TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TP. HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

AN TOÀN THÔNG TIN- INFORMATION SECURITY

CHƯƠNG 3
KỸ THUẬT MÃ HOÁ

TỔNG QUAN VỀ MẬT MÃ VÀ CÁC KỸ THUẬT GIẤU TIN

Giảng viên: TS. Trần Thế Vinh

TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Lịch sử mật mã học:

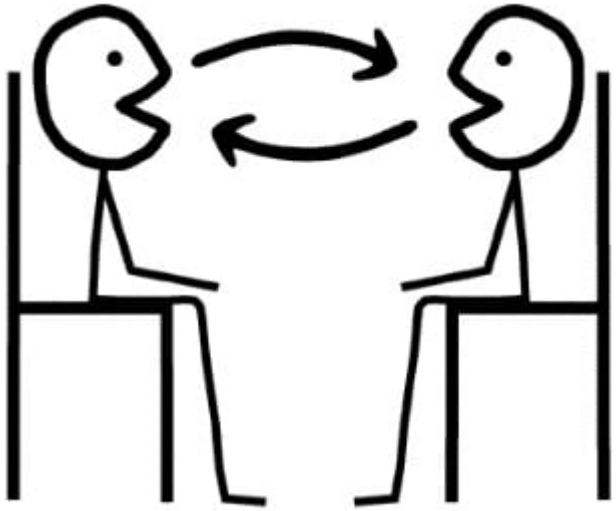
Con người từ lâu đã có 2 nhu cầu cơ bản:

- Giao tiếp và chia sẽ thông tin
- Giao tiếp có chọn lọc

Hai nhu cầu này đã dẫn đến nghệ thuật mã hóa các thông điệp theo cách mà chỉ những người dự định mới có thể tiếp cận thông tin. Những người không được ủy quyền không thể trích xuất bất kỳ thông tin nào, ngay cả khi tin nhắn bị xáo trộn rơi vào tay của họ

Nghệ thuật và khoa học che giấu các thông điệp để tạo ra tính bí mật trong bảo mật thông tin được công nhận là mật mã.

Từ 'cryptography' được tạo ra bằng cách kết hợp hai từ Hy Lạp, 'Krypto' có nghĩa là ẩn và 'graphene' có nghĩa là viết.



TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Lịch sử mật mã học:

Nghệ thuật mật mã được coi là ra đời cùng với nghệ thuật viết lách. Khi các nền văn minh phát triển, con người được tổ chức thành các bộ lạc, nhóm và vương quốc. Điều này dẫn đến sự xuất hiện của các ý tưởng như quyền lực, trận chiến, uy quyền tối cao và chính trị. Những ý tưởng này càng thúc đẩy nhu cầu tự nhiên của mọi người là giao tiếp bí mật với người nhận có chọn lọc, từ đó đảm bảo sự phát triển liên tục của mật mã.

Nguồn gốc của mật mã được tìm thấy trong các nền văn minh La Mã và Ai Cập.

TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Lịch sử mật mã học:

Có thể xem là lịch sử mật mã học bắt nguồn từ người Ai Cập vào khoảng những năm 2000 trước Công nguyên khi họ dùng những ký hiệu tượng hình khó hiểu để trang trí trên các ngôi mộ nhằm bí mật ghi lại tiểu sử và những chiến tích, công lao của người đã khuất.

Trong một thời gian dài hàng thế kỷ một trong những loại công trình nghiên cứu thu hút rất nhiều nhà khoa học trên thế giới là các nghiên cứu giải mã những "dấu tích bí mật" trên các ngôi mộ cổ Ai Cập, nhờ đó mà ta hiểu biết được khá nhiều về lịch sử, phong tục, tập quán sinh hoạt của đất nước Ai Cập cổ đại huyền bí.

Chữ tượng hình – kỹ thuật mã hóa lâu đời nhất

TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Lịch sử mật mã học:

Người Hebrew (Do Thái cổ) đã sáng tạo một thuật toán mã hóa đơn giản và hiệu quả gọi là thuật toán atbash mà chìa khóa mã hóa và giải mã là một sự thay thế (substitution) trong bảng chữ cái. Giả sử dùng chìa khóa mã hóa là bảng hoán vị:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

↓

Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Khi đó chẳng hạn từ gốc (plaintext): JERUSALEM sẽ được mã hóa thành từ mã (ciphertext): QVIFHZOVN

Thuật toán mã hóa bằng thay thế này chỉ dùng một ký tự (chữ cái) thay thế cho một ký tự nên được gọi là thuật toán mã hóa thay thế đơn (monoalphabetic substitution). Người ta cũng có thể tạo những thuật toán mã hóa thay thế khối (multiple alphabetic substitution) nếu thay vì thay thế từng ký tự ta thay thế một dãy ký tự gốc bởi một dãy ký tự mã hóa: thuật toán này cho ta nhiều khả năng tạo khóa hơn nên khả năng bị tấn công lại càng giảm xuống.

TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Lịch sử mật mã học:

Về thời Trung Cổ, hoàng đế La Mã nổi tiếng là Julius Caesar tạo một công cụ lập mã rất đơn giản cho thuật toán gọi là "mã vòng" (cyclic code) tương tự như thuật toán atbash của người Hebrew nhưng đây không phải là một sự thay thế bất kỳ mà là một sự thay thế theo hoán vị vòng quanh.

Caesar dùng hai vành tròn đồng tâm, trên cả hai vành đều ghi bảng chữ cái La-tinh, vành trong ứng với plaintext còn vành ngoài ứng với ciphertext. Chìa khóa mã hóa là phép xoay vành tròn bên ngoài một số bước, do đó các chữ cái thay đổi đi. Chẳng hạn nếu chìa khóa là +3 tức là xoay theo chiều thuận +3 ô thì các chữ cái A, B, C…X, Y, Z trong plaintext sẽ chuyển đến D, E, F …A, B, C trong ciphertext,

TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Lịch sử mật mã học:

Chính nguyên lý mã vòng của Caesar là ý tưởng cho việc phát triển một thiết bị mã hóa nổi tiếng nhất trong lịch sử: máy mã hóa Enigma của người Đức dùng trong Đại chiến thế giới lần thứ hai. Enigma có 3 ổ quay, mỗi ký tự trong plaintext khi đưa vào sẽ được thay thế 3 lần theo những quy luật định sẵn khác nhau cho nên quá trình thám mã rất khó khăn.

Về sau một nhóm các nhà mật mã học Ba Lan đã bẻ khóa được thuật toán lập mã của Enigma và cung cấp cho người Anh mọi thông tin quân sự của Đức: người ta đánh giá rằng thành công của việc phá khóa đó đã rút ngắn thời gian kéo dài của Thế chiến II bớt được 2 năm. Sau khi Thế chiến II kết thúc, bí mật của Enigma được công bố và ngày nay một máy Enigma còn được triển lãm tại Viện Smithsonian, Washington D.C, Hoa Kỳ.

TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Lịch sử mật mã học:

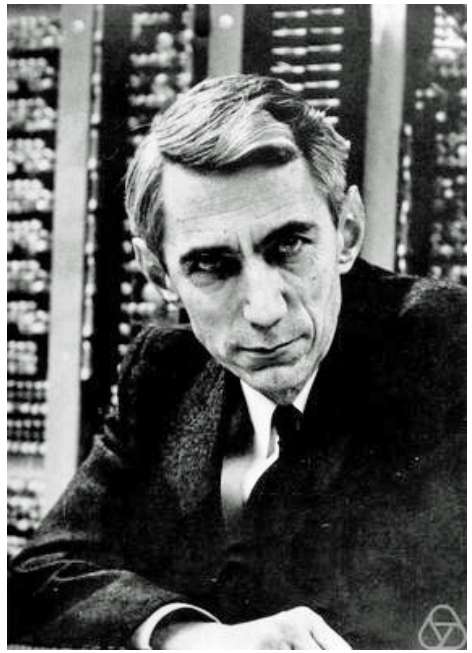
Năm 1922, William Frederic Friedman công bố tác phẩm The Index of Coincidence and Its Applications in Cryptography (Chỉ số trùng khớp và ứng dụng của nó trong mật mã học). Một trong những công trình chuẩn trong danh pháp và phân loại của mật mã. Ông được đánh giá là "người khổng lồ" trong ngành mật mã.

TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Mật mã hiện đại:

Nhiều người cho rằng kỷ nguyên của mật mã học hiện đại được bắt đầu với Claude Shannon (30/4/1916 – 24/02/2001), người được coi là "cha đẻ của mật mã toán học". Năm 1949 ông đã công bố bài "Lý thuyết về truyền thông trong các hệ thống bảo mật" trên tạp chí "Bell System Technical Journal – Tạp chí kỹ thuật của hệ thống Bell". Những công trình của ông đã thiết lập một nền tảng lý thuyết cơ bản cho mật mã học và thám mã học.



Với ảnh hưởng đó, mật mã học hầu như bị thâu tóm bởi các cơ quan truyền thông mật của chính phủ (NSA – National Security Agency) và biến mất khỏi tầm hiểu biết của công chúng. Rất ít các công trình được tiếp tục công bố, cho đến thời kỳ giữa thập niên 1970, khi mọi sự được thay đổi.

TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Tiêu chuẩn mật mã:

Thời kỳ giữa thập niên 1970 được chứng kiến 2 tiến bộ chính lớn:

- Công bố đề xuất "Tiêu chuẩn mật mã hóa dữ liệu (Data Encryption Standard – DES) (17/03/1975) được đệ trình bởi một nhóm nghiên cứu tại IBM, theo lời mời của Cục tiêu chuẩn quốc gia trong nỗ lực phát triển các phương tiện liên lạc điện tử an toàn của các doanh nghiệp như ngân hàng và các tổ chức tài chính lớn. DES là mật mã có thể truy cập công khai dầu tiên.

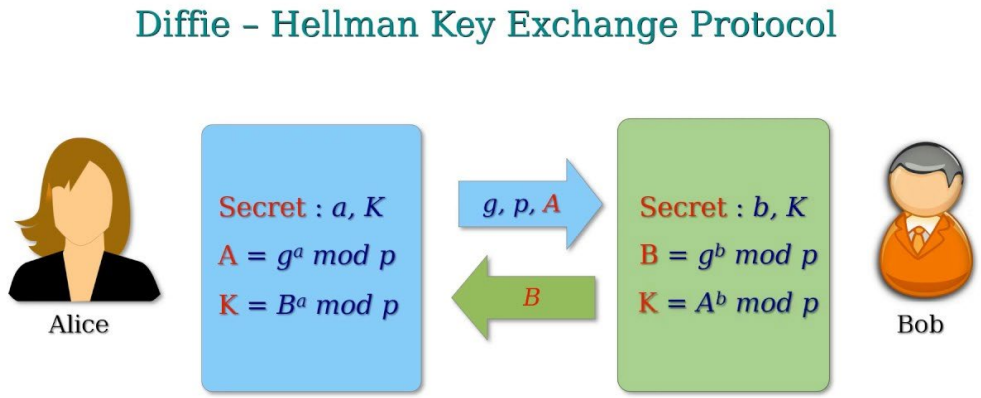
DES được chính thức thay thế bằng Tiêu chuẩn mã hóa nâng cao - Advanced Encryption Standard (AES) vào năm 2001 sau khi mật mã DES (56 bit) bị phá vỡ bởi sức mạnh tính toán của hệ máy tính và không còn an toàn nữa.

TỔNG QUAN VỀ MẬT MÃ

NGUỒN GỐC CỦA MẬT MÃ HỌC - CRYPTOGRAPHY

Tiêu chuẩn mật mã:

- Tiến triển thứ 2 còn đột phá hơn nữa, vào năm 1976 tiến triển này đã thay đổi nền tảng cơ bản trong cách làm việc của các hệ thống mật mã. Đó chính là công bố của bài viết "Phương hướng mới trong mật mã học" của Whitfield Diffie và Martin Hellman. Bài viết giới thiệu một phương pháp hoàn toàn mới về cách thức phân phối các khóa bí mật, nó được gọi là trao đổi khóa Diffie-Hellman. Bài viết kích thích sự phát triển gần như tức thời của một lớp các thuật toán mã hóa mới (thuật toán chìa khóa bất đối xứng)



TỔNG QUAN VỀ MẬT MÃ

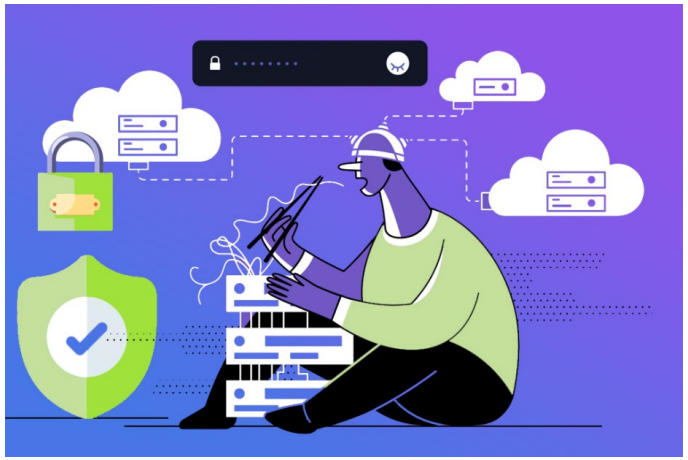
KHÁI NIỆM VỀ MẬT MÃ HIỆN ĐẠI

Nguyên tắc của mật mã hiện đại:

Mật mã hiện đại là quá trình mã hóa dữ liệu số được biểu diễn bằng chuỗi các chữ số nhị phân (binary), không giống như bảng chữ cái. Các hệ thống mật mã hiện đại cần xử lý chuỗi nhị phân này để chuyển thành chuỗi nhị phân khác.

Mật mã hiện đại dựa vào các thuật toán toán học được biết đến rộng rãi để mã hóa thông tin. Độ khó tính toán của thuật toán khiến kẻ tấn công không thể lấy được thông tin gốc ngay cả khi biết thuật toán được sử dụng để mã hóa.

Các thuật toán mật mã hiện đại quá phức tạp để con người thực thi. Các thuật toán ngày nay được thực hiện bởi máy tính hoặc thiết bị phần cứng chuyên dụng và trong hầu hết các trường hợp được thực hiện trong phần mềm máy tính.



TỔNG QUAN VỀ MẬT MÃ

KHÁI NIỆM VỀ MẬT MÃ HIỆN ĐẠI

Nguyên tắc của mật mã hiện đại:

Có thể hiểu đơn giản mã hóa là một phương pháp bảo vệ thông tin, bằng cách chuyển đổi thông tin từ dạng có thể đọc và hiểu được thông thường sang dạng thông tin không thể hiểu theo cách thông thường và chỉ có người có quyền truy cập vào khóa giải mã hoặc có mật khẩu mới có thể đọc được nó.
Việc làm này giúp ta có thể bảo vệ thông tin tốt hơn, an toàn trong việc truyền dữ liệu. Thực chất việc mã hóa dữ liệu sẽ không thể nào ngăn việc dữ liệu có thể bị đánh cắp, nhưng nó sẽ ngăn việc người khác có thể đọc được nội dung của tập tin đó, vì nó đã bị biến sang thành một dạng ký tự khác, hay nội dung khác. Dữ liệu được mã hóa thường gọi là ciphertext. Dữ liệu thông thường, không được mã hóa thì gọi là plaintext.

TỔNG QUAN VỀ MẬT MÃ

KHÁI NIỆM VỀ MẬT MÃ HIỆN ĐẠI

Mật mã hiện đại là nền tảng của bảo mật máy tính và truyền thông. Nền tảng của nó dựa trên các khái niệm toán học khác nhau như Lý thuyết số, Lý thuyết độ phức tạp tính toán và Lý thuyết xác suất.

Đặc điểm của mật mã hiện đại:
Có 3 đặc điểm chính tách biệt mật mã hiện đại khỏi cách tiếp cận cổ điển

Mật mã cổ điển	Mật mã hiện đại
Thao tác trực tiếp các ký tự truyền thống, tức là các chữ cái và chữ số	Hoạt động trên các chuỗi bit nhị phân (binary)
Chủ yếu dự trên "bảo mật thông qua che khuất". Các kỹ thuật được sử dụng để viết mã được giữ bí mật và chỉ những bên liên quan đến giao tiếp mới biết về chúng	Dựa vào các thuật toán toán học được biết đến rộng rãi để mã hóa thông tin. Bí mật có được thông qua khóa(key) bí mật được sử dụng làm hạt giống cho thuật toán. Độ khó tính toán của thuật toán, hay không có khóa bí mật ..v..v.. Khiến kẻ tấn công không thể lấy được thông tin gốc ngay cả khi biết thuật toán được sử dụng để mã hóa
Yêu cầu toàn bộ hệ thống mật mã liên lạc một cách bí mật	Mật mã hiện đại yêu cầu các bên liên quan đến thông tin an toàn cần sở hữu khóa bí mật

TỔNG QUAN VỀ MẬT MÃ

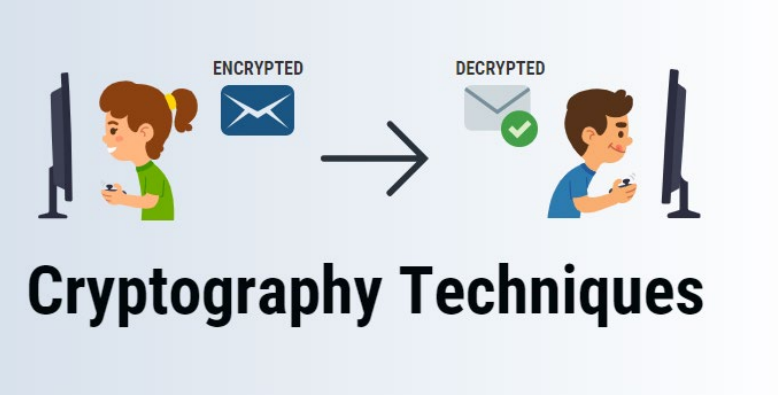
KHÁI NIỆM VỀ MẬT MÃ HIỆN ĐẠI

Mật mã học nghiên cứu về các hệ thống mật mã, có thể chia thành 2 nhánh:

- Mật mã (Cryptography)
- Phân tích mật mã (Cryptanalysis)

TỔNG QUAN VỀ MẬT MÃ

KHÁI NIỆM VỀ MẬT MÃ HIỆN ĐẠI



Mật mã (Cryptography):

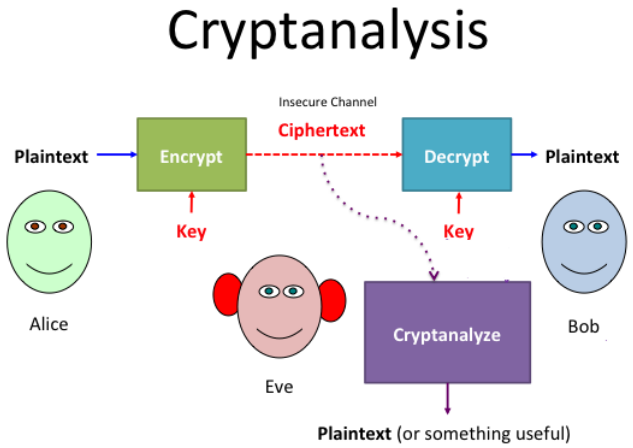
Mật mã là nghệ thuật và khoa học để tạo ra một hệ thống mật mã có khả năng cung cấp bảo mật thông tin.

Mật mã đề cập đến việc bảo mật dữ liệu kỹ thuật số. Nó biết đến với việc thiết kế các cơ chế dựa trên các thuật toán toán học, cung cấp các dịch vụ bảo mật thông tin cơ bản. Chúng ta có thể nghĩ về mật mã như việc thiết lập một bộ công cụ lớn chứa các kỹ thuật khác nhau trong các ứng dụng bảo mật.

Phân tích mật mã (Cryptanalysis):

Nghệ thuật và khoa học phá vỡ văn bản mật mã được gọi là phân tích mật mã.

Phân tích mật mã liên quan đến việc nghiên cứu cơ chế mật mã với ý định phá vỡ chúng. Nó cũng được sử dụng trong quá trình thiết kế các kỹ thuật mật mã mới để kiểm tra sức mạnh bảo mật của chúng.



Mật mã liên quan đến việc thiết kế các hệ thống mật mã, trong khi phân tích mật mã nghiên cứu việc phá vỡ các hệ thống mật mã.

TỔNG QUAN VỀ MẬT MÃ

KHÁI NIỆM VỀ MẬT MÃ HIỆN ĐẠI

Dịch vụ bảo mật mật mã:

Mục tiêu chính của việc sử dụng mật mã là cung cấp 4 dịch vụ bảo mật thông tin cơ bản sau đây.

- Tính bí mật (Confidentiality).
- Tính toàn vẹn dữ liệu (Data integrity).
- Chứng thực(Authentication).
- Không thoái thác(Non-repudiation).

TỔNG QUAN VỀ MẬT MÃ

DỊCH VỤ BẢO MẬT BẰNG MẬT MÃ

Tính bí mật (Confidentiality):

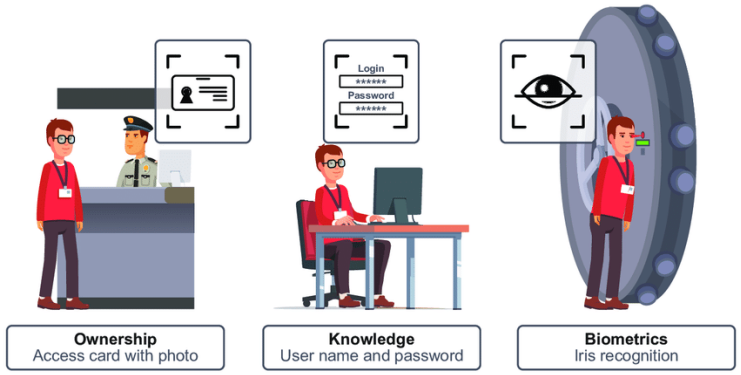
Tính bí mật là dịch vụ bảo mật cơ bản được cung cấp bảo mật mã. Đây là một dịch vụ bảo mật giữ thông tin từ một người không được ủy quyền. Nó đôi khi được gọi là quyền riêng tư (privacy) hoặc bí mật (secrecy)

Tính toàn vẹn dữ liệu (Data integrity):

Đây là dịch vụ bảo mật liên quan đến việc xác định bất kỳ thay đổi nào đối với dữ liệu. Dữ liệu có thể bị sửa đổi bởi một thực thể trái phép một cách cố ý hay vô tình. Dịch vụ toàn vẹn xác nhận rằng dữ liệu có nguyên vẹn hay không kể từ lần gần nhất nó được tạo, truyền hoặc lưu trữ bởi người được ủy quyền

TỔNG QUAN VỀ MẬT MÃ

DỊCH VỤ BẢO MẬT BẰNG MẬT MÃ



Chứng thực(Authentication):

Chứng thực cung cấp việc xác định người khởi tạo. Nó xác nhận với người nhận rằng dữ liệu nhận được chỉ được gửi bởi người gửi đã được xác định và xác minh.
Dịch vụ chứng thực có 2 biến thể:
Chứng thực tin nhắn - xác định người gửi tin nhắn mà không quan tâm đến bộ định tuyến hay hệ thống đã gửi tin nhắn.
Chứng thực thực thể - đảm bảo rằng dữ liệu đã được nhận từ một thực thể cụ thể, chẳng hạn được nhận từ 1 trang web cụ thể

Không thoái thác(Non-repudiation):

Dịch vụ bảo mật đảm bảo rằng một thực thể không thể từ chối quyền sở hữu của một cam kết hoặc một hành động trước đó. Đảm bảo rằng, người tạo ban đầu của dữ liệu không thể từ chối việc tạo hoặc truyền dữ liệu đó cho người nhận hoặc bên thứ ba.
Không thoái thác là một đặc tính được mong muốn nhất trong các tình huống có khả năng xảy ra tranh chấp về việc trao đổi dữ liệu.

TỔNG QUAN VỀ MẬT MÃ

DỊCH VỤ BẢO MẬT BẰNG MẬT MÃ

Các nguyên tắc mật mã:

Nguyên tắc mật mã là các công cụ và kỹ thuật trong mật mã. Nó có thể được sử dụng có chọn lọc để cung cấp một tập hợp các dịch vụ bảo mật theo mong muốn:

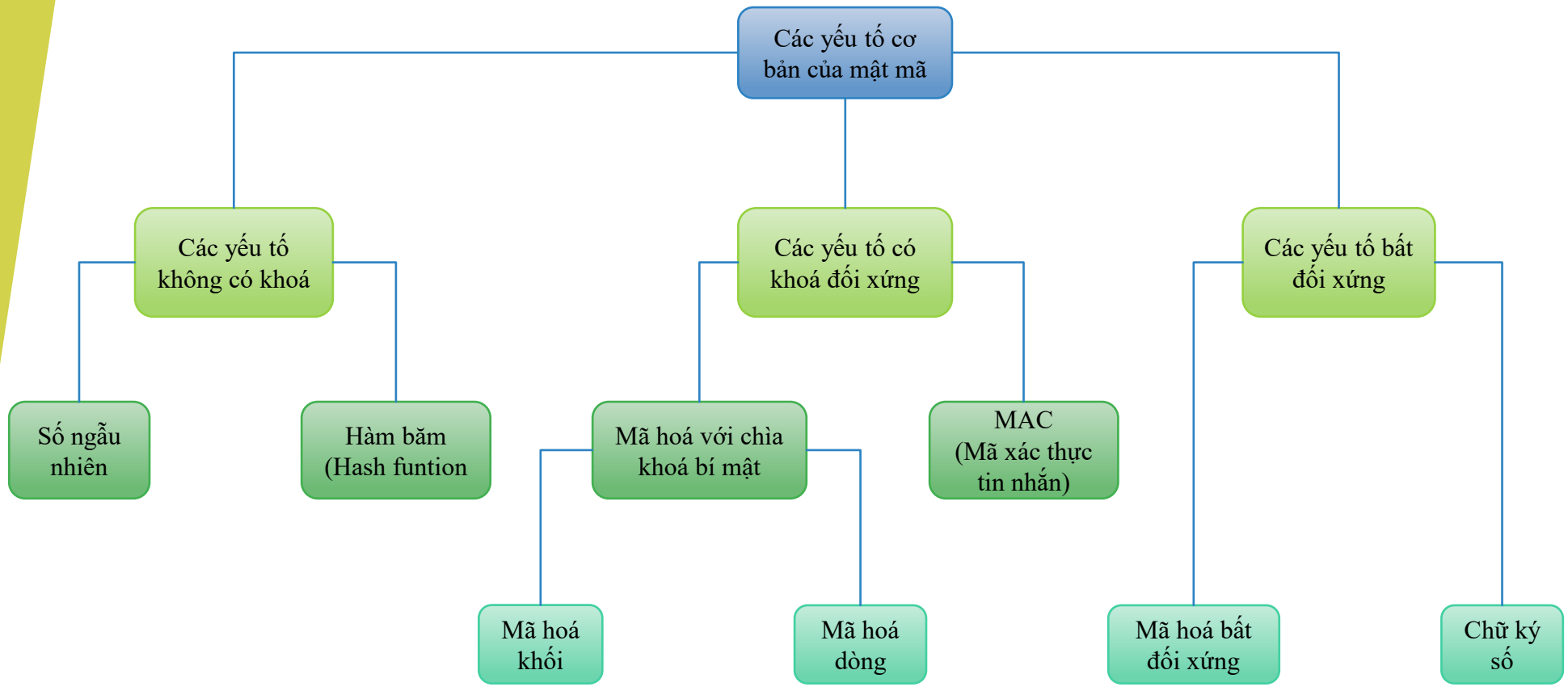
- Mã hóa (Encryption)
- Hàm băm (Hash Functions)
- Mã xác thực tin nhắn (Message Authentication codes - MAC)
- Chữ ký số (Digital Signatures).

Nguyên tắc Dịch vụ	Mã hóa	Hàm băm	MAC	Chữ ký số
Bí mật	Có	Không	Không	Không
Toàn vẹn	Không	Có thể có	Có	Có
Chứng thực	Không	Không	Có	Có
Không thoái thác	Không	Không	Có thể có	Có

Các nguyên tắc mật mã có liên quan phức tạp và chúng thường được kết hợp để đạt được một tập hợp các dịch vụ bảo mật mong muốn từ hệ thống mật mã

TỔNG QUAN VỀ MẬT MÃ

CÁC YẾU TỐ CƠ BẢN CỦA MẬT MÃ HIỆN ĐẠI



Sơ đồ các yếu tố cơ bản của mật mã

TỔNG QUAN VỀ MẬT MÃ

THÁCH THỨC CỦA HỆ THỐNG MẬT MÃ HIỆN ĐẠI

Những hạn chế của mật mã hiện đại:

Ngoài bốn yếu tố cơ bản của bảo mật thông tin, còn có các vấn đề khác ảnh hưởng đến việc sử dụng thông tin hiệu quả :

- Thông tin được mã hóa mạnh, xác thực và được ký điện tử có thể **khó truy cập ngay cả đối với người dùng hợp pháp** tại thời điểm quyết định quan trọng. Mạng hoặc hệ thống máy tính có thể bị kẻ xâm nhập tấn công và làm cho không hoạt động.
- **Tính sẵn sàng cao**, một trong những khía cạnh cơ bản của bảo mật thông tin, không thể được đảm bảo thông qua việc sử dụng mật mã. Các phương pháp khác là cần thiết để bảo vệ chống lại các mối đe dọa như từ chối dịch vụ hoặc sự cố hoàn toàn của hệ thống thông tin.
- Một nhu cầu cơ bản khác về bảo mật thông tin là **kiểm soát truy cập có chọn lọc** cũng không thể thực hiện được thông qua việc sử dụng mật mã. Kiểm soát hành chính và thủ tục, yêu cầu phải được thực hiện cùng một lúc.
- Mật mã không bảo vệ chống lại các lỗ hổng và **mối đe dọa xuất hiện từ một thiết kế kém của hệ thống**, giao thức và thủ tục. Những điều này cần được khắc phục thông qua thiết kế phù hợp và thiết lập cơ sở hạ tầng phòng thủ.
- Mã hóa đi kèm với chi phí (thời gian và tiền bạc):
  - Việc bổ sung các kỹ thuật mật mã trong quá trình xử lý thông tin dẫn đến sự chậm trễ.
  - Việc sử dụng mật mã khóa công khai yêu cầu thiết lập và bảo trì cơ sở hạ tầng khóa công khai đòi hỏi ngân sách tài chính dồi dào.

TỔNG QUAN VỀ MẬT MÃ

TƯƠNG LAI CỦA HỆ THỐNG MẬT MÃ HIỆN ĐẠI

Mật mã đường cong elip (ECC) đã được phát minh nhưng ưu điểm và nhược điểm của nó vẫn chưa được hiểu đầy đủ. ECC cho phép thực hiện mã hóa và giải mã trong thời gian ngắn hơn đáng kể, do đó cho phép truyền lượng dữ liệu cao hơn với độ bảo mật ngang nhau. Tuy nhiên, giống như các phương pháp mã hóa khác, ECC cũng phải được kiểm tra và chứng minh là an toàn trước khi được chấp nhận cho mục đích sử dụng cá nhân, thương mại và chính phủ.

Tính toán lượng tử là hiện tượng mới. Trong khi các máy tính hiện đại lưu trữ dữ liệu bằng định dạng nhị phân được gọi là "bit", trong đó có thể lưu trữ "1" hoặc "0"; một máy tính lượng tử lưu trữ dữ liệu bằng cách sử dụng chồng chất lượng tử của nhiều trạng thái. Nhiều trạng thái có giá trị này được lưu trữ trong "bit lượng tử" hoặc "qubit". Điều này cho phép tính toán các con số nhanh hơn vài bậc so với bộ xử lý bóng bán dẫn truyền thống.

Để hiểu sức mạnh của máy tính lượng tử, hãy xem xét RSA-640, một số có 193 chữ số, có thể được phân tích bởi 80 máy tính với tốc độ 2,2 GHz trong khoảng thời gian 5 tháng, một máy tính lượng tử sẽ phân tích trong vòng chưa đầy 17 giây. Những con số thường mất hàng tỷ năm để tính toán có thể chỉ mất vài giờ hoặc thậm chí vài phút với một máy tính lượng tử được phát triển đầy đủ.

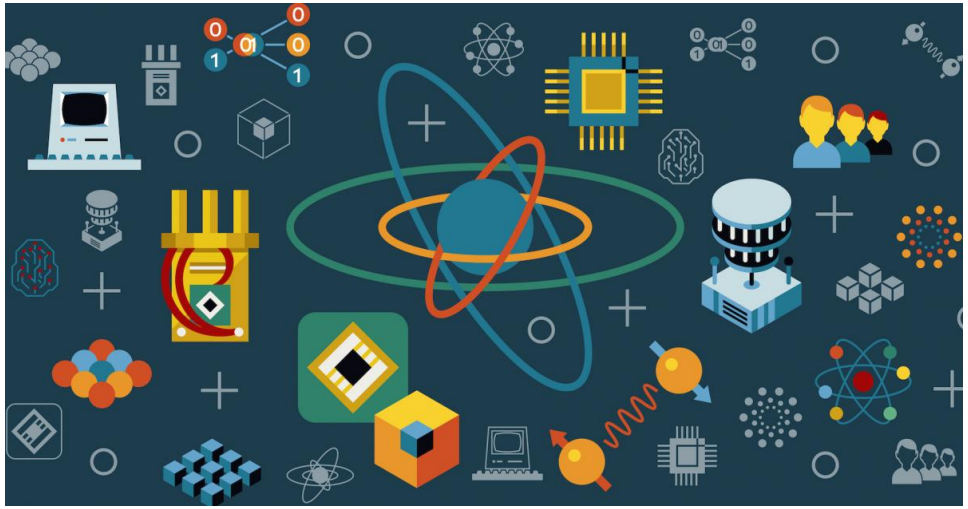
TỔNG QUAN VỀ MẬT MÃ

MẬT MÃ HẬU LƯỢNG TỬ

Sự phát triển của máy tính lượng tử mang đến những khả năng tính toán mới, trong một số trường hợp là chưa từng có. Tính bảo mật của hầu hết các ứng dụng mật mã, từ mã hóa và xác thực đơn giản đến các chức năng liên quan như đấu giá, hoặc bỏ phiếu điện tử, dựa trên các giả định nhất định về vấn đề nào dễ (có thể giải quyết nhanh chóng) và vấn đề nào khó (đòi hỏi thời gian dài). Theo đó, tính bảo mật của tất cả các ứng dụng này sẽ cần được xem xét lại dưới góc nhìn của các khả năng mới mà máy tính lượng tử mang lại.

Hai ứng dụng mật mã phổ biến nhưng khác biệt rõ ràng đang được phát triển bằng cách sử dụng các thuộc tính lượng tử, bao gồm:

- Mật mã an toàn lượng tử: Sự phát triển của các thuật toán mật mã, còn được gọi là mật mã hậu lượng tử, được bảo mật trước sự tấn công của máy tính lượng tử và được sử dụng để tạo chứng chỉ an toàn lượng tử.
- Phân phối khóa lượng tử: Quá trình sử dụng giao tiếp lượng tử để thiết lập khóa dùng chung giữa 2 bên đáng tin cậy để kẻ nghe lén không thể tìm hiểu bất kỳ điều gì về khóa đó.



TỔNG QUAN VỀ MẬT MÃ

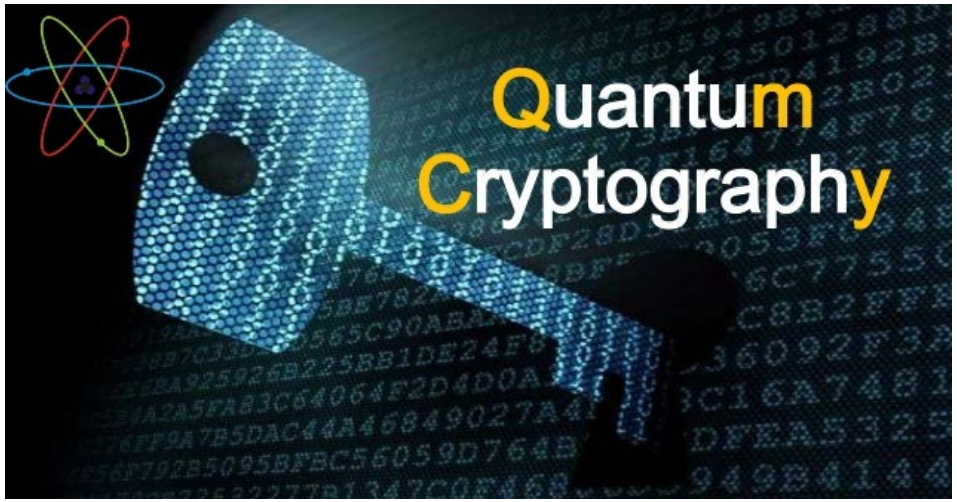
MẬT MÃ LƯỢNG TỬ - QUANTUM CRYPTOGRAPHY

Mật mã lượng tử sử dụng các nguyên tắc của cơ học lượng tử để mã hóa dữ liệu và truyền dữ liệu theo cách không thể bị hack

Mặc dù định nghĩa nghe có vẻ đơn giản, nhưng sự phức tạp nằm ở các nguyên tắc của cơ học lượng tử đằng sau mật mã lượng tử:

- Các hạt tạo nên vũ trụ vốn không chắc chắn và có thể đồng thời tồn tại ở nhiều nơi hoặc nhiều trạng thái tồn tại.
- Các photon được tạo ra ngẫu nhiên ở một trong 2 trạng thái lượng tử.
- Bạn không thể đo một thuộc tính lượng tử mà không thay đổi hoặc làm xáo trộn nó.
- Bạn có thể sao chép một số tính chất lượng tử của một hạt nhưng không phải toàn bộ hạt.

Tất cả những nguyên tắc này đóng một vai trò trong cách hoạt động của mật mã lượng tử.



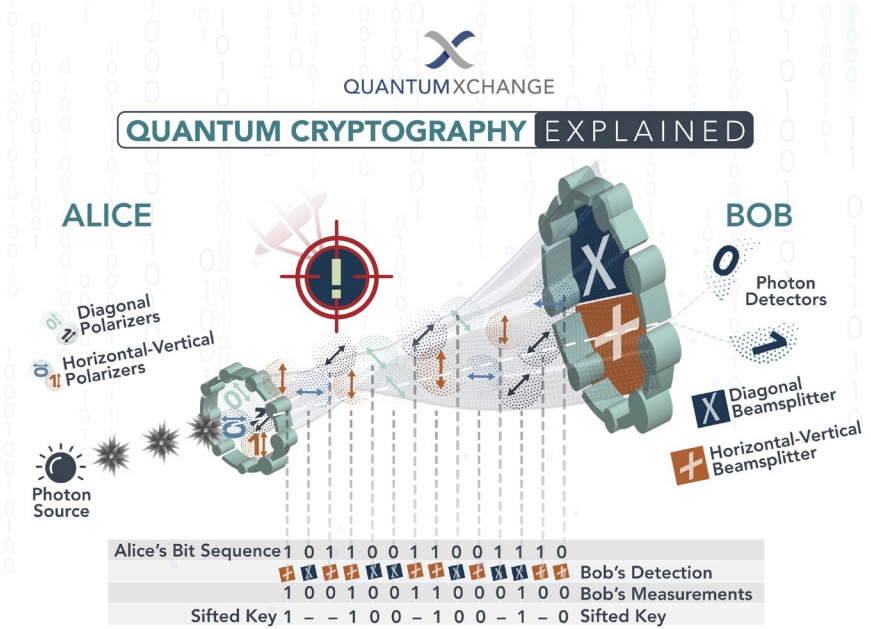
TỔNG QUAN VỀ MẬT MÃ

MẬT MÃ LƯỢNG TỬ - QUANTUM CRYPTOGRAPHY

Ví dụ về cách hoạt động của mã hóa lượng tử:

Alice và Bob muốn gửi một tin nhắn cho nhau mà không ai khác có thể ngăn chặn được. Với mã hóa lượng tử, Alice gửi cho Bob một loạt photon phân cực qua cáp quang. Cáp này không cần được bảo mật vì photon có trạng thái lượng tử ngẫu nhiên.

Nếu một kẻ nghe lén (KNL) cố gắng lắng nghe cuộc trò chuyện, hắn phải đọc từng photon để đọc được bí mật. Sau đó, KNL phải truyền photon đó cho Bob. Bằng cách đọc photon, KNL thay đổi trạng thái lượng tử của photon, điều này gây ra lỗi cho khóa lượng tử. Vấn đề này sẽ cảnh báo cho Alice và Bob biết rằng ai đó đang nghe lén và khóa đã bị xâm phạm, nên họ sẽ loại bỏ khóa. Alice phải gửi cho Bob một khóa mới không bị xâm phạm và sau đó Bob có thể sử dụng khóa đó để đọc tin nhắn.



TỔNG QUAN VỀ MẬT MÃ

MẬT MÃ TRUYỀN THỐNG VS MẬT MÃ LƯỢNG TỬ

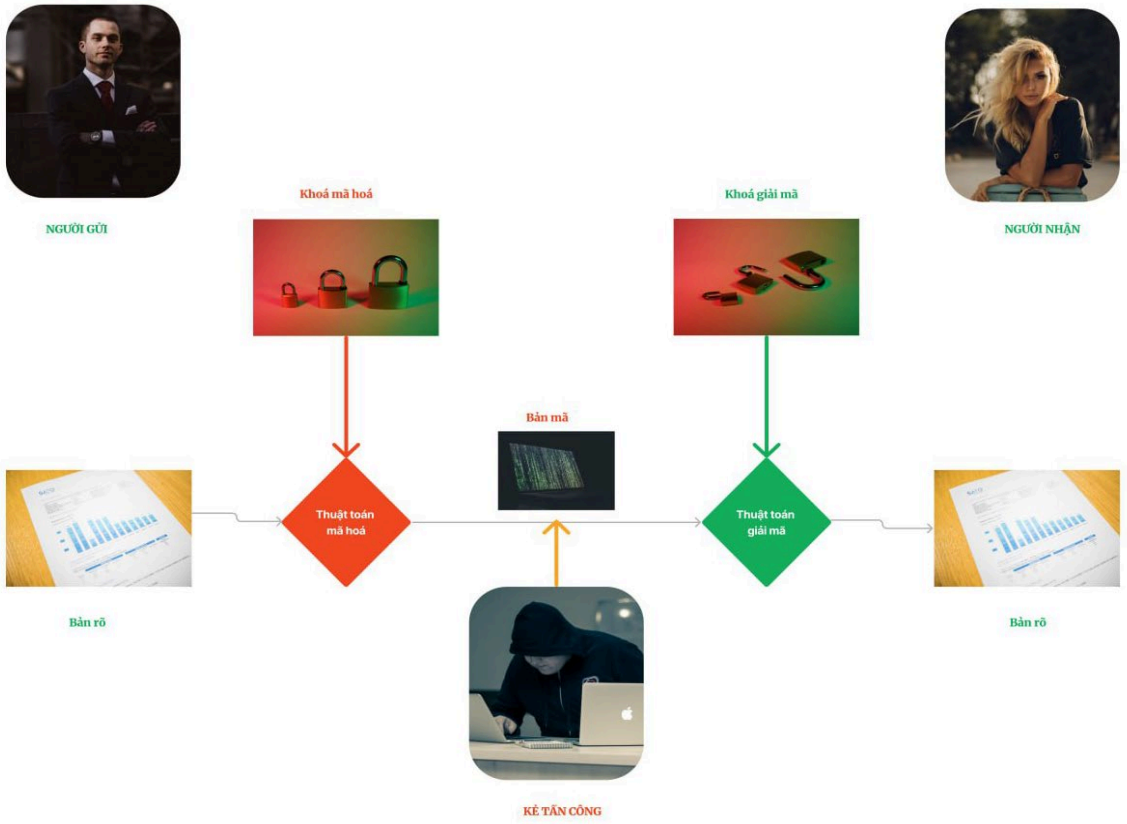
Mật mã truyền thống	Mật mã lượng tử
Sử dụng logic dựa trên logic kỹ thuật số	Sử dụng logic dựa trên lý thuyết lượng tử
Gửi tín hiệu số sử dụng bits (binary)	Gửi dữ liệu thông qua việc sử dụng các hạt hoặc photon
Thường không có phạm vi liên kết với nó	Thường có một phạm vi liên kết với nó (yêu cầu dây cáp quang và bộ repeater)
Mã hóa dựa trên các thuật toán toán học	Mã hóa dựa trên các thuộc tính của lượng tử

TỔNG QUAN VỀ MẬT MÃ

HỆ THỐNG MẬT MÃ

Hệ thống mật mã là việc triển khai các kỹ thuật mật mã và cơ sở hạ tầng đi kèm để cung cấp các dịch vụ bảo mật thông tin.

Mô hình hệ thống mật mã cơ bản:



TỔNG QUAN VỀ MẬT MÃ

HỆ THỐNG MẬT MÃ

Các thành phần của hệ thống mật mã:

- Bản rõ (plaintext): dữ liệu cần được bảo vệ trong quá trình truyền.
- Bản mã (ciphertext): phiên bản được xáo trộn của bản rõ, được tạo ra bởi thuật toán mã hóa bằng cách sử dụng một khó mã hóa cụ thể. Bản mã không được bảo vệ. Nó truyền trên kênh công cộng (public channel). Nó có thể bị chặn hoặc xâm phạm bởi bất kỳ ai có quyền truy cập vào kênh liên lạc.
- Thuật toán mã hóa(Encryption algorithm): đó là một quá trình toán học tạo ra một bản mã cho bất kỳ khóa mã hóa và bản rõ nào. Nó là thuật toán mã hóa lấy văn bản gốc và khóa mã hóa làm đầu vào để tạo ra một bản mã.
- Thuật toán giải mã(Decryption algorithm): Đây là một quá trình toán học, tạo ra một bản rõ duy nhất từ bất kỳ bản mã và khóa giải mã đã cho. Nó là một thuật toán mã hóa lấy bản mã và khóa giải mã làm đầu vào để xuất ra bản rõ. Thuật toán giải mã về cơ bản là đảo ngược của thuật toán mã hóa.
- Khóa mã hóa(Encryption key): Đó là một giá trị mà người gửi đã biết. Người gửi nhập khóa mã hóa vào thuật toán mã hóa cùng với bản rõ để tính toán ra bản mã.
- Khóa giải mã(Decryption key): là một giá trị được biết bởi người nhận. Khóa giải mã có liên quan đến khóa mã hóa, nhưng không phải lúc nào cũng giống với khóa mã hóa. Người nhận nhập khóa giải mã vào thuật toán giải mã cùng với bản mã để tính toán ra bản rõ.

Đối với một hệ thống mật mã nhất định, một tập hợp tất cả các khóa giải mã có thể được gọi là không gian khóa (key space).

Kẻ tấn công(chặn – interceptor) là một thực thể trái phép cố gắng xác định bản rõ (plaintext). Kẻ tấn công có thể xem bản mã và có thể biết thuật toán giải mã. Tuy nhiên interceptor không bao giờ biết được khóa giải mã.

TỔNG QUAN VỀ MẬT MÃ

HỆ THỐNG MẬT MÃ

Các loại hệ thống mật mã:

Về cơ bản, có 2 loại hệ thống mật mã dựa trên cách thức mã hóa – giải mã được thực hiện trong hệ thống:

- Mã hóa khóa đối xứng.
- Mã hóa khóa bất đối xứng.

Sự khác biệt chính giữa hai hệ thống mật mã này là mối quan hệ giữa khóa mã hóa và khóa giải mã. Về mặt logic, trong bất kỳ hệ thống mật mã nào, cả 2 khóa đều được liên kết chặt chẽ. Thực tế, không thể giải mã bản mã bằng khóa không liên quan đến khóa mã hóa.

Ngoài ra còn có hệ thống mật mã không khóa: hàm băm (Hash Function)

TỔNG QUAN VỀ MẬT MÃ

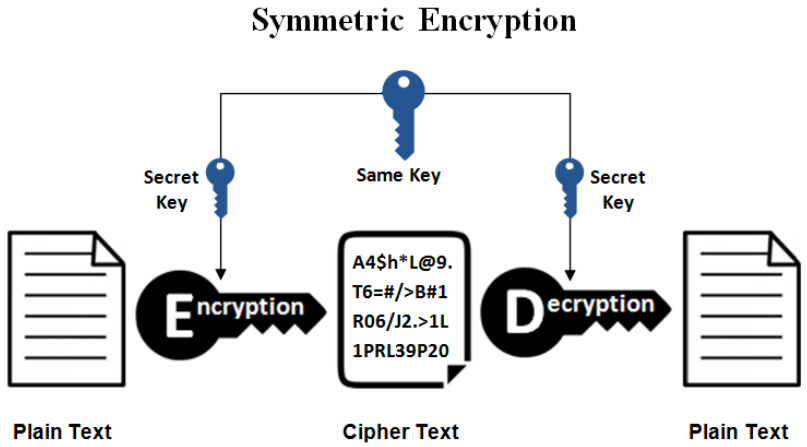
MÃ HÓA ĐỐI XỨNG – SYMMETRIC ENCRYPTION

Mã hóa khóa đối xứng (Symmetric Key Encryption):

Quá trình mã hóa, trong đó các khóa giống nhau được sử dụng để mã hóa và giải mã thông tin là Mã hóa khóa đối xứng.

Một số thuật toán nổi tiếng của mã hóa khóa đối xứng:

- Data Encryption Standard (DES – Tiêu chuẩn mã hóa dữ liệu),
- Triple-DES (3DES)
- AES – Rijndael (Advanced Encryption Standard – Tiêu chuẩn mã hóa tiên tiến)
- IDEA
- BLOWFISH
- .....



Trước năm 1970, tất các các hệ thống mật mã đều sử dụng mã hóa đối xứng. Thậm chí ngày nay, mức độ liên quan của nó là rất cao và nó đang được sử dụng rộng rãi trong nhiều hệ thống mật mã. Rất khó có khả năng mã hóa đối xứng sẽ biến mất vì nó có những ưu điểm nhất định so với mã hóa bất đối xứng.

TỔNG QUAN VỀ MẬT MÃ

MÃ HÓA ĐỐI XỨNG – SYMMETRIC ENCRYPTION

Thách thức của hệ thống mã hóa khóa đối xứng:

Có 2 thách thức hạn chế khi sử dụng mật mã khóa đối xứng:

- Thiết lập khóa: Trước bất kỳ giao tiếp nào, cả người gửi và người nhận cần đồng ý về khóa bí mật. Nó yêu cầu một cơ chế thiết lập khóa an toàn tại chỗ.

- Sự cố tin cậy: Vì người gửi và người nhận sử dụng cùng một khóa đối xứng, nên có một yêu cầu ngầm định rằng người gửi và người nhận "tin tưởng" lẫn nhau. Ví dụ: có thể xảy ra trường hợp người nhận bị mất khóa vào tay kẻ tấn công và người gửi không được thông báo.

Hai thách thức này rất hạn chế với giao tiếp hiện đại. Ngày nay, mọi người cần trao đổi thông tin với những bên không quen biết và không tin cậy. Những hạn chế này của mã hóa đối xứng đã dẫn đến các sơ đồ Mã hóa khóa bất đối xứng.

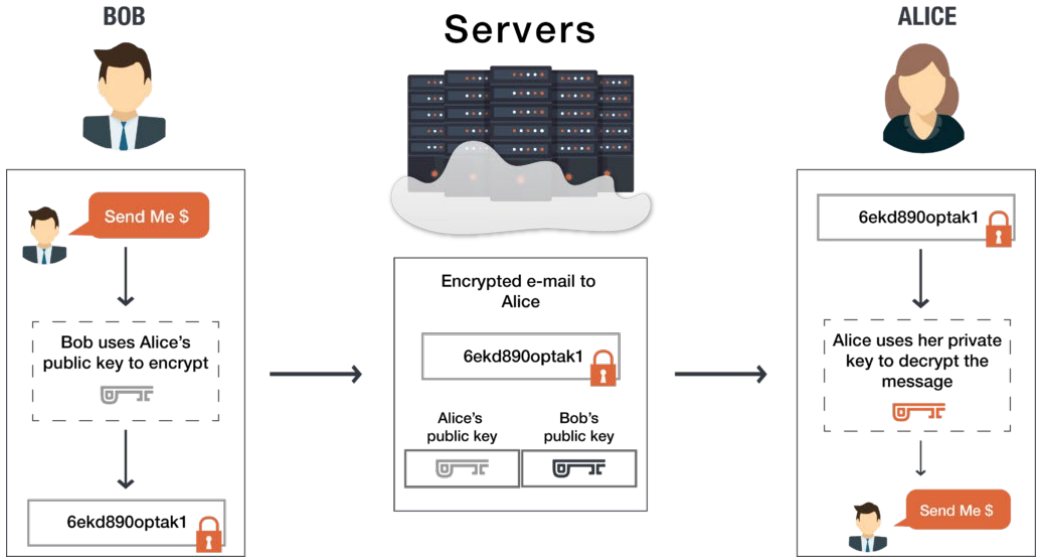
TỔNG QUAN VỀ MẬT MÃ

MÃ HÓA BẤT ĐỐI XỨNG - ASYMMETRIC ENCRYPTION

Mã hóa khóa bất đối xứng:

Quá trình mã hóa trong đó các khóa khác nhau được sử dụng để mã hóa và giải mã thông tin được gọi là Mã hóa khóa bất đối xứng.

Mặc dù các khóa khác nhau nhưng chúng có liên quan về mặt toán học, do đó việc truy xuất bản rõ bằng cách giải mã bản mã là khả thi. Quá trình được mô tả trong hình sau:



Mã hóa bất đối xứng được phát minh vào thế kỷ 20 để đáp ứng nhu cầu về khóa bí mật được chia sẻ trước giữa những người giao tiếp

TỔNG QUAN VỀ MẬT MÃ

MÃ HÓA BẤT ĐỐI XỨNG - ASYMMETRIC ENCRYPTION

Thách thức của hệ thống mã hóa khóa bất đối xứng:

Hệ thống mật mã khóa công khai có một thách thức đáng kể - người dùng cần tin tưởng rằng khóa công khai mà họ đang sử dụng để mã hóa phải đúng là khóa công khai của người mà họ cần gửi thông tin và không bị giả mạo bảo bên thứ ba.

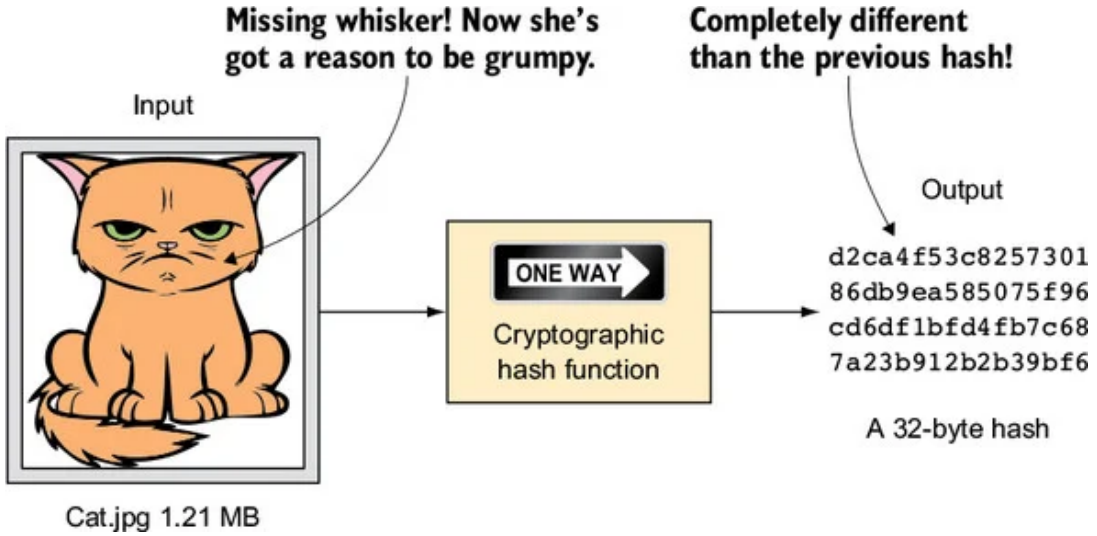
Điều này thường được thực hiện thông qua Cơ sở hạ tầng khóa công khai (KPI – Public Key Infrastructure) của bên thứ ba đáng tin cậy. Bên thứ ba quản lý an toàn và chứng thực tính xác thực của khóa công khai. Khi bên thứ ba được yêu cầu cung cấp khóa công khai cho bất kỳ người liên lạc (NLL) nào, thì họ được tin cậy để cung cấp đúng khóa công khai.

Bên thứ ba tự xác minh về danh tính người dùng bằng quy trình chứng thực, công chức hay một số quy trình khác rằng, NLL là duy nhất. Phương pháp phổ biến nhất để cung cấp các khóa công khai đã xác minh là nhúng chúng trong một chứng chỉ được ký điện tử bởi bên thứ ba đáng tin cậy.

TỔNG QUAN VỀ MẬT MÃ

HÀM BĂM – HASH FUNCTION

Hàm băm (Hash function): là một hàm toán học chuyển đổi một giá trị số đầu vào thành một giá trị số nén khác. Đầu vào của hàm băm có độ dài tùy ý nhưng đầu ra luôn có độ dài cố định. Hàm băm còn được gọi là mã hóa một chiều tức là chỉ có chiều mã hóa chứ không có chiều giải mã (vì không có key)

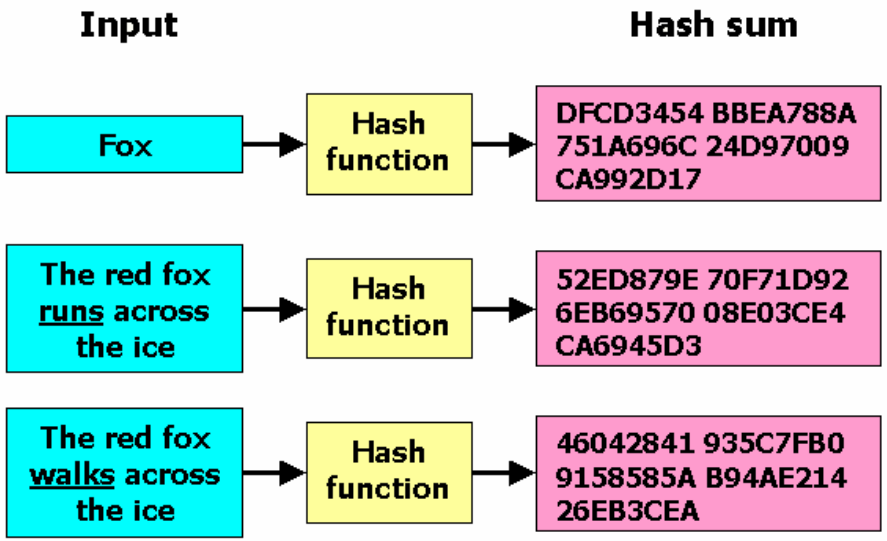


TỔNG QUAN VỀ MẬT MÃ

HÀM BĂM – HASH FUNCTION

Các tính năng điển hình của hàm băm là:

- Đầu ra độ dài cố định (Giá trị băm)
  - Hàm băm chuyển đổi dữ liệu có độ dài tùy ý thành độ dài cố định. Quá trình này được gọi là băm dữ liệu.
  - Hàm băm nhỏ hơn nhiều so với dữ liệu đầu vào, đó đó hàm băm đôi khi được gọi là hàm nén.
  - Vì hàm băm là đại diện nhỏ hơn của dữ liệu lớn hơn, nên nó còn được gọi là bản tóm tắt.
  - Hàm băm có đầu ra n bit được gọi là hàm băm n bit. Các hàm băm phổ biến tạo ra các giá trị từ 160 đến 512 bit.
- Hiệu quả hoạt động
  - Nói chung đối với bất kỳ hàm băm h nào có đầu vào x, thì việc tính toán h(x) là một thao tác nhanh.
  - Các hàm băm tính toán nhanh hơn nhiều so với mã hóa đối xứng.



Thuộc tính của hàm băm:

- Chống nghịch ảnh: tính một chiều (không thể "khôi phục" hàm băm).
- Chống nghịch ảnh thứ hai: tính duy nhất (không thể tìm thấy dữ liệu đầu vào thứ hai xung đột với một dữ liệu đầu vào cho trước).
- Kháng va chạm: hai dữ liệu đầu vào khác nhau không thể tạo ra cùng một mã băm.

TỔNG QUAN VỀ MẬT MÃ

ĐÁNH GIÁ TÍNH AN TOÀN CỦA MỘT HỆ MẬT MÃ

Ta có thể kết luận một hệ mã mật là không an toàn (insecure), bằng việc chỉ ra cách phá nó trong một mô hình tấn công phổ biến, trong đó ta chỉ rõ được các mục tiêu về an toàn bảo mật (security) không được đảm bảo đúng. Tuy nhiên để kết luận rằng một hệ mã là an toàn cao thì công việc phức tạp hơn nhiều.

Thông thường, người ta phải đánh giá hệ mật mã này trong nhiều mô hình tấn công khác nhau, với độ khó tăng dần. Để có thể khẳng định tính an toàn cao, cách làm lý tưởng là đưa ra một chứng mình hình thức (formal proof), trong đó người ta chứng minh bằng công cụ toán học là tính an toàn bảo mật của hệ mã đang xét là tương đương với một hệ mã kinh điển, mà tính an toàn của nó đã khẳng định rộng rãi từ lâu.

TỔNG QUAN VỀ MẬT MÃ

ĐÁNH GIÁ TÍNH AN TOÀN CỦA MỘT HỆ MẬT MÃ

Như đã nói trên, người ta phủ định tính an toàn của một hệ mã mật thông qua việc chỉ ra cách phá cụ thể hệ mã này trên một mô hình tấn công (attack model) cụ thể. Mỗi mô hình tấn công sẽ định nghĩa rõ năng lực của kẻ tấn công, bao gồm năng lực tài nguyên tính toán, loại thông tin mà nó có khả năng tiếp cận để khai thác và khả năng tiếp xúc với máy mật mã (thiết bị phần cứng có cài đặt thuật toán sinh và giải mã).

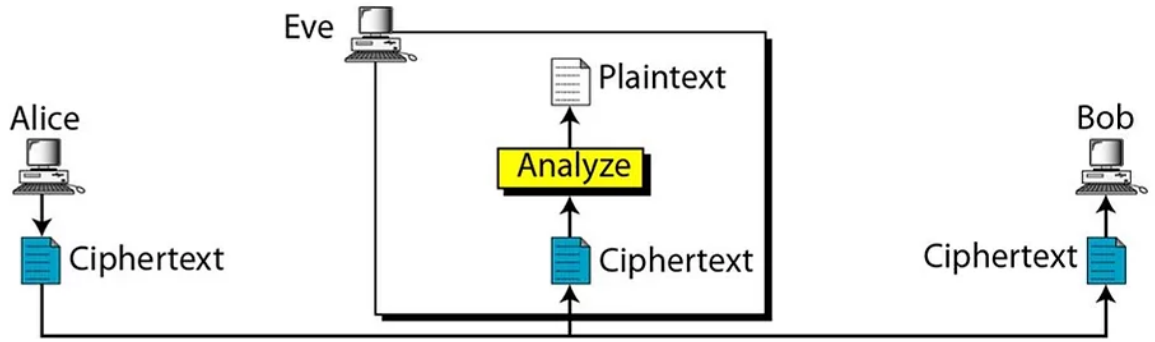
Các mô hình tấn công thường được sắp xếp theo thứ tự mạnh dần năng lực của kẻ tấn công. Nếu một hệ mật mã bị phá vỡ trong một mô hình tấn công căn bản (năng lực kẻ tấn công là bình thường) thì sẽ bị đánh giá là hoàn toàn không an toàn. Sau đây là một số mô hình tấn công phổ biến.

TỔNG QUAN VỀ MẬT MÃ

CÁC KIỂU TẤN CÔNG MẬT MÃ

Các mô hình tấn công

Tấn công chỉ-biết-bản-mã (ciphertext-only attack). Ở đây kẻ địch E chỉ là một kẻ hoàn toàn bên ngoài, tìm cách nghe trộm trên đường truyền để lấy được các giá trị Y, bản mã của thông tin gửi đi. Mặc dù kẻ địch E chỉ biết các bản rõ Y, nhưng mục tiêu nó hướng tới là khám phá nội dung một/nhiều bản rõ X hoặc lấy được khóa mật Z (trường hợp phá giải hoàn toàn).



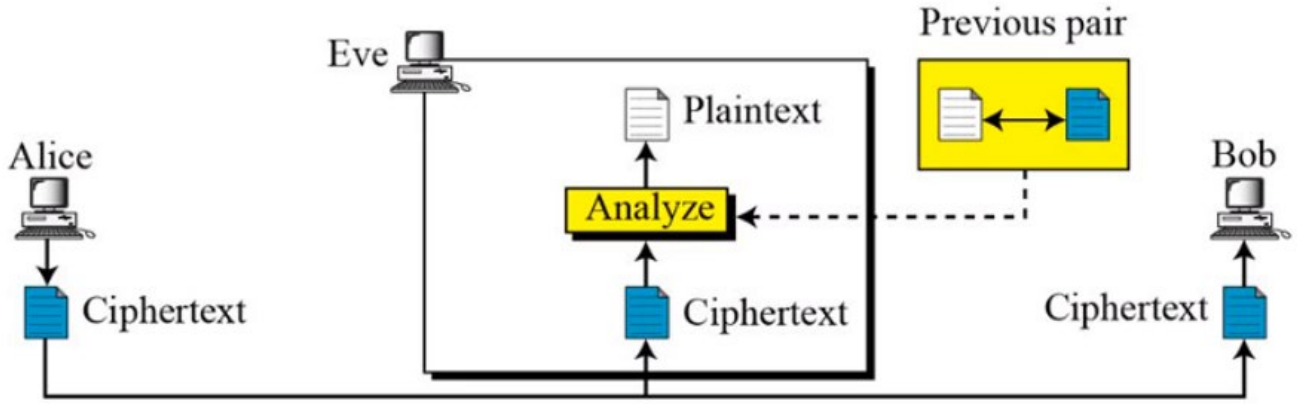
Đây là mô hình tấn công căn bản nhất trong đó kẻ địch không có năng lực quan hệ đặc biệt (như một số hình thức tấn công sau), diện thông tin tiếp xúc chỉ là các bản mã. Rõ ràng nếu một hệ mã mà không đứng vững được trong mô hình này thì phải đánh giá là không đáng tin cậy.

TỔNG QUAN VỀ MẬT MÃ

CÁC KIỂU TẤN CÔNG MẬT MÃ

Tấn công biết-bản-rõ (known-plaintext attack). Mặc dù tên gọi hơi dễ hiểu nhầm, thực chất trong mô hình này ta chỉ giả thiết là E có thể biết một số cặp X-Y (bản rõ và bản mã tương ứng) nào đó.

Nguyên nhân E thu được có thể hoàn toàn tình cờ hoặc nhờ một vài tay trong là nhân viên thấp cấp trong hệ thống. Tất nhiên mục tiêu của E là khám phá nội dung các bản rõ quan trọng khác và/hoặc lấy được khóa mật.



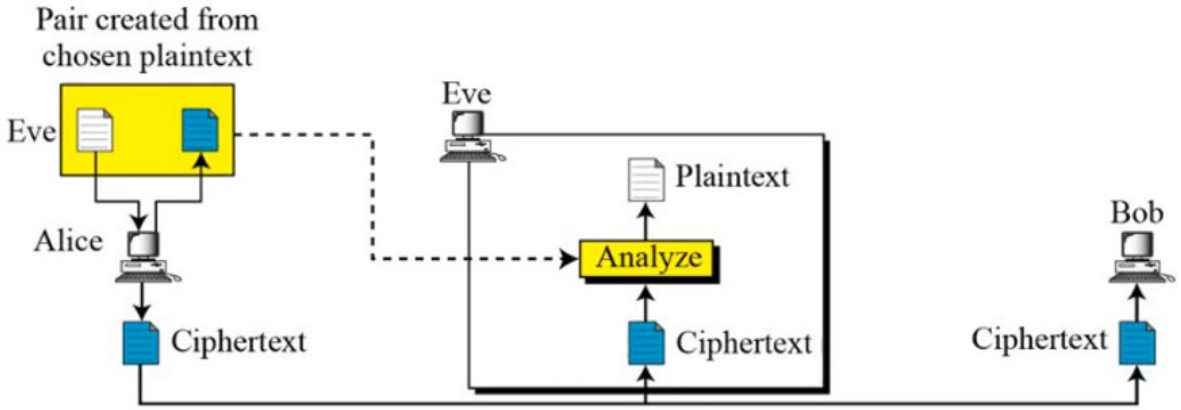
Rõ ràng mô hình tấn công này làm mạnh hơn so với tấn công chỉ qua bản mã: Việc biết một số cặp X-Y sẽ làm bổ sung thêm đầu mối phân tích; đặc biệt từ bây giờ E có thể dùng phép thử loại trừ để vét cạn không gian khóa (exshautive key search) và tìm ra khóa đúng tức là sao cho Enc (K,X)=Y.

TỔNG QUAN VỀ MẬT MÃ

CÁC KIỂU TẤN CÔNG MẬT MÃ

Tấn công bản-rõ-chọn-sẵn (chosen-plaintext attack). Trong mô hình này, không những E thu nhặt được một số cặp X-Y mà một số bản rõ X do bản thân E soạn ra (chosen plaintext).

Điều này thoạt nghe có vẻ không khả thi thực tế, tuy nhiên ta có thể tưởng tượng là E có tay trong là một thư ký văn phòng của công ty bị tấn công, ngoài ra do một qui định máy móc nào đó tất cả các văn bản dù quan trọng hay không đều được truyền gửi mật mã khi phân phát giữa các chi nhánh của công ty này.



Có thể nhận xét thấy rằng, việc được tự chọn giá trị của một số bản rõ X sẽ thêm nhiều lợi ích cho E trong phân tích quan hệ giữa bản mã và bản rõ để từ đó lần tìm giá trị khóa.

TỔNG QUAN VỀ MẬT MÃ

CÁC MÔ HÌNH ĐÁNH GIÁ TÍNH AN TOÀN CỦA MỘT HỆ MẬT MÃ

Bảo mật vô điều kiện (unconditional security):

Đây là mô hình đánh giá an toàn bảo mật mức cao nhất, trong đó "vô điều kiện" được hiểu theo ý nghĩa của lý thuyết thông tin (information theory), trong đó các ý niệm về "lượng tin" được hình thức hóa thông qua các phép toán xác suất.

Trong mô hình này, kẻ địch được coi là không bị hạn chế về năng lực tính toán, tức là có thể thực hiện bất kỳ khối lượng tính toán cực lớn nào đặt ra trong khoảng thời gian ngắn bất kỳ. Mặc dù có năng lực tính toán siêu nhiên như vậy, mô hình này chỉ giả thiết kẻ tấn công là người ngoài hoàn toàn (tức là ứng với mô hình tấn công chỉ biết-bản-mã).

Một hệ mật mã đạt được mức an toàn vô điều kiện, tức là có thể đứng vững trước sức mạnh của một kẻ địch bên ngoài (chỉ biết bản mã) có khả năng không hạn chế tính toán, được gọi là đạt đến bí mật tuyệt đối (perfect secretcy).

TỔNG QUAN VỀ MẬT MÃ

CÁC MÔ HÌNH ĐÁNH GIÁ TÍNH AN TOÀN CỦA MỘT HỆ MẬT MÃ

Bảo mật chứng minh được (provable security):

Đây cũng là một mô hình đánh giá mức rất cao, lý tưởng trong hầu hết các trường hợp. Một hệ mật mã đạt được mức đánh giá này đối với một mô hình tấn công cụ thể nào đó, nếu ta có thể chứng mình bằng toán học rằng tính an toàn của hệ mật là được qui về tính NP-khó của một bài toán nào đó đã được biết từ lâu (ví dụ bài toán phân tích ra thừa số nguyên tố, bài toán cái túi, bài toán tính logarit rời rạc ...).

Nói một cách khác ta phải chứng minh được là kẻ thù muốn phá được hệ mã thì phải thực hiện một khối lượng tính toán tương đương hoặc hơn với việc giải quyết một bài toán NP-khó đã biết.

TỔNG QUAN VỀ MẬT MÃ

CÁC MÔ HÌNH ĐÁNH GIÁ TÍNH AN TOÀN CỦA MỘT HỆ MẬT MÃ

Bảo mật tính toán được, hay bảo mật thực tiễn (computational security hay practical security):

Đây là một trong những mức đánh giá thường được áp dụng nhất trong thực tế (khi những mức bảo mật cao hơn được cho là không thể đạt tới). Khi đánh giá ở mức này với một hệ mã cụ thể, người ta lượng hóa khối lượng tính toán đặt ra để có thể phá hệ mã này, sử dụng kiểu tấn công mạnh nhất đã biết (thường kèm theo đó là mô hình tấn công phổ biến mạnh nhất).

Từ việc đánh giá được khối lượng tính toán này cùng thời gian thực hiện (với năng lực kẻ địch mạnh nhất có thể trên thực tế), và so sánh với thời gian đòi hỏi đảm bảo tính mật trên thực tế, ta có thể đánh giá hệ mã có đạt an toàn thực tiễn cao hay không. Đôi khi, cơ sở đánh giá cũng dựa vào một bài toán khó nào đó mặc dù không đưa ra được một chứng minh tương đương thực sự.

TỔNG QUAN VỀ MẬT MÃ

CÁC MÔ HÌNH ĐÁNH GIÁ TÍNH AN TOÀN CỦA MỘT HỆ MẬT MÃ

Bảo mật tự tác (ad hoc security):

Một số hệ mật mã riêng được một số công ty hoặc cá nhân tự chế để phục vụ mục đích đặc biệt dùng nội bộ. Tác giả loại hệ mật mã có thể sử dụng những lập luận đánh giá hợp lý nhất định dựa trên việc ước đoán khối lượng tính toán của kẻ địch khi sử dụng những tấn công mạnh nhấn đã biết và lập luận về tính bất khả thi thực tiễn để thực hiện.

Mặc dù vậy hệ mật mã này vẫn có thể bị phá bởi những tấn công có thể tồn tại mà chưa được biết tới đến thời điểm đó; vì vậy, thực tế bảo mật ở mức này hàm nghĩa không có một chứng minh đảm bảo thực sự, nên không thể coi là tin cậy với đại chúng.

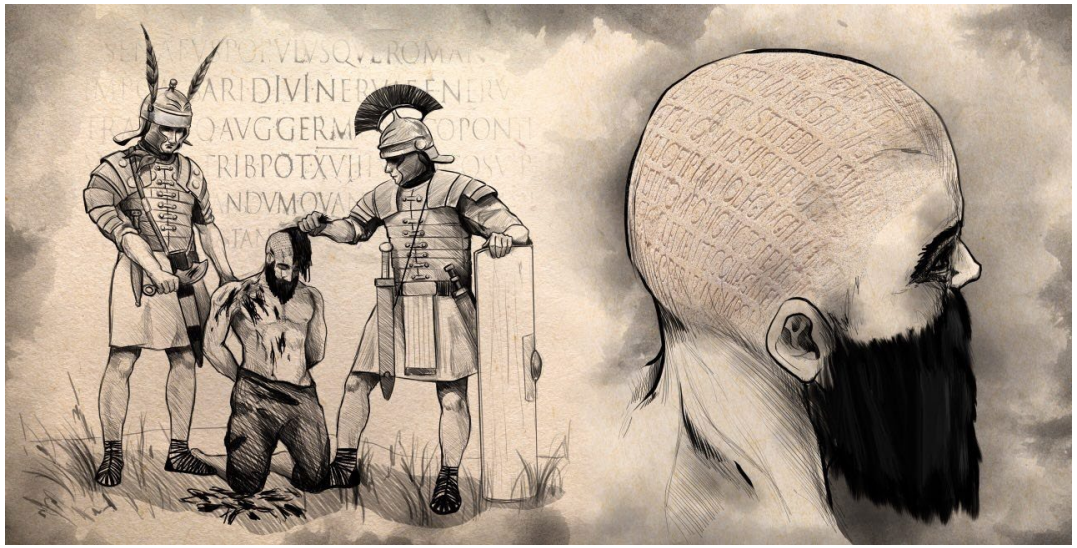
CÁC KỸ THUẬT GIẤU TIN

SƠ LƯỢC VỀ LỊCH SỬ GIẤU TIN

Ý tưởng về che giấu thông tin đã có từ hàng nghìn năm về trước nhưng kĩ thuật này được dùng chủ yếu trong quân đội và trong các cơ quan tình báo.

Mãi cho tới vài thập niên gần đây, giấu thông tin mới nhận được sự quan tâm của các nhà nghiên cứu và các viện công nghệ thông tin với rất nhiều công trình nghiên cứu. Cuộc cách mạng số hóa thông tin và sự phát triển nhanh chóng của mạng truyền thông là nguyên nhân chính dẫn đến sự thay đổi này.

Những phiên bản sao chép hoàn hảo, các kĩ thuật thay thế, sửa đổi tinh vi cộng với sự lưu thông trên mạng của các dữ liệu đa phương tiện đã sinh ra rất nhiều những vấn đề nhức nhối về nạn ăn cắp bản quyền, phân phối bất hợp pháp, xuyên tạc trái phép, đây là lúc công nghệ giấu tin được chú ý và phát triển.



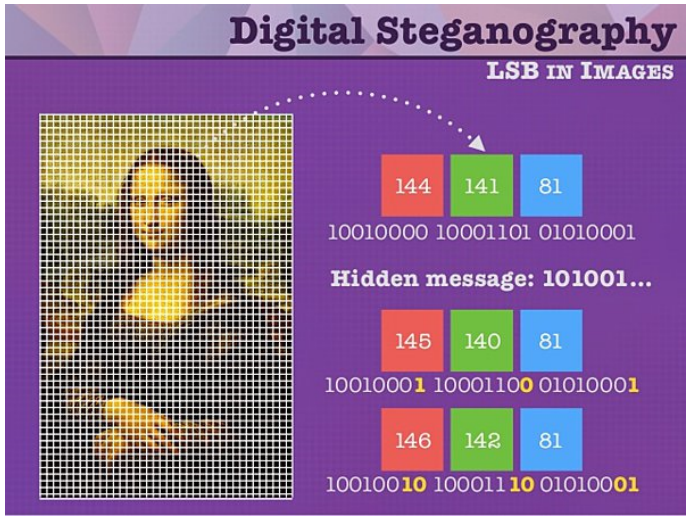
CÁC KỸ THUẬT GIẤU TIN

KHÁI NIỆM GIẤU TIN

"Giấu tin – Information hiding" là một kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác.

Kỹ thuật giấu tin nhằm hai mục đích:

- Bảo mật cho dữ liệu được đem giấu,
- Bảo vệ cho chính đối tượng mang tin giấu.



Hai mục đích khác nhau này dẫn đến hai kỹ thuật chủ yếu của giấu tin. Đó là giấu tin mật (Steganography) và thủy vân số (Watermarking).

- **Kỹ thuật giấu tin mật (Steganography):**

Với mục đích đảm bảo an toàn và bảo mật thông tin được giấu. Các kỹ thuật giấu tin mật tập trung vào việc sao cho thông tin giấu được nhiều và người khác khó phát hiện ra thông tin có được giấu trong hay không.

- **Kỹ thuật thủy vân số (Watermarking):**

Với mục đích bảo mật cho chính các đối tượng giấu tin. Đảm bảo một số các yêu cầu như: tính bền vững, khẳng định bản quyền sở hữu hay phát hiện xuyên tạc thông tin.

CÁC KỸ THUẬT GIẤU TIN

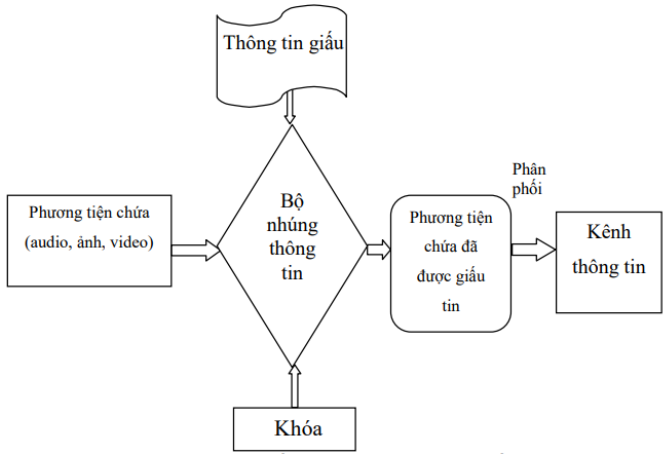
MÔ HÌNH KỸ THUẬT GIẤU THÔNG TIN CƠ BẢN

Để thực hiện giấu tin cần xây dựng được các thủ tục giấu tin. Các thủ tục này sẽ thực hiện nhúng thông tin cần giấu vào môi trường giấu tin.

Các thủ tục giấu tin thường được thực hiện với một khóa giống như các hệ mật mã để tăng tính bảo mật. Sau khi giấu tin ta thu được đối tượng chứa thông tin giấu và có thể phân phối đối tượng đó trên kênh thông tin.

Giấu thông tin vào phương tiện chứa và tách lấy thông tin là hai quá trình trái ngược nhau và có thể mô tả qua sơ đồ khối của hệ thống trong đó:

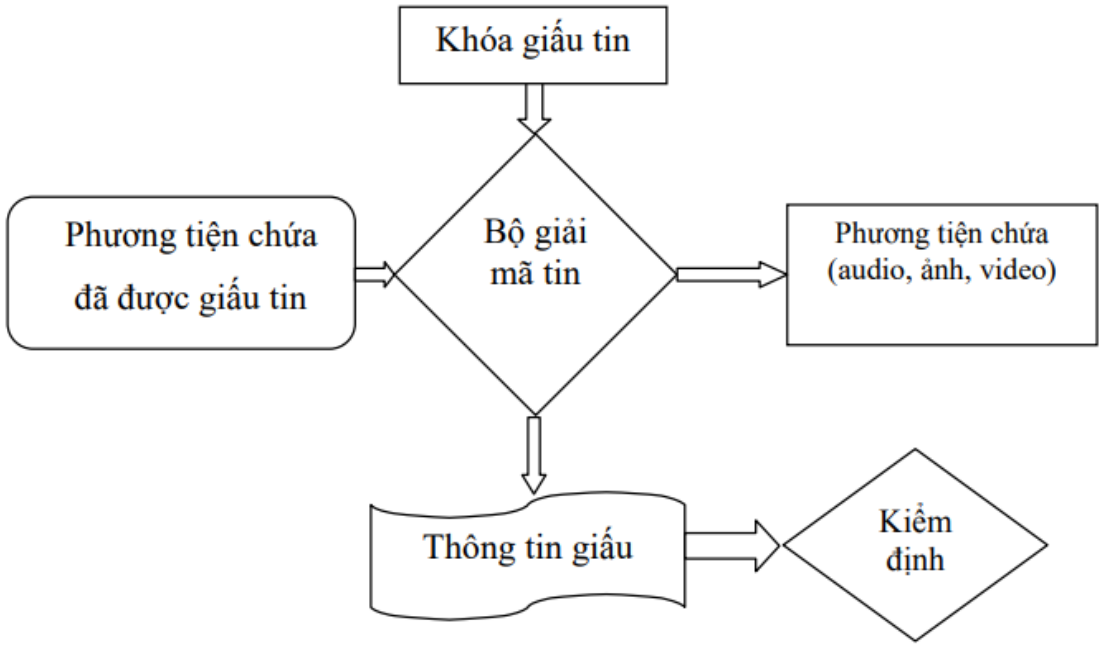
- **Thông tin cần giấu tuỳ theo mục đích của người sử dụng**, nó có thể là thông điệp (với các tin bí mật) hay các logo, hình ảnh bản quyền.
- **Phương tiện chứa**: các file ảnh, text, audio… là môi trường để nhúng tin.
- **Bộ nhúng thông tin**: là những chương trình thực hiện việc giấu tin.
- **Đầu ra:** là các phương tiện chứa đã có tin giấu trong đó.



CÁC KỸ THUẬT GIẤU TIN

MÔ HÌNH KỸ THUẬT GIẤU THÔNG TIN CƠ BẢN

Sau khi nhận được đối tượng phương tiện chứa có giấu thông tin, quá trình giải mã được thực hiện thông qua một bộ giải mã tương ứng với bộ nhúng thông tin cùng với khoá của quá trình nhúng. Kết quả thu được gồm phương tiện chứa gốc và thông tin đã giấu. Bước tiếp theo thông tin đã giấu sẽ được xử lý kiểm định so sánh với thông tin ban đầu.



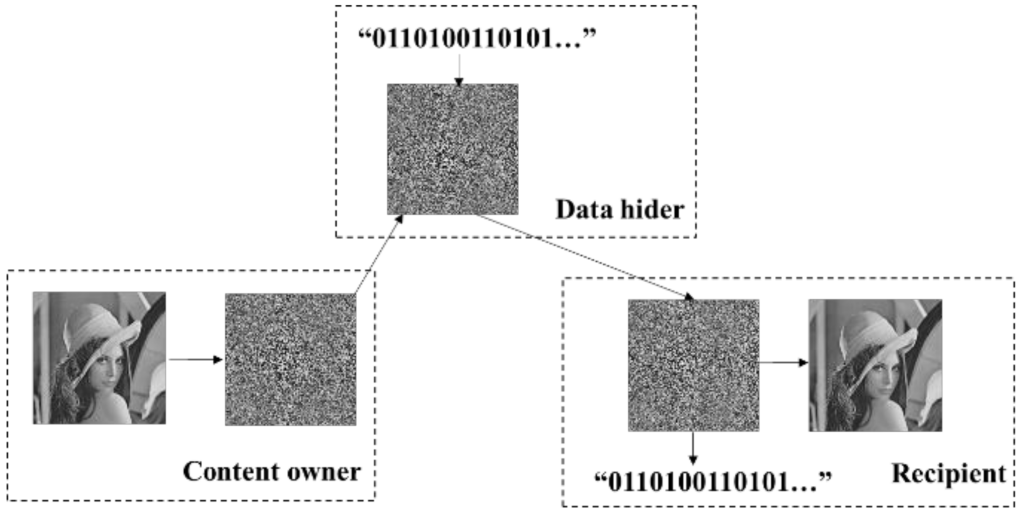
CÁC KỸ THUẬT GIẤU TIN

MÔI TRƯỜNG GIẤU TIN

Giấu thông tin trong ảnh số (Data Hiding in Image)

Giấu thông tin trong ảnh số là một phần của khái niệm giấu thông tin với việc sử dụng ảnh số làm phương tiện chứa. Hiện nay, giấu thông tin trong ảnh là một phương pháp chiếm tỉ lệ lớn nhất trong các chương trình ứng dụng.

Các phần mềm hệ thống giấu tin trong đa phương tiện bởi lượng thông tin được trao đổi trong hình ảnh là rất lớn và hơn nữa giấu thông tin trong ảnh cũng đóng vai trò hết sức quan trọng trong hầu hết các ứng dụng bảo vệ an toàn thông tin như: xác thực thông tin, xác định làm thay đổi thông tin, bảo vệ bản quyền tác giả, điều khiển truy cập, giấu thông tin mật.



CÁC KỸ THUẬT GIẤU TIN

MÔI TRƯỜNG GIẤU TIN

Giấu thông tin trong ảnh số (Data Hiding in Image) (tiếp)

Ngày nay, khi ảnh số đã được sử dụng khá phổ biến, thì giấu thông tin trong ảnh đã đem lại nhiều ứng dụng quan trọng trên các lĩnh vực của đời sống xã hội. Ví dụ như đối với các nước phát triển, chữ ký tay đã được số hoá và lưu trữ sử dụng như là hồ sơ cá nhân của các dịch vụ ngân hàng và tài chính. Nó được dùng để xác thực trong các thẻ tín dụng của người tiêu dùng.

Trong một số ứng dụng về nhận diện thẻ chứng minh, thẻ căn cước, hộ chiếu..., người ta có thể giấu thông tin trên các ảnh thẻ để xác định thông tin thực.

Một đặc điểm của giấu thông tin trong ảnh đó là thông tin được giấu một cách "vô hình". Nó như là cách thức truyền thông tin mật cho nhau mà người khác không thể biết được, bởi sau khi giấu thông tin thì chất lượng ảnh gần như không thay đổi, đặc biệt đối với ảnh màu hay ảnh xám.

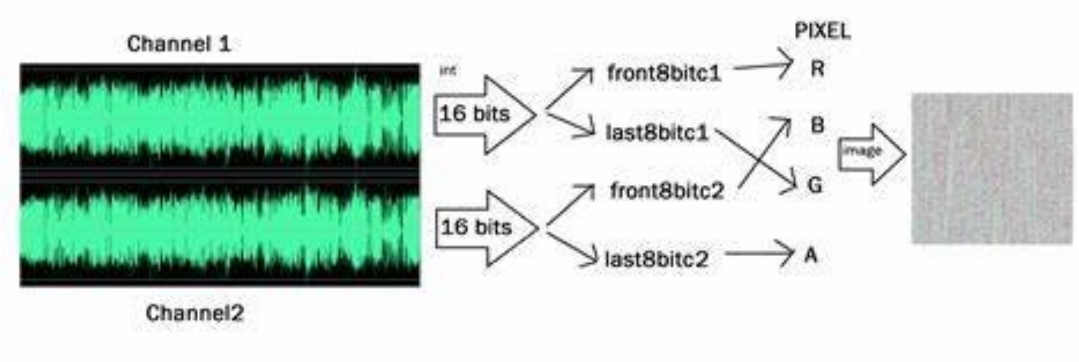
CÁC KỸ THUẬT GIẤU TIN

MÔI TRƯỜNG GIẤU TIN

Giấu thông tin trong audio (Data Hiding in Audio)

Giấu thông tin trong audio mang những đặc điểm riêng khác với giấu thông tin trong các đối tượng đa phương tiện khác. Một trong những yêu cầu cơ bản của giấu thông tin là đảm bảo tính chất "ẩn" của thông tin được giấu đồng thời không làm ảnh hưởng đến chất lượng của dữ liệu. Kỹ thuật giấu thông tin trong ảnh phụ thuộc vào hệ thống thị giác của con người - HVS (Human Vision System), còn kỹ thuật giấu thông tin trong audio lại phụ thuộc vào hệ thống thính giác - HAS (Human Auditory system).

Một vấn đề phức tạp ở đây là hệ thống thính giác của con người nghe được các tín hiệu ở các dải tần rộng và công suất lớn nên sẽ gây khó khăn đối với các phương pháp giấu tin trong audio. Nhưng thật may là thính giác con người lại kém trong việc phát hiện sự khác biệt các dải tần và công suất, có nghĩa là các âm thanh to, cao tần có thể che giấu được các âm thanh nhỏ ở tần số thấp một cách dễ dàng.



CÁC KỸ THUẬT GIẤU TIN

MÔI TRƯỜNG GIẤU TIN

Giấu thông tin trong audio (Data Hiding in Audio) (tiếp)

Các mô hình phân tích tâm lý đã chỉ ra điểm yếu trên và thông tin này sẽ giúp ích cho việc chọn các audio thích hợp cho việc giấu tin. Vấn đề khó khăn thứ hai đối với giấu thông tin trong audio là kênh truyền tin. Kênh truyền hay băng thông chậm sẽ ảnh hưởng đến chất lượng thông tin sau khi giấu.

Ví dụ để nhúng một đoạn phần mềm java applet vào một đoạn audio (16 bit, 44.100hz) có chiều dài bình thường thì các phương pháp thông thường cũng cần ít nhất tốc độ đường truyền là 20bps.

Giấu thông tin trong audio đòi hỏi yêu cầu rất cao về tính đồng bộ và tính an toàn của thông tin. Các phương pháp giấu thông tin cho audio đều lợi dụng điểm yếu trong hệ thống thính giác của con người.

CÁC KỸ THUẬT GIẤU TIN

MÔI TRƯỜNG GIẤU TIN

Giấu thông tin trong video (Data Hiding in Video)

Một phương pháp giấu tin trong video được đưa ra bởi COX là phương pháp phân bố đều. Ý tưởng cơ bản của phương pháp này là phân phối thông tin giấu dàn trải theo tần số của dữ liệu gốc. Nhiều nhà nghiên cứu đã dùng những hàm số cosin riêng và các hệ số truyền sóng riêng để giấu thông tin. Trong các thuật toán khởi nguồn thì thường chỉ có các kỹ thuật cho phép giấu các ảnh vào trong video, nhưng thời gian gần đây các kỹ thuật mới đã cho phép giấu cả âm thanh và hình ảnh vào trong video.