Module 18
Cryptography

Các Chủ Đề Chính Trong Chương Này

Giới Thiệu Cryptography

Tổng Quan Về Mã Hóa

Các Thuật Toán Băm

Public Key Infrastructure

Chữ Ký Số

Mã Hóa Dữ Liệu Trên ổ Cứng

Truecrypt

Cryptography Là Gì

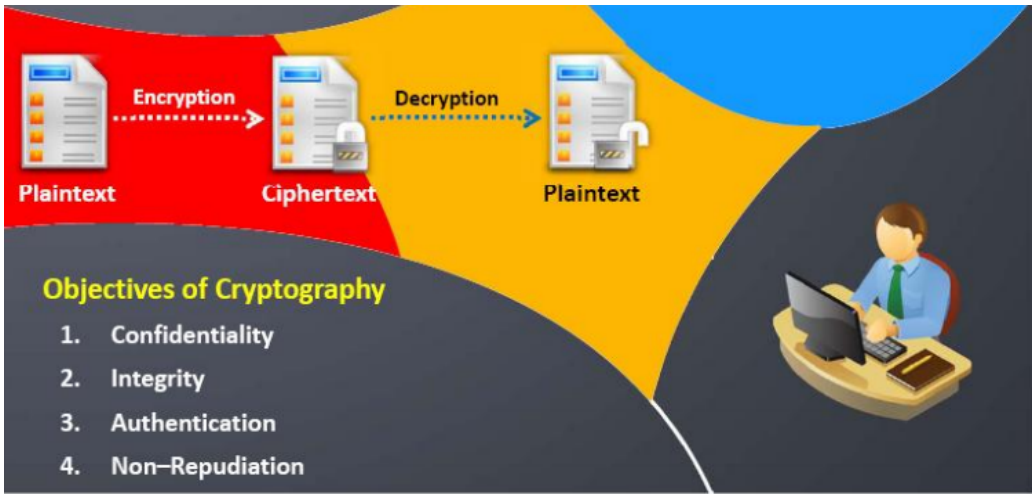
An toàn thông tin là bảo vệ các đặc tính riêng tư (confidentialy), toàn vẹn (intergrity) và khả dụng (availabilty) của thông tin.

- C : (confidential) bảo vệ tính riêng tư của dữ liệu thông qua các cơ chế chứng thực và mã hóa, ngăn ngừa những người không hợp lệ sẽ không được đọc những thông tin. *Giống như các bì thư khi phát lương thường được dán chữ Confidential, chúng ta có thể hình dung trong môi trường IT là một người chưa log vào domain sẽ không được truy cập những dữ liệu chỉ chia sẽ cho các Domain User.*

- I : (integrity) bảo vệ tính tòan vẹn của dữ liệu thông qua các thuật tóan message digesst, SHA, MD5.. ngăn ngừa attacker thay đổi các thông tin nhạy cảm trong quá trình truyền.

- A : (available) bảo đảm dữ liệu luôn ở trong trạng thái sẳn sàng đap ứng nhu cầu của người dùng. *Trong các kì thi chứng chỉ bảo mật của Security+ và SCNP các câu hỏi về CIA rất hay ra, đặc biệt lưu ý chữ A là tượng trưng cho Available chứ không phải Authentiacation.*

- Non-*Repudiation :* Tính không thể chối bỏ, nghĩa là dữ liệu người nào gởi đi thì họ phải có trách nhiệm với các thông tin của mình thông qua các xác nhận nguồn gốc như chữ kí điện tử.

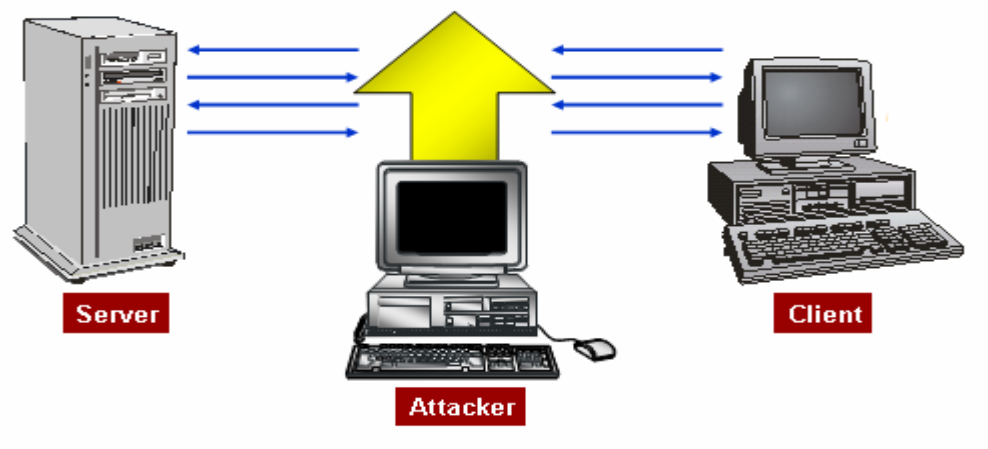


Hình 18.1 – Các mục tiêu của mã hóa.

Để thực hiện điều này chúng ta áp dụng các biện pháp xác thực và mã hóa. Và ***mật mã học*** hay **cryptography** là ngành học nghiên cứu về vấn đề mã hóa.

Mã hóa là một tiến trình biên đổi dữ liệu từ dạng ***cleartext*** (văn bản thuần túy dễ dàng nhận biết) thành kết quả ***ciphertext***, dạng dữ liệu không thể đọc được nếu không được

giải mã bằng các khóa thích hợp. Mục tiêu của mã hóa là ngăn ngừa việc tấn công man in the middle, sniffer đánh cắp dữ liệu trái phép hoặc phòng ngừa việc mất mát dữ liệu khi bị hacker tấn công vật lý như trộm đĩa cứng, máy tính xách tay hay thậm chí đột nhập vào hệ thống vẫn không thể xem được các dữ liệu riêng tư, bí mật đã được bảo vệ bằng các thuật toán mã hóa mạnh mẽ.



Hình 18.2 - Mã hóa sẽ ngăn không cho attacker xem trộm dữ liệu

Tổng Quan Về Mã Hóa

Mã hóa có thể áp dụng cho dữ liệu lưu trữ trên đĩa cứng hoặc khi chúng truyền qua mạng, và các thuật toán mã hóa sẽ có nhiệm vụ biến đổi dữ liệu từ dạng clear text sang cipher text và ngược lại là giải mã từ cipher text thành clear text. Ngay từ thời xa xưa, vị tướng lĩnh tài ba Cesar đã biết ứng dụng kỹ thuật mã hóa để biến đổi một thông điệp gốc thành một thông điệp không thể đọc được để truyền thông trong môi trường quân sự. Thuật toán này gọi là ***Cesar Shilf*** và có thể xem là thuật toán mã hóa cổ xưa nhất, hoạt động khá đơn giãn. Ví dụ một thông điệp khi truyền là ABC sẽ được ứng dụng mã hóa dịch chuyển kí tự qua phải một vị trí sẽ thành là BCD, như vậy khi nhận được sẽ ứng dụng giải mã bằng cách dịch ngược về trước mộ kí tự, đây cũng chính là khóa để giải mã. Với phương pháp này thì chỉ cần *quét cạn* với khoảng 27 lần là cho ra kết quả gốc, nhưng dựa trên ý tưởng này các nhà khoa học đã cho ra đời các thuật toán mã hóa dich chuyển *transposition* không thể bẻ khóa.

Ngoài phương pháp dịch chuyển là ***trasposition*** còn có cơ chế mã hóa khác như ***substitution*** là phương pháp thay thế kí tự này bằng một kí tự khác. Các thuật toán mã hóa sẽ ứng dụng nhưng công thức toàn học dựa trên cơ chế thay thế hay hoán đổi vị trí để tạo ra các dữ liệu an toàn.

Trong quá trình giải mã ta cần có khóa thích hợp. Có hai kiểu sử dụng khóa giải mã là ***sysmetric key encryption*** và ***asymmetric key encryption*** hay còn gọi là *mã hóa đối xứng* và *mã hóa bất đối xứng*. Mỗi phương pháp có những đại diện là các thuật toán DES, AES hay *Elgamel* mà chúng ta cần phân biệt trong các kì thi chứng chỉ CEH. Sau đây là bảng mô tả và các thuật toán thông dụng đại diện cho hai cơ ứng dụng khóa này :

Bảng 17.1 - Các Thuật Tóan Mã Hóa

Thuật Tóan Mã Hóa	Mô tả	Ví dụ
Symmetric/Private key	*Symmetric encryption (mã hóa đối xứng) còn được xem là private key encryption* tiến hành mã hóa và giải mã dựa trên một khóa duy nhất. Điều này có thuận lợi về mặt tốc độ triển khai cũng như chi phí thấp nhưng lại có tính bảo mật kém vì khi tiến hành truyền dữ liệu phải gởi kèm cả khóa dùng để giải mã vì vậy khi khóa bị đánh cắp sẽ làm cho dữ liệu bị mất an tòan. Do đó khi áp dụng cơ chế này cần có cơ chế truyền khóa an tòan. Stream cipher là symmetric *encryption*	□ Data Encryption Standard (DES) □ Triple DES (3DES) □ Advanced Encryption Standard (AES) □ Rijndael □ Rivest Cipher (RC) 4 và 5 □ Skipjack □ Blowfish □ CAST-128
Asymmetric/Public key	*Asymmetricencryption (mã hóa bất đối xứng)*, hay còn gọi là *public key encryption* là phương pháp mã hóa cao cấp hơn so với symmetric encryption và an tòan hơn. Trong cơ chế mã hóa này một cặp khóa được áp dụng gồm public key có tác dụng đối với tất cả mọi người, và dữ liệu sẽ được mã hóa bằng public key của recipent (bên nhận) và chỉ có private key của recipient mới có thể giải mã dữ liệu. Phương pháp mã hóa bất đối xứng giải quyết được vấn đề chia sẽ private key của mã hóa đối xứng, do đó tính an tòan cũng cao hơn.	□ Rivest Shamir Adelman (RSA) cryptosystem □ **Diffie-Hellman** □ Elgamel

Các Thuật Toán Băm (Hash)

Các hàm băm là những thuật toán mã hóa một chiều và không có cơ chế giải mã ví dụ như phương pháp *message digest* sử các thuật toán băm (*hashing algorithm*) như các giao thức MD5 và SHA. Khi sử dụng các thuật tóan băm sẽ tạo ra các giá trị băm (*hash value*) là *digest* với kích thước phụ thuộc vào dữ liệu gốc.

Trong qua trình truyền thông cả dữ liệu đã mã hóa (*ciphertext*) và *digest* đều được truyền đến bên nhận để phục vụ cho quá trình so sánh dữ liệu sau khi truyền với các thuật toán thích hợp. *Digital signature* ngoài việc cung cấp cơ chế bảo đảm tính tòan vẹn (*integrity*) còn lọai trừ khả năng chối bỏ trách nhiệm của bên gởi dữ liệu, đặc trưng này còn được gọi là **non-repudiation** như có trình bày trong phần trên – một trong những tính năng quan trọng trong môi trường trao đổi thông tin điện tử.

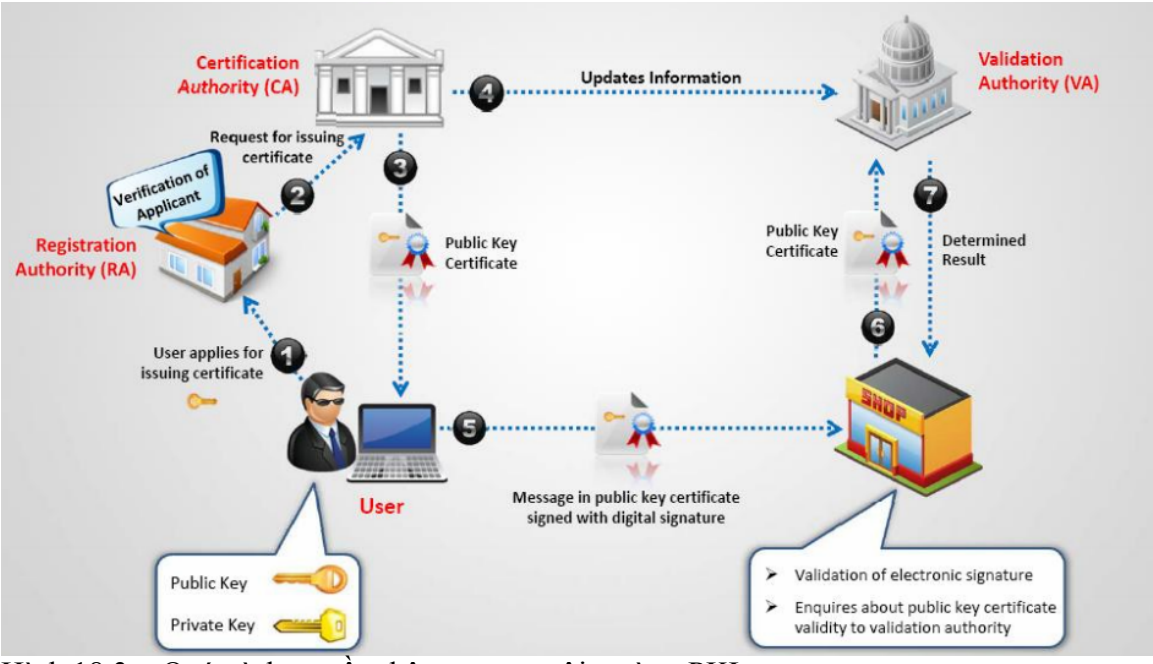
Bảng 17.2 - Các Thuật Tóan Băm

Các thuật tòan Hashing	Mô tả
Secure Hash Algorithm (SHA-1, SHA-256, SHA- 384, và SHA-512)	Là thuật tóan mã hóa mạnh nhất trong số 2 thuật tóan băm được giới thiệu. SHA-1 tạo ra các hash value 160-bitcòn SHA-256, SHA-384, và SHA-512 thì tạo ra các hash value tương ứng 256-bit, 384-bit, và 512-bit.
Message Digest 5 (MD-5)	MD5 sử dụng 128-bit message digest.

Public Key Infrastructure (PKI)

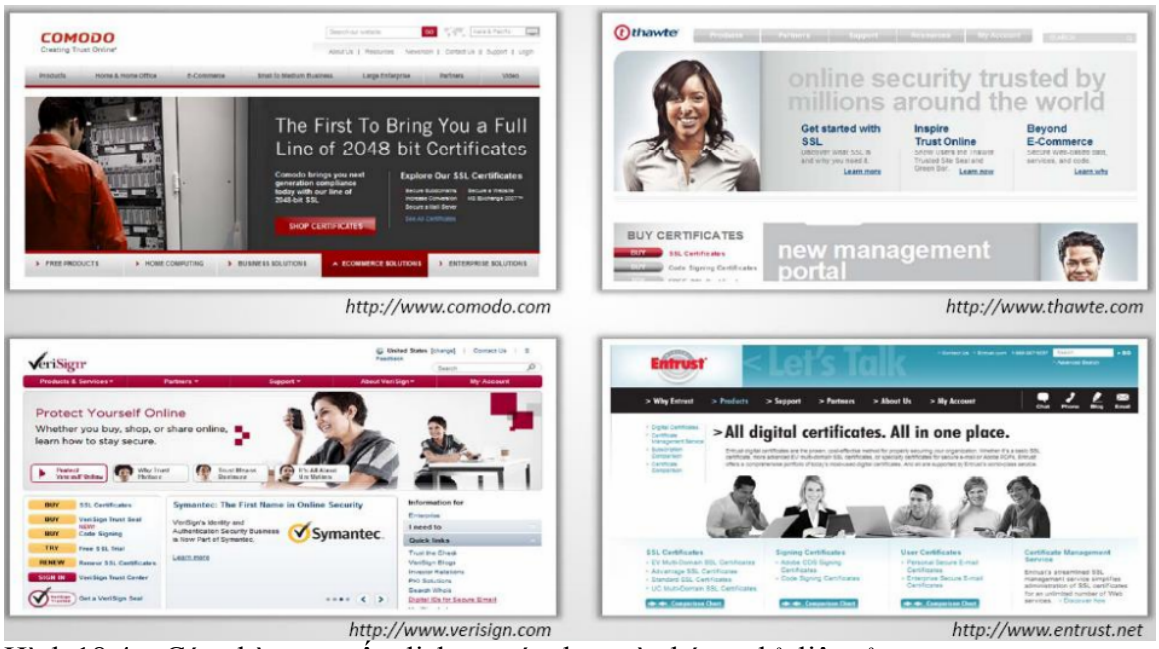
PKI hay hạ tầng khóa công khai bao gồm nhiều thành phần khác nhau như con người, chứng chỉ điện tử, chính sách, thiết bị phần cứng, phần mềm và quy trình thực hiện như trong hình minh họa. Trong các thành phần trên thì CA hay *Certification Authority* là quan trọng nhất chịu trách nhiệm cấp phát và quản lý các chứng chỉ điện tử (certificate) và xác nhận tính hợp lệ của thành phần tham gia quá trình trao đổi thông tin ứng dụng công nghệ mã hóa khóa công khai. Các bạn có thể hình dung *PKI* như là một bộ máy quản lý của chính phủ với các cơ quan quản lý và thị thực, mỗi người dân là các thành phần liên kết, trao đổi thông tin. Và chứng chỉ điện tử là chứng minh nhân dân hay *passport* (hộ chiếu). Khi chúng ta cần sư dụng một dịch vụ nào đó như di chuyển bằng máy bay thì các bạn cần phải xuất trình chứng minh nhân dân để co quan an ninh xác nhận tính hợp lệ, những cơ quan an ninh hay bộ phận quản lý này vận hành theo một quy trình do chính phủ quy định.

Quay trở về với mô hình PKI, khi một người dùng **sender** cần gởi thông tin đến người nhận là **receiver** thì cả hai phía cần phải xin một **certificate** từ đơn vị chủ quản là máy chủ CA thông qua các yêu cầu xin khóa được gọi là **enrollment**, quá trình này có thể diễn ra nhanh chóng bằng cách gởi yêu cầu trực tiếp đến CA nêu như các thành phần trên ở trong một môi trường tin cậy như Actice Directory. Nhưng đa số chúng ta phải xin khóa qua một yêu cầu theo định dạng chuẩn **PKCS #10** (tham khảo http://www.rsa.com/rsalabs/node.asp?id=2132), nếu yêu cầu hợp lệ các *certificate* được cấp phát với định dạng **X.509** chứa các thông tin gồm cặp khóa *public key, private key* và thời gian hợp lệ của các khóa này (khi hết thời gian thì không sử dụng được các khóa này nữa và phải yêu cầu một cặp khóa mới). Nếu *sender* cần gởi một email đến *receiver* thì anh ta sẽ dùng *public key* của *receiver* để mã hóa, sau đó thông điệp gởi đến bên nhận và *receiver* sẽ dùng private key của mình để giải mã, vì khóa giải mã không bao giờ được truyền trên hệ thống mạng nên độ bảo mật rất cao.



Hình 18.3 – Quá trình truyền thông trong môi trường PKI

Chúng ta có thể tự triển khai các hệ thống PKI trên Windows hay Linux nhằm phục vụ cho nhu cầu trao đổi thông tin trong nội bộ bằng cách cài đặt thêm dịch vụ CA trên hệ điều hành Windows Server 2000 / 2003 / 2008. Nếu muốn sử dụng công nghệ khóa công khai trong môi trường công cộng như ứng dụng cho trang web của cơ quan, doanh nghiệp thì cần phải mua hoặc thuê các dịch vụ cấp phát và quản lý Certificate từ nhà cung cấp bên thứ 3 là VeriSign (tại Việt Nam có VASC là đại lý của Thawte) hay Thawte, Entrust, Comodo, Sitelock … Ngoài ra, có thể sử dụng các hệ thống PKI mở như OpenPGO, GNUPG.

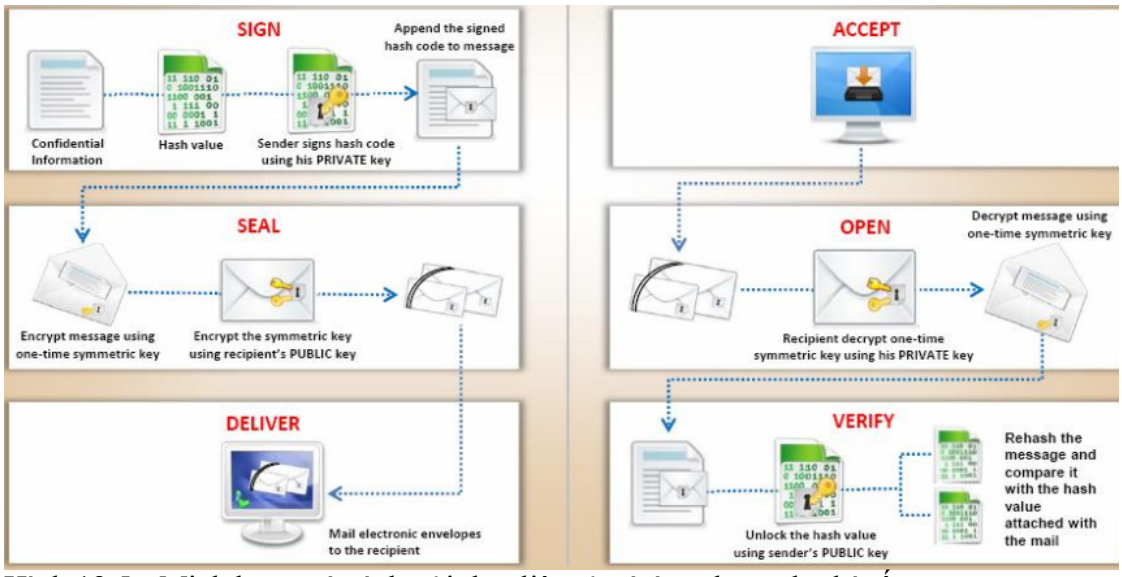


Hình 18.4 – Các nhà cung cấp dịch vụ xác thực và chứng chỉ điện tử

Chữ Ký Số (Digital Signature)

Chữ ký số chỉ là một thành phần của chữ ký điện tử. Chữ ký số là chữ ký điện tử dựa trên kỹ thuật mã hóa khóa công khai mà chúng ta đã đề cập, với một cặp khóa dành cho mỗi người là khóa bí mật (*private key*) và một khóa công khai (*public key*). Khóa bí mật không bao giờ truyền trên mạng còn khóa công khai có thể công bố cho tất cả mọi người tham gia có thể biết. Ví dụ để trao đổi thông điệp bí mật, người gửi sẽ tìm khóa công khai trong dữ liệu được công bố như trong cơ sở dữ liệu của OpenPGP (khi này chúng ta cần cài phần mềm OpenPGP) và sử dụng khóa công khai này của người nhận để mã hóa thông điệp cần gửi, tiếp theo bên nhận sẽ sử dụng khóa bí mật tương ứng của mình để giải mã thông điệp.

Chữ ký điện tử là thông tin được mã hoá bằng khoá riêng của người gửi và gửi kèm theo văn bản nhằm đảm bảo cho người nhận định danh, xác thực đúng nguồn gốc (*non-repudiation*) và tính toàn vẹn của tài liệu nhận được (*intergrity*). Chữ ký điện tử thể hiện văn bản gửi đi là đã được ký bởi chính người sở hữu một khoá riêng tương ứng với một chứng chỉ điện tử nào đó.



Hình 18.5 - Minh họa quá trình gởi thư điện tử có ứng dụng chữ kí số

Mã Hóa Dữ Liệu Trên ổ Cứng

Để bảo vệ dữ liệu trên ổ cứng chúng ta thường sử dụng các phương pháp mã hóa với thuật toán có độ mạnh nhằm phòng chống hacker đánh cắp thông tin và giải mã. Nếu sử dụng hệ thống Windows với định dạng NTFS ta có thể dùng tính năng mã hóa **EFS** (*Encrypt File System*) để bảo vệ dữ liệu trên máy tính của mình. Nhưng với phương pháp EFS nếu bị hacker đột nhập máy tính với quyền của người dùng thì kẻ tấn công có thể đọc thông tin mật mà không cần giải mã do đặc tính mã hóa và giải mã trong suốt đối với người dùng. Chính vị vậy, một ứng dụng nguồn mở được nhiều người sử dụng cho vấn đề mã hóa dữ liệu trên đĩa cứng là **TrueCrypt** với các thuật toán rất mạnh mẽ và hầu như không thể giải mã. Một trong những tính năng thú vị của *TrueCrypt* là cho phép mã hóa toàn bộ hệ thống, ngăn chặn hacker ngay từ bước đăng nhập. Và cho dù máy tính hay đĩa cứng của quý vị có bị đánh cắp thì dữ liệu riêng tư vẫn hoàn toàn bí mật.

Hướng Dẫn Sử Dụng TrueCrypt

TrueCrypt là phần mềm nguồn mở có khả năng mã hóa toàn bộ một không gian ổ cứng theo cơ chế *on-the-fly* - nghĩa là tất cả dữ liệu sẽ được mã hóa và giải mã hoàn toàn tự động khi chúng được đọc hay ghi mà không cần bất kỳ sự tương tác nào của người dùng. Điều nay gần giống với tính năng mã hóa *EFS* của hệ thống Windows Server 2000/2003 hay XP khi các bạn định dạng các phần chia theo NTFS. Tuy nhiên với *TrueCrypt* chúng ta có thể quản lý dữ liệu an toàn hơn, không thể giải mã thông tin đã bị mã hóa mà không có các khóa thích hợp, và một khi thiết lập cơ chế mã hóa với TrueCrypt toàn bộ hệ thống tập tin bao gồm các file/folder, metadata và không gian trống đều được mã hóa.

Các tập tin trên "ổ" (volume) TrueCrypt có thể sao chép, di chuyển một cách bình

thường. Khi một tập tin được đọc nó sẽ được giải mã on-the-fly (trong bộ nhớ/RAM), ngược lại khi tập tin hay thư mục được chép lên ổ TrueCrypt thì sẽ được tự động mã hoá trước khi lưu. Hẳn là các bạn sẽ thắc mắc có cần phải tăng thêm RAM khi sử dụng TrueCrypt hay không, vì quá trình mã hóa/giải mã on-the-fly tiến hành trên bộ nhớ này. Câu trả lời là không bởi vì không phải toàn bộ tập tin sẽ được nạp vào RAM cùng lúc để tiến hành mã hóa hay giải mã, mà chương trình chỉ nạp một phần tập tin vào bộ nhớ để thực hiện quá trình này, sau đó nạp tiếp những phần còn lại theo cơ chế "cuốn chiếu". Điều này làm cho bộ nhớ không bị chiếm dụng toàn bộ nhưng vẫn có thể tiến hành mã hoá/giải mã trong suốt quá trình xử lý tập tin như đọc, ghi, xem video ...

Một điều cần chú ý nữa là TrueCrypt không lưu bất kỳ dữ liệu đã được giải mã lên đĩa cứng mà chỉ tạm thời lưu trữ lên RAM, khi hệ thống shutdown/restart hoặc bị sự cố mất nguồn đột ngột thì dữ liệu vẫn được lưu trong trạng thái an toàn.

Sử Dụng 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:

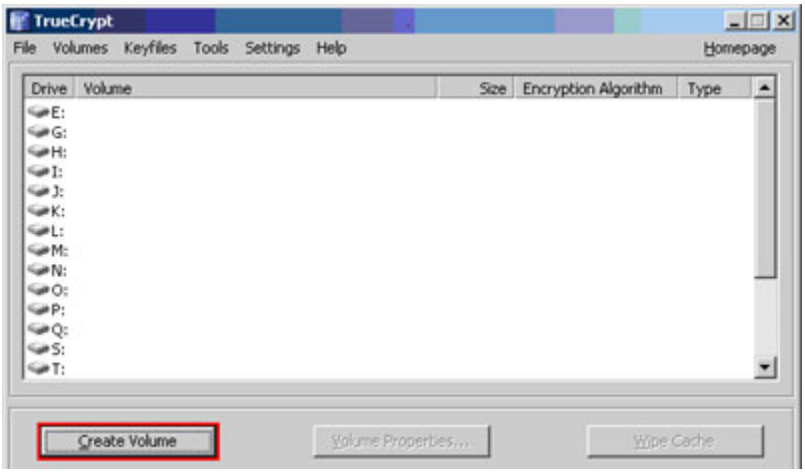
http://www.truecrypt.org

Bước 2:

Sau khi cài đặt, chạy chương trìnnh bằng cách nhấn chuột vào biểu tượng TrueCrypt trên desktop hoặc trong trình đơn Start>Programs>TrueCrypt.

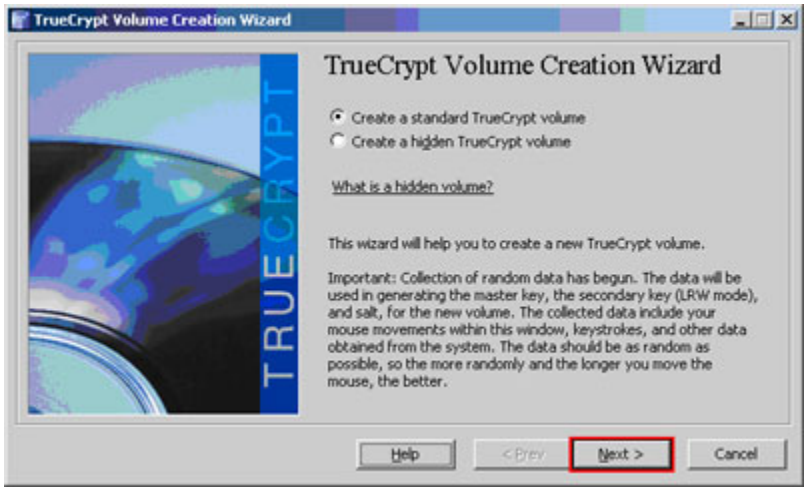
Bước 3:

Trong cửa sổ chính của TrueCrypt, hãy nhấn Create Volume.



Bước 4:

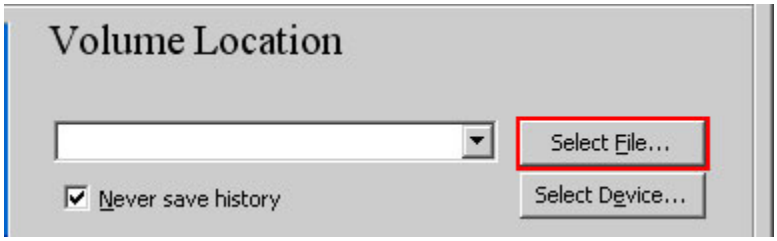
Cửa sổ TrueCrypt Volume Creation Wizard sẽ xuất hiện, nhấn Next.



Bước 5:

Trong bước này ta cần xác định vị trí tạo "ổ" (volume) TrueCrypt. Một TrueCrypt volume có thể đặt trong một file, được gọi là container, hay trong một partition (gọi là device). Ở đây chúng ta sẽ tạo một TrueCrypt volume trong một file.

Nhấn Select File để tiếp tục.

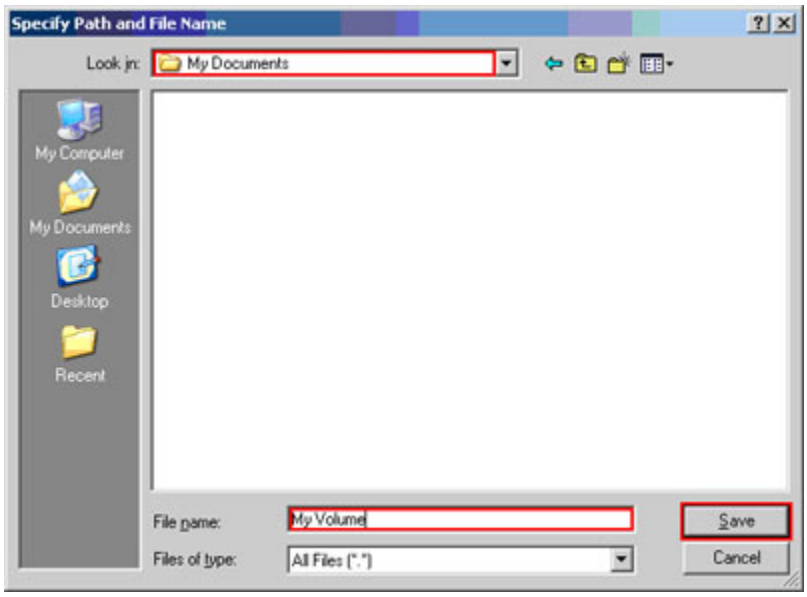


Bước 6:

Chúng ta sẽ tạo một TrueCrypt volume (container) trong folder D:\My Documents và đặt tên là My Volume. Bạn có thể chọn tên khác và lưu trữ vào vị trí tùy ý như trên ổ đĩa USB.

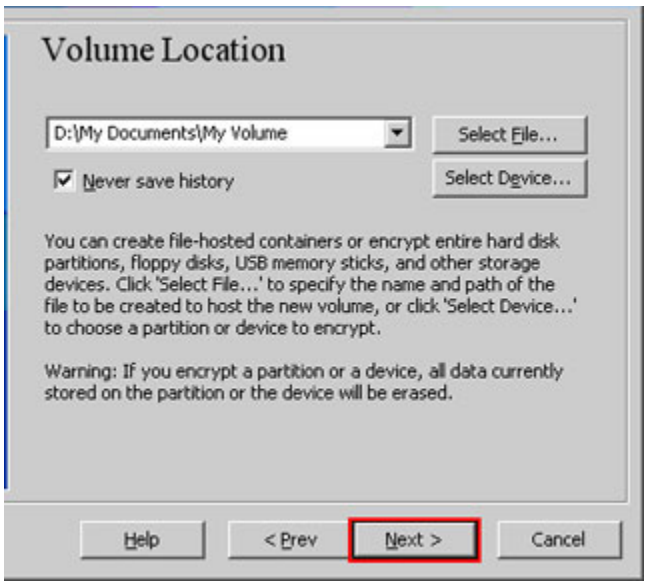
Lưu ý : TrueCrypt không mã hóa bất kỳ tập tin nào đã có sẵn trên hệ thống. Cho nên, nếu ta chọn một tập tin có sẵn thì tập tin này sẽ bị ghi đè và thay thế bằng một container. Vì vậy bạn cần tạo một volume và di chuyển tập tin vào volume này.

Nhập tên và nhấn Save để quay trở về màn hình TrueCrypt Volume Creation Wizard.



Bước 7:

Trên cửa sổ Volume Creation Wizard hãy nhấn Next.

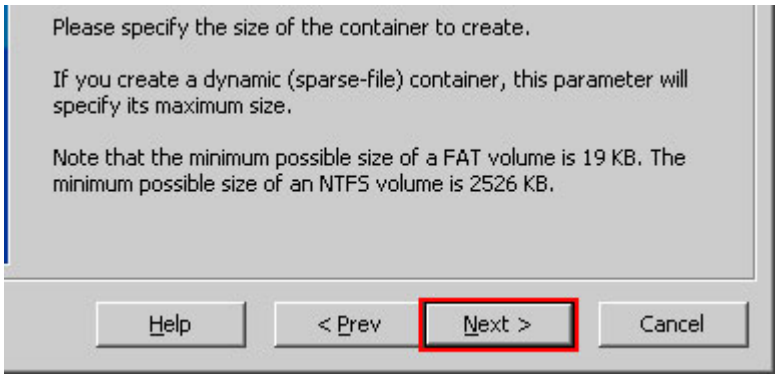


Bước 8:

Đến đây, chúng ta chọn các tham số cần thiết như thuật toán mã hóa, thuật toán băm. Ở đây sử dụng các thiết lập mặc định là AES và RIPEMD-160, rồi nhấn Next.

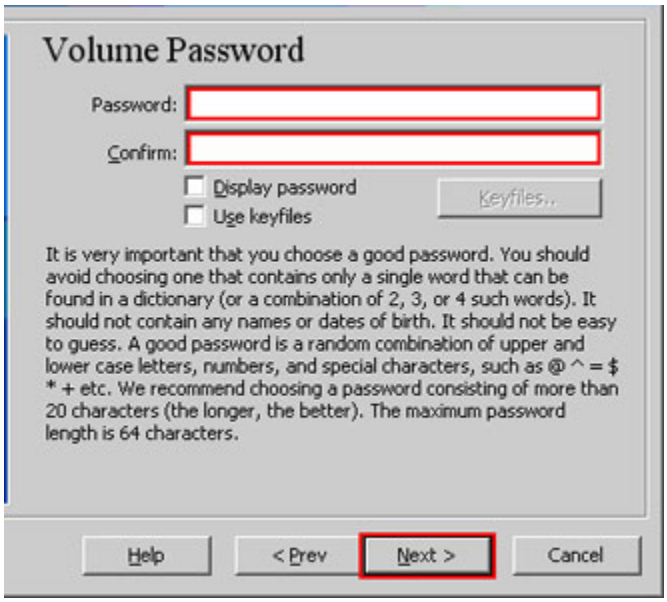
Bước 9:

Hãy xác định kích thước của TrueCrypt container, ví dụ 1 megabyte như trong hình. Bạn có thể xác định kích thước thích hợp với nhu cầu của mình và nhấn Next.



Bước 10:

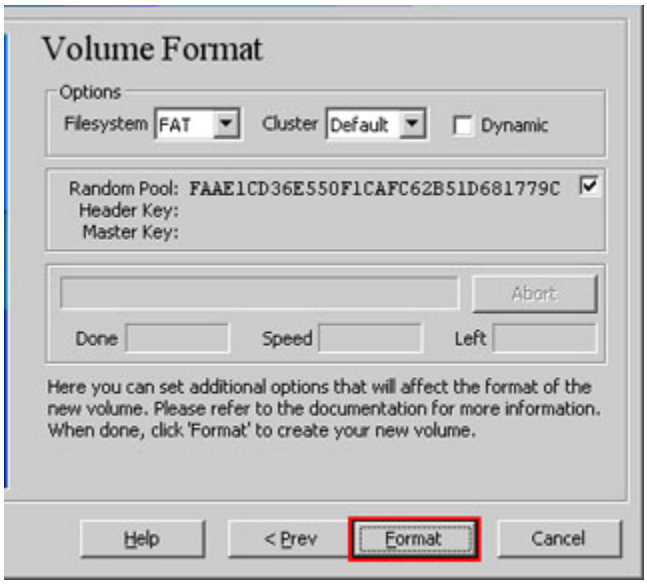
Đây là một trong những bước quan trọng nhất: xác định mật khẩu (password) cho TrueCrypt volume. Để chọn một password mạnh các bạn có thể tham khảo các tài liệu liên quan, ở đây chỉ nêu vắn tắt một mật khẩu mạnh thì độ dài ít nhất phải là 8 ký tự kết hợp chữ hoa, chữ thường, số và các kí tự đặc biệt. Sau đó nhấn Next.



Bước 11:

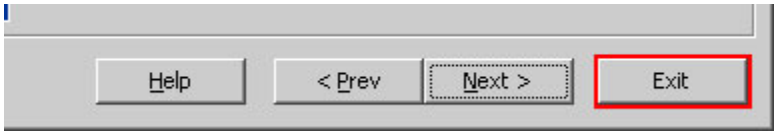
Hãy di chuyển con trỏ chuột trong phạm vi cửa sổ Volume Creation Wizard trong khoảng 30 giây. Thời gian di chuyển chuột càng lâu thì chất lượng của khóa mã hóa tạo ra càng tốt. Để tiếp tục hãy nhấn Format. Tùy thuộc vào kích thước của TrueCrypt volume mà tiến trình định dạng diễn ra lâu hay mau, sau khi hoàn tất chúng ta sẽ có một TrueCrypt volume tên là My Volume trong thư mục D:\My Documents\, và thông báo hoàn tất quá trình tạo volume.

Nhấn OK để đóng hộp thoại.



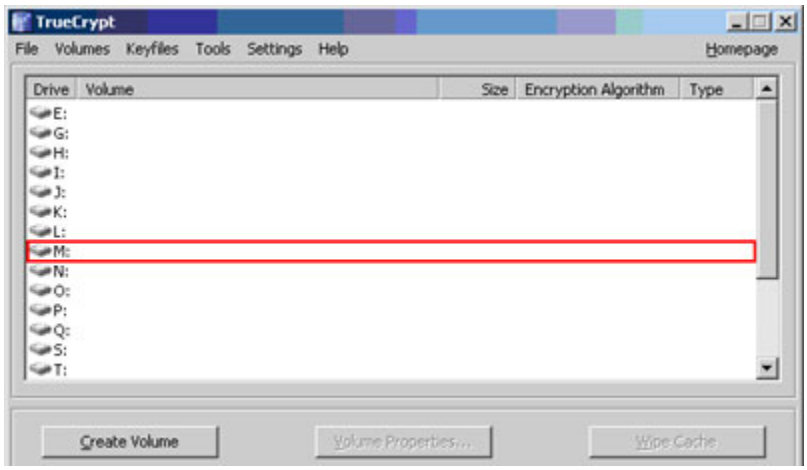
Bước 12:

Như vậy, chúng ta đã tạo xong một TrueCrypt volume (file container). Hãy đóng cửa sổ TrueCrypt Volume Creation Wizard bằng cách nhấn Exit .



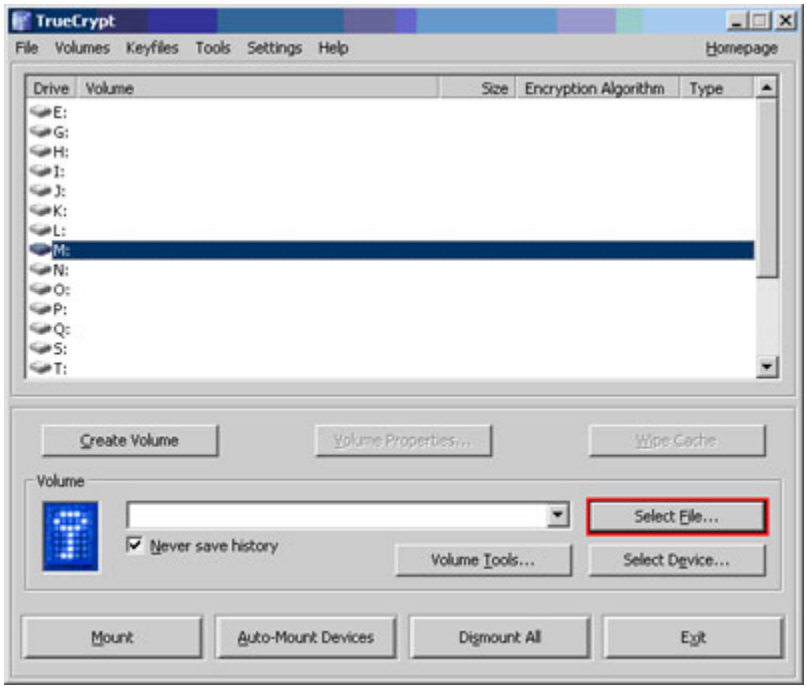
Bước 13:

Trong phần tiếp theo chúng ta sẽ "gán" (mount) volume vừa được tạo với một tên ổ đĩa. Ví dụ chúng ta gán TrueCrypt volume với tên ổ đĩa M như hình sau.



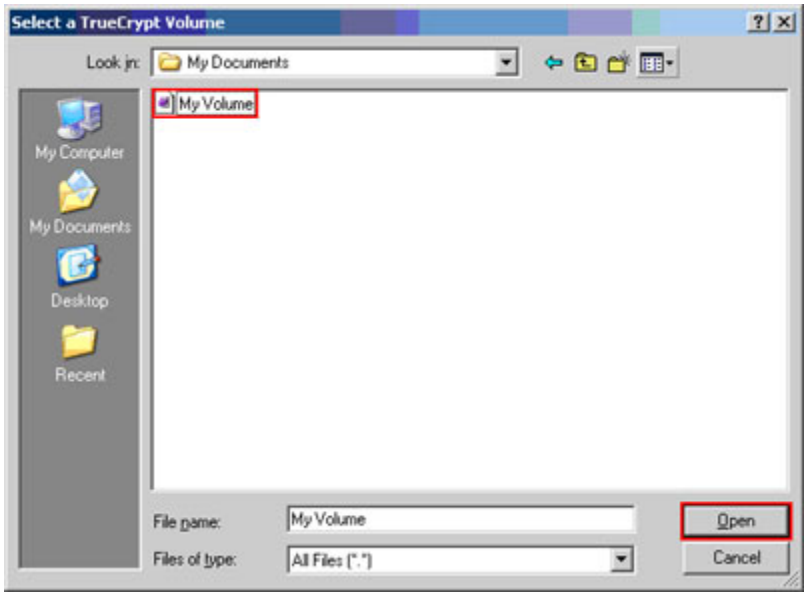
Bước 14:

Nhấn Select File.



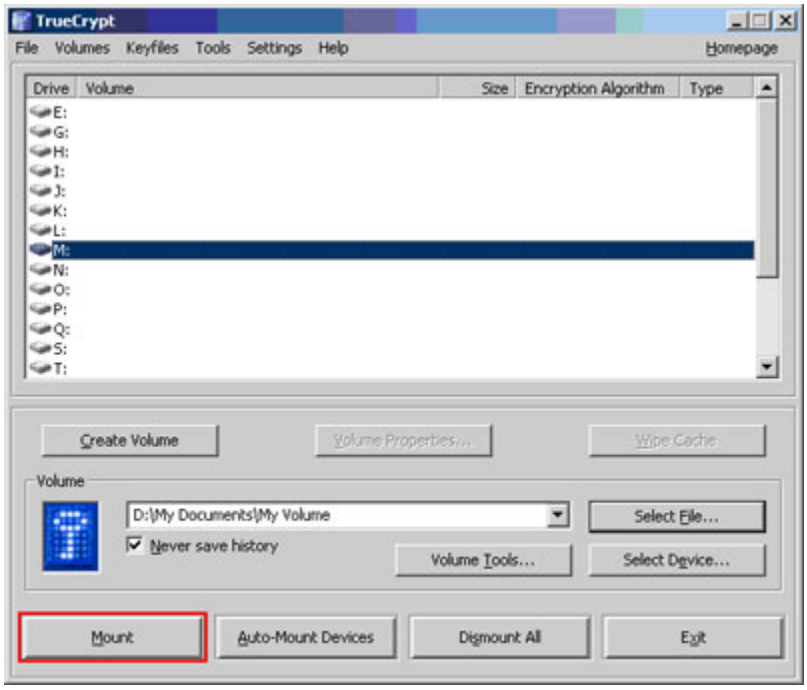
Bước 15:

Chọn tập tin My Volume mà bạn đã tạo ra trong các bước 6 đến 11 và nhấn Open.



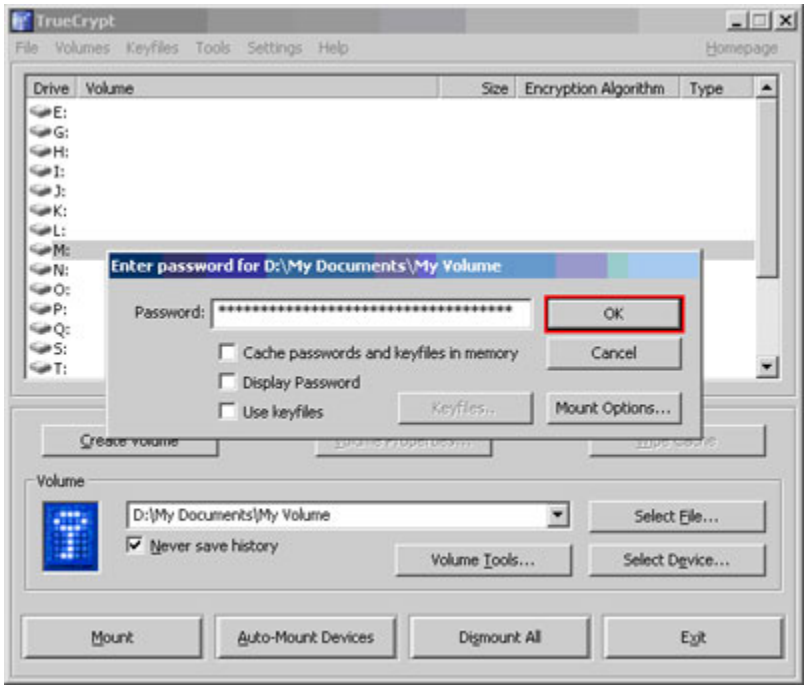
Bước 16:

Trên cửa sổ chính các bạn nhấn Mount, lúc này một hộp thoại yêu cầu cung cấp mật khẩu xuất hiện.



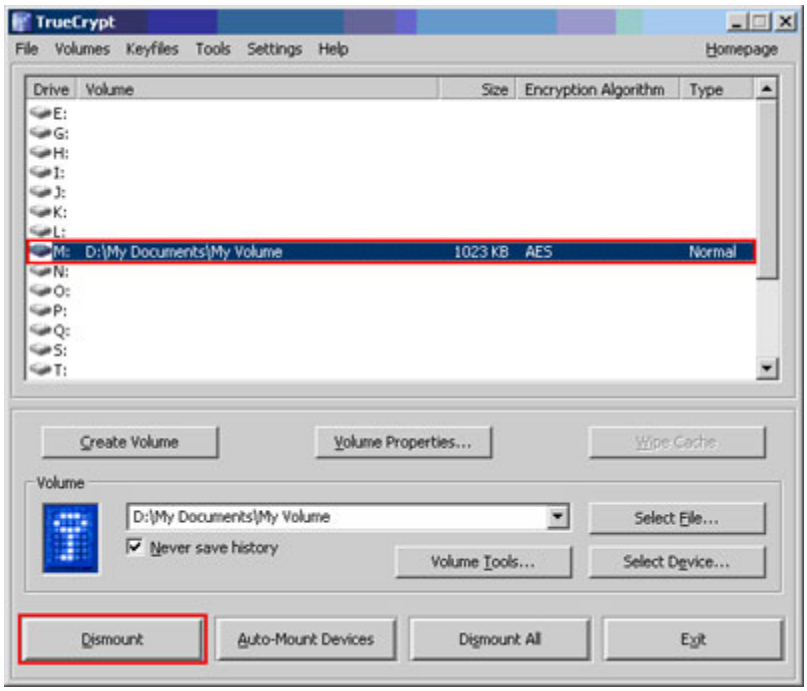
Bước 17:

Nhập mật khẩu mà bạn đã xác định trong bước 10 và nhấn OK. Nếu mật khẩu hợp lệ thì volume sẽ được hiển thị như là ổ đĩa M.

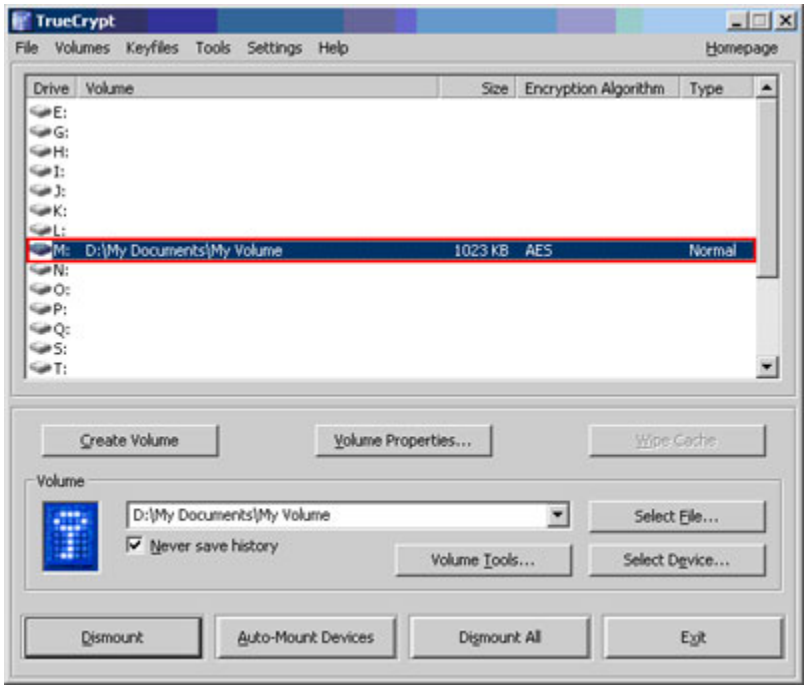


Như vậy chúng ta đã tạo ra một ổ ảo **M** mà tất cả những tập tin lưu trữ trong nó đều được mã hóa. Bạn có thể sử dụng nó như một ổ đĩa thông thường chỉ khác là dữ liệu khi lưu trữ

trong ổ đĩa này sẽ được bảo mật, và tiến trình mã hóa cũng như giải mã diễn ra một cách trong suốt và không có bất kì dữ liệu nào được lưu trên đĩa cứng mà chỉ lưu trên RAM.

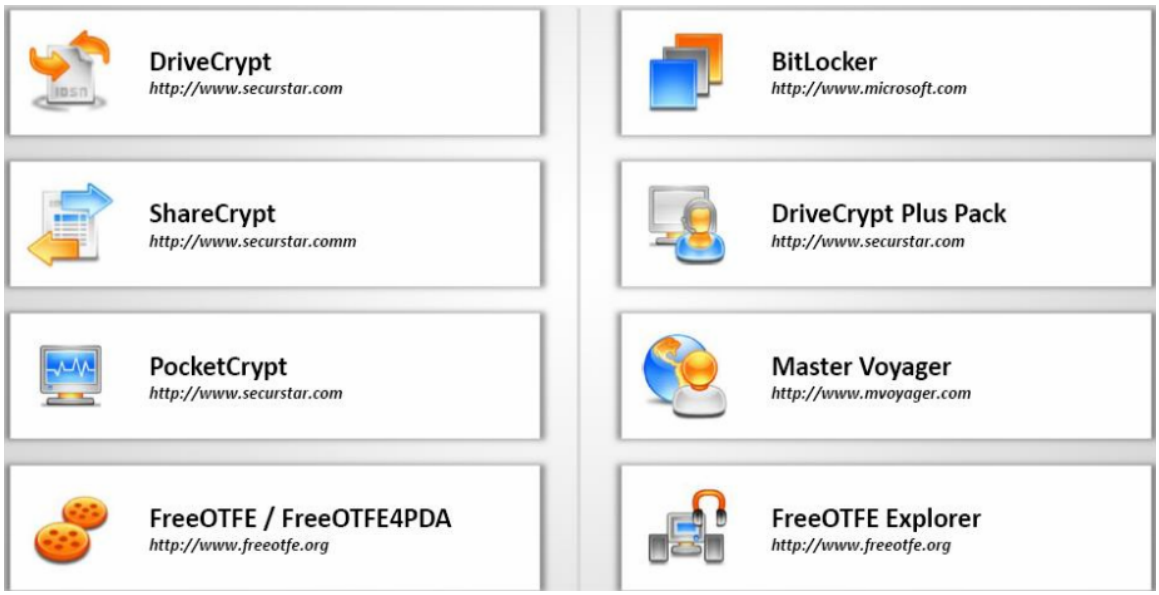


Nếu bạn muốn đóng volume và không cho phép truy nhập vào những dữ liệu được lưu trữ bên trong, hãy mở giao diện chính của chương trình TrueCrypt và chọn volume đã được mount sau đó nhấn Dismount.



Thay vì tạo các file container, các bạn có thể mã hóa toàn bộ phần chia trên ổ cứng hay thiết bị lưu trữ bằng cách tiến hành các bước tương tự từ 1 – 17, sau đó thay vì Select File, hãy chọn Select Device.

Sau đây là danh sách một số công cụ mã hóa dữ liệu trên ổ cứng



Hình 18.6 – Danh sách các công cụ mã hóa sữ liệu

Tổng Kết

Trong chương mật mã học chúng ta đã tìm hiểu về các thuật toán mã hóa với cơ chế mã hóa đối xứng hay mã hóa bất đối xứng, công nghệ mã hóa khóa công khai, chữ kí số …

Mặc dù những kỹ thuật mã hóa có khả năng phòng chống nhiều dạng tấn công nguy hiểm nhưng hacker vẫn có thể bẻ khóa nếu như những thuật toán được sử dụng không đủ độ mạnh hay mật khẩu yếu sẽ bị tấn công brute-force, dò từ điển hay bẻ khóa MD5 với các công cụ online như http://md5crack.com . Ngoài ra, khi sử dụng các chứng chỉ điện tử trong môi trường không tin cậy vẫn có khả năng bị hacker tấn công bằng phương pháp giả mạo *certificate* hay còn gọi là **Fake Certificate**, do đó trong mọi trường hợp cần tuân thủ những nguyên tắt an toàn thông tin nhằm đem đến sự bảo mật tối đa cho thông tin, dữ liệu bí mật. Trong phần cuối cùng chúng ta sẽ thảo luận về chủ đề ***Penetration Test***.