


An toàn và An ninh thông tin Mạng

PGS. Nguyễn Linh Giang
Bộ môn Truyền thông và
Mạng máy tính



Nội dung

- I. Nhập môn An toàn thông tin mạng
- II. Đảm bảo tính mật
 - I. Các hệ mật khóa đối xứng (mã hóa đối xứng)
 - II. Các hệ mật khóa công khai (mã hóa bất đối xứng)
- III. Bài toán xác thực
 - I. Cơ sở bài toán xác thực
 - II. Xác thực thông điệp
 - III. Chữ ký số và các giao thức xác thực
 - IV. Các cơ chế xác thực trong các hệ phân tán
- IV. Bảo vệ các dịch vụ Internet
- V. An toàn an ninh hệ thống
 - I. FireWall và Proxy
 - II. Hệ thống phát hiện và ngăn chặn xâm nhập (IDS)
 - III. Lỗ hổng hệ thống
 - IV. Case study Windows NT và Linux
 - V. Virus máy tính

Nội dung

- Tài liệu môn học:
 - W. Stallings “Networks and Internetwork security”
 - W. Stallings “Cryptography and network security”
 - Introduction to Cryptography – PGP
 - D. Stinson – Cryptography: Theory and Practice

Các chủ đề tiểu luận

- 1. Các hệ mật khóa công khai.
 - Cơ sở xây dựng hệ mật khóa công khai
 - Các hệ mật khóa công khai.
 - Các sơ đồ ứng dụng.
- 2. Hạ tầng khóa công khai PKI
 - Cấu trúc hạ tầng khóa công khai.
 - Chứng chỉ số, các chuẩn;
 - Triển khai thực tế. Các ứng dụng trong các giao dịch.
 - Các hệ thống mã nguồn mở.

Các chủ đề tiểu luận

- 3. Bảo mật cho mạng IP. IPSec. Mạng riêng ảo VPN. Ứng dụng.
- 4. Bài toán xác thực thông điệp.
 - Các cơ chế xác thực
 - Hàm băm và hàm mã hóa xác thực.
 - Các giao thức xác thực.
- 5. Chữ ký số.
 - Các cơ chế tạo chữ ký số. Giao thức chữ ký số.
 - Các dịch vụ chữ ký số.
 - Chữ ký mù.
 - Ứng dụng.

Các chủ đề tiểu luận

- 6. Phát hiện xâm nhập mạng.
 - Các cơ chế phát hiện xâm nhập mạng.
 - Phát hiện theo dấu hiệu
 - Phát hiện theo bất thường
 - Phân tích các đặc trưng thống kê của mạng.
 - Ứng dụng.
- 7. Bảo mật cho mạng không dây. Phân tích các đặc trưng thống kê của các dạng tấn công từ chối dịch vụ. Xác thực và bảo mật trong mạng không dây. Phát hiện bất thường trong mạng không dây.

Các chủ đề tiểu luận

- 8. Bảo mật hệ thống, bảo mật mạng. Các chính sách, các chuẩn. Phân tích đối với Windows và Unix-Linux. Các chính sách an ninh mạng cho mạng Cisco.
- 9. Bảo vệ dữ liệu đa phương tiện trong quá trình phân phối qua hệ thống mạng mở. Vấn đề bảo mật, bảo vệ bản quyền và kiểm soát sử dụng dữ liệu đa phương tiện.

Các chủ đề tiểu luận

- 10. Bảo mật cho web services;
- 11. Đăng nhập 1 lần với GSS-API;
- 12. Xác thực Kerberos;
- 13. SSL và TLS;
- 14. IPSecurity;
- 15. Xác thực X509

Các chủ đề tiểu luận

- 16. Hạ tầng khóa công khai PKI
- 17. PGP và bảo mật thư tín điện tử
- 18. S/MIME
- 19. Secure electronic transaction
- 20. Firewall, các kiến trúc;
- 21. Proxy, thiết kế và xây dựng proxy;

Các chủ đề tiểu luận

- 22. Các hệ thống phát hiện xâm nhập dựa trên dấu hiệu;
- 23. Các hệ thống phát hiện xâm nhập dựa trên bất thường;
- 24. Bảo mật mạng LAN không dây;
- 25. Các dạng tấn công vào mạng sensor.
- 26. Các dạng tấn công từ chối dịch vụ;
- 27. Tấn công SQL Injection, phát hiện và tìm kiếm lỗi SQL Injection;
- 28. Phát hiện tấn công quét cổng;
- 29. Các phương pháp, quy trình phát hiện lỗ hổng hệ thống.
- 30. Các mô hình tiền điện tử trong giao dịch điện tử.

Đánh giá

- Giữa kỳ và quá trình: 30%
 - Điểm danh: 1/3.
- Thi hết môn: 70%
- Liên hệ giáo viên:
- giangnl@soict.hust.edu.vn; số Bộ môn: 024-38682596; mobile: 0984933165

Chương I. Nhập môn

1. Nhập môn
2. Các dịch vụ, cơ chế an toàn an ninh thông tin và các dạng tấn công vào hệ thống mạng
3. Các dạng tấn công
4. Các dịch vụ an toàn an ninh
5. Các mô hình an toàn an ninh mạng

Nhập môn

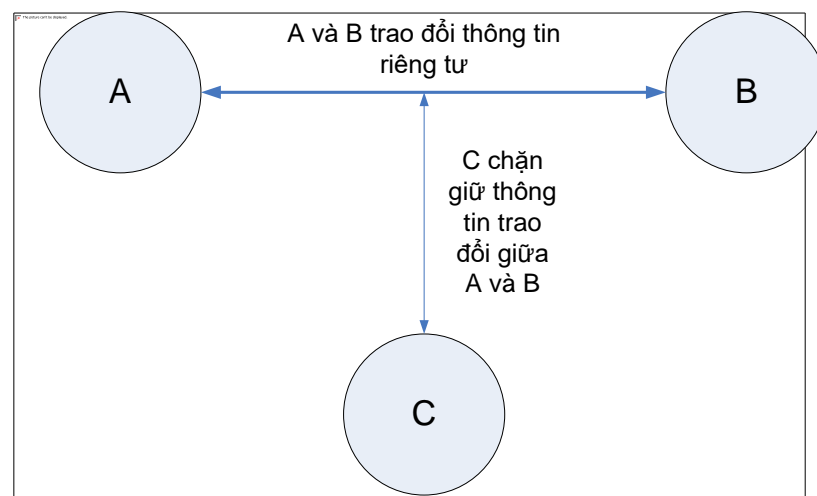
- Bối cảnh bảo mật thông tin:
 - Trước khi xuất hiện máy tính: Bảo vệ thông tin, tài liệu:
 - Các cơ chế bảo vệ;
 - Khoá kho hồ sơ lưu trữ văn bản.
 - Khi xuất hiện máy tính - bảo vệ thông tin điện tử:
 - Sao chép thông tin dễ dàng
 - Cần thiết có các công cụ tự động để bảo mật các tệp, các dạng thông tin chứa trong máy tính.
 - Đặc biệt khi hệ thống được chia sẻ tài nguyên trên mạng.
Vấn đề **Computer Security**.

Nhập môn

- Khi xuất hiện các hệ phân tán và sử dụng mạng để truyền dữ liệu và trao đổi thông tin: Bảo vệ thông tin, dữ liệu truyền trên mạng
 - Truyền dữ liệu giữa người sử dụng và máy tính,
 - Giữa máy tính và máy tính.
 - Nhu cầu bảo vệ các dữ liệu trong khi truyền → **Network Security**.
- Không có ranh giới rõ rệt giữa Computer Security và Network Security.
- Chương trình tập trung vào: an toàn thông tin liên mạng: internetwork security.

Nhập môn

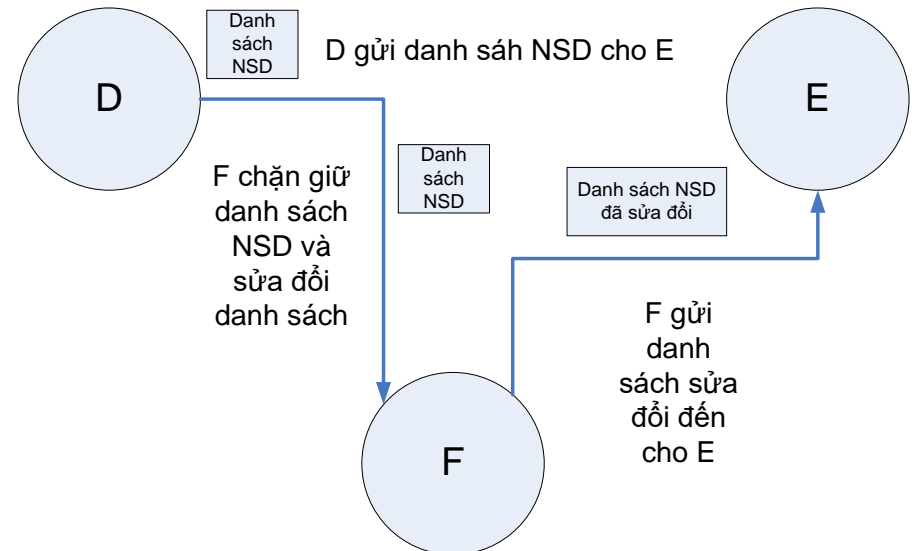
- Một số ví dụ về vấn đề bảo vệ an toàn thông tin:
 - Truyền file:
 - A truyền file cho B;
 - Trong file chứa những thông tin bí mật;
 - C không được phép đọc file nhưng có thể theo dõi được quá trình truyền file và sao chép file trong quá trình truyền.



Nhập môn

- Trao đổi thông điệp:

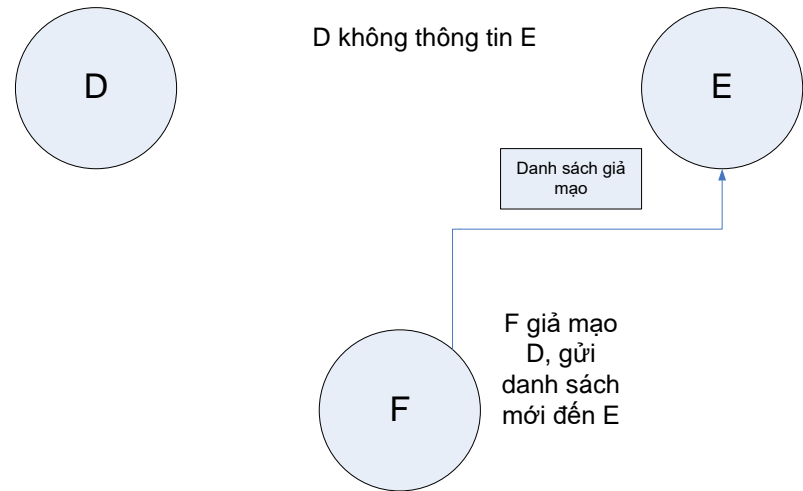
- Quản trị mạng D gửi thông điệp đến máy tính chịu sự quản trị E;
- Thông điệp chứa những thông tin về danh sách những người sử dụng mới.
- Người sử dụng F bắt thông điệp;
- F thêm các user mới vào nội dung thông điệp, rồi gửi tiếp cho E;
- E nhận thông điệp, không biết là đã bị F thay đổi, vẫn tưởng là do D gửi tới và thay đổi danh sách user của mình.



Nhập môn

- Giả mạo:

- Kịch bản giống trường hợp trước;
- F tạo một thông điệp của riêng mình, chứa những thông tin riêng có lợi cho F và gửi cho E.
- E nhận được thông tin từ F, cho rằng thông tin đó do D gửi và cập nhật những thông tin giả mạo vào CSDL



Nhập môn

- Sự phức tạp trong bài toán Bảo mật liên mạng:
 - Không tồn tại phương pháp thích hợp cho mọi trường hợp.
 - Các cơ chế bảo mật luôn đi đôi với các biện pháp đối phó.
 - Lựa chọn những giải pháp thích hợp với từng ngữ cảnh sử dụng.

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Mục tiêu:

- Đánh giá được những nhu cầu về an toàn của tổ chức một cách hiệu quả;
- Xác định và lựa chọn những sản phẩm và chính sách an ninh,

cần có:

- Những phương pháp có tính hệ thống làm cơ sở để xác định những yêu cầu an toàn an ninh mạng;
- Đặc tả được những cách tiếp cận thỏa mãn những yêu cầu đó.
- Một trong những phương hướng là khảo sát ba khía cạnh của an toàn an ninh thông tin.

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Ba khía cạnh an toàn an ninh thông tin:
 - Tấn công vào an ninh thông tin
 - Mọi tác động làm giảm mức độ an toàn an ninh thông tin của hệ thống;
 - Các cơ chế an toàn an ninh
 - Các cơ chế cho phép:
 - Phát hiện,
 - Ngăn chặn hoặc
 - Khôi phục hệ thống sau khi bị tấn công;

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Các dịch vụ an toàn an ninh thông tin:
 - Các dịch vụ làm tăng cường mức độ an toàn của hệ thống xử lý thông tin và những thông tin được truyền đi.
 - Các dịch vụ có nhiệm vụ
 - Chống lại những tấn công thông tin và
 - Sử dụng một hoặc nhiều cơ chế an toàn an ninh để cung cấp dịch vụ.

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Các dịch vụ an toàn an ninh.
 - Những vấn đề nảy sinh khi sử dụng dữ liệu điện tử:
 - Không có sự khác biệt giữa các bản sao chép số với những bản gốc;
 - Thay đổi nội dung của bản tin vật lý sẽ để lại dấu vết, nhưng thay đổi nội dung của bản tin điện tử không để lại dấu vết;
 - Tính xác thực:
 - Chứng thực văn bản vật lý phụ thuộc vào các thuộc tính vật lý của văn bản;
 - Chứng thực văn bản phải dựa vào nội dung của chính văn bản đó.

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

Danh sách các chức năng toàn vẹn thông tin

Identification	Endorsement
Authorization	Access (Egress)
Liscen and/or Certification	Validation
Signature	Time of Occurrence
Witnessing (notarization)	Authenticity-software and/or file
Concurrence	Vote
Liability	Ownership
Receipt	Registration
Certification of Origination and/or receipt	Approval/Disapproval
	Privacy (secrecy)

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Phân loại các dịch vụ an toàn an ninh:
 - **Bảo mật riêng tư (confidentiality)**: đảm bảo thông tin trong hệ thống máy tính cũng như thông tin chuyển tải trên mạng chỉ được truy cập bởi những người được uỷ quyền. Các dạng truy cập bao gồm: đọc, in, hiển thị.
 - **Xác thực (authentication)**: đảm bảo về nguồn gốc của thông điệp hoặc văn bản điện tử.
 - **Toàn vẹn thông tin (integrity)**: đảm bảo rằng chỉ có những người được uỷ quyền mới có thể thay đổi tài nguyên của hệ thống máy tính và truyền tải thông tin. Mọi thay đổi bao gồm ghi, xoá , sửa, tạo mới hoặc xem lại các thông điệp.

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- **Chống phủ định (nonrepudiation)**: yêu cầu người gửi cũng như người nhận thông điệp không thể phủ định được liên kết.
- **Kiểm soát truy cập (access control)**: yêu cầu mọi sự truy cập tới tài nguyên thông tin đều được kiểm soát chặt chẽ từ hệ thống.
- **Tính sẵn sàng (availability)**: yêu cầu hệ thống tính toán sẵn sàng đối với những bên được uỷ quyền mỗi khi cần đến.

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Các cơ chế an toàn an ninh
 - Không tồn tại một cơ chế duy nhất có thể cung cấp tất cả các dịch vụ an toàn an ninh và thực hiện hết mọi chức năng đề ra.
 - Một phần tử được hầu hết mọi cơ chế bảo mật sử dụng: **các kỹ thuật mật mã**. Các phương thức truyền tải và lưu trữ thông tin dựa trên mật mã là cơ chế phổ biến để cung cấp sự an toàn thông tin.

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Các dạng tấn công.
 - Truy nhập thông tin bất hợp pháp;
 - Sửa đổi thông tin bất hợp pháp;
 - v.v và v.v ...

Các dạng tấn công vào hệ thống

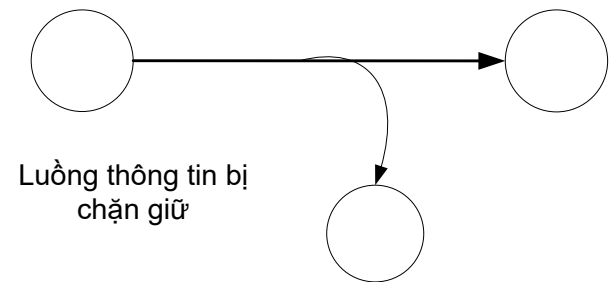
- Các dạng tấn công vào hệ thống máy tính và mạng:



- Gián đoạn truyền tin (interruption):
 - Các thông tin quý báu có thể bị phá hủy, không sử dụng được.
 - Dạng tấn công vào tính sẵn sàng của thông tin (availability).
 - Ví dụ: phá hủy đĩa cứng, cắt đường dây truyền tải, phá hỏng hệ thống quản lý file.

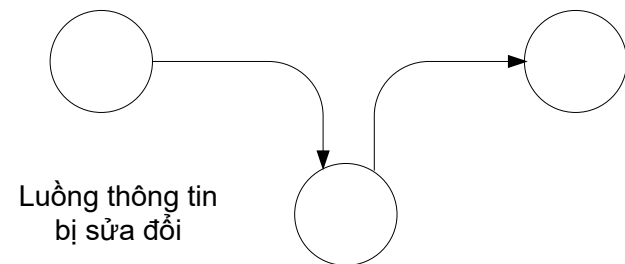
Các dạng tấn công vào hệ thống

- Chặn giữ thông tin (interception):
 - Người không được uỷ quyền cố gắng truy cập tới thông tin.
 - Dạng tấn công vào tính riêng tư của thông tin (confidentiality).
 - Ví dụ: sao chép trái phép thông tin.



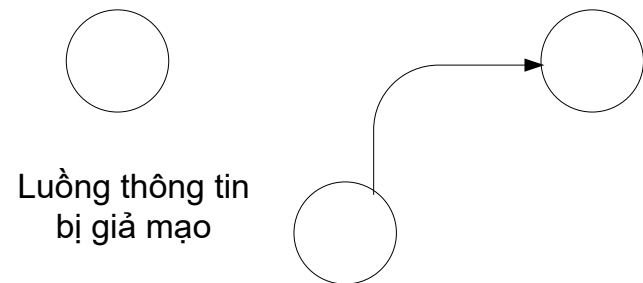
Các dạng tấn công vào hệ thống

- Sửa đổi thông tin (modification):
 - Không những truy cập trái phép thông tin mà còn sửa đổi thông tin gốc.
 - Dạng tấn công vào tính toàn vẹn thông tin.
 - Ví dụ: truy cập trái phép vào hệ thống, sửa đổi thông tin, thay đổi nội dung thông điệp được truyền tải.



Các dạng tấn công vào hệ thống

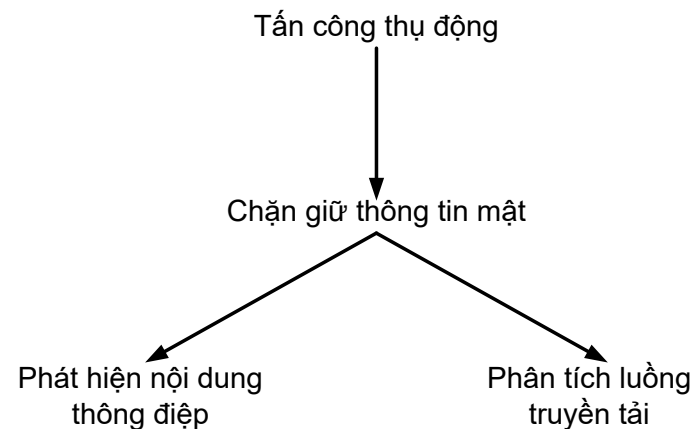
- Làm giả thông tin (fabrication).
 - Người không được uỷ quyền đưa những thông tin giả mạo vào hệ thống.
 - Dạng tấn công vào tính xác thực thông tin (authenticity).
 - Ví dụ: đưa những thông điệp giả mạo vào hệ thống, thêm những bản ghi mới vào file.



Các dạng tấn công vào hệ thống

Tấn công thụ động

- Dạng tấn công thụ động.
 - Tấn công thụ động tương tự hình thức nghe trộm, theo dõi quá trình truyền tin.
 - Mục đích của đối phương là thu được những thông tin được truyền tải.



Các dạng tấn công vào hệ thống

Tấn công thụ động

- Các dạng tấn công thụ động:
 - Phát hiện nội dung thông điệp (release of message contents).
 - Phương pháp chống: Ngăn chặn đối phương thu và tìm hiểu được nội dung của thông tin truyền tải.
 - Phân tích lưu lượng (traffic analysis).
 - Mục đích của bên truyền tải thông tin: che dấu nội dung của tin khỏi đối tượng thứ ba \Rightarrow cơ chế mật mã nội dung được sử dụng rộng rãi.
 - Vấn đề đặt ra: bên thứ ba có thể xác định được vị trí của các máy tham gia vào quá trình truyền tin, xác định được tần suất và kích thước bản tin, từ đó đoán được nội dung của bản tin.

Các dạng tấn công vào hệ thống

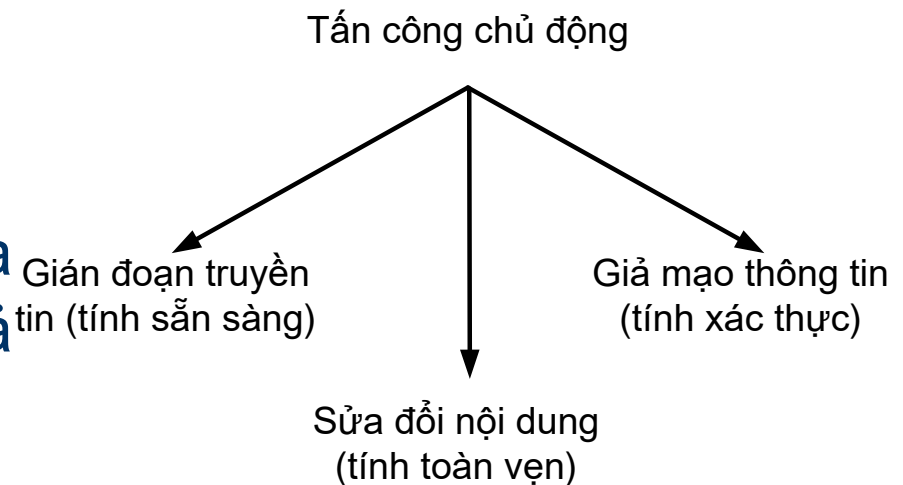
Tấn công thụ động

- Dạng tấn công thụ động rất khó bị phát hiện vì không làm thay đổi dữ liệu.
- Với dạng tấn công thụ động, nhấn mạnh vấn đề ngăn chặn hơn là vấn đề phát hiện.

Các dạng tấn công vào hệ thống

Tấn công chủ động

- Dạng tấn công chủ động.
 - Dạng tấn công chủ động bao gồm: sửa các dòng dữ liệu, đưa những dữ liệu giả, giả danh, phát lại, thay đổi thông điệp, phủ nhận dịch vụ.



Các dạng tấn công vào hệ thống

Tấn công chủ động

- Giả danh (masquerade): khi đối phương giả mạo một đối tượng được ủy quyền.
- Phát lại (replay): dạng tấn công khi đối phương chặn bắt các đơn vị dữ liệu và phát lại chúng tạo nên các hiệu ứng không được ủy quyền;

Các dạng tấn công vào hệ thống

Tấn công chủ động

- Thay đổi thông điệp (modification of message): một phần của thông điệp hợp pháp bị sửa đổi, bị làm chậm lại hoặc bị sắp xếp lại và tạo ra những hiệu ứng không được uỷ quyền.
- Phủ nhận dịch vụ (denial of service): dạng tấn công đưa đến việc cấm hoặc ngăn chặn sử dụng các dịch vụ, các khả năng truyền thông.

Các dạng tấn công vào hệ thống

Tấn công chủ động

- Dạng tấn công chủ động:
 - Rất khó có thể ngăn chặn tuyệt đối.
 - Để ngăn chặn, yêu cầu phải bảo vệ vật lý mọi đường truyền thông tại mọi thời điểm.
- Mục tiêu an toàn:
 - Phát hiện tấn công một cách nhanh nhất
 - Phục hồi lại thông tin trong các trường hợp dữ liệu bị phá hủy hoặc bị làm trệ.

Các dịch vụ an toàn an ninh

Đảm bảo tính riêng tư (Confidentiality)

- Đảm bảo tính riêng tư (Confidentiality).
 - Đảm bảo tính riêng tư của thông tin: Bảo vệ dữ liệu được truyền tải khỏi các tấn công thụ động.
 - Tương ứng với hình thức phát hiện nội dung thông điệp (release of message content) có một vài phương pháp bảo vệ đường truyền:
 - Bảo vệ mọi dữ liệu được truyền giữa hai người sử dụng tại mọi thời điểm:
 - Thiết lập đường truyền ảo giữa hai hệ thống và ngăn chặn mọi hình thức phát hiện nội dung thông điệp.
 - Ví dụ: VPN

Các dịch vụ an toàn an ninh

Đảm bảo tính riêng tư (Confidentiality)

- Bảo vệ các thông điệp đơn lẻ hoặc một số trường đơn lẻ của thông điệp.
 - Không thực sự hữu ích;
 - Trong nhiều trường hợp khá phức tạp;
 - Yêu cầu chi phí lớn khi thực hiện.
- Đảm bảo tính riêng tư: bảo vệ luồng thông tin trao đổi khỏi các thao tác phân tích
 - Yêu cầu: phía tấn công không thể phát hiện được các đặc điểm của quá trình truyền tin:
 - Nguồn và đích của thông tin;
 - Tần suất, độ dài;
 - Các thông số khác của luồng thông tin.

Các dịch vụ an toàn an ninh

Đảm bảo tính xác thực (Authentication)

- Đảm bảo tính xác thực (Authentication)
 - Dịch vụ đảm bảo tính xác thực:
 - Khẳng định các bên tham gia vào quá trình truyền tin được xác thực và đáng tin cậy.
 - Đối với các thông điệp đơn lẻ:
 - Các thông báo, báo hiệu: dịch vụ xác thực:
 - Đảm bảo cho bên nhận rằng các thông điệp được đưa ra từ những nguồn đáng tin cậy.

Các dịch vụ an toàn an ninh

Đảm bảo tính xác thực (Authentication)

- Đối với những liên kết trực tuyến, có hai khía cạnh cần phải chú ý tới:
 - Tại thời điểm khởi tạo kết nối, dịch vụ xác thực phải hai thực thể tham gia vào trao đổi thông tin phải được ủy quyền.
 - Dịch vụ cần khẳng định rằng kết nối không bị can thiệp bởi một bên thứ ba. Trong đó bên thứ ba này có thể giả mạo một trong hai bên được ủy quyền để có thể tham gia vào quá trình truyền tin và thu nhận các thông điệp.

Các dịch vụ an toàn an ninh

Đảm bảo tính sẵn sàng (Availability)

- Đảm bảo tính sẵn sàng (Availability).
 - Tấn công phá hủy tính sẵn sàng của hệ thống:
 - Thực hiện các thao tác vật lý tác động lên hệ thống.
 - Dịch vụ đảm bảo tính sẵn sàng phải:
 - Ngăn chặn các ảnh hưởng lên thông tin trong hệ thống.
 - Phục hồi khả năng phục vụ của các phần tử hệ thống trong thời gian nhanh nhất.

Các dịch vụ an toàn an ninh

Đảm bảo tính toàn vẹn(Integrity)

- Đảm bảo tính toàn vẹn (Integrity).
 - Đảm bảo tính toàn vẹn cũng có thể áp dụng cho luồng thông điệp, một thông điệp hoặc một số trường được lựa chọn của thông điệp.
 - Phương pháp hữu ích nhất là trực tiếp bảo vệ luồng thông điệp.
 - Đảm bảo tính toàn vẹn:
 - Dịch vụ bảo đảm tính toàn vẹn dữ liệu hướng liên kết;
 - Dịch vụ bảo đảm tính toàn vẹn hướng không liên kết.

Các dịch vụ an toàn an ninh

Đảm bảo tính toàn vẹn (Integrity)

- Dịch vụ bảo đảm tính toàn vẹn dữ liệu hướng liên kết:
 - Tác động lên luồng thông điệp và đảm bảo rằng thông điệp được nhận hoàn toàn giống khi được gửi, không bị sao chép, không bị sửa đổi, thêm bớt.
 - Các dữ liệu bị phá hủy cũng phải được khôi phục bằng dịch vụ này.
 - Dịch vụ bảo đảm tính toàn vẹn dữ liệu hướng liên kết xử lý các vấn đề liên quan tới sự sửa đổi của luồng các thông điệp và chối bỏ dịch vụ.

Các dịch vụ an toàn an ninh

Đảm bảo tính toàn vẹn (Integrity)

- Dịch vụ bảo đảm tính toàn vẹn hướng không liên kết:
 - Chỉ xử lý một thông điệp đơn lẻ. Không quan tâm tới những ngữ cảnh rộng hơn.
 - Chỉ tập trung vào ngăn chặn việc sửa đổi nội dung thông điệp.

Các dịch vụ an toàn an ninh

Dịch vụ chống phủ nhận (Nonrepudiation)

- Dịch vụ chống phủ nhận (nonrepudiation).
 - Dịch vụ chống phủ nhận ngăn chặn người nhận và người gửi từ chối thông điệp được truyền tải.
 - Khi thông điệp được gửi đi, người nhận có thể khẳng định được rằng thông điệp đích thực được gửi tới từ người được uỷ quyền.
 - Khi thông điệp được nhận, người gửi có thể khẳng định được rằng thông điệp đích thực tới đích.

Các dịch vụ an toàn an ninh

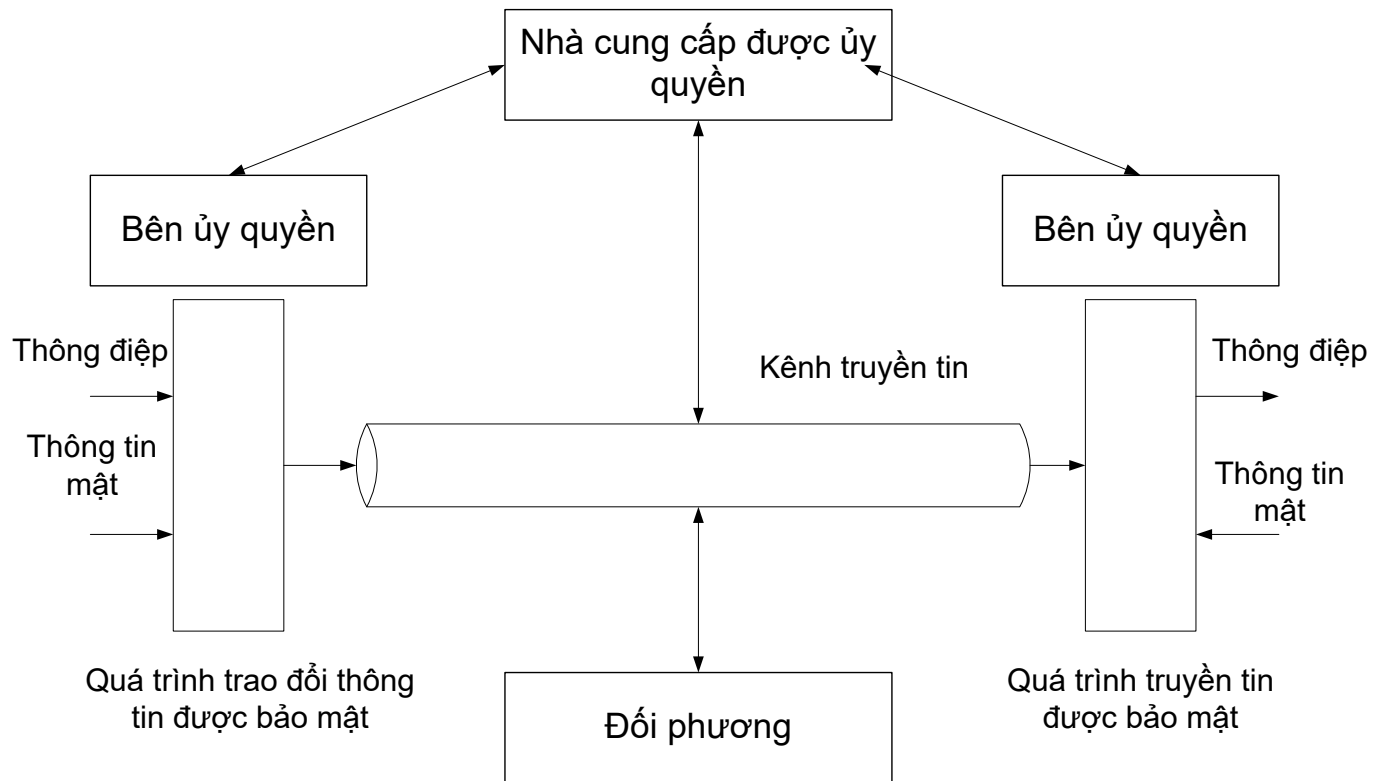
Dịch vụ kiểm soát truy cập

- Dịch vụ kiểm soát truy nhập.
 - Dịch vụ kiểm soát truy nhập cung cấp khả năng giới hạn và kiểm soát các truy nhập tới các máy chủ hoặc các ứng dụng thông qua đường truyền tin.
 - Để đạt được sự kiểm soát này, mỗi đối tượng khi truy nhập vào mạng phải được nhận biết hoặc được xác thực, sao cho quyền truy cập sẽ được gán với từng cá nhân.

Các mô hình an toàn mạng và hệ thống

- Mô hình an toàn mạng
 - Bài toán an toàn an ninh thông tin mạng nảy sinh khi:
 - Cần thiết phải bảo vệ quá trình truyền tin khỏi các hành động truy cập trái phép;
 - Đảm bảo tính riêng tư và tính toàn vẹn;
 - Đảm bảo tính xác thực; ..vv.
 - Mô hình truyền thống của quá trình truyền tin an toàn

Các mô hình an toàn mạng và hệ thống



Các mô hình an toàn mạng và hệ thống

- Tất cả các kỹ thuật đảm bảo an toàn hệ thống truyền tin đều có hai thành phần:
 - Quá trình truyền tải có bảo mật thông tin được gửi.
 - Ví dụ: mật mã thông điệp sẽ làm cho kẻ tấn công không thể đọc được thông điệp.
 - Thêm vào thông điệp những thông tin được tổng hợp từ nội dung thông điệp. Các thông tin này có tác dụng xác định người gửi.
 - Một số thông tin mật sẽ được chia sẻ giữa hai bên truyền tin.
 - Các thông tin này được coi là bí mật với đối phương.
 - Ví dụ: khóa mật mã được dùng kết hợp với quá trình truyền để mã hóa thông điệp khi gửi và giải mã thông điệp khi nhận.

Các mô hình an toàn mạng và hệ thống

- Bên thứ ba được ủy quyền: trong nhiều trường hợp, cần thiết cho quá trình truyền tin mật:
 - Có trách nhiệm phân phối những thông tin mật giữa hai bên truyền tin;
 - Giữ cho các thông tin trao đổi với các bên được bí mật đối với người tấn công.
 - Có trách nhiệm phân xử giữa hai phía truyền tin về tính xác thực của thông điệp được truyền.

Các mô hình an toàn mạng và hệ thống

- Các thao tác cơ bản thiết kế một hệ thống an ninh:
 - Thiết kế các thuật toán để thực hiện quá trình truyền tin an toàn;
 - Các thuật toán này phải đảm bảo: tấn công không làm mất khả năng an toàn của chúng.
 - Tạo ra những thông tin mật sẽ được xử lý bằng thuật toán trên.

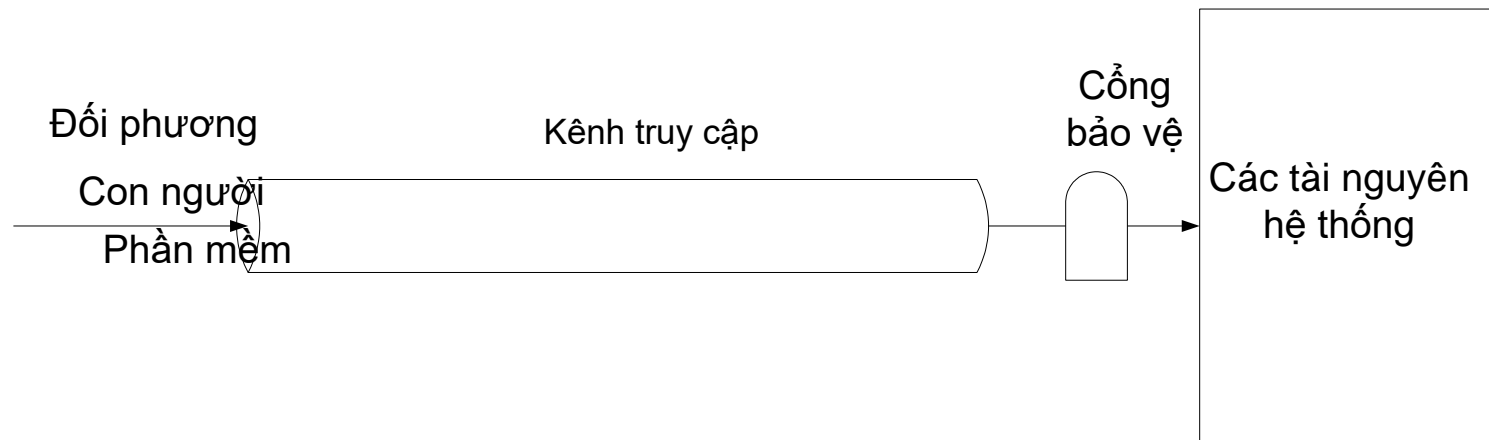
Các mô hình an toàn mạng và hệ thống

- Phát triển những phương pháp để phân phối và chia sẻ các thông tin mật.
- Đặt ra giao thức trao đổi:
 - Cho phép hai bên truyền tin trao đổi thông tin sử dụng những thuật toán an toàn;
 - Những thông tin mật đạt được độ an toàn thích hợp.

Các mô hình an toàn mạng và hệ thống

- Mô hình an toàn an ninh hệ thống
 - Truy nhập của các hacker;
 - Các lỗ hổng an ninh hệ thống;
 - Các tiến trình ngoại lai:
 - Các tiến trình truy cập tới thông tin: làm phá hủy, sửa đổi thông tin không được phép.
 - Các tiến trình dịch vụ: phát hiện các lỗi trong các dịch vụ của hệ thống để ngăn chặn việc sử dụng của những người không được ủy quyền.

Các mô hình an toàn mạng và hệ thống



Mô hình an ninh hệ thống

Chương II.

Các phương pháp mật mã khóa đối xứng

1. Sơ đồ chung của phương pháp mật mã khóa đối xứng
2. Một số phương pháp mật mã khóa đối xứng kinh điển
3. Hệ mật hoàn hảo và không hoàn hảo
4. Phương pháp DES
5. Quản trị và phân phối khóa
6. Đảm bảo tính riêng tư sử dụng phương pháp mật mã khoá đối xứng

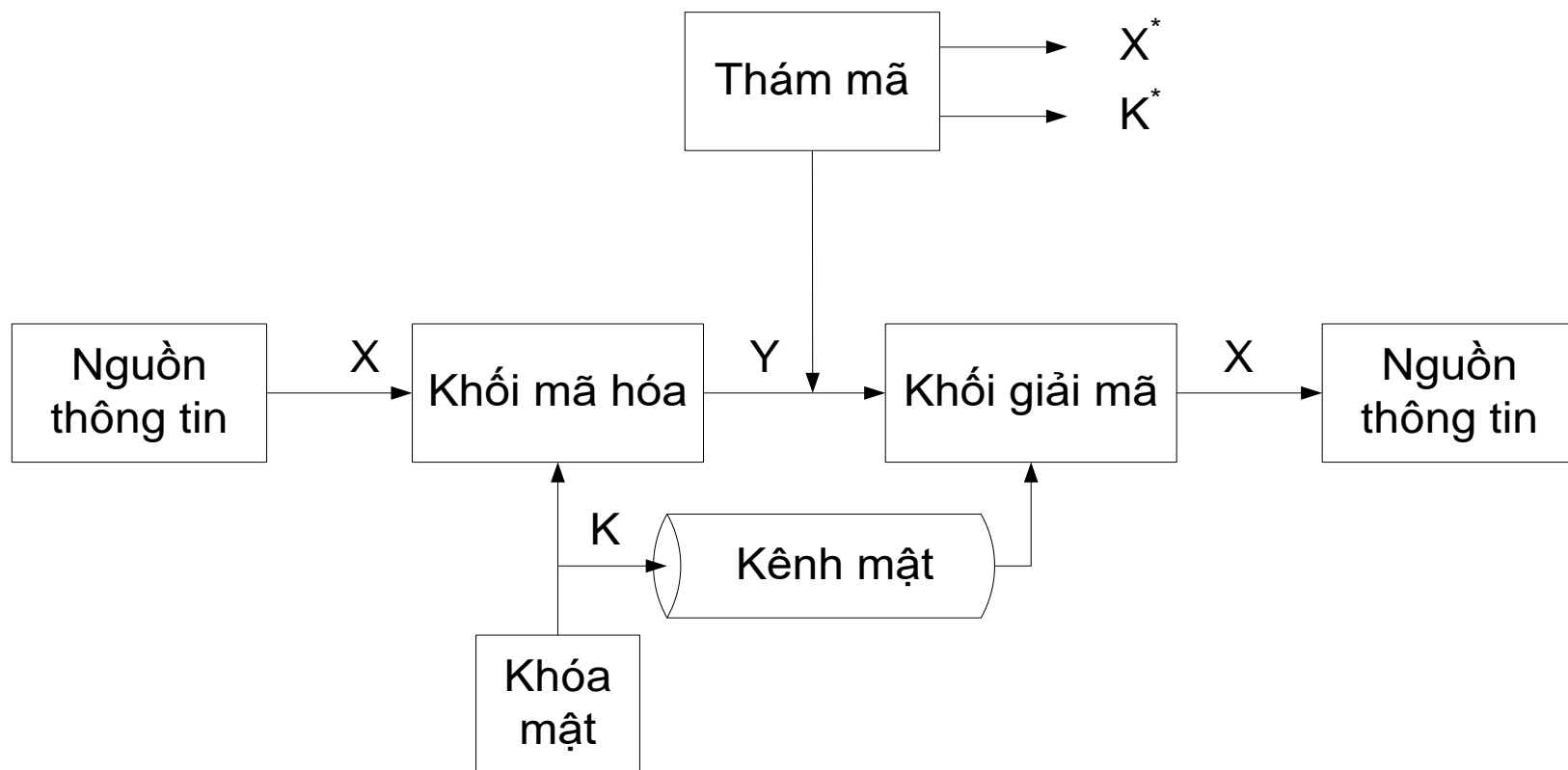
Sơ đồ chung của phương pháp mã hóa đối xứng

- Sơ đồ mã hóa đối xứng
- Mật mã và thám mã

Sơ đồ mật mã khóa đối xứng

- Một số thuộc tính của mô hình mật mã khóa đối xứng:
 - Thuật toán mã hóa phải đủ mạnh để không thể giải mã được thông điệp nếu chỉ dựa trên duy nhất nội dung của văn bản được mã hóa(ciphertext).
 - Sự an toàn của phương pháp mã hóa đối xứng chỉ phụ thuộc vào độ bí mật của khóa mà không phụ thuộc vào độ bí mật của thuật toán.
- Phương pháp mật mã khóa đối xứng giả thiết rằng:
 - Thám mã không thực hiện được nếu chỉ biết thông điệp bị mã hóa và thuật toán mã hóa.
 - Không cần giữ bí mật thuật toán.
 - Chỉ cần giữ bí mật khóa.

Sơ đồ mật mã khóa đối xứng



Mô hình hệ thống mã hóa đối xứng.

Sơ đồ chung của phương pháp mật mã khóa đối xứng

- Nguồn thông tin:
 - Tập hợp thông điệp của nguồn:
Các chuỗi ký tự $X = \{ X_1, X_2, \dots, X_M \}$;
 - Thông điệp: chuỗi ký tự độ dài m :
 $X_i = [x_{i1}, x_{i2}, \dots, x_{im}]$
 $x_{ik} \in A$; A – bảng ký tự nguồn; thông thường $A = \{0, 1\}$
 - Mỗi thông điệp X_i có một xác suất xuất hiện $P(X = X_i)$
 - thuộc tính thống kê của nguồn thông điệp:

Sơ đồ chung của phương pháp mật mã khóa đối xứng

- Khóa mật mã
 - Tập hợp khoá $K = \{ K_1, K_2, \dots K_L \}$,
 - Khóa độ dài l : $K_i = [k_{i1}, \dots, k_{il}]$;
 $k_{ij} \in C$, C - bảng ký tự khóa; thông thường $C = \{0, 1\}$
 - Xác suất tạo khóa $P\{K=k\}$ và phân bố xác suất tạo khóa.
 - Phân phối khóa giữa các bên trao đổi thông tin:
 - Phân phối khóa không tập trung: Nếu khóa K được tạo ra từ phía nguồn, khóa K cần được chuyển cho phía nhận tin thông qua một kênh bí mật .
 - Phân phối khóa tập trung: Khóa K do bên thứ ba được ủy quyền tạo ra và được phân phối cho cả hai phía gửi và nhận tin.

Sơ đồ chung của phương pháp mật mã khóa đối xứng

- Mã mật:

- Tập hợp thông điệp mã mật $Y = [Y_1, Y_2, \dots, Y_N]$
- Thông điệp mã mật: $Y_j = [y_{j1}, y_{j2}, \dots, y_{jn}]$
- $y_{jp} \in B$, B – bảng ký tự mã mật; thông thường $B = \{0, 1\}$

Sơ đồ chung của phương pháp mật mã khóa đối xứng

- Quá trình mật mã và giải mã:

- Quá trình mã hóa:

$$Y = E_K(X)$$

- Để tăng thêm độ bất định của quá trình mã hóa, sử dụng số ngẫu nhiên R

$$Y = E_{K,R}(X)$$

- Quá trình giải mã:

- Bên nhận giải mã thông điệp bằng khóa được phân phối:

$$X = D_K(Y) = D_K(E_{K,R}(X))$$

Sơ đồ chung của phương pháp mã hóa đối xứng

- Phía tấn công
 - Vấn đề đặt ra: đối phương nhận được thông điệp Y, nhưng không có được khóa K. Dựa vào thông điệp Y, đối phương phải khôi phục lại hoặc K, hoặc X hoặc cả hai.
 - Đối phương có thể chỉ cần khôi phục lại thông điệp X bằng thông điệp X^* .
 - Nếu đối phương muốn biết thêm các thông điệp trong tương lai: cần phải xác định được khóa K.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Mật mã
 - Hệ thống mật mã có thể được phân loại dựa vào các tiêu chí:
 - Dạng của phép toán tham gia vào mã hóa văn bản từ dạng thông thường sang dạng được mật mã hóa. Các phương pháp mã hóa thông thường này dựa vào các nguyên lý sau:
 - Phép thế: mỗi ký tự trong bản thông điệp sẽ được ánh xạ vào phần tử khác.
 - Phép hoán vị: các ký tự trong thông điệp ban đầu được phân bố lại.
 - Phép dịch;
 - Yêu cầu chính: không mất mát thông tin.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Phân loại các phương pháp mật mã theo số lượng khóa được dùng trong thuật toán:
 - Nếu bên gửi và bên nhận cùng dùng chung một khóa: hệ thống mã hóa đối xứng.
 - Nếu hai khóa của bên gửi và bên nhận khác nhau: phương pháp mã hóa không đối xứng.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Phân loại các thuật toán mật mã theo phương pháp xử lý dữ liệu đầu vào:
 - Mã hóa khối (block cipher): bản rõ được xử lý theo từng khối thông tin và tạo đầu ra theo từng khối thông tin.
 - Mã hóa dòng (stream cipher): bản rõ được xử lý liên tục theo từng bit.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Thăm mã
 - Quá trình xác định nội dung bản rõ X hoặc khóa K hoặc cả hai từ bên thứ ba (cryptanalyst).
 - Chiến lược được thăm mã sử dụng phụ thuộc vào bản chất của sơ đồ mã hoá và những thông tin do anh ta nắm được.
 - Các dạng thăm mã: Các dạng tấn công vào thông điệp được mã hoá.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Chỉ biết văn bản được văn bản mật (ciphertext only attack). Dạng bẻ khóa này là khó nhất. Thăm mã có thể biết:
 - Thuật toán mật mã.
 - Văn bản mã mật.
 - Phương pháp phá khóa: phương pháp vét cạn:
 - Thử tất cả các tổ hợp khóa có thể để tìm ra tổ hợp khóa thích hợp.
 - Trong trường hợp không gian khóa lớn thì phương pháp này khó thực hiện được.
 - Đối phương biết thuộc tính thống kê của nguồn tạo ra bản rõ, phân tích văn bản mật qua phân tích thống kê.
 - Đối phương biết:dạng ban đầu của văn bản rõ: ngôn ngữ, nguồn gốc, hoặc dạng file.
 - Dạng tấn công này dễ dàng đối phó nhất vì đối phương chỉ có một số lượng thông tin ít nhất để giải mã.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Nếu đối phương bắt được một số văn bản rõ và các mã mật tương ứng (known plaintext attack). Thăm mã biết:
 - Thuật toán mã hoá.
 - Mã mật.
 - Một hoặc một số cặp bản rõ –bản mật được xây dựng từ một khoá mật.
 - Dựa vào những thông tin trên, nhà phân tích tìm cách phát hiện khóa mật K .
 - Thăm mã có thể dựa vào nguồn gốc của thông điệp và ước đoán được một số thông tin trong văn bản gốc. Từ đó dựa vào cặp thông điệp xác định khóa mật.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Khi nhà phân tích thu được hệ thống nguồn, anh ta có thể sử dụng một văn bản gốc được lựa chọn trước để xác định văn bản mã hóa dựa vào đó xác định cấu trúc khóa mật (chosen plaintext attack). Nhà phân tích biết:
 - Thuật toán mã hoá.
 - Văn bản mật mã.
 - Văn bản gốc được nhà phân tích lựa chọn cùng với văn bản mật sinh ra bởi khoá mật.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Văn bản mã hoá cho trước (chosen ciphertext attack). Nhà phân tích biết:
 - Thuật toán mã hoá.
 - Văn bản mật mã.
 - Nội dung của một số văn bản mã hoá và văn bản gốc đã được giải mã tương ứng sử dụng mã mật.
 - Nhà phân tích phải giải mã văn bản mã hóa hoặc xác định được khóa mật.
- Văn bản tùy chọn (chosen text attack). Nhà phân tích biết:
 - Thuật toán mã hoá.
 - Văn bản mật mã.
 - Văn bản gốc được nhà phân tích lựa chọn cùng với văn bản mật sinh ra bởi khoá mật.
 - Nội dung của văn bản mã hoá và văn bản gốc được đã giải mã tương ứng sử dụng mã mật.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Chỉ có các thuật toán mã hóa yếu sẽ bị phá đối với loại tấn công chỉ dùng văn bản mật.
- Các thuật toán mã hóa được thiết kế để chống dạng tấn công với văn bản gốc đã biết (known plaintext attack).

Sơ đồ chung của phương pháp mã hóa đối xứng

- Sơ đồ mã hóa được coi là **an toàn vô điều kiện** (unconditional secure): nếu văn bản mã mật không chứa đủ thông tin để xác định duy nhất văn bản gốc tương ứng, không phụ thuộc vào phía đối phương có bao nhiêu văn bản mã mật.
 - Tính mật của văn bản được đảm bảo không phụ thuộc vào lượng thời gian mà đối phương dùng để phá mã mật.
 - Ngoại trừ sơ đồ mã mật sử dụng một lần (one-time pad), không có sơ đồ mã mật nào đảm bảo tính an toàn vô điều kiện.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Sơ đồ mã mật được coi là **an toàn thực tiễn** hay **an toàn theo tính toán** (computational secure) nếu thỏa mãn hai điều kiện:
 - Giá thành để bẻ khóa mật vượt quá giá trị của thông tin được mã hóa.
 - Thời gian để phá khóa mật vượt quá thời hạn giữ mật của thông tin.

Sơ đồ chung của phương pháp mã hóa đối xứng

- Ví dụ: thuật toán DES (Data Encryption Standard): Khoá nhị phân
 - Độ dài 32 bit \Rightarrow Số lượng khoá: $2^{32} \Rightarrow 35.8$ phút xử lý với tốc độ 1 phép mã hoá/ μ s $\Rightarrow 2.15$ ms với tốc độ 10^6 phép mã hoá / μ s.
 - Độ dài 56 bit \Rightarrow Số lượng khoá: $2^{56} \Rightarrow 1142$ năm xử lý với tốc độ 1 phép mã hoá/ μ s $\Rightarrow 10.01$ giờ với tốc độ 10^6 phép mã hoá / μ s.
 - Độ dài 128 bit \Rightarrow Số lượng khoá: $2^{128} \Rightarrow 5.4 \times 10^{24}$ năm xử lý với tốc độ 1 phép mã hoá/ μ s $\Rightarrow 5.4 \times 10^{18}$ năm với tốc độ 10^6 phép mã hoá / μ s.
- Ví dụ: Khoá sử dụng 26 ký tự bằng các phép hoán vị \Rightarrow Số lượng khoá: $26! \approx 4 \times 10^{26} \Rightarrow 6.4 \times 10^{12}$ năm xử lý với tốc độ 1 phép mã hoá/ μ s $\Rightarrow 6.4 \times 10^6$ năm với tốc độ 10^6 phép mã hoá / μ s.

Một số phương pháp mã hóa đối xứng kinh điển

- Các phương pháp thay thế
 - Mã Caesar
 - Các ký tự chữ cái được gán giá trị ($a = 1, b = 2, \dots$)
 - Ký tự của văn bản gốc (plaintext) p được thay thế bằng ký tự của văn bản mã mật (ciphertext) C theo luật mã hoá sau:

$$C = E(p) = (p + k) \bmod (26)$$

Trong đó k nhận các giá trị từ 1 đến 25.

- Trong phương pháp này, k chính là khoá mật mã.

Một số phương pháp mã hóa đối xứng kinh điển

- Quá trình giải mã:

$$p = D(C) = (C - k) \bmod (26)$$

- Phương pháp phá mã: một cách đơn giản: dùng các khoá k từ 1 đến 25 để giải mã cho đến khi nhận được thông điệp có ý nghĩa.
- Các vấn đề của mã Caesar:
 - Thuật toán mã hoá và giải mã đã biết trước.
 - Thám mã:
 - Không gian khóa nhỏ: chỉ có 25 khóa;
 - Khi thám mã bằng phương pháp vét cạn: chỉ cần thử với 25 khóa;
 - Ngôn ngữ trong bản gốc đã biết trước và dễ dàng nhận biết.

Một số phương pháp mật mã khóa đối xứng kinh điển

- Các vấn đề cần nghiên cứu khi khảo sát các thuật toán mật mã:
 - Thuộc tính thống kê của nguồn tin bản rõ
 - Sơ đồ tạo khóa, không gian khóa, các sơ đồ quản lý và phân phối khóa
 - Thuật toán mã hóa và giải mã
 - Độ an toàn của hệ mật.
 - Vấn đề khẳng định giải mã được đúng bản rõ.

Một số phương pháp mã hóa đối xứng kinh điển

– Mã mật Hill

- Thuật toán mã hoá

- Mỗi ký tự được gán giá trị số: $a = 0, b = 1, \dots, z = 25$
- Lựa chọn m ký tự liên tiếp của văn bản gốc;
- Thay thế các ký tự đã lựa chọn bằng m ký tự mã mật.
- Việc thay thế ký tự được thực hiện bằng m phương trình tuyến tính.
- Hệ phương trình mã hóa:

$$C = KP \pmod{26}$$

K- ma trận khóa

- Thuật toán giải mã

$$P = K^{-1}C \pmod{26}$$

Một số phương pháp mã hóa đối xứng kinh điển

- Ví dụ: với $m = 3$, hệ các phương trình tuyến tính có dạng sau:

$$C_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$

$$C_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$

$$C_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

$$\mathbf{C} = \mathbf{K}\mathbf{P}$$

Một số phương pháp mã hóa đối xứng kinh điển

- Ma trận K là ma trận khoá mật mã
- Ví dụ: với ma trận K bằng:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Xâu ký tự: “paymoremoney” sẽ được mã hoá thành
“LNSHDLEWMTRW”

“pay” $\Leftrightarrow (15, 0, 24)$; $K(15, 0, 24)^T \bmod 26 = (11, 13, 18) \Leftrightarrow$
“LNS”

Một số phương pháp mã hóa đối xứng kinh điển

- Giải mã thông điệp bằng ma trận K^{-1} .

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

- Hệ mã Hill:
- Các phép toán thực hiện theo modulo 26

$$\begin{cases} C = E_K(P) = KP \\ P = D_K(C) = K^{-1}C = K^{-1}KP = P \end{cases}$$

Một số phương pháp mã hóa đối xứng kinh điển

- Mức độ an toàn của hệ mã Hill
 - Mã mật Hill có tính mật cao khi phía tấn công chỉ có văn bản mật.
 - Thăm mã hệ mã Hill: dễ dàng bị bẻ khóa nếu bên tấn công biết được văn bản rõ và văn bản mật tương ứng (known plaintext attack)
 - Hệ mã mật Hill $m \times m$;
 - Thăm mã đã có m cặp văn bản gốc – văn bản mật, mỗi văn bản có độ dài m ;
 - Tạo các cặp: $P_j = (p_{1j} \ p_{2j} \ \dots, \ p_{mj})$ và $C_j = (C_{1j} \ C_{2j} \ \dots, \ C_{mj})$ sao cho $C_j = KP_j$ với $1 \leq j \leq m$ đối với một khoá K chưa biết.
 - Xác định hai ma trận $m \times m$, $\mathbf{X} = (p_{ij})$ và $\mathbf{Y} = (C_{ij})$

Một số phương pháp mã hóa đối xứng kinh điển

- Ta có $\mathbf{Y} = \mathbf{XK} \Rightarrow \mathbf{K} = \mathbf{X}^{-1}\mathbf{Y}$.
- Ví dụ: văn bản gốc: “friday” được mã hoá bằng mã mật Hill 2 x 2 thành “PQCFKU”.
 - Ta có: $K(5\ 17) = (15\ 16)$; $K(8\ 3) = (2\ 5)$; $K(0\ 24) = (10\ 20)$
 - Với hai cặp ban đầu ta có :

$$\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} \mathbf{K} \Rightarrow$$

$$\mathbf{K} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}$$

Một số phương pháp mã hóa đối xứng kinh điển

- Hệ thống Vernam.
 - Để chống lại quá trình thám mã, cần lựa chọn khoá thoả mãn:
 - Khoá có độ dài bằng văn bản rõ.
 - Khoá được chọn sao cho khoá và văn bản rõ độc lập thống kê.
 - Hệ mã mật Vernam:
 - Dùng cho mã nhị phân
 - $C_i = p_i \oplus k_i$
 - p_i : bit thứ i của văn bản rõ;
 - k_i : bit thứ i của khoá;
 - C_i : bit thứ i của văn bản mật;
 - \oplus : phép toán XOR.

Một số phương pháp mã hóa đối xứng kinh điển

- Giải mã bằng phép toán ngược: $p_i = C_i \oplus k_i$
- Tạo khoá: tạo vòng lặp với một khoá. Như vậy thực tế, hệ thống làm việc với một khóa rất dài nhưng lặp lại.
- Hệ thống Vernam có thể bị phá nếu đối phương biết một văn bản mã có độ dài đủ lớn, sử dụng một số văn bản rõ đã biết.
- Với khoá được sinh ngẫu nhiên, có độ dài bằng độ dài văn bản rõ, không lặp lại: sơ đồ mã sử dụng một lần (one-time pad): không thể phá khoá. Đầu ra độc lập thống kê với văn bản rõ.
- Vấn đề nảy sinh: đảm bảo mật cho quá trình gửi và nhận khoá ngẫu nhiên.

Phương pháp mật mã DES

- Văn bản rõ X, văn bản mã mật Y là các chuỗi nhị phân độ dài 64 bit.
- Khóa K có độ dài 56 bit.
- Từng khối 64 bit được mã hóa độc lập sử dụng chung một khóa.

Phương pháp mật mã DES

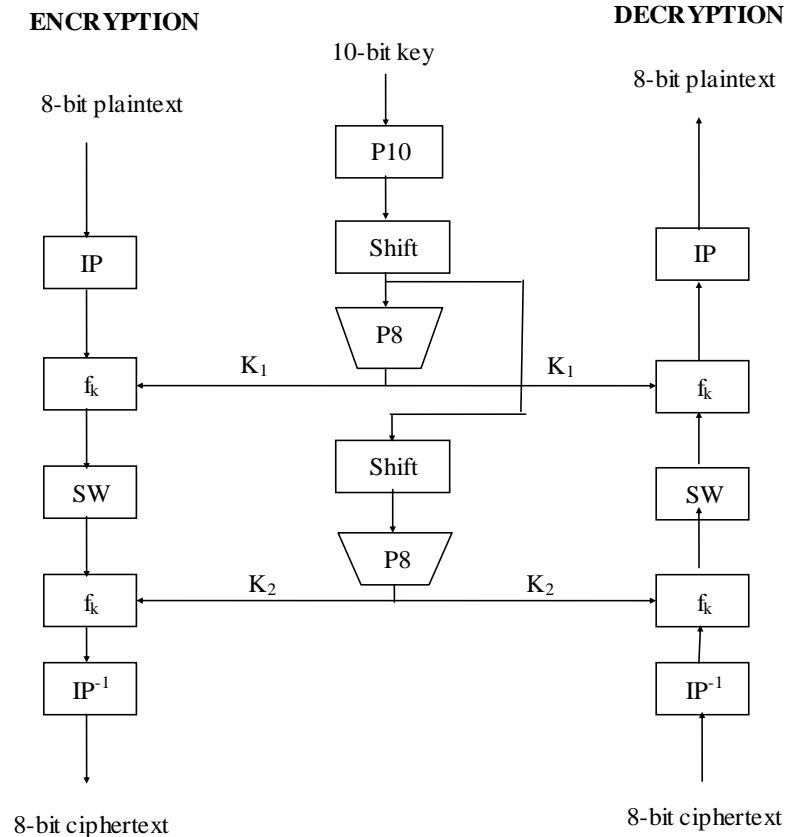
- Phương pháp S-DES(DES giản lược)
- Phương pháp mật mã DES

S- DES

(Simplified data encryption standard)

- Cấu trúc của DES là rất phức tạp
 - S-DES - phiên bản đơn giản của DES;
 - Cho phép:
 - Mã hoá và giải mã bằng tay;
 - Hiểu biết sâu về hoạt động chi tiết của giải thuật DES.
- S-DES đơn giản hơn nhiều so với DES
 - Các tham số của S-DES nhỏ hơn trong DES;
 - Do giáo sư Edward Schaefer thuộc trường đại học Santa Clara phát triển

Giải thuật S-DES(Simplified DES):



Hình 1:Sơ đồ mã hoá và giải mã S-DES

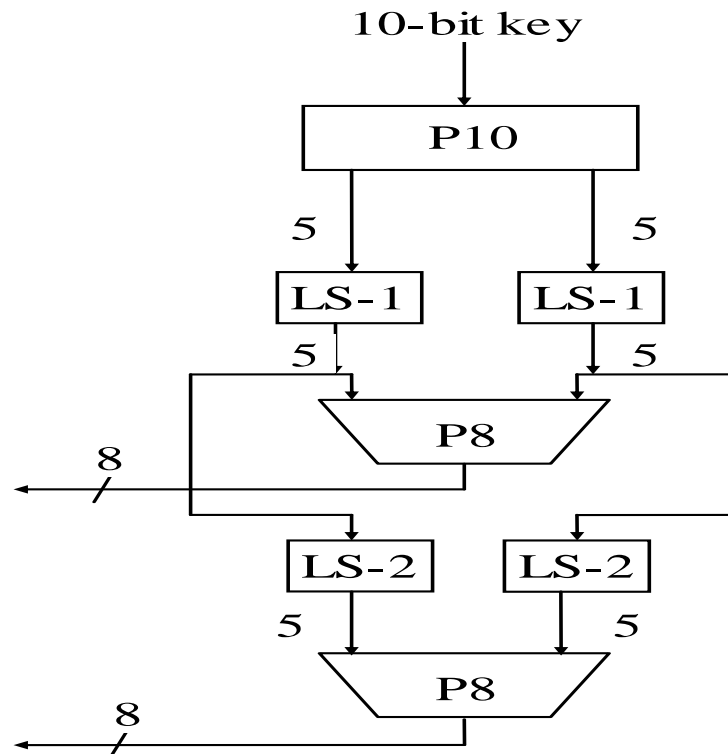
Giải thuật S-DES

- Giải thuật mã hoá S-DES sử dụng phương pháp mã hoá theo khối
- Đầu vào:
 - 8-bit block của bản rõ
 - 10-bit khoá
- Đầu ra:
 - 8-bit của bản mã

Giải thuật S-DES

- Giải thuật mã hoá bao gồm 4 hàm:
 - Hàm IP(Initial Permutation)
 - Hàm f_k
 - Hàm SW (Switch)
 - Hàm IP^{-1}
- Giải thuật mã hoá có thể biểu diễn như một hàm sau đây:
$$\text{ciphertext} = IP^{-1}(f(SW(f(IP(\text{plaintext}))))))$$
- Tương tự giải thuật giải mã có thể biểu diễn như hàm sau:
$$\text{plaintext} = IP(f(SW(f(IP^{-1}(\text{ciphertext}))))))$$

Sinh khoá trong S-DES:



Hình2: Sơ đồ tạo khóa của thuật toán S-DES

Các hàm sinh khoá:

- P10: Đây là hàm hoán vị tuân theo luật như trong bảng

P10									
3	5	2	7	4	10	1	9	8	6

- LS-1: Là hàm dịch vòng 1 bit
- LS-2: Là hàm dịch vòng 2 bit
- P8: Là hàm hoán vị tuân theo luật như trong bảng

P8							
6	3	7	4	8	5	10	9

Mã hoá S-DES:

Hàm IP và hàm IP^{-1} :

+ Hàm IP tuân theo luật sau:

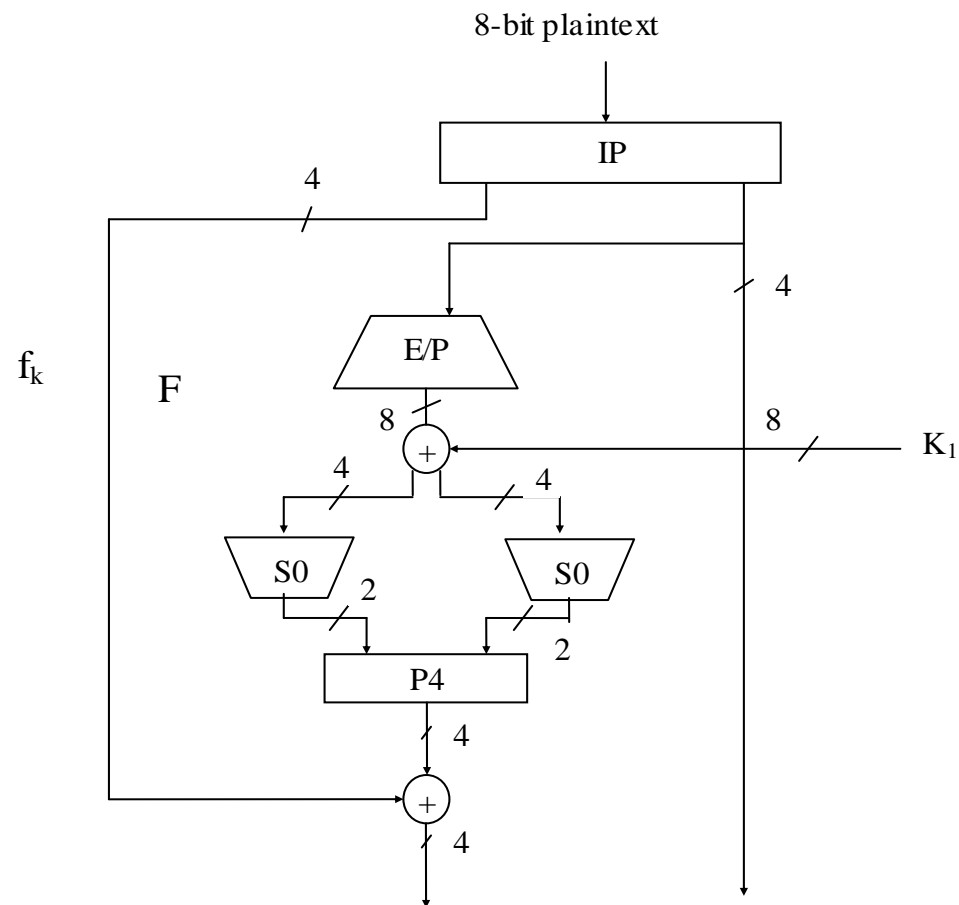
IP							
2	6	3	1	4	8	5	7

+ Hàm IP^{-1} tuân theo luật sau:

IP^{-1}							
4	1	3	5	7	2	8	6

Hàm f_k :

Hình 3: Mô hình chi tiết f_k



E/P(expension/permutation):

- Hàm E/P tuân theo luật sau:

E/P							
4	1	2	3	2	3	4	1

- Nếu gọi 4 bit đầu vào là (n_1, n_2, n_3, n_4) thì E/P được biểu diễn chi tiết như sau:

n_4	n_1	n_2	n_3
n_2	n_3	n_4	n_1

Khối thay thế S-box

- Tại đầu vào S-box một khối 8 bit được chia thành hai khối 4 bit;
- Mỗi khối 4 bit được đưa vào S_0 và S_1
- Thay thế mỗi khối 4 bit bằng khối 2 bit;
- Các khối S_0 và S_1 được định nghĩa như sau:

S_0 :

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S_1 :

0	1	2	3
2	0	1	3
3	0	1	2
2	1	0	3

Khối thay thế S-box

- Phần tử trong khối S-box có độ dài 2 bit;
- Quá trình thay thế trong S-box:
 - Với 4 bit đầu vào là (b_1, b_2, b_3, b_4) ;
 - b_1 và b_4 kết hợp thành một số chỉ hàng của S box,
 - b_2 và b_3 tạo thành số chỉ cột trong S box;
 - Phần tử nằm trên hàng và cột đã xác định thay thế cho 4 bit đầu vào của S-box đó.

Hoán vị P4

- Hoán vị P4 tuân theo luật sau:

P4			
2	4	3	1

Hàm SW

- Hàm f_k chỉ thực hiện trên 4 bit trái của đầu vào;
- Hàm SW hoán đổi 4 bit phải và 4 bit trái để lần áp dụng hàm f_k thứ 2 sẽ thực hiện trên 4 bit phải.
- Áp dụng hàm f_k lần 2 thực hiện các hàm E/P, $S_0, S_1, P4$ như trên.

Mật mã DES

(Data Encryption Standard)

- Phương pháp mật mã DES được Ủy ban tiêu chuẩn Mỹ (U.S National Bureau for Standards) công bố năm 1971 để sử dụng trong các cơ quan chính phủ liên bang.
- Thuật toán được IBM phát triển.
- DES có một số đặc điểm sau:
 - Sử dụng khoá 56 bit.
 - Xử lý khối vào 64 bit, biến đổi khối vào thành khối ra 64 bit.
 - Mã hoá và giải mã được sử dụng cùng một khoá.
 - DES được thiết kế để thực hiện hiệu quả bằng phần cứng.
 - DES thường được sử dụng để mã hoá các dòng dữ liệu mạng và mã hoá dữ liệu được lưu trữ trên đĩa.

Giải mã DES

- Với DES, có thể sử dụng cùng chức năng để giải mã hoặc mã hoá một khối.
- Điểm khác biệt: khi giải mã, các khoá phải được sử dụng theo thứ tự ngược lại.

Độ an toàn của DES

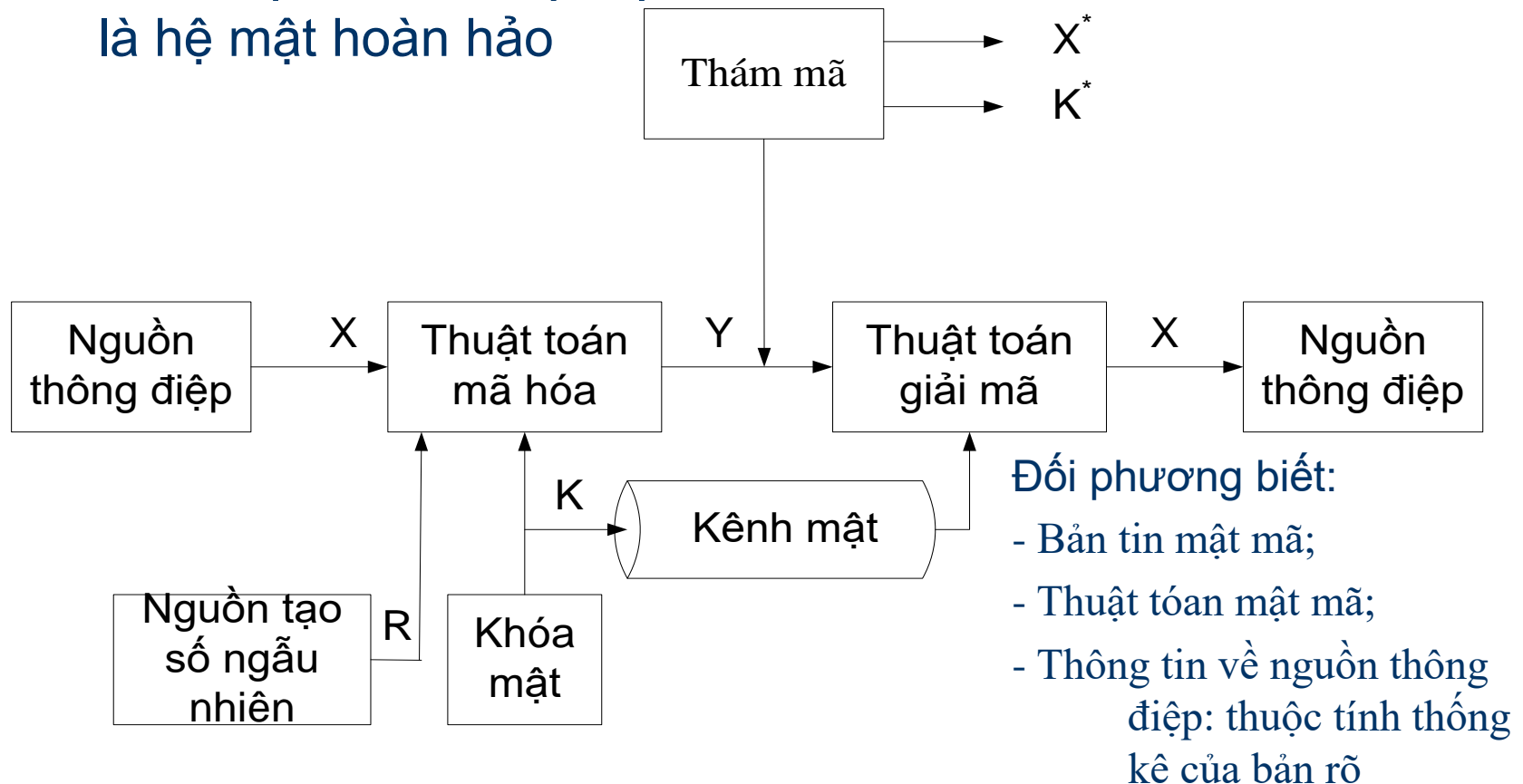
- Độ an toàn hệ mật khoá đối xứng phụ thuộc hai tham số: độ phức tạp của thuật toán và độ dài của khoá.
- Khoá có độ dài 56 bit, không gian khoá sẽ có 2^{56} khoá có thể sử dụng.
- Nếu tính mật của phương pháp chỉ phụ thuộc vào độ phức tạp của thuật toán.
 - Có nghĩa rằng sẽ không có phương pháp nào khác để phá hệ thống mật mã ngoài cách thử mọi tổ hợp khoá có thể: phương pháp tấn công vét cạn (brute-force attack).
 - Nếu một siêu máy tính có thể thử một triệu khoá trong một giây, thì thời gian tổng cộng để tìm ra khoá đúng là khoảng 2000 năm.

Kết luận:

- Tồn tại nhiều phương pháp mật mã để đảm bảo an toàn dữ liệu.
- Đánh giá tính ưu việt một giải thuật mật mã thường dựa vào:
 - Tính mật, độ phức tạp, tốc độ thực hiện giải thuật và vấn đề phân phối khoá trong môi trường nhiều người sử dụng.
- Các phương pháp mật mã kinh điển như phương pháp mã hoá thay thế, hoán vị còn đơn giản.
 - Nhược điểm:
 - Độ an toàn không cao vì thường không đạt được độ phức tạp cần thiết và
 - Rất dễ bị lộ khoá do cả người gửi và người nhận đều sử dụng cùng một khoá.
- DES đã được phân tích kỹ lưỡng và công nhận là vững chắc. Các hạn chế của nó đã được hiểu rõ và có thể xem xét trong quá trình thiết kế.
 - Để tăng độ an toàn của DES, sử dụng các hệ thống mật mã DES mở rộng
 - DES mở rộng khoá có thể là 128 bit, 192 bit,... độ lớn khối có thể là 128 bit. Do vậy, độ an toàn của DES mở rộng cao hơn rất nhiều.

Hệ mật hoàn hảo và không hoàn hảo

- Điều kiện cần để hệ mật là hệ mật hoàn hảo



Hệ mật hoàn hảo và không hoàn hảo

- Nguồn thông tin $X = [X_1, X_2, \dots, X_M]$, $X_i \in A$; A – bảng ký tự bản rõ cùng các thuộc tính thống kê (latin, nhị phân, ...).
- Khoá $K = [K_1, K_2, \dots, K_L]$, khoá K được tạo ra.
 - Các ký tự của khoá K nằm trong một bảng ký tự: bảng ký tự nhị phân $\{0, 1\}$
- Bộ tạo số ngẫu nhiên: $R = [R_1, R_2, \dots, R_J]$;
- Thông điệp được mã hóa là hàm của X , R và K : $Y = [Y_1, Y_2, \dots, Y_N]$
$$Y = E_{KR}(X)$$
- Bên nhận giải mã thông điệp bằng khoá đã phân phối:

$$X = D_K(Y)$$

Hệ mật hoàn hảo và không hoàn hảo

- Giả thiết sử dụng khóa và tạo số ngẫu nhiên:
 - Khóa mật chỉ được sử dụng một lần.
 - M bit của văn bản rõ sẽ được mã hoá trước khi khoá mật \mathbf{K} và chuỗi ngẫu nhiên \mathbf{R} thay đổi.
- Đối phương chỉ biết được văn bản mã mật \mathbf{Y} và thuật toán mã hóa, giải mã.
- Sơ đồ hệ mật hoàn hảo: Văn bản rõ \mathbf{X} độc lập thống kê với văn bản mã mật \mathbf{Y} .

$$\mathbf{P}(\mathbf{X} = \mathbf{x} \mid \mathbf{Y} = \mathbf{y}) = \mathbf{P}(\mathbf{X} = \mathbf{x})$$

đối với mọi bản tin rõ: $\mathbf{X} = [x_1, x_2, \dots, x_M]$ và bản tin mật \mathbf{Y} .

Hệ mật hoàn hảo và không hoàn hảo

- Ví dụ: hệ mã Vernam
 - Bảng chữ cái: $A = \{ 0, 1, \dots, |A|-1 \}$
 - Độ dài của văn bản gốc, khoá và văn bản mã bằng nhau: $M = L = N$.
 - Khoá được chọn ngẫu nhiên: $P(\mathbf{K} = \mathbf{k}) = |A|^{-M}$ đối với $|A|^M$ tổ hợp khoá.
 - Quá trình mã hoá: $Y_i = X_i \oplus K_i, i = 1, 2, \dots, M$.
 - Do với mỗi ký tự x_j thuộc X_i và y_i thuộc Y_j ta có duy nhất k_i thuộc K_j , do đó: $P(Y = y | X = x) = P(Z = z) = |A|^{-M}$ không phụ thuộc vào X .

Hệ mật hoàn hảo và không hoàn hảo

- Định lý: đối với hệ mật hoàn hảo

$$H(X) = H(X | Y) \leq H(K)$$

- Nếu bản rõ và bản mã cùng bảng ký tự, : $L_X = L_K$
 - Khi dấu bằng xảy ra: trong trường hợp one time pad.

• Các hệ mật không hoàn hảo

- Đặt vấn đề: khi nào thám mã có thể phá được các hệ mật không hoàn hảo ?!

Mật mã khối (block cipher)

- Định nghĩa

- Mã khối là mật mã khóa đối xứng thực hiện trên nhóm bit có độ dài cố định. Nhóm bit này được gọi là một khối. Quá trình chuyển đổi không thay đổi.
- Khi mã hóa, mã khối có thể thực hiện trên từng khối độ dài 128 bit của bản rõ tại đầu vào thứ nhất và cho ra khối 128 bit của mã mật.
 - Quá trình biến đổi được kiểm soát bằng đầu vào thứ hai: khóa mật
- Quá trình giải mã thực hiện tương tự: nhận tại đầu vào thứ nhất khối 128 bit của mật mã, khóa mật và tại đầu ra ta nhận được khối 128 bit của bản rõ

Mật mã khối (block cipher)

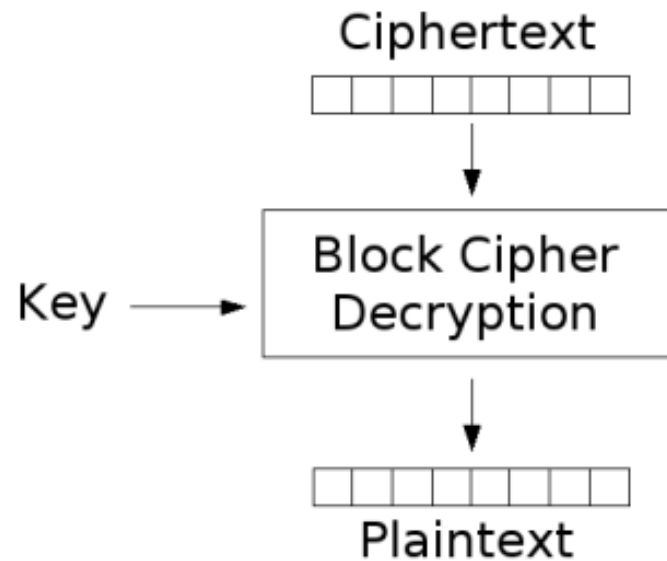
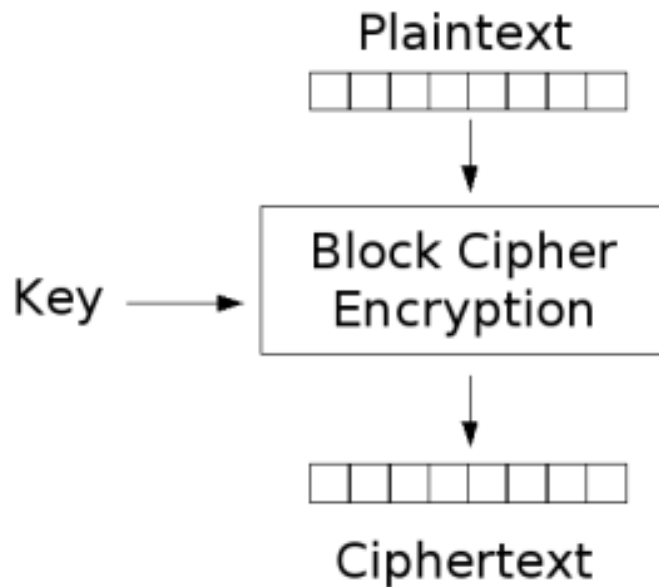
- Để mã hóa bản tin có độ dài lớn hơn kích thước khối, (ví dụ 128 bit), các chế độ xử lý (mode of operation) được sử dụng.
- Mã hóa khối tương phản với mã hóa dòng (stream cipher), trong đó mỗi ký tự được thao tác một lần và quá trình chuyển đổi thay đổi trong suốt quá trình mã hóa.
- Ví dụ mã hóa khối:
 - Thuật toán DES do công ty IBM xây dựng và công bố năm 1977.
 - Hậu duệ của DES, Advanced Encryption Standard (AES), ra đời năm 2001.

Mật mã khối (block cipher)

- Mật mã khối gồm một cặp thuật toán:
 - Thuật toán mã hóa, E , và
 - Thuật toán giải mã, E^{-1} .
 - Cả hai thuật toán đều có hai đầu vào:
 - Khối dữ liệu đầu vào kích thước n bit và
 - Khóa độ dài k bit,
 - Đầu ra là khối dữ liệu kích thước n -bit.

Mật mã khối (block cipher)

- Sơ đồ mã hóa và giải mã khối



Mật mã khối (block cipher)

- Đối với một khóa xác định, hàm giải mã là hàm ngược của hàm mã hóa:

$$E_K^{-1}(E_K (M)) = M$$

Đối với mỗi khối M và khóa K .

- Với mỗi khóa K , E_K là hoán vị (song ánh) trên tập hợp các khối đầu vào. Mỗi khóa sẽ lựa chọn một hoán vị từ tập hợp $2^n!$ phần tử.

Mật mã khối (block cipher)

- Kích thước khối n , thông thường bằng 64 hoặc 128 bit, tuy nhiên một số mật mã khối có kích thước khối thay đổi. 64 bits đã từng là kích thước thông dụng đến giữa những năm 90, trong khi đó một số thiết kế mới bắt đầu thực hiện với độ dài khối bằng 128bit.
- Một trong những kỹ thuật xử lý được dùng với sơ đồ padding cho phép bản rõ với độ dài tùy ý được mã hóa. Mỗi chế độ có một đặc tính riêng biệt phụ thuộc vào sai số truyền lan, tính dễ truy cập ngẫu nhiên và khả năng bị tổn thương đối với từng loại tấn công cụ thể.
- Kích thước khóa k thường bằng 40, 56, 64, 80, 128, 192 và 256 bits. Đến năm 2006, độ dài khóa 80 bits thường được chọn là kích thước khóa tối thiểu để ngăn chặn tấn công vét cạn (brute force attacks).

Mật mã khối (block cipher)

- **Mật mã khối lặp (Iterated block ciphers)**

- Phần lớn các mật mã khối được xây dựng trên cơ sở áp dụng lặp đi lặp lại một hàm đơn giản. Cách làm này gọi là mật mã khối lặp. Mỗi vòng lặp được gọi là một chu kỳ (round) và hàm lặp được gọi là hàm quay vòng. Thông thường số lần quay vòng từ 4 đến 32 lần.
- Nhiều mật mã khối có thể được phân loại thành các mạng Feistel, hoặc một cách tổng quát hơn là các mạng thay thế-hoán vị. Các phép toán số học, logic (đặc biệt là XOR), các S-box và các phép hoán vị khác nhau thường được sử dụng trong thành phần của phương pháp này.

Mật mã khối (block cipher)

- **Thám mã**

- Bên cạnh các phương pháp thám mã như thám mã tuyến tính, thám mã vi phân, còn có một số phương pháp khác:
 - Thám mã vi phân ngắn gọn (Truncated differential cryptanalysis);
 - Thám mã vi phân từng phần (Partial differential cryptanalysis);
 - Tấn công trượt (Slide attacks);
 - Tấn công Bu-mê-răng (Boomerang attacks),
 - Tấn công toàn phương và tích phân,
 - Tấn công XSL,
 - Tấn công vi sai bất khả và
 - Tấn công đại số
- Đối với mỗi mật mã khối mới được xây dựng, để có tính hiệu quả, mật mã đó phải thể hiện độ an toàn đối với các tấn công đã biết.

Mật mã khối (block cipher)

- **Mật mã khối và các mật mã cơ sở khác**

- Mật mã khối có thể được sử dụng để xây dựng các mật mã cơ sở khác (cryptographic primitives).
 - Để cho các phương pháp mã hóa này trở thành mật mã an toàn, những thuật toán này cần được xây dựng theo phương pháp đúng đắn.
- Các mật mã dòng có thể được xây dựng dựa trên mật mã khối.
 - Các chế độ OFB-mode và CTR mode là những chế độ theo khối.
 - Cho phép chuyển một mật mã khối thành mật mã dòng.
- Mật mã khối có thể sử dụng để xây dựng các hàm băm, và ngược lại, những hàm băm có thể là cơ sở để xây dựng những mật mã khối.
 - Ví dụ: những mật mã khối dựa trên hàm băm: SHACAL, BEAR và LION.

Mật mã khối (block cipher)

- Những bộ sinh số giả ngẫu nhiên an toàn theo phương diện mật mã có thể được tạo nên từ các mật mã khối.
- Mã xác thực thông điệp (MAC) cũng thường được xây dựng từ các mật mã khối. Ví dụ: CBC-MAC, OMAC, PMAC.
- Các mã xác thực cũng được xây dựng từ mật mã khối.
 - Cho phép thực hiện mã hóa mật và mã hóa xác thực đồng thời.
 - Điều này làm cho phương pháp cung cấp được cả tính riêng tư cũng như tính xác thực đồng thời. Ví dụ CCM, EAX, GCM, OCB.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Đặt vấn đề:
 - Trong kỹ thuật mật mã truyền thống, hai phía tham gia vào truyền tin phải chia sẻ khoá mật \Rightarrow khoá phải được đảm bảo bí mật : phải duy trì được kênh mật phân phối khóa.
 - Khóa phải được sử dụng một lần: Khoá phải được thường xuyên thay đổi.
 - Mức độ an toàn của bất kỳ hệ mật sẽ phụ thuộc vào kỹ thuật phân phối khoá.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Một số kỹ thuật phân phối khoá.
 - Phân phối khóa không tập trung: Khóa được A lựa chọn và phân phối vật lý tới B.
 - Phân phối khóa tập trung: Người thứ ba C lựa chọn khóa và phân phối vật lý tới A và B.
 - Nhận xét:
 - Hai kỹ thuật này khá cồng kềnh khi các bên tham gia vào trao đổi thông tin với số lượng lớn.

Quản trị và phân phối khóa trong mã hóa đối xứng

Sử dụng
phân
cấp khóa

Khóa
phiên

Khóa
chính



Bảo vệ bằng
mật mã



Bảo vệ bằng
mật mã



Bảo vệ
không bằng
mật mã

– Ít nhất có hai cấp khoá :

- Việc giao tiếp giữa hai trạm đầu cuối sẽ được mã hoá bằng một khoá tạm thời gọi là khoá phiên.
 - Khoá phiên sẽ được sử dụng trong thời gian một kết nối logic như trong mạng ảo hoặc liên kết vận chuyển, sau đó sẽ được loại bỏ.
 - Khoá phiên được truyền dưới dạng mã hoá bằng mã chính (master key). Khoá chính này được chia sẻ giữa KDC và trạm đầu cuối hoặc người sử dụng.

Quản trị và phân phối khóa trong mã hóa đối xứng

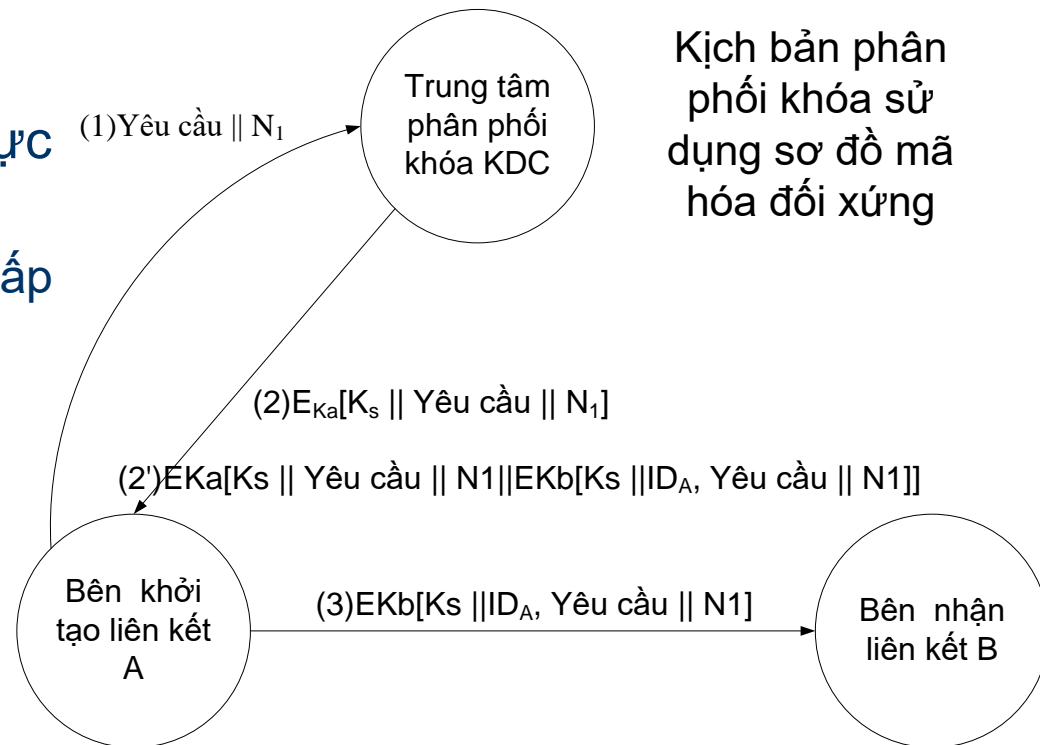
- Kịch bản quá trình phân phối khóa.
 - Giả thiết: mọi người sử dụng cùng chia sẻ một khóa mật chính với trung tâm phân phối khóa (KDC).
 - Tiền đề:
 - Người sử dụng A muốn thiết lập kết nối logic với người sử dụng B.
 - Hai phía trao đổi thông tin yêu cầu khóa phiên sử dụng một lần để bảo mật dữ liệu truyền qua kết nối.
 - Phía A có khóa mật K_{MA} , khóa này chỉ có A và KDC biết.
 - Phía B có khóa mật K_{MB} , khóa này chỉ có B và KDC biết.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Yêu cầu:

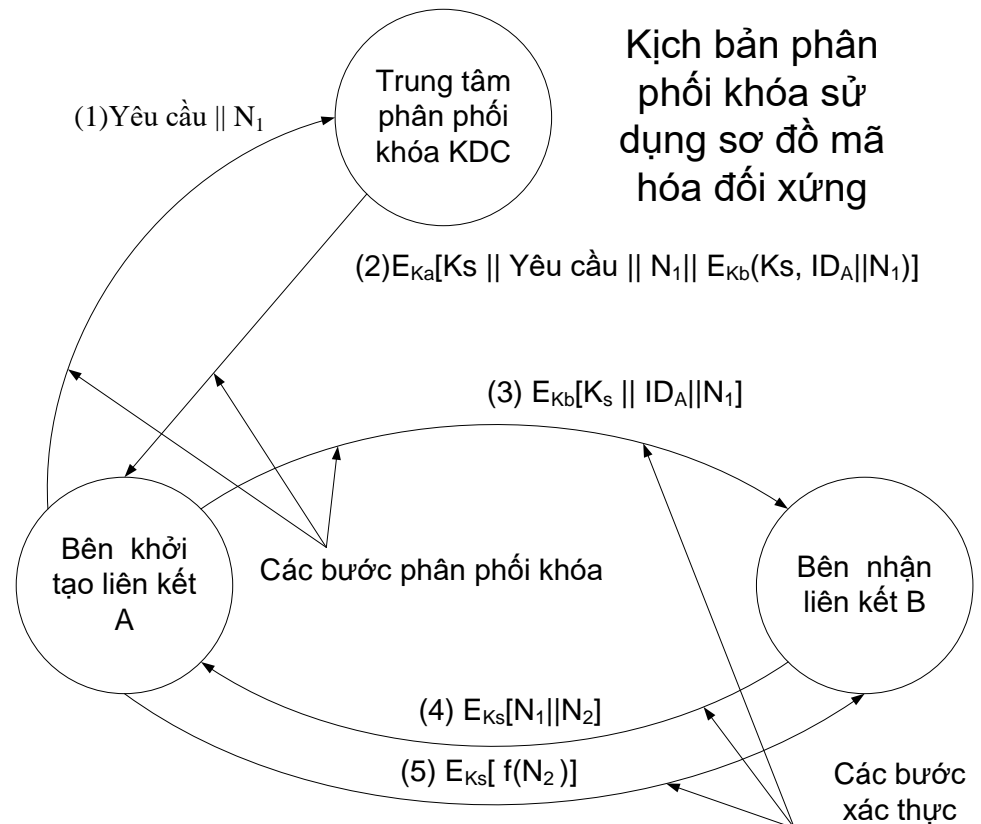
- A → KDC: KDC: xác thực A.

- $[ID_A; E_{KMA}[Yêu\ cầu\ cấp\ khóa; ID_B; N_1]]$



Quản trị và phân phối khóa trong mã hóa đối xứng

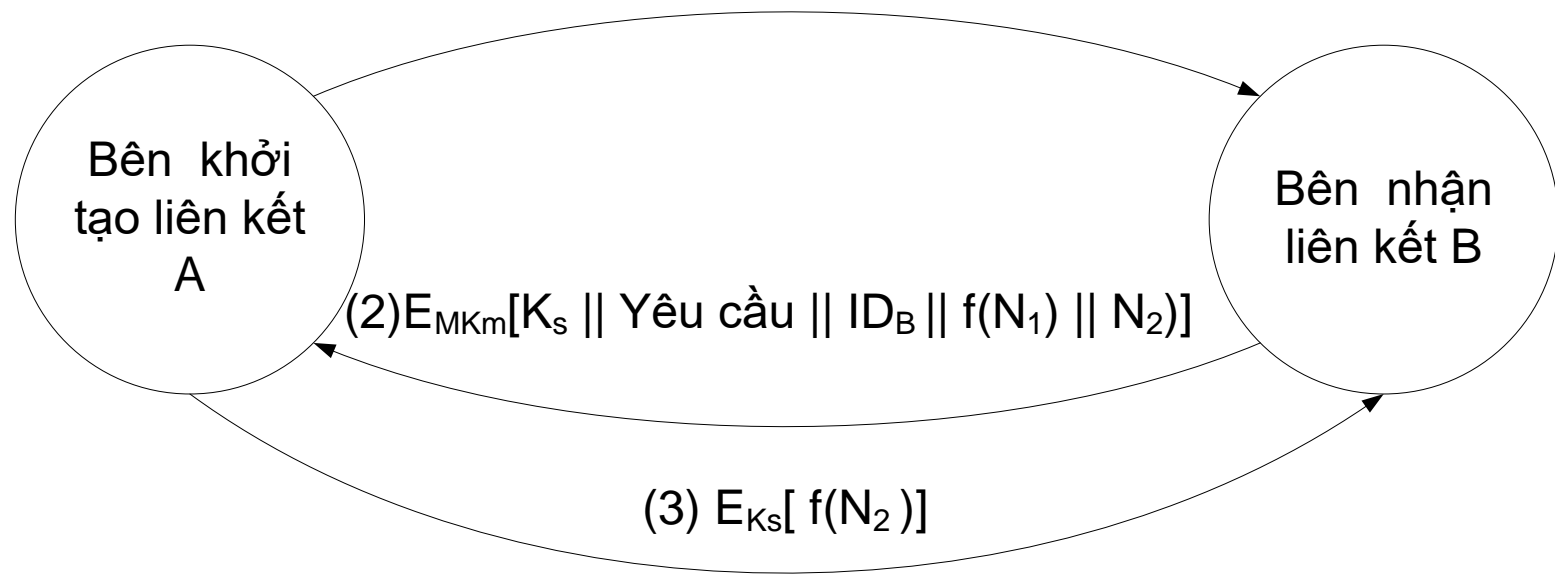
- Vấn đề xác thực:
 - B cần xác thực:
 - Nguồn gốc của $E_{kb}[K_s \parallel ID_A]$: bằng khóa K_b .
 - Tính toàn vẹn của $E_{kb}[K_s \parallel ID_A]$.
 - Xác thực A.
 - A cần xác thực:
 - Xác thực B.
 - Xác thực phiên làm việc với B.



Quản trị và phân phối khóa trong mã hóa đối xứng

Kịch bản phân phối khóa không tập trung

(1) Yêu cầu $\parallel N_1$



Đảm bảo tính riêng tư với sơ đồ mã hoá đối xứng

1. Các cơ chế đảm bảo an toàn hệ thống:

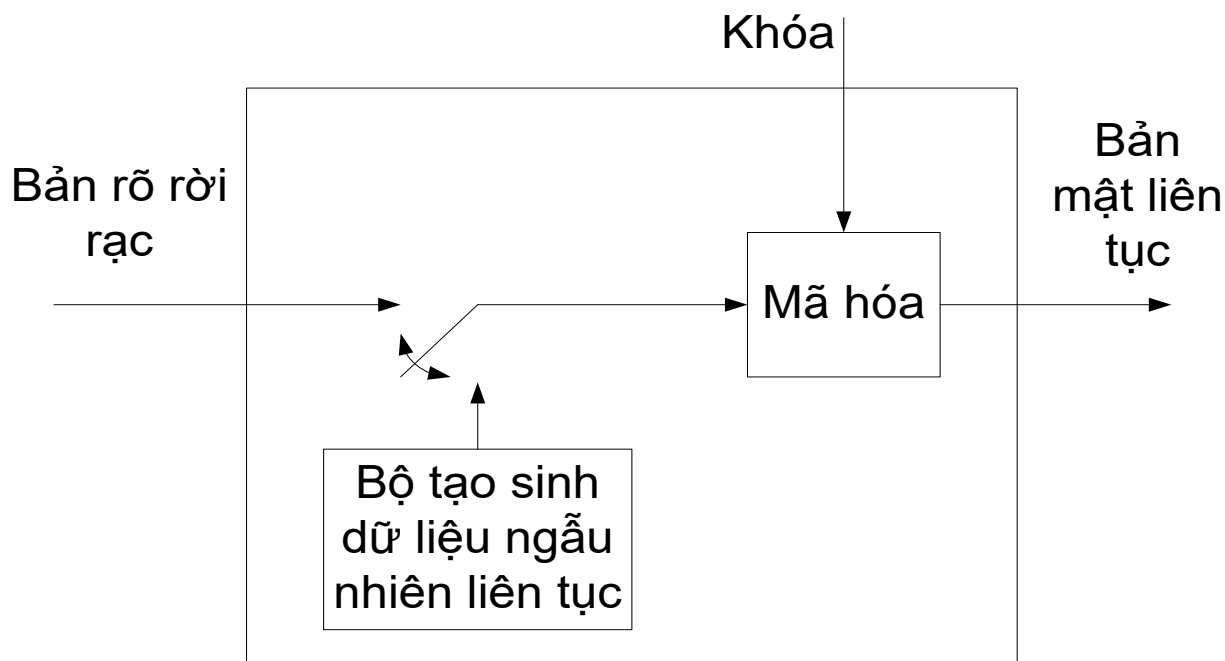
- Cơ chế bảo mật đường liên kết (link encryption approaches).
 - Mỗi đường truyền thông có thể bị tấn công đều được kết nối với các thiết bị mã hóa tại hai đầu \Rightarrow mọi quá trình truyền tải trên đường đều được bảo mật.
 - Nhược điểm:
 - Yêu cầu nhiều thiết bị mã hóa – giải mã đối với mạng lớn.
 - Thông điệp phải được giải mã mỗi khi đi vào bộ chuyển mạch gói bởi vì bộ chuyển mạch cần phải đọc địa chỉ (virtual circuit number) trong phần đầu gói tin để định tuyến cho gói.
 - Như vậy thông điệp là một điểm yếu tại mỗi bộ chuyển mạch. Do đó nếu phải làm việc với mạng công cộng, người sử dụng không thể kiểm soát được an toàn thông tin tại nút mạng.

Đảm bảo tính riêng tư với sơ đồ mã hoá đối xứng

- Cơ chế bảo mật đầu – cuối (end – to – end encryption approaches).
 - Quá trình mã hóa mật được thực hiện tại hai hệ thống đầu cuối. Máy trạm nguồn mã hóa thông tin và được truyền qua mạng tới trạm đích.
 - Trạm nguồn và trạm đích cùng chia sẻ khóa mật và do đó có thể giải mã thông điệp.
 - Dạng bảo mật này cho phép bảo đảm an toàn đối với các tấn công vào các điểm kết nối hoặc các điểm chuyển mạch.
 - Dạng bảo mật này cho phép người sử dụng yên tâm về mức độ an toàn của mạng và đường liên kết truyền thông.

Đảm bảo tính riêng tư với sơ đồ mã hoá đối xứng

- Thủ tục đệm luồng truyền tải:



Chương III. Các hệ mật khóa công khai

- Nguyên lý hệ mật khoá công khai
- Thuật toán RSA
- Quản lý khoá
- Sơ đồ trao đổi khoá Diffie-Hellman
- Một số hệ mật khóa công khai khác

Nguyên lý hệ mật khoá công khai

- Đặc điểm

- Mật mã công khai dựa trên cơ sở của các hàm toán học.
- Không dựa trên phép thay thế và đổi chỗ như trong phương pháp mã hoá đối xứng.
- Mã mật công khai là bất đối xứng.
 - Trong cơ chế mã mật khoá công khai sử dụng hai khoá: khoá mật và khoá công khai.
 - Các hệ quả của việc sử dụng hai khoá bất đối xứng: tính toàn vẹn, tính xác thực, phân phối khoá.

Nguyên lý hệ mật khoá công khai

- Xuất xứ:
 - Hệ mã mật khoá công khai được phát triển nhằm giải quyết hai vấn đề phức tạp nảy sinh từ phương pháp mã hoá đối xứng:
 - Vấn đề thứ nhất: bài toán phân phối khoá;
 - Vấn đề thứ hai: chữ ký số.

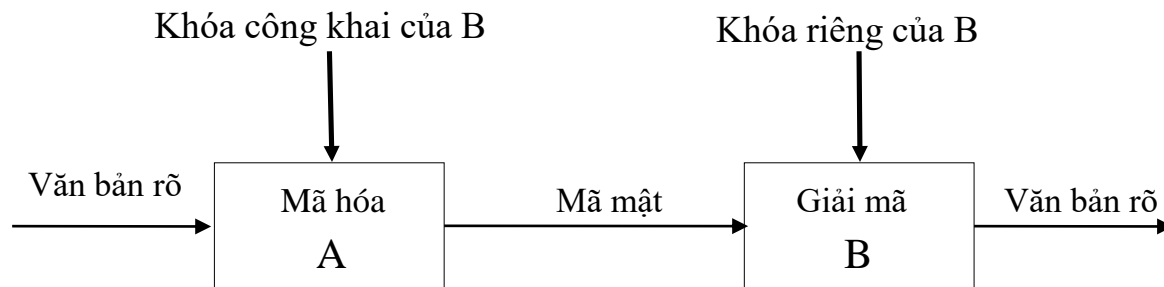
Nguyên lý hệ mật khoá công khai

- Hệ mật khoá công khai.
 - Sơ đồ mã mật khoá công khai sử dụng một khoá để mã hoá và một khoá khác có liên quan để giải mã. Các thuật toán mã hoá và giải mã có một số đặc điểm quan trọng sau:
 - Không thể xác định được khoá giải mã nếu chỉ biết thuật toán mã hoá và khoá mã hoá.
 - Một số hệ mã mật khoá công khai (như RSA) còn cung cấp khả năng sử dụng bất kỳ một khoá trong cặp khoá làm khoá mã hoá thì khoá còn lại sẽ được dùng làm khoá giải mã.

Nguyên lý hệ mật khoá công khai

– Sơ đồ mã hoá công khai:

- A và B có các cặp khóa (K_{RA}, K_{PA}) , (K_{RB}, K_{PB}) . Các khóa này dùng để mã hoá và giải mã các thông điệp.
- A và B công bố khoá công khai K_{PA} , K_{PB} trong cặp khóa, khoá còn lại được giữ mật.
- Khi gửi thông điệp cho B, A sẽ mã hoá văn bản bằng khoá công khai K_{PB} của B.
- Khi nhận được thông điệp, B sẽ giải mã bằng khoá mật K_{RB} . Bên thứ ba không giải mã được thông điệp vì chỉ có B biết khoá mật K_{RB} của B.

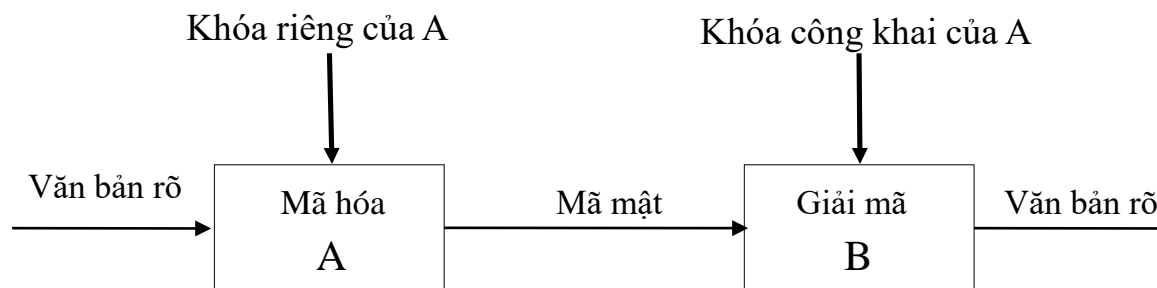


Đảm bảo tính mật

Nguyên lý hệ mật khoá công khai

– Sơ đồ xác thực:

- Nếu A muốn gửi thông điệp được xác thực cho B, A sẽ mã hoá văn bản bằng khoá riêng của A.
- Khi B nhận được thông điệp, B sẽ giải mã bằng khoá công khai của A. Không một bên thứ ba có thể giải mã được thông điệp vì chỉ có B biết khoá mật của B.



Đảm bảo tính xác thực

Nguyên lý hệ mật khoá công khai

- Các yêu cầu đối với hệ mật khoá công khai
 - Quá trình sinh cặp khóa K_P , K_R là dễ trên phương diện tính toán;
 - Quá trình mã hóa bản tin bằng khóa công khai K_P ở bên gửi là dễ:
$$Y = E_{K_P}(M);$$
 - Quá trình giải mã ra văn bản rõ khi biết khóa riêng K_R và bản tin mật Y là dễ:
$$M = D_{K_R}(Y);$$
 - Đối với thám mã, nếu chỉ biết K_P sẽ rất khó trên phương diện tính toán để tính ra K_R ;
 - Đối với thám mã, nếu chỉ biết K_P và bản tin mật Y sẽ rất khó trên phương diện tính toán để tính ra bản tin rõ M ;
 - Nguyên lý đối xứng: quá trình mã hóa – giải mã có thể áp dụng theo hai chiều: $M = D_{K_P}[E_{K_R}(M)]$

Nguyên lý hệ mật khoá công khai

- Các ứng dụng của hệ mật khoá công khai
 - Ứng dụng trong mật mã – mã hóa, giải mã (RSA):
 - Bên gửi mã hóa bằng khóa công khai của bên nhận;
 - Bên nhận giải mã bằng khóa riêng.
 - Ứng dụng trong phân phối khóa (RSA, Diffie-Helman): duy trì kênh mật phân phối khóa đối xứng bằng cơ sở mã mật công khai;
 - Ứng dụng trong chữ ký số (RSA, DSS):
 - Bên gửi ký bằng khóa riêng.
 - Bên nhận xác thực chữ ký bằng khóa công khai của bên gửi.

Thuật toán mã hoá công khai RSA

- Cơ sở lý thuyết số
- Sơ đồ thuật toán
- Thăm mã RSA

Sơ đồ thuật toán RSA

- Xuất xứ
 - RSA do Ron Rivest, Adi Shamir và Len Adlenman phát minh năm 1977;
 - Hệ thống mã khoá công khai phổ biến và đa năng:
 - Được sử dụng trong các ứng dụng mã hóa/giải mã;
 - Chứng thực;
 - Phân phối và trao đổi khoá.

Sơ đồ thuật toán RSA

- Thuật toán RSA:
 - Phương pháp mã hóa khối;
 - Văn bản rõ và văn bản mật là các số nguyên có giá trị từ 0 đến $n-1$, n – số nguyên lớn;
 - Mỗi khối có giá trị nhỏ hơn n .
 - Kích thước của khối (số bit) nhỏ hơn hoặc bằng $\log_2(n)$.
 - Thực tế, kích thước của khối là k bit với
$$2^k < n \leq 2^{k+1}.$$

Sơ đồ thuật toán RSA

- Cặp khóa: (e, d)
- Mã hoá

Bản rõ	$M < n$
Mã mật	$C = M^e \bmod n$

- Giải mã

Mã mật	C
Bản rõ	$M = C^d \bmod n = (M^e)^d \bmod n$

Sơ đồ thuật toán RSA

- Bên gửi và bên nhận phải biết số n .
- Bên gửi biết khóa công khai là cặp (e, n) .
- Bên nhận có khóa riêng là cặp (d, n) .
- Các yêu cầu:
 - Có thể tìm được các số e, d, n sao cho:
$$M^{ed} = M \bmod n \quad \forall M < n.$$
 - Thực hiện tính M^e và C^d một cách đơn giản $\forall M < n$.
 - Không thể xác định được d nếu biết e và n

Sơ đồ thuật toán RSA

- Tạo khoá

- Tìm các số e, d sao cho:

$$M^{ed} = M \bmod n$$

- Hệ quả của định lý Euler: cho p và q là số nguyên tố, n và m là hai số nguyên sao cho: $n=pq$ và $0 < m < n$, k là số nguyên bất kỳ. Đẳng thức sau nghiệm đúng:

$$m^{k\phi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n$$

- Như vậy: $ed = k\phi(n)+1$, tức là:
- $ed \equiv 1 \bmod \phi(n)$ hay $d \equiv e^{-1} \bmod \phi(n)$ có nghĩa là $\gcd(\phi(n), d) = 1$ và $\gcd(\phi(n), e) = 1$

Sơ đồ thuật toán RSA

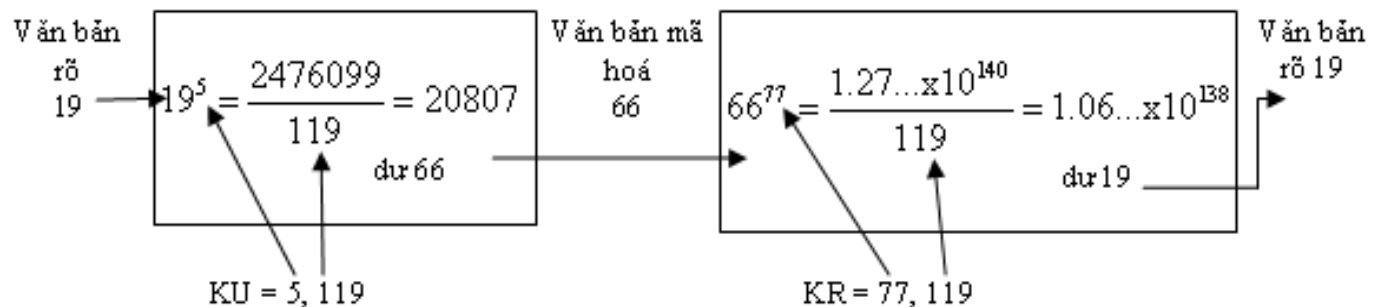
– Sơ đồ tạo khóa RSA

Chọn p, q	p và q là số nguyên tố
Tính $n = p \times q$	
Tính $\phi(n) = (p - 1)(q - 1)$	
Chọn số nguyên e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Tính d	$d \equiv e^{-1} \pmod{\phi(n)}$
Khoá công khai	$KU = [e, n]$
Khoá mật	$KR = [d, n]$

Sơ đồ thuật toán RSA

– Ví dụ

- $p = 7, q = 17$
- $n = pq = 119; \phi(n) = (p-1)(q-1) = 96$
- Chọn e nguyên tố cùng nhau với $\phi(n)$, nhỏ hơn $\phi(n)$,
 - Chọn $e = 5$;
- Tìm d : $d \equiv e^{-1} \pmod{\phi(n)}$
 - $d = 77 \Rightarrow$ cặp khóa: $e = (5, 119); d = (77, 119)$



Sơ đồ thuật toán RSA

- Mã hoá và giải mã
 - Vấn đề trong thuật toán mã hoá và giải mã RSA là việc thực hiện phép toán lũy thừa và phép toán đồng dư với số nguyên lớn.
 - Giải quyết dựa trên tính chất của phép toán modun:
 $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$
 - Tính a^m với m lớn.
 - Biểu diễn nhị phân của $m = b_k b_{k-1} \dots b_0 = \sum_{b_i \neq 0} 2^i$
 - Do đó:

$$a^m = a^{\left(\sum_{b_i \neq 0} 2^i\right)} = \prod_{b_i \neq 0} a^{2^i}$$

$$a^m \bmod n = \prod_{b_i \neq 0} a^{2^i} \bmod n = \prod_{b_i \neq 0} (a^{2^i} \bmod n)$$

Sơ đồ thuật toán RSA

- Sinh khoá

- Các bước quan trọng trong tạo khoá:
 - Xác định 2 số nguyên tố p và q . Để tránh tấn công vét cạn, p và q phải lớn.
 - Xác định e và d
- Xác định số nguyên tố p, q (sử dụng thuật toán Miller – Rabin)
 1. Chọn một số nguyên lẻ n ngẫu nhiên (sử dụng bộ sinh số giả ngẫu nhiên).
 2. Chọn một số nguyên $a < n$ ngẫu nhiên.
 3. Thực hiện thuật toán xác suất để kiểm tra số nguyên tố. Nếu n test thành công thì loại bỏ giá trị n và quay lại bước 1.
 4. Nếu n test thành công với số lượng test đủ, chấp nhận n ; mặt khác, quay lại bước 2.
- Chọn e và tính d từ e và $\phi(n)$ (sử dụng thuật toán Euclid)

Thăm mã RSA

- Tấn công vét cạn: thử vét cạn toàn bộ không gian khóa riêng.
- Tấn công toán học: thực hiện bài toán phân tích số nguyên thành tích hai số nguyên tố.
- Tấn công dựa vào thời gian: dựa vào thời gian để thực hiện thuật toán giải mã.

Thăm mã RSA - tấn công vét cạn

- Phương pháp: thực hiện vét cạn toàn bộ không gian khoá.
- Biện pháp đối phó:
 - Sử dụng không gian có khoá kích thước lớn, tức là tăng số bit của d và e .
 - Không gian khóa có kích thước lớn sẽ làm quá trình sinh khóa, mã hoá, giải mã thực hiện chậm đi.

Thăm mã RSA - Tấn công toán học

- Các phương pháp tấn công toán học vào RSA:
 - Phân tích n thành tích hai số nguyên tố p và q ;
 - Sau đó cho phép tính $\phi(n)=(p-1)(q-1)$;
 - Từ $\phi(n)$ có thể tính $d=e^{-1} \bmod \phi(n)$.
 - Xác định $\phi(n)$ trực tiếp không qua p và q ;
 - Cho phép từ $\phi(n)$ có thể tính $d=e^{-1} \bmod \phi(n)$.
 - Xác định trực tiếp d không qua tính $\phi(n)$.

Thăm mã RSA - Tấn công toán học

- Trường hợp đơn giản nhất là người thăm mã biết được $\phi(n)$
- Phân tích n thành tích của 2 thừa số nguyên tố: Có nhiều thuật toán phân tích n thành hai thừa số nguyên tố.
 - Có ba thuật toán hiệu quả trên các số rất lớn:
 - Thuật toán sàng bình phương (quadratic sieve),
 - Đường cong elip (elliptic curve) và
 - Sàng trường số.
 - Các thuật toán được biết đến nhiều trước đây:
 - Thuật toán $p - 1$ của Pollard,
 - Thuật toán $p + 1$ của William,
 - Thuật toán chia nhỏ liên tiếp
 - Thuật toán chia thử.

Thám mã RSA - Tấn công toán học

- Những yêu cầu đối với p và q :
 - p và q chỉ nên khác nhau về độ dài khoảng vài hàng số nhị phân và trong khoảng từ 10^{75} đến 10^{100} ;
 - $(p-1)$ và $(q-1)$ phải có những thừa số nguyên tố lớn;
 - $\text{Gcd}(p-1, q-1)$ phải nhỏ.
 - Thực tế cho thấy, nếu $e < n$ và $d < n^{1/4}$ thì d có thể dễ dàng tính được!

Thăm mã RSA - Tấn công dựa thời gian

- Nội dung của phương pháp này dựa vào việc theo dõi thời gian thực hiện thuật toán giải mã;
 - Có thể áp dụng đối với những hệ mật khóa công khai khác!
 - Là dạng tấn công chỉ sử dụng mã mật (ciphertext only attack)
- Biện pháp đối phó:
 - Thời gian tính mũ là hằng: Làm cho thời gian tính mũ là như nhau trước khi trả về kết quả. Biện pháp này đơn giản nhưng làm giảm hiệu năng.
 - Thực hiện trễ ngẫu nhiên: Thêm các trễ thời gian ngẫu nhiên vào thuật toán mũ hoá.
 - Làm mù: Nhân văn bản mật với một số ngẫu nhiên trước khi thực hiện mũ hoá. Khi đó thám mã sẽ không biết bit nào của mã mật được xử lý và do đó ngăn chặn được quá trình phân tích mã mật.

Quản lý khóa trong sơ đồ mật mã khóa công khai

- Các mô hình quản lý khóa
 - Bài toán phân phối khóa: tập trung xây dựng kênh mật phân phối khóa phiên bí mật.
 - Hai hướng sử dụng mật mã khóa công khai:
 - Phân phối khóa công khai;
 - Sử dụng mã hóa khóa công khai để phân phối khóa phiên

Phân phối khóa công khai

- Các mô hình
 - Công bố công khai
 - Công bố thư mục công khai
 - Trung tâm ủy quyền khóa công khai
 - Chứng thư khóa công khai

Phân phối khóa công khai

- Công bố công khai
 - Các bên tham gia trao đổi thông tin tự công bố khóa công khai;
 - Điểm mạnh: đơn giản.
 - Điểm yếu:
 - Một người thứ 3 có thể giả mạo khóa công khai;
 - Bên C giả mạo bên nhận tin B, gửi khóa công khai của mình K_{PC} cho A;
 - A mã hóa các bản tin gửi cho B bằng khóa K_{PC} của C;
 - B không đọc được bản tin A gửi
 - C có thể đọc được bản tin A gửi B

Phân phối khóa công khai

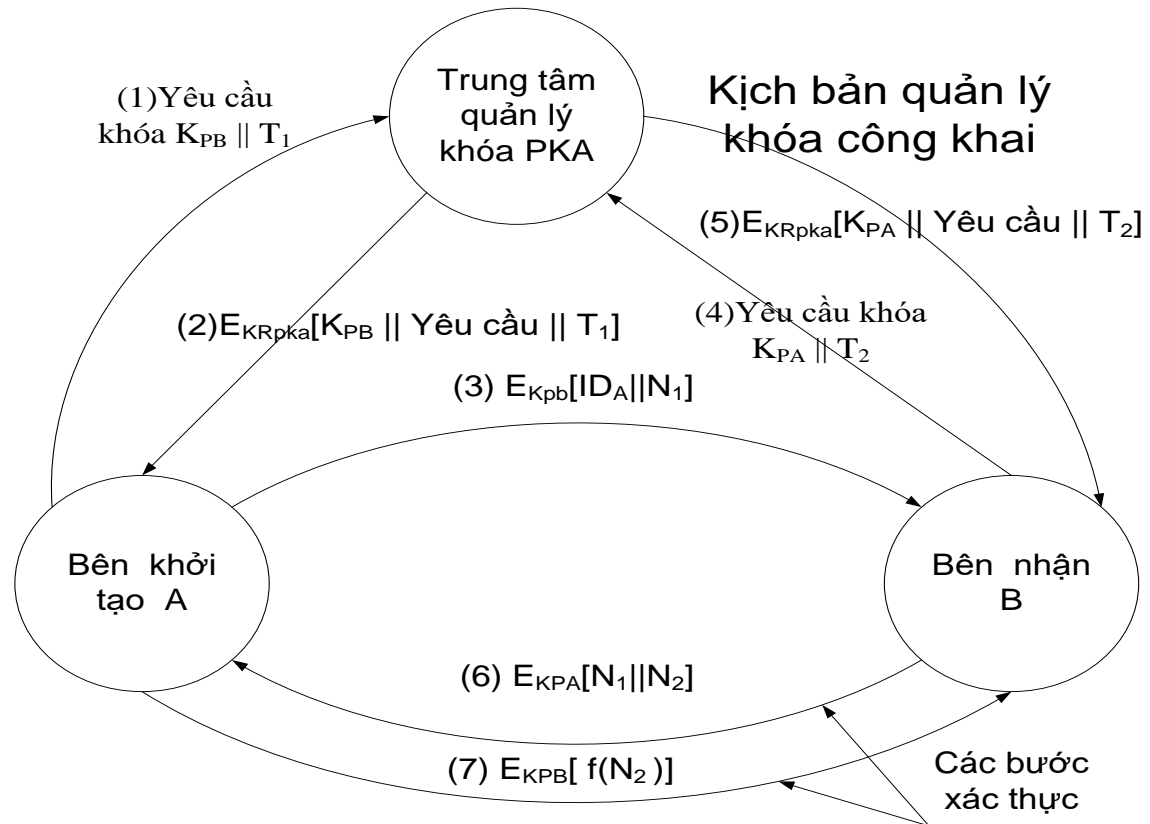
- Quản lý thư mục khóa công khai
 - Có bên thứ ba C được ủy quyền quản lý khóa công khai;
 - Bên thứ ba C tạo cho mỗi bên tham gia trao đổi thông tin một thư mục lưu trữ khóa;
 - Các bên đăng ký và gửi khóa công khai tới C. Quá trình đăng ký có thể thực hiện trên kênh bảo mật.
 - Các bên có thể thay thế khóa công khai theo nhu cầu
 - Khi đã sử dụng khóa nhiều lần để mã hóa lượng dữ liệu lớn;
 - Khi khóa riêng cần phải thay thế

Phân phối khóa công khai

- Bên C định kỳ công bố toàn bộ thư mục khóa hoặc cập nhật;
- Các bên có thể truy cập thư mục khóa qua các kênh bảo mật.
 - Vấn đề xác thực đối với bên thứ ba C.
- Điểm yếu:
 - Nếu thám mã biết được khóa riêng của C
 - Toàn bộ các khóa công khai được lưu trữ có thể bị giả mạo.
 - Có thể nghe trộm các thông điệp do các bên trao đổi .

Phân phối khóa công khai

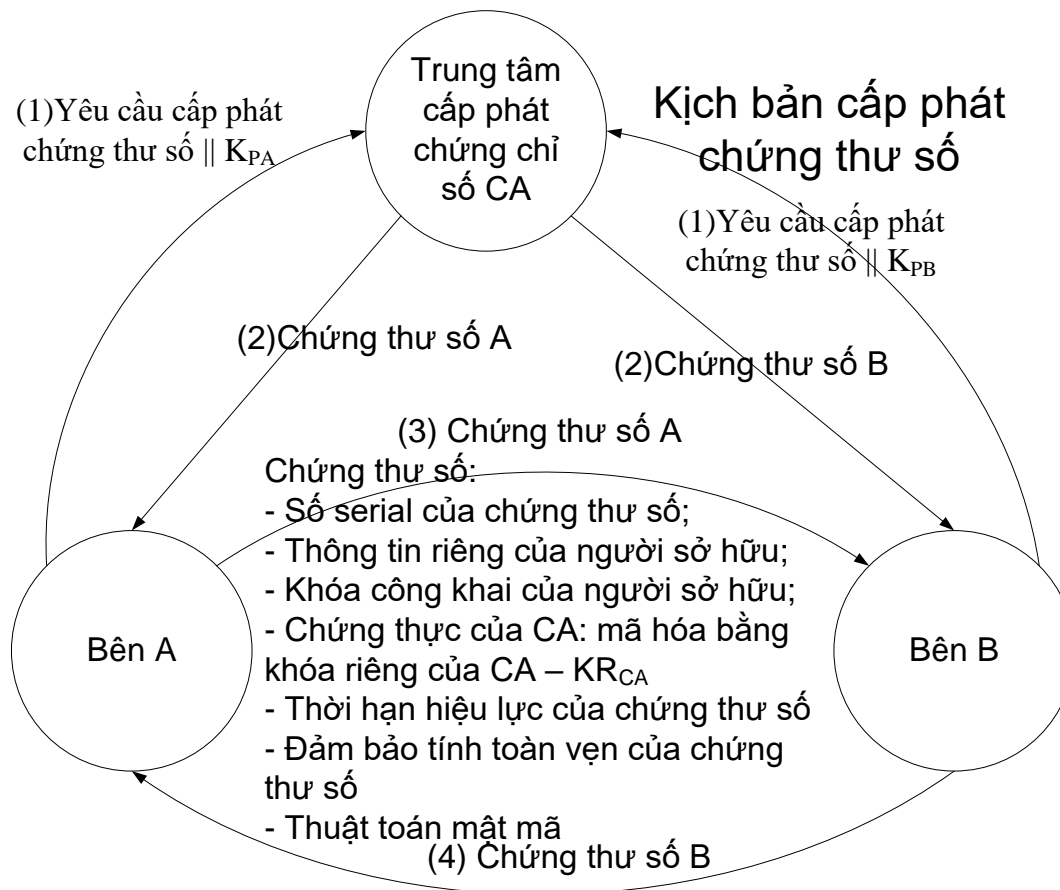
- Ủy quyền khóa công khai
 - Bên thứ ba được ủy quyền PKA tham gia lưu giữ khóa;
 - Các bên A, B biết khóa công khai của PKA;



Phân phối khóa công khai

- Chứng chỉ khóa công khai
 - Trung tâm cấp phát chứng thư số CA;
 - Chỉ cần xác nhận khóa công khai một lần;
 - Không cần truy cập CA mỗi khi cần khóa công khai;
 - Khóa công khai sẽ do các bên tự quản lý;
 - Sơ đồ hoạt động:
 - Các bên gửi khóa công khai tới CA để chứng thực;
 - Nhận chứng thư số từ CA kèm thời gian hiệu lực;
 - Các bên xuất trình chứng thư số trong các giao dịch;

Phân phối khóa công khai



Phân phối khóa mật đối xứng sử dụng mã hóa công khai

- Sơ đồ đơn giản:
 - A gửi B: $K_{PA} \parallel ID_A$
 - B tạo khóa phiên K_S và gửi lại A: $E_{KPA}(K_S)$
- Sơ đồ kèm xác thực
 - A gửi B: $E_{KPB}(N_1 \parallel ID_A)$
 - B gửi A: $E_{KPA}(N_1 \parallel N_2)$
 - A gửi B: $E_{KPB}(N_2)$
 - A gửi B: $E_{KPB}(E_{KRA}(K_S))$

Lý thuyết số

- Số học modun
- Định lý Euler và định lý Fermat
- Kiểm tra số nguyên tố
- Thuật toán Euclid
- Định lý số dư Trung Hoa
- Sinh giả ngẫu nhiên các số nguyên lớn

Hệ mật Diffie-Hellman

- Các sơ đồ quản lý khoá của hệ mật khoá công khai
 - Quản lý và chứng thực khoá công khai;
 - Cấp phát chứng thư số;
 - Trao đổi khoá mã hoá-giải mã của hệ mật khoá đối xứng:
 - Xây dựng kênh truyền bí mật để trao đổi phiên.
 - Dùng cơ chế bảo mật của hệ mật khoá công khai;

Nguyên lý trao đổi khóa Diffie-Hellman

- Được Diffie-Hellman đưa ra vào 1976
- Là sự kết hợp của hai mô hình xác thực và mật của hệ KCK
- Việc sinh ra các cặp khoá là hoàn toàn khác nhau đối với người sử dụng
- Sử dụng cơ chế trao đổi khoá trực tiếp không qua trung gian xác thực

Nguyên lý trao đổi khóa Diffie-Helman

- Sử dụng trong các ứng dụng trao đổi khóa khi sử dụng hệ mật khóa đối xứng.
- Nguyên tắc: hai người sử dụng có thể trao đổi khóa phiên an toàn - được dùng để mã hoá và giải mã các thông điệp;
- Thuật toán tự giới hạn chỉ dùng cho các ứng dụng sử dụng kĩ thuật trao đổi khóa;

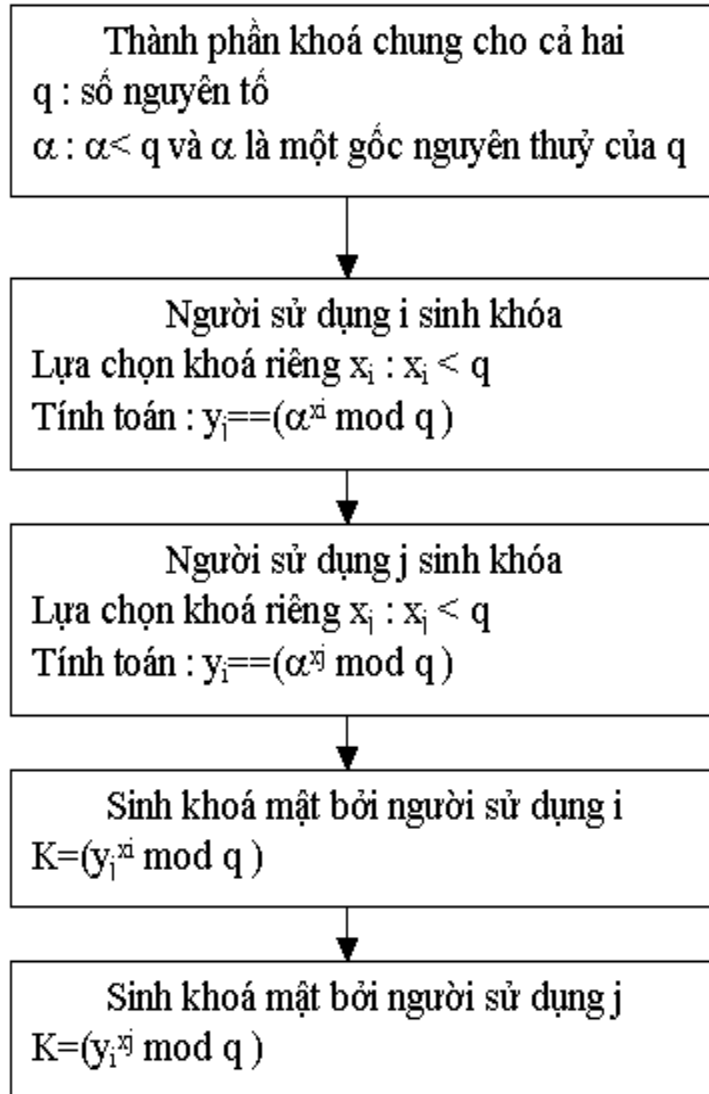
Cơ sở hình thành thuật toán

- Nguyên tắc toán học :
 - m là một số nguyên tố;
 - $y = a^i \bmod m$ là bài toán dễ;
 - Bài toán ngược là bài toán khó. Đặc biệt với m lớn.
- Dựa trên phép tính logarit rời rạc

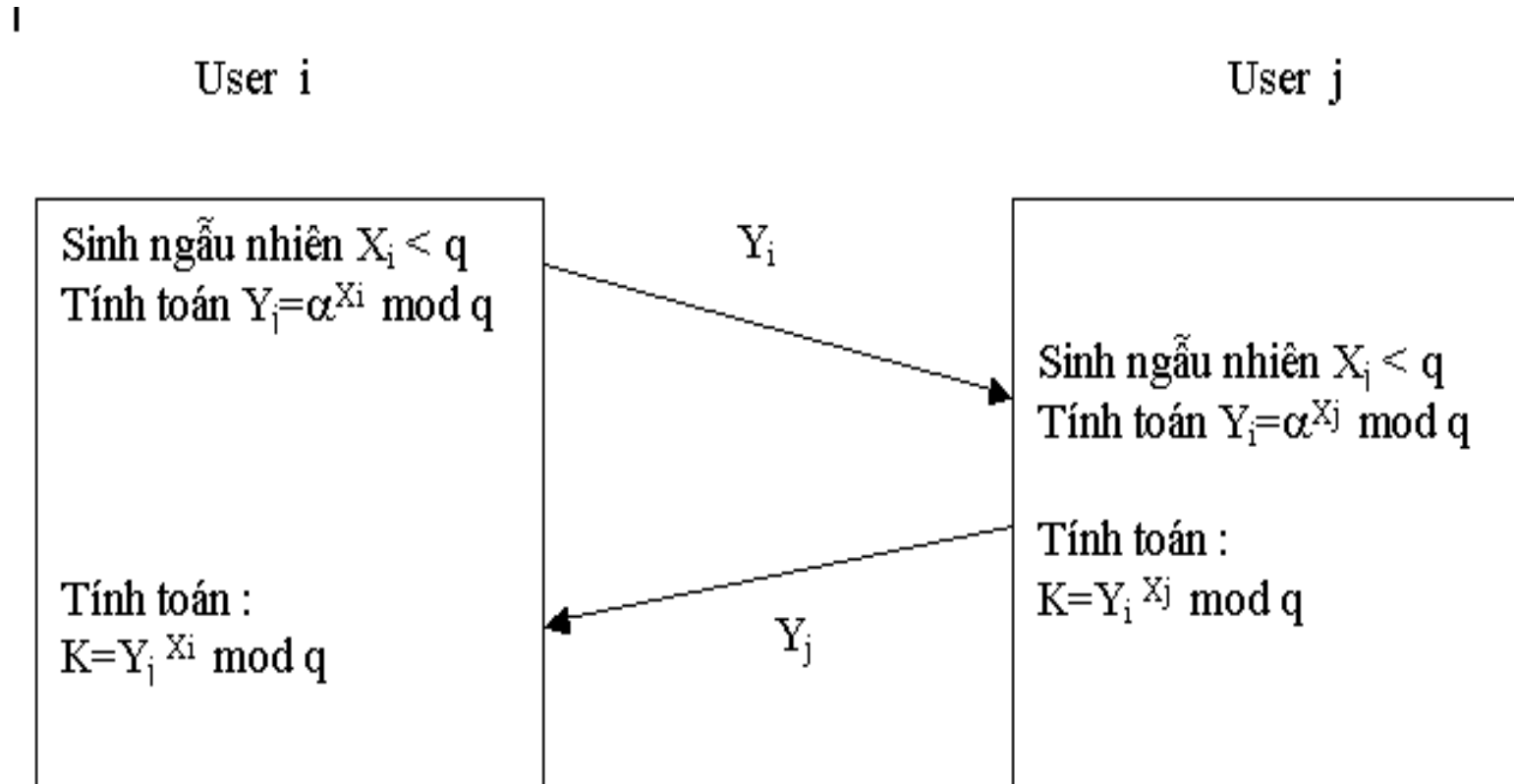
Thuật toán logarit rời rạc

- Thuật toán logarit rời rạc:
 - Một số nguyên tố p ;
 - Một gốc nguyên thủy a của p : là các số mà lũy thừa của a theo modul p thuộc $(1, p-1)$
 - Với b bất kì nguyên sẽ luôn $\exists i$ sao cho $b = a^i \bmod p$.

Thuật toán Diffie-Hellman



Thuật toán trao đổi khoá



Tính bảo mật của hệ mật

- Thám mã có sẵn các thông tin : p, a, Y_i, Y_j
- Để có thể giải được K, X bắt buộc thám mã phải sử dụng thuật toán logarit rời rạc : rất khó nếu p lớn
- Vì thế nên chọn p càng lớn càng tốt : như thế thì việc tính toán ra X coi như không thể

Hệ mật và thám mã

- Thám mã có thể tấn công vào các thông tin : p, a, Y_j, Y_j
- Và sử dụng thuật toán rời rạc để tính ra X , sau đó tính ra K
- Quan trọng nhất là độ phức tạp của thuật toán logarit phụ thuộc vào chọn số nguyên tố p
- Tấn công man in the middle

Lĩnh vực ứng dụng

- Tự quá trình thuật toán đã hạn chế ứng dụng chỉ sử dụng cho quá trình trao đổi khoá mật là chủ yếu
- Sử dụng trong chữ kí điện tử.
- Các ứng dụng đòi hỏi xác thực người sử dụng.

Bài toán xác thực



Nội dung

- Bài toán xác thực.
- Tấn công vào hệ xác thực
- Các phương pháp xác thực thông điệp
 - Mã xác thực thông điệp
 - Hàm băm
- Chữ ký số

Bài toán xác thực

- Các yêu cầu của bài toán xác thực
 - Điềm lại các dạng tấn công
 - Tấn công vào tính riêng tư:
 - Giải mật: giải mật nội dung thông điệp.
 - Phân tích luồng truyền tải: xác định mẫu thông điệp, xác định tần suất trao đổi thông điệp, định vị, xác định chức năng các trạm, định vị
 - Dạng tấn công thụ động.
 - Đảm bảo tính riêng tư: ngăn chặn bằng mật mã và làm nhiễu thông tin.

Bài toán xác thực

- Tấn công vào tính xác thực:
 - Trá hình: đưa ra các thông điệp vào hệ thống với tên giả mạo.
 - Thay đổi nội dung thông điệp: phá huỷ tính toàn vẹn.
 - Thay đổi trình tự trao đổi thông điệp: tấn công vào giao thức.
 - Thay đổi theo tiến trình thời gian: làm trễ hoặc phát lại thông điệp.
 - Từ chối dịch vụ: từ chối gửi hoặc nhận thông điệp: sử dụng chữ ký điện tử.
 - Xác thực:
 - Xác thực các bên trao đổi thông điệp.
 - Làm rõ nguồn gốc thông điệp.
 - Xác định tính toàn vẹn thông điệp – xác thực nội dung
 - Xác thực phiên làm việc
 - Chống phủ nhận.

Bài toán xác thực

- Các tiêu chuẩn xác thực
 - Xác thực chủ thể tham gia vào trao đổi thông tin
 - Thông điệp có nguồn gốc;
 - Nội dung thông điệp toàn vẹn, không bị thay đổi trong quá trình truyền tin (xác thực nội dung thông điệp);
 - Thông điệp được gửi đúng trình tự và thời điểm (xác thực phiên);
- Mục đích của bài toán xác thực:
 - Chống lại các tấn công chủ động:
 - Chống giả mạo;
 - Thay đổi nội dung dữ liệu;
 - Thay đổi trình tự trao đổi thông tin (hoạt động của các giao thức).
- Các phương pháp xác thực và chống giả mạo:
 - Mã hoá thông điệp;
 - Sử dụng mã xác thực thông điệp;
 - Sử dụng hàm băm;
 - Sử dụng các giao thức xác thực

Bài toán xác thực

- Các hàm xác thực
 - Các cơ chế xác thực được thực hiện trên hai mức:
 - Mức thấp: trong hệ thống phải có các hàm chức năng cho phép kiểm tra tính xác thực của chủ thể và thông điệp:
 - Hàm tạo các giá trị đặc trưng xác thực chủ thể và thông điệp.
 - Mức cao:
 - Sử dụng các hàm xác thực trong các giao thức xác thực.
 - Cho phép thẩm định tính xác thực của chủ thể và thông điệp.

Bài toán xác thực

- Các dạng hàm xác thực:
 - Mã hoá thông điệp: sử dụng hàm mã hoá để xác thực dựa vào việc sở hữu khoá bí mật.
 - Mã xác thực thông điệp: tạo ra mã xác thực thông điệp độ dài cố định bằng phương pháp mã hoá.
 - Hàm băm xác thực thông điệp: tạo mã băm của thông điệp với độ dài cố định.
 - Chữ ký số: tạo dấu hiệu đặc trưng xác định duy nhất chủ thể.
 - Các phương pháp tạo sinh các dấu hiệu xác thực
 - Các giao thức xác thực

Tấn công vào hệ xác thực

Xác thực và xác thực hoàn hảo

- Vấn đề giả mạo và xác thực

- Vấn đề: tồn tại hay không phương pháp xác thực hoàn hảo chống lại giả mạo !?

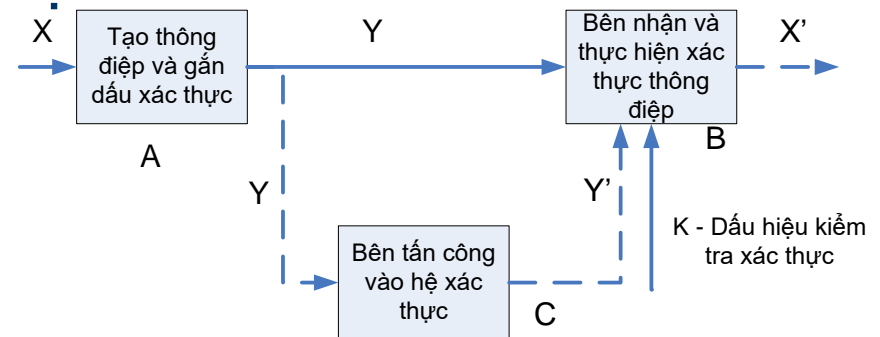
- Các kịch bản tấn công vào hệ xác thực:

- Kịch bản 1:

- A tạo bản tin X, gắn dấu hiệu xác thực, được bản tin Y và gửi Y cho B

- Kịch bản 2:

- Giữa A và B không có phiên làm việc.
- C tạo ra văn bản Y' , giả mạo A và gửi cho B



Lý thuyết xác thực Simmons

Xác thực và xác thực hoàn hảo

- Xác suất tấn công giả mạo
 - P_s : xác suất tấn công thành công bằng thay thế;
 - P_i : xác suất tấn công thành công bằng mạo danh;
 - Xác suất giả mạo thành công: $P_D = \max(P_i, P_s)$
 - Khoá K : thông tin tham gia vào quá trình xác thực
 - N_X : số lượng thông điệp gốc X_i sao cho
$$P\{X = X_i\} \neq 0$$
 - N_K : số lượng các dấu hiệu xác thực K_L : $P\{K = K_L\} \neq 0$
 - N_Y : số lượng văn bản được gán dấu hiệu xác thực Y_j , sao cho $P\{Y = Y_j\} \neq 0$

Xác thực bằng cách mã hoá

- Sử dụng phương pháp mật mã khoá đối xứng
 - Thông điệp gửi từ đúng nguồn vì chỉ có người gửi biết khoá bí mật dùng chung
 - Nội dung không thể bị thay đổi vì văn bản rõ có cấu trúc nhất định
 - Các gói tin được đánh số thứ tự và có mã hoá nén không thể thay đổi trình tự và thời điểm nhận được
- Sử dụng phương pháp mật mã khoá công khai
 - Không chỉ xác thực thông điệp mà còn tạo chữ ký số
 - Phức tạp và mất thời gian hơn mã hoá đối xứng

Xác thực bằng phương pháp mã hóa

- Xác thực: chống giả mạo
 - Xây dựng các dấu hiệu đặc trưng cho đối tượng cần xác thực:
 - Đối tượng cần xác thực:
 - Chủ thể tham gia vào quá trình trao đổi thông tin: nguồn gốc thông tin từ các nguồn được xác thực.
 - Nội dung thông tin trao đổi: không bị sửa đổi trong quá trình trao đổi – tính nguyên bản của thông tin.
 - Xác thực phiên trao đổi thông tin: giao thức trao đổi, trật tự hoạt động của giao thức, thời gian trao đổi thông tin, dấu hiệu phiên.
 - Dấu hiệu: dùng các phương pháp mã hóa để tạo dấu hiệu xác thực: dùng các thuật toán mật mã.

Xác thực bằng phương pháp mã hóa

- Quá trình xác thực
 - Tạo dấu hiệu đặc trưng từ đối tượng.
 - Bằng cách sử dụng các phương pháp mật mã.
 - Tính bền vững của dấu hiệu: khi thay đổi nội dung cần xác thực hoặc thay đổi dấu hiệu: hệ thống xác thực phát hiện dễ dàng.
 - Dấu hiệu được gắn kèm đối tượng trong quá trình trao đổi thông tin
 - Bên nhận sẽ tính toán lại dấu hiệu từ nội dung thông tin
 - So sánh dấu hiệu vừa tính được với dấu hiệu gửi kèm.
 - Nếu trùng khớp: dấu hiệu được xác thực; Ngược lại: không được xác thực.

Xác thực dùng mã xác thực thông điệp (MAC - checksum)

- Dùng mã xác thực thông điệp (MAC Message Authentication Code)
- Là khối có kích thước nhỏ cố định gắn vào thông điệp tạo ra từ thông điệp đó và khóa bí mật chung
- Bên nhận thực hiện cùng giải thuật trên thông điệp và khoá để so xem MAC có chính xác không
- Giải thuật tạo MAC giống giải thuật mã hóa nhưng không cần giải mã

Xác thực dùng mã xác thực thông điệp (MAC - checksum)

- $MAC = C_K(M)$
 - M: là bản tin
 - K: là khoá mật được chia sẻ chỉ bởi người gửi và người nhận;
 - $C_K(M)$: là một hàm xác thực, cho kết quả là một chuỗi ký tự có độ dài cố định;

Xác thực dùng mã xác thực thông điệp (MAC - checksum)

- Có thể có nhiều thông điệp có cùng chung MAC
 - Nhưng nếu biết 1 thông điệp và MAC, rất khó tìm ra một thông điệp khác cùng MAC
 - Các thông điệp có cùng xác suất tạo ra MAC
- Đáp ứng 3 tiêu chuẩn xác thực

Mã hoá bản tin và cách tấn công của đối phương

- Mã hoá bản tin
 - Đối xứng
 - Không đối xứng
- Sự an toàn của thuật toán phụ thuộc độ dài bit của khoá
- Với 1 lần tấn công
 - 2^k lần thử cho khoá k bit

Mã hoá bản tin và cách tấn công của đối phương

- Ví dụ tấn công
 - Đối phương biết bản mật C (Ciphertext)
 - $P_i = D_{K_i}(C)$ cho tất cả khoá K_i
 - Đến khi P_i khớp với bản rõ P (Plaintext)
- Đối với CheckSum
 - MAC n bit $\rightarrow 2^n$ CheckSum tạo ra
 - N bản tin áp dụng ($N \gg 2^n$)
 - Khóa K bit $\rightarrow 2^k$ khóa tạo ra

Ví dụ tấn công vào MAC

- Giả sử: $\text{size}(K) > \text{size}(\text{MAC})$ ($k > n$)
- Match (so khớp): là bản M_i tạo ra gần khớp với bản M_1
- Dùng cách tấn công vét cạn (brute-force)

Ví dụ tấn công vào MAC

- Tấn công MAC bằng cách lặp lại:
 - Vòng 1:
 - Cho: M_1 , $MAC_1 = C_K(M_1)$
 - Tính: $M_i = C_{K_i}(MAC_1)$ cho tất cả khoá
 - Số các so khớp tạo ra $\approx 2^{k-n}$
 - Vòng 2:
 - Cho: M_2 , $MAC_2 = C_K(M_2)$
 - Tính $M_i = C_{K_i}(MAC_2)$ cho khoá còn lại.
 - Số cách so khớp tạo ra $\approx 2^{k-2n}$
 - ...

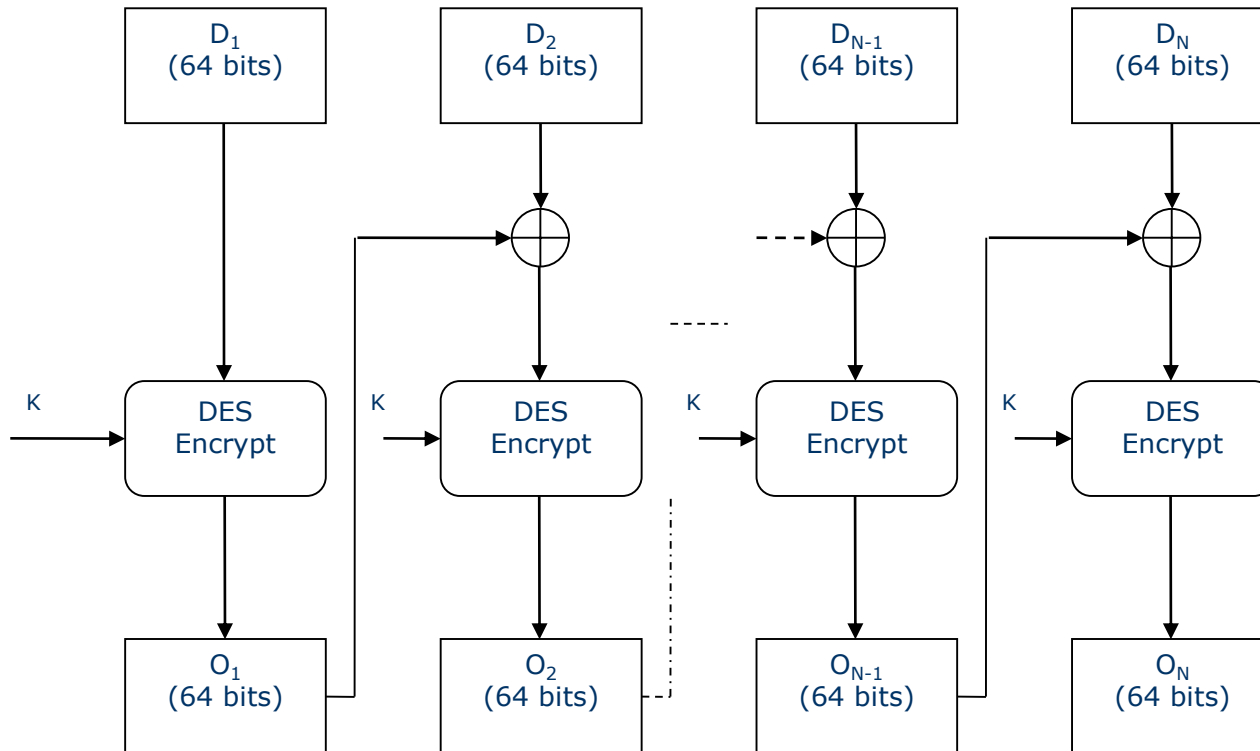
Ví dụ tấn công vào MAC

- Kết quả:
 - Nếu $k = a \cdot n \rightarrow$ mất a vòng để tìm ra
 - Nếu $k < n$ thì ngay vòng 1 tạo ra luôn sự so khớp.
 - Ví dụ
 - Nếu một khoá kích thước $k=80$ bit
 - CheckSum kích thước là $n=32$ bit
 - Thì vòng 1 sẽ tạo ra khoảng 2^{48} khóa Vòng 2 sẽ thu hẹp xuống còn 2^{16} khóa
 - Vòng 3 sẽ tạo chỉ 1 khoá đơn, và đó chính là khoá được dùng bởi người gửi.

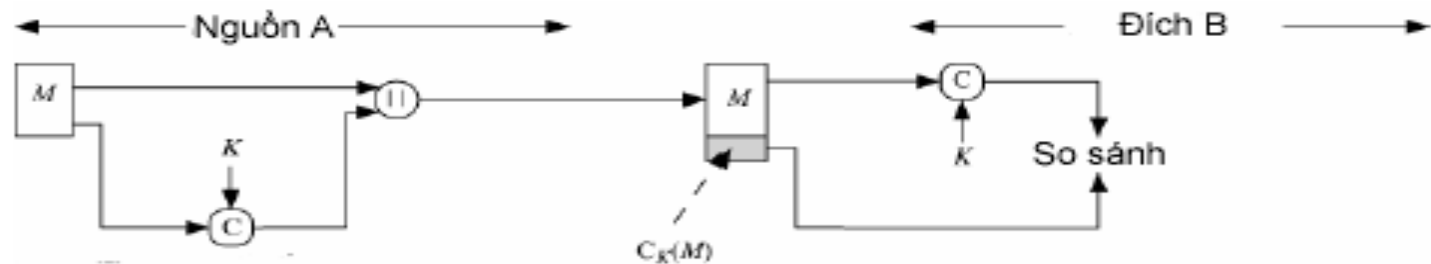
Ví dụ tấn công vào MAC

- Tồn tại khả năng có nhiều khoá thoả mãn việc so khớp
 - ⇒ Đối phương có thể thực hiện cùng một kiểm tra trên một cặp(bản tin,Checksum) mới.

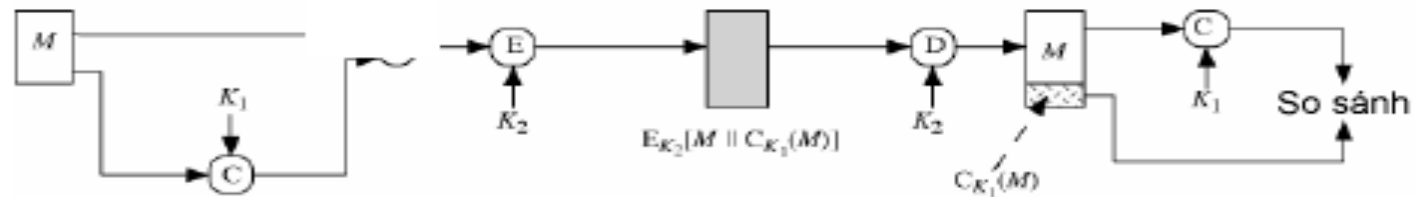
Mật mã CheckSum dựa trên DES



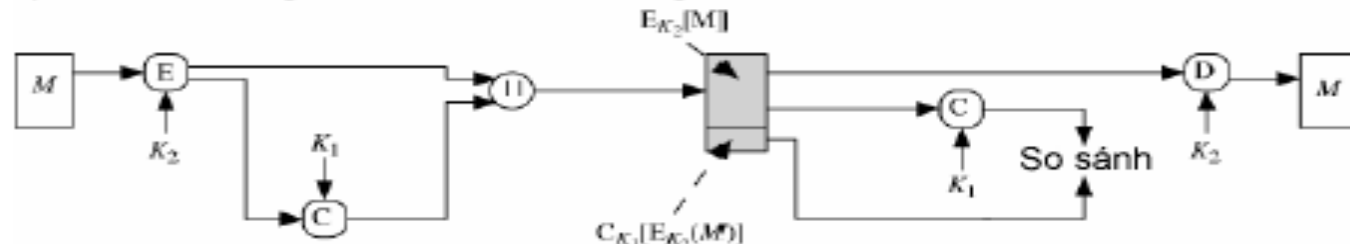
Xác thực dùng mã xác thực thông điệp (MAC - checksum)



a) Xác thực thông điệp



b) Xác thực thông báo và bảo mật; MAC gắn vào bản thô



c) Xác thực thông báo và bảo mật; MAC gắn vào bản mã

Xác thực dùng mã xác thực thông điệp (MAC - checksum)

- Chỉ cần xác thực, không cần mã hoá tốn thời gian và tài nguyên
 - Thông điệp hệ thống
 - Chương trình máy tính
- Tách riêng bảo mật và xác thực sẽ khiến tổ chức linh hoạt hơn
 - Chẳng hạn mỗi chức năng ở 1 tầng riêng
- Cần đảm bảo tính toàn vẹn của dữ liệu trong suốt thời gian tồn tại, không chỉ trong lúc lưu chuyển
 - Vì thông điệp có thể bị thay đổi sau khi giải mã

Xác thực dùng hàm băm

- Tạo ra hàm băm có kích thước xác định từ thông điệp đầu vào(không cần khoá): $h=H(M)$
- Hàm băm không cần giữ bí mật
- Giá trị băm gắn kèm với thông điệp để đảm bảo tính toàn vẹn của thông điệp
- Bất kỳ một sự thay đổi nhỏ nào trong thông điệp M cũng tạo ra sự thay đổi trong mã băm h

Các yêu cầu đối với hàm băm

- Có thể áp dụng với thông điệp M với độ dài bất kỳ
- Tạo ra giá trị băm h có độ dài cố định
- $H(M)$ dễ dàng tính được với bất kỳ M nào
- Từ h rất khó tìm được M sao cho $h=H(M)$: tính một chiều
- Từ M_1 rất khó tìm được M_2 sao cho $H(M_1)=H(M_2)$
- Rất khó tìm được cặp (M_1, M_2) sao cho $H(M_1)=H(M_2)$

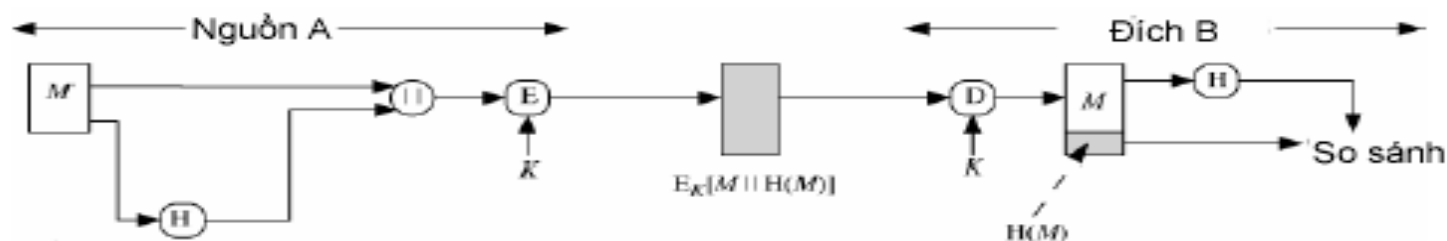
Các yêu cầu đối với hàm băm

- Đặc điểm 4 là đặc điểm "1 chiều" (one-way). Nó tạo ra 1 mã cho bản tin nhưng không thể tạo ra 1 bản tin cho 1 mã
- Đặc điểm 5 đảm bảo:
 - 1 bản tin thay thế khi bị băm không cùng giá trị băm với bản tin đã cho là
 - Bảo vệ lại sự giả mạo khi sử dụng 1 mã băm được mã hóa.

Các yêu cầu đối với hàm băm

- Một hàm băm mà thoả mãn các đặc điểm từ 1→5 trong danh sách trên thì vẫn bị coi là 1 hàm băm kém. Nếu đặc điểm 6 được thoả mãn, nó mới được coi là một hàm băm tốt.
- Đặc điểm 6 bảo vệ bản tin khỏi một lớp các tấn công tinh vi như tấn công ngày sinh (birthday attack).

Xác thực dùng hàm băm



a) Xác thực thông báo và bảo mật; mã băm gắn vào bản thô

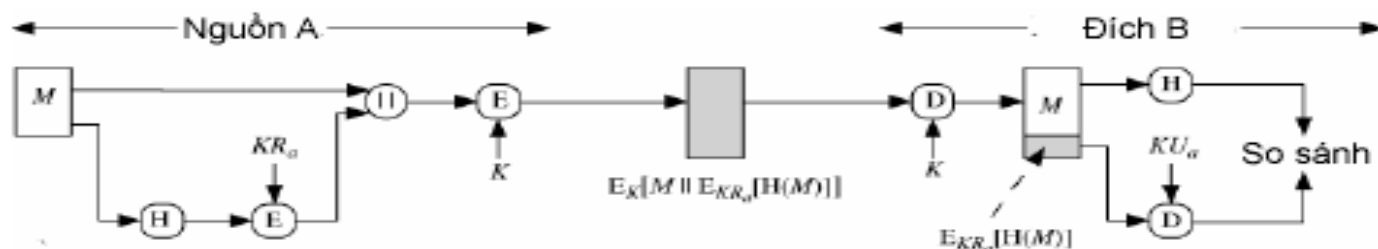


b) Xác thực thông báo; mã băm được mã hóa sử dụng phương pháp đối xứng

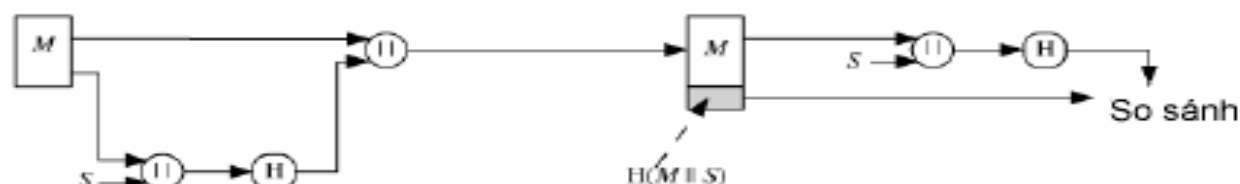


c) Xác thực thông báo; mã băm được mã hóa sử dụng phương pháp khóa công khai

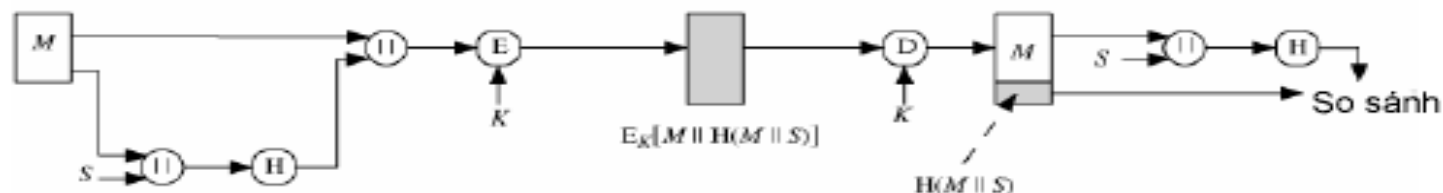
Xác thực dùng hàm băm



d) Xác thực bằng mã hóa khóa công khai và bảo mật bằng mã hóa đối xứng



e) Xác thực không cần mã hóa nhờ hai bên chia sẻ một giá trị bí mật chung



f) Xác thực nhờ một giá trị bí mật chung; bảo mật bằng phương pháp đối xứng

So sánh MAC và Hash

- Tương tự hàm MAC nhưng gọi là hash không khoá, MAC là hash có khoá

Các hàm băm đơn giản

- Nguyên tắc hoạt động chung:
 - Input: file, message.. được chia thành chuỗi các block n bit
 - Xử lý đầu vào: mỗi block được xử lý tại 1 thời điểm và lặp lại với các block khác \Rightarrow tạo ra 1 giá trị băm n bit

Hàm băm XOR

- Thực hiện phép XOR bit-by-bit
- Có thể biểu diễn như sau:

- $C_i = b_{i1} \oplus b_{i2} \oplus \dots \oplus b_{im}$

- Trong đó:

C_i : bit thứ i của mã băm ($i=1..n$)

m : Số Block n -bit của Input

b_{ij} : bit thứ i của Block j

\oplus : phép toán XOR bit

Hàm băm XOR

- Minh họa:

	Bit 1	Bit 2	Bit n
Block 1	B_{11}	B_{21}	B_{n1}
Block 2	B_{12}	B_{22}	B_{n2}
....
Block m	B_{1m}	B_{2m}	B_{nm}
Hash Code	C_1	C_2	C_n

Hàm băm RXOR

- Thực hiện: Xoay đi một bit rồi thực hiện phép XOR → tăng tính ngẫu nhiên
- Sơ đồ:
 - Khởi tạo n bit của giá trị băm bằng 0
 - Xử lý mỗi block n-bit thành công là như sau:
 - Xoay giá trị băm hiện tại sang trái 1 bit
 - XOR block với giá trị băm

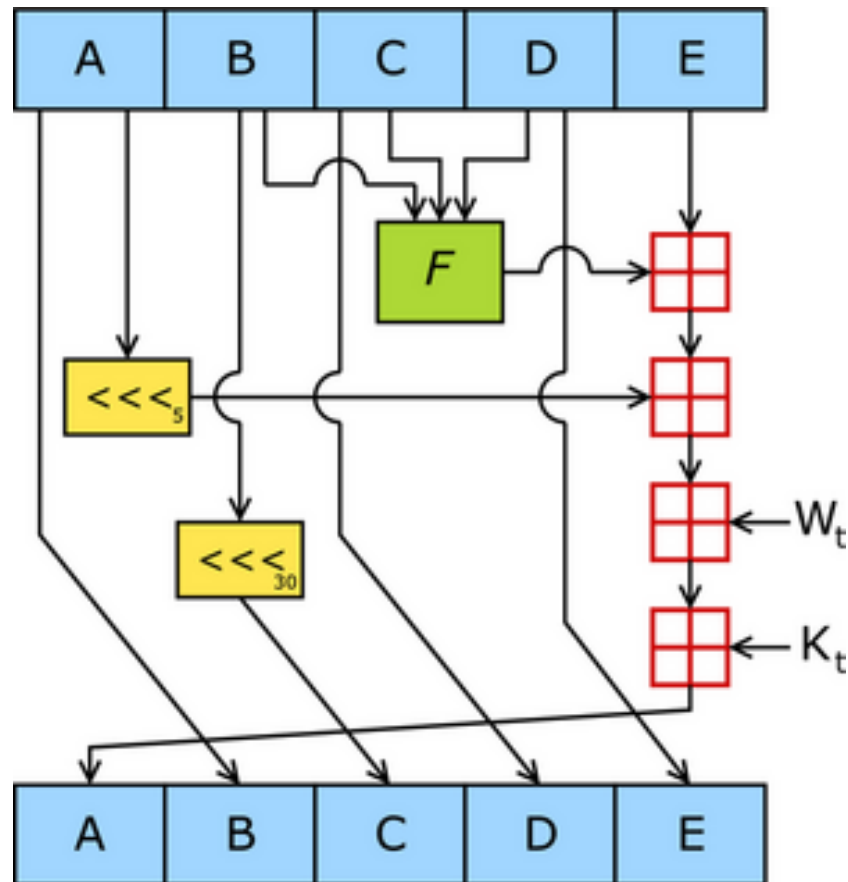
SHA-1 (Secure Hash Algorithm -1)

- Đây là một hàm băm 1 chiều
- Các phiên bản
 - SHA-0: Công bố năm 1993
 - SHA-1:
 - SHA-2: Bao gồm tập hợp SHA-224, SHA-256, SHA-384, và SHA-512
- Chúng được dùng bởi chính phủ Mỹ

SHA-1

- Đặc điểm của hàm:
 - Input: Đầu vào message có size $< 2^{64}$
 - Chia thành các Block có size = 512 bit
 - Ra: 1 Digest độ dài 160 bit
 - Bảo mật:
 - Không tính toán ra được thông điệp với 1 Digest đã cho
 - Không có 2 thông điệp cùng tạo ra 1 Digest


Sơ đồ hoạt động



Một số kết quả test

- Một số giá trị digest của SHA-1:
 - SHA1("The quick brown fox jumps over the lazy dog") == "2fd4e1c67a2d28fced849ee1bb76e7391b93eb12"
 - SHA1("The quick brown fox jumps over the lazy cog") == "de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3"
 - SHA1("") == "da39a3ee5e6b4b0d3255bfef95601890afd80709"

Chữ ký số

- Yêu cầu
 - Phân loại
 - Tạo và chứng thực chữ ký
 - Chứng thư số
- 

Yêu cầu

- Dựa trên thông điệp
- Sử dụng thông tin duy nhất thuộc về người gửi → chống giả mạo
- Dễ kiểm tra và nhận dạng
- Phải không thể tính toán để giả mạo được
- Để thoả mãn các yêu cầu trên, người ta thường sử dụng hàm băm.

Phân loại

- Thường được phân làm 2 loại:
 - ✓ Chữ ký trực tiếp
 - ✓ Chữ ký phân xử

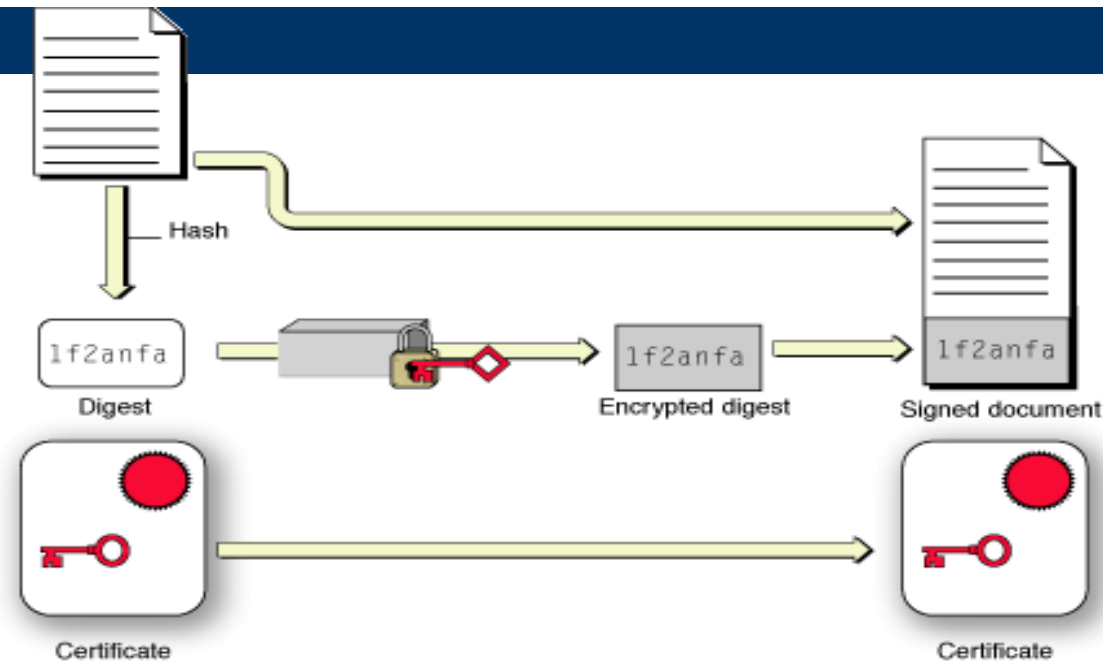
Chữ ký trực tiếp

- Chỉ bao gồm các thành phần truyền thông
- Có thể được tạo ra :
 - Mã hoả toàn bộ bản tin với khoá riêng của người gửi
 - Mã hoá mã băm của bản tin với khoá riêng của người gửi
- Tính hợp lệ của chữ ký phụ thuộc vào việc bảo mật khoá riêng của người gửi.

Chữ ký phân xử

- Hoạt động chung :
 - Mọi bản tin được gửi từ X đến Y phải thông qua A, để kiểm tra nguồn gốc và nội dung của nó
 - Bản tin được ghi lại thời gian rồi được gửi đến B + 1 thông điệp được đảm bảo bởi A.
 - Sự có mặt của A giải quyết vấn đề: X có thể phủ nhận bản tin này

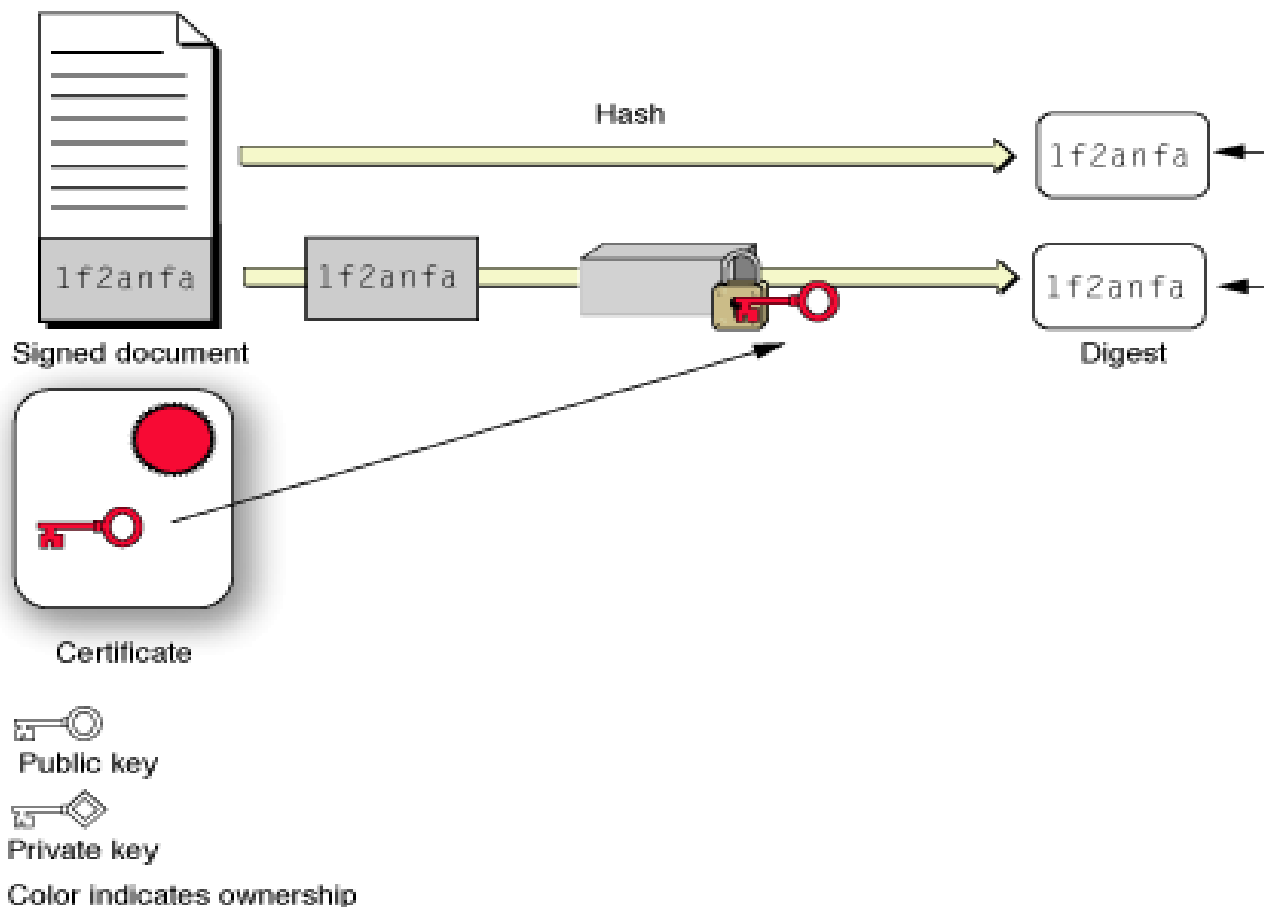
Tạo chữ ký



Quá trình xác thực gồm 2 quá trình con:

- Xác thực người gửi: thông qua khoá riêng của người gửi và kiểm chứng khoá riêng bằng khoá công khai của người gửi chứa trong chứng chỉ số
- Xác thực nội dung (tính toàn vẹn của văn bản) thông qua mẫu của thông điệp – mã băm của thông điệp.

Chứng thực chữ ký



Digital Certificate

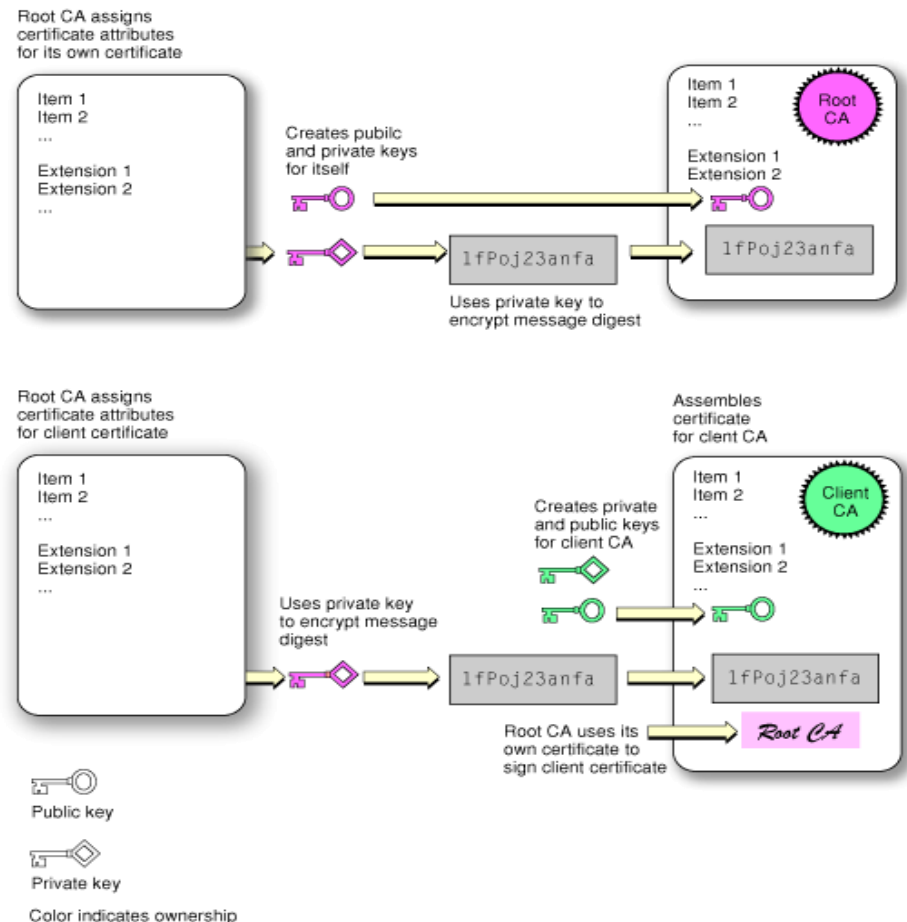
- Để chứng thực được chữ ký điện tử bắt buộc người nhận phải có khoá chung của người gửi.
- Bản chất cặp khoá này không liên hệ với thuộc tính của người sử dụng → cần có cơ chế để liên kết chúng với người dùng → các certificate
- Các Certificate được CA cung cấp

Các thông tin trong Certificate

- Phiên bản
- Số serial
- Nhà cung cấp Certificate
- Người sở hữu Certificate
- Thời gian hiệu lực của Certificate
- Các thuộc tính
- Chữ ký số của nhà cung cấp
- Khoá công khai của người sở hữu Certificate
- Thuật toán băm dùng để tạo chữ ký.

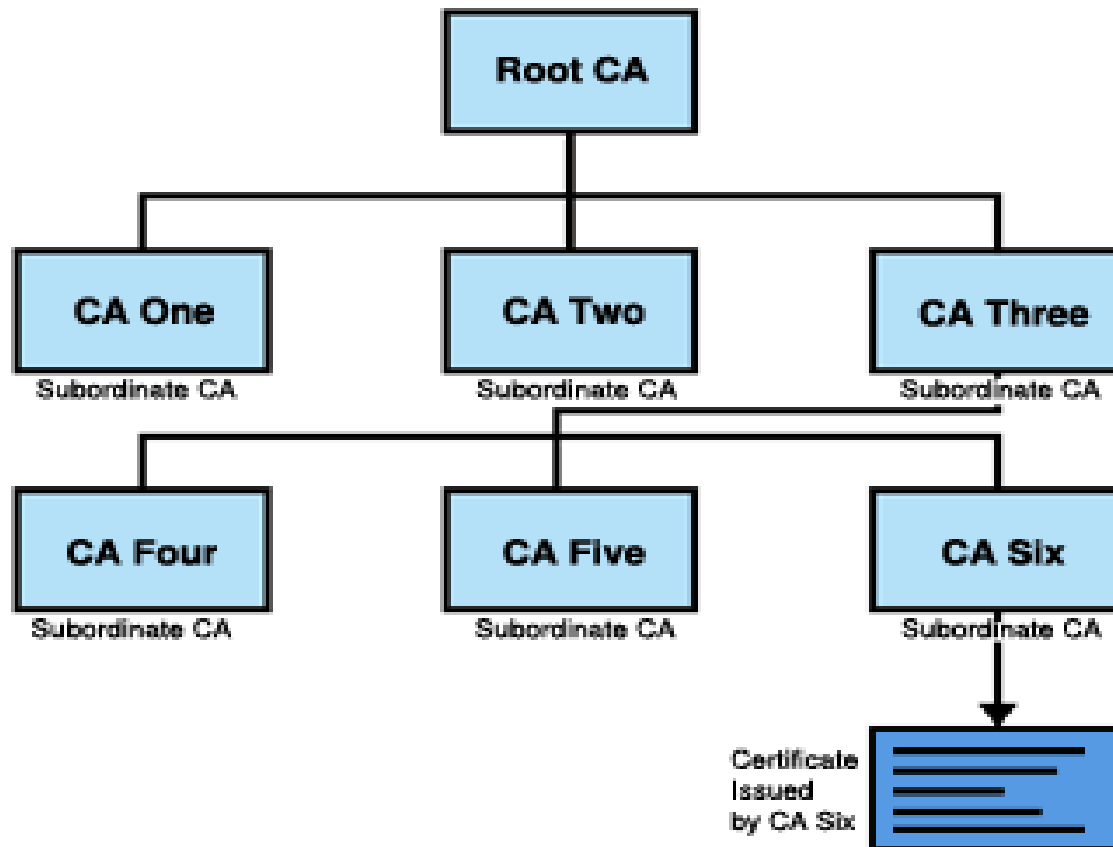
Tạo Certificate

- Các Certificate được tạo ra còn để chứng thực cho bản thân nó
- Các CA có cấu trúc phân cấp
- Minh họa quá trình tạo Certificate cho CA gốc và CA mức thấp hơn

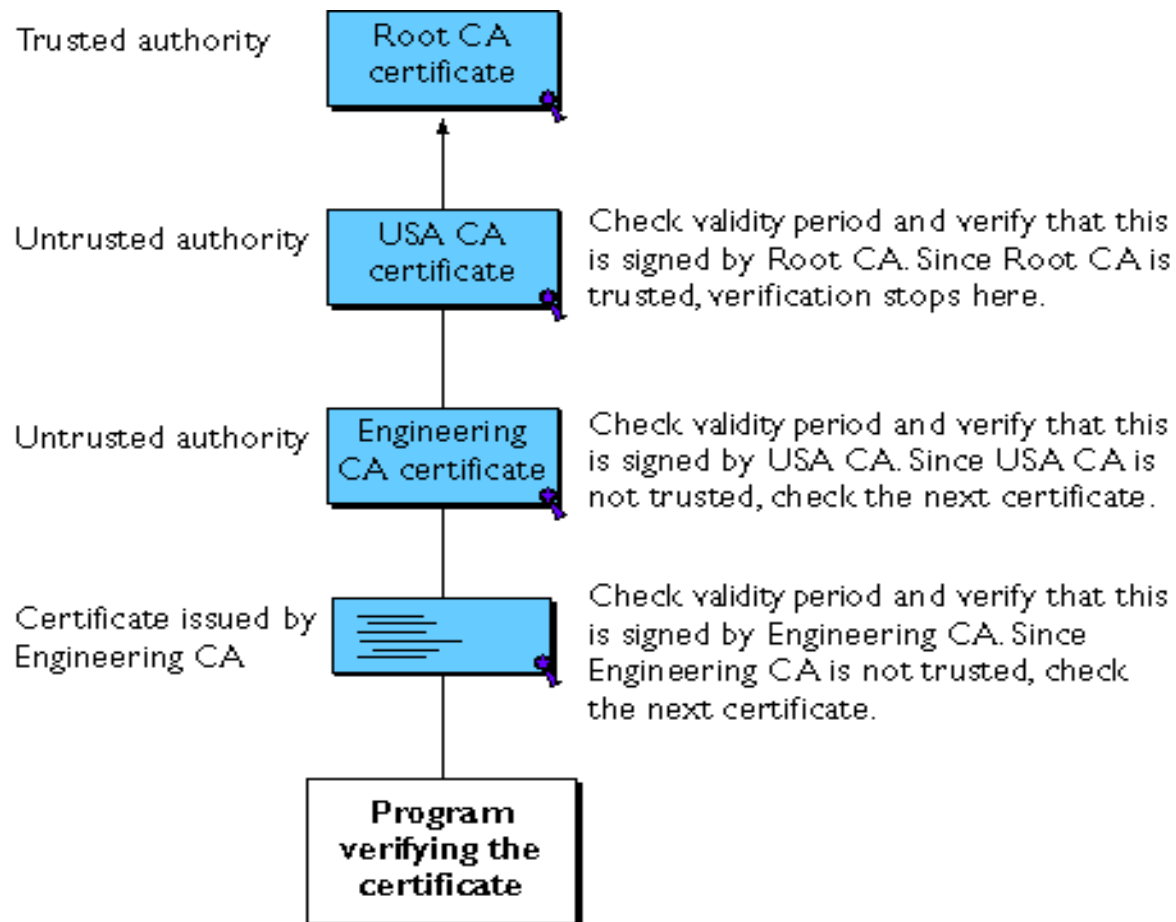


Cấu trúc phân cấp của CA

A Hierarchy of Certificate Authorities



Xác thực chuỗi Certificate



Các giao thức xác thực

- Xác thực hai bên
- Các phương pháp mã hoá cổ điển
- Phương pháp mã hoá khoá công khai

Xác thực hai bên

- Tại đây, chúng ta chỉ xem xét vấn đề quản lý phân phối khoá
- Tồn tại 2 vấn đề :
 - Tính tin cậy : ngăn chặn hiện tượng giả mạo và tấn công vào khoá phiên
 - Xác định thời điểm: chống lại kiểu tấn công replay

Phương pháp chống replay

- 2 phương pháp:
 - Timestamp: gắn 1 timestamp vào bản tin --> yêu cầu đồng bộ
 - Challenge/Response: A sẽ gửi đến B 1 nonce và đợi trả lời của B. Nếu có chứa giá trị nonce chính xác thì mới bắt đầu gửi bản tin

Đánh giá 2 phương pháp

- Timestamp: không áp dụng cho các ứng dụng hướng kết nối
 - Yêu cầu đồng bộ giữa các tiến trình đồng hồ
 - Cơ hội tấn công thành công sẽ tăng lên nếu có 1 khoảng thời gian không đồng bộ
 - Tính luôn thay đổi và không dự đoán trước được của các độ trễ trong mạng
- Challenge/Response: không áp dụng cho các ứng dụng không hướng kết nối
 - Yêu cầu bắt tay trước khi truyền thông không kết nối
 - Phương pháp tốt nhất: tạo sự đồng bộ giữa đồng hồ ở mỗi bên

Phương pháp mã hoá kinh điển

- Sử dụng 1 trung tâm phân phối khoá tin cậy(KDC)
- Mỗi bên chia sẻ 1 khoá mật với KDC:khoá chính
- KDC sẽ sinh ra các khoá phiên: sử dụng 1 trên kết nối giữa 2 bên
- KDC còn chịu trách nhiệm phân phối các khoá phiên sử dụng khoá chính để bảo vệ quá trình phân phối khoá

Mã hoá khoá công khai

- Phương pháp này đảm bảo là mỗi bên đều lưu trữ khoá công khai hiện thời của bên còn lại
- Tất cả các phương pháp trên vẫn tồn tại những điểm thiếu sót
- Có nhiều phương pháp:
 - Denny
 - Woo và Law

An ninh hệ thống



An ninh hệ thống

- Các hệ thống ngăn chặn xâm nhập
- Lỗ hổng hệ thống
- Các hệ thống phát hiện xâm nhập

Các hệ thống ngăn chặn xâm nhập

- Firewall
- Proxy

Lỗ hổng bảo mật của hệ thống

- Các lỗ hổng bảo mật
- Quét lỗ hổng bảo mật

Lỗ hổng bảo mật

- **Khái niệm lỗ hổng**
- **Phân loại lỗ hổng**
 - Lỗ hổng làm cho từ chối dịch vụ
 - Lỗ hổng cho phép người dùng bên trong mạng với quyền hạn chế có thể tăng quyền mà không cần xác thực.
 - Lỗ hổng cho phép kẻ không phải là người dùng hệ thống có thể xâm nhập từ xa không xác thực.

Khái niệm lỗ hổng

- Tất cả những đặc tính của phần mềm hay phần cứng mà cho phép người dùng không hợp lệ, có thể truy cập hay tăng quyền truy nhập mà không cần xác thực.
- Tổng quát : lỗ hổng là tất cả mọi thứ mà kẻ tấn công có thể lợi dụng để xâm nhập vào hệ thống

Lỗi hỏng làm từ chối dịch vụ

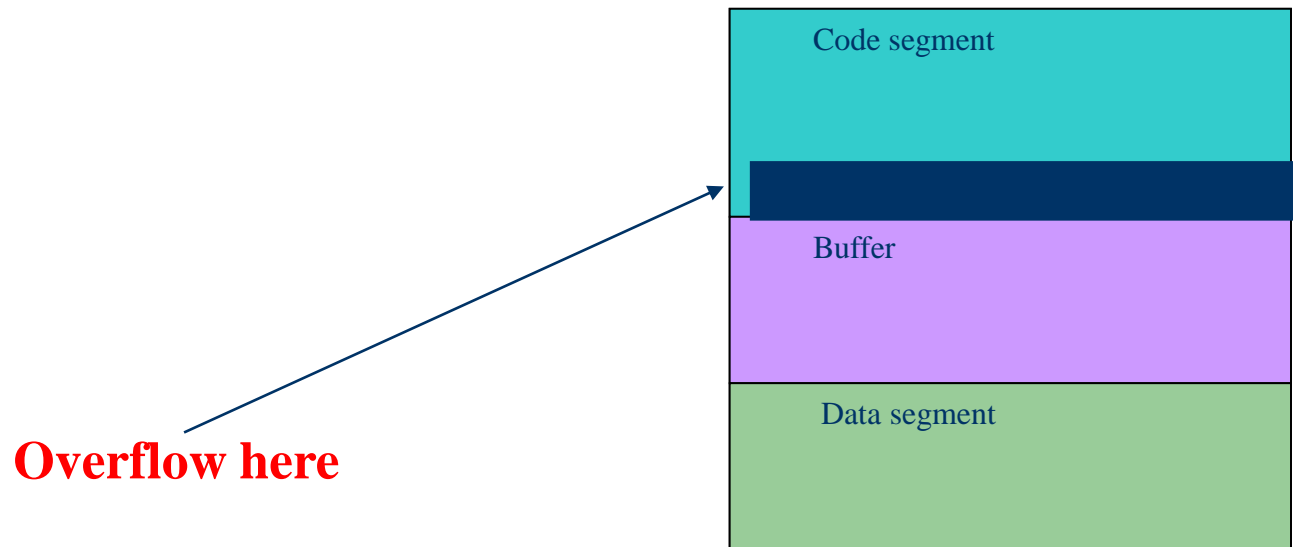
- Cho phép hacker lợi dụng làm tê liệt một số dịch vụ của hệ thống .
- Kẻ tấn công có thể làm mất khả năng hoạt động của máy tính hay một mạng, ảnh hưởng tới toàn bộ tổ chức hay công ty.
- Ba loại :
 - Bandwith/Throughput Attacks
 - Protocol Attacks
 - Software Vulnerability Attacks

Lỗi hỏng tăng quyền truy nhập không cần xác thực.

- Là lỗi ở những phần mềm hay hệ điều hành có sự phân cấp người dùng.
- Cho phép loại người dùng với mức sử dụng hạn chế có thể tăng quyền trái phép.
- Ví dụ :
 - Sendmail : cho phép người dùng bình thường có thể khởi động tiến trình sendmail, lợi dụng sendmail khởi động chương trình khác với quyền root

Lỗi hỏng tăng quyền truy nhập không cần xác thực.

- Tràn bộ đệm :



Lỗi hổng cho phép xâm nhập từ xa không xác thực.

- Là lỗi chủ quan của người quản trị hệ thống hay người dùng.
- Do không thận trọng, thiếu kinh nghiệm, và không quan tâm đến vấn đề bảo mật.
- Một số những cấu hình thiếu kinh nghiệm :
 - Tài khoản có password rỗng
 - Tài khoản mặc định
 - Không có hệ thống bảo vệ như firewall, IDS, proxy
 - Chạy những dịch vụ không cần thiết mà không an toàn : SNMP, pcAnywhere, VNC , ...

Lỗ hổng cho phép xâm nhập từ xa không xác thực.

- Phân loại :
 - Trojan / Backdoor
 - SQL injection
 - LOGIN : *'or 1 = 1; drop table users; --*
 - PASSWORD : *anything*
 - Query : *Select * from users where userName = "" or 1 = 1; drop table users;-- userPass = 'anything'*
 - Xâm nhập Web bất hợp pháp
 - Google : *allinurl:admentor*
 - One result :
<http://www.someserver.com/admentor/admin/admin.asp>
 - LOGIN : *'or "="*
 - PASSWORD: *'or "="*
 - Có thể xâm nhập vào trang web lỗi này với quyền admin

Quét lỗ hổng bảo mật của hệ thống

- Phát hiện các lỗ hổng bảo mật của hệ thống
- Phát hiện các nghi vấn về bảo mật để ngăn chặn

Các phương pháp, kỹ thuật quét lỗ hổng bảo mật

- Quét mạng
- Quét điểm yếu
- Kiểm tra log
- Kiểm tra tính toàn vẹn file
- Phát hiện virus
- Chống tấn công quay số
- Chống tấn công vào access point

Quét mạng

- Kiểm tra sự tồn tại của hệ thống đích
- Quét cổng
- Dò hệ điều hành

Quét mạng

- Kiểm tra sự tồn tại của hệ thống đích
 - Quét ping để kiểm tra xem hệ thống có hoạt động hay không
 - Phát hiện bằng IDS hoặc một số trình tiện ích
 - Cấu hình hệ thống, hạn chế lưu lượng các gói ICMP để ngăn ngừa

Quét mạng

- Quét cổng
 - Nhằm nhận diện dịch vụ, ứng dụng
 - Sử dụng các kỹ thuật quét nổi TCP, TCP FIN..., xét số cổng để suy ra dịch vụ, ứng dụng
 - Phát hiện quét dựa vào IDS hoặc cơ chế bảo mật của máy chủ
 - Vô hiệu hóa các dịch vụ không cần thiết để dấu mình

Quét mạng

- Dò hệ điều hành
 - Dò dựa vào dấu vân tay giao thức
 - Phát hiện bằng các trình phát hiện quét cổng, phòng ngừa sử dụng firewall, IDS.

Quét điểm yếu

- Liệt kê thông tin
- Quét điểm yếu dịch vụ
- Kiểm tra an toàn mật khẩu

Quét điểm yếu

- Liệt kê thông tin
 - xâm nhập hệ thống, tạo các vấn tin trực tiếp
 - Nhằm thu thập các thông tin về
 - Dùng chung, tài nguyên mạng
 - Tài khoản người dùng và nhóm người dùng
 - Ứng dụng và banner
 - Ví dụ về liệt kê thông tin trong Windows
 - Ví dụ về liệt kê thông tin trong Unix/Linux

Quét điểm yếu

- Quét điểm yếu dịch vụ
 - Quét tài khoản yếu: Tìm ra acc với từ điển khi tài khoản yếu
 - Quét dịch vụ yếu: Dựa trên xác định nhà cung cấp và phiên bản
 - Biện pháp đối phó: Cấu hình dịch vụ hợp lý, nâng cấp, vá lỗi kịp thời.

Quét điểm yếu

- Bẻ khóa mật khẩu
 - Nhanh chóng tìm ra mật khẩu yếu
 - Cung cấp các thông tin cụ thể về độ an toàn của mật khẩu
 - Dễ thực hiện
 - Giá thành thấp

Kiểm soát log file

- Ghi lại xác định các thao tác trong hệ thống
- Dùng để xác định các sự sai lệch trong chính sách bảo mật
- Có thể bằng tay hoặc tự động
- Nên được thực hiện thường xuyên trên các thiết bị chính
- Cung cấp các thông tin có ý nghĩa cao
- Áp dụng cho tất cả các nguồn cho phép ghi lại hoạt động trên nó

Kiểm tra tính toàn vẹn file

- Các thông tin về thao tác file được lưu trữ trong cơ sở dữ liệu tham chiếu
- Một phần mềm đối chiếu file và dữ liệu trong cơ sở dữ liệu để phát hiện truy nhập trái phép
- Phương pháp tin cậy để phát hiện truy nhập trái phép
- Tự động hóa cao
- Giá thành hạ
- Không phát hiện khoảng thời gian
- Luôn phải cập nhật cơ sở dữ liệu tham chiếu

Quét Virus

- Mục đích: bảo vệ hệ thống khỏi bị lây nhiễm và phá hoại của virus
- Hai loại phần mềm chính:
 - Cài đặt trên server
 - Trên mail server hoặc trạm chính (proxy...)
 - Bảo vệ trên cửa ngõ vào
 - Cập nhật virus database thuận lợi
 - Cài đặt trên máy trạm
 - Đặc điểm: thường quét toàn bộ hệ thống (file, ổ đĩa, website người dùng truy nhập)
 - Đòi hỏi phải được quan tâm nhiều của người dùng
- Cả hai loại đều có thể được tự động hóa và có hiệu quả cao, giá thành hợp lí

War Dialing

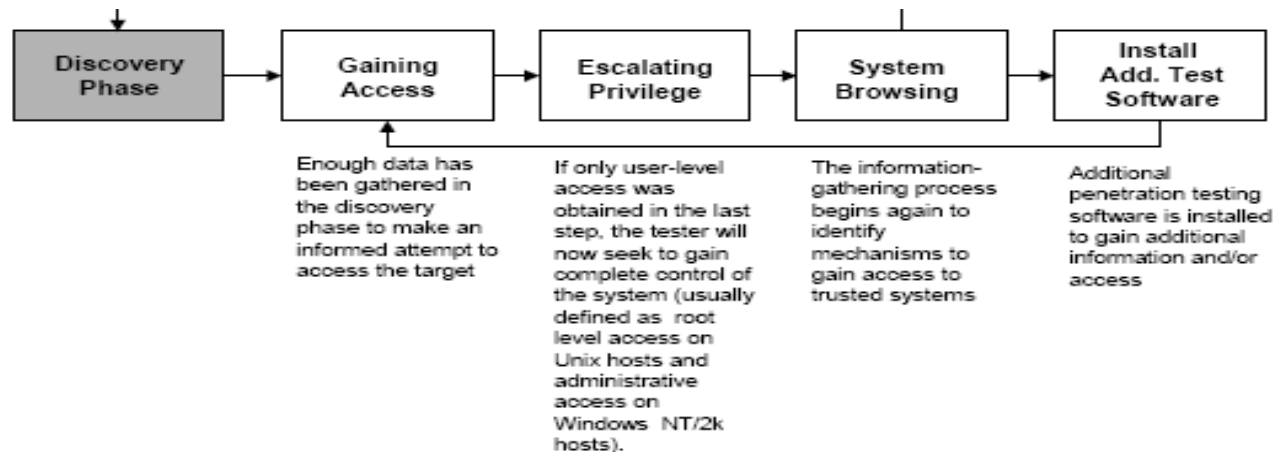
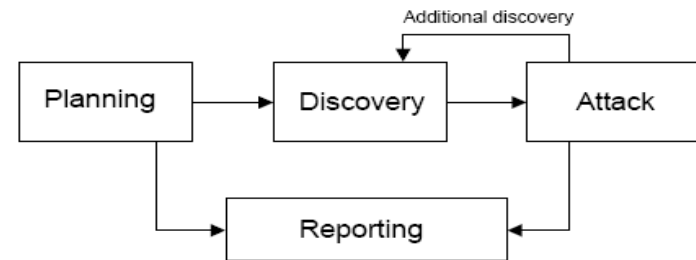
- Ngăn chặn những modem không xác thực quay số tới hệ thống
- Chương trình quay số có thể quay tự động để dò tìm cổng vào hệ thống
- Policy: hạn chế số điện thoại truy nhập cho từng thành viên
- Phương pháp này đòi hỏi nhiều thời gian

Quét LAN không dây

- Liên kết bằng tín hiệu không dùng dây dẫn -> thuận tiện cho kết nối đồng thời tạo ra nhiều lỗ hổng mới
- Hacker có thể tấn công vào mạng với máy tính xách tay có chuẩn không dây
- Chuẩn thường dùng 802.11b có nhiều hạn chế về bảo mật
- Chính sách bảo đảm an toàn:
 - Dựa trên các nền phần cứng và các chuẩn cụ thể
 - Việc cấu hình mạng phải chặt chẽ và bí mật
 - Gỡ bỏ các cổng vào không cần thiết

Kiểm thử các thâm nhập

- Dùng các kĩ thuật thực tế được sử dụng bởi những kẻ tấn công
- Xác định cụ thể các lỗ hổng và mức độ của chúng
- Chu trình:



Kiểm thử thâm nhập (Cont)

- Các loại lỗ hổng có thể được phát hiện:
 - Các lỗi của nhân hệ thống
 - Các lỗi tràn bộ đệm
 - Các liên kết đường dẫn
 - Các tấn công vào bộ mô tả file
 - Quyền truy nhập file và thư mục
 - Trojan

So sánh các phương pháp

Kiểu quét	Điểm mạnh	Điểm yếu
Quét mạng	<ul style="list-style-type: none">• nhanh so với quét điểm yếu• hiệu quả cho quét toàn mạng• nhiều chương trình phần mềm miễn phí• tính tự động hóa cao• giá thành hạ	<ul style="list-style-type: none">• không chỉ ra được các điểm yếu cụ thể• thường được dùng mở đầu cho kiểm thử thâm nhập• đòi hỏi phải có ý kiến chuyên môn để đánh giá kết quả
Quét điểm yếu	<ul style="list-style-type: none">• có thể nhanh, tùy thuộc vào số điểm được quét• một số phần mềm miễn phí• tự động cao• chỉ ra được điểm yếu cụ thể• thường đưa ra được các gợi ý giải quyết điểm yếu• giá thành cao cho các phần mềm tốt cho tới free• dễ vận hành	<ul style="list-style-type: none">• tuy nhiên tỉ lệ thất bại cao• chiếm tỉa nguyên lớn tại điểm quét• không có tính ẩn cao (dễ bị phát hiện bởi người sử dụng, tường lửa, IDS)• có thể trở nên nguy hiểm trong tay những người kém hiểu biết• thường không phát hiện được các điểm yếu mới nhất• chỉ chỉ ra được các điểm yếu trên bề mặt của hệ thống

So sánh (Cont)

Kiểm thử thâm nhập

- Sử dụng các kỹ thuật thực tế mà các kẻ tấn công sử dụng
- Chỉ ra được các điểm yếu
- Tìm hiểu sâu hơn về điểm yếu, chúng có thể được sử dụng như thế nào để tấn công vào hệ thống
- Cho thấy rằng các điểm yếu không chỉ là trên lý thuyết
- Cung cấp bằng chứng cho vấn đề bảo mật

- Đòi hỏi nhiều người có khả năng chuyên môn cao
- Tốn rất nhiều công sức
- Chậm, các điểm kiểm thử có thể phải ngừng làm việc trong thời gian dài
- Không phải tất cả các host đều được thử nghiệm (do tốn thời gian)
- Nguy hiểm nếu được thực hiện bởi những người không có chuyên môn
- Các công cụ và kỹ thuật có thể là trái luật
- Giá thành đắt đỏ

Duyệt danh sách thư mục

- Các danh sách thư mục có thể cho rất nhiều thông tin
- Query : `intitle:index.of/admin`



`intitle:index.of/admin`

Duyệt danh sách thư mục

- Các danh sách thư mục có thể cung cấp các thông tin version của server
- Query : **intitle:index.of apache server.at**



Các trang mặc định Server Pages

- Các web server với các trang mặc định có thể cung cấp khá nhiều thông tin cho hacker : version, OS
- Query : `intitle:test.page.for.apache` “it worked”
- Query : `allintitle:Netscape FastTrack Server Home Page`

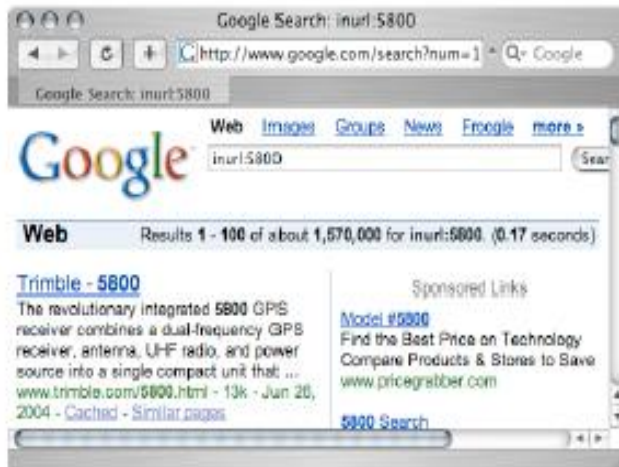


Quét CGI

- Để xác định các điểm yếu web trên mạng với quy mô lớn nhiều hacker sử dụng các bộ quét CGI.
 - Hầu hết các bộ quét có thể đọc file dữ liệu và truy vấn vào các web server để tìm các file dò rỉ.
 - /iisadmpwd/
 - /iisadmpwd/achg.htr
 - /iisadmpwd/aexp.htr
 - /iisadmpwd/aexp2.htr
 - /iisadmpwd/aexp2b.htr
- `inurl;/iisadmpwd/`
 - `inurl;/iisadmpwd/achg.htr`
 - `inurl;/iisadmpwd/aexp.htr`
 - `inurl;/iisadmpwd/aexp2.htr`
 - `inurl;/iisadmpwd/aexp2b.htr`

Quét cổng

- Các số cổng nhiều lúc xuất hiện trong url



inurl:5800



"VNC Desktop" inurl:5800

Một số dạng khác

- **Login Portals** : `inurl:admin/login.asp`
 - Microsoft Outlook Web Access
 - Coldfusion Admin Page
- **Thông tin SQL**
 - **SQL dump**: “# Dumping data for table” username password
 - **SQL injection**