**Manual document**

(Tài liệu hướng dẫn chạy chương trình)

# **Giới thiệu.**

Đây là chương trình được xây dựng theo các tiêu chí phía bên dưới bằng ngôn ngữ javascript với thư viện ReactJS. Chương trình được xây dựng thỏa 4 trong 6 tiêu chí trên với 1 file.txt hoặc 1 đoạn text nhập vào.

1. **Key mã hóa (password) do người dùng nhập vào được hash thành 1 chuỗi tối thiểu 100bit.**
2. **Việc mã hóa /giải mã phải nhanh (thời gian giải mã trong RAM phải ở mức real time).**
3. **Tuy cùng 1 key mã hóa nhưng mỗi lần mã sẽ /phải được một kết quả khác nhau (về cả chiều dài lẫn nội dung nhị phân).**
4. **Chương trình mã hóa có obfurcasted code để tăng độ an toàn, tránh không cho người khác dò ra cách làm và giải mã.**
5. Mỗi khi chương trình chạy phải hỏi và kiểm tra 1 mật khẩu "động" và nếu đúng thì mới tiếp tục chạy.
6. Chương trình có tính năng phát hiện các dấu hiệu bất thường và xử lý phù hợp (ví dụ: thấy nội dung không như ban đầu (bị crack hoặc có virus bám vào) thì tự khôi phục lại, thấy môi trường chạy không phải là môi trường "lành mạnh" (bị chạy trong sandbox hoặc trong chế độ debug, chương trình không nằm trong đĩa /máy được quy ước, ...) thì không chạy /tự hủy /gây lỗi hệ thống, ...)

# **Hướng dẫn chạy chương trình.**

## **Thiết lập môi trường.**

Chương trình sử dụng các tài nguyên sau. Vui lòng cài đặt các công cụ phía trên để tiếp hành chạy chương trình. Máy tính có kết nối internet.

* Node: <https://nodejs.org/fr>
* Visual Studio Code: <https://code.visualstudio.com/Download>
* Git: <https://git-scm.com/downloads>

## **Cách chạy chương trình.**

Đây là một web application, để chạy chương trình, vui lòng thực hiện các bước hướng dẫn sau:

* **Bước 1:** Mở **command** đến folder muốn **pull source** từ git về, sau đó dùng lệnh:

**Git clone** [**https://github.com/NgocTan2k1/encrypt.git**](https://github.com/NgocTan2k1/encrypt.git)

(bỏ qua nếu đã có sẵn source).

* **Bước 2:** Di chuyển **command** đến source bằng lệnh: **cd encrypt** (lênh folder được đặt trước đó rồi)
* **Bước 3:** Khi **command** đã di chuyển đến thư mục **encrypt** thì chạy lệnh: **npm i** (lệnh này dùng để **download** các thư viện cần thiết để chạy chương trình)
* **Bước 4:** Sau khi **download** các thư viện xong, ta chạy lệnh: **npm start** (để chạy chương trình)

**Ngoài ra:** có thể chạy lệnh **npm run build** ở **Bước 3**, sau đó chạy lệnh **serve -s build** để khởi động 1 server trên địa chỉ <http://127.0.0.1:3000> (<http://localhost:3000>)

# **Chi tiết về chương trình.**

Chương trình thỏa 4 trên 6 tiêu chí ban đầu.

Thuật toán **hash key** nhập vào là SHA-256

Mã hóa đối xứng **AES** với **key** được **hash** trên do người dung nhập vào.

Thuật toán mã hóa được thêm **salt** để mỗi lần mã hóa sẽ cho ra độ dài và nội dung **cipherText** khác nhau.

Chương trình mã hóa được chia ra làm 2 dạng:

* Dạng 1: Cho người dùng nhập đoạn Plain text mã hóa và hiển thị Cipher text
* Dạng 2: Cho người dùng tải file.txt để mã. Sau khi mã sẽ download về một file có tên là encrypt-file.txt chứa nội dung mã Cipher text.

Chương trình giải mã cũng được chia làm 2 dạng:

* Dạng 1: Cho người dùng nhập Cipher text rồi giải mã và hiển thị Plain text
* Dạng 2: Cho người dùng tải file.txt để giải mã. Sau khi giải mã sẽ download về một file có tên là decrypt.txt chứa nội dung Plain text ban đầu.

# **Kết quả chạy**

## **Chạy với đoạn text nhập vào.**

Mã hóa chữ hello với key 123

A screenshot of a computer

Description automatically generated

Mỗi lần mã là ra một bản Cipher text khác nhau

A screenshot of a computer

Description automatically generated

Giải mã Ciphet text là: ‘**U2FsdGVkX192u3qGw6Ng3/oYv5+LfwrB9JoumnouUGPbI87464+iIA8kVMIXVSsQe4HggaVQJJoSLZkF4I/gOe8LmklpTfR94j2j5n/+iLDzbkfs7WUQF7o8DX3x1tKd**’với key 123

A screenshot of a computer

Description automatically generated

Giải mã Ciphet text là: ‘**U2FsdGVkX19kQcGc1O4Dy5aqV4lMqwWzToxGkP3sLy2lvXuUY1JnbaxAktjEbeuNjpYaIVdKQ0cQTpPvzYFVNIhxrL27uA6V2tuv3bzoAkBewp14N/ojsFMtGNJXRN+r**’với key 123

A screenshot of a computer

Description automatically generated

## **Chạy với file txt.**

Chọn file test 1 với nội dung test1.txt với key là 123 ta thu được nội dung 2 file encrypt-test1.txt như sau:

A screenshot of a computer

Description automatically generated

Nội dung 2 file encrypt-test.txt

A screenshot of a computer

Description automatically generated

Để giải mã ta chọn file vừa mới mã hóa trên và nhập key cần mã vào.

File encrypt-test1.txt thứ nhất

A screenshot of a computer

Description automatically generated

File encrypt-test1.txt thứ hai

A screenshot of a computer

Description automatically generated

Kết quả thu được ở file decrypt.txt

A screenshot of a computer

Description automatically generated

# **Hướng phát triển và cải tiến.**

Hiện tại em đang nghiên cứu để có thể cải tiến thêm việc đọc được nhiều file với phần mở rộng khác nhau như word, excel, pdf..

Phần mã hóa file ảnh jpg và png em đã có làm được trong đồ án của môn học trước nhưng không có tích hợp trong chương trình lần này. Nếu có thêm thời gian có thể em sẽ tích hợp thêm vào.

# **Nơi lưu giữ source code.**

Github: https://github.com/NgocTan2k1/encrypt.git