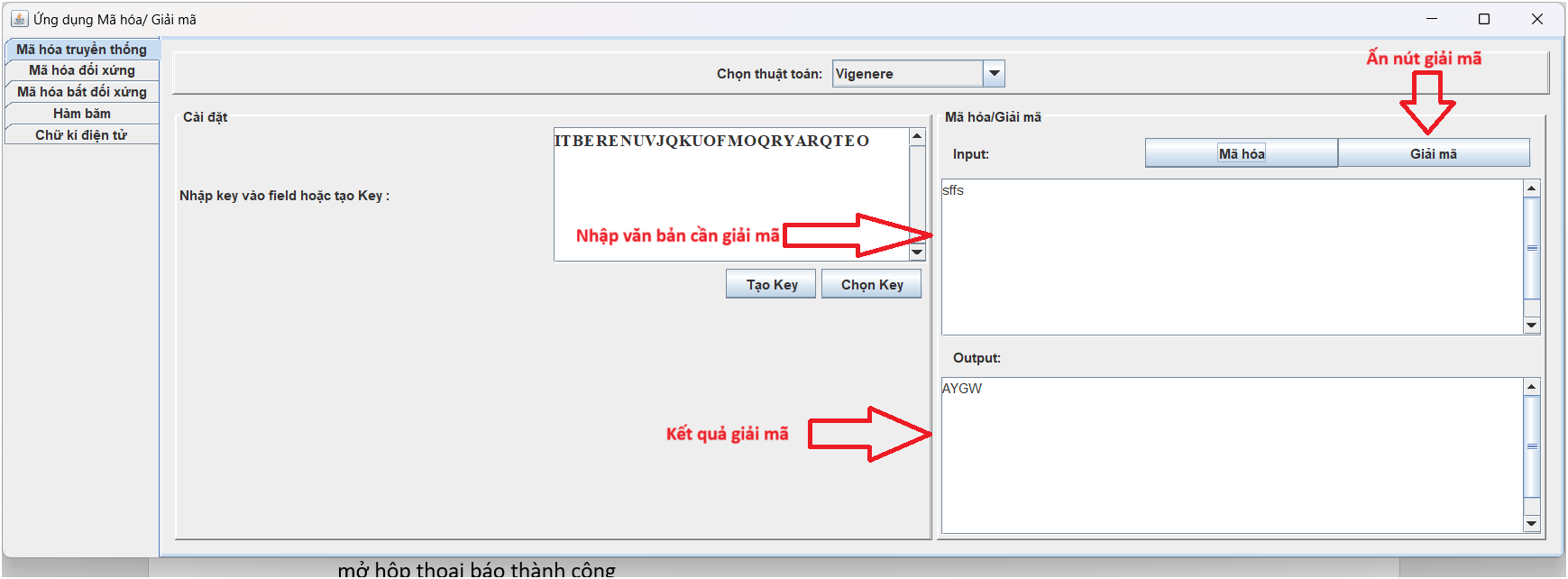
Bước 3: sau khi nhập hoạc tạo key , người dùng cần nhấn “ chọn key” để phần mềm biết quá trình nhập key đã xong. Tiến hành mã hóa/ giải mã.



Bước 3.1: sau khi nhập key , người dùng muốn mã hóa thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



Bước 3.2: sau khi nhập key , người dùng muốn giải mã thì cần nhập văn bản cần mã hóa , sau đó nhấn mã hóa, kết quả dưới định dạng base 64 sẽ được trả ra ở ô output và phần mềm mở hộp thoại báo thành công



1 số lỗi khi sử dụng

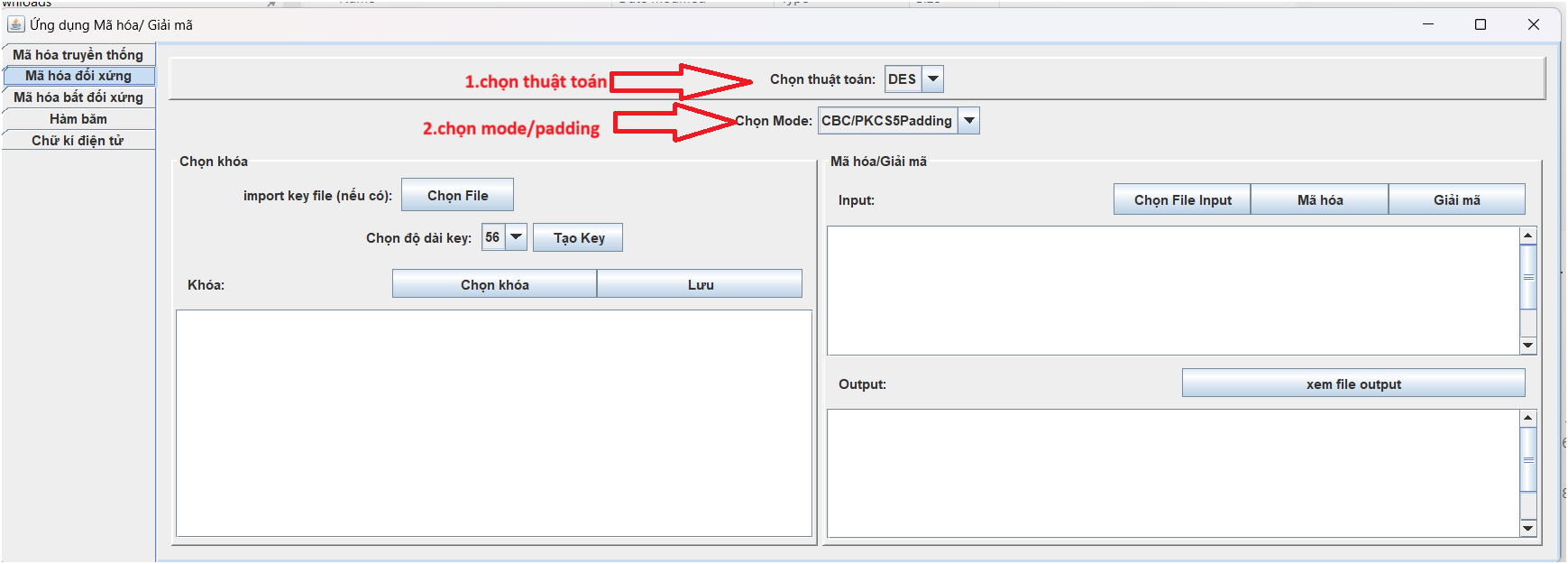
Nhập key là chữ

Key chưa được chọn

### 3.2 Hướng dẫn sử dụng mã hóa đối xứng

#### 3.2.1 DES:

Bước 1 : Chọn tab mã hóa đối xứng , chọn vào thuật toán Des

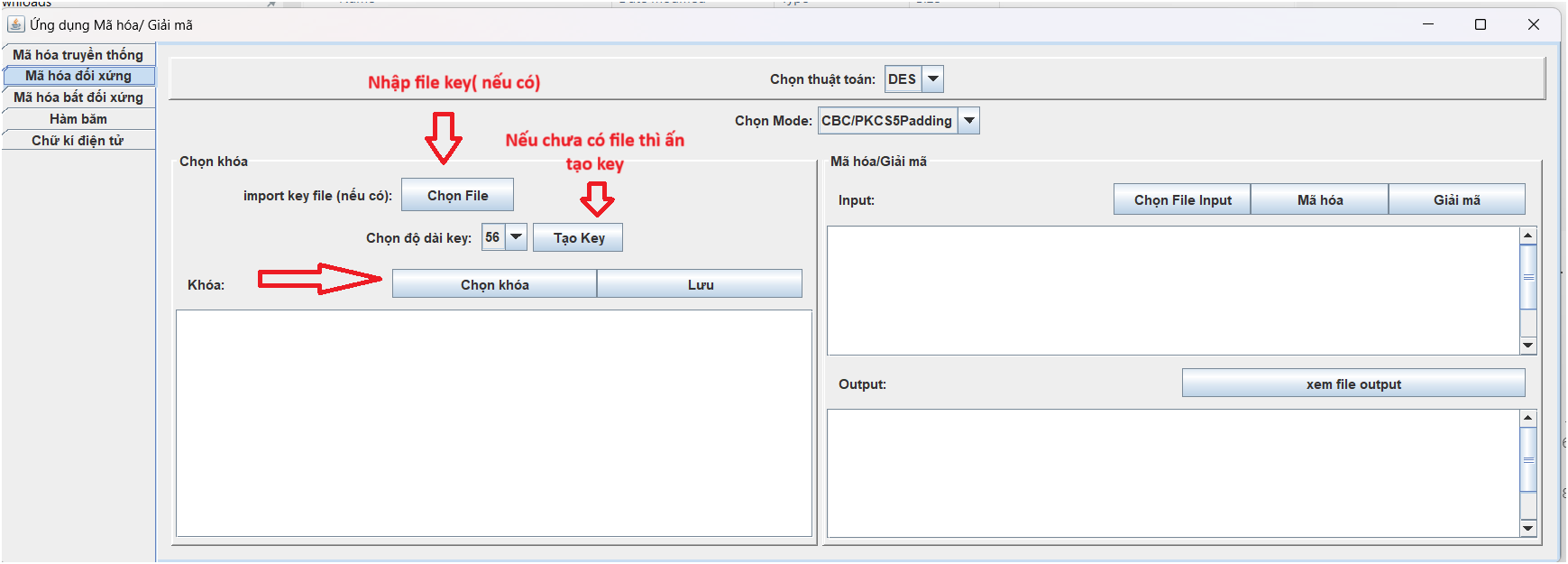


Bước 2: nếu có file key thì chọn nút chọn file , nếu người dùng không có key dạng file thì có thể nhập .Lưu ý key chỉ nhận dưới dạng base 64 nên cần nhập cho chính xác. NẾu người dùng không có key sẵn thì nhấn tạo key sẽ tạo tự động 1 key phù hợp với giải thuật

Bước 3: chọn độ dài key

Bước 4: Ấn” chọn khóa” để lưu lại key

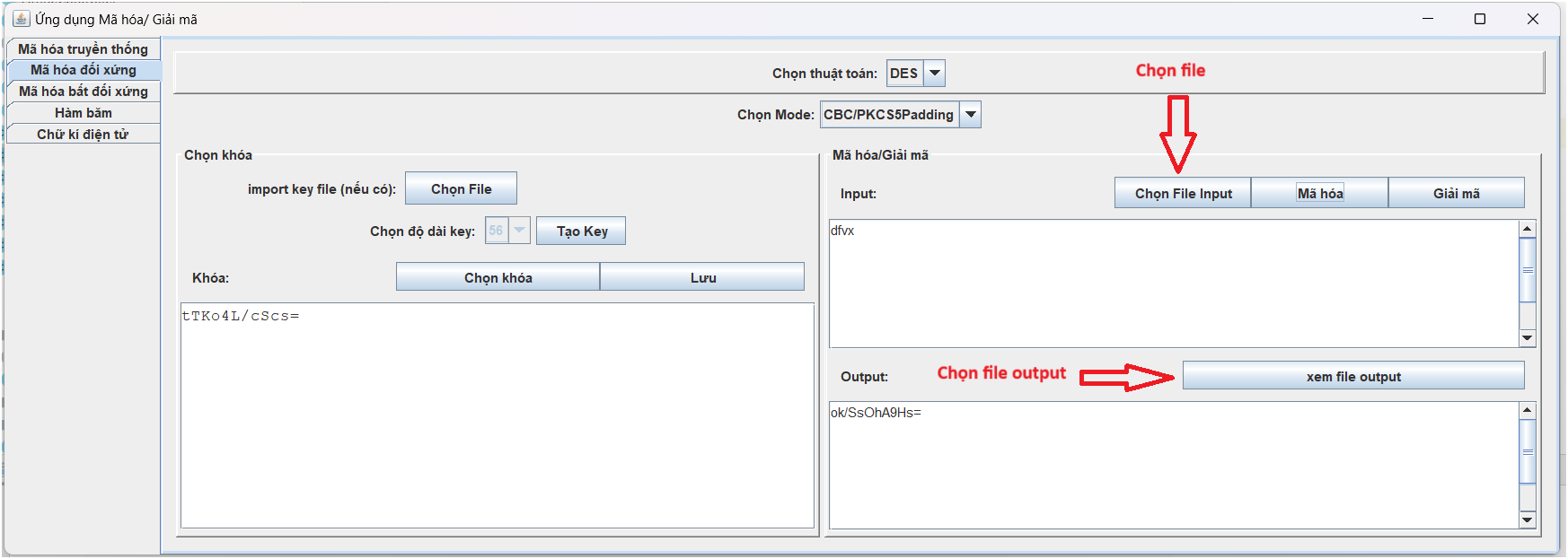
Bước 4: chọn mode/padding.



\*Lưu ý với 1 số padding như PKCS7Padding sẽ không chạy được, do qui định của provider bouncy cattle yêu cầu certificate ssl nên sẽ không thể thực hiện trong phiên bản này của phần mềm.

Bước 5: Mã hóa/ giải mã:

* Với file:Nếu người dùng muốn làm việc với file thì chọn nút “chọn file input”, khi đó phần mềm sẽ không nhận giá trị nhập trong ô nhập key nữa. Khi đã có file thì nhấn mã hóa/giải mã kết quả sẽ lưu cùng thư mục với file input, người dùng muốn xem kết quả thì nhấn xem file output, phần mềm sẽ mở file explorer và trỏ tới file mong muốn



* Với văn bản:

Nếu người dùng muốn mã hóa văn bản thì không nhập file, nhập trực tiếp vào ô nhập input, sau đó nhấn mã hóa/giải mã , kết quả sẽ có ở phần nhập chỗ output

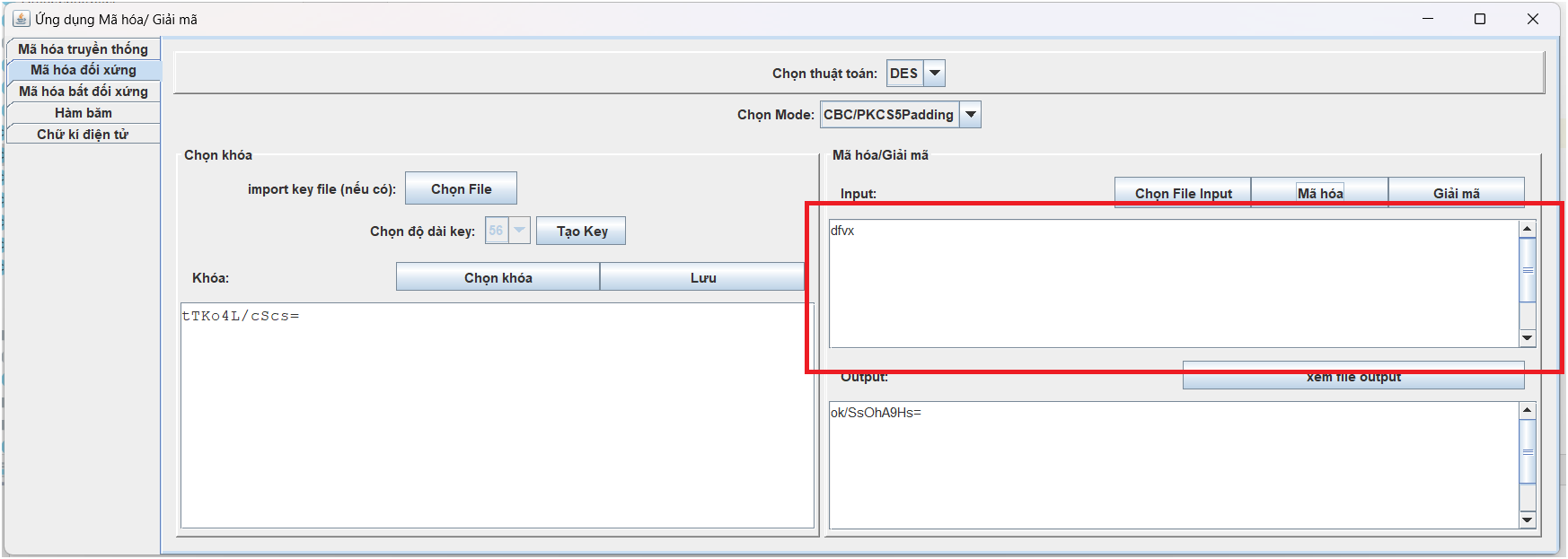


Figure ô nhập văn bản cần mã hóa/ giải mã

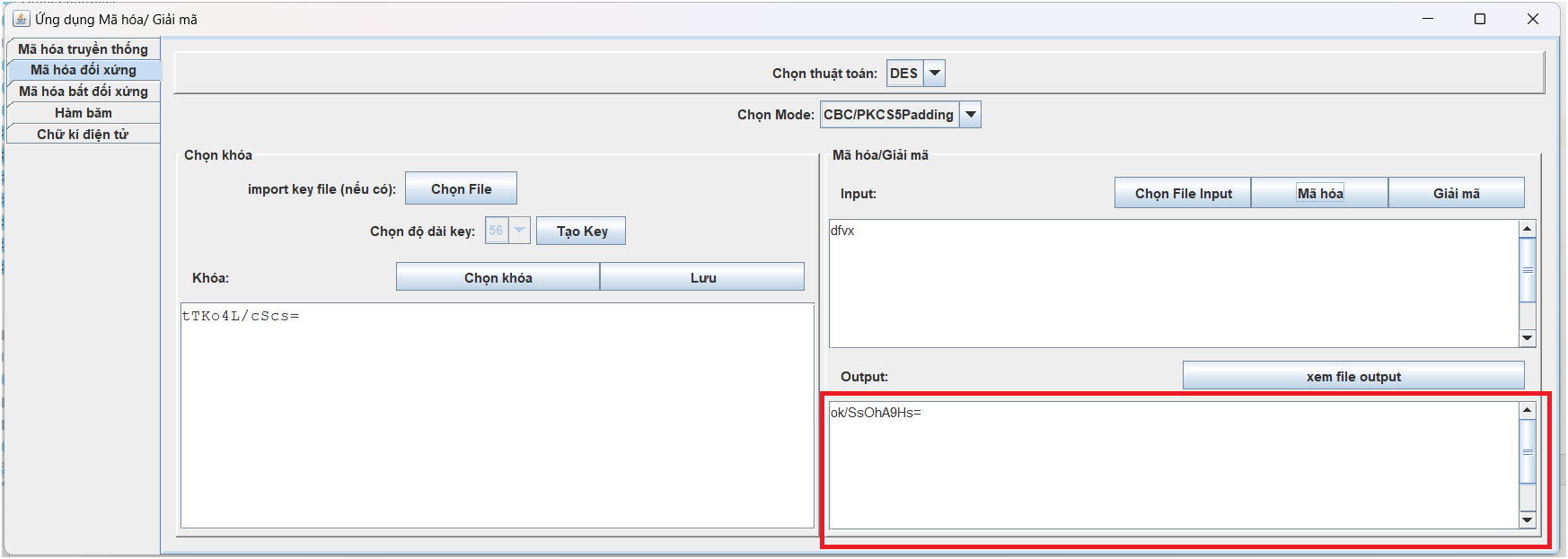


Figure đây là nơi hiển thị kết quả văn bản mã hóa/giải mã

\*Lưu ý: viêc mã hóa file văn bản như docs, txt,… sẽ mã hóa như 1 file chứ không phải là lấy nội dung file đi mã hóa rồi dán lại , nên nếu bạn muốn mã hóa nội dung những văn bản này thì cần mở file lấy nội dung và làm như đang mã hóa văn bản

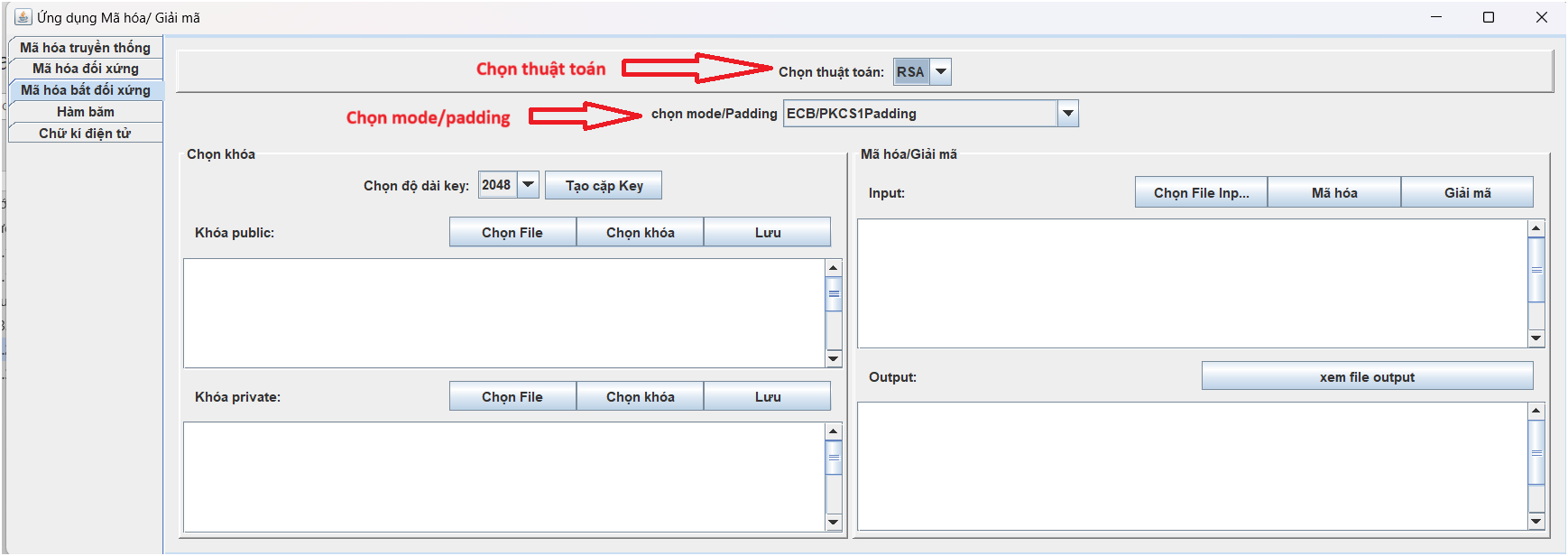
3.2.2. AES (tương tự DES)

\*Lưu ý: tương tự DES , với 1 số padding như PKCS7Padding sẽ không chạy được, do qui định của provider bouncy cattle yêu cầu certificate ssl nên sẽ không thể thực hiện trong phiên bản này của phần mềm.

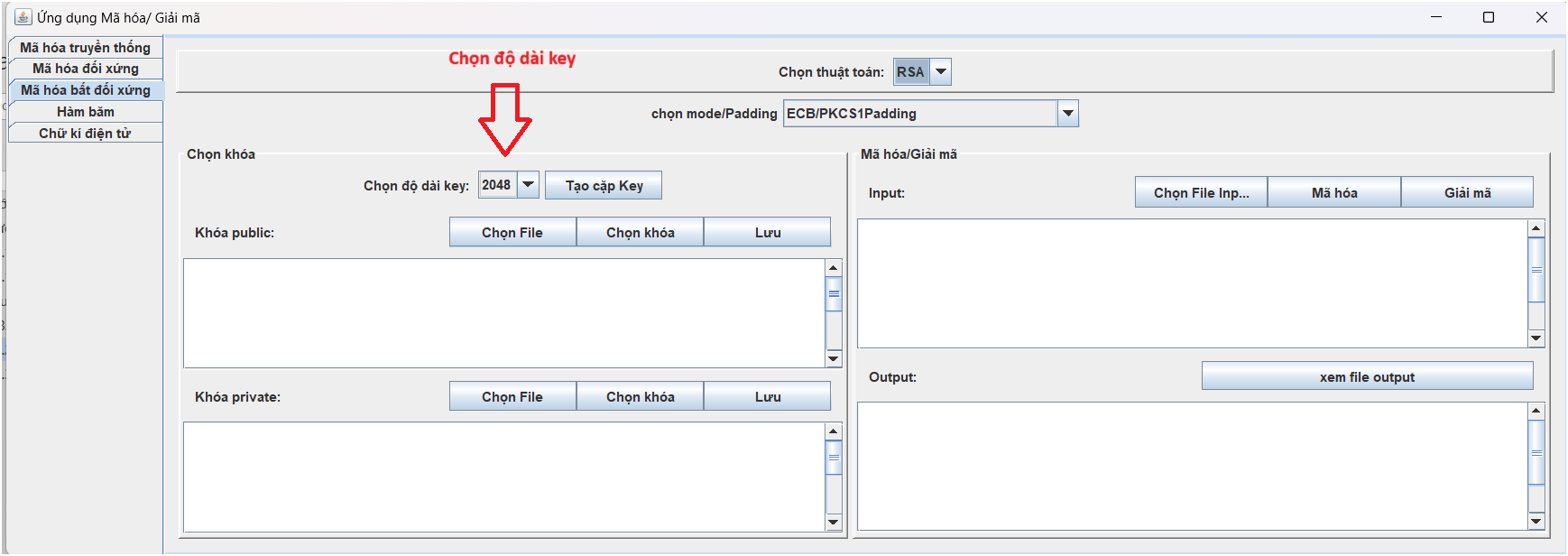
### 3.3 Hướng dẫn sử dụng mã hóa bất đối xứng :

#### 3.3.1 RSA:

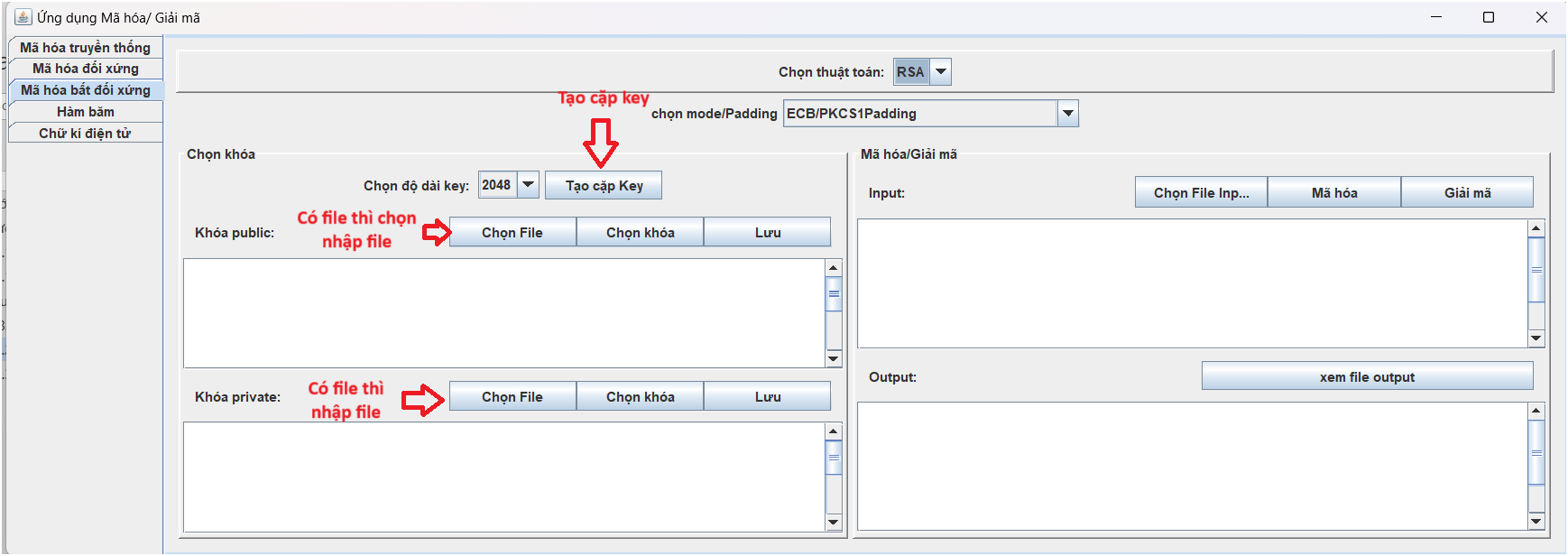
Bước 1: Chọn padding bạn muốn



Bước 2: chọn độ dài của key



Bước 3: Nếu bạn có file key (yêu cầu 1 cặp) thì ấn nút “Chọn file” để import vào. Còn nếu chưa có file key thì ấn tạo cặp khóa



Bước 4: ấn “chọn khóa” public và private

Bước 5:

Với file : Nếu người dùng muốn mã hóa/ giải mã file thì ấn nút “chọn file” , phần mềm sẽ mở cửa sổ chọn file, người dùng chọn phải muốn làm việc rồi ấn mã hóa/ giải mã , kết quả sẽ có ở cùng thư mục với file chọn làm viêc , người dùng muốn xem ấn nút “xem file output” , phần mềm sẽ mở cửa số explorer trỏ tới file mới tạo

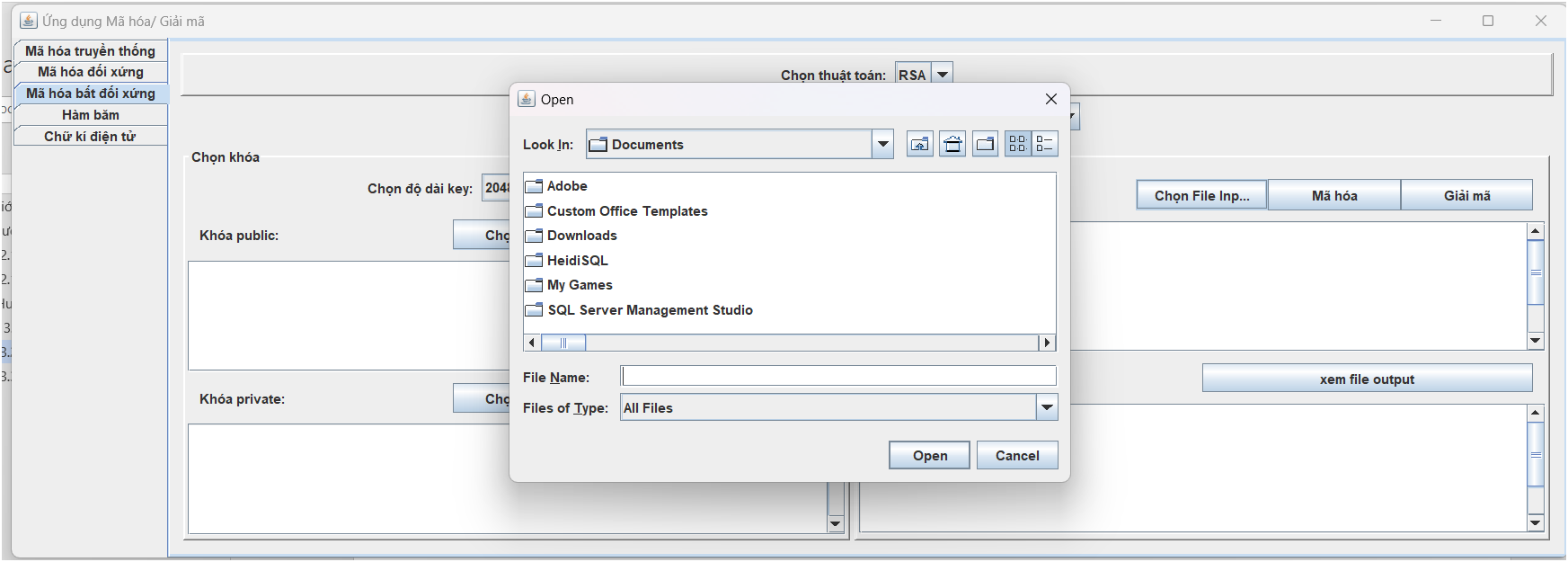
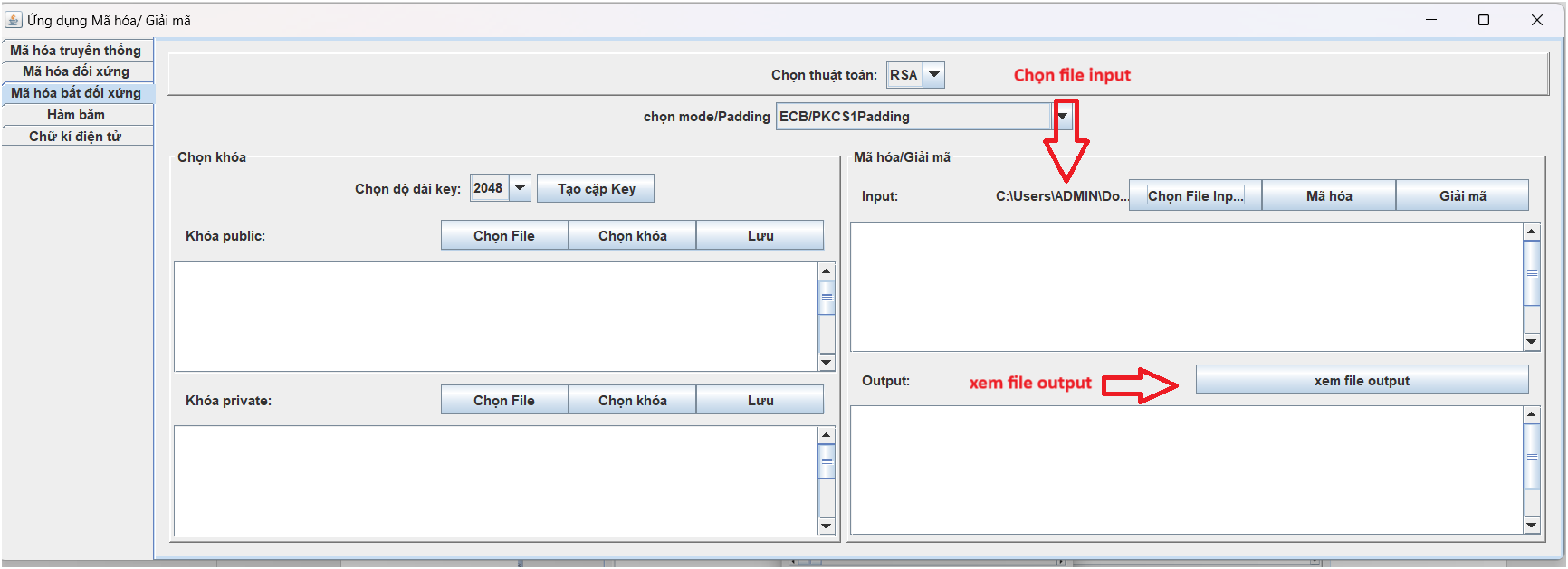
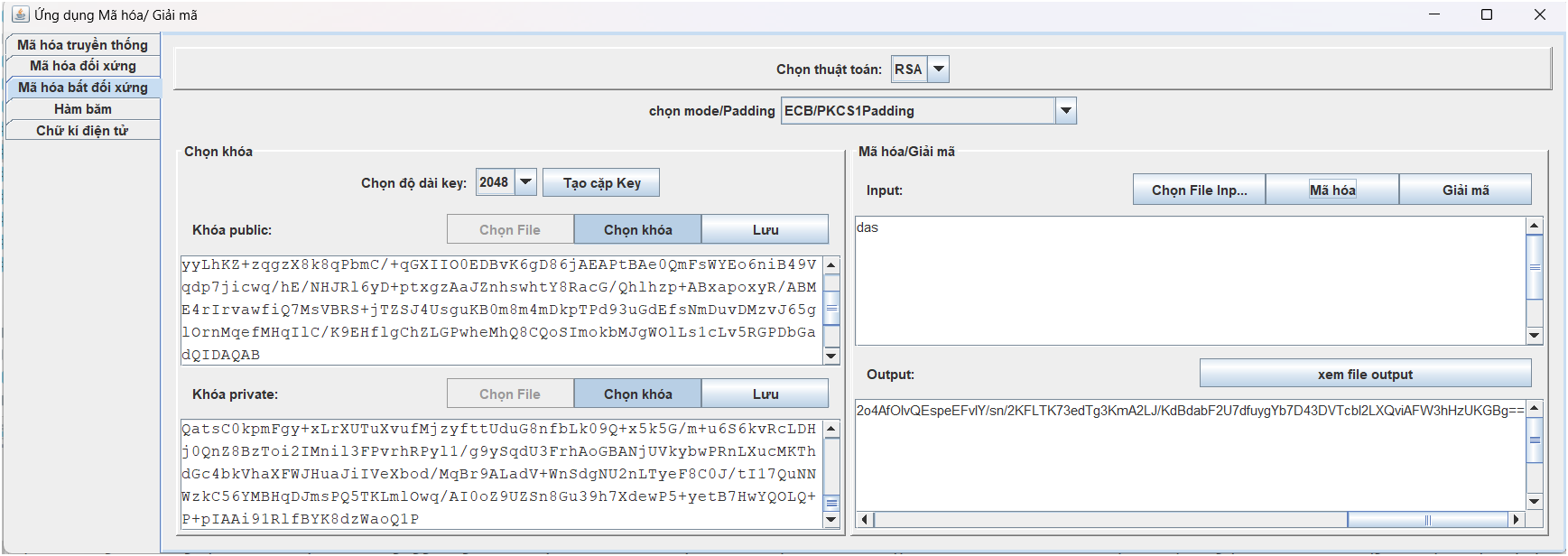


Figure ấn vào nút chọn file, 1 cửa số xuất hiện cho chọn file



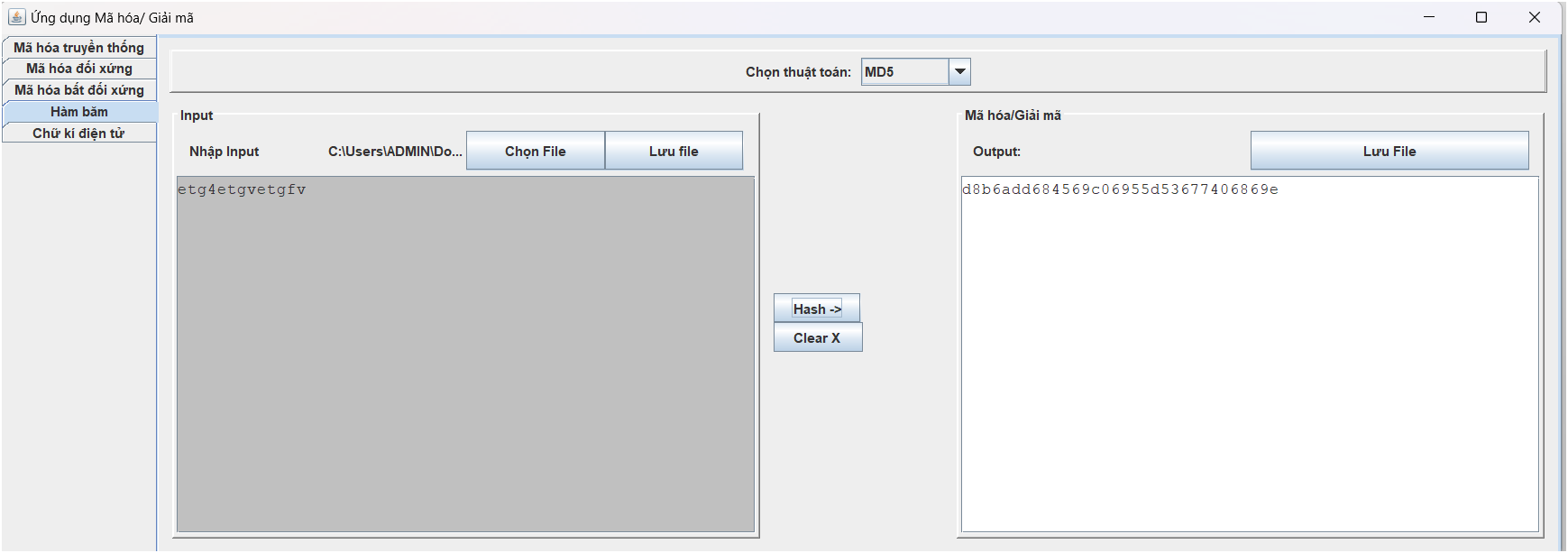
Với văn bản: Nếu người dùng muốn mã hóa/ giải mã văn bản thì nhập vào ô , người dùng chọn phải muốn làm việc rồi ấn mã hóa/ giải mã , kết quả hiện ở mục output.



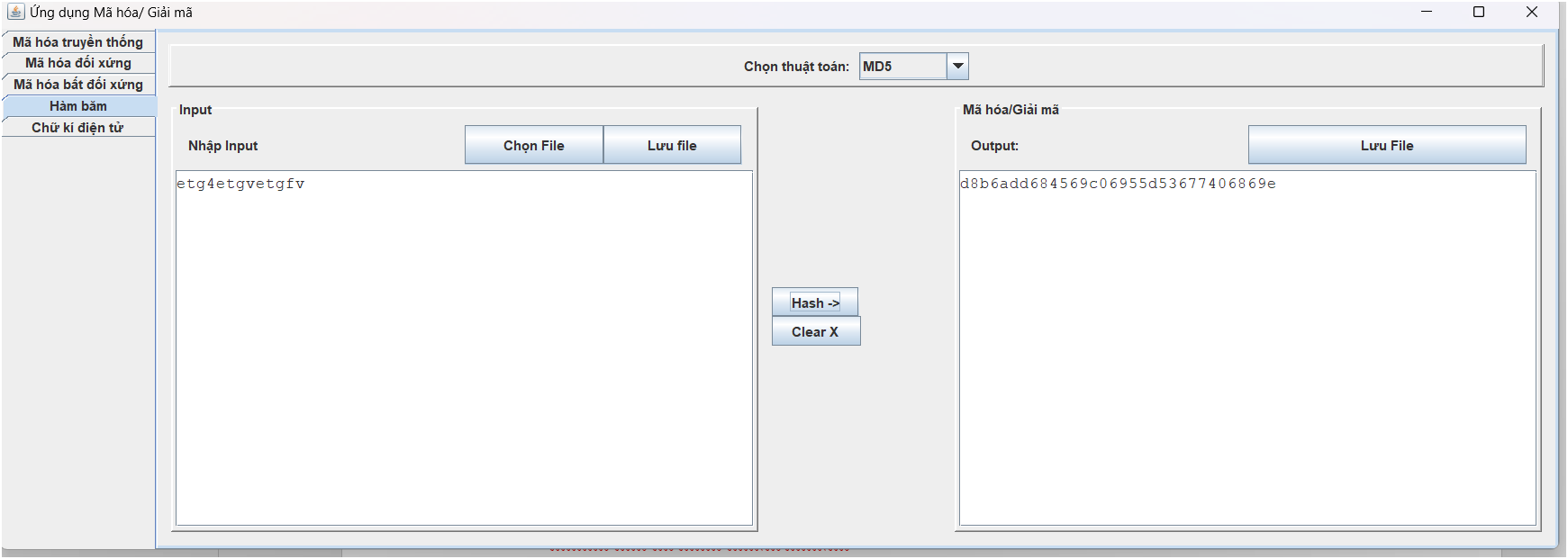
### 3.4 Hướng dẫn sử dụng hàm băm (hướng dẫn chung cho MD5, SHA,…)

Bước 1: người dùng ấn chọn tab hàm băm sau đó ấn chọn giải thuật mong muốn

Bước 2: Nếu người dùng muốn làm việc với file thì ấn chọn file để import file, sau đó ấn hash (mã hóa) , kết quả sẽ có ở ô output ,đó mã sau khi băm file, bạn có thể lưu lại dưới dạng file



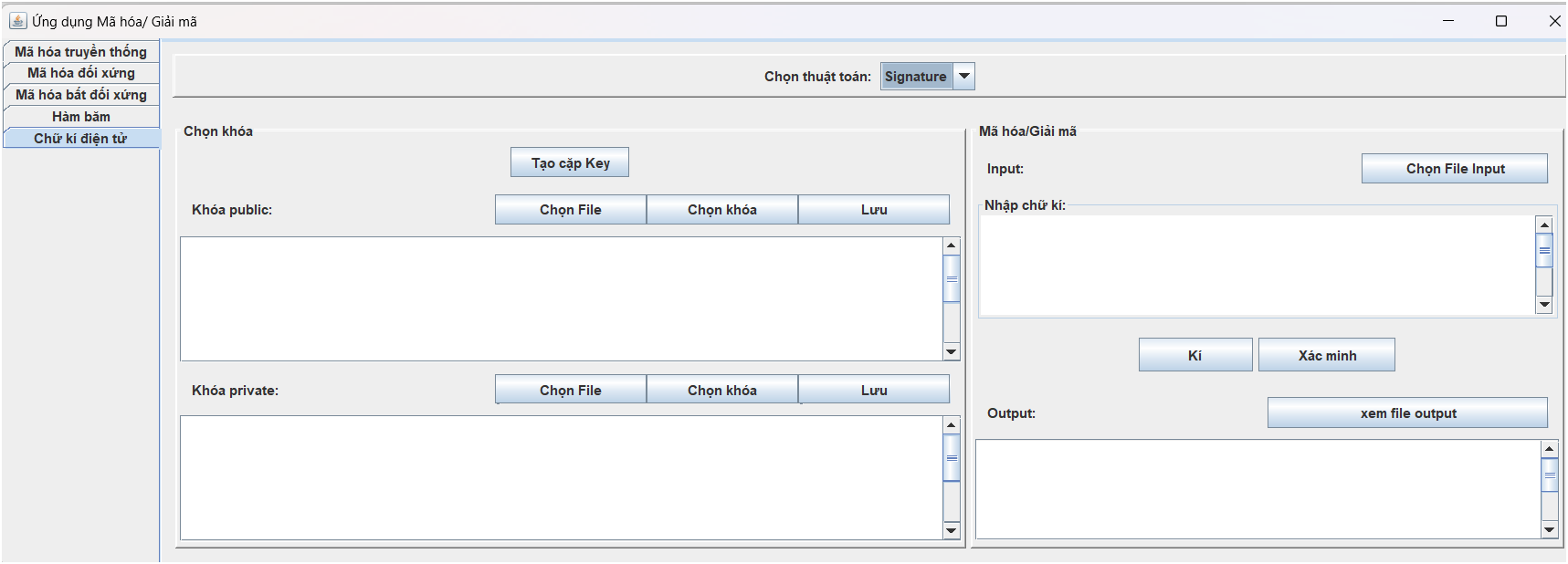
Nếu người dùng muốn làm việc với văn bản thì nhập vào ô nhập văn bản sau đó thực hiện tương tự như làm việc với file



### 3.5 Hướng dẫn sử dụng chữ kí điện tử:

Bước 1 người dùng ấn chọn tab chữ kí điện tử

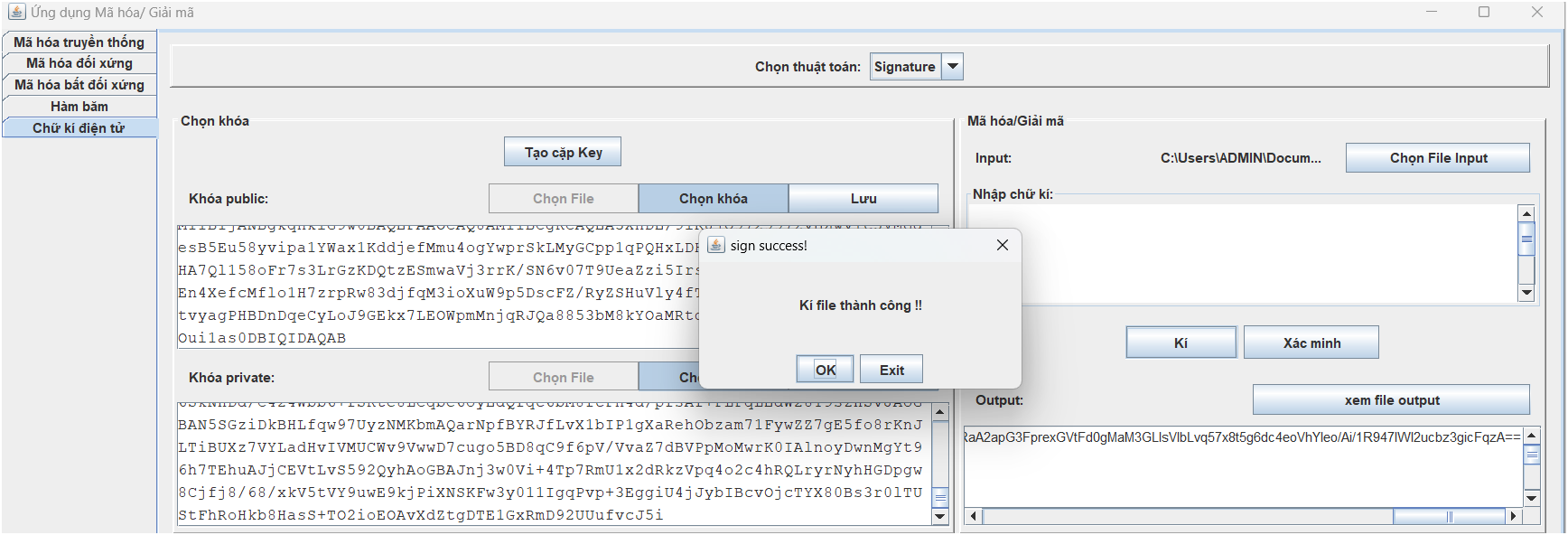
Bước 2: Nếu người dùng đã có public/ private key thì ấn chọn file rồi ấn “chọn khóa tương ứng”



Bước 3:

Người dùng muốn kí file:

Người dùng tiến hành ấn nút “chọn file input” bên phải, để nhập vào file cần kí,sau đó nhấn kí file, chữ kí sẽ xuất hiện ở ô nhập output, file đã kí sẽ xuất hiện ở chỗ “xem file output” với đuôi mở rộng signature.sig



Người dùng muốn xác mình chữ kí:

Người dùng nhập file đã kí vào nút “chọn file input” để import file, sau đó nhập chữ kí vào ô nhập chữ kí dưới định dạng base64 , sau đó nhấn “xác minh” , 1 hộp thoại xuất hiện để báo kết quả xác minh

