

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Khoa viễn thông 1

Bài giảng môn học

An ninh mạng viễn thông

Giảng viên: TS. Hoàng Trọng Minh

Email: hoangtrongminh@yahoo.com

2022

Tóm lược học phần

- **Tổng quan về an ninh mạng truyền thông**
- **Mật mã hóa đối xứng**
- **Mật mã hóa bất đối xứng**
- **Các giải thuật toàn vẹn dữ liệu**
- **Xác thực**
- **Các giao thức ứng dụng đảm bảo an ninh**

Chương 1: Tổng quan về an ninh mạng truyền thông

Đặt vấn đề

- Mạng truyền thông máy tính là sự kết hợp giữa công nghệ máy tính và công nghệ truyền thông để tạo thành môi trường giao tiếp, chủ yếu để đáp ứng nhu cầu của truyền thông dữ liệu. An toàn thông tin trên mạng máy tính bao gồm các phương pháp nhằm bảo vệ thông tin được lưu giữ và truyền trên mạng.
- Mạng máy tính có thể được coi là một nhánh của kỹ thuật điện, viễn thông, khoa học máy tính, công nghệ thông tin hoặc kỹ thuật máy tính vì nó dựa trên ứng dụng lý thuyết và thực tiễn của các ngành liên quan.

Chương 1: Tổng quan về an ninh mạng truyền thông

Đặt vấn đề

- Bảo mật là một quá trình liên tục bảo vệ một đối tượng khỏi bị truy cập trái phép. Đó là trạng thái hiện hữu hoặc cảm giác được bảo vệ khỏi bị tác động xấu hay tổn hại.
- Đối tượng ở trạng thái đó có thể là một người, một tổ chức như doanh nghiệp, hoặc truy nhập mạng như hệ thống máy tính hoặc một tệp.
- Bảo mật đến từ góc độ an toàn như của con người là trạng thái không bị làm phiền, lo lắng hoặc sợ hãi [1].

Chương 1: Tổng quan về an ninh mạng truyền thông

Đặt vấn đề

- Trạng thái an ninh này có thể được đảm bảo nếu có bốn cơ chế bảo vệ sau: cảnh báo, phòng ngừa, phát hiện và ứng phó.
 - Cảnh báo thường là tuyến phòng thủ đầu tiên chống lại những kẻ xâm nhập có thể cố gắng xâm nhập qua sự tin tưởng của hệ thống và cảnh báo hậu quả.
 - Ngăn chặn là quá trình cố gắng ngăn chặn những kẻ xâm nhập truy cập vào tài nguyên của hệ thống.
 - Phát hiện xảy ra khi kẻ xâm nhập đã thành công hoặc đang trong quá trình truy cập vào hệ thống.
 - Đáp ứng là một cơ chế tác động sau cố gắng đáp ứng sự thất bại của ba cơ chế đầu tiên. Nó hoạt động bằng cách cố gắng ngăn chặn và/hoặc ngăn chặn thiệt hại trong tương lai.

Chương 1: Tổng quan về an ninh mạng truyền thông

Cơ bản về mạng truyền thông máy tính

- Ý tưởng cơ bản trong tất cả các hình thức giao tiếp là phải có ba thành phần để giao tiếp có hiệu quả: Thực thể gửi và nhận thông tin, phương tiện truyền thông và bộ quy tắc hoặc giao thức truyền thông đã được thống nhất.
 - Hai mô hình mạng máy tính tiêu biểu là mô hình tập trung và phân tán.
 - Từ khía cạnh kích thước của nhóm các phần tử mạng và tài nguyên của chúng, mạng máy tính có thể chia thành hai loại mạng chính: mạng cục bộ LAN (Local Area Network) và mạng diện rộng WAN (Wide Area Network), mạng đô thị MAN.
 - Công nghệ truyền thông dữ liệu: mã hóa tín hiệu (tương tự/số), ghép/tách kênh (thời gian/tần số); phương tiện truyền dẫn
 - Cấu hình mạng: hình sao, bus, phân cấp, hình lưới.
 - Mô hình giao thức kết nối mạng: OSI; TCP/IP
 - Dịch vụ mạng: dịch vụ kết nối (hướng kết nối/ phi kết nối); chuyển mạch (kênh/gói)

Chương 1: Tổng quan về an ninh mạng truyền thông

Cơ bản về mạng truyền thông máy tính

- Ý tưởng cơ bản trong tất cả các hình thức giao tiếp là phải có ba thành phần để giao tiếp có hiệu quả: Thực thể gửi và nhận thông tin, phương tiện truyền thông và bộ quy tắc hoặc giao thức truyền thông đã được thống nhất.
 - Hai mô hình mạng máy tính tiêu biểu là mô hình tập trung và phân tán.
 - Từ khía cạnh kích thước của nhóm các phần tử mạng và tài nguyên của chúng, mạng máy tính có thể chia thành hai loại mạng chính: mạng cục bộ LAN (Local Area Network) và mạng diện rộng WAN (Wide Area Network), mạng đô thị MAN.
 - Công nghệ truyền thông dữ liệu: mã hóa tín hiệu (tương tự/số), ghép/tách kênh (thời gian/tần số); phương tiện truyền dẫn
 - Cấu hình mạng: hình sao, bus, phân cấp, hình lưới.
 - Mô hình giao thức kết nối mạng: OSI; TCP/IP
 - Dịch vụ mạng: dịch vụ kết nối (hướng kết nối/ phi kết nối); chuyển mạch (kênh/gói)

Chương 1: Tổng quan về an ninh mạng truyền thông

Bảo mật mạng truyền thông máy tính

- **Bảo mật máy tính.** Đây là một nhánh của khoa học máy tính nhằm tập trung vào việc tạo ra một môi trường an toàn cho việc sử dụng máy tính. Đối tượng chủ yếu là hành vi người dùng nên liên quan đến bốn lĩnh vực quan tâm: nghiên cứu đạo đức máy tính, phát triển giao thức phần mềm và phần cứng, và triển khai các thực nghiệm tốt nhất.
- Theo định nghĩa của NIST95, thì bảo mật máy tính là “Sự bảo vệ dành cho một hệ thống thông tin tự động để các đối tượng áp dụng đạt được tính toàn vẹn, tính sẵn sàng và tính bảo mật của các tài nguyên hệ thống thông tin (bao gồm phần cứng, phần mềm, phần sụn, thông tin/dữ liệu và viễn thông).

Chương 1: Tổng quan về an ninh mạng truyền thông

Bảo mật mạng truyền thông máy tính

- **Bảo mật mạng truyền thông máy tính.** Như phần trên giới thiệu, mạng máy tính là mạng phân tán kết nối các máy tính và thiết bị chia sẻ tài nguyên. Đối tượng bảo mật ở đây là một mạng lưới và thuộc nhánh nghiên cứu khoa học máy tính.
- Lĩnh vực này liên quan đến việc tạo ra một môi trường an toàn cho tất cả tài nguyên mạng và người sử dụng mạng. Vì vậy, nó liên quan tới các thiết kế toán học chi tiết về giao thức mật mã, cách thức giao tiếp, phương pháp vận chuyển và trao đổi thông tin.
- Một cách cụ thể, bảo mật mạng máy tính bao gồm bảo mật phần cứng và phi vật thể của mạng truyền thông máy tính.

Chương 1: Tổng quan về an ninh mạng truyền thông

Bảo mật mạng truyền thông máy tính

- **Bảo mật thông tin.** Đây là một lĩnh vực nghiên cứu rộng hơn cả bảo mật máy tính và bảo mật mạng máy tính.
- Bảo mật thông tin có mặt trong nhiều lĩnh vực khác nhau bao gồm khoa học máy tính, quản lý kinh doanh, nghiên cứu thông tin và các ngành kỹ thuật.
- Bảo mật thông tin liên quan đến việc tạo ra một trạng thái an toàn cho thông tin và dữ liệu trên cả cấp độ vật lý và trừu tượng.
- Do đó, bảo mật thông tin không chỉ liên quan tới các thiết kế toán học chi tiết hơn của các giao thức mật mã, giao tiếp, vận chuyển và trao đổi thông tin mà còn liên quan tới trạng thái của cả dữ liệu và thông tin.

Chương 1: Tổng quan về an ninh mạng truyền thông

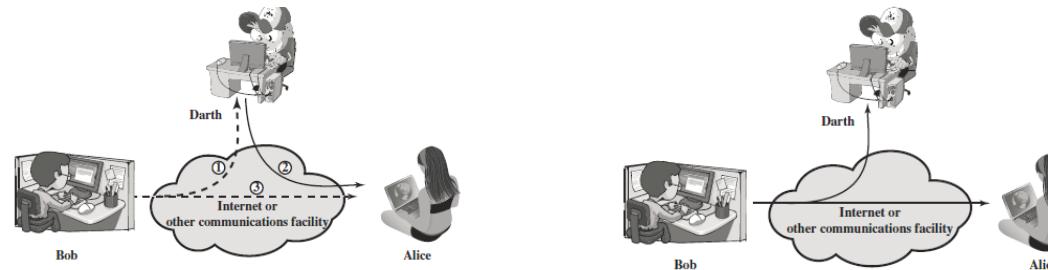
Xu hướng hội tụ mạng truyền thông máy tính

- Hiện nay, xu hướng tích hợp sâu máy tính, hệ thống truyền thông và hệ thống mạng máy tính đang tiếp tục phát triển. Cách thức hợp nhất theo hai con đường cơ bản:
- Từ hệ thống truyền thông truyền thống tích hợp công nghệ máy tính để mở rộng các dịch vụ sang hướng mạng máy tính;
- Từ các mạng máy tính tích hợp hệ thống truyền thông để hỗ trợ các dịch vụ tiên tiến hơn.
- Như vậy, các đối tượng mạng truyền thông máy tính và tài nguyên mạng mở rộng hơn sẽ là thách thức mới đối với lĩnh vực bảo mật mạng. .

Chương 1: Tổng quan về an ninh mạng truyền thông

Các kiểu tấn công an ninh mạng

- Từ góc độ cơ bản, tấn công an ninh bao gồm hai dạng: tấn công chủ động và tấn công bị động theo X.800 và RFC4949.
- Tấn công chủ động là cách thức tấn công làm thay đổi tài nguyên hệ thống hoặc ảnh hưởng đến hoạt động của mạng.
- Tấn công bị động là kiểu cố gắng tìm hiểu hoặc sử dụng thông tin từ hệ thống nhưng không ảnh hưởng đến tài nguyên hệ thống.



Chương 1: Tổng quan về an ninh mạng truyền thông

Các kiểu tấn công an ninh mạng

- **Các kiểu tấn công chủ động:**

- Masquerade. Cuộc tấn công giả trang/ mạo danh diễn ra khi một thực thể giả làm một thực thể khác.
- Sửa đổi bản tin. Loại tấn công này sửa đổi một phần hoặc toàn bộ bản tin, thay đổi hoặc trì hoãn bản tin để tạo ra hệ quả trái phép.
- Thoái thác. Loại tấn công này có thể được thực hiện từ phía gửi hoặc phía nhận thông qua việc thoái thác đã thực hiện một hoạt động nào đó.
- Phát lại. Loại tấn công này liên quan tới việc bắt giữ bản tin và truyền lại liên tiếp để tạo hệ quả xấu.

- **Các kiểu tấn công bị động:**

- Rò rỉ thông tin. Loại tấn công này thu thập các thông tin hữu ích từ bản tin để phục vụ các mục đích xấu.
- Giám sát lưu lượng. Đặc trưng của lưu lượng có thể phản ánh nội dung dịch vụ. Vì vậy loại tấn công này có thể có được các thông tin cần bảo vệ thông qua phân tích lưu lượng truyền trên mạng.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các kiểu tấn công an ninh mạng

	Tấn công chủ động	Tấn công bị động
1.	Tấn công chủ động dẫn tới việc sửa đổi thông tin.	Tấn công bị động không dẫn tới việc sửa đổi thông tin.
2.	Tấn công chủ động gây ra nguy hiểm cho tính toàn vẹn cũng như tính khả dụng.	Tấn công bị động gây nguy hiểm cho tính Bảo mật .
3.	Phát hiện là giải pháp tốt nhất cho tấn công chủ động.	Phòng ngừa là giải pháp tốt nhất cho tấn công thụ động.
4.	Tấn công chủ động luôn gây tác động trực tiếp đối với hệ thống.	Tấn công bị động không gây tác động trực tiếp đối với hệ thống.
5.	Trong cuộc tấn công chủ động nạn nhân nhận thức được tác động tấn công.	Trong cuộc tấn công bị động, nạn nhân không nhận thức được tác động tấn công.
6.	Tài nguyên hệ thống bị tác động thay đổi dưới tấn công chủ động.	Tài nguyên hệ thống không bị tác động thay đổi dưới tấn công chủ động.
7.	Tấn công chủ động ảnh hưởng đến các dịch vụ của hệ thống.	Tấn công thụ động chỉ thu thập thông tin và bản tin hệ thống.
8.	Tấn công chủ động dễ phát hiện nhưng khó ngăn chặn.	Tấn công bị động dễ ngăn chặn nhưng khó phát hiện.

Bảng so sánh hai dạng tấn công

Chương 1: Tổng quan về an ninh mạng truyền thông

Các cơ chế bảo vệ mạng

a) Điều khiển truy nhập

Hệ thống kiểm soát truy cập phần cứng

- Thiết bị đầu cuối truy cập
- Giám sát sự kiện trực quan
- Thẻ nhận dạng
- Nhận dạng sinh trắc học
- Giám sát bằng video

Hệ thống kiểm soát truy cập mềm

- Giám sát điểm truy cập
- Giám sát từ xa.



Chương 1: Tổng quan về an ninh mạng truyền thông

Các cơ chế bảo vệ mạng

b) Xác thực

- Xác thực là một dịch vụ được sử dụng để xác định danh tính thực thể hoặc người dùng hợp pháp.
- Cơ chế này cung cấp một hệ thống có khả năng xác minh rằng người dùng hợp pháp như đã biết hoặc đại diện người dùng hợp pháp qua các phương pháp kiểm tra.
- Một số phương pháp thông dụng là kiểm tra chữ ký, nhận dạng sinh trắc học, vị trí địa lý hoặc các tham số khác.

c) Bảo mật

- Dịch vụ bảo mật bảo vệ dữ liệu hệ thống và thông tin khỏi bị tiết lộ trái phép.
- Khi dữ liệu rời khỏi thiết bị vào môi trường mạng là môi trường không ủy thác. Do đó, phía nhận không thể hoàn toàn tin tưởng sự an toàn dữ liệu do có thực thể trung gian hoặc bên thứ 3.
- Bảo mật sử dụng các thuật toán mã hóa để đảm bảo thông tin không bị lộ.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các cơ chế bảo vệ mạng

b) Xác thực

- Xác thực là một dịch vụ được sử dụng để xác định danh tính thực thể hoặc người dùng hợp pháp.
- Cơ chế này cung cấp một hệ thống có khả năng xác minh rằng người dùng hợp pháp như đã biết hoặc đại diện người dùng hợp pháp qua các phương pháp kiểm tra.
- Một số phương pháp thông dụng là kiểm tra chữ ký, nhận dạng sinh trắc học, vị trí địa lý hoặc các tham số khác.

c) Bảo mật

- Dịch vụ bảo mật bảo vệ dữ liệu hệ thống và thông tin khỏi bị tiết lộ trái phép.
- Khi dữ liệu rời khỏi thiết bị vào môi trường mạng là môi trường không ủy thác. Do đó, phía nhận không thể hoàn toàn tin tưởng sự an toàn dữ liệu do có thực thể trung gian hoặc bên thứ 3.
- Bảo mật sử dụng các thuật toán mã hóa để đảm bảo thông tin không bị lộ.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các cơ chế bảo vệ mạng

d) Toàn vẹn dữ liệu

- Dịch vụ toàn vẹn bảo vệ dữ liệu khỏi các tấn công làm thay đổi dữ liệu.
- Cũng giống như tính bảo mật của dữ liệu, dữ liệu trong quá trình chuyển đổi giữa bên gửi và bên nhận có thể bị thêm, bớt hay thay đổi theo ý đồ của kẻ tấn công.
- Dịch vụ này thông qua các thuật toán mã hóa và băm để đảm bảo rằng tính toàn vẹn của dữ liệu.

e) Chống từ chối/ thoái thác

- Đây là một dịch vụ bảo mật cung cấp bằng chứng về nguồn gốc của các bên cung cấp/sử dụng dịch vụ và/hoặc thông tin liên quan tới giao tiếp.
- Trong cuộc sống thực, có thể người gửi có thể từ chối quyền sở hữu dữ liệu kỹ thuật số được trao đổi có nguồn gốc từ họ.
- Dịch vụ này, thông qua các thuật toán mã hóa và chữ ký số, đảm bảo rằng dữ liệu kỹ thuật số chống từ chối bằng cách cung cấp bằng chứng xuất xứ khó có thể chối cãi.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các nguy cơ và lỗ hổng bảo mật mạng máy tính

Các nguy cơ ảnh hưởng

- **Các điểm yếu trong cơ sở hạ tầng mạng và các giao thức truyền thông.** Triết lý xây dựng hạ tầng mạng truyền thông và mạng máy tính;
- **Sự phát triển mạnh mẽ của không gian mạng** tiến gần tới các lĩnh vực thương mại, quản lý, chính trị hay hạ tầng quốc gia. Sự gắn kết và phụ thuộc của con người với các hệ thống kết nối mạng);
- **Sự phát triển mạnh của các cộng đồng hacker.** Sự thay đổi vai trò của các cộng đồng hacker với đa dạng tiêu chí mục tiêu;
- **Lỗ hổng từ các hệ điều hành máy tính** trong môi trường mạng truyền thông (các hệ điều hành khác nhau có các lỗ hổng khác nhau cùng tham gia vào môi trường chung);
- **Các kỹ thuật xã hội (social engineering) phát triển.** Sử dụng kỹ thuật thao tác tâm lý của người dùng để thực hiện các hành động hoặc tiết lộ thông tin bí mật;
- **Sự thay đổi/chuyển đổi mục tiêu bảo mật.** Ứng dụng thực tế, phương pháp đánh cắp hoặc quy mô.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các nguy cơ và lỗ hổng bảo mật mạng máy tính

Các dạng lỗ hổng bảo mật

- **Sai lỗi thiết kế.** Hai thành phần chính của hệ thống máy tính là phần cứng và phần mềm, thường có sai sót trong thiết kế. Một số yếu tố gây ra lỗi thiết kế phần mềm từ góc độ bảo mật gồm: yếu tố con người, độ phức tạp của phần mềm và nguồn phần mềm đáng tin cậy.
- **Quản lý bảo mật yếu.** Quản lý bảo mật là cả một quy trình bảo mật kỹ thuật và quản trị liên quan đến các chính sách và kiểm soát bảo mật mà tổ chức quyết định đưa ra để cung cấp mức độ bảo vệ cần thiết. Liên quan đến việc giám sát an ninh và đánh giá hiệu quả của các chính sách đó. Đánh giá rủi ro bảo mật thông qua chính sách bảo mật và truy cập an toàn vào tài nguyên mạng là rất phức tạp vì liên quan tới nhiều bên và sự phối hợp không đồng nhất sẽ gây ra lỗ hổng.
- **Sự tương thích trong triển khai.** Vấn đề tương thích và tiêu chuẩn hóa là một trở ngại lớn với các hệ thống truyền thông mạng máy tính khi số lượng và chủng loại không thể đồng nhất và tiêu chuẩn hóa.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các nguy cơ và lỗ hổng bảo mật mạng máy tính

Các dạng lỗ hổng bảo mật

- **Kết nối liên mạng.** Sự phát triển và ứng dụng mạnh mẽ của hai lĩnh vực công nghệ vô tuyến và máy tính đã tạo ra đa dạng mạng ứng dụng tiềm cận gần nhất tới con người. Bên cạnh điểm yếu, lỗ hổng, khe hở của công nghệ và kỹ thuật là nhận thức và hành vi, đạo đức sử dụng đã dẫn tới các lỗ hổng mới trong kết nối liên mạng.
- **Sự thay đổi tự nhiên của công nghệ tấn công.** Các công nghệ xấu dùng để xâm nhập hệ thống tăng lên tự nhiên theo sự mở rộng công nghệ. Các tài nguyên cho công nghệ xấu phổ biến hơn nhờ sử dụng công cụ tìm kiếm, thời gian, kiến thức thu thập trên môi trường mạng. Xuất hiện các kiểu tấn công mới, mạnh mẽ, ẩn tượng, tàn phá lớn, lây lan nhanh chóng và thời gian quay vòng rất nhanh gây khó khăn đối với hệ thống phòng chống. Các công nghệ tấn công sử dụng chính các công nghệ tiên tiến như trí tuệ nhân tạo AI để thực hiện tạo sức ép và khai thác các lỗ hổng.

○

Chương 1: Tổng quan về an ninh mạng truyền thông

Các thách thức thực tiễn

- **Bảo mật máy tính và mạng máy tính là một lĩnh vực vừa hấp dẫn vừa phức tạp**
 - Bảo mật không đơn giản chỉ vì mục đích dễ hiểu là đảm bảo yêu cầu tính bảo mật, xác thực, không từ chối và tính toàn vẹn của đối tượng cần bảo mật. Các cơ chế được sử dụng để đáp ứng những yêu cầu trên luôn có độ phức tạp lớn và việc hiểu rõ thường liên quan tới các lý luận khá tinh vi.
 - Khi phát triển một cơ chế hoặc thuật toán bảo mật cụ thể, ta luôn phải đánh giá các cuộc tấn công tiềm ẩn bên cạnh các nguy cơ hay lỗ hổng vào các tính năng bảo mật đó. Trong nhiều trường hợp, các cuộc tấn công thành công được thiết kế bằng cách nhìn vấn đề theo một cách hoàn toàn khác khi khai thác một điểm yếu không mong muốn trong cơ chế hoạt động của hệ thống.
 - Do lý do phía trên, các thủ tục hoặc logic sử dụng cụ thể thường phản trực giác. Thông thường, một cơ chế bảo mật rất phức tạp và khó thể hiện qua bằng chứng cụ thể, chỉ khi các khía cạnh khác nhau của mối đe dọa được xem xét thì các cơ chế bảo mật phức tạp mới có ý nghĩa.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các thách thức thực tiễn

- **Bảo mật máy tính và mạng máy tính là một lĩnh vực vừa hấp dẫn vừa phức tạp**
 - Sử dụng các cơ chế bảo mật đúng chỗ cũng là một thách thức do phải phù hợp cả về mặt vật lý và mặt logic.
 - Các cơ chế bảo mật thường liên quan đến nhiều hơn một thuật toán hoặc giao thức cụ thể. Bên cạnh các thuật toán tạo khóa, cách thức phân phối và bảo vệ khóa bí mật cũng yêu cầu thêm các nhiệm vụ phát triển cơ chế bảo mật. Các đặc trưng vật lý và tài nguyên mạng sẽ tác động tới các yêu cầu thiết kế cơ chế bảo mật.
 - An ninh mạng truyền thông máy tính thực chất là cuộc chiến đấu trí giữa một kẻ thù cố gắng tìm ra các lỗ hổng và nhà thiết kế hoặc quản trị mạng cố gắng đóng chúng lại. Lợi thế lớn mà kẻ tấn công có được là chỉ cần tìm ra một điểm yếu duy nhất, trong khi người bảo vệ phải tìm và loại bỏ tất cả các điểm yếu để đạt được sự bảo mật hoàn hảo.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các thách thức thực tiễn

- **Bảo mật máy tính và mạng máy tính là một lĩnh vực vừa hấp dẫn vừa phức tạp**
 - Người dùng và người quản lý hệ thống có xu hướng nhận thấy ít lợi ích từ việc đầu tư bảo mật cho đến khi xảy ra lỗi bảo mật.
 - Bảo mật đòi hỏi sự giám sát thường xuyên, thậm chí liên tục và điều này là khó khăn trong môi trường quá tải, ngắn hạn ngày nay.
 - Bảo mật vẫn thường được đưa vào một hệ thống sau khi thiết kế hoàn thành hơn là một phần không thể thiếu của quá trình thiết kế.
 - Nhiều người dùng (và thậm chí cả quản trị viên bảo mật) coi bảo mật mạnh mẽ như một trở ngại đối với hoạt động hiệu quả và thân thiện với người dùng của hệ thống thông tin hoặc việc sử dụng thông tin.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các tổ chức tiêu chuẩn và chuẩn bảo mật

- Các tổ chức tiêu chuẩn

- **Các tổ chức quốc tế.** Lực lượng đặc nhiệm kỹ thuật Internet (IETF), Viện kỹ sư điện và điện tử (IEEE), Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) và Liên minh Viễn thông Quốc tế (ITU).
- **Các tổ chức đa quốc gia.** Ủy ban tiêu chuẩn hóa Châu âu (CEN), Ủy ban liên minh Châu âu (CEU) và Viện tiêu chuẩn điện tử Châu âu (ETSI).
- **Các tổ chức chính phủ quốc gia.** Viện tiêu chuẩn và công nghệ quốc gia (NIST), Viện tiêu chuẩn quốc gia Mỹ (ANSI) và Hội đồng tiêu chuẩn Canada (CSC)
- **Các tổ chức theo lĩnh vực cụ thể.** Ủy ban Châu âu về tiêu chuẩn ngân hàng (ECBS), Hiệp hội các nhà sản xuất máy tính Châu âu (ECMA) và Viện kỹ sư điện và điện tử (IEEE)
- **Các tiêu chuẩn ngành.** RSA, Nhóm mở (OSF +X/Open), Nhóm quản lý đối tượng (OMG), Tổ chức World Wide Web Consortium (W3C) và Tổ chức phát triển tiêu chuẩn thông tin có cấu trúc (OASIS)

Chương 1: Tổng quan về an ninh mạng truyền thông

Các tổ chức tiêu chuẩn và chuẩn bảo mật

- Tiêu chuẩn X.800 của ITU
 - ITU-T đưa ra khuyến nghị X.800 định nghĩa kiến trúc an ninh cho mô hình OSI.
 - Tấn công an ninh: bất kỳ hành động nào mà làm hại đến tính an toàn thông tin của một tổ chức nào đó.
 - Cơ chế an ninh: quá trình được thiết kế để phát hiện, ngăn ngừa, hay khôi phục lại các kiểu tấn công an toàn.
 - Dịch vụ an ninh: dịch vụ truyền thông làm tăng cường tính an toàn của hệ thống xử lý dữ liệu và thông tin của một tổ chức. Các dịch vụ này thường dùng để chống lại các tấn công an toàn, và các dịch vụ này tận dụng một hoặc nhiều cơ chế an toàn để cung cấp dịch vụ.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các tổ chức tiêu chuẩn và chuẩn bảo mật

- Tiêu chuẩn X.800 của ITU
 - ITU-T đưa ra khuyến nghị X.800 định nghĩa kiến trúc an ninh cho mô hình OSI.
 - Tấn công an ninh: bất kỳ hành động nào mà làm hại đến tính an toàn thông tin của một tổ chức nào đó.
 - Cơ chế an ninh: quá trình được thiết kế để phát hiện, ngăn ngừa, hay khôi phục lại các kiểu tấn công an toàn.
 - Dịch vụ an ninh: dịch vụ truyền thông làm tăng cường tính an toàn của hệ thống xử lý dữ liệu và thông tin của một tổ chức. Các dịch vụ này thường dùng để chống lại các tấn công an toàn, và các dịch vụ này tận dụng một hoặc nhiều cơ chế an toàn để cung cấp dịch vụ.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các tổ chức tiêu chuẩn và chuẩn bảo mật

- Tiêu chuẩn X.800 của ITU
 - Mỗi quan hệ giữa dịch vụ an ninh và cơ chế đảm bảo an ninh

SERVICE	MECHANISM							
	Enchipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y				Y	Y		
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

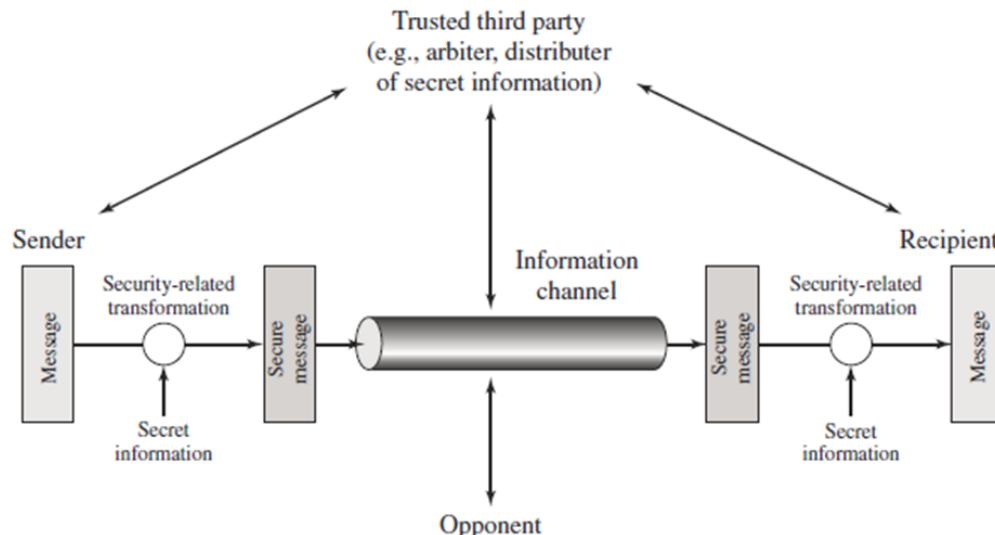
X.800 định nghĩa dịch vụ an ninh là một dịch vụ được cung cấp bởi lớp giao thức của các hệ thống truyền thông và đảm bảo tính an toàn của các hệ thống hoặc của việc truyền dữ liệu.
RFC 4949 định nghĩa dịch vụ an ninh thực hiện các chính sách an toàn và được thực thi bởi các cơ chế an toàn.

Chương 1: Tổng quan về an ninh mạng truyền thông

Các tổ chức tiêu chuẩn và chuẩn bảo mật

- Mô hình truyền thông an toàn

-



Mô hình an toàn với các thành phần tham gia truyền thông

Chương 1: Tổng quan về an ninh mạng truyền thông

Kết luận chương

- Các vấn đề cần ôn tập
 1. Các cơ chế bảo vệ mạng truyền thông máy tính.
 2. Phân loại kiểu tấn công và các hậu quả tác động tới mạng.
 3. Hình thức và giải pháp bảo mật mạng truyền thông máy tính.
 4. Các nguy cơ tiềm ẩn ảnh hưởng tới an toàn mạng truyền thông máy tính.
 5. Các lỗ hổng bảo mật trong mạng truyền thông máy tính.
 6. Tìm hiểu thêm về các mục tiêu xây dựng chuẩn hóa an ninh mạng của các tổ chức.
 7. Tiêu chuẩn X.800 của ITU về an ninh mạng truyền thông.
 8. Mô hình an ninh mạng truyền thông máy tính.

Chương 2: Mật mã hóa khóa đối xứng

Giới thiệu về mật mã

- Một số khái niệm
 - Mật mã (cryptography) là một ngành khoa học giữ bí mật. Mục đích của mật mã hóa để cung cấp các phương pháp ngăn chặn vi phạm tới thông tin cần giữ bí mật (cung cấp tính bảo mật confidentiality).
 - Mật mã được sử dụng để cung cấp giải pháp cho các vấn đề như: đảm bảo tính toàn vẹn dữ liệu, nhận thực, và chống chối bỏ.
 - Phân tích mật mã là khoa học nghiên cứu các cuộc tấn công chống lại các lược đồ mã hóa. Mật mã và phân tích mật mã thường được gộp chung bằng thuật ngữ khoa học mật mã (cryptology).

Chương 2: Mật mã hóa khóa đối xứng

Giới thiệu về mật mã

- **Một số khái niệm**
 - Mật mã (cryptography) là một ngành khoa học giữ bí mật. Mục đích của mật mã hóa để cung cấp các phương pháp ngăn chặn vi phạm tới thông tin cần giữ bí mật (cung cấp tính bảo mật confidentiality).
 - Mật mã được sử dụng để cung cấp giải pháp cho các vấn đề như: đảm bảo tính toàn vẹn dữ liệu, nhận thực, và chống chối bỏ.
 - Phân tích mật mã là khoa học nghiên cứu các cuộc tấn công chống lại các lược đồ mã hóa. Mật mã và phân tích mật mã thường được gộp chung bằng thuật ngữ khoa học mật mã (cryptology).
 - Cho đến cuối thế kỷ 20, mật mã thực sự là một nghệ thuật và vì vậy được coi là mật mã cổ điển/truyền thống. Lĩnh vực này được coi là nghệ thuật vì việc xây dựng các mã tốt hoặc phá vỡ các mã hiện có dựa trên sự sáng tạo và ý thức phát triển về cách mã hoạt động.

Chương 2: Mật mã hóa khóa đối xứng

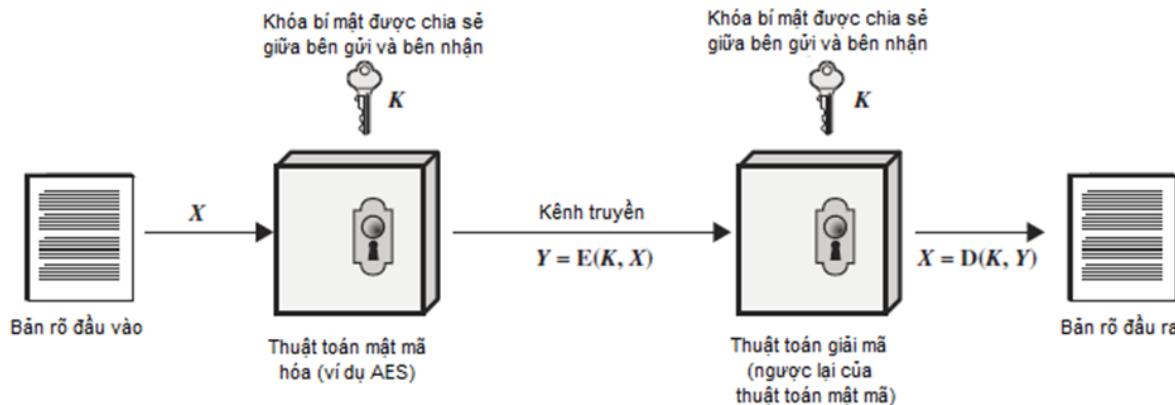
Giới thiệu về mật mã

- **Một số khái niệm**
 - Vào những năm 1970-1980, nhận thức về mật mã đã thay đổi hoàn toàn khi lĩnh vực sản sinh ra các lý thuyết phong phú và chặt chẽ như một ngành khoa học liên quan chặt chẽ tới toán học. Mật mã hiện đại ra đời liên quan đến việc nghiên cứu các kỹ thuật toán học để bảo mật cho thông tin kỹ thuật số, các hệ thống và các tính toán phân tán để chống lại các cuộc tấn công của đối thủ.
 - Một vấn đề khác biệt giữa hai loại mật mã chính là phạm vi người dùng, mật mã cổ điển chủ yếu sử dụng cho quân sự và chính phủ và mật mã hiện đại được dùng bởi tất cả mọi người.
 - Một giả định cơ bản trong phân tích mật mã được dựa trên nguyên lý Kerckhoffs. *(1) duy trì bí mật của một khóa dễ hơn giữ bí mật lược đồ mã hóa; (2) dễ thay đổi khóa hơn lược đồ nếu bị lộ; (3) lược đồ mã hóa cần được kiểm chứng rộng rãi và công khai để phát hiện điểm yếu.*

Chương 2: Mật mã hóa khóa đối xứng

Mô hình và thành phần lược đồ mã hóa

- Mô hình mật mã khóa đối xứng điển hình



Mô hình mật mã khóa đối xứng đơn giản

Chương 2: Mật mã hóa khóa đối xứng

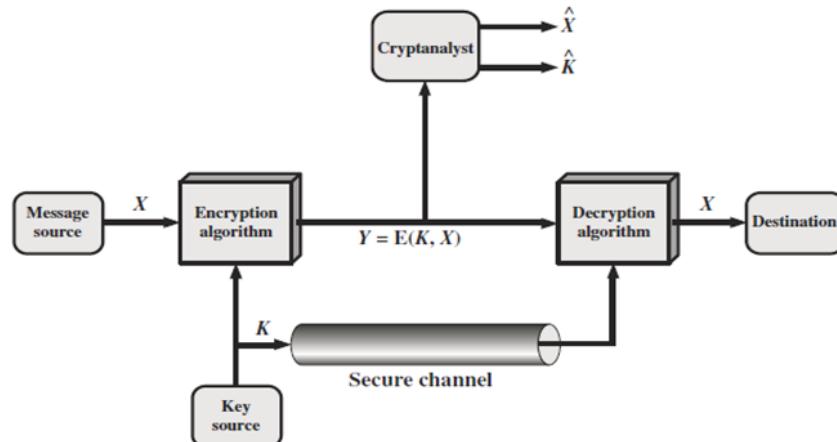
Mô hình và thành phần lược đồ mã hóa

- **Các thành phần**
 - **Bản rõ:** đây là dữ liệu hoặc bản tin ban đầu, được xem như là đầu vào của khối thuật toán mật mã.
 - **Thuật toán mật mã hóa:** thuật toán mật mã hóa thực hiện rất nhiều phép biến đổi và thay thế trên bản rõ.
 - **Khóa bí mật:** khóa bí mật cũng là một đầu vào của khối thuật toán mật mã hóa. Khóa là một giá trị độc lập với bản rõ và thuật toán. Thuật toán sẽ cho ra một đầu ra khác nhau phụ thuộc vào khóa cụ thể được sử dụng tại thời điểm đó. Các phép biến đổi và thay thế chính xác được thực hiện bởi thuật toán phụ thuộc vào khóa đó.
 - **Bản mã:** đây là bản tin đầu ra khối thuật toán mật mã. Bản mã này phụ thuộc vào bản rõ và khóa bí mật. Với một bản tin xác định, hai khóa khác nhau sẽ tạo ra hai bản mã khác nhau.
 - **Thuật toán giải mật mã:** là thuật toán thực hiện ngược lại với thuật toán mật mã hóa. Khối này nhận bản mã và khóa bí mật để tạo ra bản rõ ban đầu

Chương 2: Mật mã hóa khóa đối xứng

Mô hình và thành phần lược đồ mã hóa

- Phân tích mã và tấn công
 - Yêu cầu cho việc sử dụng an toàn mật mã hóa truyền thống: Thuật toán đủ mạnh và khóa được giữ bí mật tại hai bên tham gia giao tiếp truyền thông.



Mô hình truyền thông an toàn cho khóa đối xứng

Chương 2: Mật mã hóa khóa đối xứng

Mô hình và thành phần lược đồ mã hóa

• Phân tích mã và tấn công

- Một đặc tính quan trọng của mã hóa đối xứng là khóa phải được giữ bí mật giữa người gửi và người nhận, hay nói cách khác khóa phải được chuyển một cách an toàn từ người gửi đến người nhận. (kênh an toàn, dùng nhiều lần);
- Đặc tính quan trọng thứ hai của một hệ mã hóa đối xứng là tính an toàn của hệ mã. Một bản mã có thể dễ dàng suy ra được bản rõ ban đầu mà không cần biết khóa bí mật.
- Do đó một hệ mã hóa đối xứng được gọi là an toàn khi và chỉ khi nó không thể bị phá mã - không cần khóa (điều kiện lý tưởng) hoặc thời gian phá mã là bất khả thi. Tấn công vét cạn/ toàn diện/ Brute-force.

Kích thước khóa (bit)	Số lượng khóa	Thời gian thực hiện (tốc độ thử: 10^3 khóa/giây)	Thời gian thực hiện (tốc độ thử: 10^9 khóa/giây)
32	$2^{32} \approx 4.3 \times 10^9$	35.8 phút	2.15 mili giây
56	$2^{56} \approx 7.2 \times 10^{16}$	1142 năm	10.01 giờ
128	$2^{128} \approx 3.4 \times 10^{38}$	5.4×10^{24} năm	5.4×10^{18} năm
168	$2^{168} \approx 3.7 \times 10^{50}$	5.9×10^{36} năm	5.9×10^{30} năm
hoán vị 26 ký tự	$26! \approx 4 \times 10^{26}$	6.4×10^{12} năm	6.4×10^6 năm

Chương 2: Mật mã hóa khóa đối xứng

Một số mật mã cổ điển

- **Mật mã Ceasar**
 - Thế kỷ thứ 3 trước công nguyên, nhà quân sự người La Mã Julius Ceasar đã nghĩ ra phương pháp mã hóa một bản tin như sau: thay thế mỗi chữ trong bản tin bằng chữ đứng sau nó k vị trí trong bảng chữ cái. (ví dụ $k=3$)

Chữ ban đầu: 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

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

(sau Z sẽ vòng lại là A, do đó $x \rightarrow A$, $y \rightarrow B$ và $z \rightarrow C$)

Giả sử có bản tin gốc (*bản rõ*): meet me after the toga party

Như vậy bản tin mã hóa (*bản mã*) sẽ là: PHHW PH DIWHU WKH WRJD SDUWB

$C = (p + k) \text{ mod } 26$	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
$p = (C - k) \text{ mod } 26$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$E(k, m_1, m_2, \dots, m_l) = c_1, c_2, \dots, c_j; \quad c_i = (m_i + k) \bmod 26$$

$$D(k, c_1, c_2, \dots, c_l) = m_1, m_2, \dots, m_l; \quad m_i = (c_i - k) \bmod 26$$

Chương 2: Mật mã hóa khóa đối xứng

Một số mật mã cổ điển

- **Mật mã thay thế đơn chữ cái**
 - Phương pháp đơn bảng tổng quát hóa phương pháp Ceasar bằng cách dòng mã hóa không phải là một dịch chuyển k vị trí của các chữ cái A, B, C, ... nữa mà là một hoán vị của 26 chữ cái này (mỗi hoán vị được xem như là một khóa).
 - Tấn công phá mã vét cạn khóa là bất khả thi;
 - Al-Kindi đã phát hiện ra một phương pháp phá mã khả thi dựa trên tần suất xuất hiện của chữ cái. Phương pháp mã hóa đơn bảng ánh xạ một chữ cái trong bản rõ thành một chữ cái khác trong bản mã. Do đó các chữ cái trong bản mã cũng sẽ tuân theo luật phân bố tần suất trên.
 - Theo thống kê, chữ e và chữ t trong tiếng Anh xuất hiện nhiều nhất (12,7% và 9.1%).

Chương 2: Mật mã hóa khóa đối xứng

Một số mật mã cổ điển

- **Mật mã Playfair**
 - Mật mã Playfair xem hai ký tự đứng sát nhau là một đơn vị mã hóa, hai ký tự này được thay thế cùng lúc bằng hai ký tự khác.
 - Playfair dùng một ma trận 5x5 các ký tự như sau.
 - Từ khóa được xếp vào hàng đầu;
 - Ký tự cùng hàng thì thay tiếp theo hàng và vòng lại; ar RM
 - Ký tự cùng cột thì thay tiếp theo cột và vòng lại; ov HO
 - Còn lại, ký tự được thay bằng vị trí trên đường chéo của hình chữ nhật. hs – BP, ea JM

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

(Bài tập với mã Playfair với biến từ khóa và bản rõ khác nhau)

Chương 2: Mật mã hóa khóa đối xứng

Một số mật mã cổ điển

- **Mật mã đa chữ cái Vigenère**
 - Mỗi chữ cái được gán cho một con số nguyên từ 0 đến 25
 - Thực hiện mã hóa một lần m ký tự bản rõ (p_1, p_2, \dots, p_m) thành m bản mã (c_1, c_2, \dots, c_m).

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Với $m=3$, ta có hệ phương trình tuyến tính

$$c_1 = k_{11}p_1 + k_{12}p_2 + k_{13}p_3 \ mod \ 26$$

$$c_2 = k_{21}p_1 + k_{22}p_2 + k_{23}p_3 \ mod \ 26$$

$$c_3 = k_{31}p_1 + k_{32}p_2 + k_{33}p_3 \ mod \ 26$$

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \ mod \ 26$$

- Mã hóa: $C=KP \ mod \ 26$, P và C là vector đại diện cho bản rõ và bản mã, K là ma trận khóa.
- Giải mã: $K^{-1}C \ mod \ 26 = K^{-1}KP \ mod \ 26 = P$. Điều kiện, tồn tại ma trận nghịch đảo của K .

Chương 2: Mật mã hóa khóa đối xứng

Một số mật mã cổ điển

- Mật mã đa chữ cái Vigenère

- Mỗi chữ cái được gán cho một con số nguyên từ 0 đến 25
- Thực hiện mã hóa một lần m ký tự bản rõ (p_1, p_2, \dots, p_m) thành m bản mã (c_1, c_2, \dots, c_m).

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Với $m=3$, ta có hệ phương trình tuyến tính

$$c_1 = k_{11}p_1 + k_{12}p_2 + k_{13}p_3 \ mod \ 26$$

$$c_2 = k_{21}p_1 + k_{22}p_2 + k_{23}p_3 \ mod \ 26$$

$$c_3 = k_{31}p_1 + k_{32}p_2 + k_{33}p_3 \ mod \ 26$$

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \ mod \ 26$$

- Mã hóa: $C=KP \ mod \ 26$, P và C là vector đại diện cho bản rõ và bản mã, K là ma trận khóa.
- Giải mã: $K^{-1}C \ mod \ 26 = K^{-1}KP \ mod \ 26 = P$. Điều kiện, tồn tại ma trận nghịch đảo của K .

Plaintext: tellhimaboutme
Key (repeated): cafecafecafeca
Ciphertext: VEQPJIREDZXOE

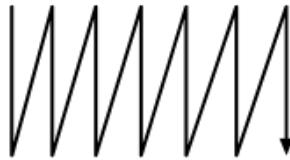
Chương 2: Mật mã hóa khóa đối xứng

Một số mật mã cổ điển

- **Mật mã hoán vị Hill**

- Xáo trộn thứ tự của các chữ cái trong bản rõ;
- Một cách thực hiện đơn giản là ghi bản rõ theo từng hàng, sau đó kết xuất bản mã dựa trên các cột;

a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	u	i	l
h	i	s	n	o	o	n



Bài học cơ bản là thiết kế mật mã an toàn rất khó và không phải lược đồ phức tạp nào cũng có độ an toàn cần thiết.

attackpostponeduntilthisnoon

AODHTSUITTNSAPTNCOIOKNLOPETN

- Một cơ chế phức tạp hơn là chúng ta có thể hoán vị các cột trước khi kết xuất bản mã. Ví dụ chọn một khóa là MONARCH, ta có thể hoán vị các cột;

M	O	N	A	R	C	H		A	C	H	M	N	O	R
a	t	t	a	c	k	p		a	k	p	a	t	t	c
o	s	t	p	o	n	e	→	p	n	e	o	t	s	o
d	u	n	t	u	i	l		t	l	t	d	n	u	i
h	i	s	n	o	o	n		n	o	n	h	s	i	o

APTNKNLOPETNAODHTTNSTSUICOIO

Chương 2: Mật mã hóa khóa đối xứng

Mật mã đối xứng hiện đại

- Các nguyên lý cơ bản

- Nguyên lý 1- Các định nghĩa chính thức
- Các định nghĩa chi tiết về thiết kế, nghiên cứu, đánh giá và sử dụng các nguyên bản mật mã cũng như cho phép so sánh có ý nghĩa các lược đồ.
- Các giả định về tấn công có thể đưa ra chi tiết hơn.
 1. *Tấn công chỉ bằng bản mã (Ciphertext-only attack).*
 2. *Tấn công bản rõ đã biết (Known-plaintext attack).*
 3. *Tấn công bản rõ lựa chọn (Chosen-plaintext attack).*
 4. *Tấn công bản rõ được chọn theo cách thích ứng (Adaptively-chosen-plaintext attack)*
 5. *Các cuộc tấn công bản mã được lựa chọn và thích ứng (Chosen- and adaptively-chosen-ciphertext attacks).*

Mật mã cổ điển hướng về nghệ thuật hơn là một khoa học. Mật mã hiện đại được phát triển và phân tích một cách hệ thống và được chứng minh an toàn dựa trên bằng chứng cụ thể.

Chương 2: Mật mã hóa khóa đối xứng

Mật mã đối xứng hiện đại

- Các nguyên lý cơ bản
 - Nguyên lý 2- Các giả thiết chính xác
 - Hầu hết các cấu trúc mật mã hiện đại không thể được chứng minh là an toàn vô điều kiện. Những chứng minh như vậy hiện chưa có câu trả lời do lý thuyết về độ phức tạp tính toán chưa giải quyết được.
 - Bằng chứng bảo mật thường dựa trên các giả định và đặt ra yêu cầu phải được thực hiện rõ ràng và chính xác về mặt toán học.
 - Các vấn đề quan trọng của giả thiết
 1. Xác thực các giả định
 2. So sánh các giả định
 3. Hiểu rõ các giả định căn bản

Chương 2: Mật mã hóa khóa đối xứng

Mật mã đối xứng hiện đại

- Các nguyên lý cơ bản
 - Nguyên lý 3- Bằng chứng bảo mật
 - Hai nguyên tắc đầu cho phép đạt được mục tiêu là cung cấp bằng chứng chặt chẽ cho một lược đồ mật mã thỏa mãn một định nghĩa nhất định theo các giả định nhất định. Giả định này hợp lý trong bối cảnh kẻ tấn công đang nỗ lực tấn công mà thành công.
 - Tuy nhiên, cũng không có bằng chứng cho thấy kẻ tấn công có tài nguyên chỉ định giống trực giác của ta. Vì vậy, nỗ lực bổ sung thêm năng chứng bảo mật lý thuyết và thực tiễn là nâng cao độ tin cậy của lược đồ.
 - Việc phụ thuộc vào các định nghĩa, giả định và bằng chứng tạo thành một cách tiếp cận chặt chẽ đối với mật mã hiện đại khác biệt với cách tiếp cận không chính thức của mật mã cổ điển.

Chương 2: Mật mã hóa khóa đối xứng

Mật mã đối xứng hiện đại

- Các nguyên lý cơ bản
 - Bản tin: attack
 - Mã ASCII: 97 116 116 97 99 107
 - Biểu diễn nhị phân: 01100001 01110100 01110100 01100001 01100011 01101011;
 - bản tin nhị phân cũng tồn tại một số đặc tính thống kê nào đó mà người phá mã có thể tận dụng để phá bản mã;
 - Mã hóa hiện đại quan tâm đến vấn đề chống phá mã trong các trường hợp biết trước bản rõ (known-plaintext), hay bản rõ được lựa chọn (chosen-plaintext).
 - Giả sử dùng một khóa K gồm 4 bit 0101 để mã hóa bản rõ trên bằng phép XOR

bản rõ: 1111 0000 0011 (head)

khóa: 0101 0101 0101

bản mã: 1010 0101 0110 (FBCG)

Chương 2: Mật mã hóa khóa đối xứng

Mật mã luồng

- **Bộ tạo số giả ngẫu nhiên**
 - Một chuỗi giả ngẫu nhiên cần đảm bảo đặc trưng ngẫu nhiên gồm: hàm phân bố đồng dạng và độc lập ngẫu nhiên.
 - Một chuỗi bit ngẫu nhiên thực là kết quả của một ánh xạ từ nguồn ngẫu nhiên (high-entropy) tới chuỗi bít.
 - Một chuỗi giả ngẫu nhiên là kết quả của một nguồn ngẫu nhiên đóng vai trò hạt giống và kết hợp với thuật toán tất định còn gọi là trình tạo chuỗi số giả ngẫu nhiên.
 - Bộ/trình tạo chuỗi số giả ngẫu nhiên G là một thuật toán tất định, hiệu quả để biến đổi một chuỗi ngắn và đồng nhất (được gọi là hạt giống) thành chuỗi đầu ra dài hơn.

Gọi G là một thuật toán đa thức tất định thời gian sao cho bất kỳ đầu vào n và bất kỳ hạt giống $s \in \{0,1\}^n$, kết quả $G(s)$ là một chuỗi có độ dài $l(n)$. G là bộ tạo số ngẫu nhiên giả nếu đảm bảo các điều kiện sau.

Chương 2: Mật mã hóa khóa đối xứng

Mật mã luồng

- **Bộ tạo số giả ngẫu nhiên**
 - Một chuỗi giả ngẫu nhiên cần đảm bảo đặc trưng ngẫu nhiên gồm: hàm phân bố đồng dạng và độc lập ngẫu nhiên.
 - Một chuỗi bit ngẫu nhiên thực là kết quả của một ánh xạ từ nguồn ngẫu nhiên (high-entropy) tới chuỗi bít.
 - Một chuỗi giả ngẫu nhiên là kết quả của một nguồn ngẫu nhiên đóng vai trò hạt giống và kết hợp với thuật toán tất định còn gọi là trình tạo chuỗi số giả ngẫu nhiên.
 - Bộ/trình tạo chuỗi số giả ngẫu nhiên G là một thuật toán tất định, hiệu quả để biến đổi một chuỗi ngắn và đồng nhất (được gọi là hạt giống) thành chuỗi đầu ra dài hơn.

Gọi G là một thuật toán đa thức tất định thời gian sao cho bất kỳ đầu vào n và bất kỳ hạt giống $s \in \{0,1\}^n$, kết quả $G(s)$ là một chuỗi có độ dài $l(n)$. G là bộ tạo số ngẫu nhiên giả nếu đảm bảo các điều kiện sau.**1. Mở rộng. Với mọi n thì có $l(n) > n$.** **2. Ngẫu nhiên theo xác suất**

Chương 2: Mật mã hóa khóa đối xứng

Mật mã luồng

- **Bộ tạo số giả ngẫu nhiên**
 - Một chuỗi giả ngẫu nhiên cần đảm bảo đặc trưng ngẫu nhiên gồm: hàm phân bố đồng dạng và độc lập ngẫu nhiên.
 - Một chuỗi bit ngẫu nhiên thực là kết quả của một ánh xạ từ nguồn ngẫu nhiên (high-entropy) tới chuỗi bít.
 - Một chuỗi giả ngẫu nhiên là kết quả của một nguồn ngẫu nhiên đóng vai trò hạt giống và kết hợp với thuật toán tất định còn gọi là trình tạo chuỗi số giả ngẫu nhiên.
 - Bộ/trình tạo chuỗi số giả ngẫu nhiên G là một thuật toán tất định, hiệu quả để biến đổi một chuỗi ngắn và đồng nhất (được gọi là hạt giống) thành chuỗi đầu ra dài hơn.

Gọi G là một thuật toán đa thức tất định thời gian sao cho bất kỳ đầu vào n và bất kỳ hạt giống $s \in \{0,1\}^n$, kết quả $G(s)$ là một chuỗi có độ dài $l(n)$. G là bộ tạo số ngẫu nhiên giả nếu đảm bảo các điều kiện sau.**1. Mở rộng. Với mọi n thì có $l(n) > n$.** **2. Ngẫu nhiên theo xác suất**

Chương 2: Mật mã hóa khóa đối xứng

Mật mã luồng

Mã luồng (stream cipher) Kích thước một đơn vị mã hóa: gồm k bít. Bản rõ được chia thành các đơn

Mã luồng có các đặc tính sau: vị mã hóa: $P \rightarrow p_0 p_1 p_2 \dots p_{n-1}$ ($p_i : k$ bít)

Một bộ sinh dãy số ngẫu nhiên: dùng một khóa K ban đầu để sinh ra các số ngẫu nhiên có kích thước bằng kích thước đơn vị mã hóa:

$StreamCipher(K) \rightarrow S = s_0 s_1 s_2 \dots s_{n-1}$ ($s_i : k$ bít)

Mỗi số ngẫu nhiên được XOR với đơn vị mã hóa của bản rõ để có được bản mã.

$$c_0 = p_0 \oplus s_0, c_1 = p_1 \oplus s_1 \dots ; C = c_0 c_1 c_2 \dots c_{n-1}$$

Quá trình giải mã được thực hiện ngược lại, bản mã C được XOR với dãy số ngẫu nhiên S để cho ra lại bản rõ ban đầu

$$p_0 = c_0 \oplus s_0, p_1 = c_1 \oplus s_1 \dots$$

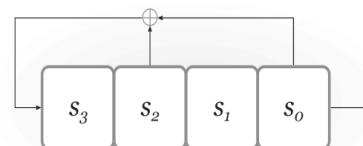
Điểm quan trọng nhất của các mã luồng là bộ sinh số ngẫu nhiên.

Mật mã luồng được xác định bởi hai thuật toán tất định (Init; Next).

Chương 2: Mật mã hóa khóa đối xứng

Mật mã luồng

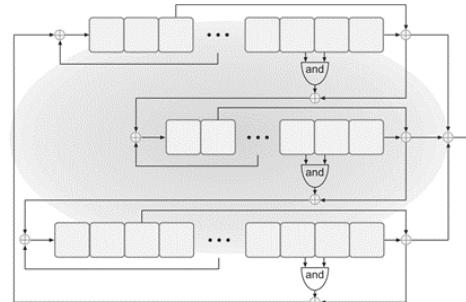
- **Thanh ghi dịch chuyển phản hồi tuyến tính**
 - Các thanh ghi dịch chuyển phản hồi tuyến tính LFSR (linear-feedback shift registers) được sử dụng để tạo số giả ngẫu nhiên do tính hiệu quả khi triển khai trong phần cứng và có thuộc tính thống kê ngẫu nhiên tốt.
 - LFSR không hàm chứa trình tạo giả ngẫu nhiên.
 - Mỗi thanh ghi lưu trữ một bit duy nhất, trạng thái của LFSR tại thời điểm bất kỳ là toàn bộ các bit có trong các thanh ghi. Trạng thái này được cập nhật trong mỗi khoảng thời gian bằng cách dịch chuyển tất cả các giá trị của các thanh ghi sang bên phải, và đặt giá trị mới của thanh ghi ngoài cùng bên trái bằng cách XOR của một số tập con thanh ghi hiện thời (qua hệ số phản hồi)



Chương 2: Mật mã hóa khóa đối xứng

Mật mã luồng

- **Mật mã luồng trivium**
 - Trivium sử dụng ba FSR được ghép nối, phi tuyến được ký hiệu là A, B và C và có độ 93, 84 và 111 tương ứng.
 - Đầu ra của mỗi FSR là XOR của thanh ghi ngoài cùng bên phải của nó và một thanh ghi bổ sung; đầu ra của Trivium là XOR của các bit đầu ra của ba FSR.
 - Hàm phản hồi trong mỗi trường hợp là phi tuyến. Thuật toán Init của Trivium chấp nhận khóa 80 bit và IV 80 bit.



Chương 2: Mật mã hóa khóa đối xứng

Mật mã luồng

- **Mật mã RC4**

- LFSRs hiệu quả khi được triển khai trong phần cứng nhưng có hiệu suất kém trong phần mềm. Vì thế xuất hiện các thiết kế thay thế ví dụ như mật mã RC4 do Ron Rivest đưa ra năm 1987.

Init algorithm for RC4	Next algorithm for RC4
Input: 16-byte key k Output: Initial state (S, i, j) (Note: All addition is modulo 256) for $i = 0$ to 255: $S[i] := i$ $k[i] := k[i \bmod 16]$ $j := 0$ for $i = 0$ to 255: $j := j + S[i] + k[i]$ Swap $S[i]$ and $S[j]$ $i := 0, j := 0$ return initial state (S, i, j)	Input: Current state (S, i, j) Output: Output byte y ; updated state (S, i, j) (Note: All addition is modulo 256) $i := i + 1$ $j := j + S[i]$ Swap $S[i]$ and $S[j]$ $t := S[i] + S[j]$ $y := S[t]$ return y and (S, i, j)

RC4 đảm bảo được tính giả ngẫu nhiên bằng hoán vị ban đầu với thuận toán Init và có được khuếch tán (trộn lẫn) tốt bằng thuận toán Next

Chương 2: Mật mã hóa khóa đối xứng

Mật mã luồng

- **Mật mã luồng ChaCha20**
 - Mật mã luồng ChaCha20 được giới thiệu vào năm 2008 với mục đích hiệu quả nhất với thiết kế phần mềm.
 - Giao thức bảo mật lớp truyền tải TLS (Transport Layer Security) là sự kết hợp của ChaCha20 với mã xác thực bản tin Poly1305.
 - Lõi của ChaCha20 là một hoán vị cố định P hoạt động trên chuỗi 512 bit. Hoán vị này được xây dựng trên ba toán tử: Phép cộng (modulo 2³²), bitwise (tuần hoàn), và XOR. Nên hoán vị này có tên gọi là ARX và gọi là mô hình hoán vị ngẫu nhiên.

Chương 2: Mật mã hóa khóa đối xứng

Mật mã khối

- Định nghĩa

- Định nghĩa mật mã khối. Mật mã khối là lược đồ mật mã đối xứng với $M = C = \{0,1\}^n$ và không gian khóa $K = \{0,1\}^r$. Lược đồ mã hóa như sau $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n, (k, m) \rightarrow E(k, m)$
- Sử dụng khóa bí mật k có độ dài r , thuật toán mã hóa E mã hóa các khối bản rõ m có độ dài cố định n và bản mã $c = E(k, m)$ cũng có độ dài n .
- Các ý tưởng từ mật mã cổ điển về hoán vị và thay thế đưa ra một tiếp cận khó tìm hàm ngược theo các liên hệ toán học.

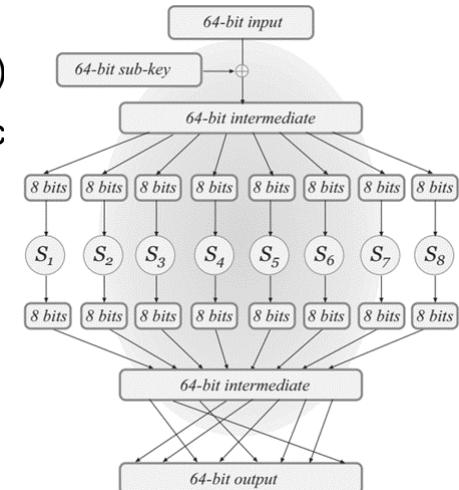
Chương 2: Mật mã hóa khóa đối xứng

Mật mã khối

- **Mạng SPN (Substitution-Permutation Network)**

- Để chống phá mã trong trường hợp known-plaintext hay chosen-plaintext, chỉ có thể là làm cho P và C không có mối liên hệ toán học. Điều này chỉ có thể thực hiện được nếu ta lập một bản tra cứu ngẫu nhiên giữa bản rõ và bản mã.
- Phép thay thế (substitution, S-box), Phép hoán vị (Permutation, P-box)
- Tính chất bảo mật của mạng được đánh giá qua các vòng gồm các bước
 - 1. *Trộn khóa: Đặt $x' = x \oplus k$, với k là khóa phụ vòng hiện tại;*
 - 2. *Phép thay thế: với x'_i là byte thứ i của x' ;*
 - 3. *Hoán vị: Hoán vị các bit của x' để lấy đầu ra của vòng.*

Tính khuếch tán và Tính gây lẫn



Chương 2: Mật mã hóa khóa đối xứng

Mật mã khối

- **Mật mã Feistel**

- Mạng Feistel cung cấp một cách để xây dựng một hàm có thể đảo ngược từ các thành phần không thể đảo ngược. Khác với tiếp cận SPN.
- Các hàm khóa vòng f_i là cố định và công khai nhưng khóa trong các vòng là bí mật.

$$P \xrightarrow{k_1} C_1 \xrightarrow{k_2} C_2 \dots \xrightarrow{k_{n-1}} C_n$$

- Vòng thứ i của mạng Feistel hoạt động như sau.

$$L_i := R_{i-1}; R_i := L_{i-1} \oplus f_i(R_{i-1})$$

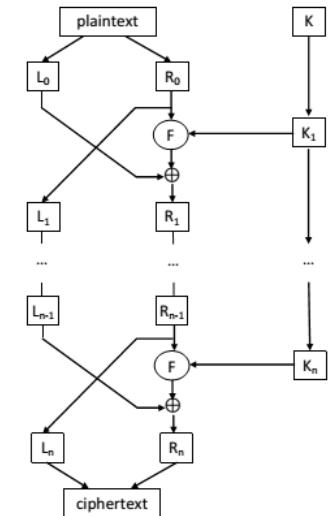
$$P = (LE_0, RE_0), C_i = (LE_i, RE_i); i=1,2,\dots,n$$

$$LE_i = RE_{i-1}, RE_i = LE_{i-1} \oplus F(LE_{i-1}, K_i); C = (RE_n, LE_n).$$

$$LD_0 := RE_n, RD_0 := LE_n;$$

$$LD_i = RD_{i-1}, RD_i = LD_{i-1} \oplus F(RD_{i-1}, K_i)$$

$$P = (RD_n, LD_n)$$



Chương 2: Mật mã hóa khóa đối xứng

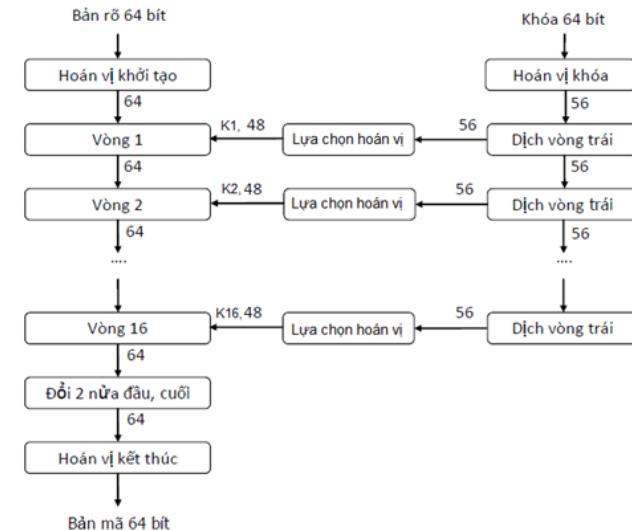
Mật mã khối

- **Mật mã DES (Data Encryption Standard)**

- Sử dụng mạng Feistel 16 vòng, ngoài ra DES có thêm một hoán vị khởi tạo trước khi bắt đầu vòng 1 và một hoán vị kết thúc sau vòng 16.
- Kích thước khối là 64 bit; Kích thước khóa là 56 bit.
- Mỗi vòng của DES dùng khóa con có kích thước 48 bit được trích ra từ khóa chính.

Quá trình xử lý bản rõ diễn ra trong ba giai đoạn.

- (1) Hoán vị khởi tạo,
- (2) hoán vị và thay thế theo 16 vòng mạng Feistel,
- (3) hoán vị nghịch đảo cho ra bản mã.



Chương 2: Mật mã hóa khóa đối xứng

Mật mã khối

- Mật mã DES (Data Encryption Standard)
 - Hoán vị khởi tạo và kết thúc

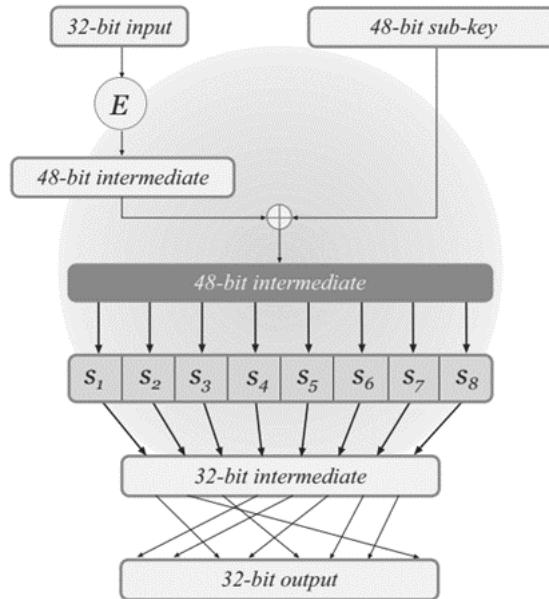
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7
56	48	40	32	24	16	8	0
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6

39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25
32	0	40	8	48	16	56	24

($b_0 b_1 b_2 \dots b_{62} b_{63} \rightarrow b_{57} b_{49} b_{41} \dots b_{14} b_6$)

Toàn bộ lược đồ lấy khóa (cách chia khóa, và bit sử dụng để tạo khóa k_i) là cố định và công khai, và bí mật duy nhất là chính khóa chính.

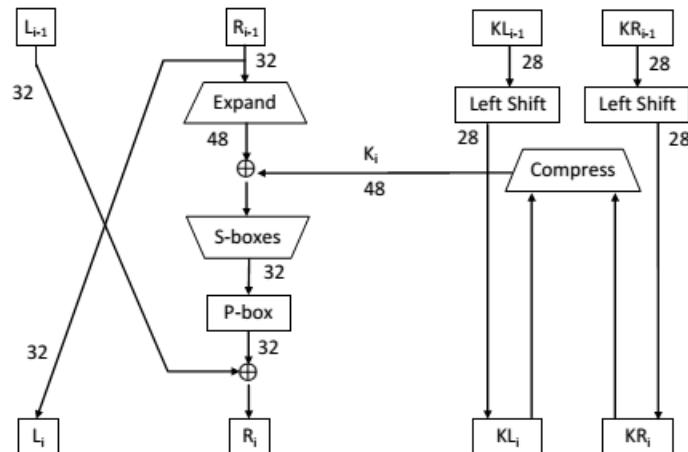
- Hàm vòng tương đương hoán vị thay thế



Chương 2: Mật mã hóa khóa đối xứng

Mật mã khối

- Mật mã DES (Data Encryption Standard)
 - Cấu trúc một vòng của DES



Expand(R_{i-1})

Mở rộng R 32 bit thành 48 bit

S-boxes

Nén K 48 bit thành 32 bit

P-box

Hoán vị 32 bit

$$F(R_{i-1}, K_i) = P\text{-}box(S\text{-}boxes(\text{Expand}(R_{i-1}) \oplus K_i))$$

Chương 2: Mật mã hóa khóa đối xứng

Mật mã khối

- **Mật mã DES (Data Encryption Standard)**
 - **Sbox có 3 thuộc tính chính**
 - (1) Mỗi Sbox là một hàm 4 đổi 1;
 - (2) Mỗi hàng chứa một giá trị chuỗi 4 bit đơn nhất;
 - (3) Thay đổi một bit bất kỳ đầu vào luôn kéo theo ít nhất hai bit đầu ra.
 - **Hiệu ứng lan truyền/ khuếch tán mạnh**
 - **Điểm yếu lớn nhất của DES là độ dài khóa 56 bit, với kiểu tấn công vét cạn đã thành công (1997).**

Chương 2: Mật mã hóa khóa đối xứng

Mật mã khối

- **Mật mã AES (Advanced Encryption Standard)**

- Vào tháng 10 năm 2000, NIST thông báo rằng thuật toán chiến thắng cuộc thi chọn mật mã mới thay cho DES là Rijndael (một mật mã khối được thiết kế bởi các nhà mật mã học người Bỉ Vincent Rijmen và Joan Daemen).
- Trái ngược với mật mã DES sử dụng cấu trúc Feistel, AES về cơ bản là một mạng thay thế-hoán vị SPN. Trong quá trình tính toán thuật toán AES, các khối mã hóa được đưa vào mảng trạng thái (4x4 byte) và thay đổi theo các vòng. Đến vòng cuối, trạng thái được chuyển tới đầu ra.
- Cấu trúc đại số của AES Rijndael. Rijndael sử dụng trường hữu hạn \mathbb{F}_{2^8} được xác định bởi đa thức tối giản $m(x) = x^8 + x^4 + x^3 + x + 1$, $m(x)$ không phải là nguyên hàm.
- *Phép cộng hai đa thức được định nghĩa là phép cộng hai đa thức mà hệ số của chúng bị giảm đi theo modulo 2.*
- *Phép nhân hai đa thức được định nghĩa là phần dư của tích các đa thức này chia cho $m(x)$.*

Chương 2: Mật mã hóa khóa đối xứng

Mật mã khối

- **Mật mã AES (Advanced Encryption Standard): Các thao tác trên một vòng**
 - Giai đoạn 1 {AddRoundKey}: Đưa vào một khóa phụ 128 bit có gốc từ khóa chính và được xem như một mảng 4×4 byte. Mảng trạng thái được cập nhật bằng cách XOR chính nó với khóa phụ này. (state, roundkey) \rightarrow state \oplus roundkey.
 - Giai đoạn 2 {SubBytes}: Trong bước này, mỗi byte của mảng trạng thái được thay thế bằng một byte khác theo một bảng tra cứu cố định duy nhất Sbox. Sbox là một hoán vị trên trường $\{0,1\}^8$.
 - Giai đoạn 3 {ShiftRows}: Tiếp theo, các byte trong mỗi hàng của mảng trạng thái được xáo trộn như sau: hàng đầu tiên của mảng không được tác động, mỗi byte của hàng thứ hai được dịch sang trái một vị trí, hàng thứ ba được dịch chuyển sang trái hai vị trí, và hàng thứ tư được dịch sang trái ba vị trí.
 - Giai đoạn 4 {MixColumns}: Cuối cùng, một phép biến đổi tuyến tính có thể đảo ngược được áp dụng cho bốn byte trong mỗi cột. Phép biến đổi này có đặc tính là nếu hai đầu vào khác nhau $b > 0$ byte, thì các kết quả đầu ra khác nhau ít nhất $(5 - b)$ byte.

Chương 2: Mật mã hóa khóa đối xứng

Mật mã khối

Mật mã AES (Advanced Encryption Standard): Các thao tác trên vòng

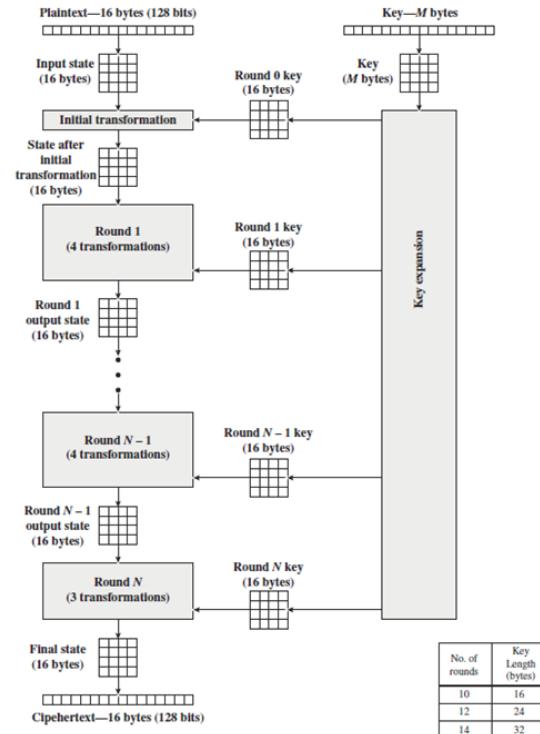
- Trong vòng cuối cùng, MixColumns được thay thế bằng AddRoundKey.
- Điều này ngăn không cho kẻ tấn công đảo ngược ba giai đoạn cuối mà không phụ thuộc vào chìa khóa.

Số vòng phụ thuộc vào độ dài khóa.

10 vòng được sử dụng cho AES-128;

12 vòng cho AES-192;

14 vòng cho AES-256.



Chương 2: Mật mã hóa khóa đối xứng

Các phương thức hoạt động của mật mã khối

- Chế độ sổ mã điện tử (Electronic Codebook Mode)

Chế độ sổ mã điện tử là chế độ tương minh. Thuật toán mã hóa là tất định (các khối bản rõ giống hệt nhau dẫn đến các khối bản mã giống hệt nhau).

Mã hóa hoạt động giống như một cuốn sách mã với mỗi khối của bản tin m được mã hóa độc lập với các khối khác.

Các lỗi bit truyền trong một khối bản mã đơn chỉ ảnh hưởng đến việc giải mã của khối đó.

```
bitString ecbEncrypt(bitString m)
    1  divide  $m$  into  $m_1 \dots m_l$ 
    2  for  $i \leftarrow 1$  to  $l$  do
        3       $c_i \leftarrow E_k(m_i)$ .
    4  return  $c_1 \dots c_l$ 
```

Chương 2: Mật mã hóa khóa đối xứng

Các phương thức hoạt động của mật mã khối

- Chế độ chuỗi khối mật mã (Cipher-Block Chaining Mode)

Trong chế độ chuỗi khối mật mã, ta có $r=n$. Mã hóa trong chế độ chuỗi khối mật mã được thực hiện bởi thuật toán sau

bitString *cbcEncrypt*(bitString *m*)

- 1 select $c_0 \in \{0, 1\}^n$ at random
- 2 divide *m* into $m_1 \dots m_l$
- 3 for $i \leftarrow 1$ to l do
- 4 $c_i \leftarrow E_k(m_i \oplus c_{i-1})$
- 5 return $c_0c_1 \dots c_l$

bitString *cbcDecrypt*(bitString *c*)

- 1 divide *c* into $c_0c_1 \dots c_l$
- 2 for $i \leftarrow 1$ to l do
- 3 $m_i \leftarrow E_k^{-1}(c_i) \oplus c_{i-1}$
- 4 return $m_1 \dots m_l$

Việc chọn giá trị khởi tạo c_0 một cách ngẫu nhiên nhằm tránh bị tấn công vào các khối bản mã giống nhau.

Trong cả hai chế độ ECB và CBC đều yêu cầu có hàm ngược giải mã.

Chương 2: Mật mã hóa khóa đối xứng

Các phương thức hoạt động của mật mã khối

- Chế độ phản hồi mật mã (Cipher Feedback Mode)

Chế độ phản hồi mật mã dựa trên sự dịch chuyển phản hồi các vòng.

Trong chế độ phản hồi mật mã, chúng ta có $1 \leq r \leq n$

```
bitString fbEncrypt(bitString m, x1)  
1 divide m into m1 ... ml  
2 for i ← 1 to l do  
3     ci ← mi ⊕ msbr(Ek(xi))  
4     xi+1 ← lsbn-r(xi)||ci  
5 return c1 ... cl
```

Luồng khóa được tính bằng cách sử dụng thuật toán mã hóa khóa E_k cho khóa k theo giá trị x_1 và khôi bǎn mã đã tính.

Bản tin được xử lý theo từng bit và cơ sở bản tin có thể có độ dài tùy ý mà vẫn được mã hóa không cần đếm

Chương 2: Mật mã hóa khóa đối xứng

Các phương thức hoạt động của mật mã khối

- Chế độ phản hồi đầu ra (Output Feedback Mode)

Tương tự như trong CFM, ta có $1 \leq r \leq n$, cho $x_1 \in \{0, 1\}^n$. Chế độ phản hồi đầu ra được triển khai theo thuật toán sau.

```
bitString ofbEnCrypt(bitString m, x1)
1  divide m into  $m_1 \dots m_l$ 
2  for  $i \leftarrow 1$  to  $l$  do
3       $c_i \leftarrow m_i \oplus \text{msb}_r(E_k(x_i))$ 
4       $x_{i+1} \leftarrow E_k(x_i)$ 
5  return  $c_1 \dots c_l$ 
```

Các chế độ phản hồi đầu ra tương tự như chế độ phản hồi mật mã ngoại trừ việc giá trị đầu ra của hàm để phản hồi cho vòng mã hóa tiếp theo vì các bản mã.

Vì vậy, tất cả các bit của khối đầu ra sẽ được gửi phản hồi thay vì một số bit đã chọn

Chương 2: Mật mã hóa khóa đối xứng

Kết luận chương

- Các vấn đề cần ôn tập
 1. Các tiếp cận mật mã cổ điển.
 2. Các đặc trưng hoán vị và thay thế.
 3. Vấn đề khuếch tán và gây lẩn.
 4. Đặc trưng của vấn đề mật mã hiện đại.
 5. Các đặc điểm của chuỗi ngẫu nhiên, hàm ngẫu nhiên và các mô tả toán học.
 6. Các mô hình mật mã luồng và ưu nhược điểm.
 7. Nguyên tắc hoạt động, ưu nhược điểm của các lược đồ mật mã Fiestel, DES và AES.
 8. Các phương thức hoạt động của mật mã khối.

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Mã hóa đối xứng dù rằng đã phát triển từ cổ điển đến hiện đại, vẫn tồn tại hai điểm yếu sau;

- *Vấn đề trao đổi khóa giữa người gửi và người nhận (kênh an toàn là khó khả thi)*
- *Tính bí mật của khóa: không có cơ sở quy trách nhiệm nếu khóa bị tiết lộ.*

Whitfield Diffie và Martin Hellman đã tìm ra phương pháp mã hóa công khai/ mã khóa bất đối xứng.

Có phương pháp nào để việc mã hóa và giải mã dùng hai khóa khác nhau?
Có nghĩa là $C = E(P, K1)$ và $P = D(C, K2)$.

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

- Người nhận giữ bí mật khóa K_2 , còn khóa K_1 thì công khai cho tất cả. Người gửi dùng khóa K_1 để mã hóa, người nhận dùng K_2 để giải mã. (đảm bảo bảo mật)
- Người gửi giữ bí mật khóa K_1 , còn khóa K_2 thì công khai cho tất cả. Người gửi dùng khóa K_1 để mã hóa, người nhận dùng K_2 để giải mã. (không đảm bảo bảo mật nhưng đảm bảo tính chứng thực và tính không từ chối)
- Khóa riêng (bi mật) là K_R . Khóa công khai là K_U , Bản rõ được ký hiệu là M , còn bản mã là C ;

$$C = E(M, K_U) \qquad C = E(M, K_R)$$

$$M = D(C, K_R) \qquad M = D(C, K_U)$$

- $K_R = fK_U$ là các hàm một chiều; các phương pháp Knapsack, RSA, Elgaman, và ~~phương pháp đường cong elliptic ECC...~~

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

- Phương pháp RSA là một phương pháp mã hóa khóa công khai. RSA được xây dựng bởi các tác giả Ron Rivest, Adi Shamir và Len Adleman tại học viện MIT vào năm 1977;
- Về mặt tổng quát RSA là một phương pháp mã hóa theo khối.
- Trong đó bản rõ M và bản mã C là các số nguyên từ 0 đến 2^i với i số bít của khối.
- Kích thước thường dùng của i là 1024 bít. RSA sử dụng hàm một chiều là phân tích một số thành thừa số nguyên tố.

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

- Nguyên tắc thực hiện của RSA:
- Để thực hiện mã hóa và giải mã, RSA dùng phép lũy thừa modulo của lý thuyết số.
 - 1) Chọn hai số nguyên tố lớn p và q và tính $N = pq$. Cần chọn p và q sao cho: $M < 2^{i-1} < N < 2^i$
 - Với $i = 1024$ thì N là một số nguyên dài khoảng 309 chữ số.
 - 2) Tính $n = (p - 1)(q - 1)$
 - 3) Tìm một số e sao cho e nguyên tố cùng nhau với n
 - 4) Tìm một số d sao cho $e \cdot d \equiv 1 \pmod{n}$ (d là nghịch đảo của e trong phép modulo n)
 - 5) Hủy bỏ n , p và q . Chọn khóa công khai K_U là cặp (e, N) , khóa riêng K_R là cặp (d, N)

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

- Nguyên tắc thực hiện của RSA:

6) Việc mã hóa thực hiện theo công thức:

- Theo phương án 1, mã hóa bảo mật: $C = E(M, K_U) = M^e \text{ mod } N$
- Theo phương án 2, mã hóa chứng thực: $C = E(M, K_R) = M^d \text{ mod } N$

7) Việc giải mã thực hiện theo công thức:

- Theo phương án 1, mã hóa bảo mật: $\bar{M} = D(C, K_R) = C^d \text{ mod } N$
- Theo phương án 2, mã hóa chứng thực: $\bar{M} = D(C, K_U) = C^e \text{ mod } N$

Bản rõ M có kích thước $i-1$ bit, bản mã C có kích thước i bit.

Chương 3: Mật mã hóa khóa bất đối xứng

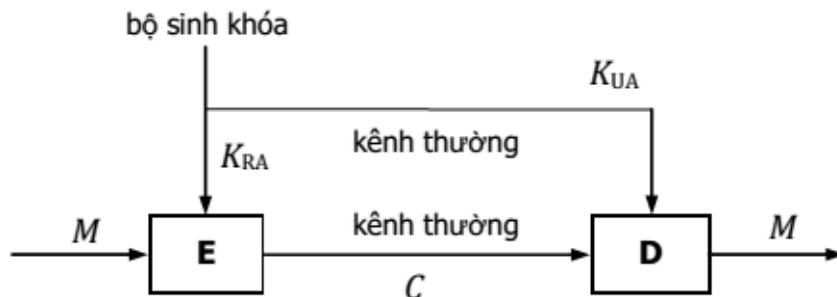
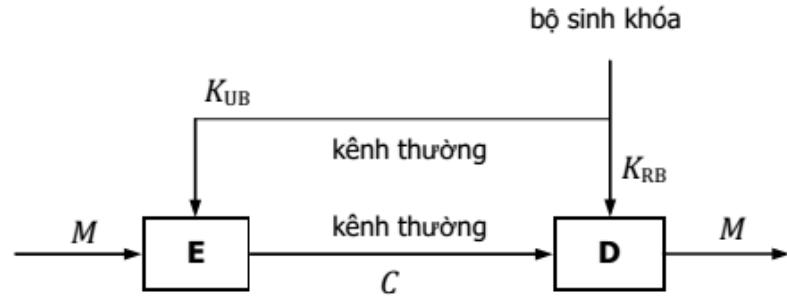
Mã hóa công khai

- Độ an toàn của RSA
- Vết cạn khóa: cách tấn công này thử tất cả các khóa d có thể có để tìm ra bản giải mã có ý nghĩa, tương tự như cách thử khóa K của mã hóa đối xứng. Với N lớn, việc tấn công là bất khả thi;
- Phân tích N thành thừa số nguyên tố $N = pq$: Chúng ta đã nói rằng việc phân tích phải là bất khả thi thì mới là hàm một chiều, là nguyên tắc hoạt động của RSA. (Thuật toán mới, tốc độ tính toán: khả thi);
- Đo thời gian: Đây là một phương pháp phá mã không dựa vào mặt toán học của thuật toán RSA, mà dựa vào một “hiệu ứng lè” sinh ra bởi quá trình giải mã RSA. Hiệu ứng lè đó là thời gian thực hiện giải mã bằng thuật toán bình phương liên tiếp để tìm d.

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Mô hình bảo mật và không chối từ



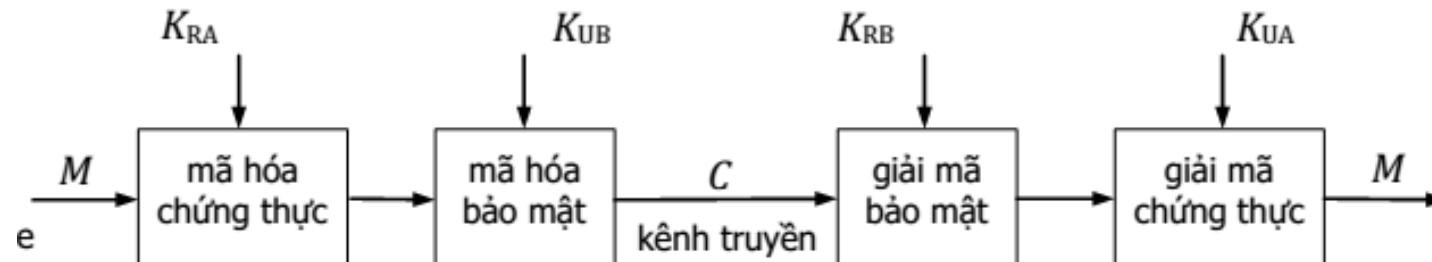
Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Kết hợp bảo mật, không từ chối và chứng thực

$$C = E(E(M, K_{RA}), K_{UB})$$

$$M = D(D(C, K_{RB}), K_{UA})$$



Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

- Trao đổi khóa
- Giảm gánh nặng cho từng cá nhân, một mô hình gọi là „chứng chỉ khóa công khai“ (public-key certificate) được sử dụng. Trong mô hình này có một tổ chức làm nhiệm vụ cấp chứng chỉ được gọi là trung tâm chứng thực (Certificate Authority – CA).



Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

- **Cấp chứng chỉ**
 - A gửi định danh ID_A và khóa công khai K_UA của mình đến trung tâm chứng thực.
 - Trung tâm chứng nhận kiểm tra tính hợp lệ của A, ví dụ nếu ID_A là „Microsoft”, thì Alice phải có bằng chứng chứng tỏ mình thực sự là công ty Microsoft.
 - Dựa trên cơ sở đó, trung tâm chứng thực cấp một chứng chỉ CA để xác nhận rằng khóa công khai K_UA đó là tương ứng với ID_A . Chứng chỉ được ký chứng thực bằng khóa riêng của trung tâm để đảm bảo rằng nội dung của chứng chỉ là do trung tâm ban hành.

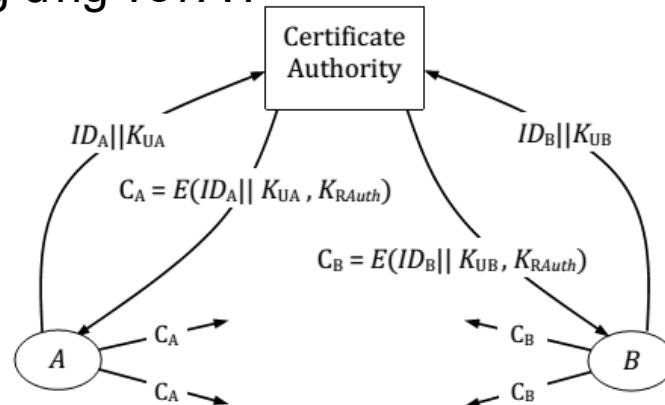
$$C_A = E(ID_A || K_{UA}, K_{RAuth})$$

($||$ là phép nối dãy bit)

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

- A công khai chứng chỉ CA .
- B muốn trao đổi thông tin với A thì sẽ giải mã CA bằng khóa công khai của trung tâm chứng thực để có được khóa công khai K_{UA} của A . Do đó nếu B tin tưởng vào trung tâm chứng thực thì B sẽ tin tưởng là K_{UA} là tương ứng với ID_A , tức tương ứng với A .



Chương 3: Mật mã hóa khóa bất đối xứng

Chứng chỉ số của khóa công khai

Vấn đề của khóa công khai:

- Khi A nhận được khóa công khai của B (từ Web site, e-mail, ...); Làm thế nào để biết đó là khóa công khai của B, chứ không phải của người mạo danh?
- Giải pháp:
- Thẩm quyền chứng chỉ tin cậy (trusted certification authority - CA).

Chương 3: Mật mã hóa khóa bất đối xứng

Chứng chỉ số của khóa công khai

Các yếu tố chính

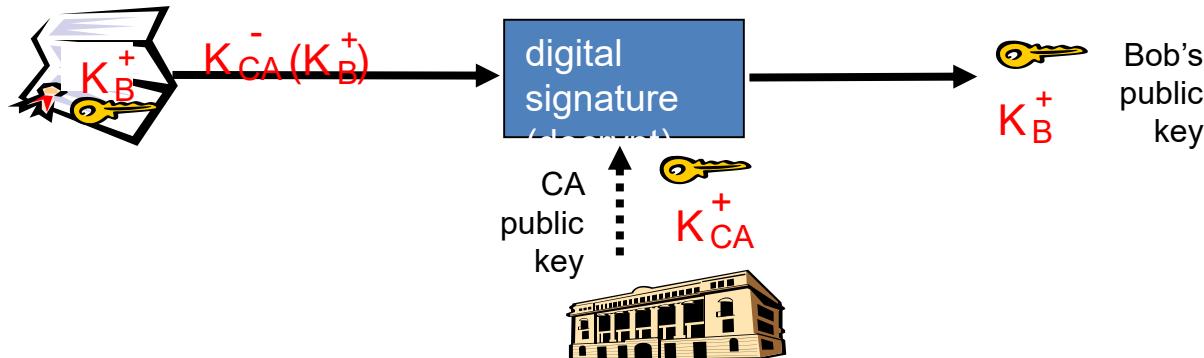
- Chứng chỉ số Certification Authority (CA): liên kết khóa công khai với thực thể cụ thể E.
- E đăng ký khóa công khai với CA.
- E cung cấp “bằng chứng định danh” (proof of identity) cho CA.
- CA mở chứng chỉ (certificate) ràng buộc E với khóa công khai của nó.
- Chứng chỉ chứa khóa công khai của E được ký số bởi CA: CA thông báo “Đây chính là khóa công khai của E”.

Chương 3: Mật mã hóa khóa bất đối xứng

Chứng chỉ số của khóa công khai

Cơ chế lấy khóa

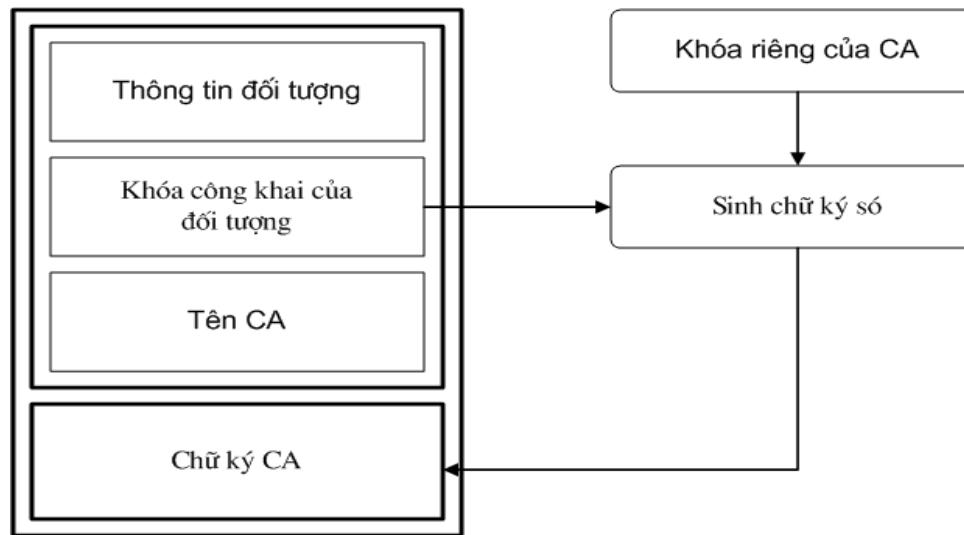
- Khi A muốn khóa công khai của B:
- Lấy chứng chỉ số của B (từ B hoặc từ đâu đó).
- Áp dụng khóa công khai của CA cho chứng chỉ của B, giải mã để lấy khóa công khai của B.



Chương 3: Mật mã hóa khóa bất đối xứng

Chứng chỉ số của khóa công khai

Cơ chế lấy khóa



Chương 3: Mật mã hóa khóa bất đối xứng

Chứng chỉ số của khóa công khai

Mô hình đệ quy

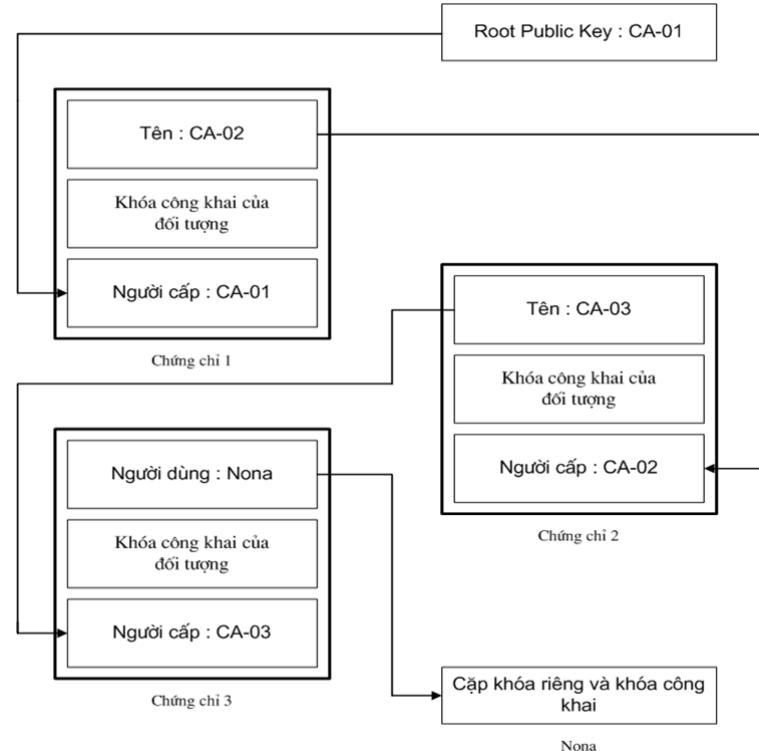
Các loại chứng chỉ số

Chứng chỉ SSL cho máy khách

Sử dụng để chứng thực máy khách với máy dịch vụ bằng giao thức bảo mật SSL. Bình thường, định danh của một máy khách có thể được thừa nhận với định danh của một người, ví dụ nhân viên của một công ty, một công dân.

Chứng chỉ SSL cho máy dịch vụ

Sử dụng để chứng thực máy dịch vụ với máy khách bằng giao thức SSL. Chứng thực máy dịch vụ là một điều kiện cần thiết cho một phiên làm việc trong giao thức bảo mật SSL.



Chương 3: Mật mã hóa khóa bất đối xứng

Chứng chỉ số của khóa công khai

Chứng thư S/MIME (S/MIME certificates)

Dùng để ký và mã hóa thư điện tử. Với một chứng thư SSL cho máy khách định danh của máy khách được thừa nhận như định danh của một người. Một chứng chỉ đơn cũng có thể được sử dụng chung cho hai loại chứng thư S/MIME và chứng thư SSL cho máy khách (Client SSL certificate)..

Chứng thư ký cho đối tượng

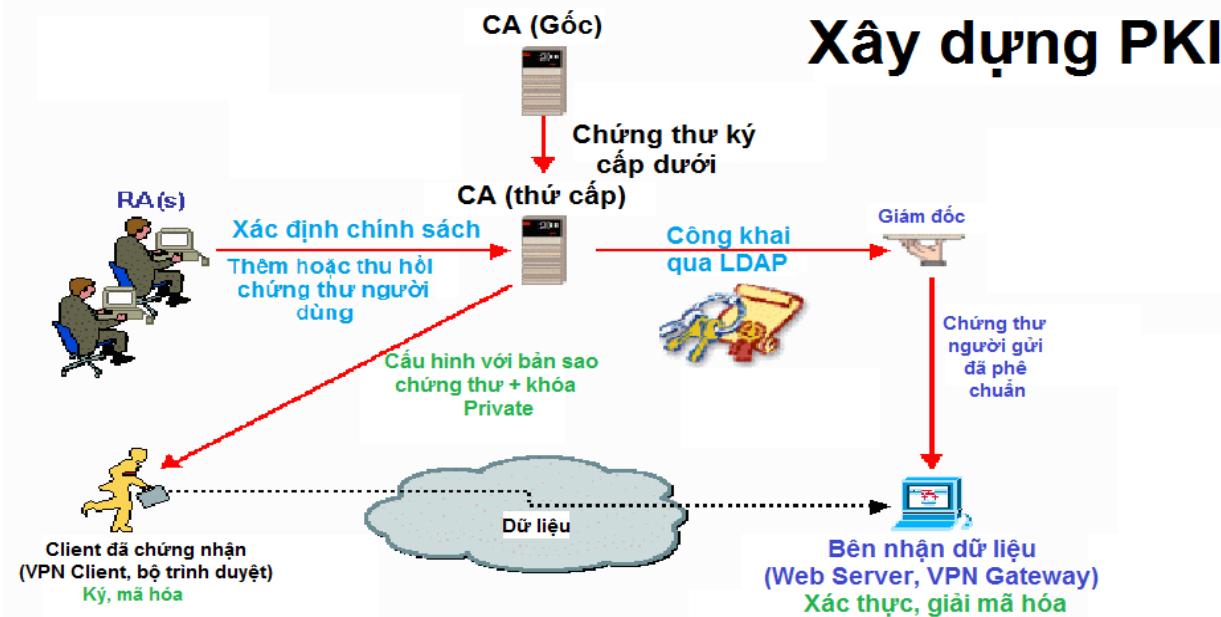
Dùng để chứng thực những người ký cho Java code, Javascript, hoặc những file và phần mềm cần được ký.

Chứng thư cho CA

Sử dụng để chứng thực cho các CA. Phần mềm máy khách và máy dịch vụ sử dụng chứng thư của CA để xác định các chứng thư khác có tin tưởng được không.

Chương 3: Mật mã hóa khóa bất đối xứng

Hệ tầng khóa công cộng



Chương 3: Mật mã hóa khóa bất đối xứng

Chứng chỉ số của khóa công khai

Các thành phần

Tổ chức phát hành chứng chỉ (Certificate Authority - CA):

Là một bên thứ ba được tin cậy có trách nhiệm tạo, quản lý, phân phối, lưu trữ và thu hồi các chứng chỉ số. CA sẽ nhận các yêu cầu cấp chứng chỉ số và chỉ cấp cho những ai đã xác minh được nhận dạng của họ.

Tổ chức đăng ký (Registration Authority - RA):

Đóng vai trò trung gian giữa CA và người dùng. Khi người dùng cần chứng chỉ số mới, họ gửi yêu cầu tới RA và RA sẽ xác nhận tất cả các thông tin nhận dạng cần thiết trước khi chuyển tiếp yêu cầu đó tới CA để CA thực hiện tạo và ký số lên chứng chỉ rồi gửi về cho RA hoặc gửi trực tiếp cho người dùng.

Chương 3: Mật mã hóa khóa bất đối xứng

Chứng chỉ số của khóa công khai

Các thành phần

Kho và lưu trữ chứng thư (Certificate Repository và Archive - CRA)

Đầu tiên là kho lưu trữ công khai và phân phối các chứng thư và CRL (chứa danh sách các chứng thư không còn hiệu lực). Kho thứ hai là một cơ sở dữ liệu được CA dùng để sao lưu các khóa hiện đang sử dụng và lưu trữ các khóa hết hạn, kho này cần được bảo vệ an toàn như chính CA.

Máy chủ bảo mật (Security Server - SS)

Là một máy chủ cung cấp các dịch vụ quản lý tập trung tất cả các tài khoản người dùng, các chính sách bảo mật chứng thư số, các mối quan hệ tin cậy (trusted relationship) giữa các CA trong PKI, lập báo cáo và nhiều dịch vụ khác.

Chương 3: Mật mã hóa khóa bất đối xứng

Chứng chỉ số của khóa công khai

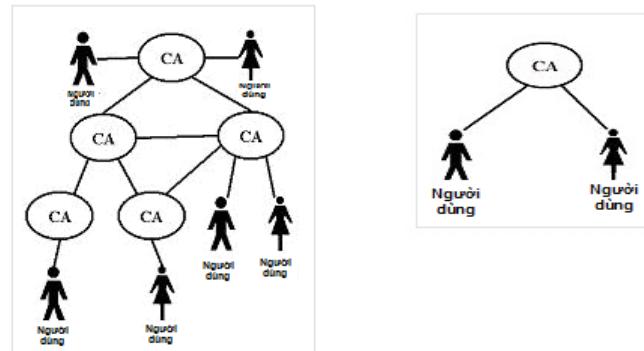
Các thành phần

Các ứng dụng cho phép PKI và những người sử dụng PKI (PKI-enabled applications và PKI users):

Bao gồm người dùng sử dụng các dịch vụ của PKI và các phần mềm có hỗ trợ cài đặt và sử dụng các chứng thư số như các trình duyệt web, các ứng dụng email ở phía máy khách.

Các mô hình

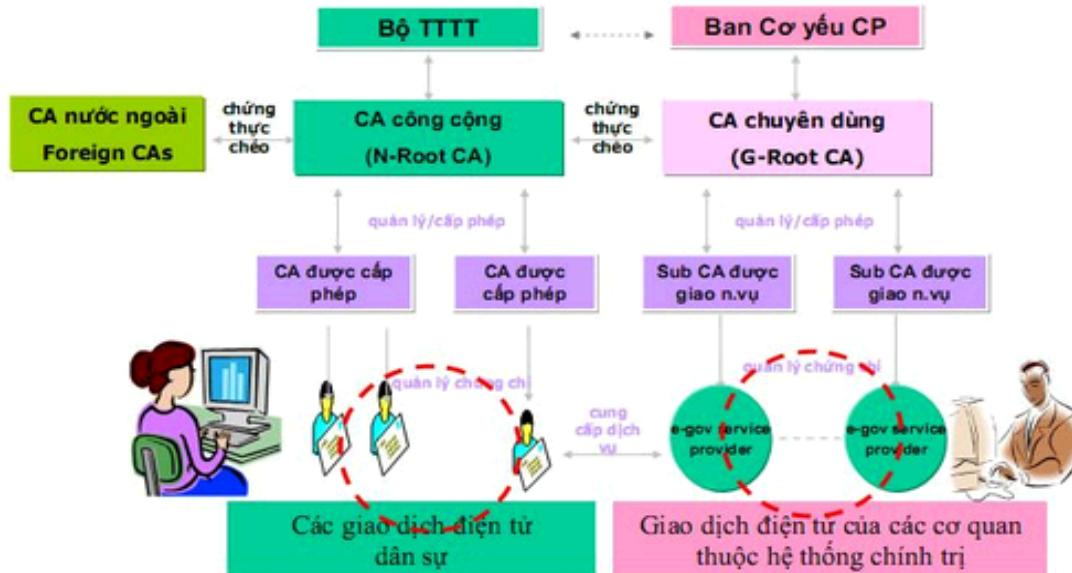
PKI phân cấp;
PKI dạng lưới;
CA đơn lẻ - Single CA.



Chương 3: Mật mã hóa khóa bất đối xứng

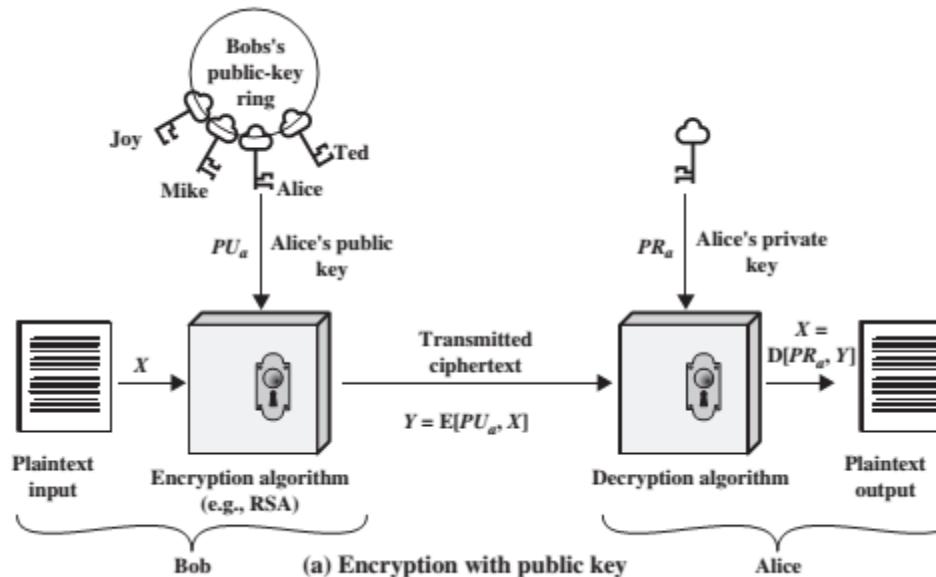
Chứng chỉ số của khóa công khai

Hệ tầng tại Việt Nam



Chương 3: Mật mã hóa khóa bất đối xứng

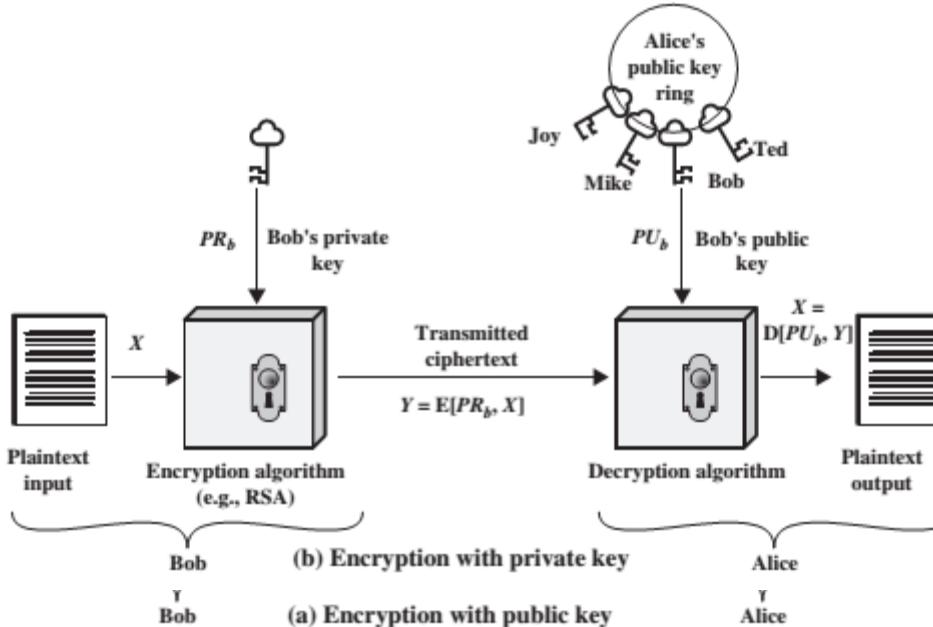
Mã hóa công khai



Sử dụng khóa công khai trong mã hóa

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai



Sử dụng khóa công khai trong giải mã

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Một số bước cơ bản có thể gồm:

- Mỗi người sử dụng tạo ra một cặp khóa được sử dụng để mã hóa và giải mã các bản tin.
- Mỗi người sử dụng đặt một trong hai khóa làm khóa công cộng và khóa kia bí mật.
- Nếu Bob muốn gửi một bản tin bí mật cho Alice, Bob mã hóa bản tin bằng khóa công khai của Alice.
- Khi Alice nhận được bản tin, cô giải mã bằng khóa riêng của mình. Không người nhận nào khác có thể giải mã bản tin bởi vì chỉ có Alice biết khóa riêng của Alice.

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Mã hóa truyền thống	Mã hóa công khai
<p>Yêu cầu hoạt động</p> <ul style="list-style-type: none">- Cùng thuật toán và cùng khóa để mã hóa và giải mã- Bên gửi và bên nhận phải chia sẻ thuật toán và khóa <p>Yêu cầu bảo mật</p> <ul style="list-style-type: none">- Khóa phải giữ bí mật- Phải bất khả thi trong việc giải mã nếu không có khóa bí mật- Hiểu biết về thuật toán và các mẫu của bản mã không đủ để xác định khóa	<p>Yêu cầu hoạt động</p> <ul style="list-style-type: none">- Một thuật toán và một khóa để mã hóa và một thuật toán khác và một khóa khác để giải mã- Bên gửi và bên nhận phải giữ một khóa riêng <p>Yêu cầu bảo mật</p> <ul style="list-style-type: none">- Một trong hai khóa phải giữ bí mật- Phải bất khả thi trong việc giải mã nếu không có khóa bí mật- Hiểu biết về thuật toán và các mẫu của bản mã không đủ để xác định khóa

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Các ứng dụng cho hệ mật khẩu công khai

Thuật toán	Mã hóa/Giải mã	Chữ ký số	Trao đổi khóa
RSA	Yes	Yes	Yes
Đường cong elliptic	Yes	Yes	Yes
Diffie-hellman	No	No	Yes
DSS	No	Yes	No

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Trao đổi khóa Diffie-Hellman

Thuật toán khóa công khai đầu tiên được xuất hiện trong báo cáo của Diffie và Hellman được gọi là mật mã hóa công khai [DIFF76b] và thường được nhắc đến là trao đổi khóa Diffie-Hellman.

Trao đổi khóa Diffie-Hellman dùng để thiết lập một khóa bí mật giữa người gửi và người nhận mà không cần dùng đến mã hóa công khai.

Phương pháp này dùng hàm một chiều làm hàm logarith rời rạc. Diffie-Hellman không có ý nghĩa về mã hóa giống như RSA.

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Trao đổi khóa Diffie-Hellman

Trước tiên A và B sẽ thống nhất sử dụng chung một số nguyên tố p và một số g nhỏ hơn p và là primitive root của p (nghĩa là phép toán $g^x \text{ mod } p$ khả nghịch)

Hai số p và g không cần giữ bí mật. Sau đó A chọn một số a và giữ bí mật số a này. B cũng chọn một số b và giữ bí mật số b . Tiếp theo A tính và gửi $g^a \text{ mod } p$ cho B, B tính và gửi $g^b \text{ mod } p$ cho A.

(g là căn nguyên thủy của n , với tất cả số nguyên là nguyên tố cùng nhau với n thì tồn tại k sao cho $g^k \equiv a \pmod{n}$).

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Trao đổi khóa Diffie-Hellman

- Trên cơ sở đó A tính $(g^b)^a \text{ mod } p = g^{ab} \text{ mod } p$

Trên cơ sở đó B tính $(g^a)^b \text{ mod } p = g^{ab} \text{ mod } p$

Do đó A và B có chung giá trị $g^{ab} \text{ mod } p$. Giá trị này có thể dùng làm khóa cho phép mã hóa đối xứng.

Muốn tính được $g^{ab} \text{ mod } p$, kẻ phá mã có thể có được g, p, g^a và g^b

Tuy nhiên, việc tính a hay b theo công thức: $a = \text{dlog}_{g, p} g^a$

hay $b = \text{dlog}_{g, p} g^b$ là không khả thi do tính phức tạp của phép logarithm rắc rối.

Khóa dùng chung được trao đổi bí mật giữa A và B.



Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Trao đổi khóa Diffie-Hellman

Gốc ban đầu của một số nguyên tố p là một số mà lũy thừa của nó modulo p tạo ra tất cả các số nguyên từ 1 đến $p-1$. Có nghĩa là nếu a là một gốc ban đầu của một số nguyên tố p thì các số $a \bmod p, a^2 \bmod p, \dots, a^{p-1} \bmod p$ là các số nguyên phân biệt từ 1 đến $p-1$. Với bất kỳ số nguyên b và một gốc ban đầu a của số nguyên tố p , ta có thể tìm ra một số mũ duy nhất i sao cho: $b \equiv a^i \pmod{p}$ với $0 \leq i \leq (p-1)$



Alice và Bob chia sẻ một số nguyên tố q và một số nguyên α , sao cho $\alpha < q$ và α là một căn nguyên thuy của q

Alice tạo một khóa riêng X_A sao cho $X_A < q$

Alice tính toán một khoá công khai $Y_A = \alpha^{X_A} \bmod q$

Alice nhận được khoá công khai Y_B dưới dạng bản rõ

Alice tính toán khoá bí mật $K = (Y_B)^{X_A} \bmod q$

Alice và Bob chia sẻ một số nguyên tố q và một số nguyên α , sao cho $\alpha < q$ và α là căn nguyên thuy của q

Bob tạo một khóa riêng X_B sao cho $X_B < q$

Bob tính toán một khoá công khai $Y_B = \alpha^{X_B} \bmod q$

Bob nhận được khoá công khai Y_A của Alice dưới dạng bản rõ

Bob tính toán khoá bí mật $K = (Y_A)^{X_B} \bmod q$

Số mũ i được gọi là thuật toán ròi rạc của b với căn nguyên thuy a , mod p .

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Trao đổi khóa Diffie-Hellman

Đặc trưng cơ bản của trao đổi khóa Diffie – Hellman

Các khóa bí mật chỉ được tạo khi cần thiết. Không cần phải chứa các khóa bí mật trong một khoảng thời gian dài.

Việc thỏa thuận dựa trên các tham số chung.

Nhược điểm bảo mật trao đổi khóa Diffie – Hellman

Nó không cung cấp thông tin bất kỳ về các định danh của các bên.

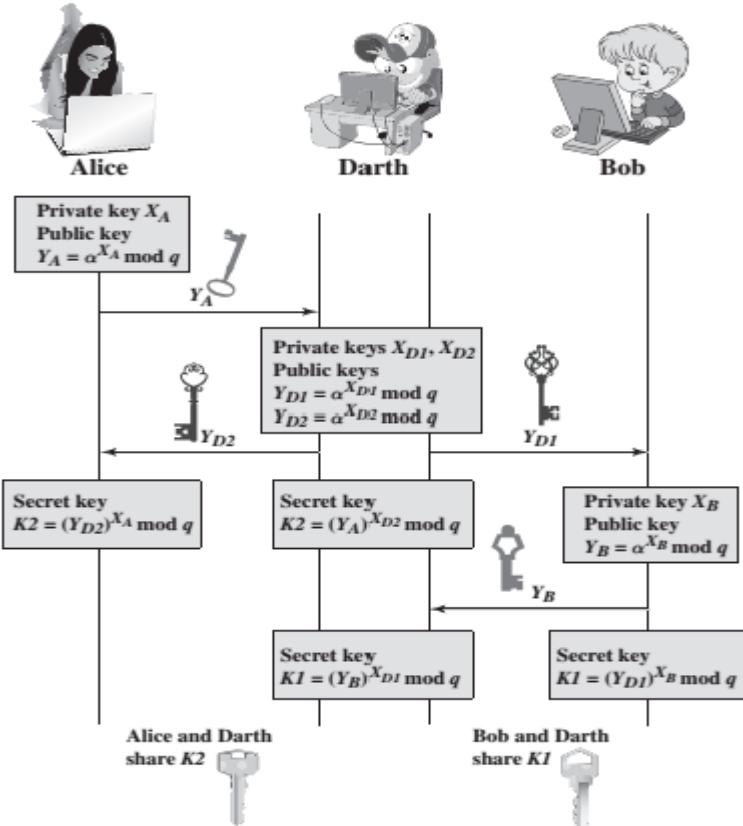
Nó an toàn đối với việc tấn công thụ động nghĩa là một người thứ ba biết a, b sẽ không tính được K . Tuy nhiên giao thức là không an toàn đối với việc tấn công chủ động bằng cách đánh tráo giữa đường hay còn gọi là kiểu tấn công “Man in the Middle”.

Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Tấn công ở giữa

1. Darth chuẩn bị cho quá trình tấn công bằng việc tạo ra 2 khóa ngẫu nhiên X_{D1} và X_{D2} . Sau đó tính toán ra khóa công khai tương ứng là Y_{D1} và Y_{D2} .
2. Alice gửi Y_A sang cho Bob.
3. Darth xen vào nhận Y_A và gửi Y_{D1} cho Bob. Darth cũng tính toán $K2 = (Y_A)^{X_{D2}} \text{ mod } q$.
4. Bob nhận được Y_{D1} và tính toán $K1 = (Y_{D1})^{X_B} \text{ mod } q$.
5. Bob gửi Y_B cho Alice.
6. Darth xen vào nhận Y_B và gửi Y_{D2} cho Alice. Darth tính toán $K1 = (Y_B)^{X_{D1}} \text{ mod } q$
7. Alice nhận Y_{D2} và tính toán $K2 = (Y_{D2})^{X_A} \text{ mod } q$



Chương 3: Mật mã hóa khóa bất đối xứng

Mã hóa công khai

Tấn công ở giữa

Ở đây, Bob và Alice đều nghĩ rằng họ chia sẻ một khóa bí mật nhưng thay vào đó là Bob và Darth chia sẻ khóa bí mật K1, Darth và Alice chia sẻ khóa bí mật K2. Tất cả những thông tin trao đổi giữa Bob và Alice đều được thỏa hiệp theo cách sau: Alice gửi bản tin đã được mã hóa $M:E(K2,M)$.

Darth xen vào nhận bản tin đã được mã và giải mã nó thành M .
Darth gửi cho Bob bản $E(K1,M)$ hoặc $E(K1,M')$ mà M' là bất kỳ bản tin nào. Trong trường hợp đầu tiên Darth chỉ đơn giản muốn nghe trộm thông tin mà không thay đổi chúng. Trường hợp sau Darth muốn làm sai lệch thông tin gửi đến Bob.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Vấn đề toàn vẹn và xác thực

Các tấn công

- Cải trang (Massquerade) : chèn các bản tin vào mạng từ một nguồn lừa đảo. Cải trang bao gồm cả việc tạo ra các bản tin bởi kẻ tấn công nhưng lại có vẻ như đến từ người ủy nhiệm.
- Sửa đổi nội dung (Content modification) : thay đổi nội dung của bản tin bao gồm các thao tác chèn, xóa, chuyển vị hay sửa đổi.
- Sửa đổi thứ tự (Sequence modification) : sửa đổi dãy bản tin giữa các bên bao gồm thao tác chèn, xóa, và thay đổi thứ tự các thông báo trong dãy.
- Sửa đổi thời gian (Timing modification) : làm trễ hoặc dùng lại bản tin.

Xác thực:

- Đảm bảo bản tin xuất phát đúng từ người gửi
- Đảm bảo bản tin không bị thay đổi, giả mạo.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Vấn đề toàn vẹn và xác thực

Các hàm xác thực được chia thành ba lớp như sau:

- Tổng kiểm tra mật mã (Cryptographic checksum): Một hàm chung của bản tin và một khoá bí mật tạo thành một giá trị độ dài cố định để làm bằng chứng xác thực
- Hàm băm (Hash functions) : Một hàm chung ánh xạ một bản tin có độ dài bất kỳ thành một giá trị Hash để làm bằng chứng xác thực.
- Lập mã bản tin (Message encryption) : bản mã của thông báo là bằng chứng xác thực.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Vấn đề toàn vẹn và xác thực

Checksum

- Internet checksum có một số đặc tính giống như hàm băm hash:
- Tạo ra các tóm tắt độ dài cố định (16-bit sum);
- Ánh xạ many-to-one.
- Không an toàn: Có thể dễ dàng tạo ra 2 bản tin khác nhau có cùng checksum.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Hàm băm

Các yêu cầu

- H có thể thao tác với khối dữ liệu kích thước bất kỳ.
- H tạo ra đầu ra độ dài cố định.
- $H(x)$ được tính dễ dàng với x bất kỳ.
- Với giá trị m bất kỳ của hàm Hash, không thể tìm ra x để $H(x) = m$.
- Với khối x bất kỳ, không thể tìm $y \neq x$ để $H(y) = H(x)$.
- Không thể tìm ra cặp (x,y) thoả mãn $H(x) = H(y)$.

MD5 hash function (RFC 1321) - 128-bit.

SHA-1 - US standard [NIST, FIPS PUB 180-1], 160-bit.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Hàm băm

Yêu cầu	Mô tả
Kích thước biến đầu vào	H có thể ứng dụng cho một khối dữ liệu có kích thước.
Kích thước đầu ra cố định	H tạo ra đầu ra có độ dài cố định.
Hiệu quả	$H(x)$ dễ dàng tính toán cho một x bất kỳ cho trước, có thể triển khai trên cả phần cứng và phần mềm.
Tính chất một chiều	Với bất kỳ giá trị băm h, tính toán y để $H(y)=h$ là bất khả thi.
Kháng xung đột yếu	Với bất kỳ một khối x, tính toán để tìm với $H(y)=H(x)$ là bất khả thi.
Kháng xung đột mạnh	Bất khả thi trong tính toán tìm kiếm một cặp bất kỳ (x,y) để $H(y)=H(x)$.
Giả ngẫu nhiên	Đầu ra của H đảm bảo tính giả ngẫu nhiên

Chương 4: Các giải thuật toàn vẹn dữ liệu

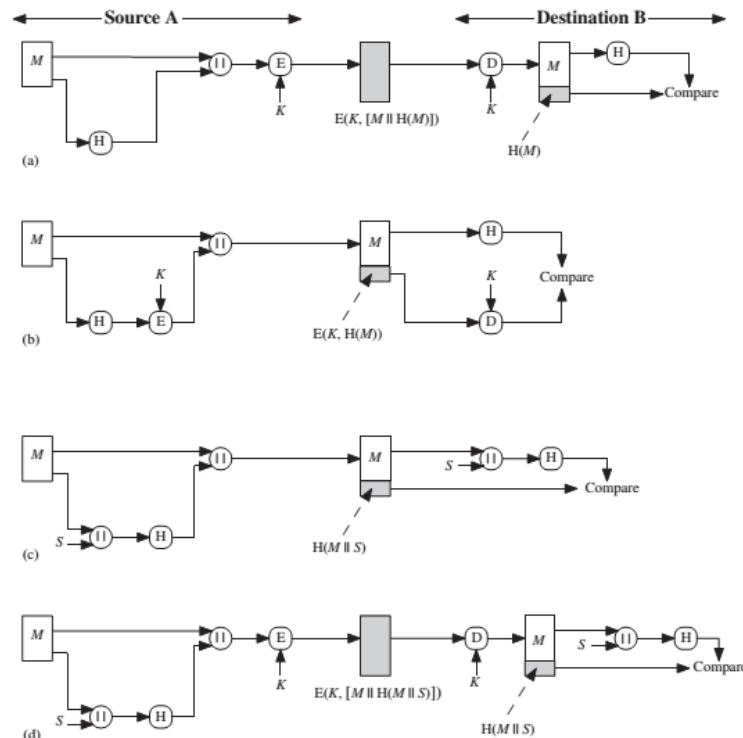
Hàm băm

i) Mã băm được nối vào bản tin, sau đó được mã hoá bởi mã hoá đối xứng. Vì chỉ có A và B biết khoá bí mật nên bản tin được đảm bảo truyền từ A và không bị sửa đổi. Do cả mã băm và bản tin đều được mã hoá nên tính bảo mật cũng được cung cấp trong trường hợp này.

ii) Chỉ có các mã băm được mã hoá bằng mã hoá đối xứng. Giúp giảm gánh nặng xử lý cho các ứng dụng không yêu cầu bảo mật.

iii) Giả sử bên gửi và nhận chia sẻ một giá trị bí mật S. Giá trị này được nối vào bản tin M và được sử dụng để tính toán giá trị băm. Sau đó, giá trị băm này được cộng với bản tin và truyền đi. Tại đầu nhận, B cũng có khả năng tính toán giá trị băm vì nó cũng biết S. Vì chỉ có A và B biết S, nên kẻ xấu không thể sửa đổi hoặc làm giả bản tin. Tính bảo mật không được cung cấp.

iv) Phương pháp này khác phương pháp (iii) ở việc tính bảo mật được thêm vào để mã hoá toàn bộ bản tin và mã băm trước khi truyền đi.



Chương 4: Các giải thuật toàn vẹn dữ liệu

Hàm băm

Các tấn công đoán thử đúng sai

Tấn công đoán thử đúng sai không phụ thuộc vào một thuật toán cụ thể mà chỉ phụ thuộc vào độ dài bit. Trong trường hợp của hàm băm, tấn công đoán thử đúng sai chỉ phụ thuộc vào độ dài của giá trị băm.

Tấn công vào nghịch ảnh và nghịch ảnh bậc hai

Đối với tấn công vào nghịch ảnh hoặc nghịch ảnh bậc hai, kẻ tấn công muốn tìm một giá trị y theo hàm $H(y)$ có giá trị bằng giá trị băm h cho trước. 2^{m-1}

Tấn công vào chống xung đột

Đối với tấn công vào đặc tính chống xung đột, kẻ xấu muốn tìm hai bản tin hoặc các khối dữ liệu x và y , có cùng một hàm băm $H(x) = H(y)$.

Nếu biến ngẫu nhiên được phân bố đều trong dải từ 0 đến $N-1$ thì xác suất để một phần tử lặp lại vượt quá 0.5 sau $N^{1/2}$ lựa chọn.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã xác thực bản tin

Đặc tính

Một kỹ thuật nhận thực liên quan đến việc sử dụng khóa bí mật để tạo khối dữ liệu nhỏ có kích thước cố định, được biết đến như là tổng kiểm tra mã hóa hoặc MAC, được thêm vào bản tin.

$$MAC = C(K, M)$$

M là bản tin đầu vào

C là hàm MAC

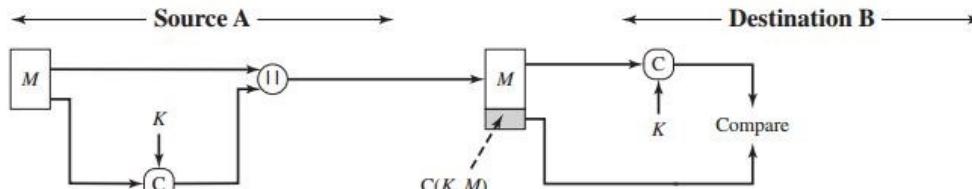
K là khóa bí mật chia sẻ

MAC là mã xác thực bản tin

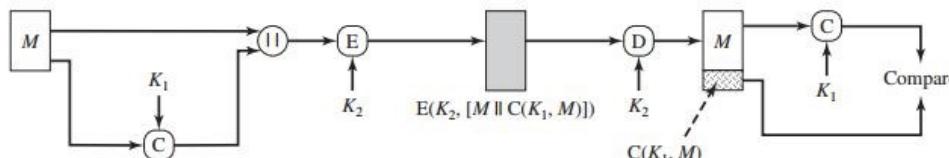
Bản tin cùng với MAC được truyền tới người nhận mong muốn. Người nhận thực hiện các thao tác tương tự đối với bản tin đến, sử dụng cùng một khóa bí mật, để tạo một giá trị MAC mới

Chương 4: Các giải thuật toàn vẹn dữ liệu

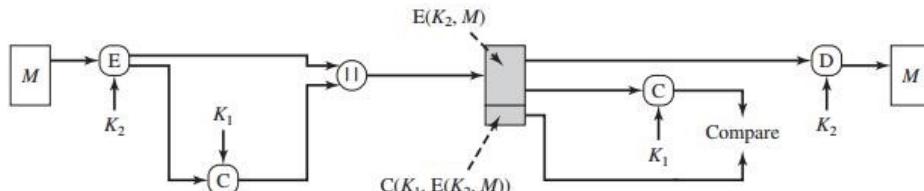
Mã xác thực bản tin



(a) Message authentication



(b) Message authentication and confidentiality; authentication tied to plaintext



(c) Message authentication and confidentiality; authentication tied to ciphertext

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã xác thực bản tin

Nếu ta giả sử chỉ có duy nhất bên nhận và bên gửi biết khóa chia sẻ, và MAC nhận được khớp với MAC được tính, khi đó:

1. Bên nhận được đảm bảo rằng bản tin đã không bị thay đổi. Nếu một kẻ tấn công thay đổi bản tin nhưng không thay đổi MAC, khi đó giá trị MAC được bên nhận tính lại sẽ không khớp với MAC nhận được. Bởi vì kẻ tấn công được giả thiết rằng không biết khóa bí mật, kẻ tấn công không thể thay đổi giá trị MAC tương ứng với sự thay đổi trong bản tin.
2. Bên nhận được đảm bảo rằng bản tin đến từ đúng người gửi. Bởi vì không ai khác biết được khóa chia sẻ, không ai khác có thể tạo một bản tin với MAC đúng.
3. Nếu bản tin bao gồm một số thứ tự (như được sử dụng trong HDLC, X.25, và TCP), khi đó người nhận có thể được đảm bảo số thứ tự đó là đúng bởi vì một kẻ tấn công không thể thay đổi được số thứ tự.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã xác thực bản tin

Một điểm khác biệt với mã hóa là thuật toán MAC cần phải đảm bảo không thể nghịch đảo, vì nó phải dùng cho giải mã.

Tổng quát, hàm MAC là hàm nhiều-tới-một. Miền của hàm bao gồm các bản tin có độ dài tùy ý, trong khi khoảng giá trị bao gồm tất cả các MAC có thể và tất cả các khóa có thể.

Nếu một giá trị MAC n -bit được sử dụng, khi đó có 2^n giá trị MAC có thể xảy ra, trong khi có N bản tin có thể có với $N >> 2^n$. Hơn nữa, với một khóa k bit có thể có 2^k khóa khác nhau.

$$T = \text{MAC}(K, M)$$

M là bản tin có độ dài thay đổi; K là khóa bí mật; $\text{MAC}(K, M)$ là ký hiệu nhận thực có chiều dài cố định (nhãn). Nhãn được thêm vào bản tin ở nguồn tại thời điểm mà bản tin được đảm bảo hoặc được xem là đúng. Bên nhận nhận thực bản tin này bằng cách tính lại nhãn.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã xác thực bản tin

Có các tình huống trong đó mã xác thực bản tin được sử dụng:

1. Có một số các ứng dụng trong đó cùng một bản tin được phát quảng bá tới một số lượng các điểm đích. Do vậy, bản tin phải được quảng bá dưới dạng bản rõ với một mã xác thực bản tin đi kèm. Hệ thống chịu trách nhiệm sở hữu khóa bí mật và thực hiện nhận thực.
2. Kịch bản khác cần đến nhận thực là khi có một trao đổi trong đó một bên có chịu tải nặng và không đủ thời gian để giải mã tất cả các bản tin đến. Việc chứng thực được thực hiện dựa trên một số cơ sở được chọn lọc, các bản tin được chọn ngẫu nhiên để kiểm tra.
3. Nhận thực một chương trình máy tính dưới dạng bản rõ cho phép thực hiện nhanh các tiến trình. Nếu một mã xác thực bản tin được đính kèm vào chương trình, nó có thể được kiểm tra khi có yêu cầu về tính toàn vẹn của chương trình.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã xác thực bản tin

Tính an toàn của MAC

1. Các tấn công vét cạn

Một tấn công vét cạn đối với MAC khó thực hiện hơn so với tấn công vét cạn vào hàm băm bởi vì nó yêu cầu biết trước các cặp bản tin-nhãn.

Kẻ tấn công muốn khám phá mã MAC có hiệu lực đối với bản tin x cho trước. Có hai loại tấn công có thể xảy ra: tấn công không gian khóa và tấn công giá trị MAC.

a, Nếu một kẻ tấn công có thể xác định khóa MAC, khi đó hắn có thể tạo một giá trị MAC hợp lệ đối với bất kỳ đầu vào x nào.

b, Một kẻ tấn công cũng có thể tập trung vào nhãn mà không cần tạo lại khóa. Ở đây, mục tiêu là tạo ra nhãn hợp lệ đối với bản tin cho trước hoặc tìm ra một bản tin khớp với nhãn cho trước.

Nỗ lực đối với tấn công vét cạn vào thuật toán MAC có thể được tính bằng $\min(2^k, 2^n)$.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã xác thực bản tin

Tính an toàn của MAC

1. Phân tích mã

Các tấn công phân tích mã đối với MAC tìm kiếm để khai thác đặc tính nào đó của thuật toán để thực hiện một tấn công nào đó được cho là phổ biến hơn là tìm kiếm vét cạn.

Có nhiều biến thể trong cấu trúc của MAC hơn so với trong các hàm băm, do vậy việc tổng quát hóa các tấn công phân tích mã đối với MAC sẽ là khó khăn hơn.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã xác thực bản tin dựa trên hàm băm

Mục tiêu thiết kế sau đây của HMAC

- Để sử dụng mà không cần sửa đổi các hàm băm có sẵn. Đặc biệt, để sử dụng các hàm băm thực hiện tốt trong phần mềm và mã chương trình là miễn phí và phổ biến.
- Để cho phép khả năng thay thế các hàm băm được nhúng nếu các hàm băm khác nhanh hơn hoặc bảo mật hơn được tìm ra hoặc yêu cầu.
- Để kế thừa hiệu năng ban đầu của hàm băm mà không gây ra sự suy giảm đáng kể.
- Để sử dụng và xử lý khóa theo một cách đơn giản.
- Để có được các phân tích mã hóa dễ hiểu về độ mạnh của cơ chế nhận thực dựa trên các giả thiết hợp lý về hàm băm được nhúng.

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã xác thực bản tin dựa trên hàm băm

Nguyên tắc hoạt động của HMAC

H = hàm băm được nhúng (ví dụ MD5, SHA-1, RIPEMD-160)

IV = giá trị khởi tạo đầu vào của hàm băm

M = bản tin đầu vào cho HMAC (bao gồm phần đệm xác định trong hàm băm được nhúng)

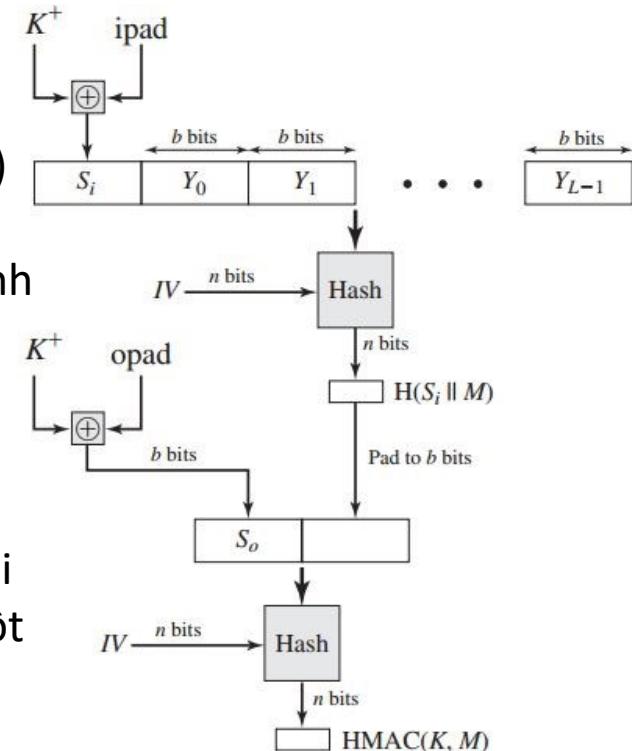
Y_i , block thứ i của M, $0 \leq i \leq (L - 1)$

L = số block trong M; b = số bit trong một block

n = chiều dài mã băm được tạo bởi hàm băm được nhúng

K = khóa bí mật; chiều dài được đề xuất $\geq n$; nếu chiều dài khóa lớn hơn b, khóa là đầu vào của hàm băm để tạo ra một khóa n bit

K^+ = K bit được đếm vào phía trái để được chiều dài b bit



Ipad = 00110110 (36 trong hệ hexa); Opad = 01011100 (5C trong hệ hexa)

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã xác thực bản tin dựa trên hàm băm

Độ an toàn của HMAC

An ninh của một hàm HMAC được biểu diễn tổng quát theo xác suất giả mạo thành công với cùng khoảng thời gian cho trước và số cặp bản tin-mã cho trước được tạo với cùng một khóa.

Xác suất tấn công vào HMAC thành công tương đương với một trong các tấn công sau đây vào hàm băm được nhúng:

Kẻ tấn công có khả năng tính toán một đầu ra của hàm nén ngay cả với một IV ngẫu nhiên, bí mật và kẻ tấn công không biết trước. 2^n

Kẻ tấn công tìm các xung đột trong hàm băm ngay cả khi IV là ngẫu nhiên và bí mật. $H(M) = H(M') - \text{Tấn công ngày sinh. } 2^{n/2}$

Chương 4: Các giải thuật toàn vẹn dữ liệu

Mã hóa xác thực (Authenticated Encryption)

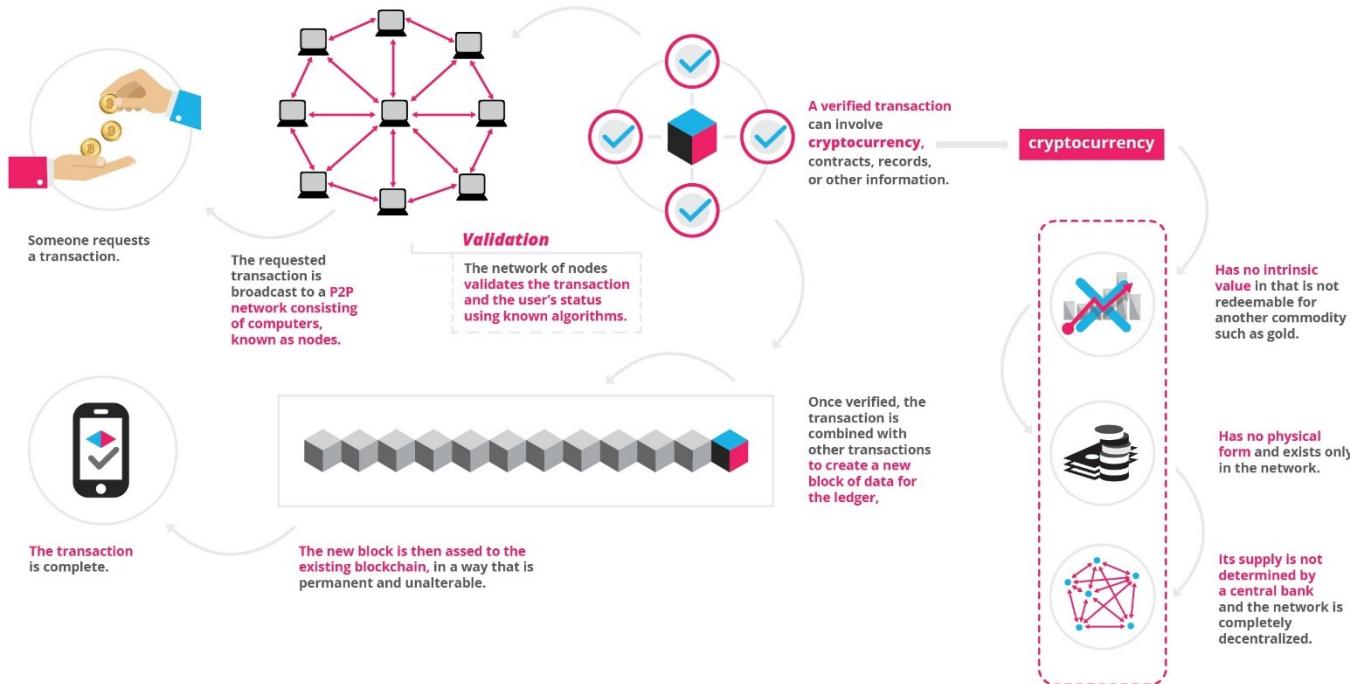
- Mã hóa sau khi Băm (H > E): Đầu tiên tính toán mã hàm băm trên bản tin M bằng $h=H(M)$. Sau đó thực hiện mã hóa bản tin đã được thêm hàm băm: $E(K,(M \parallel h))$
- Mã hóa sau sau khi xác thực (A > E): Sử dụng hai khóa. Đầu tiên nhận thực bản rõ bằng tính toán giá trị MAC bởi $T = \text{MAC}(K_1, M)$. Sau đó mã hóa bản tin được thêm mã xác thực bản tin: $E(K_2, [M \parallel T])$

Tiếp cận này được thực hiện bởi các giao thức SSL/TLS.

- Nhận thực sau khi mã hóa (E > A): Sử dụng hai khóa. Đầu tiên mã hóa bản tin thành bản mã . Sau đó xác thực bản mã với để tạo thành cặp . Tiếp cận này được sử dụng trong giao thức IPSec.
- Độc lập mã hóa và nhận thực (E + A): Sử dụng hai khóa. Mã hóa bản tin thành bản mã . Xác thực bản rõ với để tạo thành cặp . Hoạt động này có thể được thực hiện độc lập và được ứng dụng trong giao thức SSH.

Khái quát Bitcoin và blockchain

Lược đồ tổng quát



Khái quát Bitcoin và blockchain

Lược đồ tổng quát

- 1998, W. Dai viết một bài ngắn có tên là “b-money”. 2008 Satoshi Nakamoto viết một bài khác với tựa đề “Bitcoin: A Peer-to-Peer Electronic Cash System” (<https://bitcoin.org/bitcoin.pdf>) “chuyển khoản” trực tiếp cho nhau mà không cần trung gian. Việc định danh sử dụng phương pháp Private - Public Key.

Thách thức lớn nhất là làm thế nào để giải quyết vấn đề “double spending”: tất cả các bên tham gia đều có sổ cái (ledger) ghi lại toàn bộ các giao dịch.

Blockchain: Satoshi Nakamoto đưa ra một ý tưởng mới gọi là block chain

Các khối này liên kết với nhau theo trực thời gian: cứ khoảng 10 phút sinh ra một khối mới. Khối sau được sinh ra liên kết với tất cả các khối trước đó theo một quy tắc nhất định. Tất cả các giao dịch mới đều được đặt vào khối mới phát sinh này. Chúng ta sẽ thấy rằng khối mới được sinh ra là kết quả của cuộc cạnh tranh “khốc liệt” giữa các nút.

Khái quát Bitcoin và blockchain

Lược đồ tổng quát

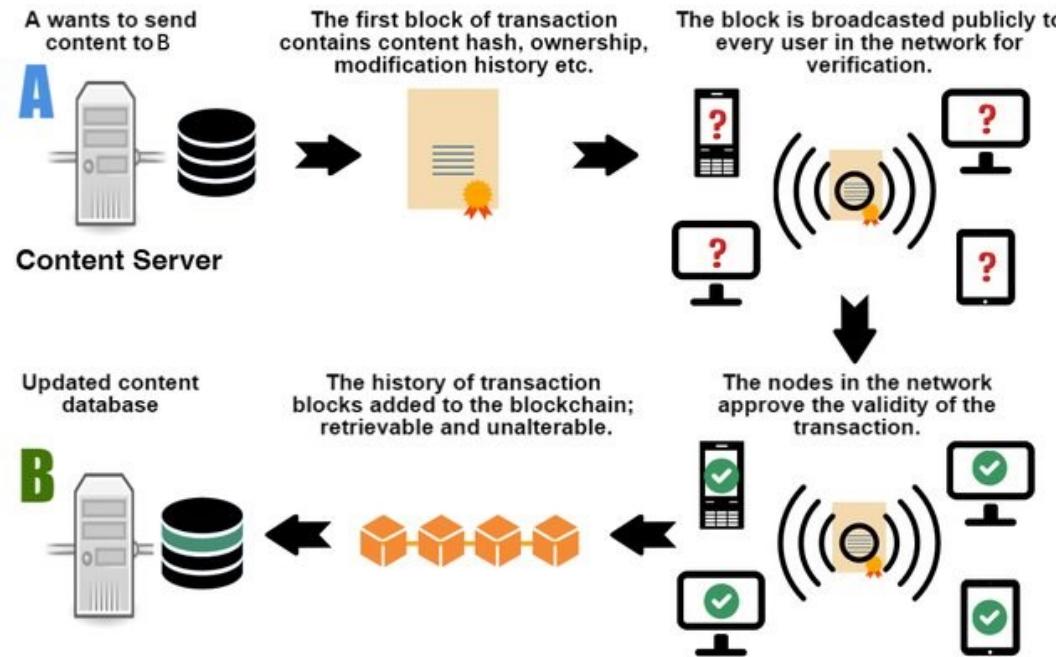
- Vấn đề phát hành bitcoin: đúc tiền ảo, mining.

Satoshi Nakamoto quy định là người tìm ra khối mới sẽ được “thưởng” một lượng tiền ảo nhất định. Trong thời gian 4 năm đầu tiên, mỗi một khối mới được thưởng 50 bitcoins. Bốn năm tiếp theo lượng thưởng giảm đi một nửa: 25 bitcoins, bốn năm tiếp theo sau giảm đi tiếp một nửa, chỉ còn 12.5 bitcoins, ... Với quy tắc này thì số bitcoins không bao giờ vượt qua 21 triệu

Trong blockchain, Satoshi Nakamoto dùng phương pháp mã hashcash. Phương pháp này độc đáo ở chỗ: khối sau là kết quả “băm” của tổ hợp của khối ngay phía trước và một số có tên gọi là nonce. Kết quả băm này phải nhỏ hơn một “ngưỡng” nào đấy. Thực chất của việc này là tăng dần số nonce, thực hiện hàm băm và xem xem kết quả đã nhỏ hơn ngưỡng chưa. Satoshi Nakamoto gọi quá trình là proof-of-work (tạm dịch: chứng minh nỗ lực). Khi chạy trong thực tế các nút phải cạnh tranh xem ai là người đầu tiên tìm ra kết quả băm theo quy định.

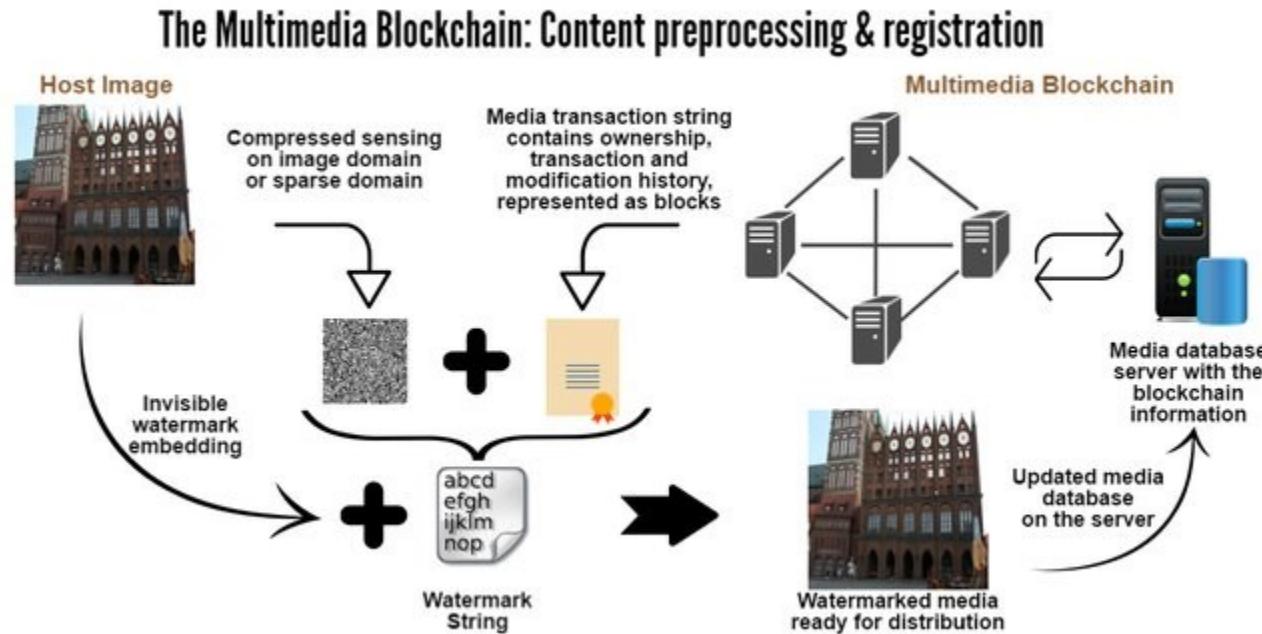
Khái quát Bitcoin và blockchain

Lược đồ tổng quát



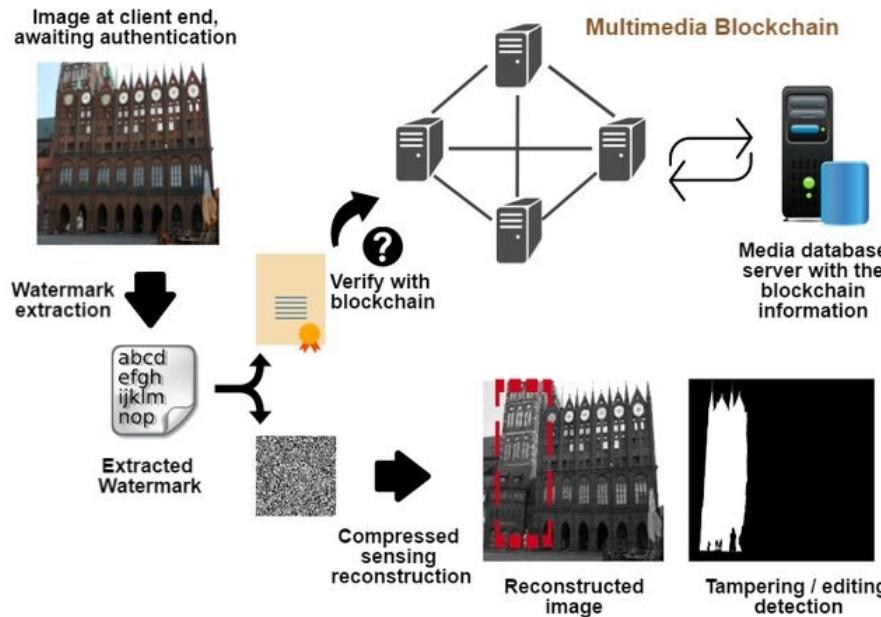
Khái quát Bitcoin và blockchain

Lược đồ tổng quát



Khái quát Bitcoin và blockchain

Lược đồ tổng quát

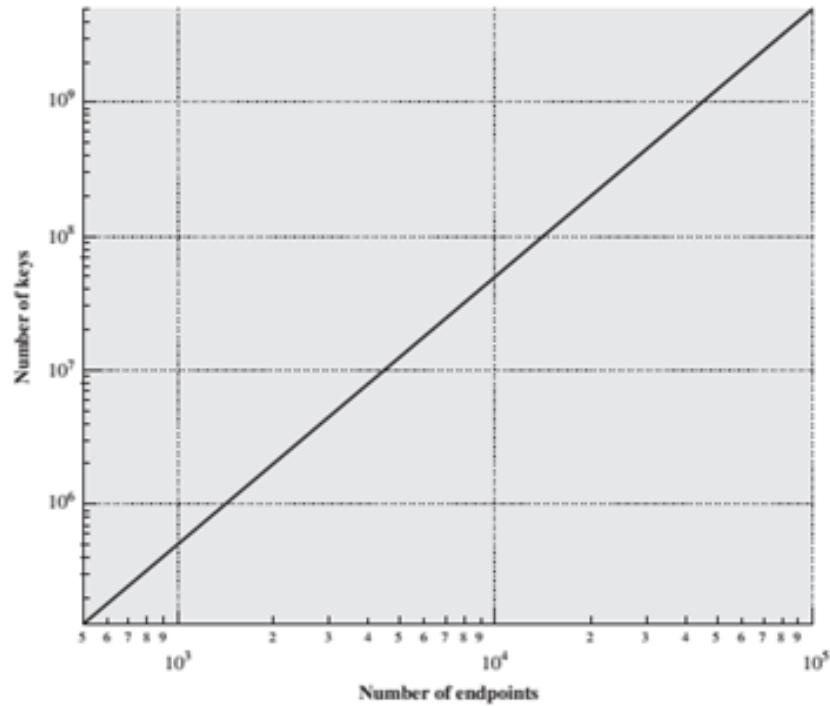


Chương 5: Xác thực

Quản lý và phân phối khóa

Các kịch bản phân phối khóa

1. A lựa chọn một khóa và chuyển phát tới B.
2. Một thành viên thứ 3 lựa chọn khóa và chuyển phát tới A và B.
3. Nếu A và B cùng sử dụng một khóa trước đó, một thành viên có thể chuyển một khóa mới dựa trên việc mã hóa khóa cũ.
4. Nếu A và B có một kết nối mã hóa với một thành viên C, C có thể chuyển phát khóa cho cả A và B.

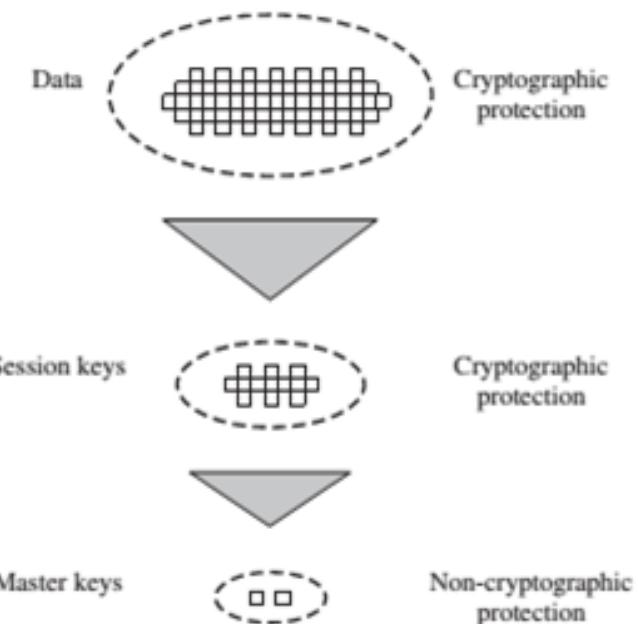


Chương 5: Xác thực

Quản lý và phân phối khóa

Các kịch bản phân phối khóa

Trong lược đồ này, một trung tâm phân phối khóa chịu trách nhiệm phân phối khóa cho các cặp người dùng (máy chủ, các quy trình, các ứng dụng) khi cần thiết. Mỗi người dùng phải chia sẻ một khóa duy nhất với các trung tâm phân phối khóa

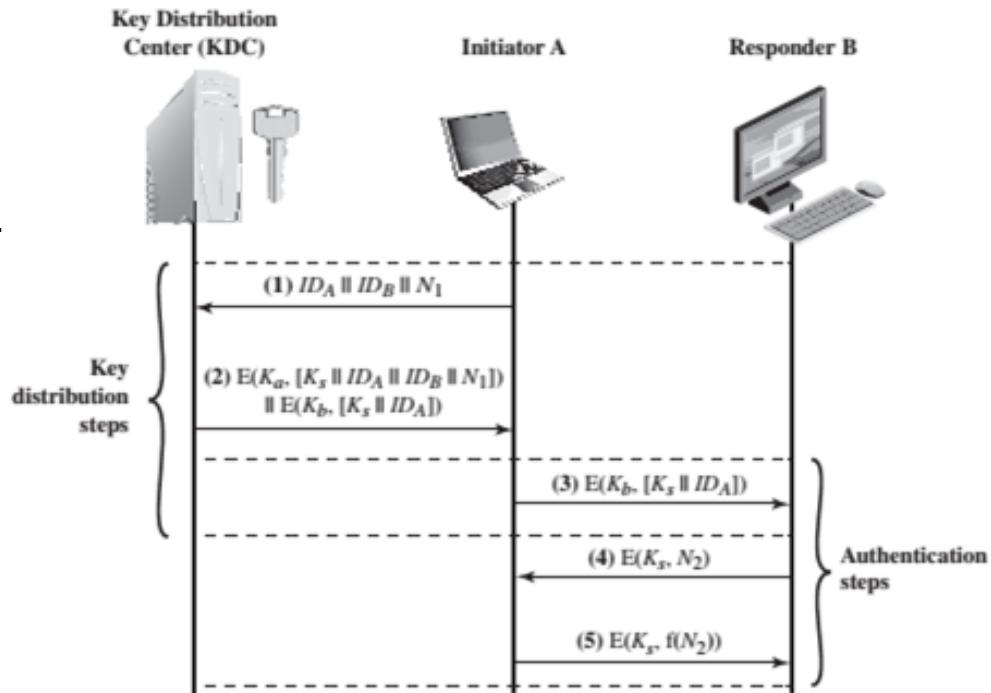


Chương 5: Xác thực

Quản lý và phân phối khóa

Trung tâm phân phối khóa

Giả thiết mỗi người dùng chia sẻ một khóa chủ duy nhất với trung tâm phân phối khóa KDC (Key Distribution Center).

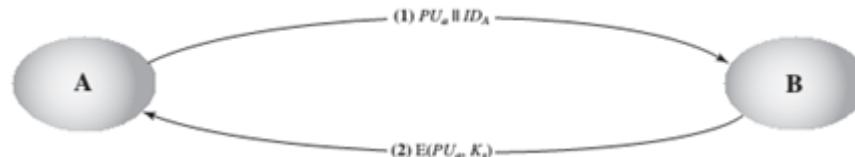


Chương 5: Xác thực

Quản lý và phân phối khóa

Phân phối khóa đối xứng bằng mật mã hóa bất đối xứng

Lược đồ đơn giản (Merkle)



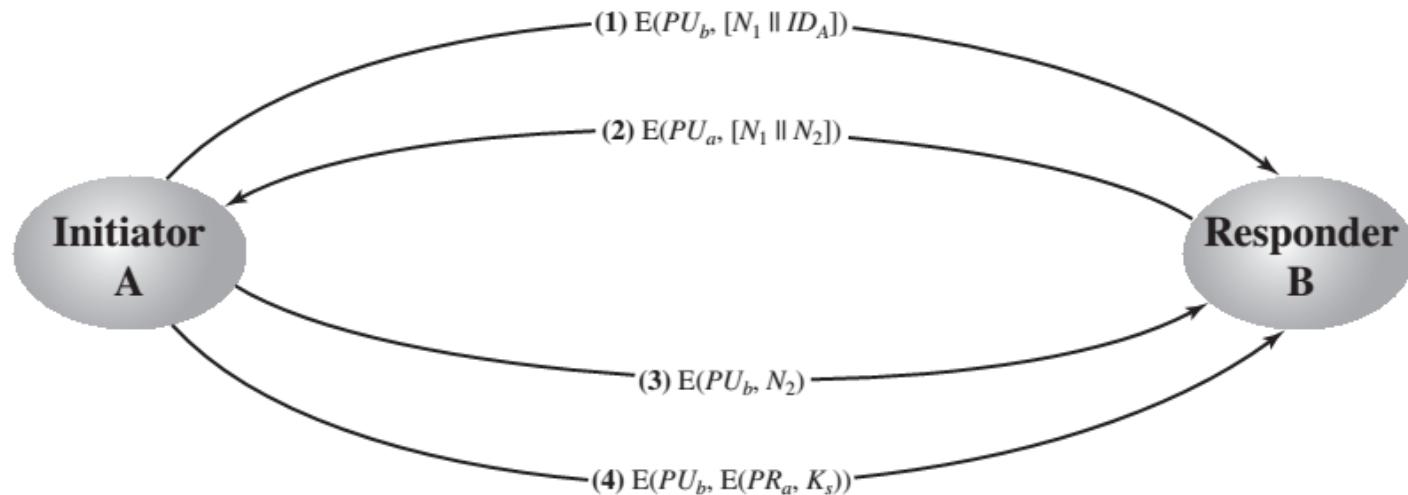
1. Tạo ra một cặp khóa công khai / riêng $\{PU_a, PR_a\}$ và phát đi một bản tin tới B gồm PUa và định danh của A, IDA.
2. B tạo ra một khóa bí mật K_s và truyền nó cho A, được mã hóa với khóa công khai của A.
3. A tính D (PR_a , $E(PU_a, K_s)$) để khôi phục lại các khóa bí mật. Bởi vì chỉ có A có thể giải mã bản tin, chỉ có A và B sẽ biết nhận dạng của K_s .
4. A loại bỏ PU_a và PR_a và B loại bỏ PU_a .

Chương 5: Xác thực

Quản lý và phân phối khóa

Phân phối khóa đối xứng bằng mật mã hóa bất đối xứng

Phân phối khóa bí mật với nhận thực và bảo mật



Chương 5: Xác thực

Quản lý và phân phối khóa

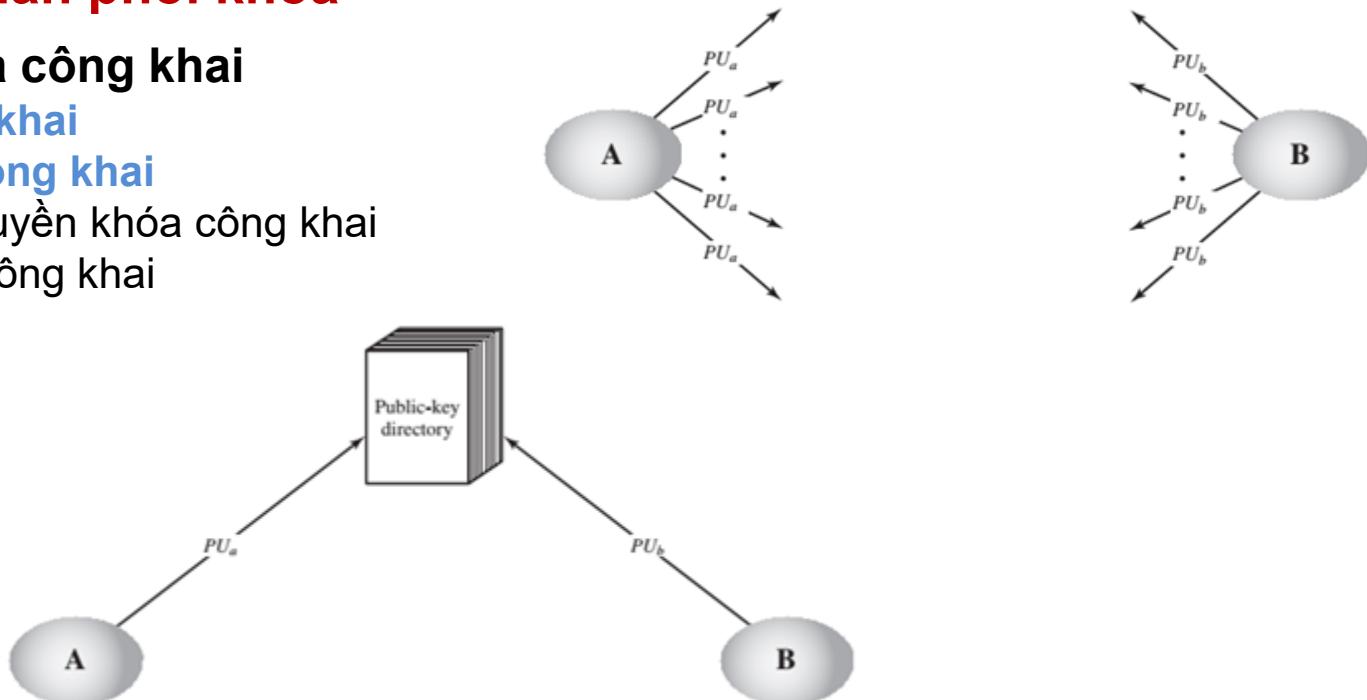
Phân phối khóa công khai

Thông báo công khai

Thư mục khóa công khai

Trung tâm thẩm quyền khóa công khai

Chứng thư khóa công khai



Chương 5: Xác thực

Quản lý và phân phối khóa

Phân phối khóa công khai

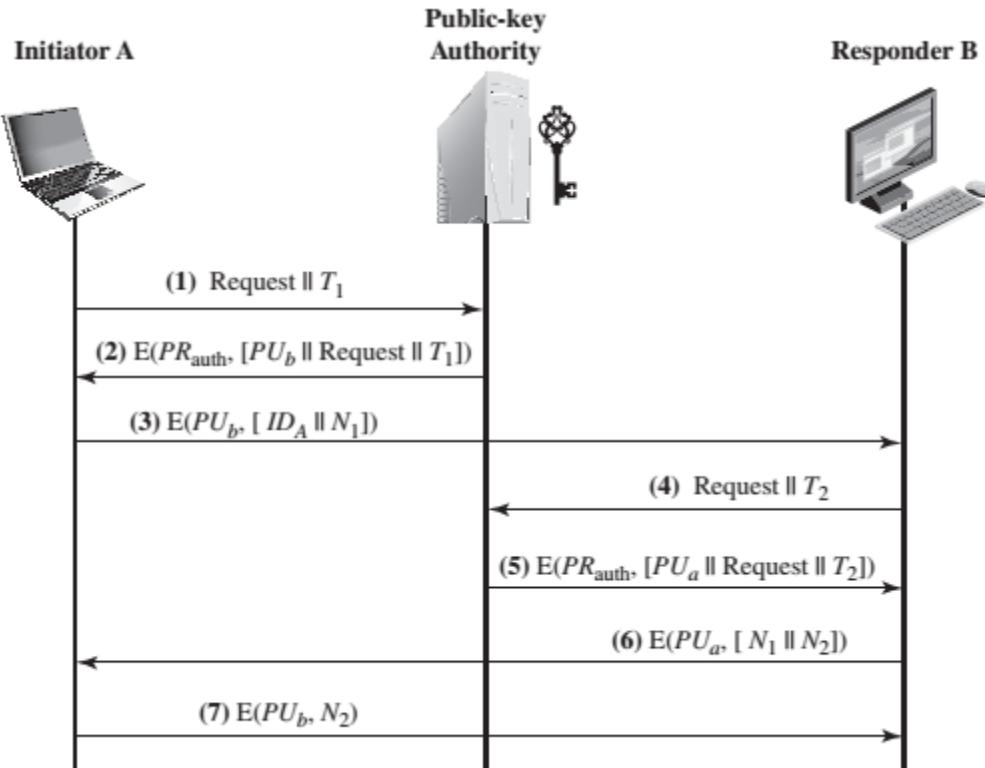
Thông báo công khai

Thư mục khóa công khai

Trung tâm thẩm quyền khóa công khai

Chứng thư khóa công khai

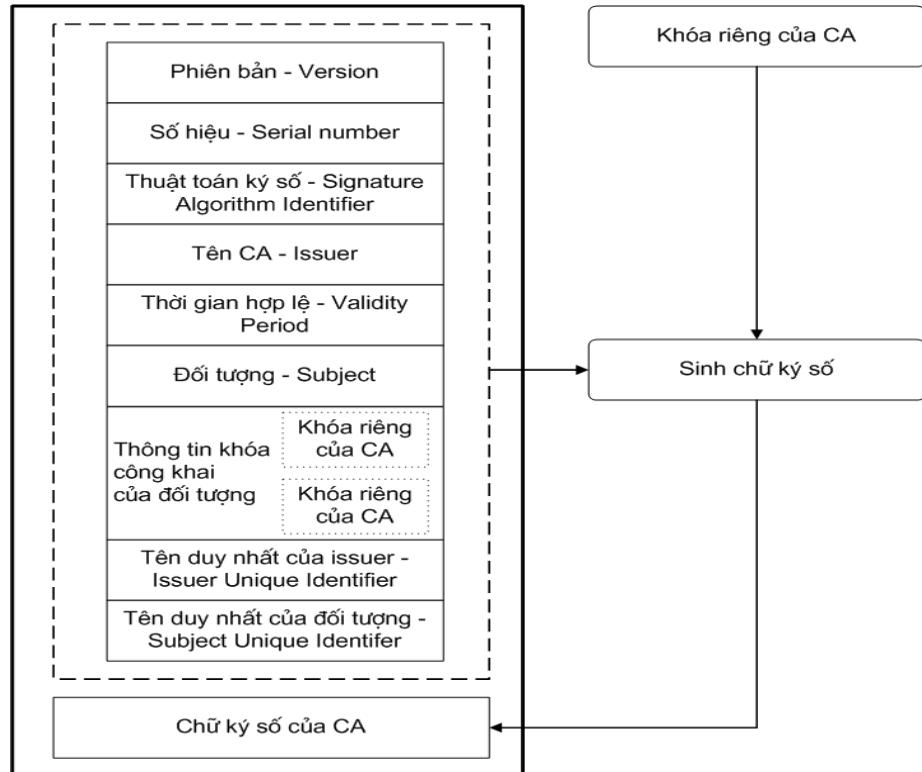
Về bản chất, một giấy chứng thư bao gồm một khóa công khai, một nhận dạng của chủ sở hữu chính và toàn bộ khối chữ ký của một bên thứ ba đáng tin cậy.



Chương 5: Xác thực

Chứng chỉ X.509

X.509 v1 và X.509 v2



Chương 5: Xác thực

Chứng chỉ X.509

X.509 v3

Đối tượng có thể có các chứng chỉ khác nhau với các khóa công khai khác nhau và giả thiết rằng các cặp khóa cần được cập nhật định kỳ, do vậy cần phải có cách để phân biệt các chứng chỉ khác nhau của đối tượng này một cách dễ dàng.

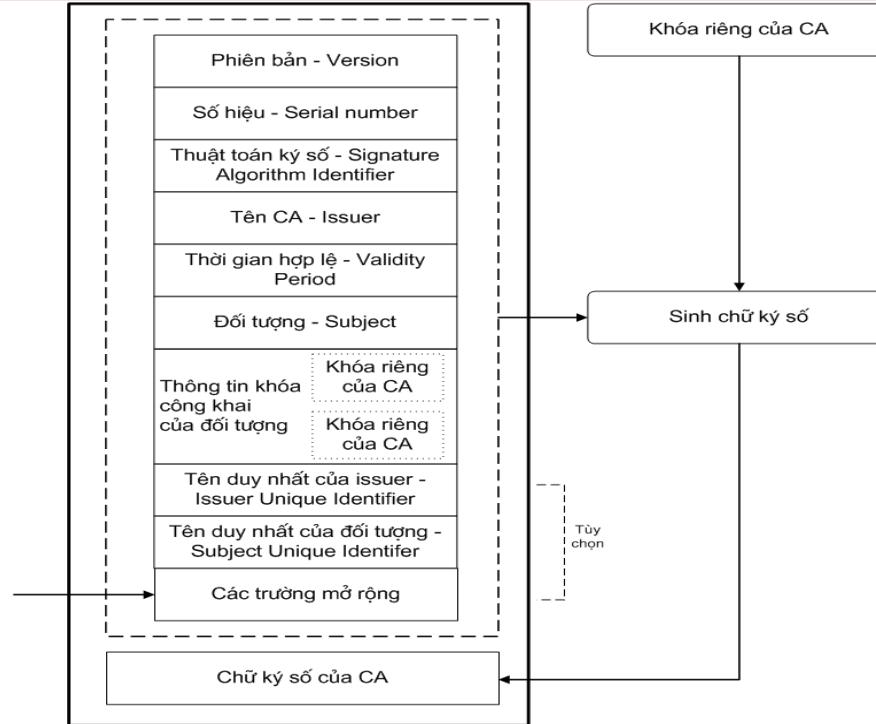
Một tên đối tượng trở thành tên duy nhất nhưng nó không có đủ thông tin cho những người sử dụng chứng chỉ khác nhận dạng đối tượng, do đó cần có thêm thông tin nhận dạng đối tượng.

Một số các ứng dụng cần nhận dạng những người sử dụng thông qua các dạng tên xác định ứng dụng. Ví dụ: trong an toàn thư tín điện tử; trong việc gắn kết một khóa công khai với một địa chỉ thư tín điện tử.

Chương 5: Xác thực

Chứng chỉ X.509

X.509 v3



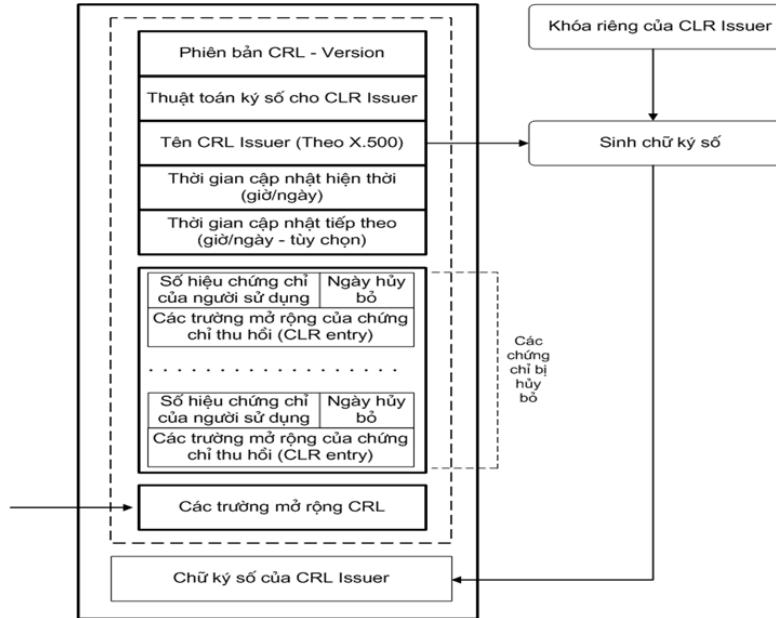
Định dạng trường mở rộng

Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị
Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị
Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị

Chương 5: Xác thực

Chứng chỉ X.509

Thu hồi chứng chỉ



Định dạng trường mở rộng

Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị
Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị
Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị

Chương 5: Xác thực

Chứng chỉ X.509

Xác thực người sử dụng

Có bốn phương tiện tổng quát đối với danh tính người dùng có thể được sử dụng độc lập hay kết hợp.

Một vài điều chỉ người dùng bên biết: Ví dụ như mật khẩu, một số nhận dạng cá nhân (Personal Identification Number - PIN) hoặc các câu trả lời đối với một tập câu hỏi được sắp xếp trước.

Một vài điều cá nhân sở hữu: Ví dụ như các khóa mật mã, các thẻ khóa điện, các thẻ thông minh và các thẻ vật lý. Loại phương tiện nhận thực này được xem như một dấu hiệu.

Một vài điều thuộc về bản chất người dùng (các tham số sinh trắc học tĩnh): Ví dụ bao gồm sự nhận dạng bằng vân tay, võng mạc và khuôn mặt.

Một vài điều người dùng làm (các tham số sinh trắc học động): Các ví dụ bao gồm sự nhận dạng bằng mẫu giọng nói, các đặc tính chữ viết tay và nhịp gõ.

Chương 5: Xác thực

Xác thực người sử dụng

Xác thực lẫn nhau

Các khóa bí mật K_a và K_b được chia sẻ
tương ứng giữa A với KDC và B với KDC.

Phân phối một cách an toàn khóa phiên K_s tới A và B.

Bản tin trong bước 3 có thể được giải mã, và chỉ B mới có thể hiểu được.

Bước 4 B gửi lại K_s cho A, và bước 5 A đảm bảo khóa K_s cho B, và đảm bảo với B rằng đây là
bản tin mới vì sử dụng N_2 .

Mục đích của bước 4 và 5 là để ngăn chặn một số loại tấn công phát lại.

1. A -> KDC: $ID_A \parallel ID_B \parallel N_1$
2. KDC -> A: $E(K_a, [K_s \parallel ID_B \parallel N_1 \parallel E(K_b, [K_s \parallel ID_A])])$
3. A -> B: $E(K_b, [K_s \parallel ID_A])$
4. B -> A: $E(K_s, N_2)$
5. A -> B: $E(K_s, f(N_2))$

Chương 5: Xác thực

Xác thực người sử dụng

Xác thực lẫn nhau

Các khóa bí mật K_a và K_b được chia sẻ
tương ứng giữa A với KDC và B với KDC.

Phân phối một cách an toàn khóa phiên K_s tới A và B.

Bản tin trong bước 3 có thể được giải mã, và chỉ B mới có thể hiểu được.

Bước 4 B gửi lại K_s cho A, và bước 5 A đảm bảo khóa K_s cho B, và đảm bảo với B rằng đây là
bản tin mới vì sử dụng N_2 .

Mục đích của bước 4 và 5 là để ngăn chặn một số loại tấn công phát lại.

KIỂM TRA BÀI 2

Câu hỏi

Trình bày các đặc trưng của HMAC.

Yêu cầu làm bài

1. Trình bày trên giấy A4.

2. Trang đầu tiên kẹp thẻ sinh viên vào góc trên ngoài cùng bên phải, chụp ảnh cùng bài.

3. Lưu tên và gửi lên drive theo định dạng sau:

số thứ tự. Họ và tên. Nhóm lớp. Bai2. pdf

Ví dụ.

12.MinhHT.nhom2.bai2.pdf

4. ghi tổng số tờ làm bài trên trang đầu

5. Các bạn ký ở trang cuối cùng

