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

**KHOA CÔNG NGHỆ THÔNG TIN**

**Logo

Description automatically generated**

**Tài liệu hướng dẫn sử dụng**

**MÔN: AN TOÀN VÀ BẢO MẬT THÔNG TIN**

ĐỀ TÀI:

ỨNG DỤNG MÃ HÓA THÔNG TIN

Giảng viên hướng dẫn: Phan Đình Long.

Sinh viên: 18130258 – Nguyễn Ngọc Trung

TP. Hồ Chí Minh, tháng 12 năm 2021

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

**KHOA CÔNG NGHỆ THÔNG TIN**

**Logo

Description automatically generated**

**Tài liệu hướng dẫn sử dụng**

**MÔN: AN TOÀN VÀ BẢO MẬT THÔNG TIN**

ĐỀ TÀI:

ỨNG DỤNG MÃ HÓA THÔNG TIN

Giảng viên hướng dẫn: Phan Đình Long.

Sinh viên: 18130258 – Nguyễn Ngọc Trung

TP. Hồ Chí Minh, tháng 12 năm 2021

Nhân xét của giáo viên:

Mục lục

[I. Link demo: 4](#_Toc91490468)

[II. Giới thiệu về ứng dụng. 4](#_Toc91490469)

[1. Chức năng. 4](#_Toc91490470)

[2. Giao diện. 4](#_Toc91490471)

[2.1. Giao diện bắt đầu: 4](#_Toc91490472)

[2.2. Giao diện Symmetric (Màn hình chính). 5](#_Toc91490473)

[2.3. Giao diện tạo key Symmetric. 5](#_Toc91490474)

[2.4. Giao diện Asymmetric. 6](#_Toc91490475)

[2.5. Giao diện tạo key Asymmetric. 6](#_Toc91490476)

[2.6. Giao diên Mix. 7](#_Toc91490477)

[2.7. Giao diện Hash. 7](#_Toc91490478)

[2.8. Giao diện PBE. 8](#_Toc91490479)

[2.9. Giao diện thông báo. 8](#_Toc91490480)

[III. Chi tiết chức năng. 9](#_Toc91490481)

[1. Symmetric và Symmetric key. 9](#_Toc91490482)

[2. Asymmetric và Asymmetric key. 9](#_Toc91490483)

[3. Mix. 9](#_Toc91490484)

[4. Hash. 9](#_Toc91490485)

[5. PBE. 9](#_Toc91490486)

[IV. Hướng dẫn sử dụng. 10](#_Toc91490487)

[1. Tải document và thoát. 10](#_Toc91490488)

[2. Truy cập vào chức năng tạo khóa. 10](#_Toc91490489)

[3. Chức năng tạo khóa Symmetric (đối xứng). 11](#_Toc91490490)

[4. Chức năng tạo khóa Asymmetric (bất đối xứng). 11](#_Toc91490491)

[5. Chức năng mã hóa, giải mã Text Symmetric (chuỗi hoặc text bằng phương pháp đối xứng). 12](#_Toc91490492)

[6. Chức năng mã hóa, giải mã File Symmetric (File bằng phương pháp đối xứng). 13](#_Toc91490493)

[7. Chức năng mã hóa Text Asymmetric (chuỗi hoặc đoạn văn bản bằng phương pháp bất đối xứng). 14](#_Toc91490494)

[8. Chức năng mã hóa Mix (Mã hóa File kết hợp giữa thuật toán RSA bất đối xứng và thuật toán đối xứng). 15](#_Toc91490495)

[9. Chức năng Hash Text (hàm băm). 16](#_Toc91490496)

[10. Chức năng Hash File. 17](#_Toc91490497)

[11. Chức năng PBE (sử dụng mật khẩu). 18](#_Toc91490498)

# Link demo:

<https://drive.google.com/file/d/1IL4BAXfKb6rz23knQ_YLhzv7gdnOXarw/view>?usp=sharing

# Giới thiệu về ứng dụng.

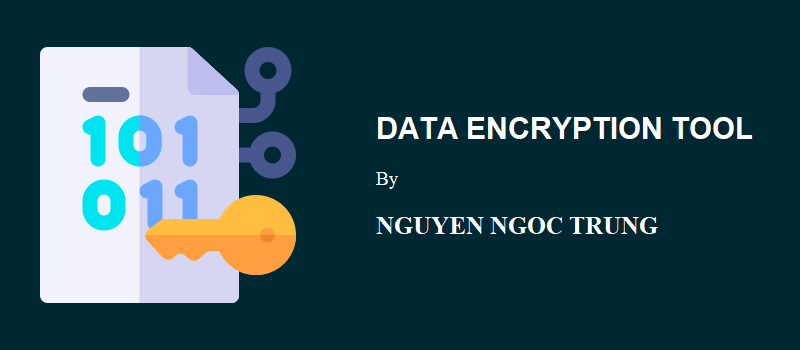
## Chức năng.

* Ứng dụng gồm có 5 chức năng chính (**Sử dụng JDK 1.8**):

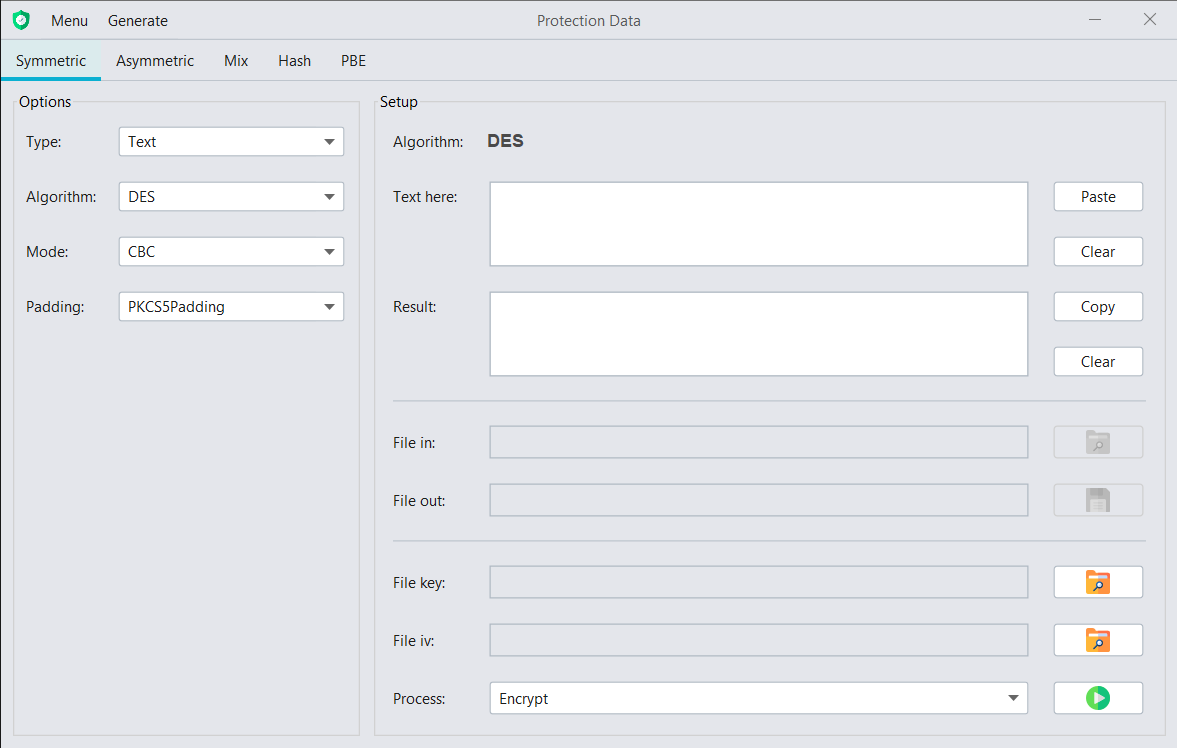
1. **Symmetric** (Mã hóa đối xứng), **Symmetric key** (Tạo khóa đối xứng).
2. **Asymmetric** (Mã hóa bất đối xứng), **Asymmetric key** (Tạo khóa bất đối xứng).
3. **Mix** (Mã hóa kết hợp).
4. **Hash** (Hàm băm).
5. **PBE** (Mã hóa mật khẩu).

## Giao diện.

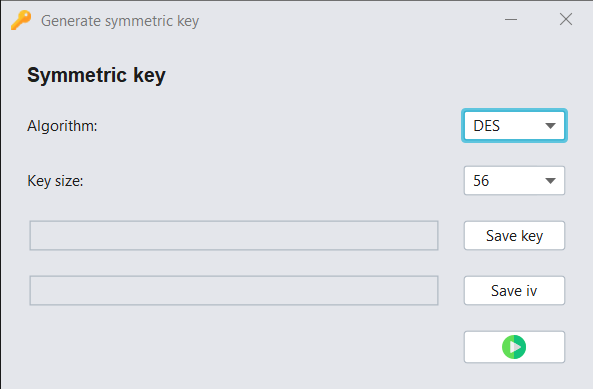
### Giao diện bắt đầu:



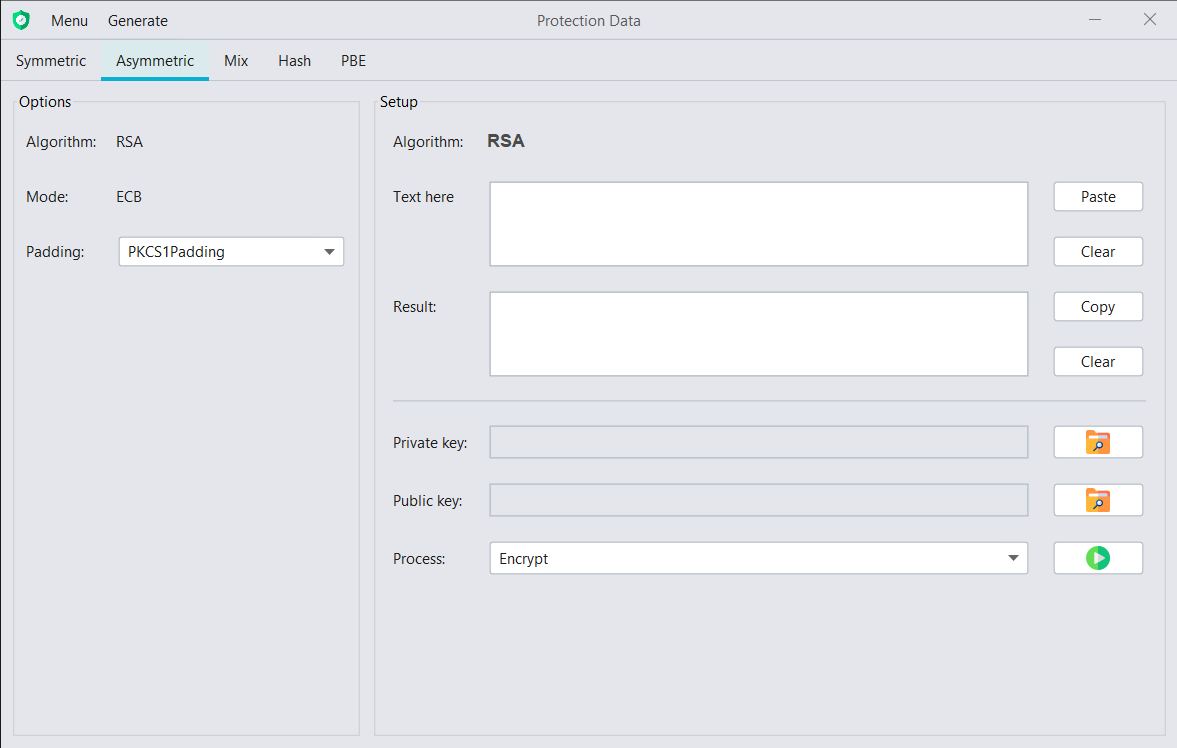
### Giao diện Symmetric (Màn hình chính).



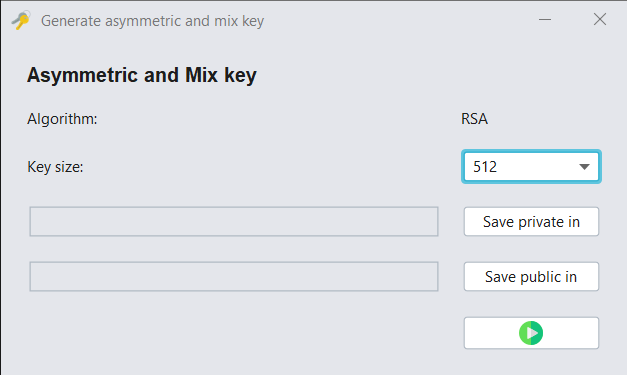
### Giao diện tạo key Symmetric.



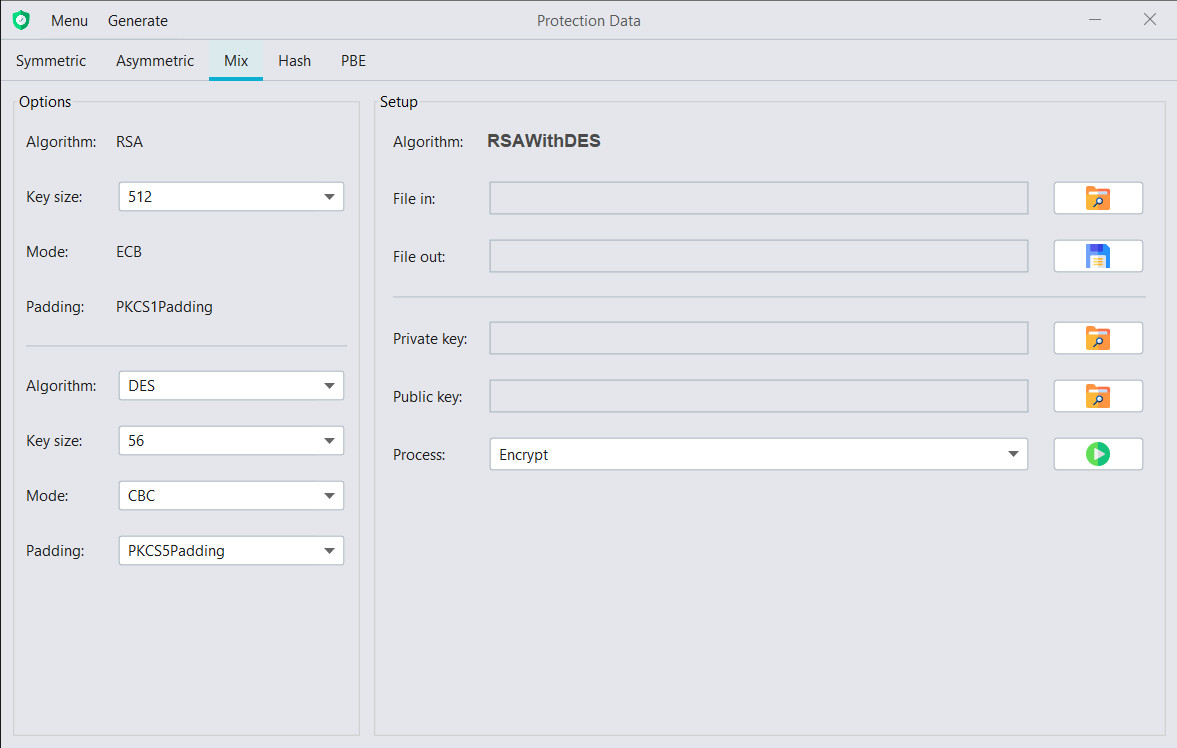
### Giao diện Asymmetric.



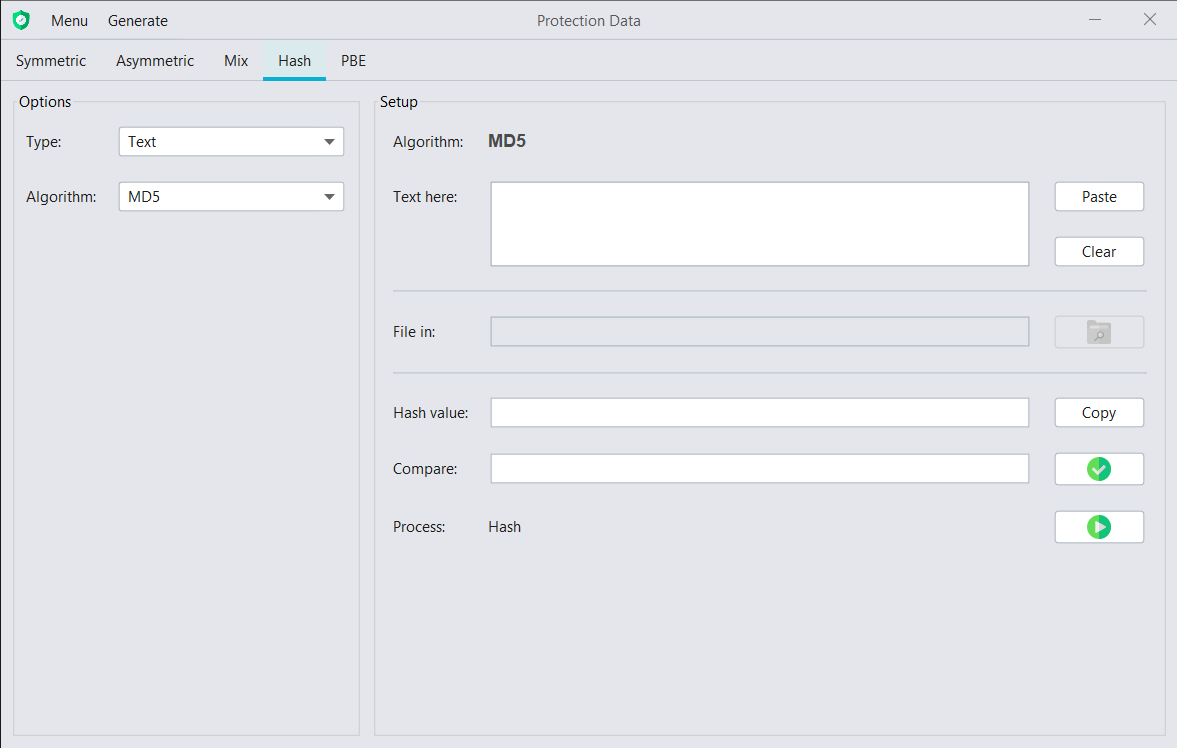
### Giao diện tạo key Asymmetric.



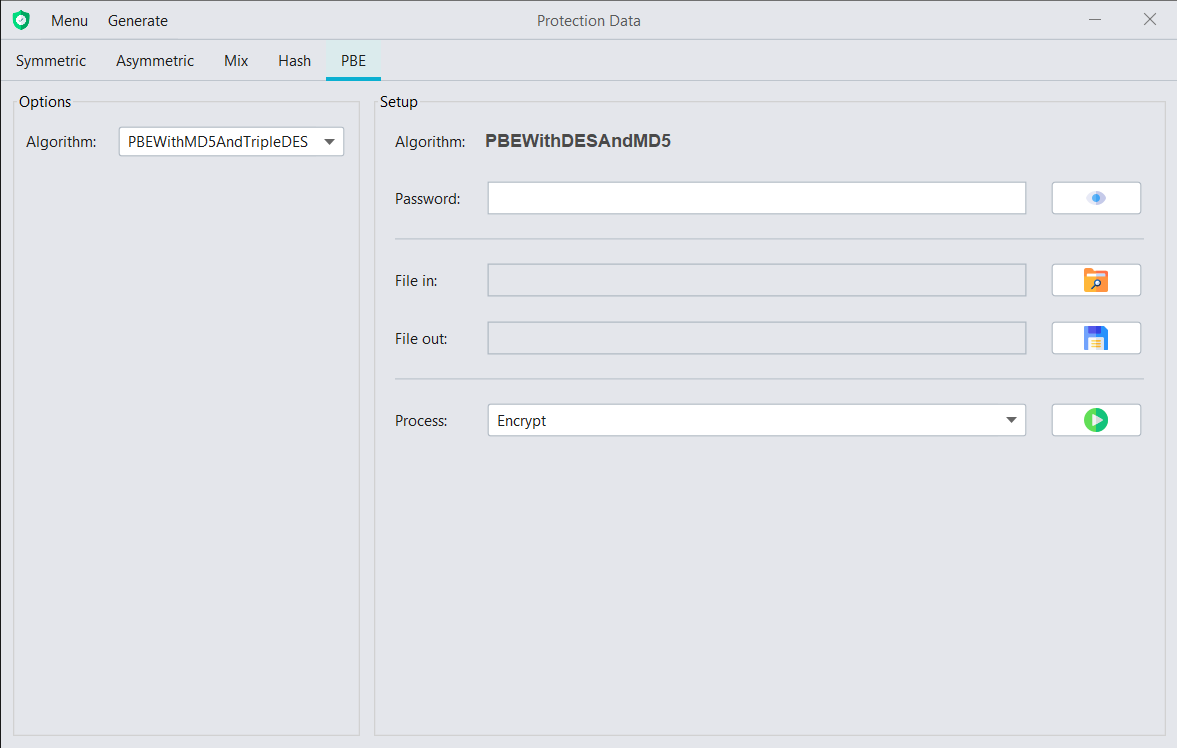
### Giao diên Mix.



### Giao diện Hash.

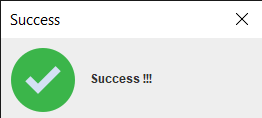


### Giao diện PBE.

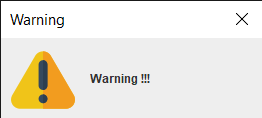


### Giao diện thông báo.

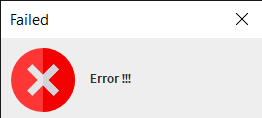
1. Thông báo thành công.



1. Cảnh báo.



1. Thông báo thất bại.



# Chi tiết chức năng.

## Symmetric và Symmetric key.

* Hỗ trợ các thuật toán: DES, DESede, AES, ARIA, RC2, RC5, RC6, Serpent, Blowfish, Twofish, Camellia, IDEA, SEED (thuật toán ngoài java).
* Hỗ trợ Text và File.
* Hỗ trợ các mode: CBC, CFB, OFB, CTR.
* Hộ trợ các padding: NoPadding, PKCS5Padding, PKCS7Padding, ISO10126Padding, ISO7816-4Padding.
* Hỗ trợ tạo key Base64 dạng file.

## Asymmetric và Asymmetric key.

* Hỗ trợ thuật toán: RSA.
* Hỗ trợ mã hóa đoạn văn bản nhỏ.
* Hỗ trợ tạo key Base64 dạng file.

## Mix.

* Hỗ trợ kết hợp đa thuật toán RSA với tất cả các thuật toán trong Symmetric.
* Hỗ trợ tạo key Base64 dạng file.

## Hash.

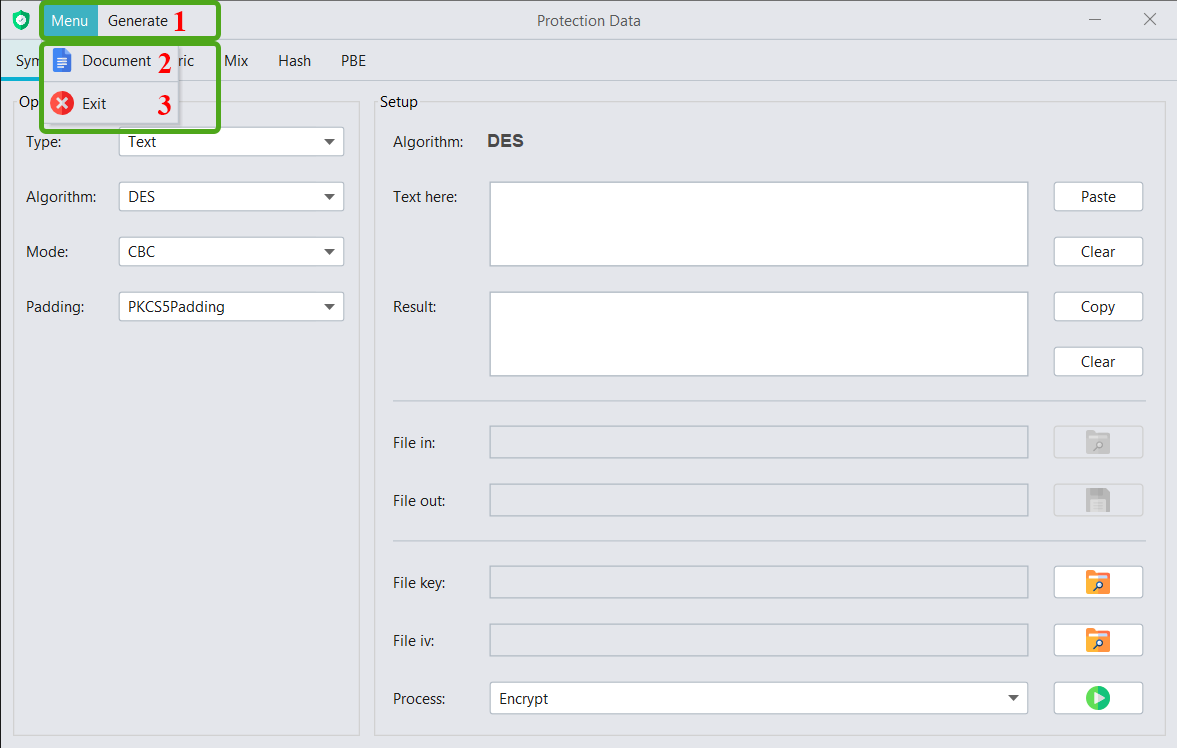
* Hỗ trợ hash Text và File.
* Hỗ trợ check 2 giá trị hash.

## PBE.

* Hỗ trợ mã hóa, giải mã mật khẩu, đơn giản dễ sử dụng với các thuật toán cho sẵn.

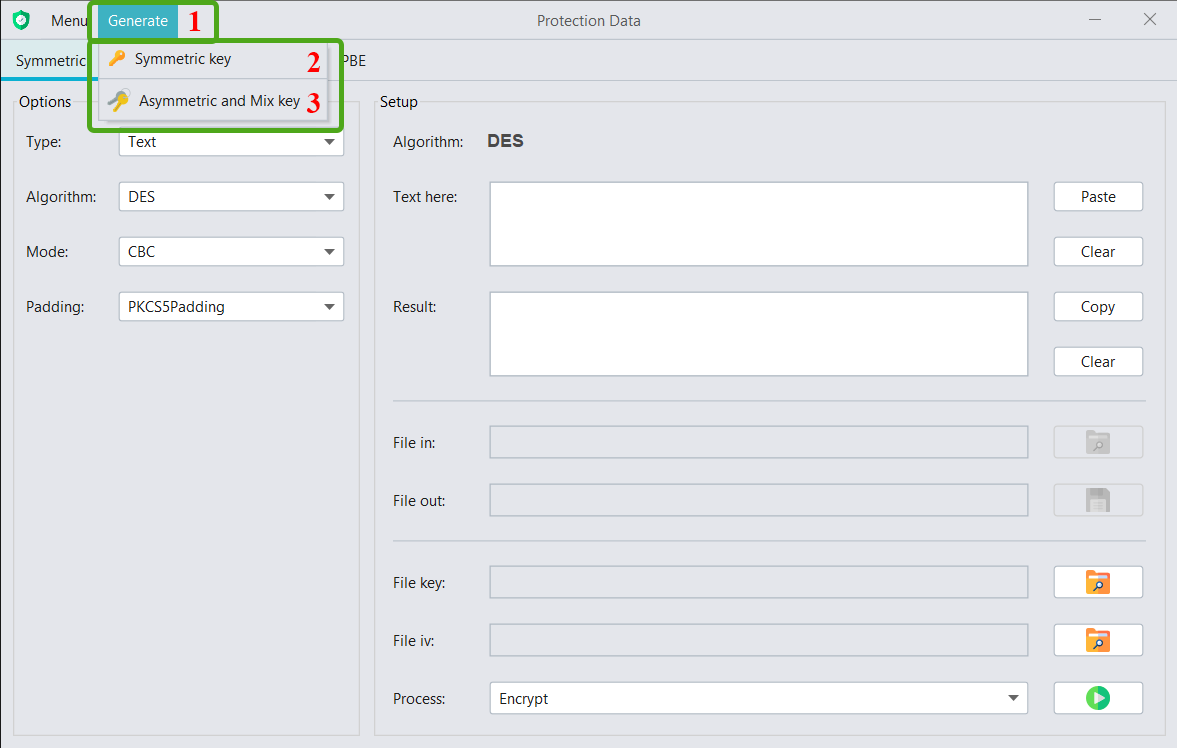
# Hướng dẫn sử dụng.

## Tải document và thoát.



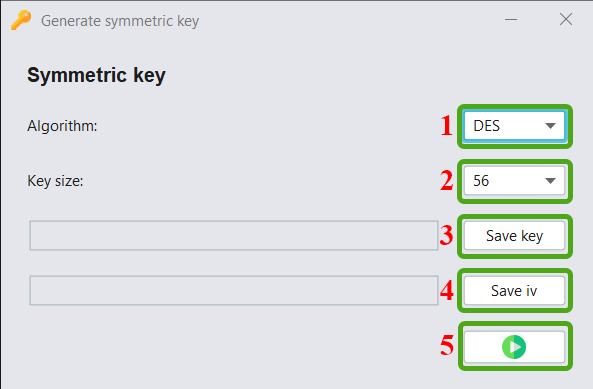
* Tại giao diện chính chọn Menu (1) => chọn item Document (2) để tải tài liệu online hoặc item Exit (3) để thoát.

## Truy cập vào chức năng tạo khóa.



* Tại giao diện chính nhấn chọn generate (1) => chọn item Symmetric key (2) hoặc item Asymmetric and Mix key (3).

## Chức năng tạo khóa Symmetric (đối xứng).



B1: chọn thuật toán (1) và key size (2).

B2: chọn nơi lưu File key (3) và File iv (4), nhấn nút Run (5).

B3: kết quả sẽ được hiển thị qua thông báo.

## Chức năng tạo khóa Asymmetric (bất đối xứng).

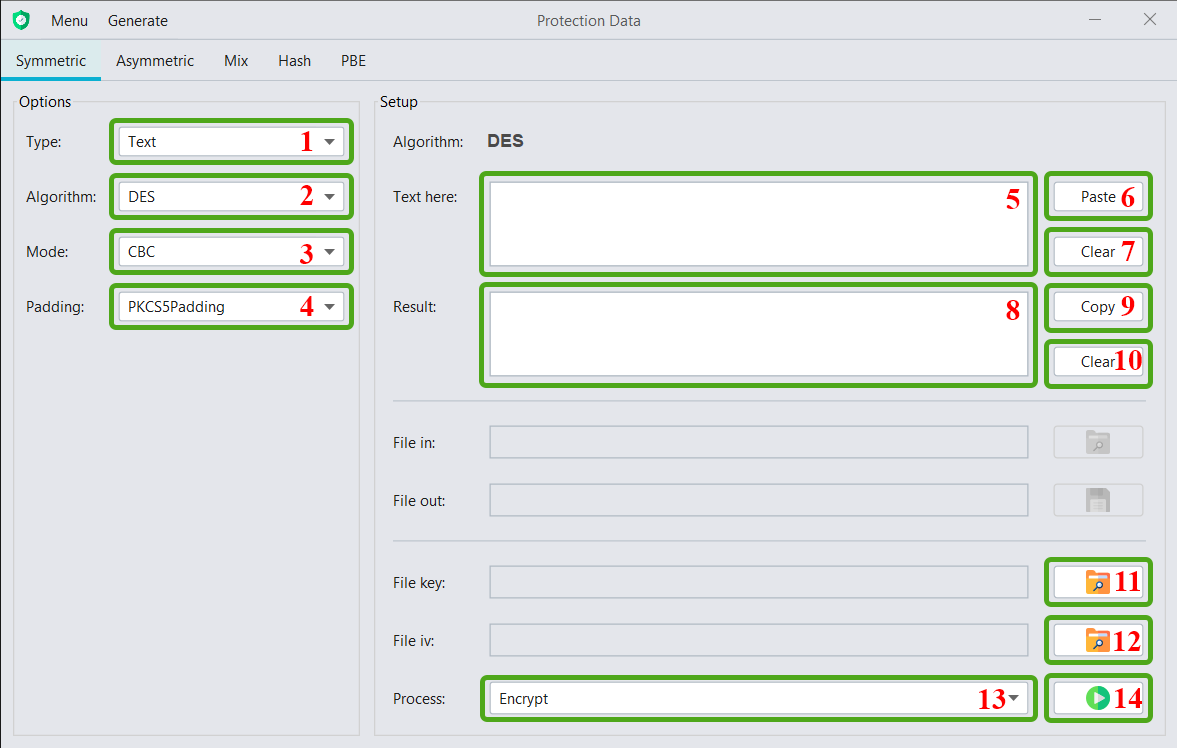


B1: thuật toán mặc định là RSA, chọn key size (1).

B2: chọn nơi lưu File private key (2) và File public key (3), nhấn nút run (4).

B3: kết quả sẽ được hiển thị qua thông báo.

## Chức năng mã hóa, giải mã Text Symmetric (chuỗi hoặc text bằng phương pháp đối xứng).



B1: tại giao diện chính của ứng dụng, ta giữ nguyên type là Text (1), lần lượt chọn các option tiếp theo như: Algorithm (2), Mode (3), Padding (4). Các trường này cần phải đảm bảo đúng, để không dẫn đến kết quả sai lệch.

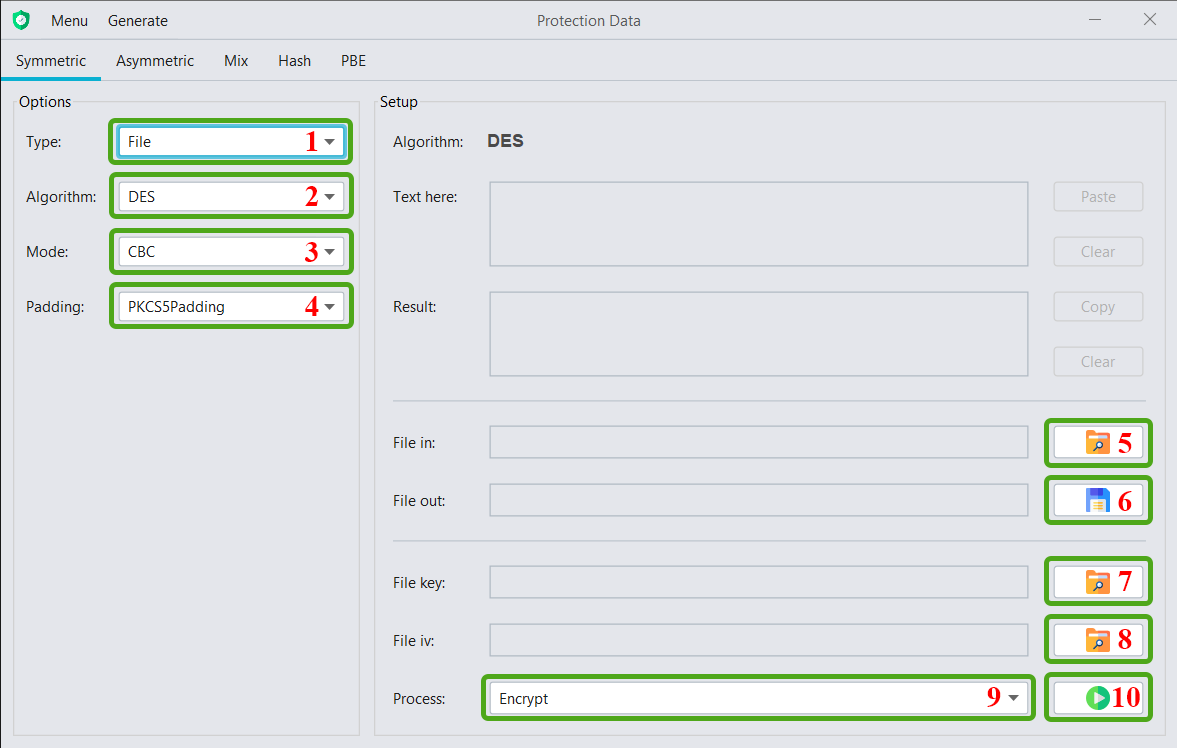
B2: nhập nội dung muốn mã hóa hoặc giải mã (5), có thể dán nội dung đã copy bằng nút Paste (6), xóa nội dung bằng nút Clear (7).

B3: chọn file key (11) và file iv (12) bằng nút Browse.

B4: chọn phương thức xử lí là Encrypt hoặc Decrypt (13) và nhấn nút Run (14).

B5: kết quả mã hóa hoặc giải mã Text sẽ được hiển thị (8), ta có thể copy bằng cách nhấn nút copy (9) và xóa bằng nút clear (10).

## Chức năng mã hóa, giải mã File Symmetric (File bằng phương pháp đối xứng).



B1: tại giao diện chính của ứng dụng, ta chọn type là File (1), lần lượt chọn các option tiếp theo như: Algorithm (2), Mode (3), Padding (4). Các trường này cần phải đảm bảo đúng, để không dẫn đến kết quả sai lệch.

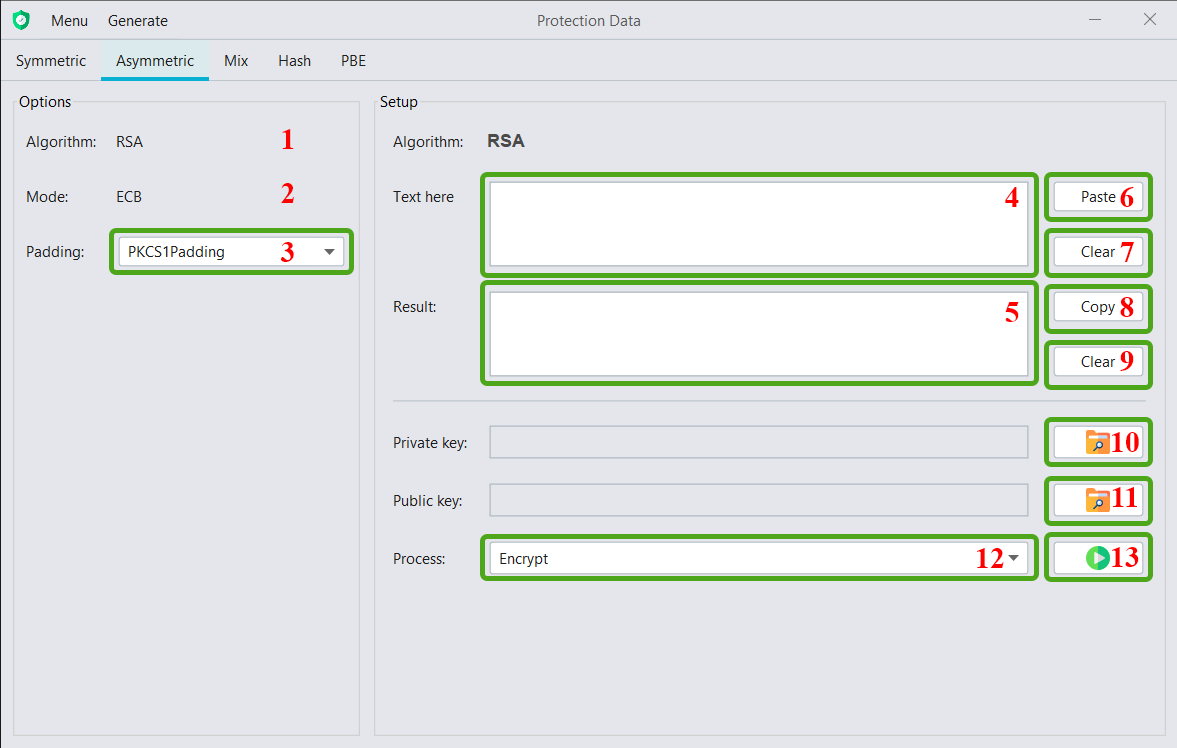
B2: chọn file cần được mã hóa hoặc giải mã (5) và nơi lưu file sau khi mã hóa hoặc giải mã (6).

B3: chọn file key (7) và file iv (8) bằng nút Browse.

B4: chọn phương thức xử lí là Encrypt hoặc Decrypt (9) và nhấn nút Run (10).

B5: kết quả sẽ được hiển thị qua thông báo.

## Chức năng mã hóa Text Asymmetric (chuỗi hoặc đoạn văn bản bằng phương pháp bất đối xứng).



B1: chuyển sang tab Asymmetric.

B2: thuật toán và mode được hỗ trợ sẽ mặc định là RSA (1) và ECB (2).

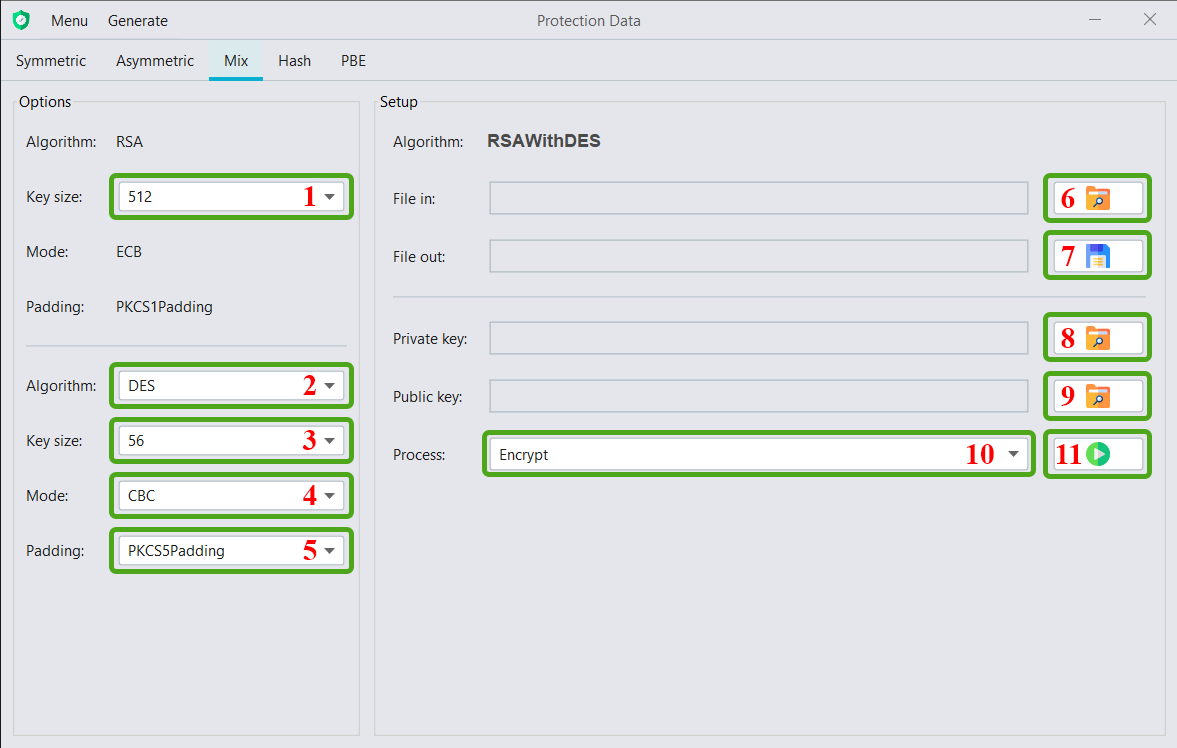
B3: nhập nội dung muốn mã hóa hoặc giải mã (4), có thể dán nội dung đã copy bằng nút Paste (6), xóa nội dung bằng nút Clear (7).

B4: chọn Public key file (10) và Private key file (11).

B5: chọn phương thức xử lí là Encrypt hoặc Decrypt (12) và nhấn nút Run (13).

B6: kết quả mã hóa hoặc giải mã Text sẽ được hiển thị (5), ta có thể copy bằng cách nhấn nút copy (8) và xóa bằng nút clear (9).

## Chức năng mã hóa Mix (Mã hóa File kết hợp giữa thuật toán RSA bất đối xứng và thuật toán đối xứng).



B1: chuyển sang tab Mix.

B2: Algorithm RSA, Mode ECB, Padding PKCS1 sẽ là mặc định cho Asymmetric, chọn key size (1) trùng với giá trị key size đã chọn ở B1 phần tạo key Asymmetric.

B3: chọn lần lượt thuật toán Symmetric: Algorithm (2), Key size (3), Mode (4), Padding (5).

B4: kiểm tra lại các option đã được chọn trong B1 và B2. Các trường cần phải đảm bảo đúng, để không dẫn đến kết quả sai lệch.

B5: chọn file cần được mã hóa hoặc giải mã (6) và nơi lưu file sau khi mã hóa hoặc giải mã (7).

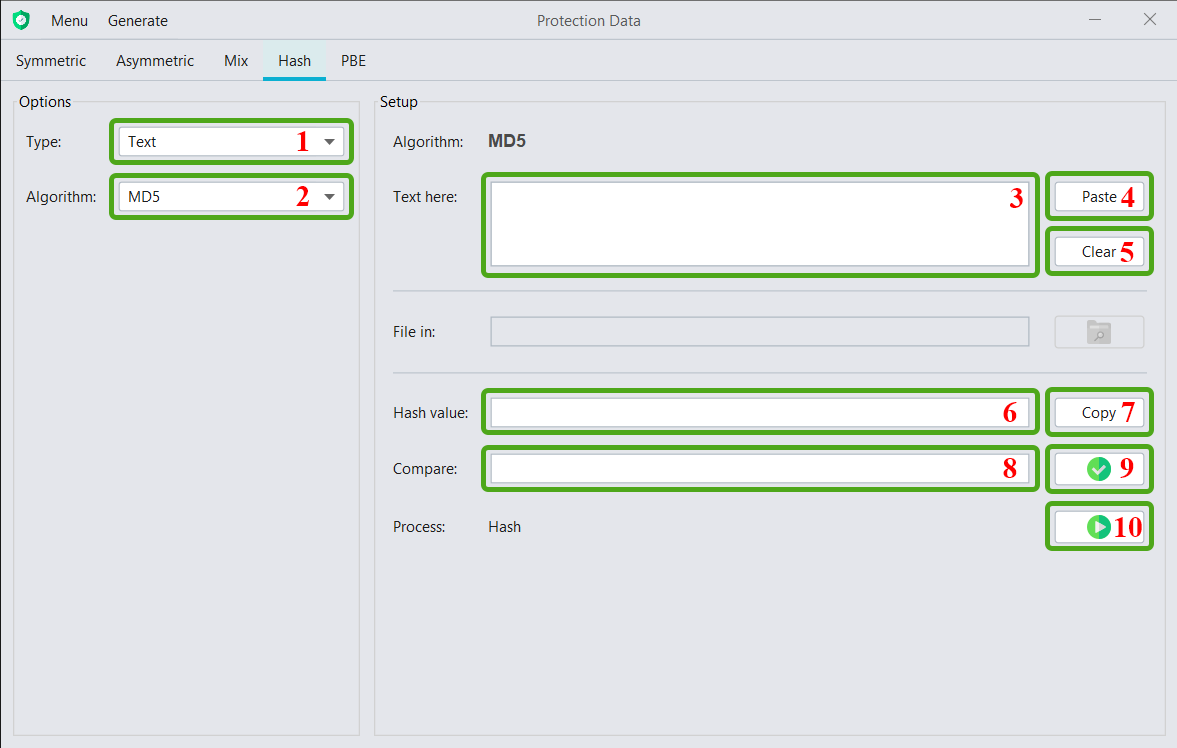
B6: chọn Public key file (8) và Private key file (9).

B7: chọn phương thức xử lí là Encrypt hoặc Decrypt (10) và nhấn nút Run (11).

B8: kết quả sẽ được hiển thị qua thông báo.

***Lưu ý:*** không như Symmetric và Asymmetric, key size trong Mix sẽ trực tiếp ảnh hưởng đến kết quả của mã hóa và giải mã, hãy đảm bảo bạn chọn đúng các trường.

## Chức năng Hash Text (hàm băm).



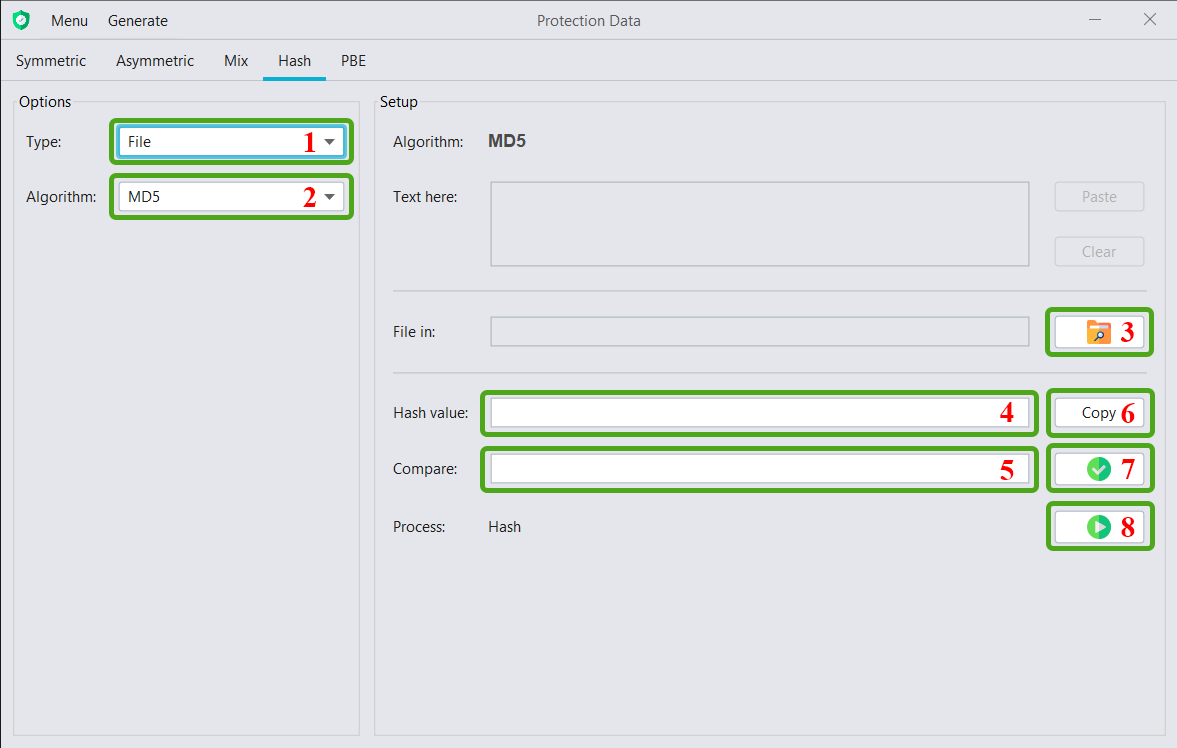
B1: Type mặc định là text (1), ta có thể chọn thuật toán khác (2).

B2: nhập nội dung muốn hash (3), có thể dán vào bằng nút Paste (4) và xóa bằng nút Clear (5). Nhấn nút run (10).

B3: hash value sẽ được hiển thị (6), chúng ta có thể kiểm tra nó với giá trị khác bằng cách nhập giá trị hash (8) và nhấn nút check (9).

B4: kết quả sẽ được hiển thị qua thông báo.

## Chức năng Hash File.



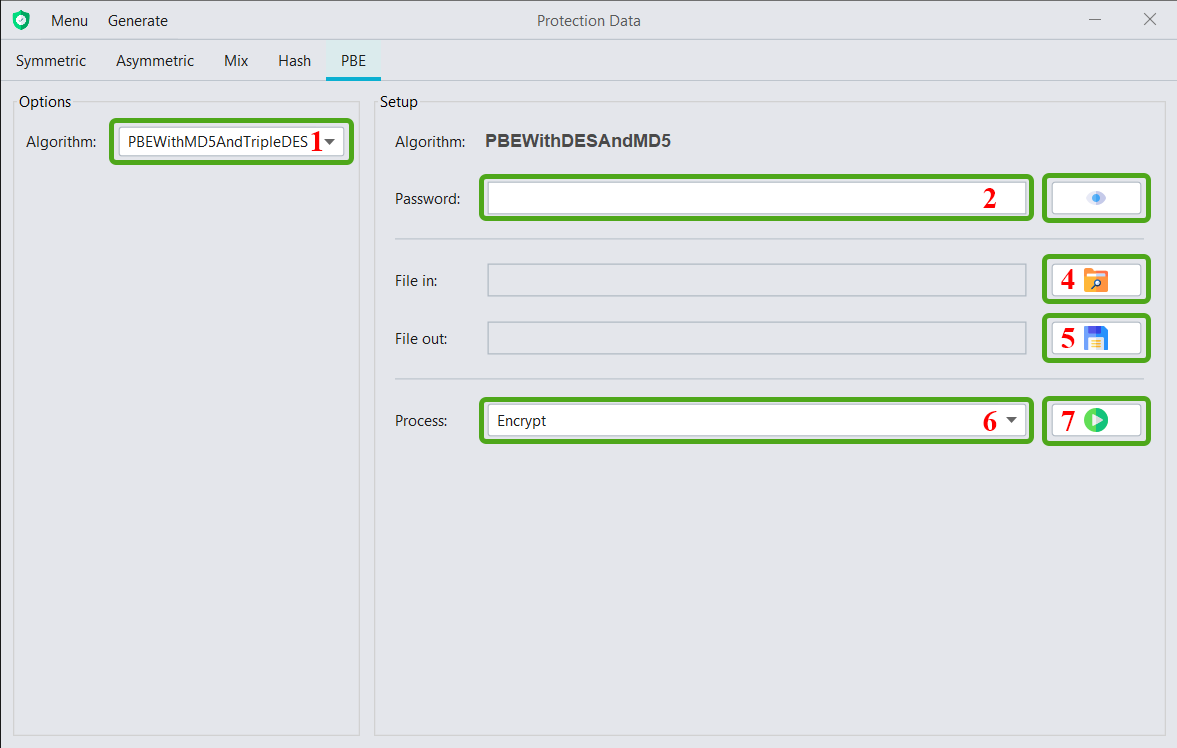
B1: chọn Type sang File (1), ta có thể chọn thuật toán khác (2).

B2: chọn file (3) và nhấn nút run (8).

B3: hash value sẽ được hiển thị (4), chúng ta có thể kiểm tra nó với giá trị khác bằng cách nhập giá trị hash (5) và nhấn nút check (7).

B4: kết quả sẽ được hiển thị qua thông báo.

## Chức năng PBE (sử dụng mật khẩu).



B1: chọn thuật toán (1).

B2: nhập mật khẩu (2), có thể xem lại mật khẩu (3).

B3: chọn file muốn mã hóa hoặc giải mã (4) và nơi lưu file sau khi mã hóa hoặc giải mã (5).

B4: chọn phương thức xử lí (6) và nhấn nút Run (7).

B5: kết quả sẽ được hiển thị qua thông báo.