

Bài 9. Một số công cụ mã hóa

Học phần: ĐẢM BẢO VÀ AN TOÀN THÔNG TIN

NỘI DUNG

Bài 1: Tìm hiểu công cụ Bitlocker

Bài 2: Tìm hiểu công cụ TrueCrypt

Bài 3: Thư viện OpenSSL

Bài 4: Giáo viên giao bài tập lớn theo danh sách kèm theo. (30p cuối giờ)

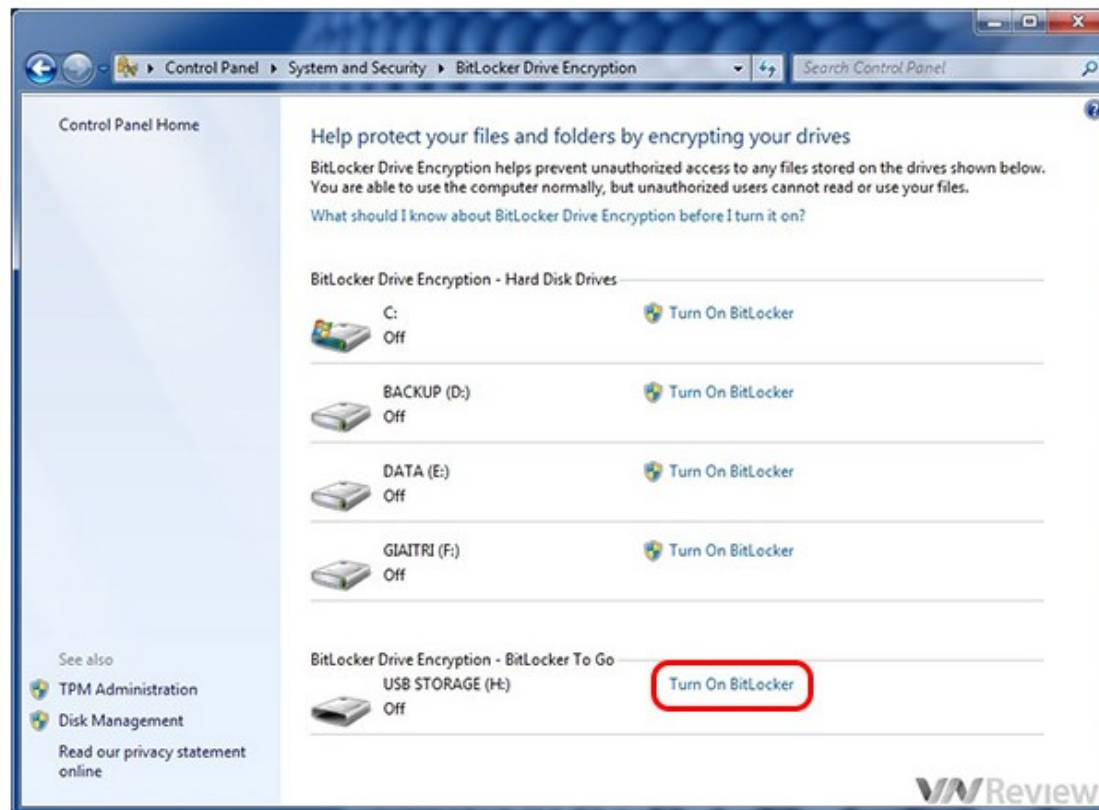
Bài 1: Tìm hiểu công cụ Bitlocker

BitLocker là gì?

BitLocker là chương trình mã hóa độc quyền, để sử dụng của Microsoft dành cho Windows có thể mã hóa toàn bộ ổ đĩa của bạn cũng như giúp bảo vệ chống lại những thay đổi trái phép vào hệ thống, chẳng hạn như phần mềm độc hại cấp firmware.

Bài 1: Tìm hiểu công cụ Bitlocker

1) Cắm USB muốn mã hóa vào máy
Vào Control Panel > System and Security > BitLocker Drive Encryption > mở ra bảng chứa các ổ cứng và ổ USB trên máy > chọn ổ USB muốn mã hóa > Turn On BitLocker



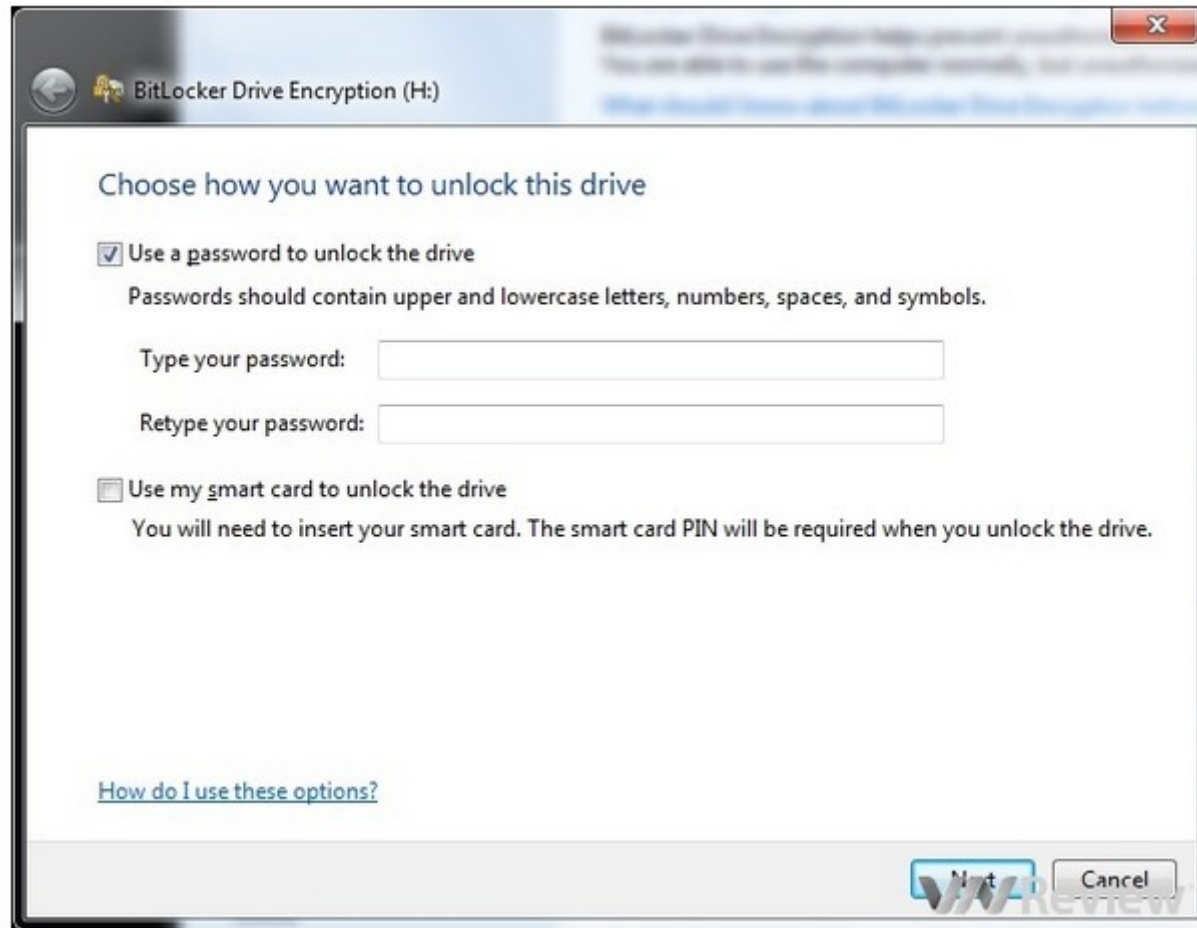
Bài 1: Tìm hiểu công cụ Bitlocker

2) Hộp thoại mới hiện ra với hai lựa chọn để check vào:

- Use a password to unlock the drive: Lựa chọn này cho phép bạn sử dụng mật khẩu để mở ổ mã hóa, cần nhập chính xác mật khẩu vào hai ô trống bên dưới
- Use my smart card to unlock the drive: sử dụng thẻ thông minh để mở ổ mã hóa. Cần cắm thẻ vào máy để xác nhận

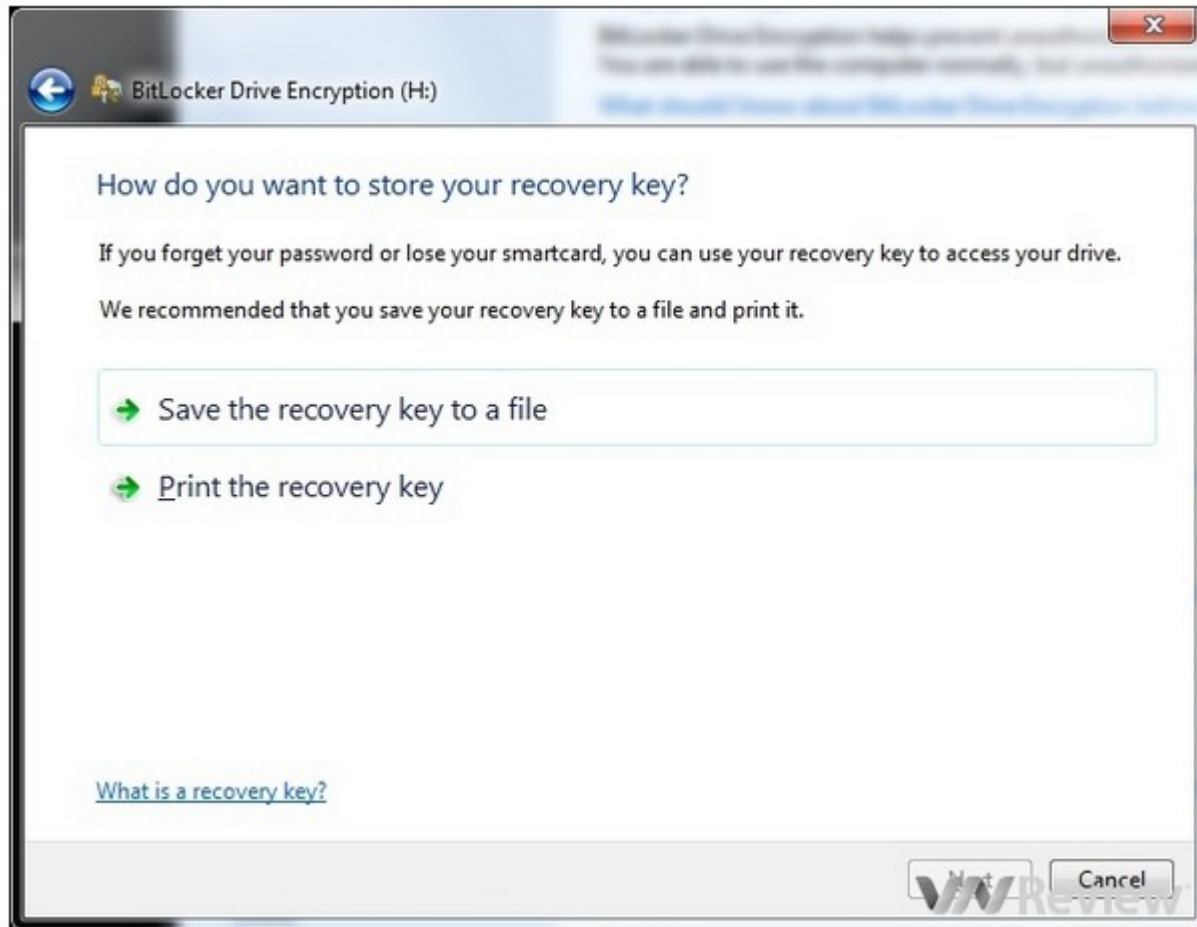
Bài 1: Tìm hiểu công cụ Bitlocker

2) Hộp thoại mới hiện ra với hai lựa chọn để check vào:



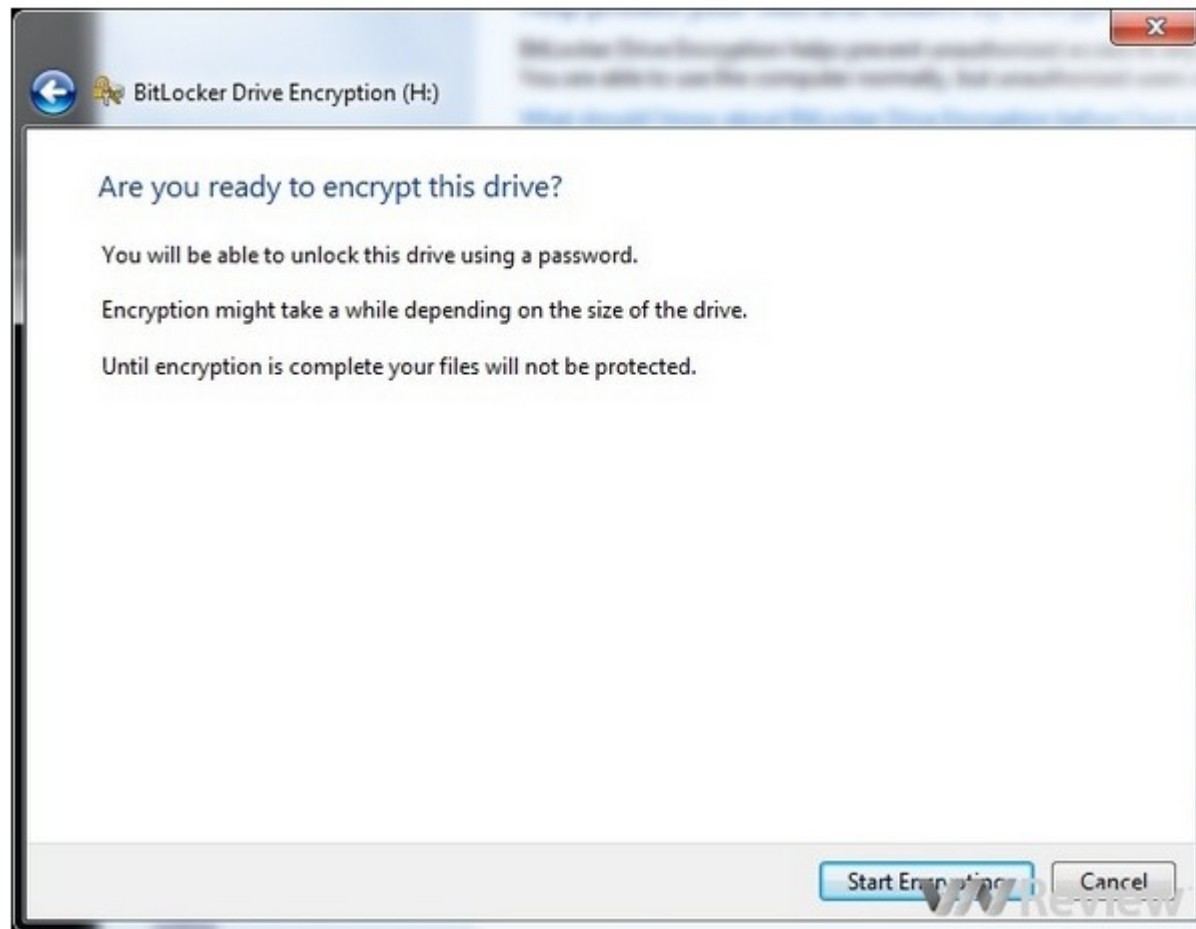
Bài 1: Tìm hiểu công cụ Bitlocker

3) Hộp thoại khác hiện ra yêu cầu bạn chọn "lưu giữ key phục hồi" hoặc "in key phục hồi"



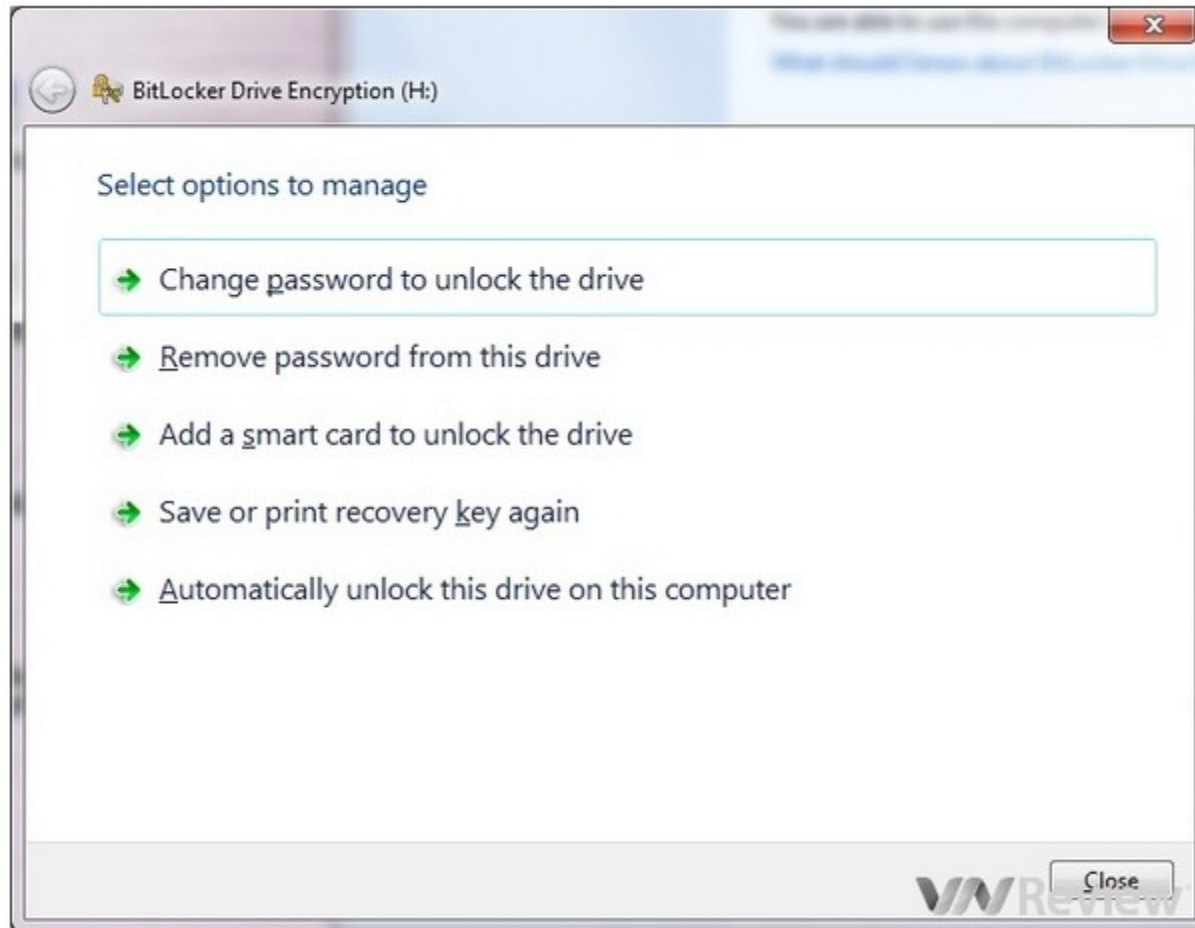
Bài 1: Tìm hiểu công cụ Bitlocker

4) Hộp thoại mới hiện ra hỏi bạn có sẵn sàng để mã hóa ổ này > bấm Start Encrypting để bắt đầu



Bài 1: Tìm hiểu công cụ Bitlocker

5) Quản lý bitlocker



Bài 1: Tìm hiểu công cụ Bitlocker

6) Tắt BitLocker

1) Cắm ổ USB đã mã hóa vào máy

2) Nhập mật khẩu BitLocker rồi ấn Unlock

3) Vào Control Panel > System and Security > BitLocker Drive Encryption > mở ra bảng chứa các ổ cứng và ổ USB trên máy > chọn ổ USB trước đó đã Unlock > Turn Off BitLocker

Bài 2: Tìm hiểu công cụ TrueCrypt

- TrueCrypt là chương trình giúp bảo mật các tệp bằng các ngăn cản các truy cập nếu không có mật khẩu hợp lệ.
- TrueCrypt giúp bạn tạo ra những vùng mã hóa trên máy tính nơi bạn có thể lưu trữ các tệp một cách an toàn.
- Khi bạn tạo hoặc lưu dữ liệu trong các vùng mã hóa, TrueCrypt sẽ tự động mã hóa mọi thông tin trong vùng đó.
- Khi bạn mở hoặc lấy thông tin ra, chương trình sẽ tự động giải mã. Quy trình này gọi là tiến trình mã hóa-tức thời.

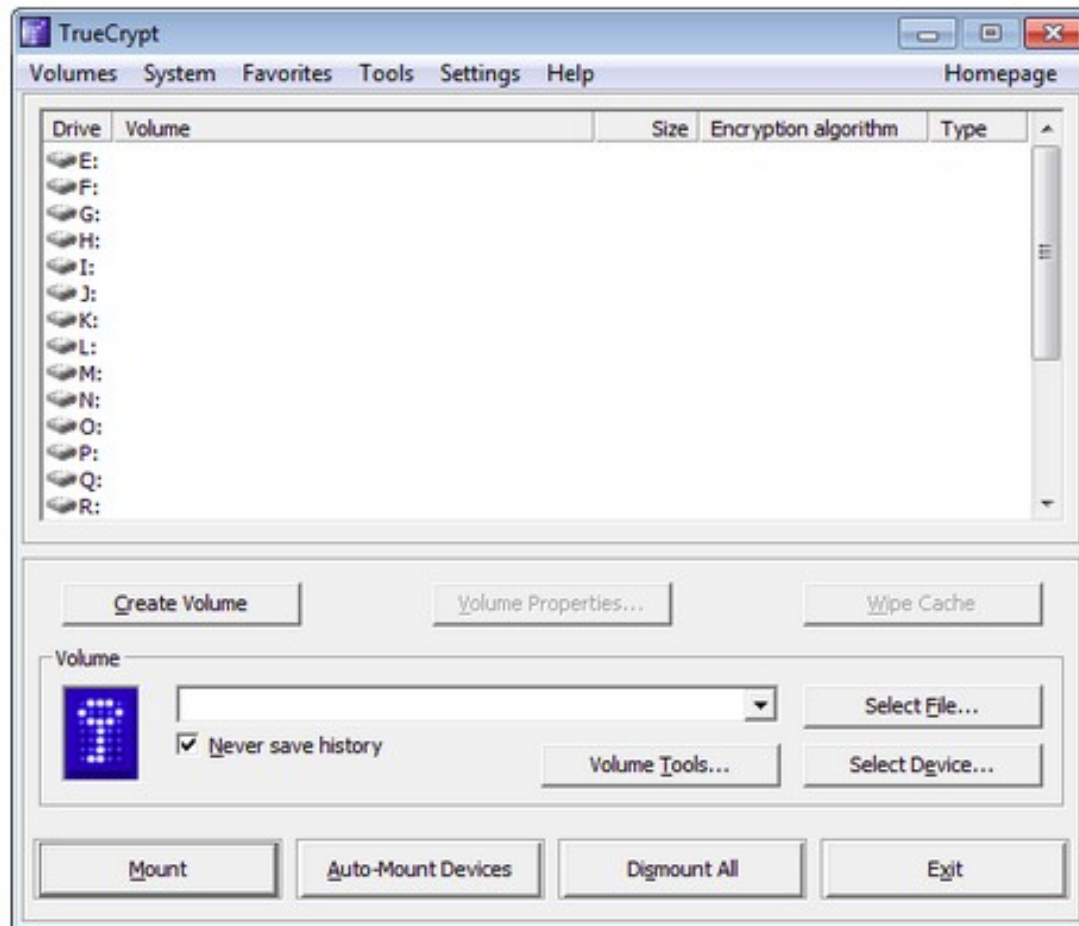
Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 1:

Đầu tiên chúng ta tải về phần mềm và cài đặt trên máy tính của mình. Các bạn có thể tải TrueCrypt từ địa chỉ:
<http://truecrypt.sourceforge.net/OtherPlatforms.html>

Bài 2: Tìm hiểu công cụ TrueCrypt

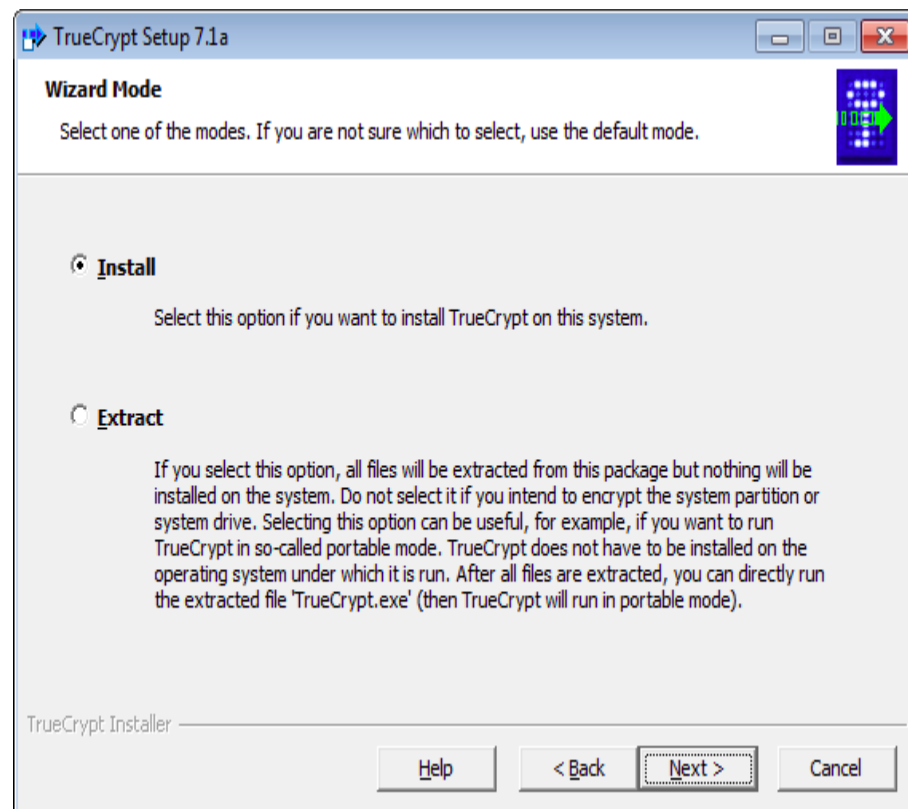
Bước 2: Chọn một ổ đĩa trong danh sách để lưu trữ các tài liệu mã hóa, sau đó bấm Create Volume.



Bài 2: Tìm hiểu công cụ TrueCrypt

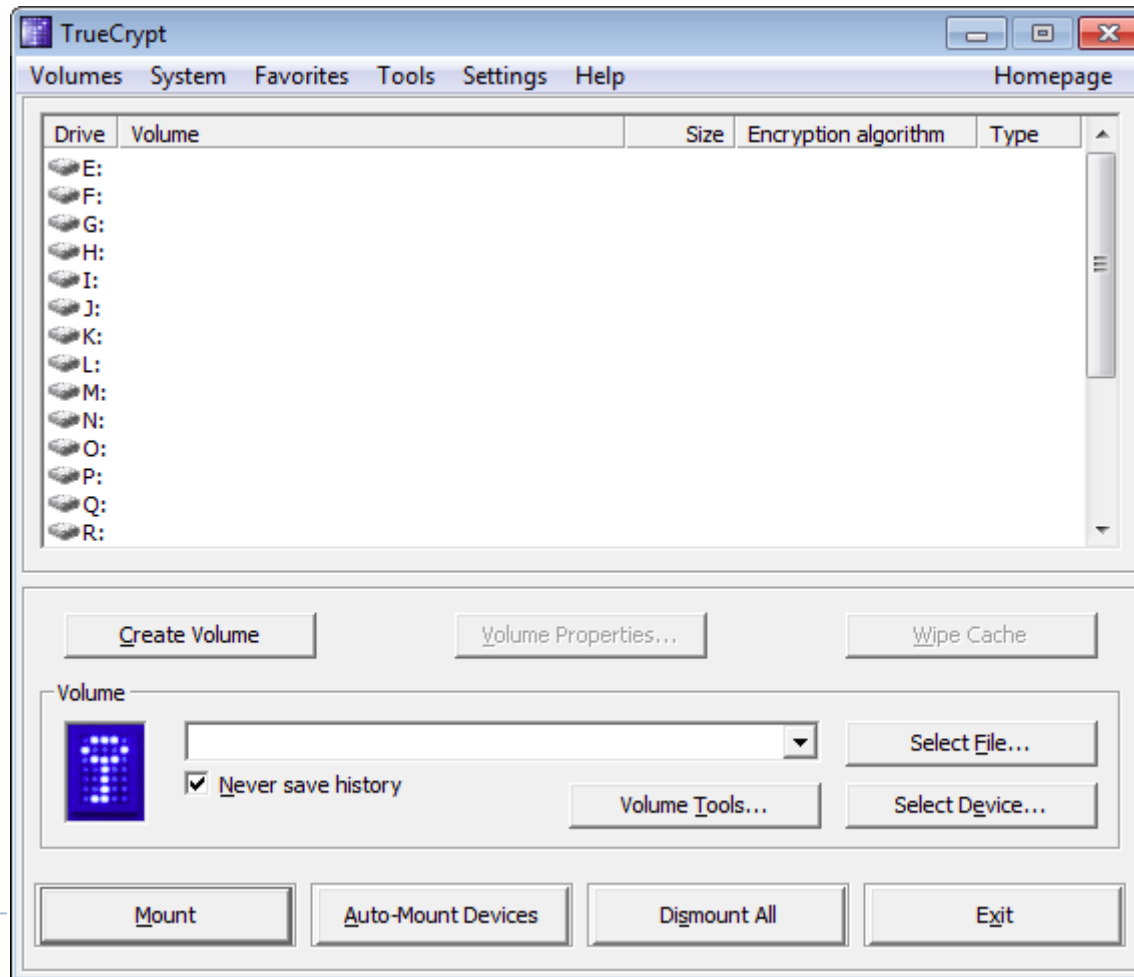
Bước 3: chọn Install rồi bấm Next.

- Install: Lựa chọn này dành cho những người dùng không cần che dấu việc sử dụng chương trình TrueCrypt trên máy tính.
- Extract: Lựa chọn này dành cho người dùng muốn lưu phiên bản chạy không cần cài đặt của TrueCrypt trên một thẻ nhớ USB và không muốn cài đặt TrueCrypt vào máy tính.



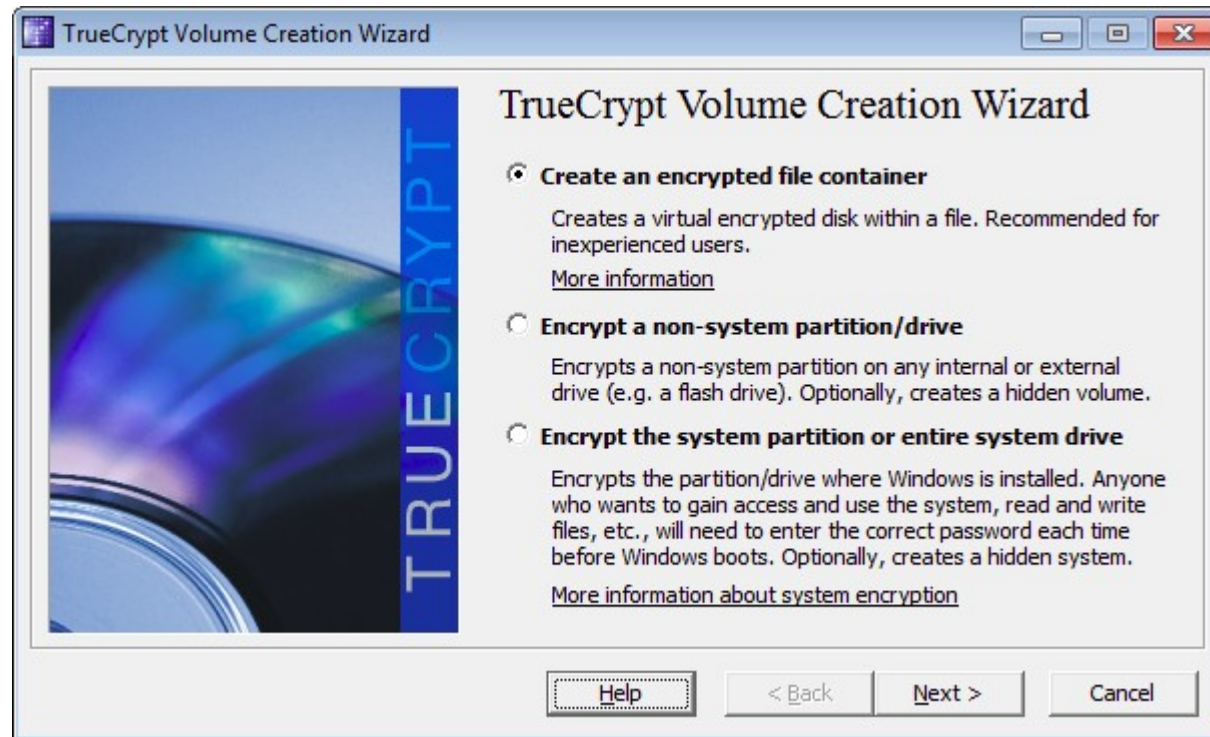
Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 2: Chọn một ổ đĩa trong danh sách để lưu trữ các tài liệu mã hóa, sau đó bấm Create Volume.



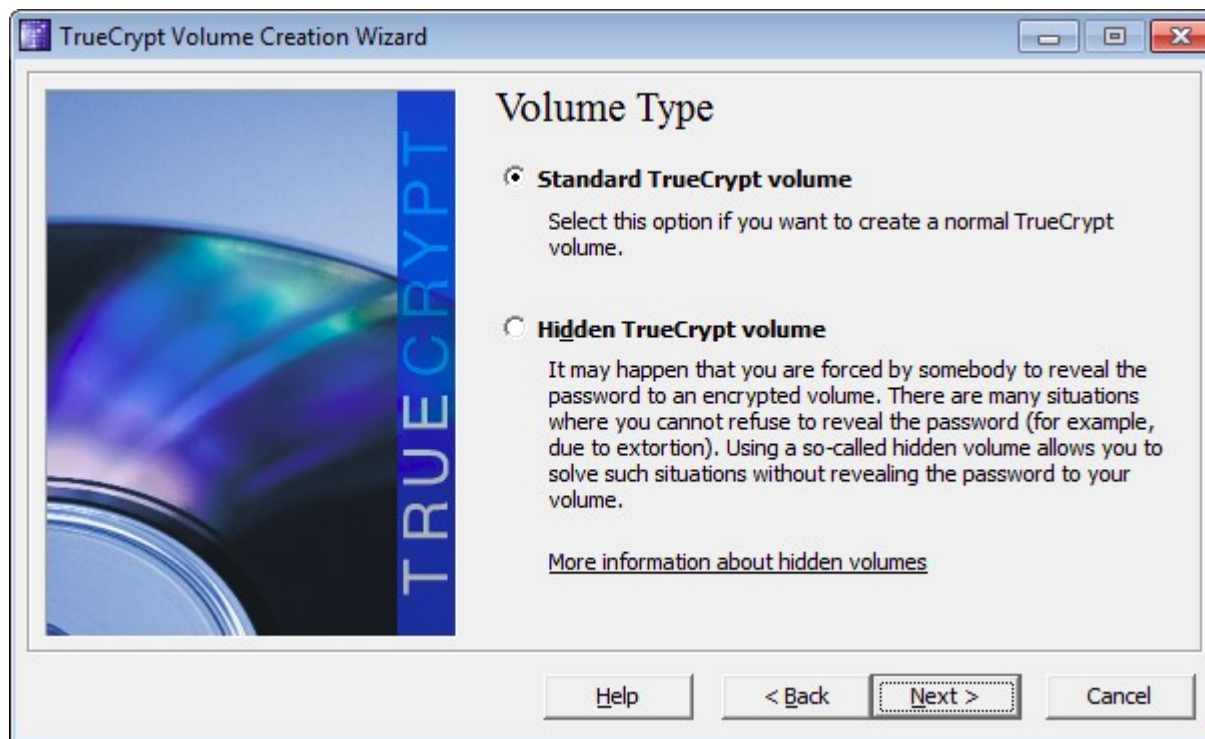
Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 3: Có ba lựa chọn mã hóa một Vùng Mã hóa Chuẩn. Trong phần này, chúng ta sẽ tạo một encrypted file container (vùng mã hóa dạng tệp). Bấm Next.



Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 4: Có 2 lựa chọn tạo vùng mã hóa chuẩn hoặc vùng mã hóa ẩn. Chọn Standard TrueCrypt volume rồi bấm Next.



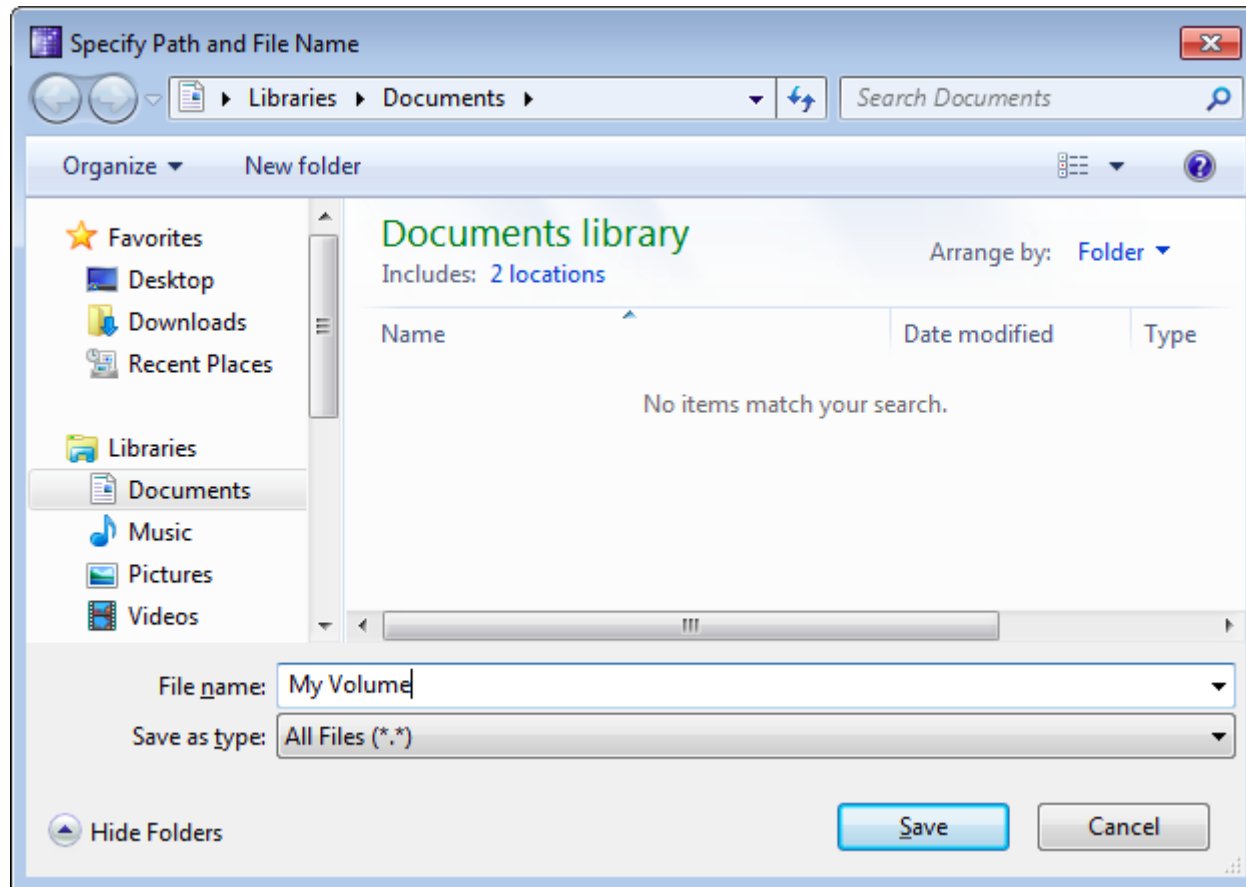
Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 5: chọn nơi lưu trữ, nhập tên tệp vào ô trống hoặc nhấn Select File...



Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 6: Chọn tên một Vùng Mã hóa chuẩn



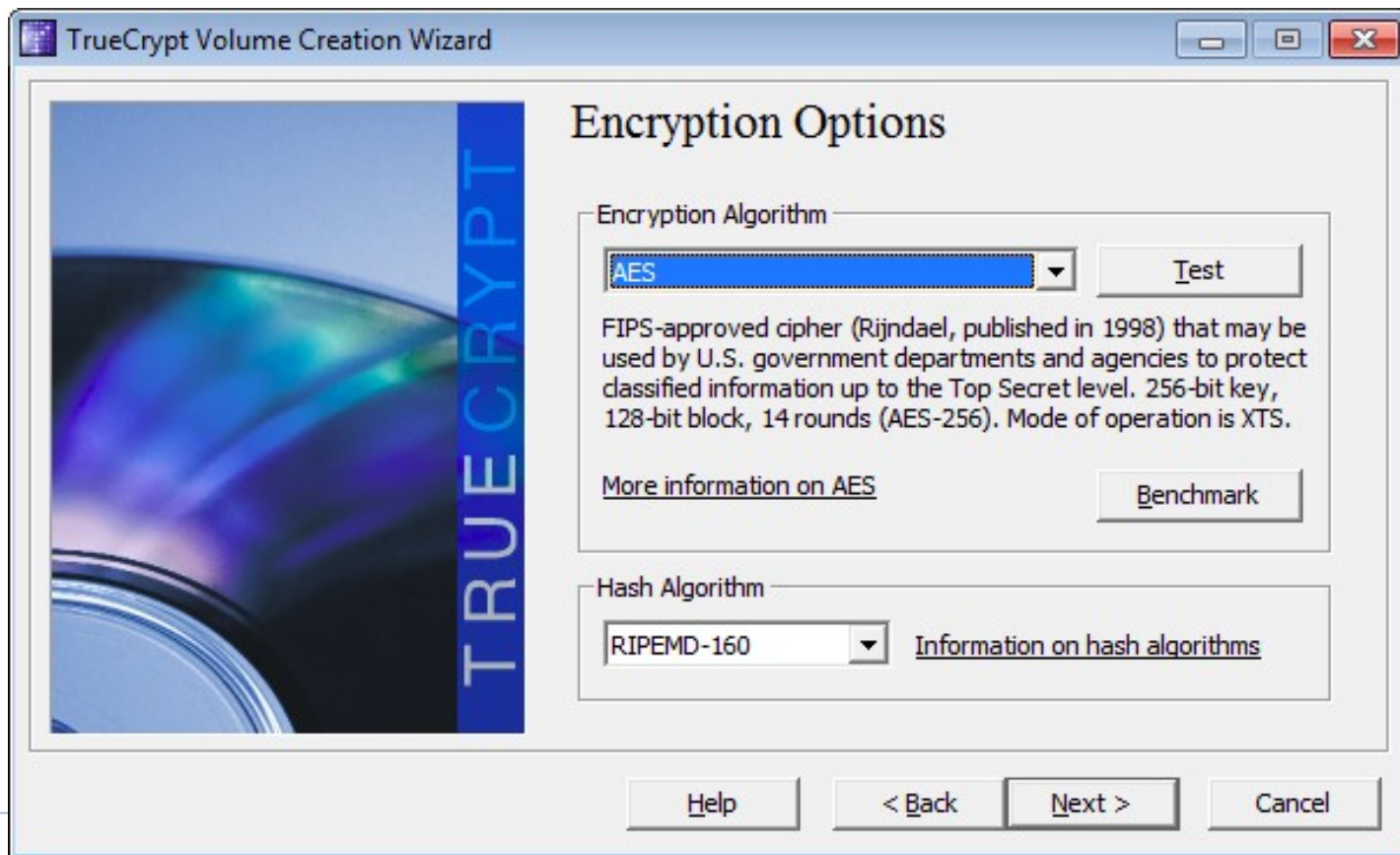
Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 7: bấm Next.



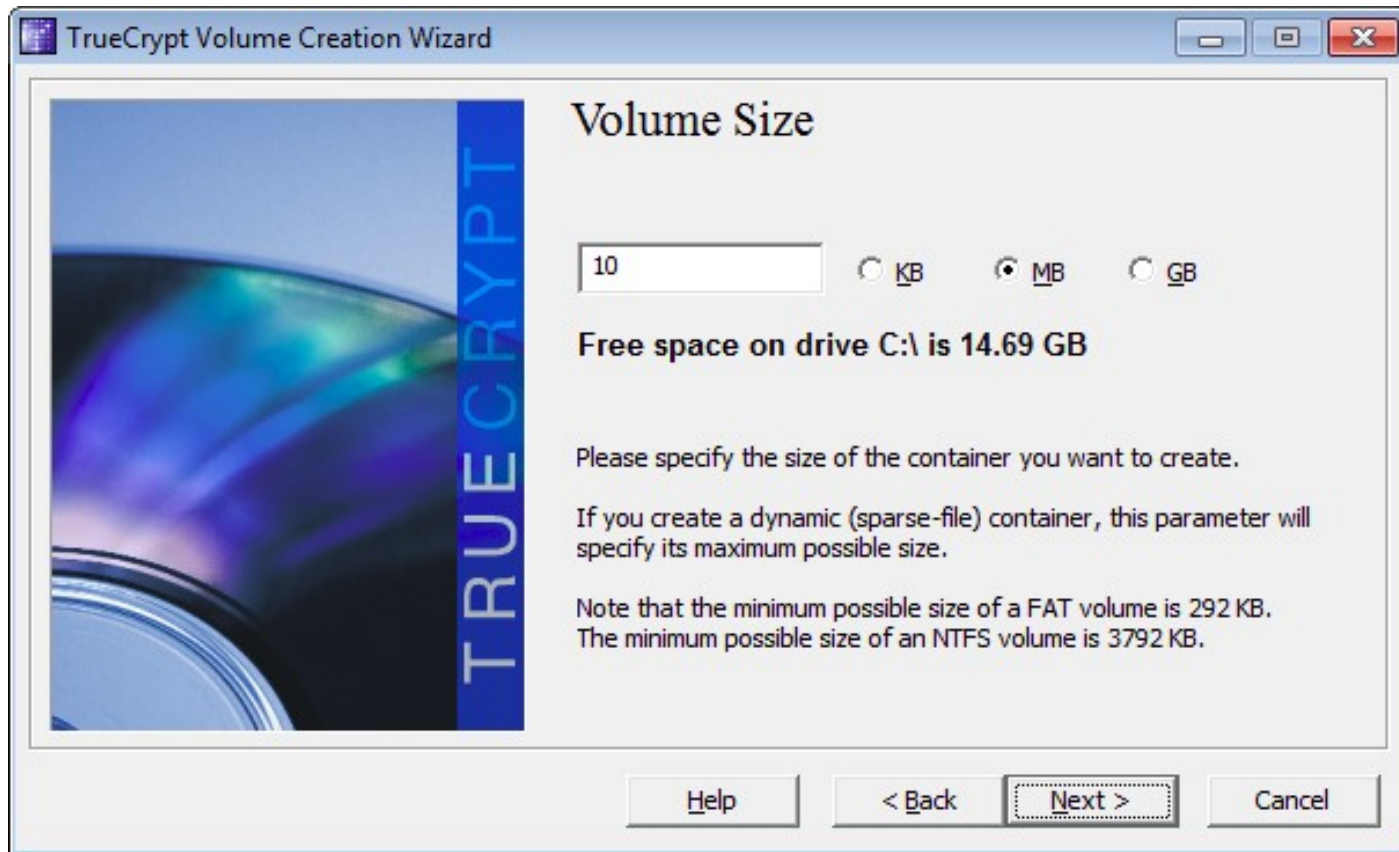
Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 8: chọn một phương pháp mã hóa cho Vùng Mã hóa Chuẩn trong danh sách. Nhấn Next để mở cửa sổ TrueCrypt Volume Creation Wizard



Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 9: Cửa sổ Volume Creation Wizard cho phép bạn xác định kích thước Vùng mã hóa.



Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 10: Nhập và xác nhận mật khẩu.



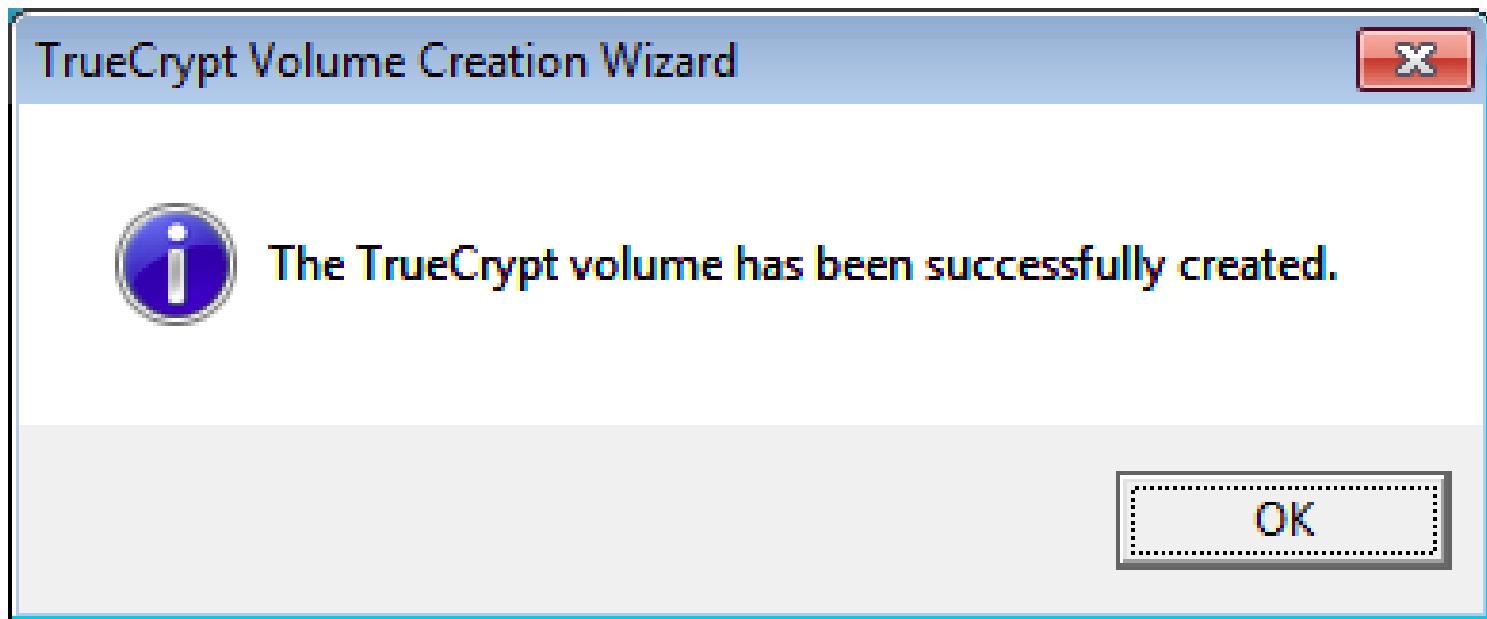
Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 11: Trong cửa sổ này, TrueCrypt sẽ tiến hành tạo Vùng mã hóa Chuẩn. Di chuyển con trỏ chuột một cách ngẫu nhiên trong cửa sổ TrueCrypt Volume Creation Wizard trong khoảng ít nhất 30 giây. Bạn càng di chuyển chuột càng lâu càng tốt. Việc này giúp tăng độ phức tạp của khóa mã hóa.



Bài 2: Tìm hiểu công cụ TrueCrypt

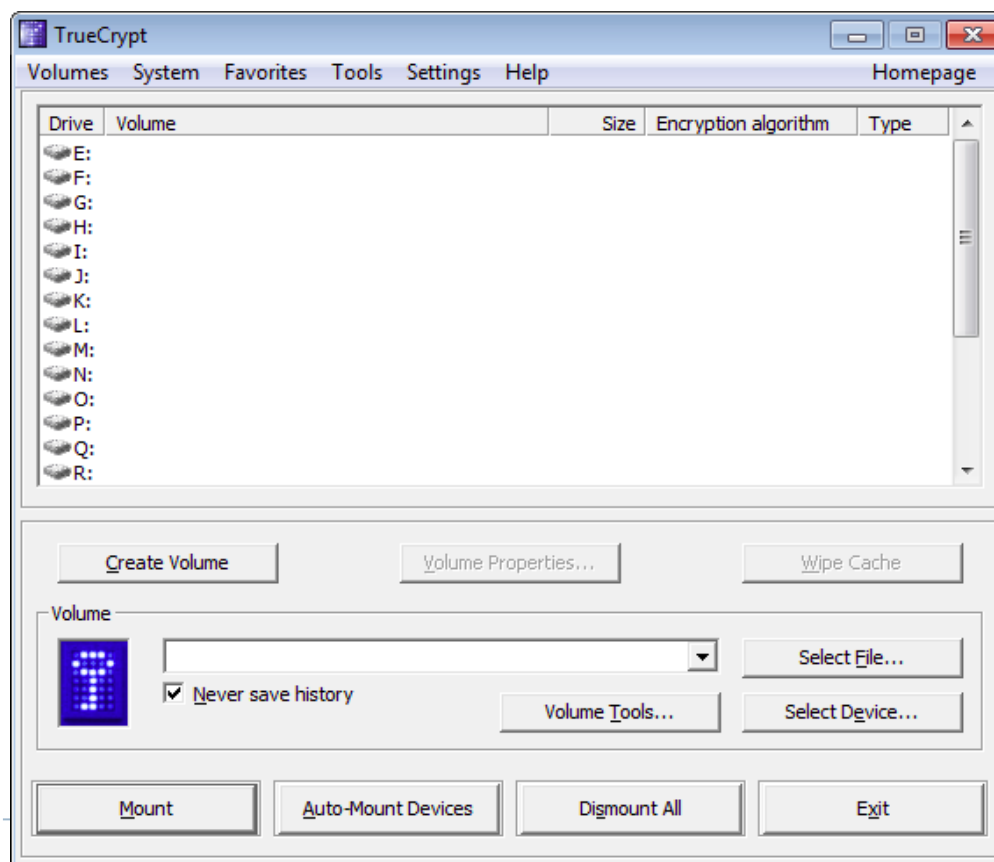
Bước 12: với những chọn lựa ở trên, TrueCrypt sẽ tạo một tệp có tên là My Volume trong thư mục My Documents



Bài 2: Tìm hiểu công cụ TrueCrypt

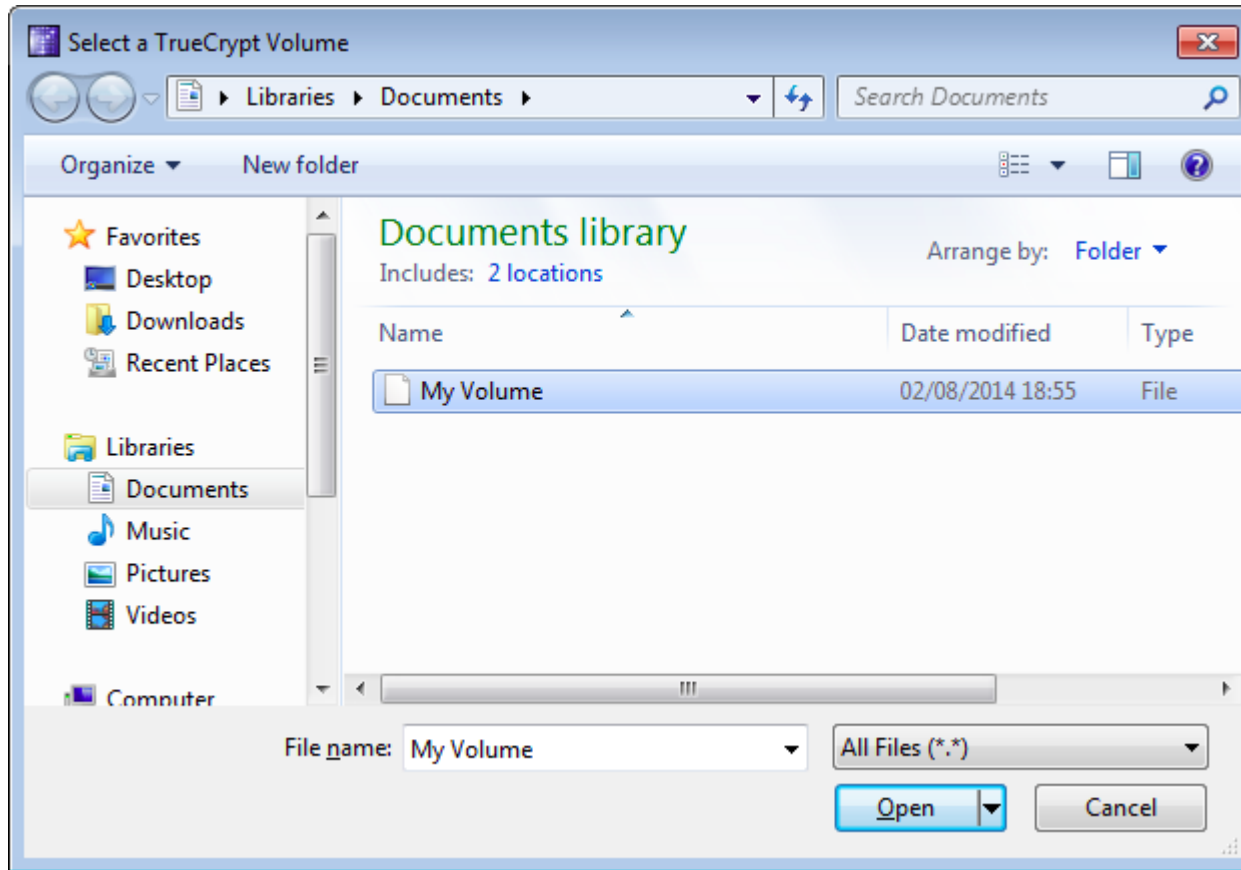
Hướng dẫn gắn vùng Mã hóa chuẩn

Bước 1: Chọn một ổ đĩa trong danh sách như bên dưới. Nhấn Select File...



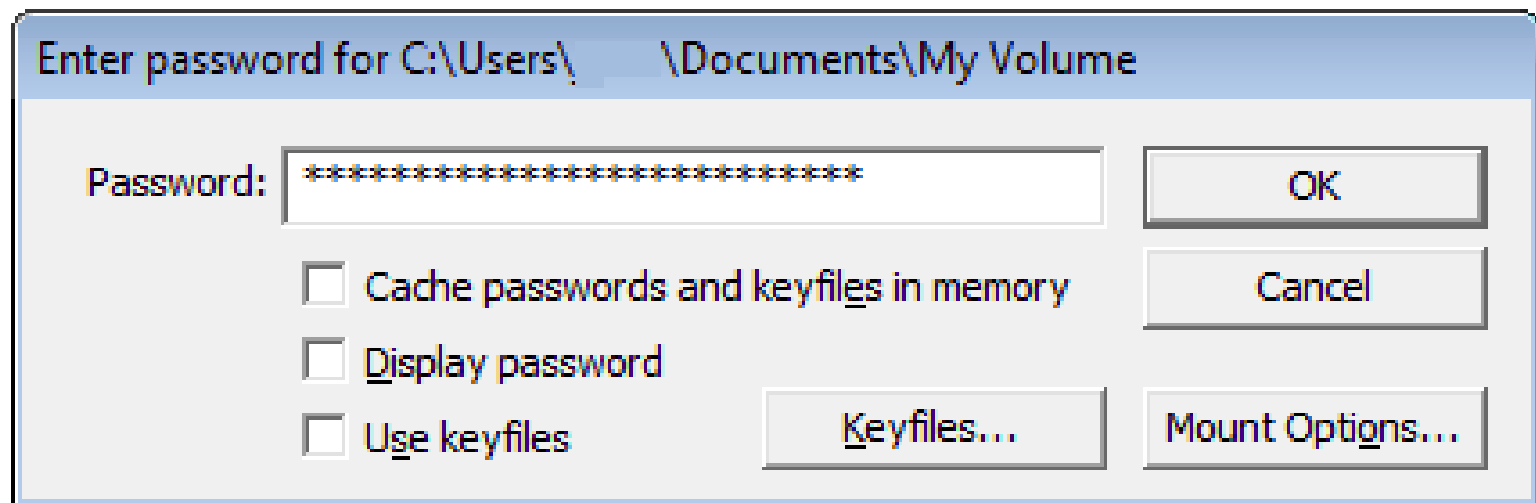
Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 2: Chọn một tệp Vùng mã hóa bạn đã tạo, và nhấn












Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 3: Nhấn Mount để kích hoạt cửa sổ Nhập mật mã như sau, nhập mật khẩu vào ô trống, bấm OK.



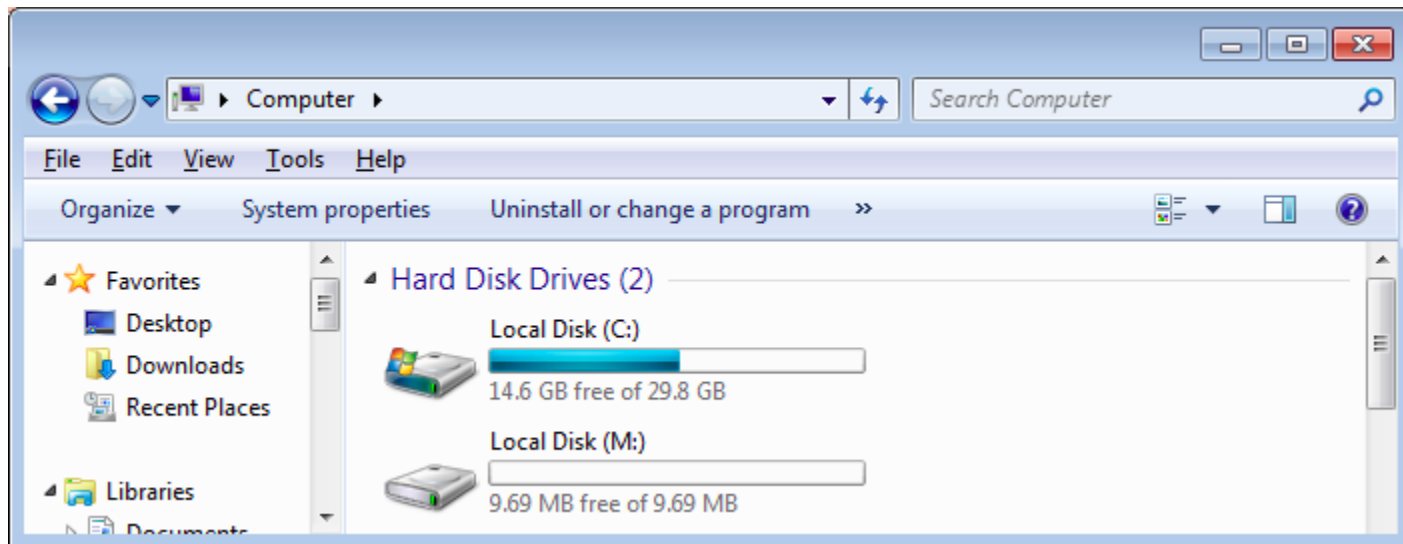
Bài 2: Tìm hiểu công cụ TrueCrypt

Nếu mật khẩu nhập vào không đúng, TrueCrypt sẽ thông báo và bạn cần nhập lại mật khẩu và nhấn OK. Nếu mật khẩu thích hợp, Vùng mã hóa Chuẩn sẽ được gắn vào hệ thống như sau:

Drive	Volume	Size	Encryption algorithm	Type
 E:				
 F:				
 G:				
 H:				
 I:				
 J:				
 K:				
 L:				
 M:	C:\Users\ \Documents\My Volume	9.8 MB	AES	Normal

Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 5: Nhấn đúp chuột vào mục đánh dấu trong cửa sổ TrueCrypt hoặc nhấn đúp chuột vào ký tự ổ đĩa tương ứng trong My Computer để mở Vùng mã hóa đã được gắn vào ổ đĩa M: trên máy tính của bạn.












Bài 2: Tìm hiểu công cụ TrueCrypt

- Chúng ta vừa gắn thành công Vùng mã hóa My Volume thành ổ đĩa ảo M
 - 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.
 - Một tệp bất kỳ sẽ được mã hóa mỗi khi được sao chép, di chuyển hoặc lưu nó vào trong ổ đĩa ảo này (tiến trình này gọi là sự mã hóa tức thời).
 - Khi di chuyển một tệp ra khỏi Vùng mã hóa, nó sẽ tự động được giải mã hóa.
 - Ngược lại, nếu bạn chuyển một tệp vào trong Vùng mã hóa, TrueCrypt sẽ tự động mã hóa nó.
 - Nếu máy tính của bạn bị treo hay tự nhiên bị tắt, TrueCrypt sẽ ngay lập tức đóng Vùng mã hóa lại.
-

Bài 2: Tìm hiểu công cụ TrueCrypt

Hướng dẫn gỡ một vùng mã hóa chuẩn

Bước 1: Chọn ổ muốn gỡ từ danh sách các ổ được gắn vào hệ thống trong cửa sổ TrueCrypt.

Drive	Volume	Size	Encryption algorithm	Type
 E:				
 F:				
 G:				
 H:				
 I:				
 J:				
 K:				
 L:				
 M:	C:\Users\ \Documents\My Volume	9.8 MB	AES	Normal

Bước 2: Nhấn Dismount để gỡ (hay đóng) một Vùng mã hóa TrueCrypt.

Bài 2: Tìm hiểu công cụ TrueCrypt

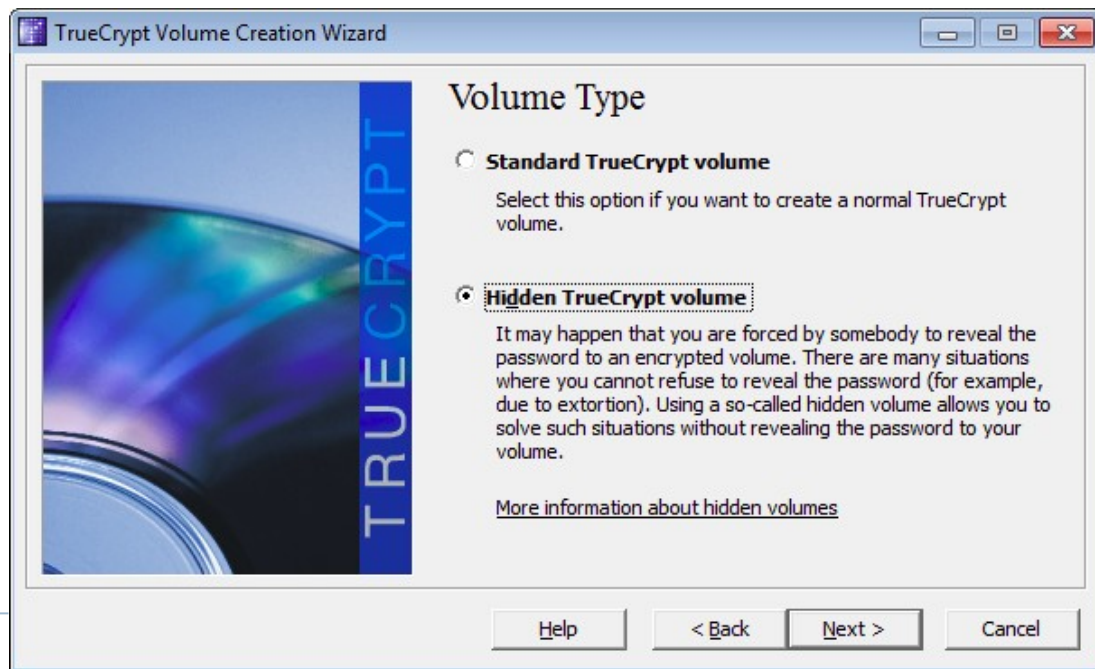
Hướng dẫn tạo vùng mã hóa ẩn

Bước 1: Khởi động chương trình TrueCrypt

Bước 2: Nhấn Create volume để mở TrueCrypt Volume Creation Wizard.

Bước 3: Nhấn Next để chọn lựa chọn mặc định Create an encrypted file container.

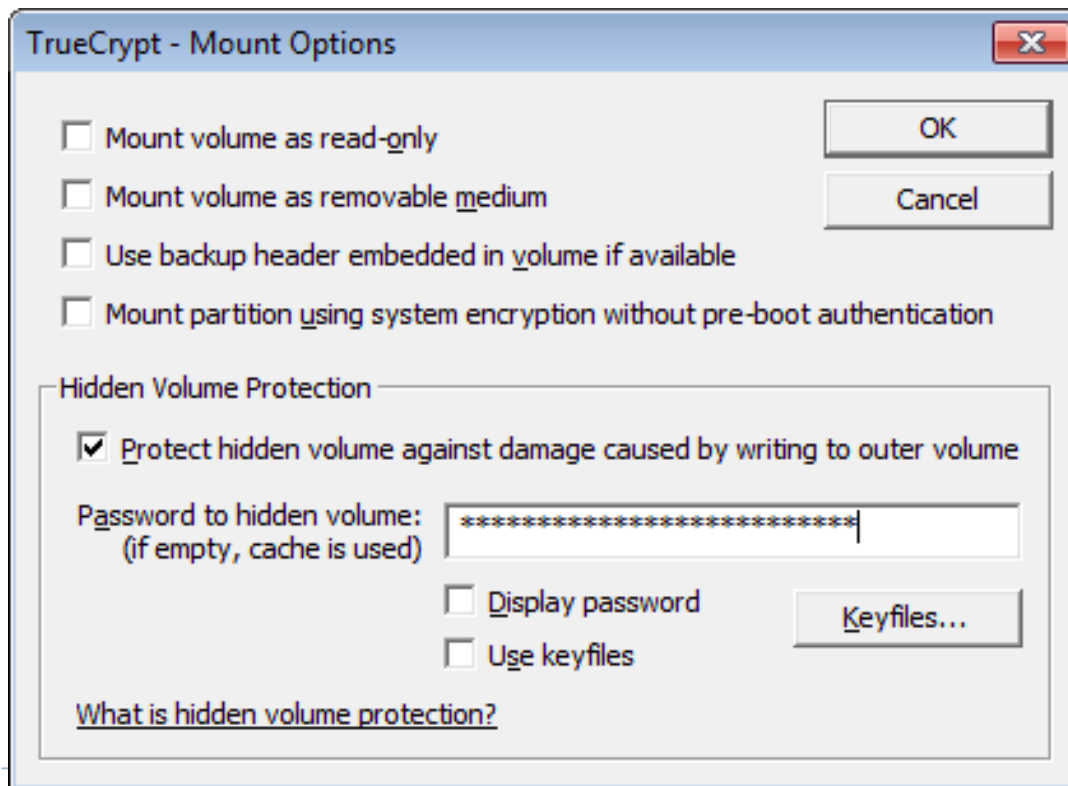
Bước 4: bấm chọn Hidden TrueCrypt volume. Sau đó bấm Next.



Bài 2: Tìm hiểu công cụ TrueCrypt

Để sử dụng tính năng Bảo vệ Vùng mã hóa Ẩn, thực hiện các bước sau

Bước 1: Nhấn Mount options trên cửa sổ Nhập Mật khẩu. Cửa sổ Tùy chọn Gắn sẽ xuất hiện như sau:



Bài 2: Tìm hiểu công cụ TrueCrypt

Bước 2: Lựa chọn Protect hidden volume against damage caused by writing to outer volume.

Bước 3: Nhập mật khẩu của Vùng mã hóa Ẩn và nhấn OK.

Bước 4: Nhấn Mount để gắn Vùng mã hóa Chuẩn. Sau khi việc gắn thành công bạn có thể thêm các ‘tệp mới’ mà không lo làm hỏng Vùng mã hóa Ẩn

Bước 5: Nhấn Dismount để đóng vùng mã hóa chuẩn, sau khi bạn thực hiện xong việc thay đổi nội dung bên trong đó

Bài 3: Thư viện OpenSSL

1. Lệnh đơn giản để mã hóa tập tin với OpenSSL là:

openssl aes-256-cbc -a -salt -in gocit.txt -out gocit.txt.enc

- Trong đó:

aes-256-cbc : encryption cipher được sử dụng để mã hóa.

-a : xuất kết quả đã mã hóa dưới dạng base64 encoded.

-salt: thêm độ mạnh mã hóa

-in gocit.txt : đường dẫn tập tin cần mã hóa

-out gocit.txt.enc : đường dẫn để lưu tập tin đã được mã hóa

Khi lệnh trên được thực thi OpenSSL sẽ hỏi mật khẩu để mã hóa.

Bài 3: Thư viện OpenSSL

2. Để giải mã tập tin đã mã hóa sử dụng lệnh sau:

*openssl aes-256-cbc -d -a -in gocit.txt.enc -out
gocit.txt.new*

- Trong đó:
- d : ra lệnh cho OpenSSL giải mã tập tin
- a : thông báo cho OpenSSL dữ liệu đầu vào ở trong dạng base64 encoded

Các thông số khác tương tự câu lệnh mã hóa trên.

OpenSSL sẽ hỏi mật khẩu đã dùng mã hóa để giải mã tập tin. Sau khi giải mã thu được tập tin gocit.txt.new (theo ví dụ trên)

Bài 3: Thư viện OpenSSL

2. Để giải mã tập tin đã mã hóa sử dụng lệnh sau:

openssl aes-256-cbc -d -a -in gocit.txt.enc -out gocit.txt.new

- Trong đó:
- d : ra lệnh cho OpenSSL giải mã tập tin
- a : thông báo cho OpenSSL dữ liệu đầu vào ở trong dạng base64 encoded

Các thông số khác tương tự câu lệnh mã hóa trên.

OpenSSL sẽ hỏi mật khẩu đã dùng mã hóa để giải mã tập tin. Sau khi giải mã thu được tập tin gocit.txt.new (theo ví dụ trên)

Bài 3: Thư viện OpenSSL

3. Tạo CSR(Certificate Signing Request) trong việc cài đặt chứng chỉ số SSL

Sinh viên tự tìm hiểu

HỎI VÀ ĐÁP