I. Giới thiệu ứng dụng

MidTerm ATBMHTTT - Pblues: Ứng dụng hỗ trợ mã hóa, giải mã, băm và chữ ký điện tử cho tệp hoặc văn bản.

1. Mã hóa và giải mã (Encryption and Decryption)

- Thuật toán mã hóa đối xứng cơ bản (Basic Symmetric Encryption Algorithms)

  Bao gồm các thuật toán: *Shift Cipher, Substitution Cipher, Affine Cipher, Vigenere Cipher, Permutation Cipher, Hill Cipher*
- Thuật toán mã hóa đối xứng hiện đại (Modern Symmetric Encryption Algorithms)
  - Các thuật toán được Java support

    Bao gồm các thuật toán: *DES, DESede, AES, Blowfish, RC4, ChaCha20*
  - Các thuật toán khác từ thư viện Bouncy Castle

    Bao gồm các thuật toán: *Twofish, Serpent, CAST, Camellia*
- Thuật toán bất đối xứng (Asymmetric Encryption Algorithms)

  Thuật toán *RSA* (chỉ mã hóa text)

  Thuật toán *RSA kết hợp AES* (mã hóa text và file)

2. Băm văn bản hoặc tập tin (Hash)

- Các thuật toán băm được Java support:

  MD2, MD5, SHA-1, SHA-224, SHA-256, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512
- Các thuật toán băm khác từ thư viện Bouncy Castle

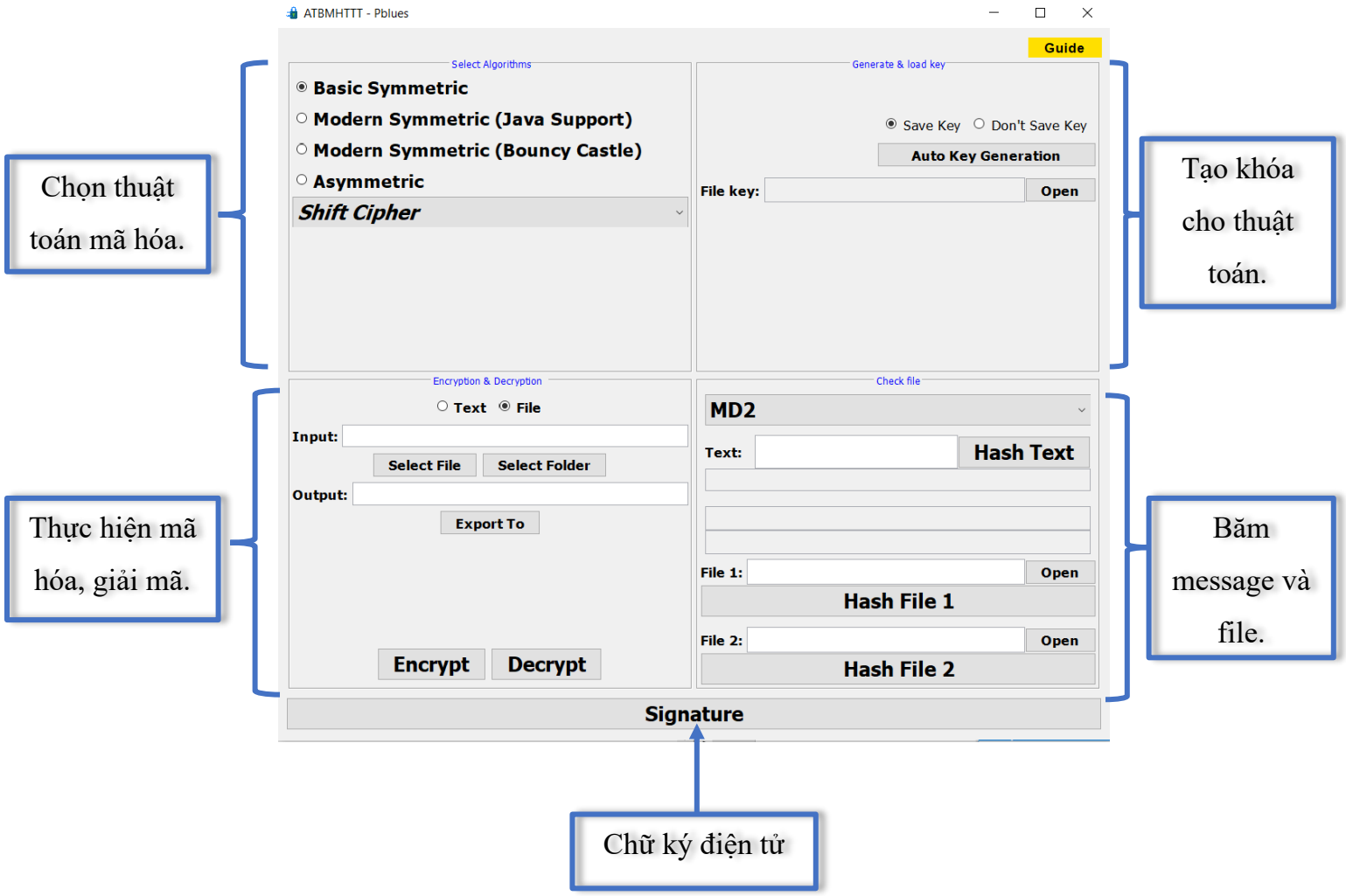
  MD4, Whirlpool, Tiger, GOST3411, RIPEMD160

3. Ứng dụng chữ ký điện tử (Signature)

Thuật toán: *DSA + SHA1PRNG* và provider: *SUN*

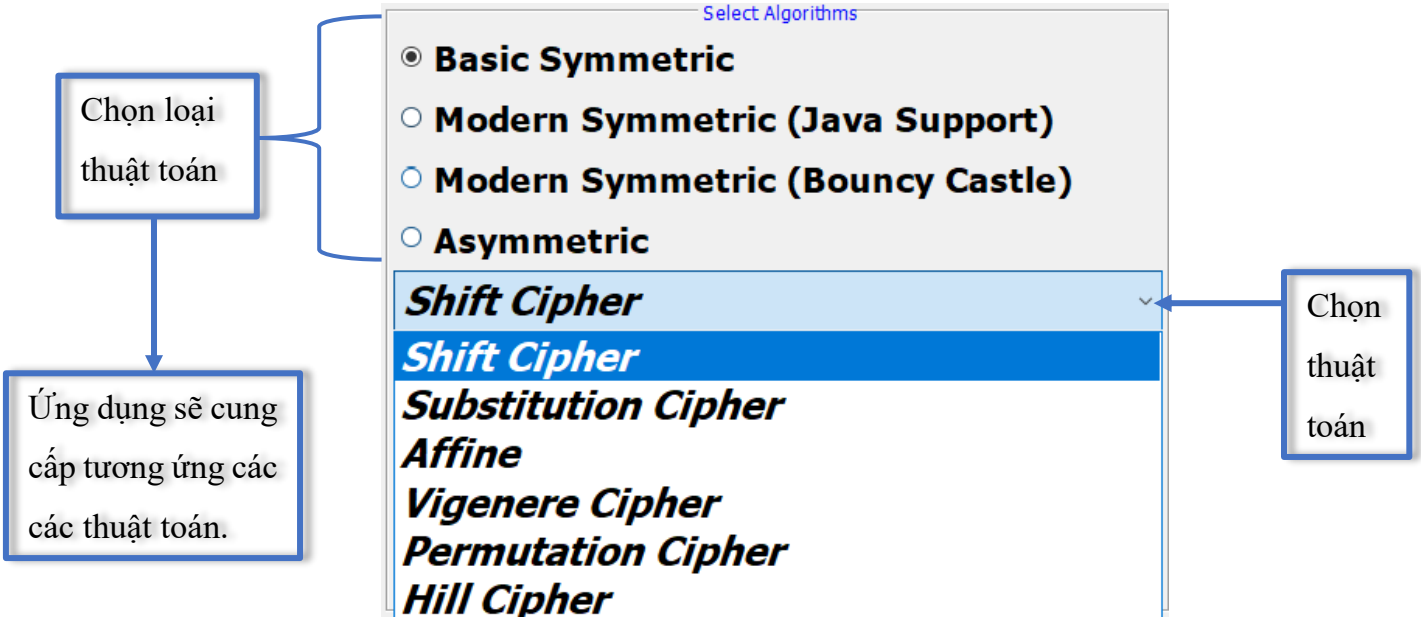
II. Hướng dẫn sử dụng

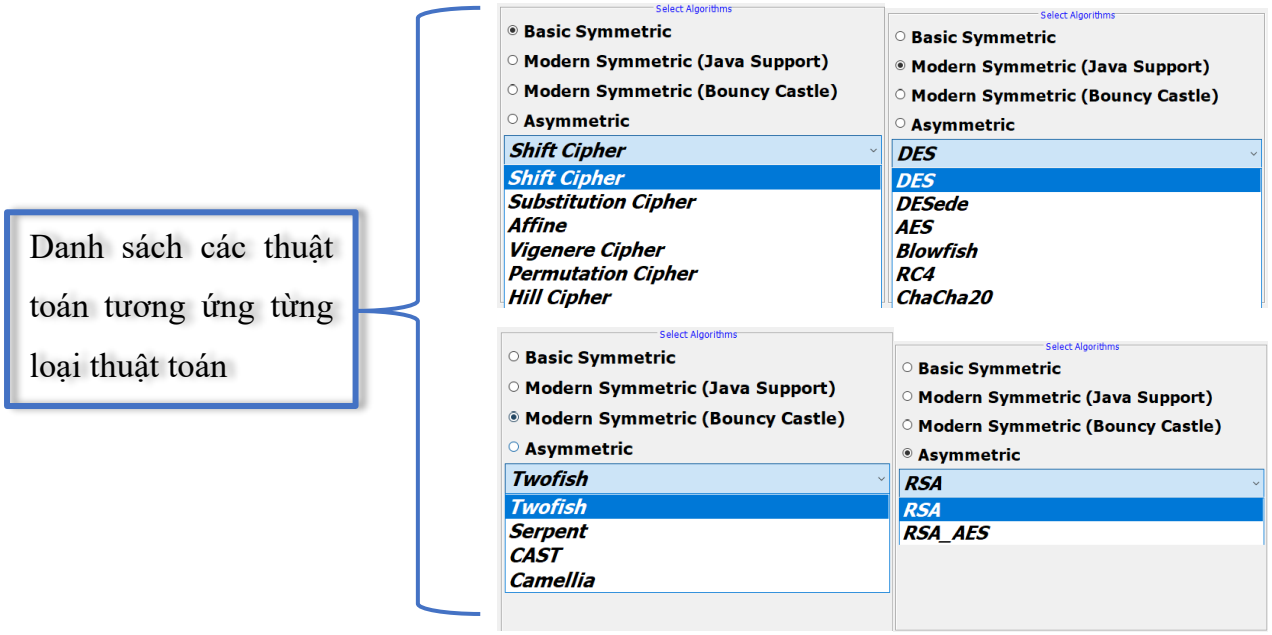
1. Tổng quan giao diện



2. Mã hóa, giải mã

❖ Trong Select Algorithms: Chọn thuật toán mã hóa

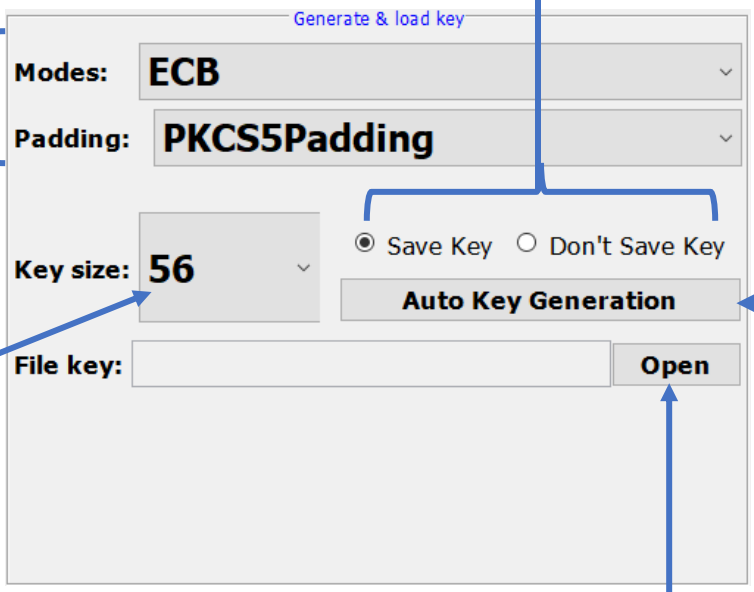




❖ Trong Generate & Load Key: Tạo khóa cho thuật toán

Để nâng cao chất lượng mã hóa thì tương ứng từng thuật toán, ứng dụng đưa ra các tùy chọn các chế độ mã hóa (Mode) và tương ứng từng thuật toán và chế độ mã hóa thì có các tùy chọn Padding.

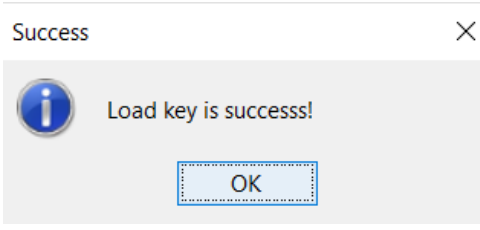
Mặc định ứng dụng sẽ chọn sẵn lựa chọn lưu khóa thành file "Save Key" để nhằm mục đích giải mã sau này. Nếu không muốn lưu khóa, hoàn toàn có thể chọn "Don't Save Key".



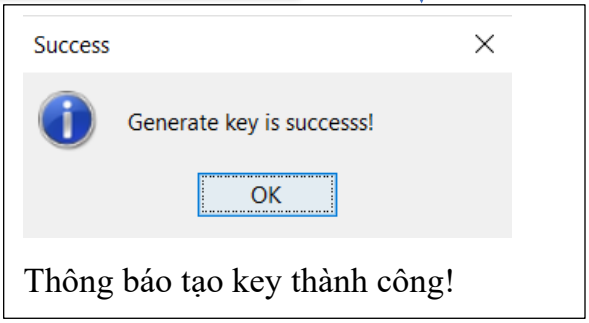
Với lựa chọn thuật toán thuộc các loại thuật toán Modern Symmetric và Asymmetric, việc lựa chọn Key Size là điều cần thiết cho việc khởi tạo thuật toán đó.

Lựa chọn "Auto Key Generation" phù hợp khi người dùng chưa sở hữu khóa nào hoặc muốn một khóa hoàn toàn mới cho thuật toán đã chọn.

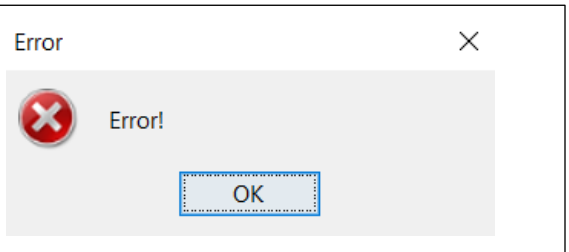
Lựa chọn tải khoa lên "Open" phù hợp khi người dùng đã có khóa cho thuật toán. Nếu hợp lý, ứng dụng sẽ dựa vào file khóa đó tính toán và lấy Key Size tương ứng (đối với thuật toán Modern Symmetric và Asymmetric) và tiến hành load khóa



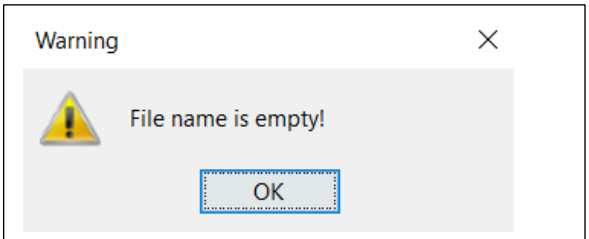
Thông báo load file key thành công!



Thông báo tạo key thành công!

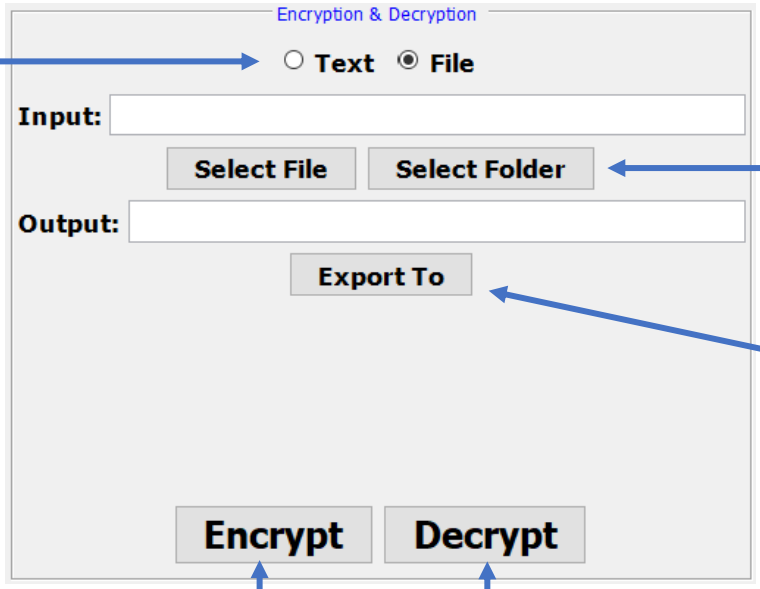


Thông báo lỗi khi file key không đúng!



Thông báo file name rỗng khi lưu key!

❖ Trong Encryption & Decryption: Thực hiện mã hóa và giải mã



Lựa chọn mã hóa đối với văn bản (text) hoặc tập tin (file).

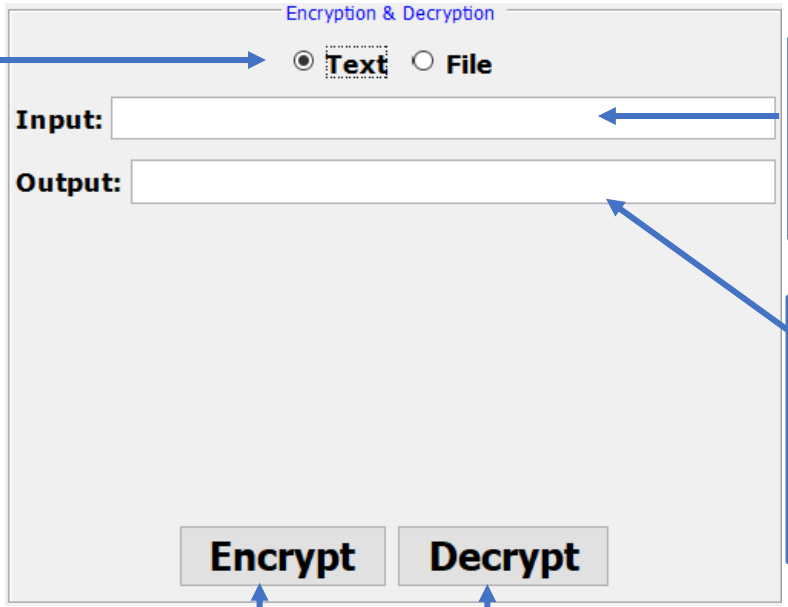
Vì thuật toán RSA không hỗ trợ với mã hóa file ra thì mặc định ứng dụng bắt đầu với lựa chọn "File".

Chọn file hoặc folder để mã hóa hoặc giải mã.

Chọn nơi lưu kết quả file hoặc folder đã mã hóa hoặc giải mã.

Thực hiện mã hóa.

Thực hiện giải mã.



Lựa chọn mã hóa đối với văn bản (text).

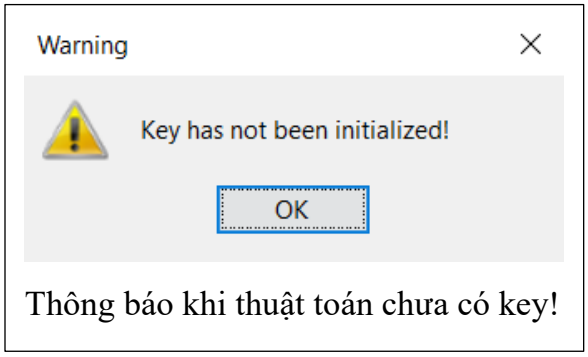
Nhập đoạn văn bản để mã hóa hoặc giải mã.

Hiển thị kết quả mã hóa hoặc giải mã.

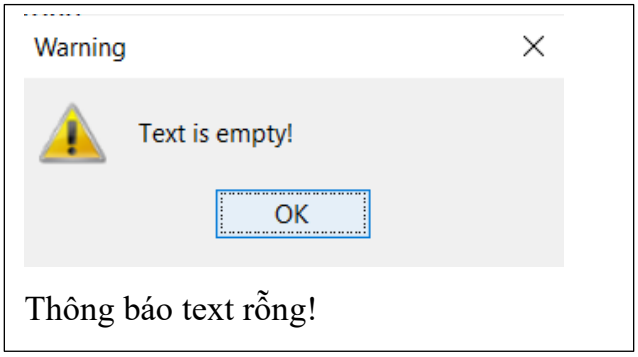
Thực hiện mã hóa.

Thực hiện giải mã.

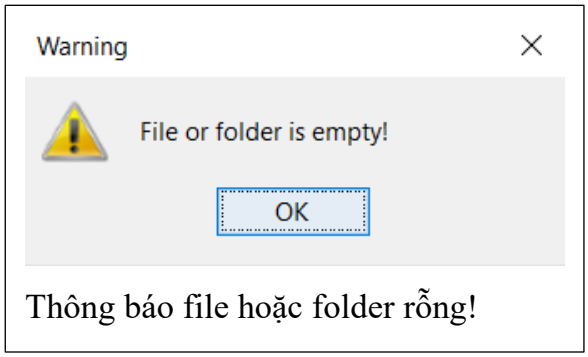
Việc thực hiện không đúng thao tác hoặc thông báo kết quả, ứng dụng sẽ đưa ra các thông báo để nhận biết:



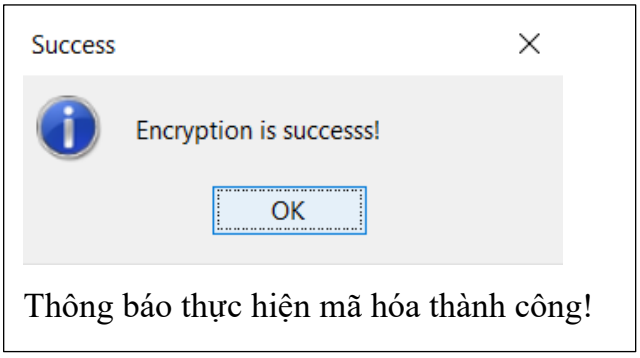
Thông báo khi thuật toán chưa có key!



Thông báo text rỗng!



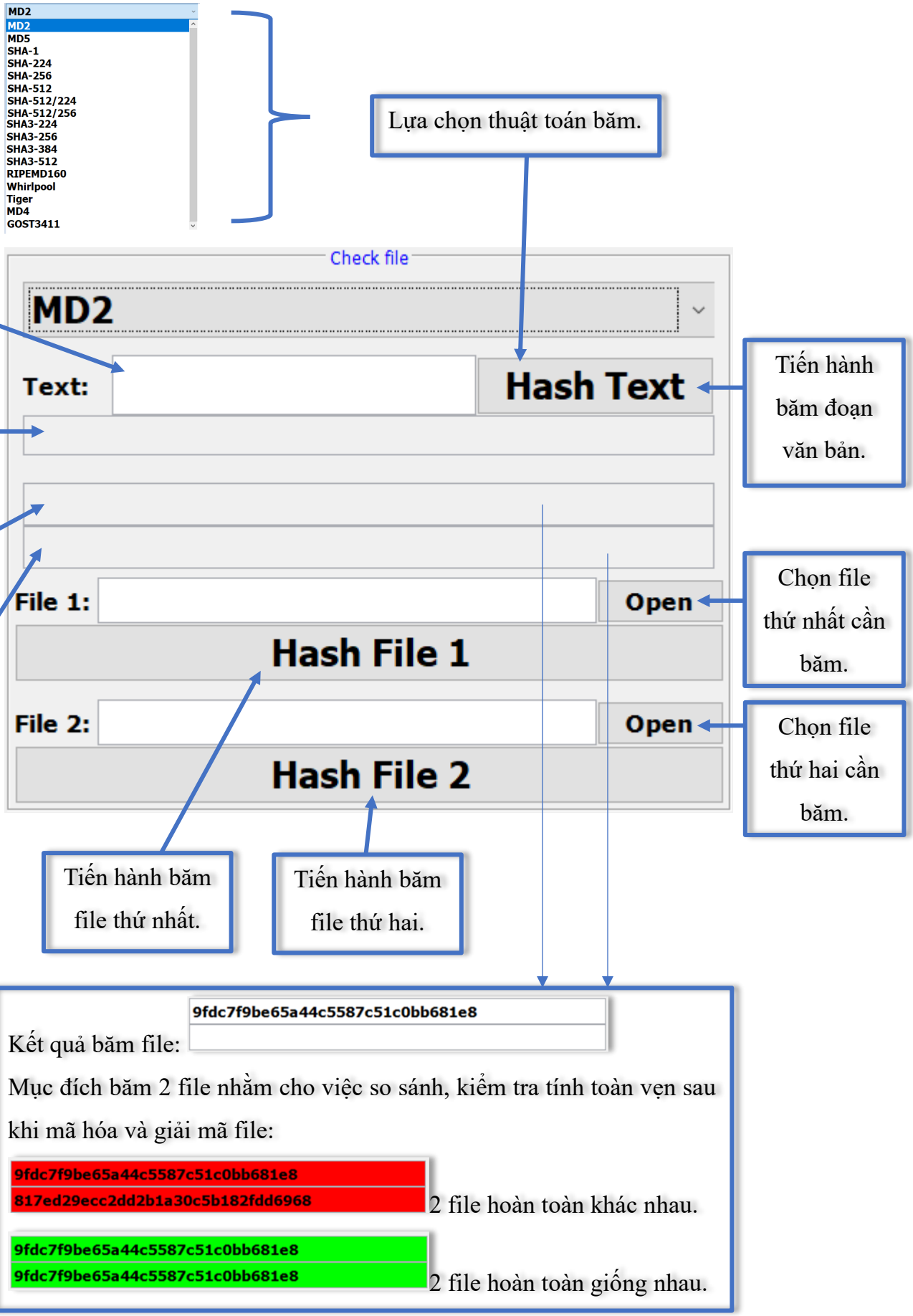
Thông báo file hoặc folder rỗng!



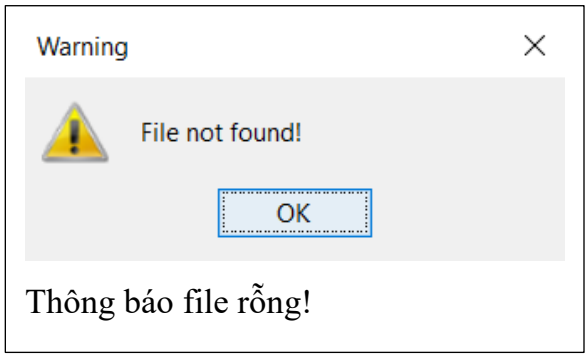
Thông báo thực hiện mã hóa thành công!

Thông báo lỗi khi thực hiện!

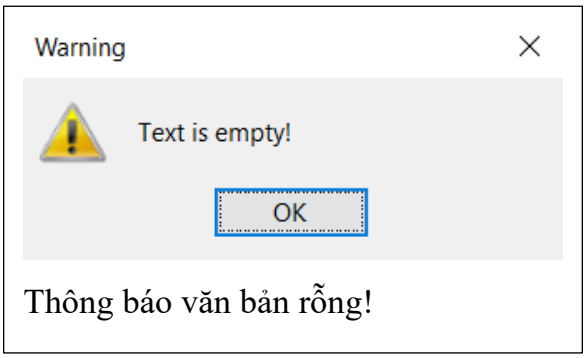
3. Hash


MD2
MD2
MD5
SHA-1
SHA-224
SHA-256
SHA-512
SHA-512/224
SHA-512/256
SHA3-224
SHA3-256
SHA3-384
SHA3-512
RIPEMD160
Whirlpool
Tiger
MD4
GOST3411
Lựa chọn thuật toán băm.
Check file
MD2
Text:
Hash Text
Nhập đoạn văn bản cần băm.
Tiến hành băm đoạn văn bản.
Kết quả băm đoạn văn bản.
Kết quả băm file thứ nhất.
Kết quả băm file thứ hai.
File 1:
Open
Hash File 1
File 2:
Open
Hash File 2
Chọn file thứ nhất cần băm.
Chọn file thứ hai cần băm.
Tiến hành băm file thứ nhất.
Tiến hành băm file thứ hai.
Kết quả băm file:
9fdc7f9be65a44c5587c51c0bb681e8
Mục đích băm 2 file nhằm cho việc so sánh, kiểm tra tính toàn vẹn sau khi mã hóa và giải mã file:
9fdc7f9be65a44c5587c51c0bb681e8
817ed29ecc2dd2b1a30c5b182fdd6968
2 file hoàn toàn khác nhau.
9fdc7f9be65a44c5587c51c0bb681e8
9fdc7f9be65a44c5587c51c0bb681e8
2 file hoàn toàn giống nhau.

Việc thực hiện không đúng thao tác hoặc thông báo kết quả, ứng dụng sẽ đưa ra các thông báo để nhận biết:



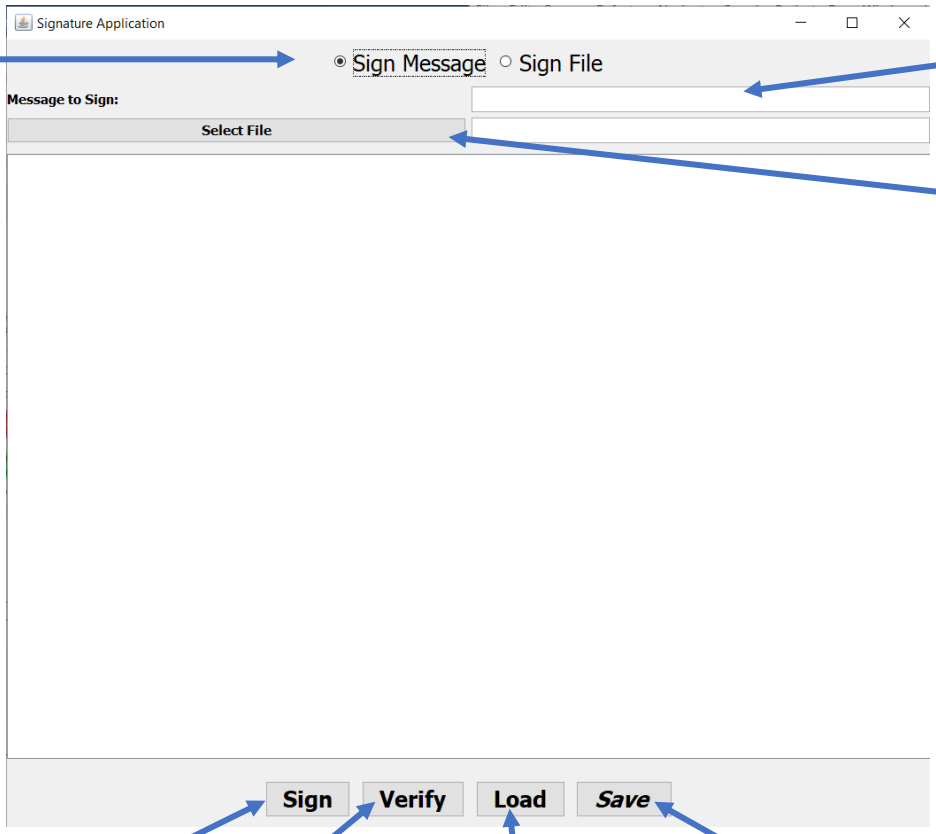
Thông báo file rỗng!



Thông báo văn bản rỗng!

4. Chữ ký điện tử

Tùy chọn sign với Message hoặc File.



Nhập Message.

Mở File.

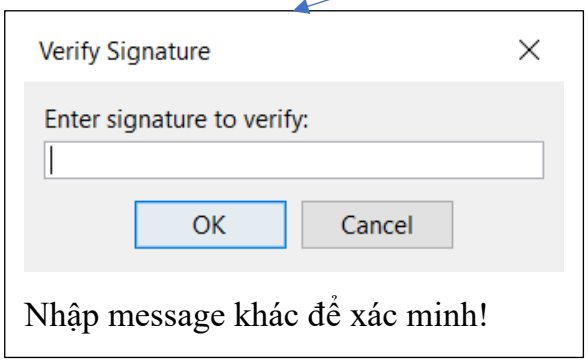
Nơi hiển thị kết quả.

Tiến hành Sign.

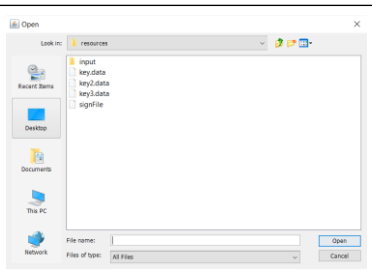
Tiến hành Verify.

Nhấn "Load" để cung cấp 1 file chứa kết quả sign trước đó.

Sau khi sign và có kết quả. Nhấn "Save" để lưu dữ liệu cần thiết nhằm việc xác minh (verify) mà không cần file hay message gốc.

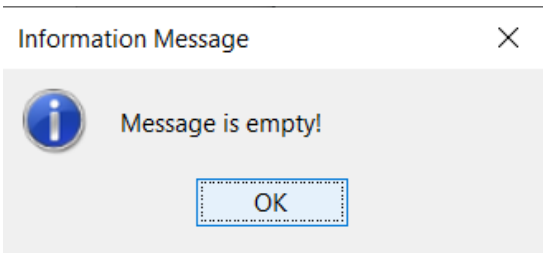


Nhập message khác để xác minh!

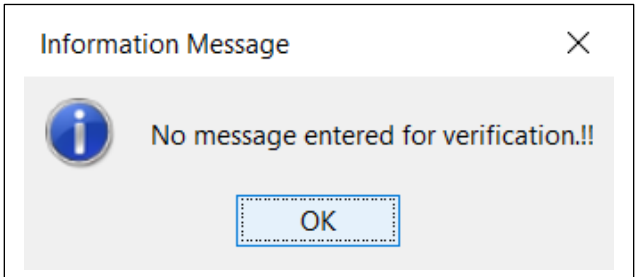


Chọn file khác để xác minh!

Việc thực hiện không đúng thao tác hoặc thông báo kết quả, ứng dụng sẽ đưa ra các thông báo để nhận biết:

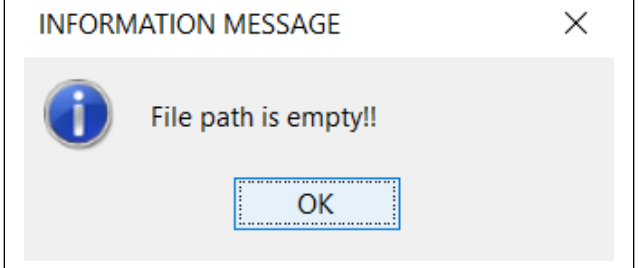


Message rỗng khi tiến hành sign!

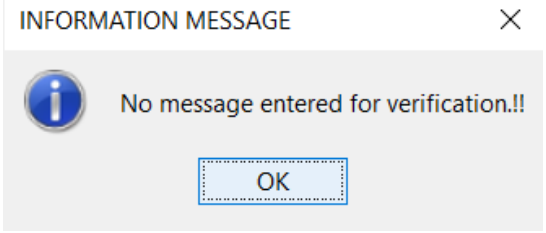


Chưa có kết quả trước khi verify!

Chưa có kết quả trước khi lưu thành file!

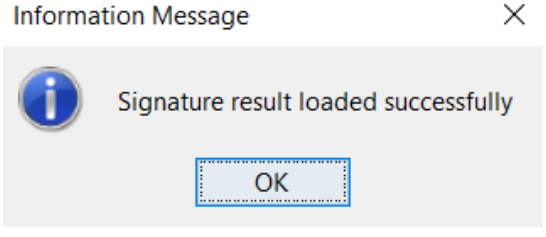


Thông báo file rỗng khi tiến hành sign!

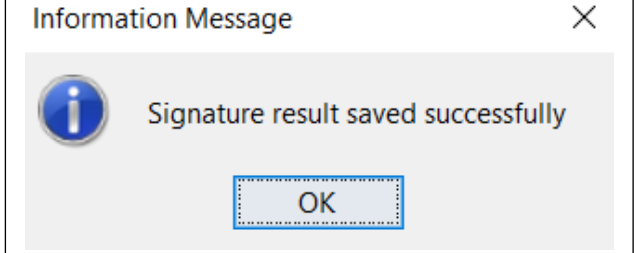


Thông báo kết quả sign rỗng khi tiến hành verify!

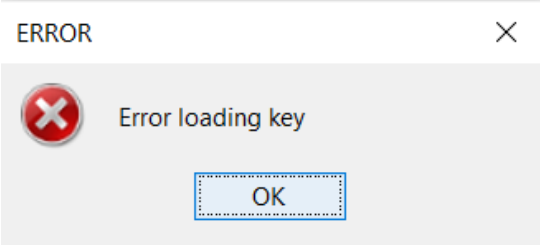
Thông báo mesage rỗng trong khi tiến hành verify!



Thông báo load signature từ file thành công!



Thông báo lưu signature thành file thành công!



Thông báo lỗi khi load kết quả sign từ file!

III. Link cài đặt ứng dụng trên môi trường Microsoft Windows

en_de_hash_signature