MỤC LỤC

1. [Tìm hiểu lý thuyế t 2](file:///C:\Users\Acer\Downloads\Bài-thực-hành-13_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark0)
   1. [Tìm hiểu về phần mề m True Crypt 2](file:///C:\Users\Acer\Downloads\Bài-thực-hành-13_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark1)
   2. [Giải thuật mã hóa AES 2](file:///C:\Users\Acer\Downloads\Bài-thực-hành-13_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark2)
   3. [Cách thức, phương pháp mà True Crypt sử dụng để mã hóa file 4](file:///C:\Users\Acer\Downloads\Bài-thực-hành-13_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark3)
2. [Nội dung thực hành 5](file:///C:\Users\Acer\Downloads\Bài-thực-hành-13_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark4)
   1. [Tiế n hành cài đặt True Crypt trên Windows 5](file:///C:\Users\Acer\Downloads\Bài-thực-hành-13_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark5)
   2. [Sử dụng công cụ True Crypt để mã hóa file 7](file:///C:\Users\Acer\Downloads\Bài-thực-hành-13_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark6)
3. [Tài liệ u tham khảo 15](file:///C:\Users\Acer\Downloads\Bài-thực-hành-13_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark7)

# Tìm hiểu lý thuyết

# Tìm hiểu về phần mềm TrueCrypt

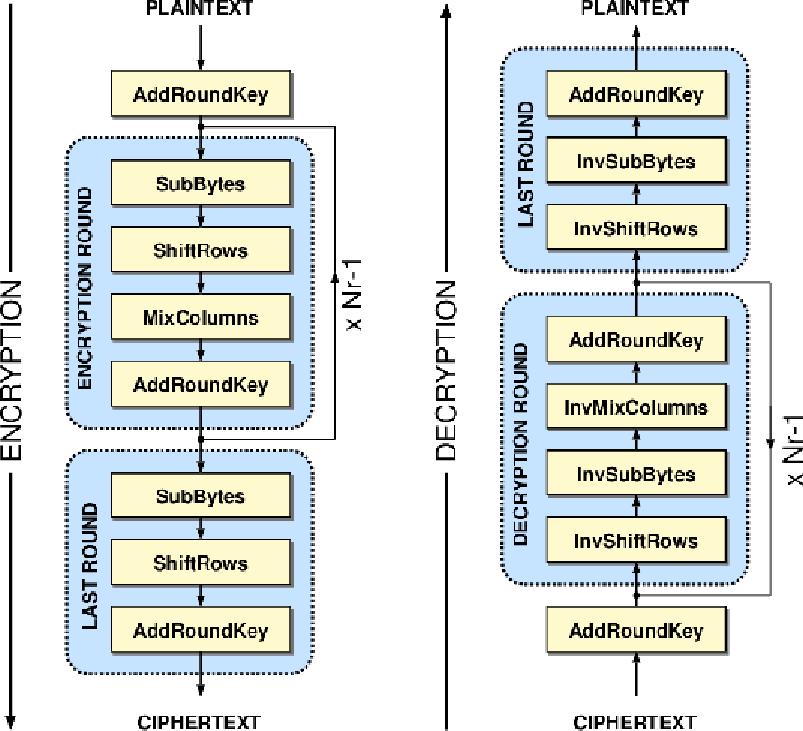
* + - TrueCrypt là một hệ thống phần mềm để thiết lập và duy trì một ổ đĩa được mã hóa nhanh chóng (thiết bị lưu trữ dữ liệu).
    - Mã hóa trực tuyến nghĩa là dữ liệu được mã hóa tự động ngay trước khi được lưu và giải mã ngay sau khi được tải mà không có bất kỳ sự can thiệp nào của người dùng.
    - Không có dữ liệu nào được lưu trữ trên ổ đĩa được mã hóa có thể được đọc (đã giải mã) mà không sử dụng (các) mật khẩu / tệp khóa chính xác hoặc các khóa mã hóa chính xác.
    - Các file có thể được sao chép vào và từ một ổ đĩa TrueCrypt được gắn kết giống như chúng được sao chép vào / từ bất kỳ đĩa thông thường nào (ví dụ: bằng các thao tác kéo và thả đơn giản).
    - Các file sẽ tự động được giải mã một cách nhanh chóng (trong bộ nhớ / RAM) khi chúng đang được đọc hoặc sao chép từ một ổ đĩa TrueCrypt được mã hóa. Tương tự, các tệp đang được ghi hoặc sao chép vào ổ đĩa TrueCrypt sẽ tự động được mã hóa nhanh (ngay trước khi chúng được ghi vào đĩa) trong RAM.

# Giải thuật mã hóa AES

* + - AES được xây dựng dựa trên Rijndael cipher phát triển bởi 2 nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen.
    - Đặc điểm của AES
      * Kích thước khối dữ liệu của AES là 128 bít.
      * Kích thước khóa có thể là 128, 192, hoặc 256 bit.
      * AES được thiết kế dựa trên mạng hoán vị-thay thế (substitution- permutation network) và có thể đạt tốc độ cao trên cả phần mềm và phần cứng
    - AES vận hành dựa trên một ma trận 4x4, được gọi là state.
    - Kích thước của khóa quyết định số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã:
      * 10 vòng lặp với khóa 128 bit
      * 12 vòng lặp với khóa 192 bit
      * 14 vòng lặp với khóa 256 bit
    - Mô tả khái quát giải thuật AES:
      * Mở rộng khóa (KeyExpansion): các khóa phụ dùng trong các vòng lặp được sinh ra từ khóa chính AES sử dụng thủ tục sinh khóa Rijndael.
      * Vòng khởi tạo: AddRoundKey: Mỗi byte trong state được kết hợp với khóa phụ sử dụng XOR.
      * Các vòng lặp chính:
        + Sub-byte: bước thay thế phi tuyến tính, trong đó mỗi byte trong state được thay thế bằng một byte khác sử dụng bảng tham chiếu.
        + ShiftRows: bước đổi chỗ, trong đó mỗi dòng trong state được

dịch một số bước theo chu kỳ

* + - * + MixColumn: trộn các cột trong state, kết hợp 4 bytes trong mỗi cột
        + AddRoundKey
      * Vòng cuối
        + SubBytes
        + ShiftRows
        + AddRoundKey



# Sơ đồ hoạt động của AES

# Cách thức, phương pháp mà TrueCrypt sử dụng để mã hóa file

* + - Các thuật toán mã hóa được TrueCrypt sử dụng trong bảng sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **Thuật toán** | **Người thiết kế** | **Kích thước khóa (bit)** | **Kích thước khối (bit)** |
| AES | J. Daemen, V. Rijmen | 256 | 128 |
| Serpent | R. Anderson, E. Biham, L. Knudsen | 256 | 128 |
| Twofish | B. Schneier, J. Kelsey, D. Whiting,  D. Wagner, C. Hall,  N. Ferguson | 256 | 128 |
| AES-Twofish |  | 256; 256 | 128 |
| AES-Twofish- Serpent |  | 256; 256; 256 | 128 |
| Serpent-AES |  | 256; 256 | 128 |
| Serpent-Twofish- AES |  | 256; 256; 256 | 128 |
| Twofish-Serpent |  | 256; 256 | 128 |

Khi gắn ổ đĩa TrueCrypt hoặc khi thực hiện xác thực trước khi khởi động, các bước sau được thực hiện:

* + - 512 byte đầu tiên của ổ đĩa (tiêu đề ổ đĩa tiêu chuẩn) được đọc vào RAM, trong đó 64 byte đầu tiên là salt. Để mã hóa hệ thống, 512 byte cuối cùng của rãnh ổ đĩa logic đầu tiên được đọc vào RAM.
    - Các byte 65536–66047 của khối lượng được đọc vào RAM. Đối với mã hóa hệ thống, các byte 65536–66047 của phân vùng đầu tiên nằm sau phân vùng hoạt động được đọc.
    - Bây giờ TrueCrypt cố gắng giải mã tiêu đề ổ đĩa tiêu chuẩn đã đọc ở bước 1.

Tất cả dữ liệu được sử dụng và tạo trong quá trình giải mã được lưu trong

RAM (TrueCrypt không bao giờ lưu chúng vào đĩa). Các thông số sau là không xác định và phải được xác định thông qua quá trình thử và sai:

* + - * RF được sử dụng bởi chức năng dẫn xuất khóa tiêu đề có thể là một

trong những chức năng sau: HMAC-SHA-512, HMAC-RIPEMD-160, HMAC-Whirlpool.

* + - * Thuật toán mã hóa: AES-256, Serpent, Twofish, AES-Serpent, AES- Twofish- Serpent ...
      * Phương thức hoạt động: XTS, LRW (không dùng nữa / kế thừa), CBC

(không dùng nữa / kế thừa).

* + - * Kích thước khóa.
    - Giải mã được coi là thành công nếu 4 byte đầu tiên của dữ liệu được giải mã chứa chuỗi ASCII “TRUE” và nếu tổng kiểm tra CRC-32 của 256 byte cuối cùng của dữ liệu được giải mã (tiêu đề tập) khớp với giá trị nằm ở byte # 8 của dữ liệu được giải mã.
    - Bây giờ chúng ta có mật khẩu chính xác, thuật toán mã hóa chính xác, chế độ, kích thước khóa và thuật toán dẫn xuất khóa tiêu đề chính xác.
    - Quy trình mã hóa được khởi động lại bằng khóa chính và khóa chính phụ (chế độ XTS) được truy xuất từ tiêu đề ổ đĩa được giải mã Các khóa này có thể được sử dụng để giải mã bất kỳ khu vực nào của ổ đĩa, ngoại trừ vùng tiêu đề ổ đĩa (hoặc vùng dữ liệu khóa, để mã hóa hệ thống), đã được mã hóa bằng các khóa tiêu đề. Ổ đĩa được gắn.

# Nội dung thực hành

# Tiến hành cài đặt TrueCrypt trên Windows

A screenshot of a computer

Description automatically generated

Chọn Install, nhấn Next

A screenshot of a computer program

Description automatically generated with medium confidence

Quá trình cài đặt diễn ra

A screenshot of a computer program

Description automatically generated with medium confidence

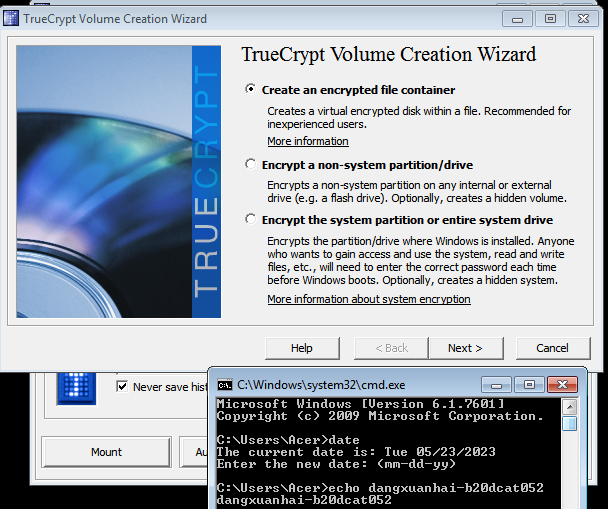
Giao diện chính của ứng dụng sau khi cài đặt thành công

A screenshot of a computer

Description automatically generated

# Sử dụng công cụ TrueCrypt để mã hóa file

* + - Tạo vùng mã hóa chuẩn
      * Tại giao diện chính của TrueCrypt, ta chọn Create Volume
      * Chọn Create an encrypted file container ( Tạo vùng mã hóa dạng tệp)



* + - * Tại mục Volumn Type (Loại vùng mã hóa), ta chọn Standard TrueCrypt volumn

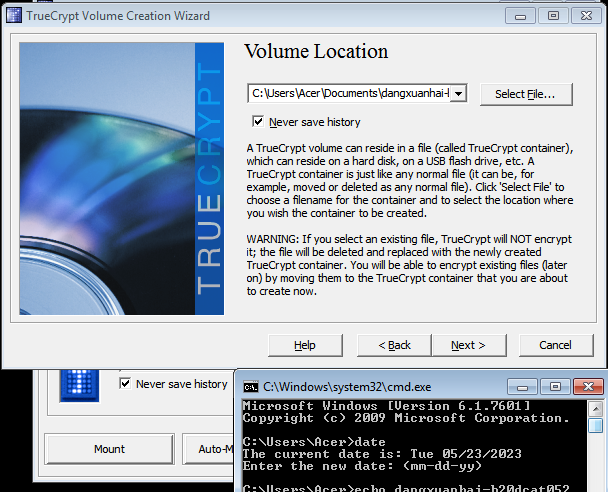
A screenshot of a computer

Description automatically generated

* + - * Chọn vị trí lưu trữ

A screenshot of a computer

Description automatically generated

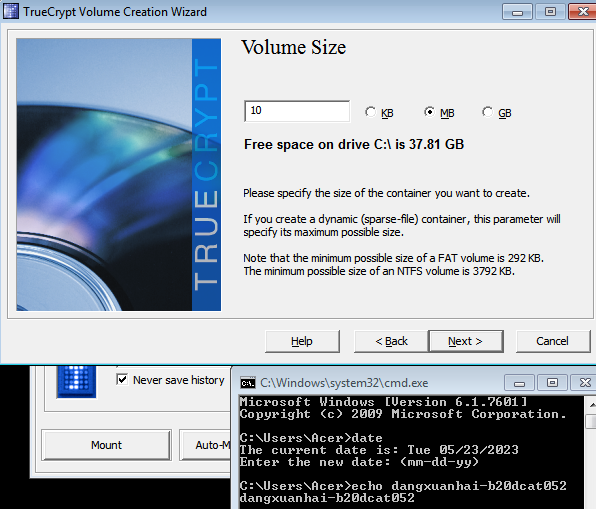


* + - * Tại giao diện tùy chọn mã hóa, thuật toán mã hóa ta chọn AES

A screenshot of a computer

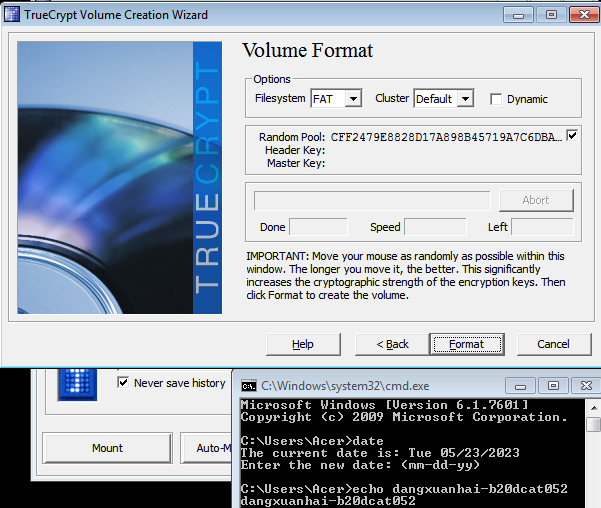
Description automatically generated with medium confidence

* + - * Chọn kích thước vùng mã hóa



* + - * Tạo password cho vùng mã hóaA screenshot of a computer

        Description automatically generated
      * Tạo độ phức tạp cho mã hóa khóa



* + - * Tạo vùng mã hóa thành công

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

* + - Gắn vùng mã hóa chuẩn: gắn (mount) là quá trình làm cho vùng mã hóa sẵn sàng được sử dụng
      * Tại giao diện chính, ta chọn ổ H để gắn vào, chọn đường dẫn tới vùng mã

hóa, chọn Mount để tiến hành gắn file

A screenshot of a computer program

Description automatically generated with medium confidence

* + - * Vùng mã hóa được gắn vào ổ đĩa ảo J: :. Ổ đĩa ảo này hoạt động giống như một ổ đĩa hệ thống bình thường, ngoại trừ một điều là nó được mã hóa toàn bộ nghĩa là một tệp bất kỳ sẽ được mã hóa mỗi khi người dùng sao chép, di chuyển hoặc lưu nó vào trong ổ đĩa ảo này.

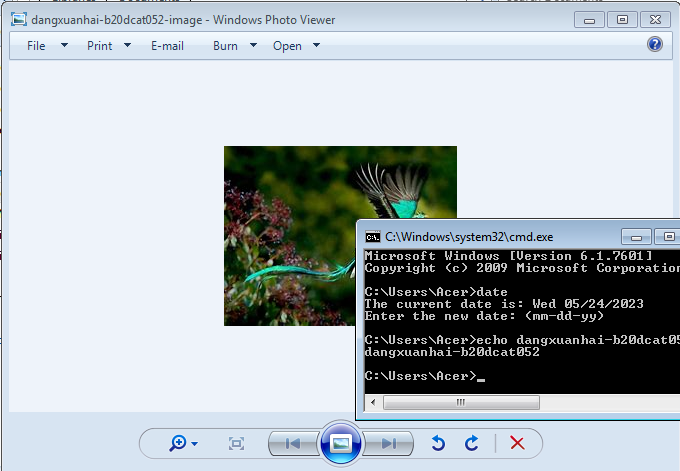
A computer screen shot of a computer

Description automatically generated with low confidence

* + - * Tạo một folder chứ file văn bản và file phương tiện (ảnh)

A picture containing text, electronics, screenshot, software

Description automatically generated

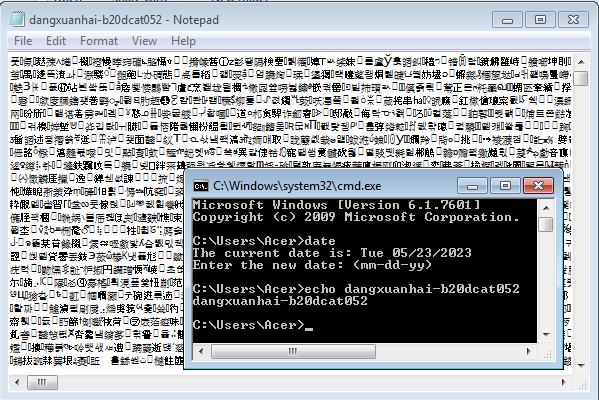


* Gỡ vùng mã hóa chuẩn
  + - * Tại giao diện chính, ta chọn Dismount, vùng mã hóa sẽ được khóa lại

A screenshot of a computer

Description automatically generated

* + - * Khi người dùng truy cập từ bên ngoài thì sẽ không thể xem được, tức file đã được mã hóa => mã hóa thành công



A screenshot of a computer

Description automatically generated

* 1. Sao lưu khóa mã hóa của công cụ TrueCrypt
* Tại giao diện chính, chọn Volume Tool -> Chọn Backup Volumn Header. Header là nơi lưu trữ khóa

A picture containing text, screenshot, software, computer icon

Description automatically generated

* Chọn The volumn does not contain a hidden volumn

A picture containing text, screenshot, software, display

Description automatically generated

* Tạo file backup

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated with medium confidence

* Sao lưu khóa thành công

A screenshot of a computer

Description automatically generated

# Tài liệu tham khảo

* 1. [How to Encrypt Your Files With TrueCrypt (lifewire.com)](https://www.lifewire.com/how-to-encrypt-your-files-with-truecrypt-2377854)
  2. [Microsoft Word - TrueCrypt tutorial.docx (gbls.org)](https://www.gbls.org/sites/default/files/2018-02/TruCrypt%20Tutorial.pdf)
  3. [Encryption Scheme - Truecrypt (truecrypt71a.com)](https://www.truecrypt71a.com/documentation/technical-details/encryption-scheme/)
  4. Đỗ Xuân Chợ, Bài giảng Mật mã học cơ sở, Học viện Công Nghệ Bưu Chính Viễn Thông, 2021.