CHƯƠNG 7: MỘT SỐ VẤN ĐỀ CHUYÊN SÂU

1. Thời lượng: GV giảng: 3;Thảo luận: 3;Thực hành: 0;Bài tập: 3;Tự học: 9.
2. **Mục đích, yêu cầu:**

- Mục đích: Giúp sinh viên nắn được một số vấn đề chuyên sâu hơn về mạng máy tính. Bao gồm vấn đề rất quan trọng và cấp bách hiện nay là an toàn và bảo mật mạng máy tính. Bên cạnh đó có hệ thống, công nghệ được sử dụng nhiều ở các công ty cơ quan là mạng riêng ảo. Ngoài ra, sơ lược về nội dung quản trị mạng và các ứng dụng khác cũng được đề cập trong chương.

CHƯƠNG 7: MỘT SỐ VẤN ĐỀ CHUYÊN SÂU

- **Yêu cầu:**
  - ✓Học viên tham gia học tập đầy đủ.
  - ✓Nghiên cứu trước các nội dung có liên quan đến bài giảng (đã có trên http://http:/fit.mta.edu.vn/~thiennd/).
  - ✓Chuẩn bị bài thảo luận.
  - ✓Chuẩn bị bài tập ở nhà và làm trên lớp.

An toàn thông tin trên mạng
Network Security

1. Khái niệm an toàn
2. Mô hình bảo vệ
3. Các hình thức tấn công mạng
4. Các phương pháp bảo vệ thông tin
5. Hạ tầng khóa công khai

3

1. Khái niệm về sự an toàn thông tin trên mạng

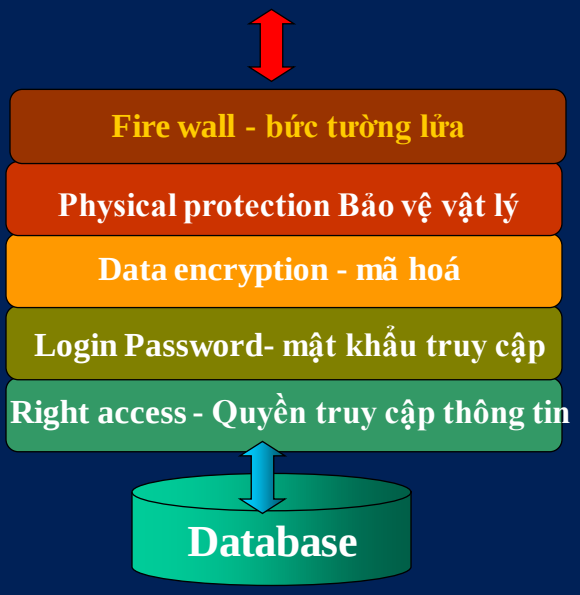
Mạng máy tính ngày càng mở rộng và phát triển, tài nguyên thông tin ngày càng được chia sẻ cho người sử dụng, tuy nhiên trong thực tế tồn tại những thông tin cần phải được bảo vệ và chia sẻ một cách có chọn lọc, do đó cần phải có cơ chế bảo đảm sự an toàn thông tin trên mạng.

Cơ chế an toàn thông tin trên mạng phải thoả mãn hai mục tiêu cơ bản sau:

- Bảo đảm điều kiện thuận lợi cho những người sử dụng hợp pháp trong quá trình khai thác và sử dụng tài nguyên trên mạng
- Ngăn chặn có hiệu quả những kẻ truy cập và khai thác, phá hoại các tài nguyên bất hợp pháp.

Về bản chất nguy cơ các vi phạm bất hợp pháp được chia làm hai loại: vi phạm thụ động và vi phạm chủ động. Vi phạm thụ động đôi khi do vô tình hoặc không cố ý, còn vi phạm chủ động có mục đích phá hoại rõ ràng và hậu quả khôn lường.

2. Mô hình các lớp bảo vệ thông tin trên mạng



a. Lớp quyền truy cập – Right Acces.

Nhằm kiểm soát các tài nguyên thông tin của mạng và quyền hạn sử dụng tài nguyên đó. Việc kiểm soát càng chi tiết càng tốt

b. Lớp đăng nhập tên/mật khẩu Login Password.

Nhằm kiểm soát quyền truy cập ở mức hệ thống. Mỗi người sử dụng muốn vào được mạng để sử dụng tài nguyên đều phải đăng ký tên và mật khẩu. Người quản trị mạng có trách nhiệm quả lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của người sử dụng khác tuỳ theo không gian và thời gian.

c. Lớp mã hoá thông tin Data Encryption.

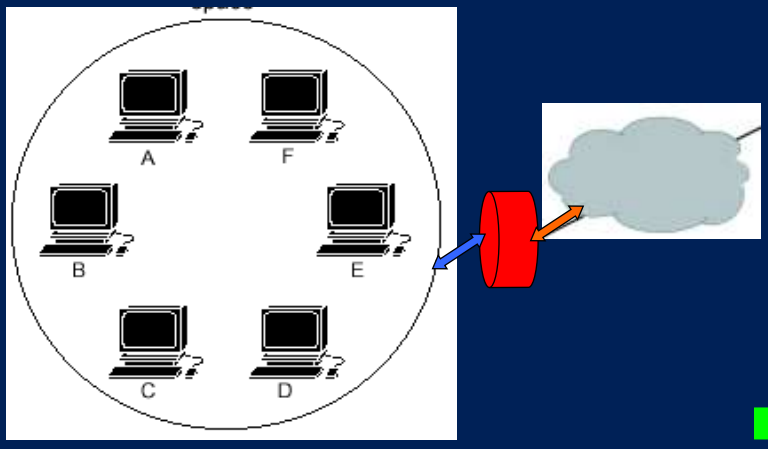
Để bảo mật thông tin truyền trên mạng người ta còn sử dụng các phương pháp mã hoá thông tin trên đường truyền. Có hai phương pháp cơ bản: mã hoá đối xứng và bất đối xứng, người ta đã xây dựng nhiều phương pháp mã hoá khác nhau.

d. Lớp bảo vệ vật lý Physical Protection.

Thường dùng các biện pháp truyền thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy mạng, quy định chặt chẽ các chế độ khai thác và sử dụng mạng,...

e. Lớp bảo vệ bức tường lửa .

Để bảo vệ từ xa một mạng máy tính hoặc cho cả một mạng nội bộ người ta dùng một hệ thống đặc biệt là bức tường lửa để ngăn chặn các thâm nhập trái phép, lọc bỏ các gói tin không cho gửi hoặc nhận từ trong ra ngoài hoặc ngược lại



Các phương pháp mã hóa

1. **Mã hóa cổ điển**
   - ✓ **Phương pháp thay thế**
   - ✓ **Phương pháp dịch chuyển**
   - ✓ **Phương pháp hoán vị**
2. **Mã hóa đối xứng (mã hóa bí mật)**
   - ✓ **DES**
   - ✓ **AES**
3. **Mã hóa bất đối xứng (Mã hóa công khai)**
   - ✓ **Hệ mật RSA**
   - ✓ **Hệ mật Elgamal**
   - ✓ **Phương pháp ECC**

Các chức năng cơ bản của mật mã hiện đại

- **Đảm bảo tính bí mật** (***confidentiality***) – giải quyết vấn đề bảo vệ thông tin chống lại sự tìm hiểu nội dung thông tin từ các đối tượng không có quyền truy nhập chúng.
- Thuật ngữ sự bí mật (*secrecy*) hoặc sự riêng tư (*privacy*) cũng đồng nghĩa với *confidentiality*.

(tiếp)

- **Đảm bảo tính toàn vẹn dữ liệu** (*data integrity*) – đảm bảo khả năng phát hiện sửa đổi trái phép thông tin.
- Để đảm bảo toàn vẹn dữ liệu, cần có các phương pháp đơn giản và tin cậy phát hiện bất kỳ sự can thiệp không mong muốn vào dữ liệu (các can thiệp như chèn, xóa và thay thế trong bản tin).
- **Đảm bảo tính sẵn sàng**

(tiếp)

- **Đảm bảo sự xác thực** (*authentication*) – chức năng này có liên hệ với sự định danh (*identification*). Vì thế nó được thực hiện xác thực trên cả thực thể (hai đối tượng trong một phiên liên lạc sẽ định danh lẫn nhau) và bản thân thông tin (thông tin được truyền trên kênh truyền sẽ được xác thực về nguồn gốc, nội dung, thời gian gửi, ...).
- Vì thế vấn đề xác thực trong mật mã được chia thành hai lớp chính – xác thực thực thể (*identity authentication*) và xác thực nguồn gốc dữ liệu (*data origin authentication*).

(tiếp)

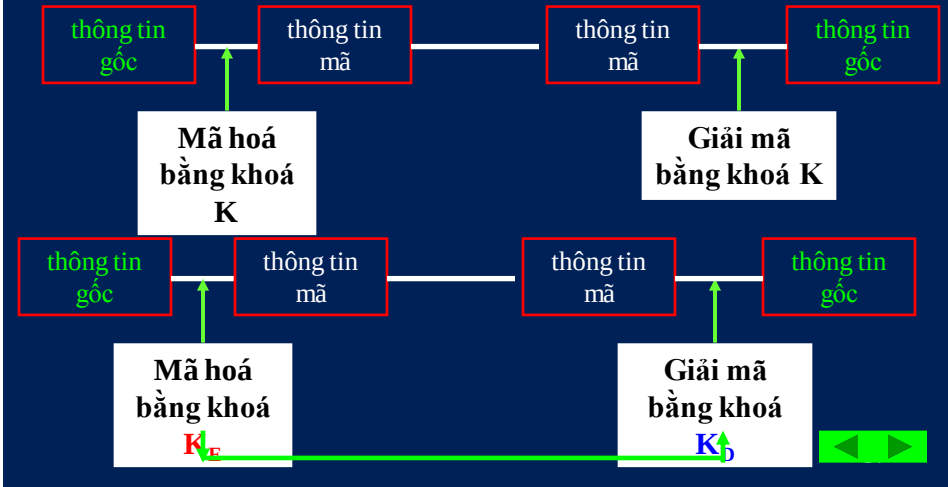
- **Đảm bảo chống sự từ chối** (*non-repudiation*) – chức năng ngăn ngừa một thực thể từ chối (phủ nhận) một cam kết hoặc hành động trước đó.
- Khi xuất hiện tranh chấp vì một thực thể từ chối một hành động chắc chắn đã xảy ra, một biện pháp giải quyết là cần thiết.

Nhận xét

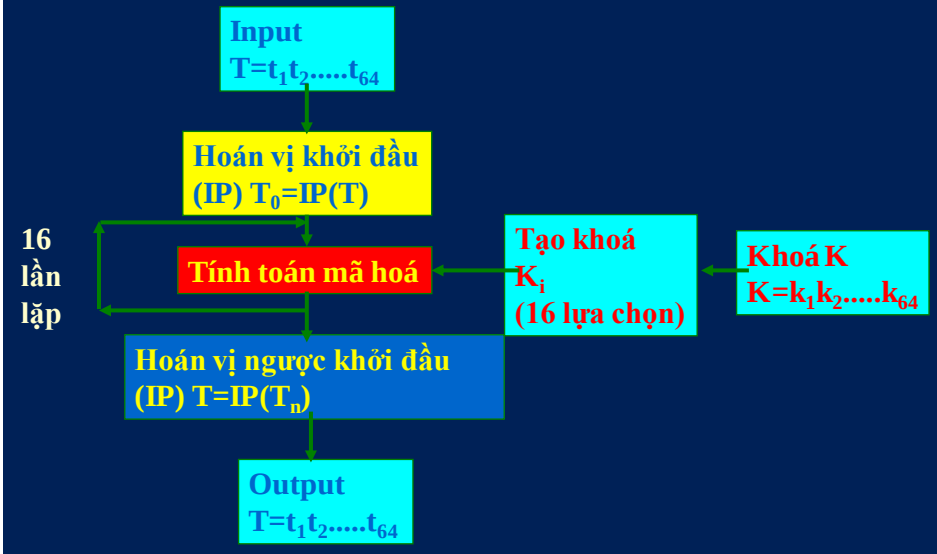
- Trong số các chức năng trên, chức năng đầu tiên đã được biết đến từ hàng ngàn năm trước, còn các chức năng sau liên quan đến các dịch vụ thông tin mới.
- Tuy nhiên, chức năng bảo vệ bí mật thông tin vẫn luôn mang tính thời sự.

Mô hình mã hóa

Các phương pháp mã hoá thường chia làm hai loại đối xứng và bất đối xứng:



Mã hoá đối xứng. Kỹ thuật mã hoá DES trong đó 56 bits dùng làm khoá và 8 bits dùng để kiểm soát lỗi. Sơ đồ thuật toán như sau:



Phương pháp mã hoá công khai RSA (Rivest, Shamir, Adleman)

Năm 1978 Rivest, Shamir và Adleman đã đề xuất phương pháp mã hoá RSA – mã Công khai. Thuật toán RSA dựa trên nhận xét sau: có thể dễ dàng sinh ra 2 số nguyên tố lớn và nhân chúng với nhau, nhưng cực kỳ khó phân tích một hợp số thành 2 số nguyên tố. Thuật giải được mô tả như sau:

1- Chọn 2 số nguyên tố lớn p và q
2- Tính n= pxq và $\psi(n)=(p-1)(q-1)$
3- Chọn ngẫu nhiên D ($3 < D < \psi(n)$) sao cho USCLN(D, ψ (n))=1
4- Chọn E sao cho ED Mod $\psi(n) = 1$
5- n và E là khoá công khai D là khoá bí mật.

Giả sử văn bản gốc là V ta biểu diễn V dưới dạng các số nguyên dương T gồm các số nằm trong [1,n-1], khi đó văn bản mã được tính như sau:

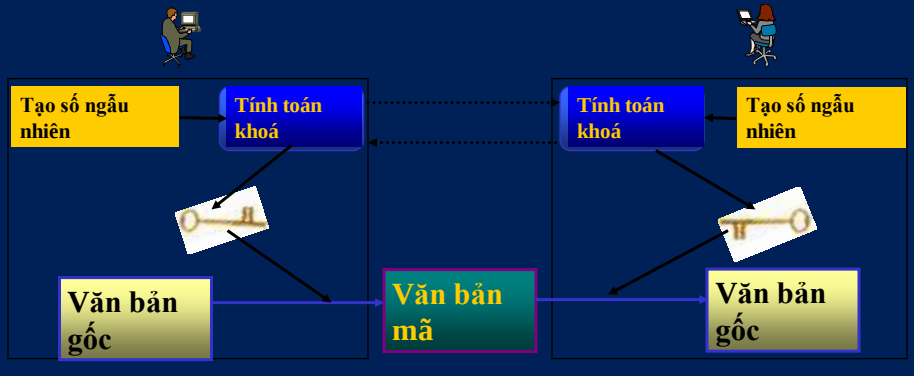
Mã hóa: $W = T^E \text{ Mod } n$.
Giải mã: $T = W^D \text{ Mod } n$.

Ví dụ RSA

- Chọn hai số nguyên tố, chẳng hạn p = 11, q = 17.
- Tính tích: n = p × q = 11 × 17 = 187.
- Tính $\phi(n) = (p-1) \times (q-1) = 10 \times 16 = 160$.
- Chọn e là số nguyên tố cùng nhau với $\phi(n) = 160$ và phải nhỏ hơn $\phi(n)$. Trong trường hợp này chọn e = 7.
- Xác định d để de = 1 mod 160 và d < 160. Giá trị phù hợp để chọn là d = 23 , bởi vì $23 \times 7 = 161 = 1 \times 160 + 1$.

Trao đổi khóa Diffie – Hellman (DH)

Tạo ra một giá trị bí mật dùng chung mà sau đó có thể được dùng như một khoá chung cho thuật toán mã hoá khoá bí mật.



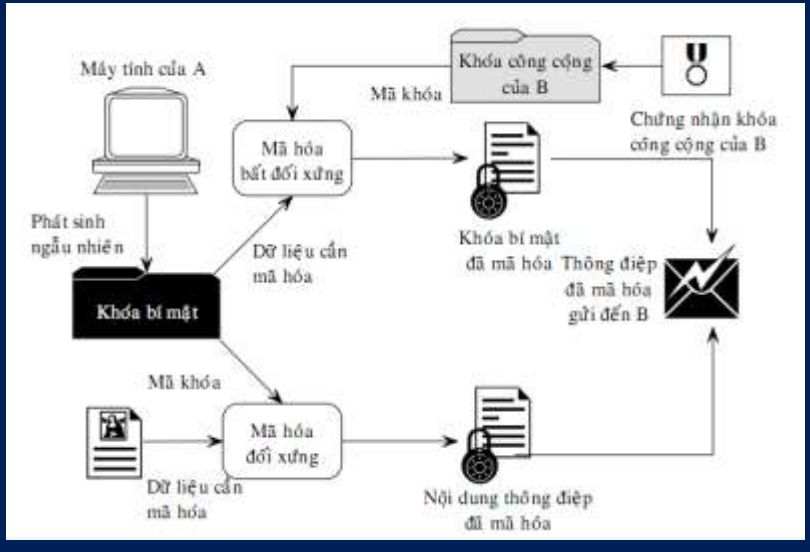
Trao đổi khóa Diffie – Hellman (DH)

Giao thức này dựa trên nguyên lý của bài toán logarit rời rạc trên trường số nguyên hữu hạn. Các thao tác thực hiện trao đổi khóa Diffie-Hellman giữa hai đối tác A và B như sau:

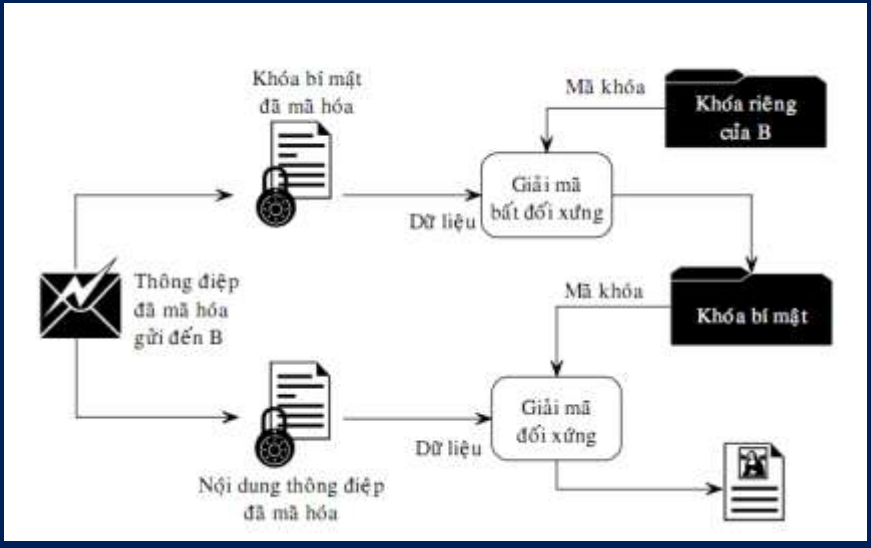
- A và B thống nhất các giá trị g và số nguyên tố $p < g$
- A chọn một số ngẫu nhiên m. A tính giá trị $Q_A = g^m$ và gởi Q_A cho B
- B chọn một số ngẫu nhiên n. B tính giá trị $Q_B = g^n$ và gởi Q_B cho A
- A nhận được Q_B và tính giá trị $k = (Q_B)^m = g^{n \times m}$
- B nhận được Q_A và tính giá trị $k = (Q_A)^n = g^{m \times n}$

k chính là giá trị bí mật được quy ước chung.

Quy trình mã hóa thư điện tử



Quy trình mã hóa thư điện tử



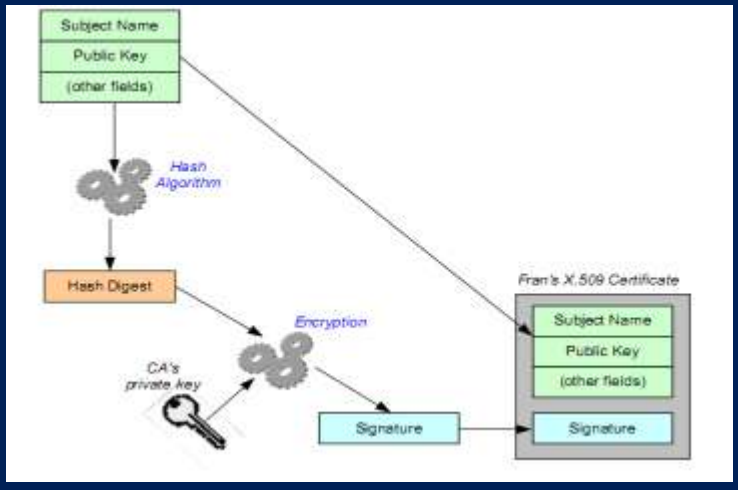
Hạ tầng khóa công khai PKI

- Public key infrastructure, viết tắt (PKI) là một cơ chế để cho một bên thứ 3 (thường là nhà cung cấp chứng thực số) cung cấp và xác thực định danh các bên tham gia vào quá trình trao đổi thông tin.

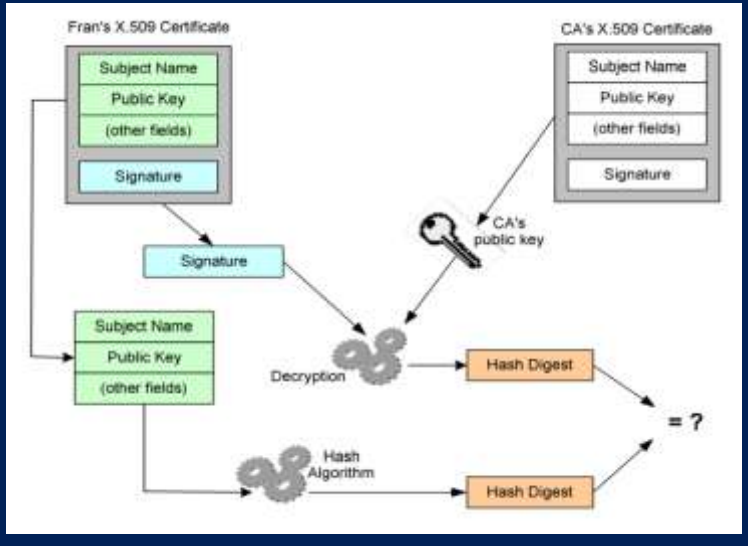
- Cơ chế này cho phép gán cho mỗi người sử dụng trong hệ thống một cặp Key là public/private.

- Khái niệm hạ tầng khóa công khai (PKI) thường được dùng để chỉ toàn bộ hệ thống bao gồm nhà cung cấp chứng thực số (CA) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mật mã khoá công khai trong trao đổi thông tin.

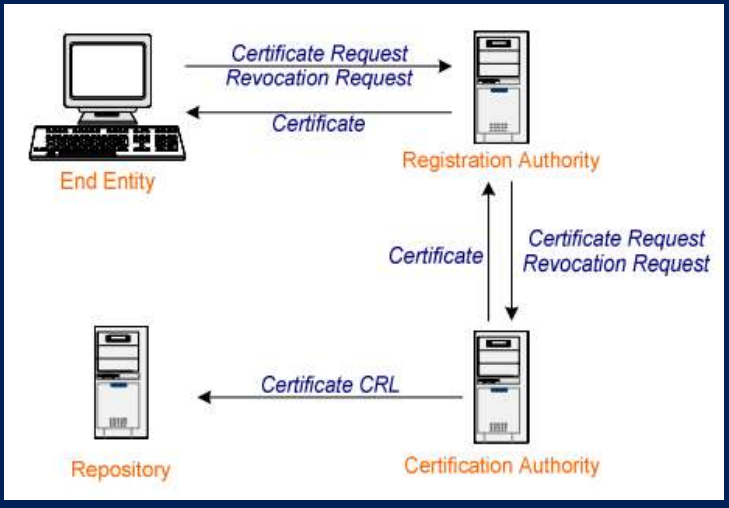
Quá trình ký chứng nhận



Quá trình kiểm tra chứng nhận



Mô hình PKI cơ bản



Các pp tấn công mạng

1. Nghe lén thông tin
2. Tấn công lỗ hổng (Tiêm mã SQL, chèn mã lệnh…)
3. Tấn công từ chối dịch vụ
4. Lan truyền virus, mã độc
5. Chiến tranh thông tin trên mạng