1. Trình bày các đặc điểm chính của thông tin

Tính tường minh: Thông tin cần phải rõ ràng và dễ hiểu để có thể truyền tải và sử dụng được.

Tính đầy đủ: Thông tin cần phải chứa đầy đủ thông tin liên quan để đáp ứng yêu cầu của người quản lý.

Tính thích hợp và dễ hiểu: Thông tin cần truyền đạt đến người nhận phù hợp với khả năng tiếp thu và dễ hiểu của họ.

Độ tin cậy khác nhau: Thông tin có mức độ tin cậy khác nhau, phụ thuộc vào nguồn gốc và xử lý.

2. Tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống thông tin?

Bảo vệ Quyền Riêng Tư: Thông tin cá nhân, dữ liệu tài chính và y tế cần được bảo vệ khỏi việc truy cập trái phép. Đảm bảo an toàn thông tin giúp ngăn chặn việc lộ thông tin cá nhân và bảo vệ quyền riêng tư của mọi người.

Ngăn Chặn Sự Tấn Công: Hệ thống thông tin thường bị những cuộc tấn công từ phía hacker, virus, mã độc và các thủ phạm khác. Bảo mật thông tin giúp ngăn chặn sự xâm nhập và bảo vệ hệ thống khỏi sự phá hủy và mất dữ liệu.

Bảo Vệ Quyền Sở Hữu Trí Tuệ: Thông tin về sản phẩm, dịch vụ và nghiên cứu cần được bảo vệ khỏi việc sao chép trái phép. An toàn thông tin đảm bảo rằng quyền sở hữu trí tuệ được bảo vệ và khuyến khích sáng tạo.

Đảm Bảo Khả Năng Hoạt Động Liên Tục: Hệ thống thông tin quan trọng cho hoạt động của tổ chức và xã hội. Bảo mật thông tin giúp đảm bảo rằng hệ thống hoạt động liên tục mà không bị gián đoạn bởi các cuộc tấn công hay lỗi kỹ thuật.

Tuân Thủ Quy Định Pháp Luật: Các quy định về bảo mật thông tin và quyền riêng tư đang ngày càng nghiêm ngặt. Đảm bảo an toàn thông tin giúp tổ chức tuân thủ các quy định này và tránh vi phạm pháp luật.

3. Mục đích bảo vệ thông tin trong hệ thống thông tin?

Ngăn ngừa mất mát, gây nhiễu, tung tin ...

Ngăn ngừa đe dọa an ninh của cá nhân, xã hội, quốc gia

Ngăn ngừa những hoạt động trái phép nhằm tiêu hủy, gây nhiễu, sao

chép, gây tắc nghẽn thông tin; ngăn ngừa các dạng quấy rối vào tài

nguyên thông tin và hệ thống thông tin

Bảo vệ quyền công dân về sự riêng tư và tính bảo mật của dữ liệu cá

nhân trong các hệ thống thông tin

Bảo vệ bí mật quốc gia, tính bảo mật của thông tin văn bản tương

ứng với quy định của luật pháp

Bảo đảm quyền lợi của các chủ thể trong quá trình truyền thông, chế

tác, sản xuất và sử dụng hệ thống thông tin

4. An ninh thông tin là gì? Nêu vai trò của An ninh thông tin?

An ninh – bảo đảm không thể gây hại đến hoạt động và

thuộc tính của một đối tượng nào đó, kể cả cấu trúc và thành

phần của nó

An ninh của một đối tượng có thể phân chia thành nhiều

dạng khác nhau.

Một trong những dạng đó là an ninh thông tin (bảo vệ thông

tin và những hoạt động với thông tin)

---

Vai trò An ninh thông tin

▪ Thông tin đối với con người cũng rất cần thiết như không khí, thức

ăn, nước uống.

▪ Thông tin giúp con người nâng cao hiệu quả công việc, phát sinh nhu

cầu xã hội, phát triển cá tính, tự tin ...

▪ Thông tin là phương tiện cơ bản trong giao tiếp, thiếu phương tiện

này đa phần các nhiệm vụ không thể hoàn thành

▪ Thông tin giúp tồn tại quá trình đào tạo, giáo dục để truyền đạt kiến

thức, kinh nghiệm ...

▪ Gây tổn hại đến thông tin hay khả năng tiếp nhận, suy nghĩ của một

người chính là làm giảm sức sống của người đó

▪ An ninh thông tin cá nhân là đảm bảo an toàn thông tin riêng tư, hoạt

động xã hội dựa trên cơ sở suy luận, suy nghĩ từ thông tin nhận được

5. Trong các kiểu tấn công mạng, hãy cho biết khái niệm DoS, DDoS ? Phân biệt sự khác

nhau cơ bản của DoS và DDoS?

Dos là xâm nhập vào mạng / máy chủ >>>khiến người dùng không truy cập máy chủ / mạng

DDoS là loại tấn công mạng sử dụng một số lượng lớn máy tính để gửi lưu lượng truy cập giả mạo đến một mục tiêu, khiến cho dịch vụ trở nên không hoạt động.

Khác nhau

Dos là phương thức sử dụng 1 thiết bị để tấn công 1 đối tượng khác

Ddos là sử dụng cùng lúc nhiều thiết bị / nguồn để tấn công 1 hoặc nhiều mục tiêu

6. Kỹ thuật tấn công kiểu Sniffing là gì? Hãy mô tả sơ lược về kỹ thuật tấn công này

sniffing là kĩ thuật đánh cấp thông tin truyền trên đường mạng

Khi A truyền thông tin cho B thì thông tin có thể bị đánh cấp bởi C mà A,B không biết

C có thể xem thông tin của A gửi cho B , gọi là nghe trộm

C có thể sửa thông tin của A sau đó gửi cho B , gọi là lừa đảo

Cách giảm thiểu:

1. Mã hóa dữ liệu trước khi truyền ra ngoài
2. Trao đổi khóa trên đường truyền an toàn
3. Sử dụng các kỉ thuật xác thuật toàn vẹn thông tin

7. Kỹ thuật tấn công kiểu Ransomware là gì? Hãy mô tả sơ lược về kỹ thuật tấn công này.

Rasonware là kĩ thuật tống tiền người dùng

Phương pháp 1 là mã hóa dữ liệu người dùng rồi yêu cầu tiền chuột để giải mã dữ liệu

Phương pháp 2 khóa thiết bị của người dùng rồi yêu cầu tiền chuột để mở khóa

Phương pháp 3 đánh cấp thông tin nhạy cảm rồi yêu cầu tiền chuộc để không công bố trên mạng xã hội

8. Vai trò của mã hóa trong an toàn thông tin?

Mã hóa thông tin:

Khái niệm:

Mã hóa là làm biến đổi thông tin gốc => thông tin mã hóa.

Có khả năng giải mã thông tin mã hóa => thông tin ban đầu

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Vai trò:

Đảm bảo tính bí mật (Confidentiality) cho thông tin.

Bên mã hóa có quyền lựa chọn bên giải mã (cung cấp khóa mã).

Một số thuật toán mã hóa cung cấp thêm tinh xác thực, tính toàn vẹn,

tính chống thoái thác...

9. Áp dụng phương pháp mã hóa đổi chỗ (hoán vị):

- Cho Plaintext là HAIPHONG, ngắt đoạn từng nhóm 4 ký tự; thứ tự tự nhiên trong mỗi nhóm là 1234;

- Khóa mã nhóm 1 là 2413 và khóa mã nhóm 2 là 3142.

- Hãy xác định Ciphertext?Plaintext: HAIP HONG

Nhóm 1: HAIP -> Khóa mã nhóm 1 (2413) -> APHI

Nhóm 2: HONG -> Khóa mã nhóm 2 (3142) -> NHGO

Vậy, Ciphertext tương ứng với Plaintext “HAIPHONG” khi sử dụng khóa mã đã cho là “APHI NHGO”.

10.

Cho bản rõ (Plaintext): “DAIHOCNGUYENTATTHANH”

a. Dùng phương pháp ma trận (5 cột) để chuyển vị “hàng thành cột” cho Plaintext trên.

b. Sử dụng mật mã Ceasar để mã hóa chuỗi đã chuyển vị ở phần trên với K=1

Cho biết bảng chữ cái:

a. Đầu tiên, ta sẽ sắp xếp Plaintext “DAIHOCNGUYENTATTHANH” thành một ma trận có 5 cột:

D A I H O

C N G U Y

E N T A T

T H A N H

Chuỗi sau khi chuyển vị là: “DCETANNHGTHUAYTH”.

: Sử dụng mật mã Ceasar với K=1. Mật mã Ceasar hoạt động bằng cách dịch chuyển mỗi ký tự trong bảng chữ cái xuống K vị trí. Với K=1, ‘A’ sẽ trở thành ‘B’, ‘B’ sẽ trở thành ‘C’, v.v., và ‘Z’ sẽ trở thành ‘A’.

A -> B ,B -> C, C -> D ,D -> E ,E -> F ,F -> G ,G -> H, H -> I ,I -> J ,J -> K

K -> L, L -> M ,M -> N ,N -> O, O -> P ,P -> Q, Q -> R, R -> S, S -> T ,T -> U ,U -> V

V -> W ,W -> X ,X -> Y ,Y -> Z ,Z -> A

Vậy, chuỗi “DCETANNHGTHUAYTH” sau khi được mã hóa bằng mật mã Ceasar với K=1 trở thành “EDFUBOOIHUIVBZUI”.

11. Vẽ sơ đồ và trình bày những đặc điểm các giải thuật mã hóa khóa đối xứng. Algorithm

|

+-----------------------+

| Symmetric |

| Encryption |

+-----------------------+

|

+------------------------------+

| |

Block Cipher Stream Cipher

| |

+-------------------------+ +-------------------------+

| Feistel Network | | Synchronous Stream |

| (e.g., DES) | | (e.g., RC4) |

+-------------------------+ +-------------------------+

| |

+-----------------------+ +-----------------------+

| Substitution | | XOR Operation |

| Permutation | | |

+-----------------------+ +-----------------------+

| |

+-------------------------+ +-------------------------+

| Key Schedule | | Key Stream |

| Generation | | Generation |

+-------------------------+ +-------------------------+

| |

+-----------------------------------------------+

| Key Management |

+-----------------------------------------------+

Symmetric Encryption Algorithm: Các thuật toán mã hóa khóa đối xứng sử dụng cùng một khóa cho cả quá trình mã hóa và giải mã.

Block Cipher vs. Stream Cipher:

Block Cipher: Dữ liệu được chia thành các khối có kích thước cố định trước khi mã hóa. Mỗi khối được mã hóa độc lập với các khối khác.

Stream Cipher: Dữ liệu được mã hóa bit theo bit hoặc byte theo byte.

Feistel Network: Một cấu trúc mã hóa block cipher mà mỗi khối dữ liệu được chia thành hai nửa và thực hiện một loạt các hoán vị và thay thế lặp lại trên nửa khối.

Substitution-Permutation Network: Cấu trúc trong đó các phần tử dữ liệu được thay thế và hoán vị theo một cách cụ thể để tạo ra sự phức tạp và hiệu quả trong việc mã hóa.

XOR Operation: Trong stream cipher, dữ liệu được mã hóa bằng cách thực hiện phép toán XOR với key stream, mỗi bit key stream được tạo ra từ khóa và được lặp lại hoặc sinh ra từ một hàm pseudo-random.

Key Schedule Generation: Quá trình tạo ra các khóa con từ khóa chính để sử dụng trong các vòng lặp hoặc trong các phép toán mã hóa.

Key Management: Quá trình quản lý, tạo ra, phân phối và bảo vệ khóa trong hệ thống mật mã.

Các thuật toán mã hóa khóa đối xứng cung cấp sự bảo mật hiệu quả khi sử dụng một khóa bí mật chung giữa người gửi và người nhận. Tuy nhiên, việc quản lý khóa là một yếu tố quan trọng cần được xem xét cẩn thận để tránh các vấn đề về an ninh.

12

Cho Plantext “NTTU” (biểu diễn theo ASCII: 01001110 01010100 01010100

01010101).

Sử dụng khóa là "CNTT" (01000011 01001110 01010100 01010100). Hãy xác định

Ciphertext theo phương pháp XOR ?

01001110 01010100 01010100 01010101

01000011 01001110 01010100 01010100

->00001101 00011010 00000000 000000001

13

Cho Plaintext P gồm 32 bit: “1100 0000 1010 1000 0001 1010 1000 0001”.

a. Sử dụng hệ mã dòng (Stream Cipher) để tạo bản mã C cho chuỗi Plaintext bằng thuật

toán XOR với khóa K = 8 bits “10101010”

b. Hãy sử dụng khóa K’ (8 bit bất kỳ và khác với khóa K trên) để giải mã cho bản mã C

trên để tạo thành bản rõ P’.

c. So sánh P’ và P.

a.

1100 0000 1010 1000 0001 1010 1000 0001

1010 1010 1010 1010 1010 1010 1010 1010

-> 0110 1010 0000 0010 1011 0000 0010 1011

b. k’ = 11001100

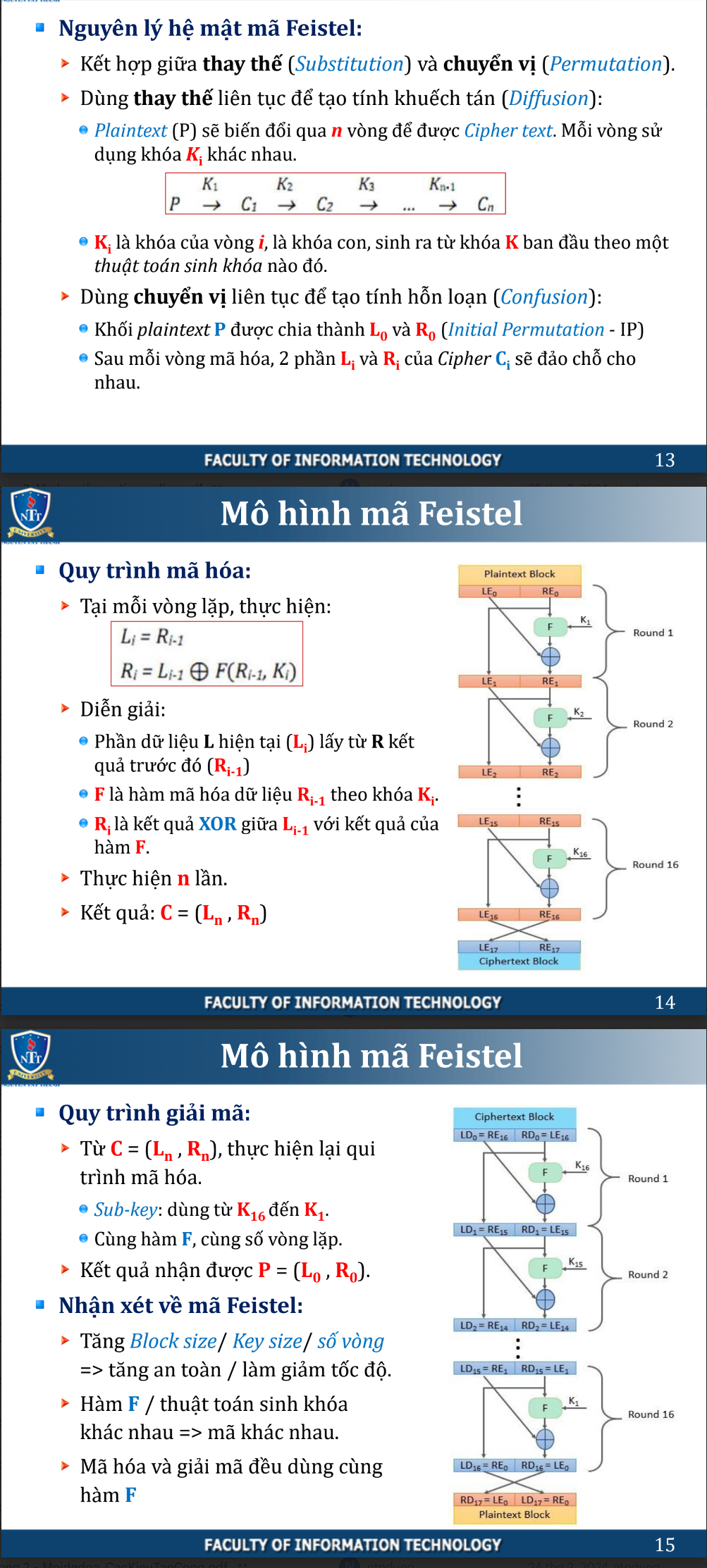
0110 1010 0000 0010 1011 0000 0010 1011

1100 1100 1100 1100 1100 1100 1100 1100

-> 1010 0110 1100 1110 0111 1100 1110 0111

c. p p’ kh giống nhau tại khác k

14. Trình bày tiến trình mã hóa Feitel.



15. Trình bày tổng quát về chuẩn mã hóa DES.

Tổng quan hệ mật mã DES:

Thiết kế bởi IBM (1975), chuẩn NIST (1977)

DES là dạng mã hóa Khóa đối xứng (Symmetric key).

Dùng phương pháp mã khối dựa theo hệ mã Feistel.

Block size = 64 bit (L-Block = R-Block = 32 bit).

Key size = 56 bit (Key dùng 48 bit, 8 bit dùng kiểm tra)

Số vòng lặp: 16 vòng.

Mã DES hiện nay không còn được coi là an toàn:

1998: “DES Cracker” phá mã DES trong 56 giờ

2006: COPACOBANA phá mã DES trong 9 ngày

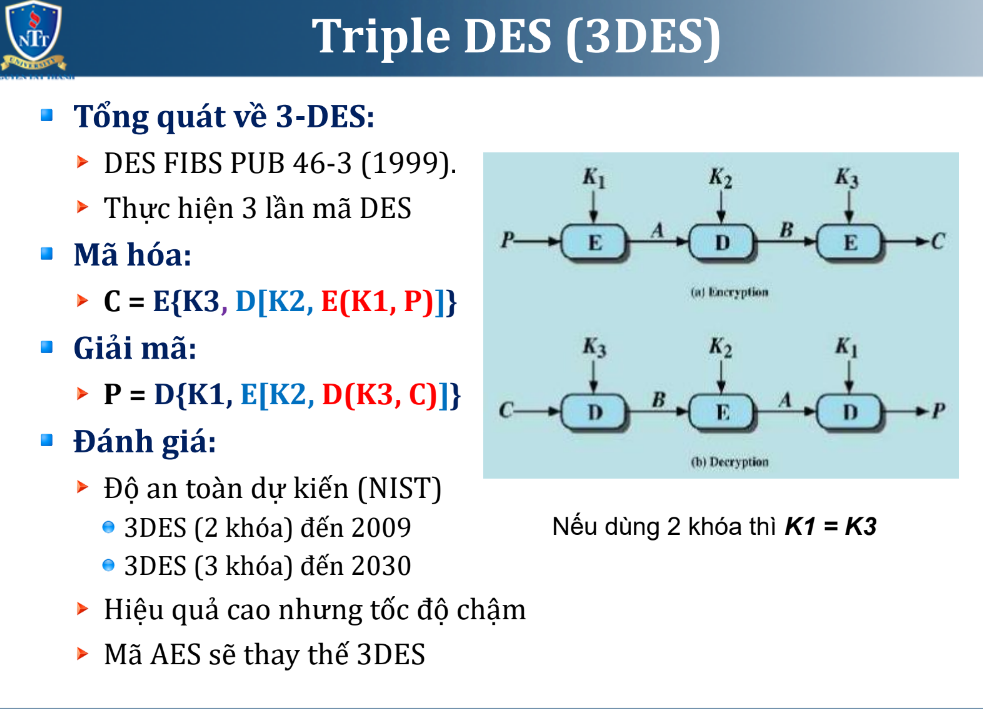
2006: Hệ thống khoảng 10.000 PC phá mã DES trong 1 đêm

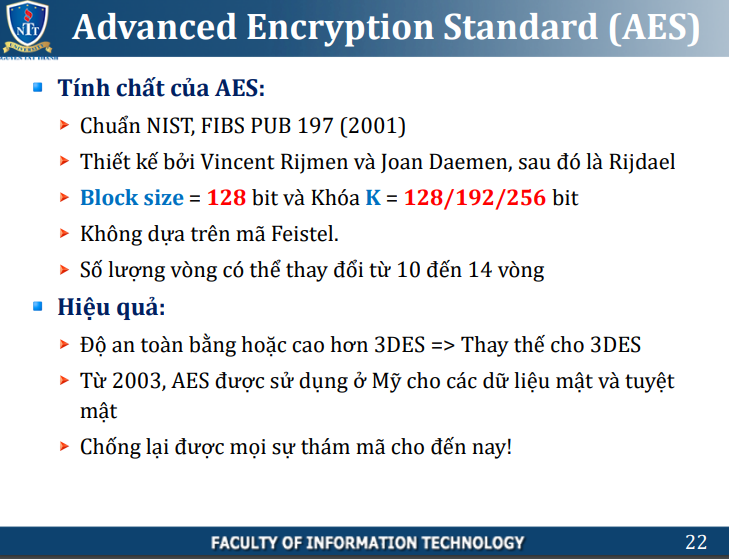
16. Chuẩn mã hóa 3-DES:

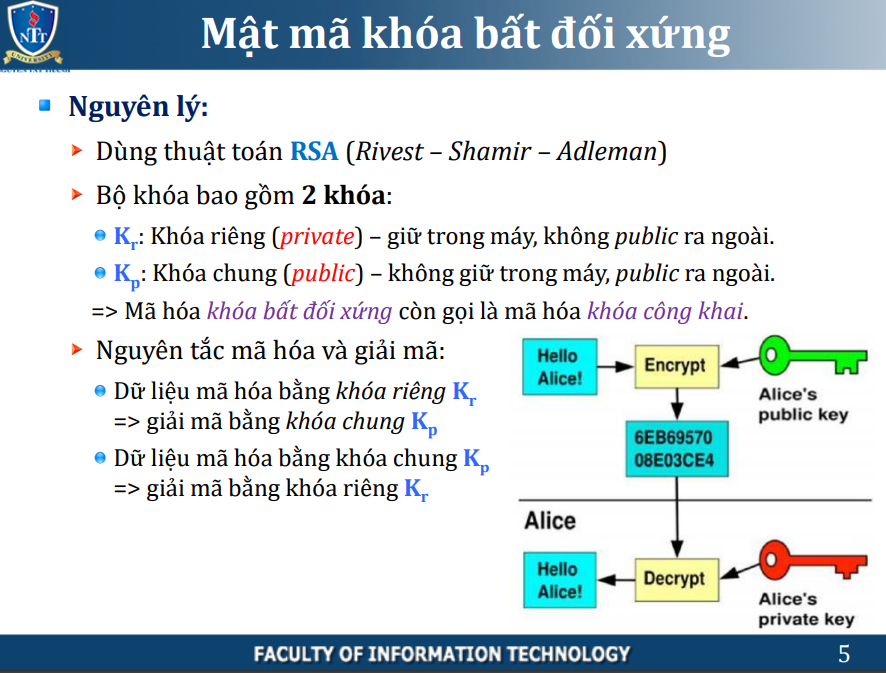
a. Viết công thức tổng quát của quy trình mã hóa thông điệp M theo chuẩn 3-DES dùng 3

khóa K1, K2, K3.

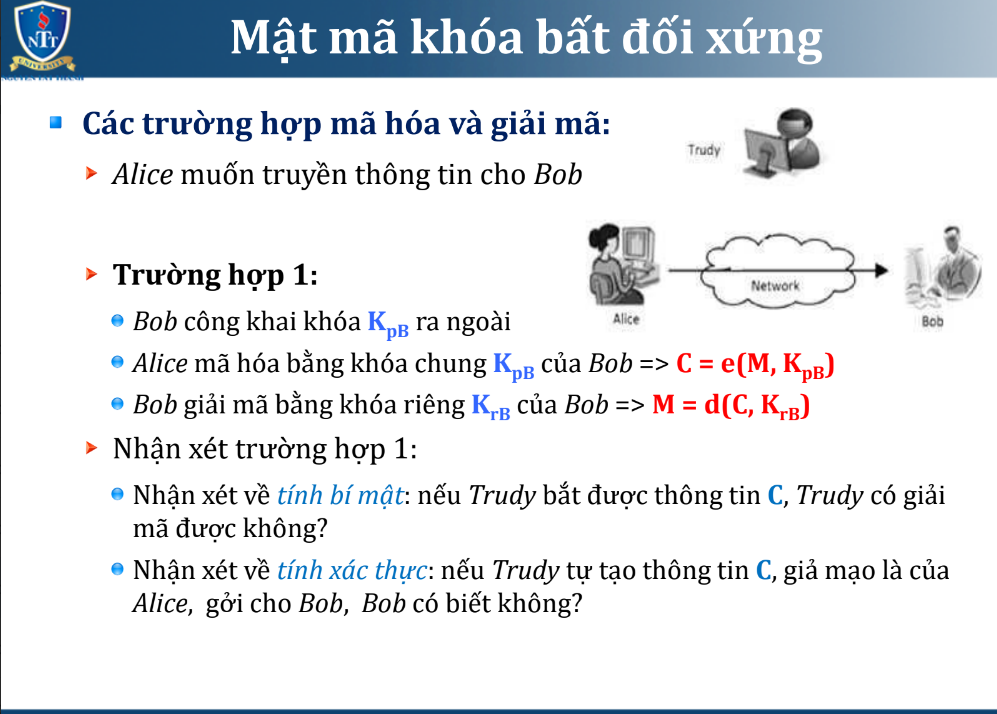
b. Viết công thức tổng quát của quy trình giải mã thông điệp C theo chuẩn 3-DES dùng 3

khóa K1, K2, K3

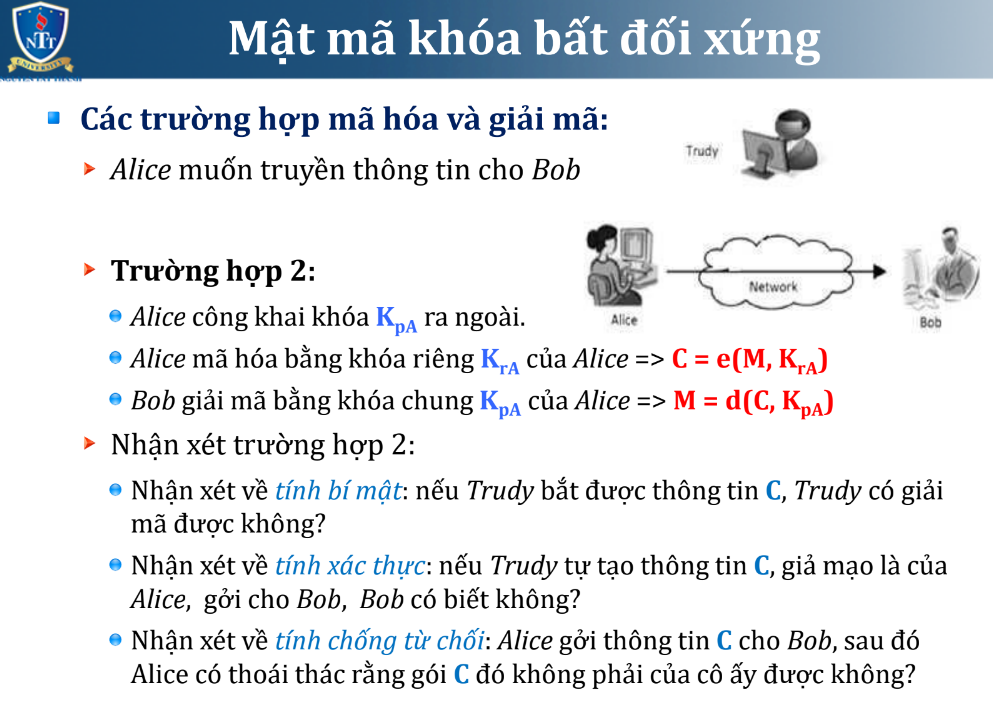
17. Đặc điểm của giải thuật mã hóa khóa đối xứng AES

18. Trình bày nguyên lý hoạt động của mã hóa khóa công khai (hay khóa bất đối xứng).

19. Trình bày quy trình sử dụng mã hóa khóa công khai nhằm đảm bảo tính bí mật

(Confidentiality) cho thông tin truyền từ Alice sang Bob.

20. Trình bày quy trình sử dụng mã hóa khóa công khai nhằm đảm bảo cho Bob xác thực

thông điệp nhận là từ Alice

21. Áp dụng thuật toán bình phương liên tiếp để tính

721 mod 13

71 mod 13 = 7

72 mod 13 = 10

74 mod 13 = 9

78 mod 13 = 3

716 mod 13 = 9

721 mod 13 = 716+4+1 mod 13

= (716 mod 13\*74 mod 13\*71 mod 13) mod 13

=(9\*9\*7) mod 13 = 567 mod 13 =8

22.

Tính và chọn cặp khóa Public key và Private key bằng thuật toán RSA theo lựa chọn

2 số nguyên tố: p = 3, q = 11

Cho biết quy trình RSA như sau:

- Tính số n = p.q

- Tính φ(n) = (p-1)(q-1)

- Chọn e sao cho: gcd(e, φ(n))=1

- Chọn d sao cho: (e.d)%φ(n)=1

- Khóa công khai KU = (e, n).

- Khóa bí mật KR = (d, n).

- Tính số n = p.q =33

- Tính φ(n) = (p-1)(q-1) = 20

- Chọn e sao cho: gcd(e, φ(n))=1 BẤM MÁY ->e=3 GCD(X,20) calc nào ra 1 thì chọn (không chọn 1)

- Chọn d sao cho: (e.d)%φ(n)=1 bấm máy ->d=7 (3.X)mod20 calc nào ra 1 là được

- Khóa công khai KU = (e, n). (3,33)

- Khóa bí mật KR = (d, n). (7,33)

23. Áp dụng thuật giải RSA: giả sử:

- Có cặp khóa: Public key KU(e,n) = (11,15) và Private key KR(d,n) = (3,15).

- Cho bản rõ M = 8.

Hãy tính:

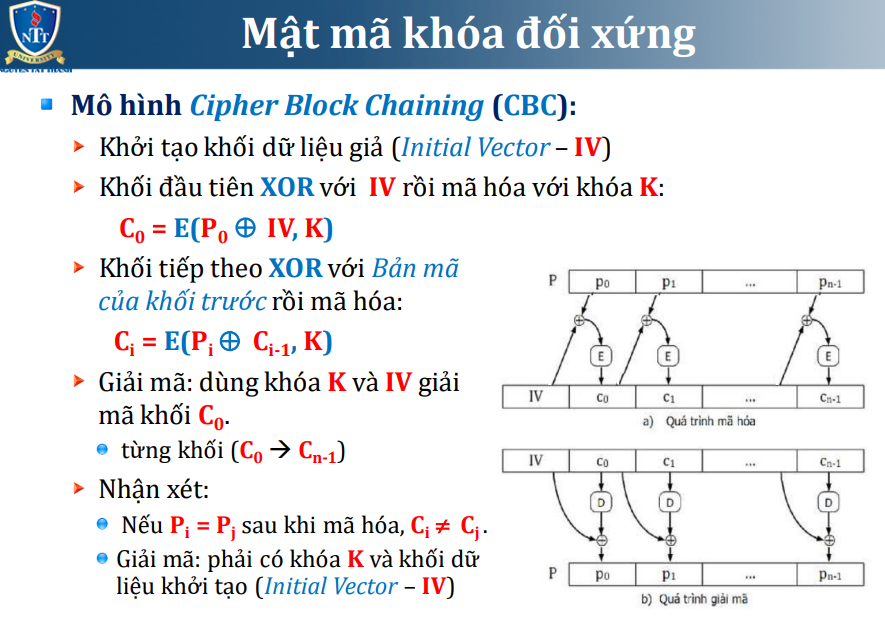
a. Mã hóa M bằng Public Key theo công thức: C = Me mod n

b. Giải mã C bằng Private Key theo công thức: M’ = Cd mod n

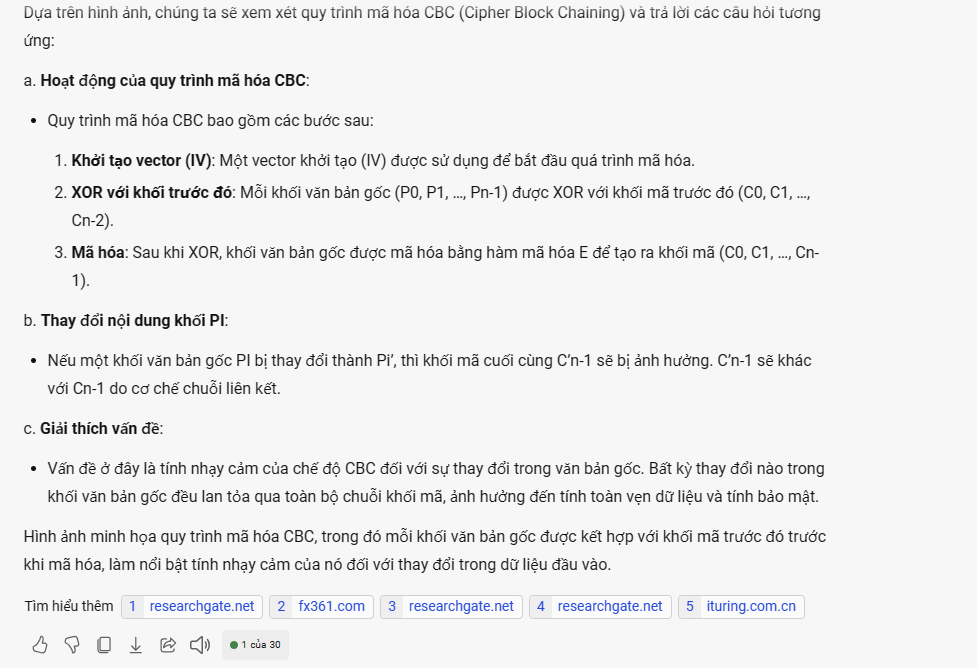
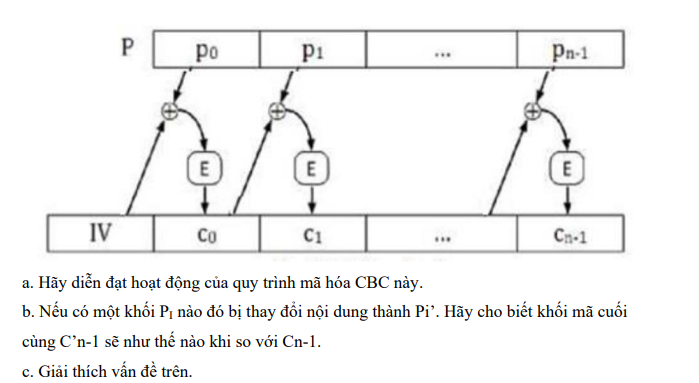
C=Me mod n =811mod 15=2

M=Cd mod n =23mod 15= 8

24. Vẽ sơ đồ quy trình mã hóa của mô hình mật mã chuỗi khối CBC (Cipher Block Chaining)



25. Cho quy trình mã hóa của mô hình mật mã chuỗi khối CBC (Cipher Block Chaining) như ảnh bên dưới:



26. Cho Message M 32 bit: “1100 0000 1010 1000 0001 1010 1000 0001”

a. Dùng thuật toán XOR để băm (hash) M trên thành mã băm 8 bit.

b. Giả sử: 4 bit đầu tiên để M đã bị sửa đổi thành 1001. Tiến hành dùng XOR để băm bản

sửa đổi (M’) thành mã băm 8 bit.

c. Cho biết kết luận sau khi so sánh 2 mã băm của M và M’.

a. b.

1100 0000 1001 0000

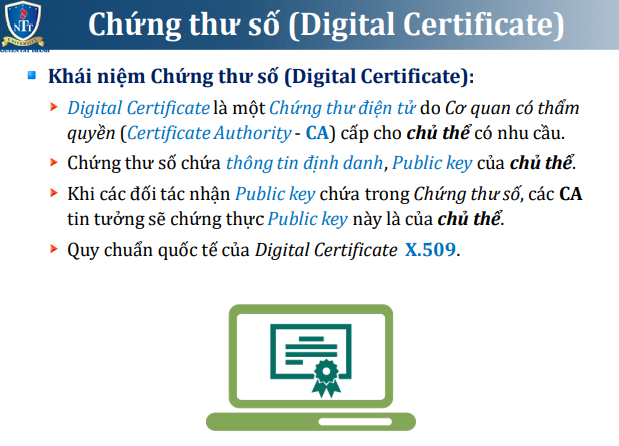
1010 1000 1010 1000

0001 1010 0001 1010

1000 0001 1000 0001

1111 0011 1010 0011

c. không giống nhau tại không giống m32 bit

27. Khái niệm chứng chỉ số là gì? Mô tả các thành phần chính trong chứng chỉ số ? 

Chứng chỉ số (digital certificate) là một loại giấy tờ điện tử được sử dụng để xác minh danh tính của một thực thể trực tuyến, chẳng hạn như một cá nhân, một tổ chức hoặc một trang web. Chứng chỉ số thường được sử dụng trong môi trường mạng để bảo đảm tính toàn vẹn, xác thực và an ninh trong việc truyền tải dữ liệu.

Các thành phần chính của một chứng chỉ số bao gồm:

Thông tin chứng chỉ (Certificate Information): Đây là phần chứa thông tin cơ bản về chứng chỉ, bao gồm tên của thực thể được xác thực (ví dụ: tên của một trang web hoặc tên của một tổ chức), địa chỉ email, thời gian hiệu lực của chứng chỉ, và các chi tiết khác như thuật toán mã hóa và chữ ký số.

Thông tin về công khai (Public Key Information): Phần này chứa khóa công khai của thực thể được xác thực, được sử dụng để mã hóa dữ liệu hoặc tạo chữ ký số. Người nhận có thể sử dụng khóa công khai này để giải mã dữ liệu được mã hóa bằng khóa riêng tư tương ứng, hoặc để xác minh tính toàn vẹn của dữ liệu bằng cách so sánh chữ ký số được tạo bởi khóa riêng tư.

Chữ ký số (Digital Signature): Đây là một phần quan trọng của chứng chỉ số. Chữ ký số được tạo ra bằng cách sử dụng khóa riêng tư của tổ chức phát hành chứng chỉ, và nó xác định rằng chứng chỉ đã được phát hành bởi một thực thể nhất định và chưa bị sửa đổi sau khi được tạo ra.

Thông tin về tổ chức phát hành (Issuer Information): Phần này chứa thông tin về tổ chức hoặc cơ quan đã phát hành chứng chỉ, bao gồm tên của tổ chức, địa chỉ và thông tin liên lạc. Điều này giúp người sử dụng xác minh tính xác thực của chứng chỉ.

Cơ quan chứng thực (Certificate Authority - CA): CA là tổ chức đáng tin cậy có trách nhiệm xác thực và phát hành các chứng chỉ số. CA đảm bảo rằng thông tin trong chứng chỉ được kiểm tra và xác thực đúng cách trước khi chứng chỉ được phát hành.

28. Vai trò và tính chất của hàm băm trong việc xác định tính toàn vẹn của thông tin?

Hàm băm giúp kiểm tra tính toàn vẹn của thông tin. Khi thông tin được băm, nếu có bất kỳ thay đổi nào, dù chỉ là một ký tự, giá trị băm sẽ thay đổi. Do đó, nếu giá trị băm của thông tin không thay đổi, chúng ta có thể tin tưởng rằng thông tin không bị thay đổi. Đây là cách hàm băm giúp xác định tính toàn vẹn của thông tin.

29. Cho biết khái niệm về IDS và IPS? So sánh giữa IDS và IPS?

IDS – Intrusion Detection System:

• Hệ thống phát hiện tấn công, xâm nhập;

IPS - Intrusion Prevention System:

• Hệ thống ngăn chặn tấn công, xâm nhập.

So sánh IDS/IPS:

Giống: Về cơ bản IPS và IDS giống nhau về chức năng

giám sát.

Khác:

• IPS thường được đặt giữa đường truyền thông và có

thể chủ động ngăn chặn các tấn công/xâm nhập bị phát

hiện;

• IDS thường được kết nối vào các bộ định tuyến, switch,

card mạng và chủ yếu làm nhiệm vụ giám sát/cảnh báo,

không có khả năng chủ động ngăn chặn tấn công, xâm

nhập.

30. Trong hệ thống hạ tầng mạng bảo mật, các hệ thống IDS/IPS thường đặt ở đâu trong hệ thống mạng? Giải thích lý do

Thường hệ thống IDS/IPS được đặt ở các điểm truy cập vào mạng, như cổng ra internet hoặc giữa mạng nội bộ và internet, để phát hiện và ngăn chặn các mối đe dọa trước khi chúng có thể gây hại cho hệ thống.

Hệ thống IDS/IPS thường được đặt sau firewall trong mạng. Lý do là để giám sát và phát hiện các cuộc tấn công từ bên trong mạng và các hoạt động xâm nhập đã vượt qua hệ thống bảo mật. Đây là cách để tăng cường bảo mật mạng.

31. Trình bày các loại tường lửa trong hệ thống mạng

Các loại tường lửa:

Lọc gói tin (Packet-Filtering):

• Áp dụng một tập các luật cho mỗi gói tin đi/đến để quyết

định chuyển tiếp hay loại bỏ gói tin.

• Các tường lửa dạng này thường lọc gói tin lớp IP.

Các cổng ứng dụng (Application-level gateway):

• Còn gọi là proxy server, thường dùng để phát lại (relay)

traffic của mức ứng dụng.

• Tường lửa ứng dụng web (WAF – Web Application

Firewall) là dạng cổng ứng dụng được sử dụng rộng rãi.

Cổng chuyển mạch (Circuit-level gateway):

• Hoạt động tương tự các bộ chuyển mạch.