ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA

MẬT MÃ VÀ AN NINH MẠNG

Bài Tập Lớn 1

GVHD: Nguyễn Hữu Hiếu
Sinh Viên: Châu Văn Hoài Lâm - 1711893
Lớp: L02

Tp. Hồ Chí Minh, 5/2020

Mục lục

1 Tóm Tắt **2**

2 Giới Thiệu **3**

2.1 Phạm vi và giới hạn của đề tài 3

2.2 Tổng quan nội dung công việc đã làm 3

2.3 Chương trình 3

3 Cơ Sở Lý Thuyết **4**

3.1 Mã hóa và Giải mã: 4

3.2 Hàm băm: 4

4 Nội Dung Công Việc Thực Hiện **5**

4.1 Tổng quan cách hiện thực 5

4.2 Quá trình mã hóa 6

4.3 Quá trình giải mã 7

4.4 Tính năng nâng cao 8

5 Phân tích Và Kết Luận **9**

6 Hướng phát triển **10**

7 Tham Khảo **10**

8 Phụ Lục **11**

1 Tóm Tắt

- Giới Thiệu :

  Trình bày tổng quan về công việc đã làm, phạm vi cũng như giới hạn của đề tài. Ngoài ra còn giới thiệu một số tính năng của chương trình.

- Cơ Sở lý thuyết:

  Trình bày ngắn gọn những nội dung lý thuyết được dùng để hiện thực chương trình.

- Nội dung công việc:

  Phần này sẽ trình bày chi tiết các công việc đã làm bao gồm các tính năng cơ bản và nâng cao, nêu rõ ý tưởng từng bước giải thuật cùng một số hình ảnh minh họa.

- Phân tích và kết luận:

  Tổng kết lại các nội dung đã hiện thực, đạt được. Đánh giá, phân tích tốc độ mã hóa, giải mã của chương trình và một số hạn chế.

- Hướng phát triển:

  Tập trung vào những ý tưởng có thể hiện thực trong tương lai, cố gắng khắc phục những hạn chế...

Cuối cùng, là những tài liệu đã tham khảo để hiện thực chương trình và phụ lục hướng dẫn cùng một số lưu ý khi sử dụng chương trình.

2 Giới Thiệu

Mã hoá là phương pháp giúp bảo vệ dữ liệu cá nhân nhạy cảm trên máy tính của bạn, cho dù bạn có gởi dữ liệu cho cá nhân, tổ chức nào đó qua mạng Internet, hay sao lưu dữ liệu cá nhân trên các máy chủ, Cloud,..., thì việc mã hoá sẽ ngăn chặn bất cứ ai có thể đọc được dữ liệu trước khi được sự cho phép của bạn.

2.1 Phạm vi và giới hạn của đề tài

Thực hiện một chương trình mã hóa để giữ cho các tập tin và thư mục trên máy tính của mình thật sự an toàn. Cụ thể là xây dựng chương trình mã hóa và giải mã các tập tin và thư mục sử dụng các giải thuật mã hóa được sử dụng phổ biến trong thực tế như DES, AES, RSA...

2.2 Tổng quan nội dung công việc đã làm

- Môi Trường: Sử dụng ngôn ngữ lập trình Java cùng thư viện Java Cryptography Architecture (JCA) trên Eclipse IDE.
- Mã Hóa và giải mã: sử dụng Data Encryption Standard (DES) - thuật toán mã hóa dữ liệu.
- Kiểm tra tính toàn vẹn dữ liệu: sử dụng Secure Hash Algorithm 256 (SHA - 256) - thuật toán băm.

2.3 Chương trình

Chương trình cung cấp cho người dùng hai tính năng cơ bản: mã hóa (Encrypt) và giả mã (Decrypt):
- Quá trình mã hóa:

- Input: tập tin hoặc thư mục có định dạng bất kì trừ định dạng ".enc"(file đã mã hóa) và tập tin chứa khóa (key).
- Output: những file và thư mục đã được mã hóa (có định dạng ".enc").

- Quá trình giải mã: đầu vào là Output của quá trình mã hóa, đầu ra là những tập tin hay thư mục trước khi mã hóa.

Chi tiết các quá trình mã hóa và giải mã sẽ được trình bày ở mục 4.

3 Cơ Sở Lý Thuyết

3.1 Mã hóa và Giải mã:

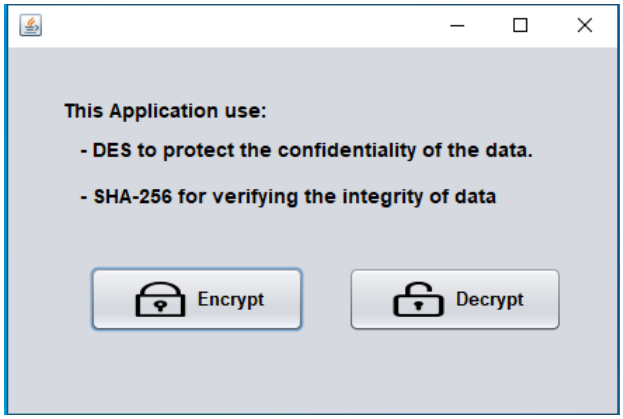
- Mã hóa (encryption): là hành động xáo trộn bản rõ (plaintext) để chuyển thành bản mã (ciphertext) nhằm mục đích bảo đảm an toàn thông tin trên đường truyền.
- Giải mã (decryption): là hành động xáo trộn bản mã (ciphertext) để chuyển thành bản rõ (plaintext).
- DES là loại mã hóa đối xứng (mã hóa khóa bí mật), sử dụng một khóa bí mật (private key) duy nhất cho cả quá trình mã hóa và giải mã.
  - là dạng mã hóa khối, kích thước khối vào 64 bit.
  - Khóa 64 bit trong đó chỉ sử dụng 56 bit, 8 bit dùng cho kiểm tra chẵn lẻ.
  - DES sử dụng chung một giải thuật cho mã hóa và giải mã.

3.2 Hàm băm:

- Băm (hashing) là quá trình chuyển đổi đầu vào gồm các chữ cái và ký tự có kích thước không cố định để tạo đầu ra có kích thước cố định. Quá trình này được thực hiện bằng cách sử dụng các công thức toán học như các hàm băm (được thực hiện dưới dạng các thuật toán băm).
- Secure Hash Algorithm 256 (SHA-256) là một thuật toán băm dùng để chuyển một đoạn dữ liệu bất kì thành một đoạn dữ liệu có chiều dài 256 bit với xác suất khác biệt cao.

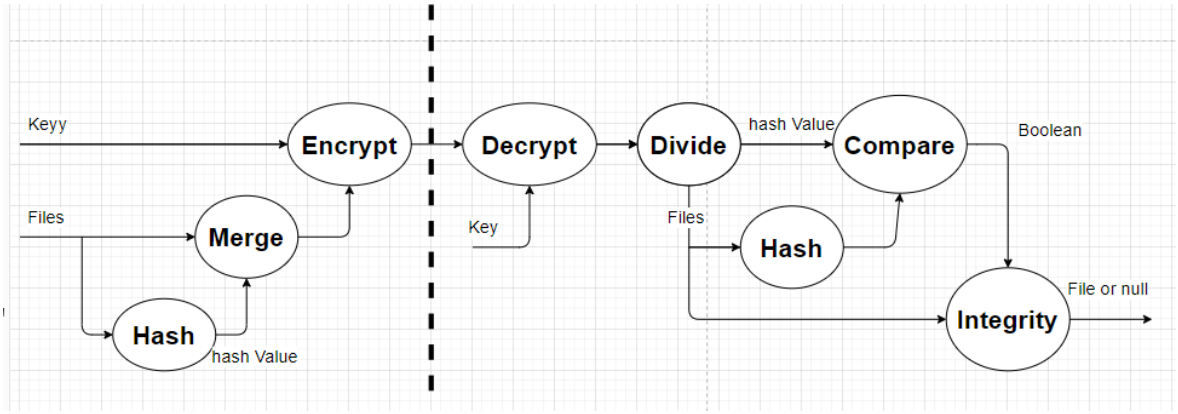
4 Nội Dung Công Việc Thực Hiện

4.1 Tổng quan cách hiện thực



Hình 1: Giao diện tổng

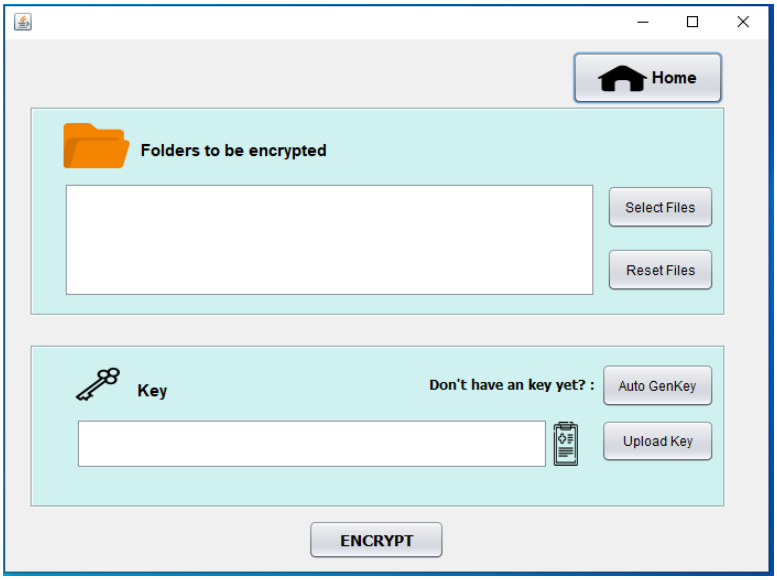
Chương trình thực hiện hai tính năng cơ bản là mã hóa và giải mã. Hình 2 sẽ cho thấy cách hiện thực bên dưới của chương trình.



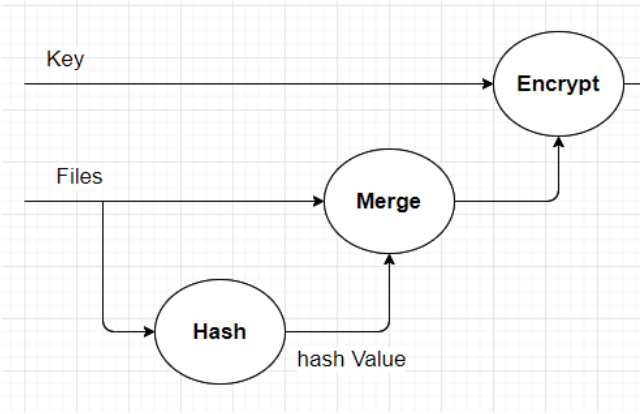
Hình 2: Tổng quan hiện thực chương trình

Ngoài ra còn có một số tính năng nâng cao: tạo khóa tự động, hiển thị thanh trạng thái, mã hóa giải mã toàn bộ tập tin trong một thư mục được chọn.

4.2 Quá trình mã hóa



Hình 3: Giao diện mã hóa



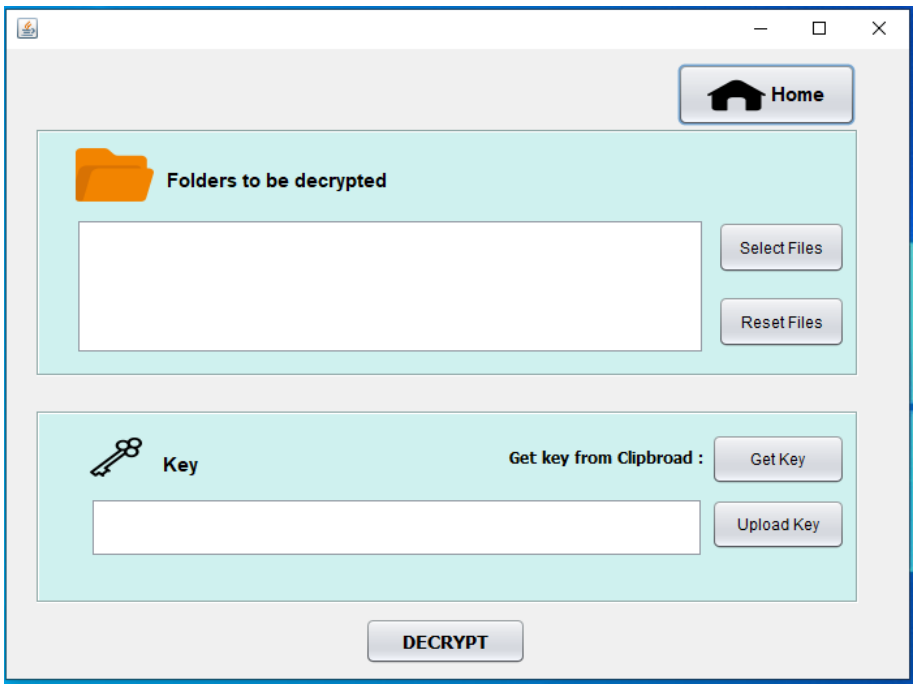
Hình 4: Quá trình mã hóa

Quá trình mã hóa là tập hợp tuần tự của các bước sau:

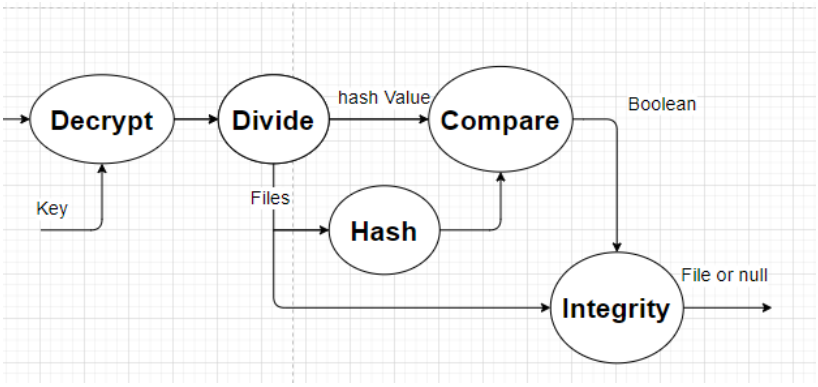
- nhận vào File với định dạng bất kì (trừ .enc) và Key từ người dùng.
- Sử dụng hàm băm SHA-256 để băm file. Nhằm phục vụ quá trình kiểm tra tính toàn vẹn của dữ liệu ở bước giải mã.

- Tiến hành nối giá trị băm vào cuối file.
- Sử dụng Key và giải thuật mã hóa DES để mã hóa file vừa nối tạo ra file đã mã hóa(có định dạng .enc).

4.3 Quá trình giải mã



Hình 5: Giao diện giải mã



Hình 6: Quá trình giải mã

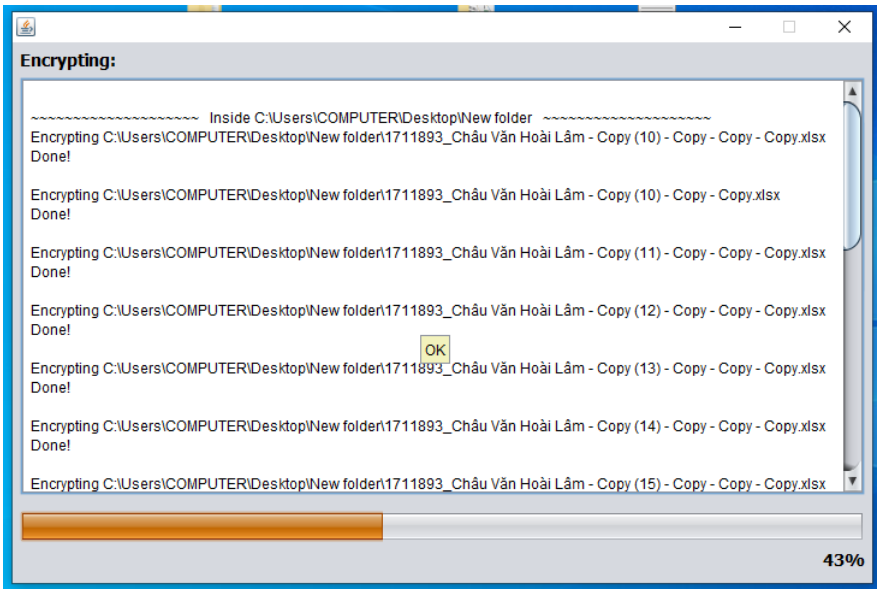
Quá trình giải mã bao gồm các bước tuần tự như sau:

- Nhận vào file .enc và Key từ người dùng.
- Giải mã file bằng thuật DES.
- Tiến hành tách file đã giải mã thành 2 phần: file gốc và giá trị băm (256 bit cuối).
- Băm file gốc sử dụng SHA-256.
- So sánh hai giá trị băm để kết luận tính toàn vẹn của dữ liệu.
- Nếu giá trị băm khác nhau sẽ cảnh báo người dùng file không còn toàn vẹn. Ngược lại, giải mã thành công và kết thúc quá trình giải mã.

4.4 Tính năng nâng cao

- Hiển thị thanh trạng thái:

  - Trước khi mã hóa ta tính toán kích thước tổng của các file.



Hình 7: thanh trạng thái

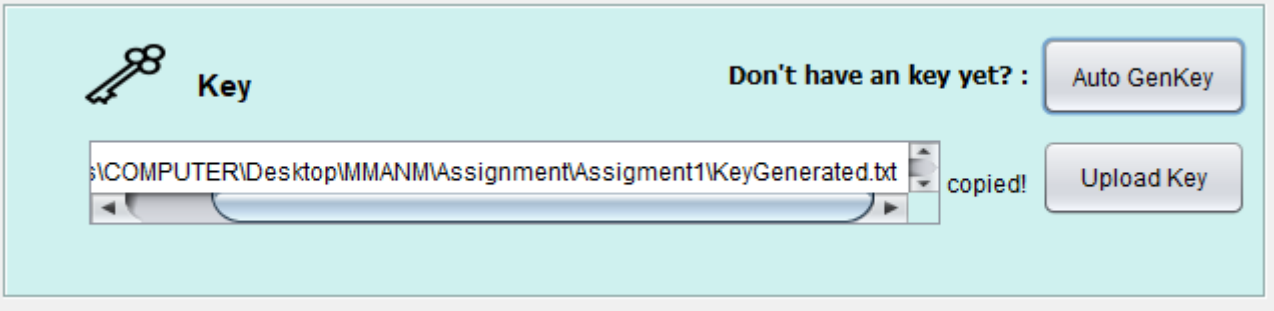
- trong quá trình mã hóa ta cập nhật kích thước file đã mã hóa được để cập nhật lên thanh trạng thái.

- Mã hóa tất cả tập tin từ thư mục:

  trước khi mã hóa ta kiểm tra xem nó là thư mục hay tập tin, nếu là tập tin thì chuyển đến quá trình mã hóa. Ngược lại, ta gọi đệ quy đến tất cả các file trong thư mục đó.

- Tự động tạo khóa:

  Sử dụng thư viện Javax.cypto để tạo khóa tự động cho giải thuật mã hóa DES.



Hình 8: Tạo khóa tự động

5 Phân tích Và Kết Luận

- Kết quả đạt được:

  - Chương trình có thể mã hóa và giải mã hầu hết các định dạng tập tin như hình ảnh, âm thanh, văn bản, pdf...

  - Khi bị tấn công, bị đánh cấp tập tin mã hóa thì kẻ tấn công không thể lấy được nội dung vì chỉ chứa những nội dung đã mã hóa nhờ đó tính bí mật của dữ liệu được bảo vệ.

  - Khi kẻ tấn công thay đổi nội dung tập tin mã hóa, ta sẽ biết được nhờ giá trị băm không trùng khớp, từ đó tính toàn vẹn của dữ liệu được xác thực.

  - Có thể mã hóa và giải mã toàn bộ tập tin bên trong thư mục.

  - Hiển thị được thanh trạng thái trong quá trình mã hóa/giải mã, có thể thấy được quá trình mã hóa, giải mã khá nhanh do giải thuật mã hóa DES khá đơn giản.

  - Tốc độ của quá trình mã hóa và giải mã xấp xỉ tốc độ ghi, đọc file.

- Hạn chế:

  - chưa hiện thực được quá trình phân phối khóa.

  - DES là một trong những giải thuật mã hóa ra đời sớm, sử dụng kích thước khóa nhỏ (64 bit) nên dễ bị tấn công.

6 Hướng phát triển

Hiện thực thêm tính năng phân phối khóa bằng cách sử dụng khóa công khai. Tích hợp vào các ứng dụng như filesharing, chat.

7 Tham Khảo

Tài liệu

[1] Textbook Cryptography and Network Security, Principles and Practice, William Stallings, Pearson, seventh edition, 2017

[2] https://stackjava.com/demo/sha-la-gi-code-vi-du-sha1-sha2-voi-java.html

[3] https://stackjava.com/demo/code-java-vi-du-ma-hoa-giai-ma-voi-des.html (lần cuối truy cập ngày 1/6/2020).

[4] https://www.cse.wustl.edu/ jain/cse567-06/ftp/encryption_perf/

8 Phụ Lục

Hướng dẫn sử dụng:

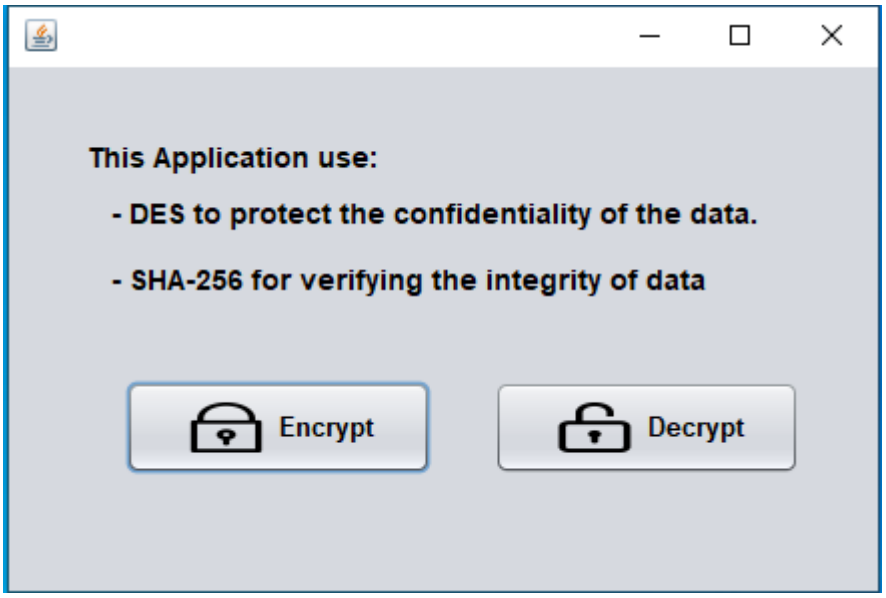
- Chuẩn bị :

  - Tập tin dùng để mã hóa với định dạng bất kì (ngoại trừ .enc).

  - Tập tin chứa khóa định dạng .txt.

  * Lưu ý quá trình mã hóa và giải mã phải dùng chung 1 khóa.

- Bắt đầu:

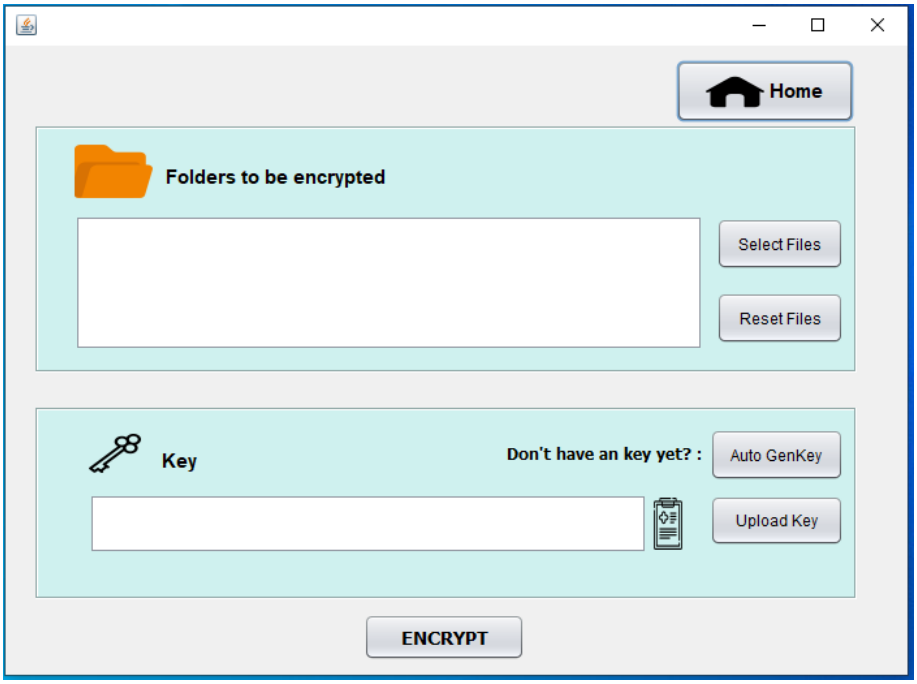


Hình 9: Menu screen

- Chọn Encrypt nếu bạn muốn bắt đầu mã hóa tập tin.

- Chọn Decrypt nếu bạn muốn bắt đầu giải mã tập tin.

- Mã hóa :



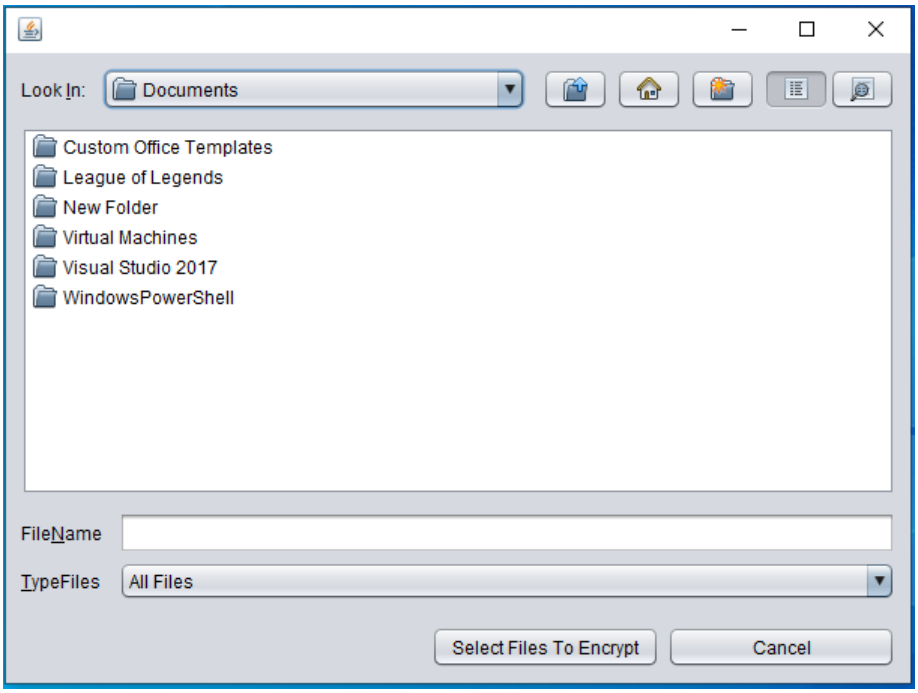
Hình 10: encrypt screen

1. Chọn tập tin để mã hóa :
   (a) Select Files : để chọn các tập tin hay thư mục bạn muốn mã hóa
   (b) Reset Files : bỏ chọn tất cả các tập tin đã chọn.
2. Chọn khóa :
   (a) Auto GenKey : nếu chưa chuẩn bị khóa có thể sử dụng tính năng tạo khóa ngẫu nhiên và đương nhiên là hoàn toàn miễn phí.
   (b) Upload Key : tải lên khóa đã chuẩn bị từ trước.
   (c) Icon copy (cạnh link Khóa) : copy khóa vào clipbroad, để sử dụng cho quá trình giải mã mà không cần phải tải lên khóa. Khuyến khích dùng để tránh trường hợp quên vị trí đặt tập tin khóa.
3. ENCRYPT button : tiến hành mã hóa tập tin.

*Lưu Ý bắt buộc phải có ít nhất một tập tin mã hóa và khóa. Nếu thiếu 1 trong 2 sẽ không thể tiến hành mã hóa tập tin.

- Chọn tập tin:

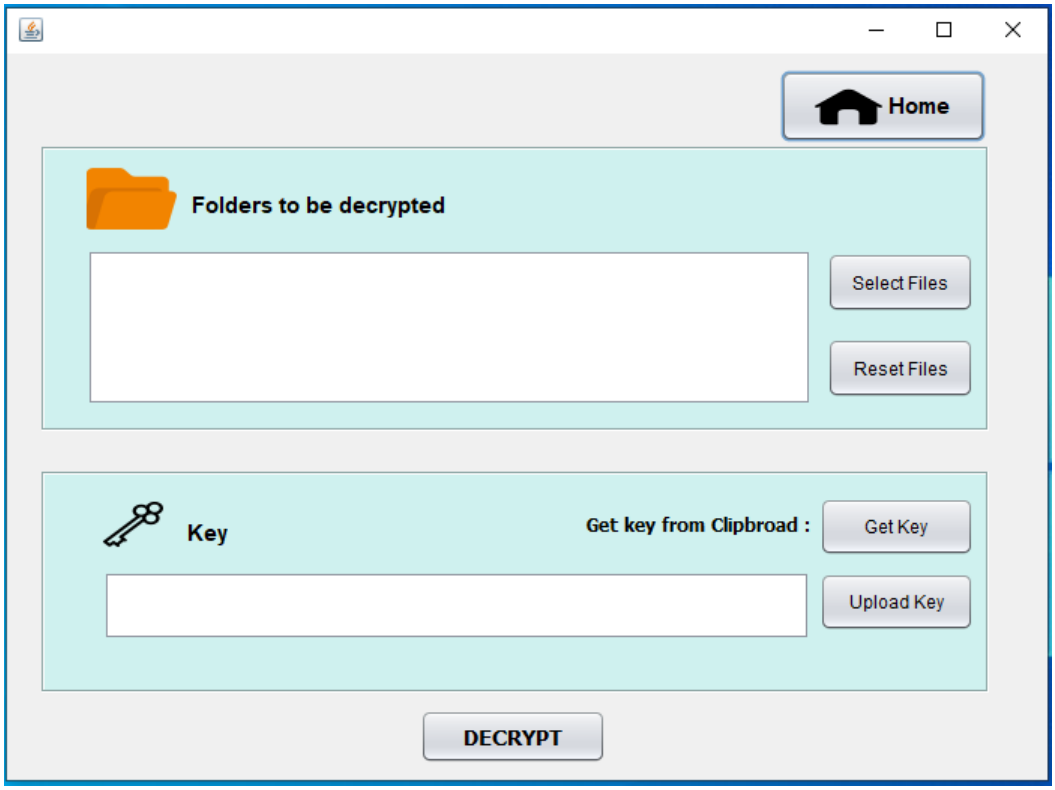
  - Cho phép người dùng chọn cùng lúc nhiều tập tin để giải mã hay mã hóa.



Hình 11: choose files

*Lưu ý khi chọn tập tin để mã hóa thì phải chọn định dạng khác .enc, chọn tập tin để giải mã thì chọn định dạng .enc.

- Giải mã:

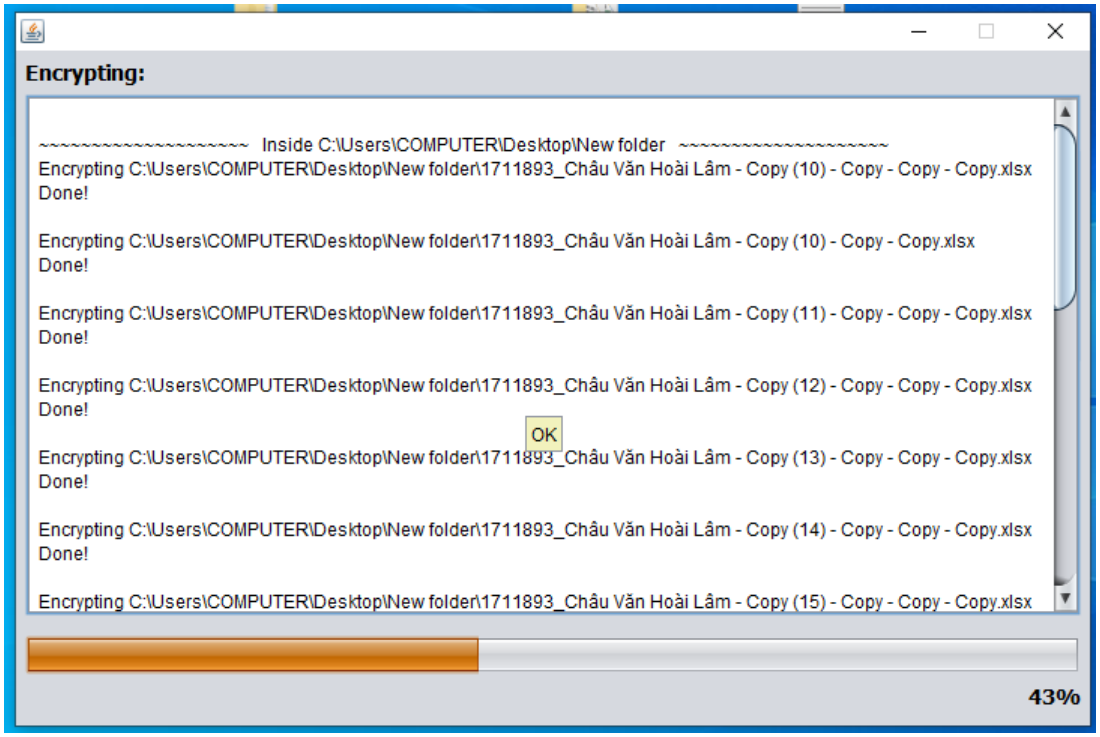


Hình 12: decrypt screen

- Các chức năng cơ bản giống với bước mã hóa chỉ khác button Get key: làm nhiệm vụ lấy key đã copy vào clipbroad từ bước mã hóa.

*Lưu ý quá trình mã hóa cũng bắt buột phải có cả khóa và ít nhất là một tập tin đã mã hóa (định dạng .enc)

- Hoàn thành:



Hình 13: finish screen

Tiến hành mã hóa. khi chạy xong 100% nghĩa là quá trình mã hóa, giải mã đã hoàn thành.

* Lưu ý là tập tin mã hóa hay giải mã sau khi hoàn thành sẽ đặt tại vị trị folder tập tin trước khi mã hóa, giải mã.