Câu 1 : so sánh đặc điểm hệ mật mã khóa đối xứng và không đối xứng

|  |  |
| --- | --- |
| Hệ mật mã khóa đối xứng | Hệ mật mã khóa bất đối xứng |
| * Khóa bí mật * Sử dụng một khóa duy nhất cho cả quá trình mã hóa và giải mã * Kích thước ngắn (64,128,192bit ) * Tốc độ nhanh * Khó quản lý và phân phối | * Khóa công khai * Sử dụng một cặp khóa một khóa cho mã hóa và một khóa cho giải mã * Kích thước lớn (1024-3072 bit) * Tốc độ chậm * Độ an toàn cao * Thuận lợi quản lý và phân phối |

Câu 2: Giải thích vì sao phải đảm bảo an toàn cho thông tin

* Do chúng ta sống trong thế giưới kết nối

+ mọi thiết bị tính toán truyền thông đều có kết nối internet

* Có nhiều nguy cơ , đe dọa mất an toàn thông tin , hệ thống, mạng

+ tấn công từ tin tặc , lạm dụng người dùng

+ lây nhiễm qua các phần mềm độc hại

+ nghe trộm đánh cắp sửa đổi thông tin

+lỗi trong phầm cứng hoặc phần mềm

Câu 3: Hãy giải thích các lớp phòng vệ điển hình trong mô hình đảm bảo an toàn hệ thống thông tin có chiều sâu defence in depth

Defense-in-Depth: phòng thủ theo chiềều sâu

* Có 7 lớp phòng vệ

+ lớp thủ tục chính sách: thiết lập quy định, chính sách bảo mật, kế hoạch khôi phục thảm họa

+ lớp vật lý : sử dụng khóa , thẻ từ cam giám sát … để bảo vệ máy chủ , thiết bị mạng và dữ liệu

+ lớp ngoại vi: bảo vệ biên giới giữa mạng nội bộ và mạng bên ngàoi sử dụng Tường lửa, vpn,..

+ lớp nội bộ mạng : bảo vệ mạng nội bộ nơi thiết bị và ng dùng giao tiếp với nhau sử dụng IDS/IPS giám sát phân tích lưu lượng mạng ngăn chặn các mối đe dọa

+ lớp host: bảo vệ máy chủ và các thiết bị cá nhân trong mạng : phần mềm diệt viruts , quản lý cập nhật …

+ lớp ứng dụng : bảo vệ các ứng dụng sử dụng xác thực phân quyền , kiếm tra lỗ hộng bảo mật

+ lớp dữ liệu : bảo vệ dữ liệu khi nhận và truyền tải bằng cách mã hóa dữ liệu , sao lưu định kì , kiểm soát truy cập dữ liệu

Câu 4: Giải thích các thuộc tính an ninh an toàn của hệ thống thông tin theo mô hình CIA

Gồm 3 thuộc tính chính :

* Confidentiality( tính bí mật ):

+ chỉ người dùng có thẩm quyền mới được truy cập thông tin

+ được đảm bảo bằng kênh mã hóa vpn

* Integrity( tính toàn vẹn):

+thông tin chỉ được sửa đổi bởi người có thẩm quyền

+ liên quan đến tính hợp lệ và chính xác của dữ liệu

* Availability(tính sẵn dùng)

+ thông tin có thể truy nhập bởi người dùng hợp pháp bất cứ lúc nào họ có yêu cầu

+ được đo bằng các yếu tố : thời gian cung cấp dịch vụ, thời gian khắc phục sự cố ,…..

Câu 5: giải thích quan hệ giữa mối đe dọa và lỗ hổng trong hệ thống thông tin và liệt kê các mối đe dọa thường gặp

+ mối đe dọa : hành động gây hại cho hệ thống

+ lỗ hổng : điểm yếu của hệ thống

* Quan hệ:

+ Các mối đe dọa thường khai thác một hoặc một số lỗ hổng đã biết để thực hiện các cuộc tấn công phá hoại;

+ Nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực;

+ Không thể triệt tiêu được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tận dụng để tấn công.

* Các mối đe dọa:

+ Phần mềm độc hại

+ Hư hỏng phần cứng hoặc phần mềm

+ Kẻ tấn công ở bên trong

+ Mất trộm các thiết bị

+ Kẻ tấn công ở bên ngoài

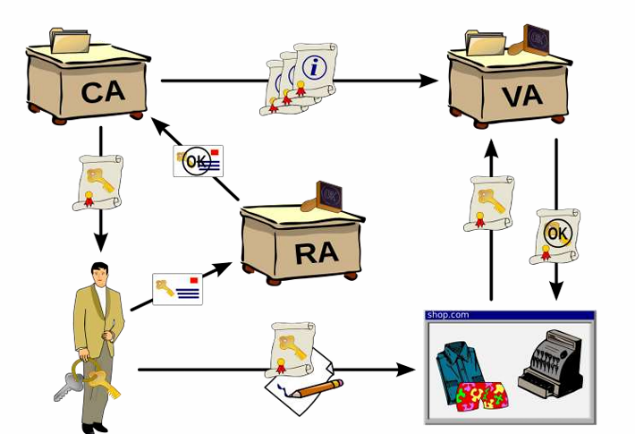
+ Tai họa thiên nhiên

+ Gián điệp công nghiệp

+ Khủng bố phá hoại.

Câu 6: giống câu 5

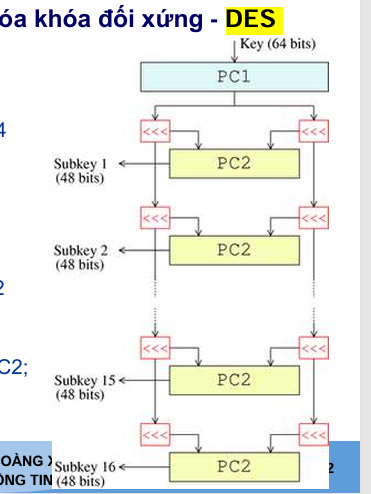
Câu 7: Hãy vẽ sơ đồ cấp và sử dụng chứng chỉ số , giải thích sơ đồ (111)



Giải thích:

* Người dùng đăng kí chứng chỉ số với RA
* RA kiểm tra thông tin người dùng cung cấp nếu mọi thông tin hợp lệ thì RA gửi thông tin đến CA(bộ phận cấp ccs)
* CA gửi lại khóa công khai và bí mật cho ng dùng
* Người dùng tiến hành tài khoản để mua hàng,…trên trang tmđt
* Trang TMĐT gửi yêu cầu về bộ phận VA (xác nhận thông tin)
* CA gửi thông tin về cho VA để xác thực
* Nếu hợp lệ thì VA gửi thông báo oke đến trang TMĐT cho phép ng dùng sd

Câu 8: Trong hệ mã hóa DES , vẽ sơ đồ thuật toán các bước sinh khóa phụ của hệ mã , giải thích sơ đồ



Giải thích:

+ khóa được cung cấp dưới dạng 64 bit

+ 56 bit dùng cho khóa chính PC1 , 8 bit được hủy hoặc kiểm tra chẵn lẻ

+ 56 bit chia thành 2 phần xử lý riêng và mỗi phần được quay trái 1 or 2 bit (tạo ra nửa khóa mới cho từng vòng)

+ 2 phần được ghép lại và 48 bit được chọn làm khóa phụ 1 bởi PC

+ lặp lại để tạo 15 khóa phụ còn lại

Câu 9: so sánh 2 loại phần mềm độc hại virus và worm

| **Tiêu chí** | **Virus** | **Worm** |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| **Cách lây lan** | Cần phải gắn vào một tệp tin hoặc chương trình để lây lan. | Lây lan độc lập, không cần gắn vào tệp tin. |

|  |  |  |
| --- | --- | --- |
| **Tác động** | làm hỏng hoặc thay đổi tệp tin và chương trình. | gây tắc nghẽn mạng ,tiêu tốn băng thông. |

|  |  |  |
| --- | --- | --- |
| **Khả năng tự nhân bản** | Virus không tự nhân bản; nó cần một hành động từ người dùng (ví dụ: mở tệp tin). | Worm có khả năng tự nhân bản và phát tán qua mạng mà không cần sự can thiệp của người dùng. |

|  |  |  |
| --- | --- | --- |
| **Phương thức lây lan** | Lây lan qua tệp tin, ổ đĩa USB, email, hoặc mạng chia sẻ. | Lây lan qua mạng (Internet, mạng LAN) thông qua các lỗ hổng bảo mật. |

|  |  |  |
| --- | --- | --- |
| **Mục tiêu** | Nhắm đến tệp tin và chương trình trên máy tính. | Nhắm đến mạng và hệ thống, tìm kiếm các máy tính dễ bị tổn thương. |

|  |  |  |
| --- | --- | --- |
| **Khả năng ẩn nấp** | Thường ẩn mình trong các tệp tin hợp pháp. | Có thể hoạt động công khai, nhưng sử dụng các kỹ thuật để ẩn mình khỏi các phần mềm chống virus. |

|  |  |  |
| --- | --- | --- |
| **Nguy cơ** | Có thể gây thiệt hại cho dữ liệu cá nhân và hệ thống. | Có thể gây hại nghiêm trọng cho toàn bộ mạng, làm chậm hoặc tê liệt hệ thống. |

Câu 10: Nêu biện pháp điều khiển truy cập DAC , cho ví dụ

* Là các cơ chế hạn chế truy nhập đến các đối tượng dựa trên thông tin nhận dạng của chủ thể or nhóm chủ thể
* Các thông tin nhận dạng

+ bạn là ai (cmnd , vân tay, blx)

+những cái bạn biết(tên truy nhập, mk, số pin)

+ bạn có gì (thẻ ATM, thẻ tín dụng )

* DAC cho phép ng dùng cấp or hủy quyền truy nhập các ng dùng khác đến các đối tượng thuộc quyền điều khiển của họ
* Vd : driver, fb, shopee, zalo

Câu 11: phân tích kĩ thuật kiểm soát truy nhập trên tường lửa , liệt kê hạn chế của tường lửa

* Kiểm soát dịch vụ : xác định dv nào đc truy nhập, hướng ra và vào
* Kiểm soát hướng: điều khiển hướng đc phép đi của các gói tin của mỗi dịch vụ
* Kiểm soát người dùng: xđ người dùng nào được quyền truy nhập (thường là ng dùng trong nội bộ mạng)
* Kiểm soát hành vi: kiểm soát việc sử dụng các dịch vụ cụ thể vd: tl có thể lọc loại bỏ thư rác, hạn chế truy nhập đến một bộ phận thông tin của máy chủ
* Hạn Chế:

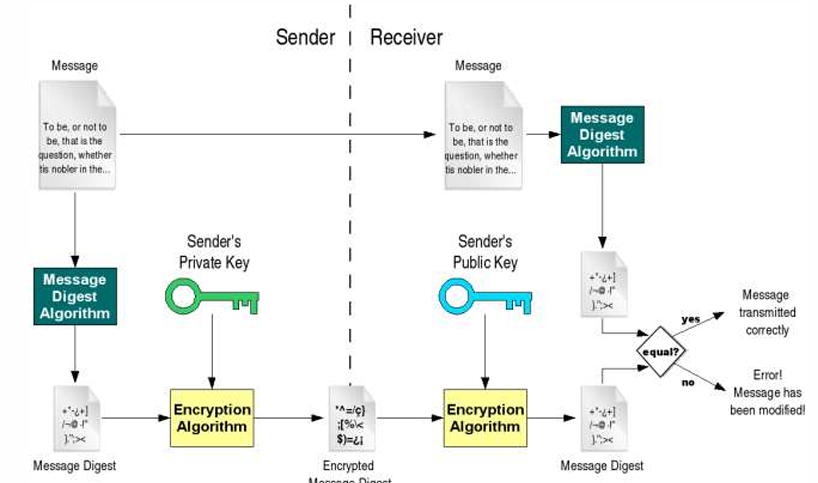
+ không thể chống các các nhân o đi qua nó

+ không chống các tấn công hướng dữ liệu or tấn công vào lỗ hổng an ninh của phần mềm

+ không chống lại hiểm họa từ bên trong (mạng nội bộ)

+ không ngăn chặn các chương trình, file nhiễm virus hoặc phầm mềm độc hại

Câu 12: Vẽ sơ đồ quá trình tạo kiểm tra chữ kí số , giải thích



* Các bước của quá trình ký một thông điệp (bên người gửi):

♣ Tính toán chuỗi đại diện (message digest/hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm);

♣ Chuỗi đại diện được ký sử dụng khóa riêng (Private key) của người gửi và một giải thuật tạo chữ ký (Signature/Encryption algorithm). Kết quả là chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encrypted message digest);

♣ Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được ký (Signed message);

♣ Thông điệp đã được ký (Signed message) được gửi cho người nhận.

* Các bước của quá trình kiểm tra chữ ký (bên người nhận):

♣ Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;

♣ Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký);

♣ Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số ◊ chuỗi đại diện thông điệp MD2;

♣ So sánh MD1 và MD2:

• Nếu MD1 = MD2 ◊ chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).

• Nếu MD1 <> MD2 ◊ chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

Câu 13: Giải thích cách tấn công social engineering và nêu cách phòng chống

* Giải thích: sử dụng các kĩ thuật xã hội đã thuyết phục người dùng tiết lộ thông tin truy nhập hoặc các thông tin có giá trị cho kẻ tấn công hoặc lợi dụng sự ngây tho và long tham của con người
* Ví dụ:
* Cách phòng chống:

+ kiểm tra , cảnh giác về nguồn gốc thông tin

+ bảo mật thông tin cá nhân

+ sử dụng xác thực 2 yếu tố

+ nâng cao hiểu biết về các hình thức tấn công

Câu 14: cho biết thành phần chức năng của hạ tầng quản lý khóa công khai

* Chức năng : là một tập hợp các phần cứng , phần mềm , nhân lực , chính sách và các thủ tục để tạo , quản lý , phân phối, sử dụng , lưu trữ và thu hồi các chứng chỉ số
* Thành phần:

+CA: cơ quan cấp và kiểm tra chứng chỉ số

+RA: bộ phận kiểm tra thông tin nhận dạng của nd theo yêu cầu của CA

+VA: cơ quan xác nhận thông tin nhận dạng của nd thay mặt CA

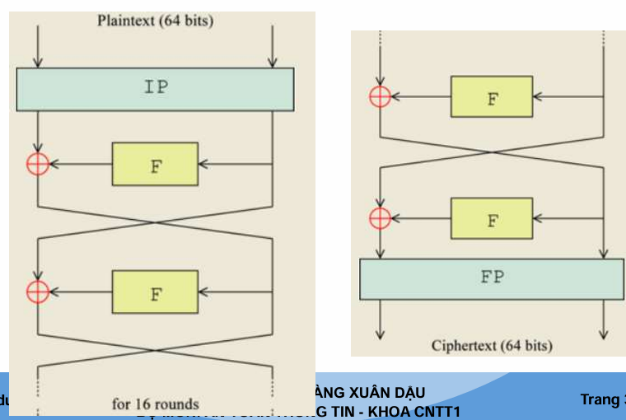
+CD: Nơi lưu danh mục và lập chỉ số các khóa

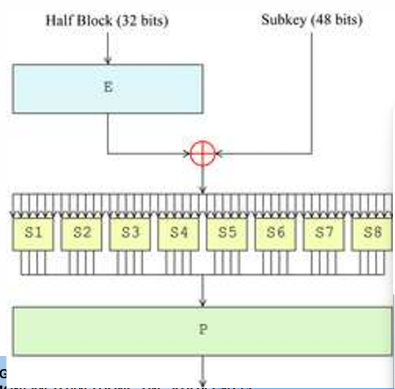
+ Hệ thống quan lý chứng chỉ

+Chính sách về chứng chỉ

Câu 15: Trong hệ mã hóa des , hãy vẽ sơ đồ thuật toán các bước xử lý chính của hệ mã và giải thích sơ đồ

* Sơ đồ





* Giải thích

+ Chia 64 bit thành 2 khối 32 bit và xử lý lần lượt và thực hiện hàm fiestel với khối 32 bit

+E : thực hiện mở rộng 32bit thành 48 bit (nhân dôi một nửa số bit)

+hàm so(+): trộn 48bit ở bước E với khóa phụ 48bit . Có 16 khóa phụ được tạo từ khóa chính để sử dụng cho 16 vòng lặp

+Si: khối dl 48bit chia thành 8 khối 6bit và chuyển cho các bộ thay thế (s1-s8)

Mỗi bộ thay thế sử dụng phép chuyển đổi phi tuyến tính để chuyển 6bit vào thành 4 bit ra theo bảng tham chiếu .các bộ thay thế là thành phần nhân an ninh của DES

+P: 32 bit đầu ra từ các bộ thay thế đc xắp sếp bằng phép hoán vị cố định cho đầu ra 32bit

Câu 16: Giải thích cơ chế phát hiện xâm nhập dựa trên chữ kí của hệ thống IDS/IPS

* Cơ sở dữ liệu chữ kí : chứa các mẫu tấn công và dấu hiệu của các tấn công đã biết
* Khi dữ liệu được thu thập từ nguồn chuyển đến bộ phân tích của hệ thống
* Bộ phân tích sẽ so sánh dữ liệu với cơ sở dữ liệu chữ kí
* Nếu trùng khớp , hệ thống xác định đây là một cuộc tấn công và tiến hành cảnh báo ngăn chặn tới ng dùng
* IDS ghi lại sự kiện và gửi cảnh báo
* IPS: ngăn chặn bằng cách chặn lưu lượng ….

Câu 19: Trình bày cơ chế điều khiển truy nhập MAC và cho ví dụ

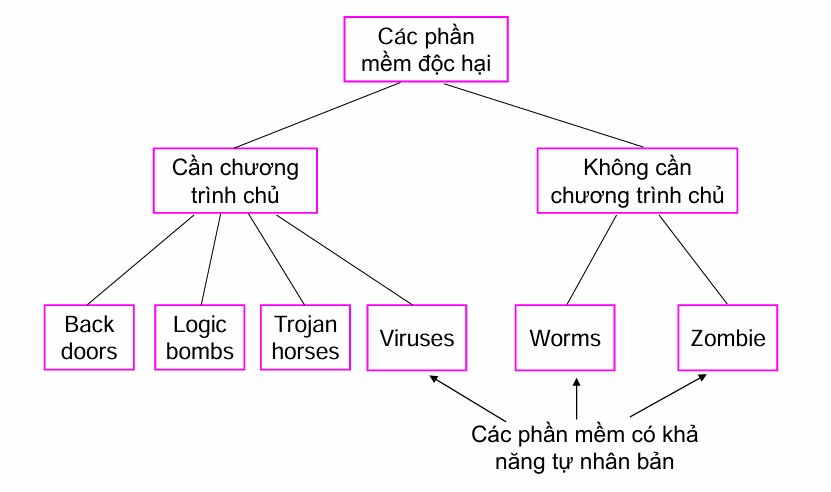
* Mỗi tài nguyên và người dùng được gắn nhãn bảo mật
* Quyền truy cập đc thiết lập dựa trên bảo mật ng dùng o thể thay đổi
* Khi một ng dùng truy nhập vào hệ thống hệ thống sẽ so sánh nhãn của ng dùng và nhãn của hệ thống
* Nếu nhãn trùng thì sẽ được truy nhập
* VÍ DỤ : người dùng A được cấp nhãn SECRET

Tài liệu 1 có nhãn Top Secret

Tài liệu 2 có nhãn secret

* Người dùng A đc phép truy nhập tài liệu 2 và o đc tn vào tl1

Câu 20: Sơ đồ phân loại và cách phòng chống phần mềm độc hại



* Biện pháp phòng chống

+ Cập nhật hệ thống thường xuyên

+ sử dụng các biện pháp kiểm xoát truy nhập

+ khi hệ thống đã nhiễm thì cần : phát hiện, nhận dạng và loại bỏ

+ Cài các phần mềm diệt vius và các phần mềm độc hại

AVG antivirus

MACAFree