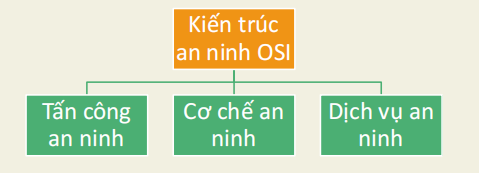
1, Kiến trúc an ninh OSI:  
 **kiến trúc an ninh osi: xác định cách tiếp cận có hệ thống để cung cấp các giải pháp bảo mật ở mỗi lớp trong mô hình 7 lớp OSI nhằm bảo mật dl truyền qua mạng**

  
 tấn công an ninh: được định nghĩa bất kỳ hành động nào mà làm tổn hại đến hệ thống

Cơ chế an ninh: 1 quy trình mà được thiết lập để ngăn chặn , phát hiện, khắc phục 1 hành   
 1 hành vi tấn công gây xâm hại nào đó

Dịch vụ an ninh: 1 dịch vụ giúp tăng cường bảo mật cho hệ thống, nhằm ngăn chặn các

Cuộc tấn công gât xâm hại

Có 2 loại tấn công an ninh: thụ động và chủ động   
 thụ động: là cuộc tấn công cố gắng tìm hiểu tài nguyên của hệ thống nhưng ko gây ảnh hưởng đến hệ thống, hình thức nghe lén, giám sát (do tấn công thụ động ko làm thay đổi tài nguyên hệ thống nên khó phát hiện, cần phải có các kĩ thuật phòng ngừa như mã hóa)  
 chủ động: là cuộc tấn công cố gắng thay đổi tài nguyên hệ thống từ đó làm ảnh hưởng đến hệ thống. Chia làm 4 loại: giả mạo(1 thực thể giả vờ là thực thể khác), phát lại(nắm bắt dữ liệu thụ động và truyền lại sau đó tạo hiệu ứng ko xác thực), sửa đổi thông tin(tin nhắn đã bị sửa để tạo ra hiệu ứng ko xác thực), từ chối dịch vụ(là việc ngăn chặn truy cập các dịch vụ của máy chủ). Cũng khó để ngăn chặn tấn công chủ động, Mục tiêu là phát hiện và khắc phục

Cơ chế an ninh: Là những cơ chế bảo mật ở các lớp giao thức cụ thể. Gồm có cơ chế an ninh chuyên biệt và cơ chế an ninh phổ quát

Dịch vụ an ninh: là 1 dịch vụ được cung cấp bởi 1 lớp giao thức của hệ thống mở truyền thông. Đảm bảo bảo mật dữ liệu. Có 5 laoij dịch vụ an ninh: xác thực(đảm bảo thực thể là đáng tin cậy), điều khiển truy cập(ngăn chặn sử dụng trái phép tài nguyên), bảo mật dl(bảo vệ dữ liệu ko bị tiết lộ 1 cách trái phép), toàn vẹn dl(đảm bảo dữ liệu khi nhận thì sẽ toàn vẹn như khi gửi mà lúc đó người gủi đã được xác thực), tính chối bỏ(cung cấp sự bảo vệ để chống lại sự từ chối bởi 1 trong các thực thể tham gia vào 1 or nhiều giao tiếp truyền thông)

---------------------------------------------------------------------------------------------------------------------

Mật mã học gắn liền với quá trình mã hóa

Mật mã học giúp đảm bảo các yếu tố sau:  
 tính bảo mật: đảm bảo thông tin ko bị tiết lộ trái phép  
 tính toàn ven: thông tin đến người nhận là giống như lúc gửi  
 tính xác thực: đảm bảo người gửi or nhận là đúng họ  
 tính chống chối bỏ: người gửi or nhận sau này ko thể chối bỏ việc đã gửi or nhận thông tin

Phân loại thao tác để chuyển bản rõ thành bản mã: thay thế, chuyển vị  
Số khóa sử dụng: khóa đơn-khóa bí mất(mã hóa đối xứng) và hai khóa-khóa công khai(mã hóa bất đối xứng)   
cách xử lý bản rõ: mã hóa khối và mã hóa luồng

Thám mã: phân tích mật mã  
Các pp tấn công thám mã: tìm khóa vét cạn, phân tích thống kê, phân tích toán học

DES:   
Đặc điểm: là 1 thuật toán mã hóa khối, mỗi khối dài 64 bit  
 khóa dùng trong des có độ dài 64 bit, tuy nhiên chỉ có 56 bit thực sự được dùng và 8 bit dành cho việc kiểm tra  
 des xuất ra bản mã 64 bit  
 thuật toán thực hiện 16 vòng lặp, khác nhau về khóa trong mỗi vòng lặp đó  
 mã hóa, giải mã thì sử dụng cùng 1 khóa  
Khái quát thuật toán DES:  
 với mỗi khóa k và bản rõ x, quá trình lập mã diễn ra như sau:  
 ban đầu, dùng 1 phép hoán vị ip: từ x 64 bit được chia ra làm 2 nửa L0 và R0 mỗi nửa 32 bit  
 từ cặp L0, R0 sẽ dùng 15 lần phép toán giống nhau để được các cặp (L1, R1)...(L15,R15) sau đó dùng phép toán hoán vị đảo nghịch R15L15 ta sẽ được bản mã y tương ứng

Three-DES:  
Thuật toán mã hóa 3DES gồm 3 chìa khóa 64 bit, tức là toàn bộ chiều dài khóa là 192 bit: 3 khóa DES là k1, k2, k3

Thủ tục mã hóa cũng tương tự DES nhưng nó lặp lại3 lần. Dữ liệu được mã hóa với chìa khóa 1, sau đó giải mã với chìa khóa 2 và được mã hóa lần nữa với chìa khóa 3 => thu được dữ liệu mã hóa cuối cùng

Ưu điểm: An toàn hơn so với DES do được mã hóa 3 lần  
Nhược điểm: vì 3DES sử dụng 3 lần mã hóa nên tốc độ mã hóa chậm hơn so với DES. Phần mềm ứng dụng tỏ ra rất chậm đối với hình ảnh số và 1 số ứng dụng dữ liệu tốc độ vào vì kích thước khối 64bit vẫn là nhược điểm đối với những hệ thống hiện nay

AES:  
AES được nghiên cứu và phát triển để thay thế DES  
AES là giải pháp tốt nhất để bảo vệ thông tin nhạy cảm cho chính phủ mỹ vào thế kỷ 21  
AES gồm 3 mật mã khối: AES-128,192,256, t.ứng với độ dài của key là 128bit, 192bit và 256bit. Số vòng của key khác nhau cụ thể 10 vòng cho 128bit, 12 vòng cho 192bit và 14 vòng cho 256 bit  
Mỗi vòng đều thực hiện 3 bước thay thế, biến đổi và hòa trộn khối plainText thành cipherText

#.Mã Hóa Công Khai:  
Vì sao ra đời mã hóa công khai: Ko cần trao đổi khóa

Hệ mật RSA:   
Là hệ mật dùng phổ biến trong Chữ ký số, mã hóa , thương mại điện tử  
Trao đổi khóa diffie-hellman:  
là 1 trong những phát triển quan trọng của mã hóa công khai, dùng phổ biến trong các giao thức bảo mật  
Cho phép 2 bên chưa từng gặp nhau trước đây thiết lập 1 khóa an toàn để trao đôit thông tin   
Có 2 khía cạch khác biệt đối với việc sử dụng mật mã khóa công khai về vấn đề quản lý khóa:  
Phân phối khóa công khai và sử dụng hệ thống khóa mã hóa công khai để phân phối khóa bí mật(mã hóa công khai được dùng để thiết lập khóa bí mật cho mỗi phiên trao đổi dữ liệu của mã hóa đối xứng)  
Một số kỹ thuật được dùng để phân phối khóa công khai:  
Thông báo công khai[1], thẩm quyền khóa công khai, chứng thực khóa công khai

-- Thông báo công khai:   
 Khi 2 người muốn truyền dữ liệu cho nhau bằng mã hóa khóa công khai trước tiên họ phải trao đổi khóa công khai với nhau

Ưu điểm: Thuận lợi  
 Nhược điểm: bất kỳ ai cũng có thể giả mạo người khác để quảng bá khóa công khai của mình

-- Thẩm quyền khóa công khai:   
Trung tâm thẩm quyền duy trì 1 thư mục động chứa tất khóa công khai của tất cả người tham gia. Ngoài ra mỗi người tham gia đều biết khóa công khai của trung tâm và chỉ trung tâm mới biết khóa bí mật tương ứng   
< một phần nữa để tại màn hình chính >

--Chứng thực khóa công khai:  
chứng thực bao gồm khóa công khai ghép với số nhận dạng của chủ sở hữu khóa, toàn bộ thông tin đc kí bởi bên thứ 3 đáng tin câyj thường là cơ quan nhà nước  
chứng thực khóa công khai có 4 yêu cầu:  
+, bất kỳ người tham gia nào cũng có quyền đọc chứng thực để xác minh tên và khóa công khai của chủ sở hữu khác  
+, Bất kỳ người tham gia nào cũng có thể xác minh rằng chứng thực có nguồn gốc  
+, bất kỳ người tham gia nào cũng có thể xác minh tính hiện thời của chứng thực  
+, Chỉ tổ chức chức phát hành chứng thực mới có thể tạo và câph nhật chứng thực  
< một phần nữa để tại màn hình chính >

Hàm băm mật mã : là 1 hàm băm với 1 số tính chất bảo nhật nhất định phù hợp cho các ứng dụng bảo mật thông tin  
Hàm băm nhận đầu vào là 1 sâu ký tự tùy ý và tạo ra kết quả có độ dài nhất định. 1 số hàm băm md5, sha-1

Chữ kí số sử dụng RSA:  
- để tạo chữ kí người gửi sẽ dùng private key và người nhận sẽ dùng public key để xác thực  
-Chữ kí số thường dùng pp mã hóa giá trị Hash của bản tin  
- HASH là hàm 1 chiều vì vậy dù có hash cũng ko biết được abrn tin gốc  
 độ dài hash thường rất nhỏ, vì thế chữ kí số sẽ ko chiếm nhiều dung lượng

Chữ kí số sử dụng RSA để:  
xác định nguồn gốc  
Bảo toàn bản tin  
CHống chối bỏ