# Phần I: Bài tập

## Bài tập về hệ mã hóa Affine

### Hãy mã hóa thông điệp P=ATvới khóa a=3;b=5 sử dụng hệ mã hóa Affine

a. FL

b. FT

c. AK

d. FK

### Hãy mã hóa thông điệp P=CN với khóa a=11;b=4 sử dụng hệ mã hóa Affine

a. XF

b. FD

c. AM

d. AR

### Hãy mã hóa thông điệp P=VN với khóa a=11;b=12 sử dụng hệ mã hóa Affine

a. JZ

b. JK

c. AL

d. JX

### Hãy mã hóa thông điệp P=CN với khóa a=7;b=9 sử dụng hệ mã hóa Affine

a. WX

b. KX

c. XK

d. XW

### Hãy mã hóa thông điệp P=FE với khóa a=7;b=8 sử dụng hệ mã hóa Affine

a. RK

b. GL

c. RX

d. RJ

### Hãy mã hóa thông điệp P=GT với khóa a=3;b=5 sử dụng hệ mã hóa Affine

a. XK

b. NX

c. AN

d. XN

### Hãy mã hóa thông điệp P=SR với khóa a=3;b=5 sử dụng hệ mã hóa Affine

a. HS

b. HE

c. HT

d. KE

### Hãy mã hóa thông điệp P=VT với khóa a=7;b=12 sử dụng hệ mã hóa Affine

a. TH

b. DP

c. TG   
d. DF

### Hãy giải mã thông điệp P=SR với khóa a=3;b=5 sử dụng hệ mã hóa Affine

a. NT

b. AE

c. NE

d. RE

### Hãy giải mã thông điệp P=VT với khóa a=11;b=4 sử dụng hệ mã hóa Affine

a. LZ

b. XL

c. LX

d. DX

### Hãy giải mã thông điệp P=VN với khóa a=1;b=3 sử dụng hệ mã hóa Affine

a. SK

b. SX

c. SY

d. YT

### Hãy giải mã thông điệp P=CN với khóa a=3;b=4 sử dụng hệ mã hóa Affine

a. PJ

b. ID

c. IX

d. PT

### Hãy giải mã thông điệp P=KS với khóa a=5;b=7 sử dụng hệ mã hóa Affine a.LX  b.TX  c.DX  d. LT

### Hãy giải mã thông điệp P=TK với khóa a=3;b=5 sử dụng hệ mã hóa Affine a.TU b.TS c.WA d. WT

### Hãy giải mã thông điệp P=FE với khóa a=5;b=4 sử dụng hệ mã hóa Affine

a. NX

b. NA

c. VN

d. VA

## Bài tập về hệ mã hóa Vigenere

### Hãy mã hóa sử dụng hệ mã Vigenere với: Thông điệp = VIETNAMNET Khóa K =KENH

a. FRRAXEZUOX

b. FMRAXEZUOX

c. FMRAXSZUOX

d. FMRAYEZUOX

### Hãy mã hóa sử dụng hệ mã Vigenere với: Thông điệp = TRAINGHEO Khóa K=VOZ a.KFRTDBFBSN b.OFZDBFCSN c.OWZEBFCRN d. XVOCZDFHB

### Hãy mã hóa sử dụng hệ mã Vigenere với: Thông điệp = ENGLISH Khóa K =DKT

a. GZHOZKI

b. HZOXSKJ

c. HXZOSLK

d. HXZOSKL

### Hãy mã hóa sử dụng hệ mã Vigenere với: Thông điệp = KHOAHOC Khóa K =VNU

a. UFXVIX

b. FUIVIX --- Chính xác là FUIVUIX

c. IUFVXI

d. FUVIXI

### Hãy mã hóa sử dụng hệ mã Vigenere với: Thông điệp=CHAUAU khóaK=HOT

1. JBONVT
2. JVTBON
3. JTPBTV
4. JTVPBN

### Hãy giải mã sử dụng hệ mã Vigenere với: Thông điệp = VIETNAMNET Khóa K =KENH

a. LERMDWZGUP

b. LESMDWZGUP

c. LYRMDWZGUP

d. LERMDEZGUP

## Bài tập về hệ mã hóa Hill

### Hãy mã hóa thông điệp FE sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (21-2;24-15)

a. ST

b. XS

c. TS

d. SX

### Hãy mã hóa thông điệp VE sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (17-20;4-5)

a. JY

b. YT

c. YJ

d. TX

### Hãy mã hóa thông điệp AB sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (5-10;6-13)

a. NG

b. GN

c. KT

d. AX

### Hãy mã hóa thông điệp DH sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (23-14;18-25) a.KL b.NJ c.LK d. JN

### Hãy mã hóa thông điệp BO sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (9-16;8-17)

a. RU

b. UK

c. KU

d. UR

### Hãy mã hóa thông điệp CV sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (7-21;2-11)

a. EN

b. VD

c. CX

d. TK

### Hãy mã hóa thông điệp AV sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (7-21;2-11) a.DX b.SX c.QX d. QT

### Hãy mã hóa thông điệp LO sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (22-5;17-6)

a. MJ

b. VE

c. MK

d. JK

### Hãy mã hóa thông điệp VO sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (18-13;21-22)

a. JW

b. WX

c. JX

d. WJ

### Hãy mã hóa thông điệp LO sử dụng hệ mã Hill với khóa K là ma trận 2x2=(22-5;17-6)

1. MK
2. VE
3. MJ
4. JK

### Hãy giải mã thông điệp AV sử dụng hệ mã Hill với khóa K là ma trận 2x2=(7-21;2-11)

a.RZ

b.EZ

c.ET

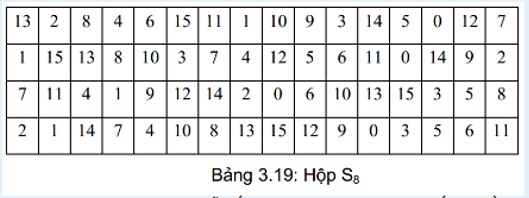
d.ES

## Bài tập về hệ mã hóa RSA

### Cho hệ mã RSA có p = 23, q = 31, e = 3. Số lượng bản mã trùng bản rõ vào khoảng a.9 b.10 c.8 d. 12

## Bài tập về DES

### Trong thuật toán DES, khi chuỗi số 010001 đi qua hộp S trên thì kết quả đầu ra là:



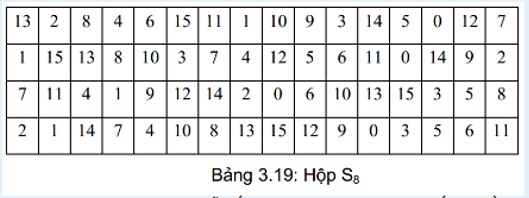
a. 0101

b. 000111

c. 1100

d. 1010

### Trong thuật toán DES, khi chuỗi số 111111 đi qua hộp S trên thì kết quả đầu ra là:



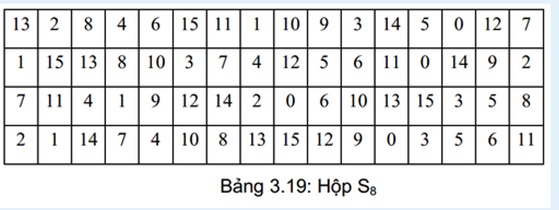
a. 0101

b. 101001

c. 1011

d. 1010

### Trong thuật toán DES, khi chuỗi số 100001 thông qua hộp S trên thì kết quả đầu ra là:



a. 0101

b. 010101

c. 1011

d. 0010

### Trong thuật toán DES, khi chuỗi số 100011 qua hộp S trên thì kế quả đầu ra là:

a. 101010

b. 0011

c. 0001

d. 1000

# Phần II: Lý thuyết

## Chữ kí điện tử

### Chữ ký điện tử được hiểu là :

a. Một phép kiểm tra trong đó những người biết khóa qui ước mới có thể kiểm tra được

b. Một phép kiểm tra trong đó mọi người có thể kiểm tra, duy nhất 1 người có thể mã hóa

c. Một phép kiểm tra trong đó 1 người có thể mã hóa và duy nhất 1 người có thể kiểm tra

d. Chữ ký nằm dưới dạng dữ liệu số

### Trong một chữ ký điện tử tiêu chuẩn, phát biểu nào sau đây là đúng.

a. Chữ ký thường có kích thước bằng chính văn bản cần ký

b. Chữ ký trên các văn bản khác nhau sẽ có kích thước khác nhau và thường < 1% nội dung thông điệp

c. Tất cả chữ ký trên mọi văn bản đều có kích thước như nhau

d. Chữ ký trên các văn bản khác nhau sẽ có kích thước khác nhau và thường bằng 1% nội dung thông điệp

### Không thể sử dụng các thuật toán cổ điển để xây dựng chữ ký điện tử vì

a. Các thuật toán cổ điển có không gian khóa thấp  
b. Các thuật toán cổ điển đơn giản nên việc giải mã và giả mạo là dễ  
c. Các thuật toán cổ điển là hệ mã hóa đối xứng  
d. Các thuật toán cổ điển có không gian từ mã thấp

### Chức năng chính của chữ ký điện tử là

a. Nhằm giúp xác thực tính sở hữu của văn bản

b. Nhằm tăng tính bảo mật nội dung văn bản

c. Nhằm không cho phép thay đổi nội dung văn bản

d. Nhằm tăng tính bảo mật khóa của văn bản

### Hãy cho biết phát biểu nào sau đây đúng về chữ ký điện tử

a. Chữ ký điện tử có kích thước bằng đúng nội dung ký lên.

b. Chữ ký điện tử có kích thước xác định với mọi nội dung ký lên

c. Chữ ký điện tử có kích thước nhỏ hơn nhiều lần với nội dung ký lên

d. Chữ ký điện tử có kích thước phụ thuộc vào loại chữ ký sử dụng và không phụ thuộc vào văn bản ký

### Phát biểu nào sau đây đúng về chữ ký điện tử

a. Chữ ký điện tử có thể được sử dụng để nén dữ liệu

b. Chữ ký điện tử có thể sử dụng để xác thực tính toàn vẹn dữ liệu

c. Chữ ký điện tử có thể sử dụng để bảo toàn sự bí mật của dữ liệu

d. Chữ ký điện tử không thể sử dụng để xác thực tính toàn vẹn dữ liệu

### Phát biểu nào sau đây đúng về chữ ký điện tử

a. Chữ ký điện tử chỉ có thể được xây dựng trên các hệ mã hóa phi đối xứng (Công khai)

b. Chữ ký điện tử có thể sử dụng để bảo toàn về an ninh dữ liệu

c. Sử dụng hệ mã hóa khối để xây dựng chữ ký điện tử sẽ tận dụng được khả năng tính toán nhanh dựa trên việc xây dựng các module phần cứng

d. Sử dụng hệ mã hóa cổ điển để xây dựng chữ ký điện tử sẽ khiến chữ ký số dễ dàng bị thám mã và giả dạng

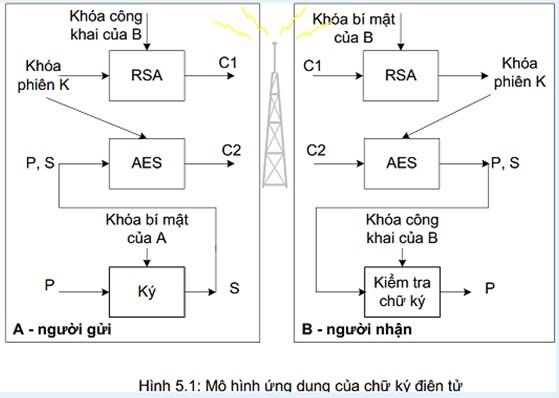
### Không thể sử dụng các thuật toán cổ điển để xây dựng chữ ký điện tử vì

1. Các thuật toán cổ điển là hệ mã hóa đối xứng
2. Các thuật toán cổ điển đơn giản nên việc giải mã và giả mạo là dễ
3. Các thuật toán cổ điển có không gian kháo thấp
4. Các thuật toán cổ điển có không gian từ mã thấp

### Phát biểu nào sau đây đúng về chữ kí điện tử:

1. Chữ ký điện tử không thể sử dụng để xác thực tính toàn vẹn dữ liệu
2. Chữ ký điện tử có thể được sử dụng để nén dữ liệu
3. Chữ ký điện tử có thể được sử dụng để bảo toàn sự bí mật của dữ liệu
4. Chữ ký điện tử có thể sử dụng để xác thực tính toàn vẹn dữ liệu

### Chọn câu đúng



a. Khóa K được mã hóa bằng thuật toán RSA vì kích thước khóa K là nhỏ, thuật toán RSA chỉ mã hóa được các dữ liệu nhỏ

b. Khóa K được mã hóa bằng thuật toán RSA vì kích thước khóa K là lớn, thuật toán RSA có tốc độ xử lý nhanh

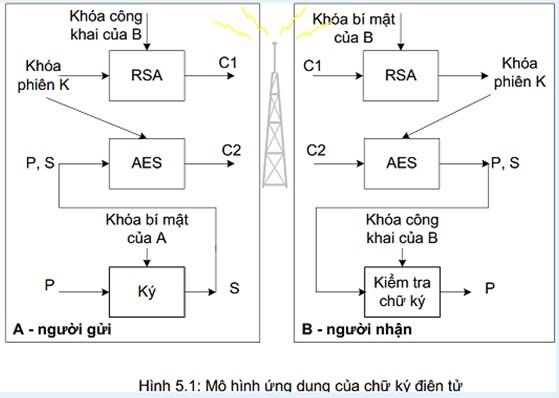
c. Khóa K được mã hóa bằng thuật toán RSA vì thuật toán RSA chuyển sử dụng để mã hóa khóa

d. Khóa K được mã hóa bằng thuật toán RSA vì kích thước khóa K là nhỏ, thuật toán RSA có độ án toàn cao hơn ( trang 82 sgk)

### Phát biểu nào sau đây sai về chữ ký điện tử:

1. Chữ ký điện tử có thể sử dụng để xác định tính bản quyền dữ liệu
2. Chữ ký điện tử chỉ được tạo với các hệ mã hóa phi đối xứng
3. Chữ ký điện tử có thể tạo bởi các hệ mã hóa phi đối xứng hoặc đối xứng
4. Chữ ký điện tử có thể sử dụng để bảo toàn tính toàn vẹn dữ liệu

### Chọn câu đúng



a. Người ta sẽ sinh khóa K dựa trên khóa bí mật A vì khi đó B có thể biết khóa K bằng bao nhiêu thông qua khóa công khai của A

b. Người ta sẽ sinh khóa K dựa trên khóa công khai của B vì chỉ có B mới biết được khóa K bằng bao nhiêu thông qua khóa bí mật

c. Người gửi sẽ tự sinh khóa K rồi mã hóa khóa K bằng khóa công khai của B và gửi cho B nhằm đảm bảo an toàn

d. Khóa K được quy ước cho cả 2 bên, các khóa bí mật và khóa công khi của A và B sẽ kết hợp với khóa K để tăng cường an toàn cho hệ mã

### Phát biểu nào là đúng về chữ ký điện tử sau

a. Chữ ký điện tử có thể được xây dựng trên hệ mã bí mật

b. Chữ ký điện tử có thể xác minh đây đúng là văn bản của đối tượng sở hữu chữ ký hay không?

c. Chữ ký điện tử có thể chỉ rõ ai là đối tượng ký

d. Chữ ký điện tử có thể được phát triển trên hệ mã khối

## Chữ ký số

### Sử dụng chữ ký điện tử lên đại diện nội dung số phục vụ mục đích

a. Giúp tăng tính bảo mật của chữ ký số trên nội dung số

b. Giúp giảm thiểu kích thước cần ký trên nội dung số

c. Giúp tăng tính bảo mật của nội dung số

d. Giúp tăng thời gian xác thực của chữ ký

### Chữ ký số giống với hệ mã hóa khóa công khai ở các điểm

a. Cùng sử dụng 2 khóa bí mật và công khai

b. Cùng sử dụng 2 khóa bí mật và công khai như nhau

c. Cùng sử dụng chung các thuật toán mã hóa và giải mã như nhau.

d. Cùng sử dụng 2 khóa bí mật và công khai, khóa bí mật được sử dụng để mã hóa và công khai để giải mã

### Chữ ký số khác với hệ mã hóa khóa công khai ở điểm

a. Sử dụng 2 khóa bí mật và công khai nhưng 2 khóa được định nghĩa khác nhau hoàn toàn

b. Sử dụng 02 khóa bí mật và công khai như nhau nhưng vai trò đối tượng tham gia được đổi lại

c. Trong chữ ký số vai trò của khóa bí mật và công khai không rõ ràng

d. Sử dụng 2 khóa bí mật và công khai hoàn toàn khác nhau

### Giải thuật chữ ký số tiêu chuẩn DSA sử dụng hàm băm SHA-1 sinh chữ ký độ dài

a. 160 bít

b. 128 bít

c. 320 bít

d. 512 bít

### Kết luận nào sau là đúng cho giải thuật chữ ký số

a. giải thuật chữ ký số tương tự giải thuật mã hóa khóa công khai

b. có thể xác nhận chữ ký và văn bản đã ký

c. kết hợp các kết luận trên cùng đúng

d. có thể giải mã chữ ký trở thành văn bản gốc

### Giải thuật chữ ký số nào là cơ sở của giải thuật chữ ký số tiêu chuẩn

a. giải thuật chữ ký số Merkle - Hellman

b. giải thuật chữ ký số trên đường cong Eliptic

c. giải thuật chữ ký số El Gamal

d. giải thuật chữ ký số RSA

### Kết luận nào là đúng cho hệ chữ ký số El-Gamal

a. giải thuật chữ ký số có thể giải mã chữ ký trở thành văn bản gốc

b. giải thuật chữ ký số có thể sinh một chữ ký từ một văn bản

c. giải thuật chữ ký số được áp dụng cho mã hóa và giải mã văn bản

d. giải thuật chữ ký số có thể sinh nhiều chữ ký khác nhau từ một văn bản

### Cấu tạo của một chữ ký số tiêu chuẩn gồm

a. Chỉ gồm chữ ký trên đại diện

b. Một phần thông điệp và chữ ký trên đại diện

c. Đại diện thông điệp và chữ ký trên đại diện

d. Chỉ gồm chữ ký trên thông điệp

### Kết luận nào sau là đúng:

1. Chữ ký số được hình thành từ các thuật toán mã hóa khóa công khai
2. Chữ ký số là dãy số đặc biệt
3. Chữ ký số được hình thành từ các thuật toán mã hóa khóa bí mật
4. Giải mã chữ ký số được văn bản gốc

## Hàm băm

### Hãy cho biết những đặc điểm đúng về hàm băm

a. Với cùng một giá trị đầu vào, khóa khác nhau sẽ thu được các giá trị đầu ra khác nhau

b. Với một giá trị đầu ra, ta có thể tính toán đầu vào duy nhất

c. Các đầu vào khác nhau sẽ băm được các giá trị đầu ra khác nhau ( ko đúng lắm với trường hợp đụng độ bảng băm)

d. Với mỗi giá trị đầu vào chỉ duy nhất có một giá trị đầu ra tương ứng

### Hàm băm Md-5 tạo ra được bao nhiêu giá trị băm

a. 4 lũy thừa 80

b. 128

c. 4 lũy thừa 64

d. 128 lũy thừa 2

### **Hàm băm SHA-1 tạo ra được bao nhiêu giá trị băm** a. 4 lũy thừa 80 b. 160 c. 2 lũy thừa 128 d. 160 lũy thừa 2

### Hãy cho biết những đặc điểm đúng về hàm băm

1. Với cùng 1 giá trị đầu vào,khóa khác nhau sễ thu được các giá trị đầu ra khác nhau
2. Các đầu vào khác nhau sẽ băm được các giá trị đầu ra khác nhau
3. Với mỗi giá trị đầu vào chỉ duy nhất có 1 giá trị đầu ra tương ứng
4. Với 1 giá trị đầu ra,ta có thể tính toán đầu vào duy nhất

### Kết luận nào sau là đúng cho hàm băm:

a. kết hợp các kết luận trên cùng đúng

b. Giá trị băm sử dụng trong mã hóa và giải mã thông tin

c. Hàm băm sử dụng trong mã hóa khối

d. Hàm băm xác thực sự toàn vẹn thông tin

### Phát biểu nào sau đây đúng về hàm băm

1. Tỉ lệ sai khác của 2 đầu ra khác nhau phụ thuộc vào tỉ lệ sai khác giữa 2 đầu vào
2. Có thể tìm dc đầu vào bằng cách xây dựng giải thuật giải mã hàm băm
3. Hai đầu vào khác nhau chắc chắn sẽ băm ra các giá trị đầu ra khác nhau
4. Hai đầu vào khác nhau có thể ra các đầu ra giống nhau

### Phát biểu nào sau đây đúng về hàm băm

a. Kích thước đầu ra của hàm băm chắc chắn nhỏ hơn kích thước dữ liệu đầu vào

b. Kích thước đầu ra hàm băm phụ thuộc vào kích thước dữ liệu đầu vào nhưng không theo một tỉ lệ nhất định

c. Kích thước đầu ra của một hàm băm phụ thuộc vào kích thước dữ liệu đầu vào theo một tỉ lệ

d. Kích thước đầu vào hàm băm không phụ thuộc vào kích thước dữ liệu đầu vào và giống nhau với mọi đầu vào.

### Vì sao ta coi kết quả băm của một thông điệp qua hàm băm là đại diện của thông điệp đó

a. Kết quả băm được có kích thước nhỏ hơn kích thước của thông điệp là là duy nhất

b. Kết quả băm được có kích thước nhỏ hơn kích thước của thông điệp và là duy nhất và có khả năng dịch ngược lại để xác minh thông điệp

c. Kết quả băm được có kích thước bằng chính kích thước của thông điệp và là duy nhất.

d. Kết quả băm được có kích thước nhỏ hơn kích thước của thông điệp và được coi là duy nhất vì khả năng 2 thông điệp băm cùng kết quả có xác xuất rất thấp

### Một thông điệp có độ lớn là 1024 byte. Sau khi qua hàm băm lần 1 thu được kết quả là 512 byte. Hỏi nếu qua 3 lần hàm băm liên tiếp ta thu được kết quả bao nhiêu?

A. 512 byte

B. 128 byte

C. 317 byte

D. 256 byte

### Nếu một thông điệp có độ lớn P < k là kích thước giới hạn của hàm băm, kết quả thu được sẽ là

a. Đại diện P có kích thước k

b. Sẽ xảy ra sự cố khi băm thông điệp

c. Đại diện P sẽ có kích thước P và bị chèn vào một số lượng khoảng trống để đạt được kích thước k

d. Đại diện P vẫn có kích thước bằng P

### Hiện tượng xung đột bảng băm được hiểu

a. Hiện tượng bảng băm không thể xuất các giá trị đầu ra  
b. Hiện tượng với hai dữ liệu đầu vào khác nhau, giá trị đầu ra bảng băm là như nhau

c. Với tất cả các dữ liệu đầu vào, chỉ duy nhất một giá trị đầu ra  
d. Với tất cả các giá trị đầu vào, giá trị đầu ra không bị thay đổi

### Khi sử dụng hàm băm, ta sẽ thu được đại diện của thông điệp có đặc điểm

a. Đại diện là không duy nhất do còn phụ thuộc vào khóa sử dụng cùng bảng băm  
b. Đại diện là duy nhất và có kích thước luôn cố định  
c. Đại diện thông điệp không thể lập lại với một thông điệp khác  
d. Đại diện là duy nhất nên ta có thể sử dụng đại diện để suy ngược lại thông điệp nhưng thuật toán rất phức tạp

### Phát biểu nào sau đây đúng về Hàm băm

a. Có thể tìm được đầu vào bằng cách xây dựng giải thuật giải mã hàm băm

b. Tỉ lệ sai khác của hai đầu ra khác nhau phụ thuộc vào tỉ lệ sai khác giữa 2 đầu vào

c. hai đầu vào khác nhau có thể ra các đầu ra giống nhau

d. hai đầu vào khác nhau chắc chắn sẽ băm ra các giá trị đầu ra khác nhau( giá trị chứ không phải kích thước, kích thước thì có thể giống nhau)

## Mã hóa khối

### Để có thể tận dụng ưu điểm của hệ mã hóa khối và hệ mã hóa công khai, mô hình kết hợp của hai hệ mã được sử dụng như sau

a. Hệ mã hóa công khai sẽ mã hóa thông điệp và hệ mã hóa khối sẽ mã hóa đại diện của thông điệp qua hàm băm

b. Hệ mã hóa công khai sẽ mã hóa chữ ký của thông điệp và hệ mã hóa khối sẽ mã hóa thông điệp

c. Hệ mã hóa công khai sẽ mã hóa thông điệp với khóa K, hệ mã hóa khối sẽ mã hóa khóa K

d. Hệ mã hóa khối sẽ mã hóa thông điệp với khoa K, hệ mã hóa công khai sẽ mã hóa khóa K

### Thuật toán mã hóa khối được hiểu là:

A.Đầu vào dữ liệu là một chuỗi bít có độ dài tùy ý, đầu ra là các khối có kích thước quy ước

B.Đầu vào dữ liệu là chuỗi byte có độ dài tùy ý, đầu ra là các khối có kích thước bằng dữ liệu đầu vao

C.Dữ liệu đầu vào được đem đi mã hóa sẽ được chia thành các khối có độ dài quy ước

D.Dữ liệu sẽ được chạy qua các khối(hộp), mỗi khối có 1 chức năng mã hóa riêng

### Thuật ngữ AES được hiểu

a. Thuật toán mã hóa khối

b. Một thuật toán mã hóa bí mật

c. Một chuẩn mã hóa bí mật

d. Thuật toán mã hóa công khai

### Chuẩn mã hóa khối hiện nay là:

1. Des
2. Không xác định
3. TripleDes
4. Aes

### **Tốc độ xử lý của hệ mã hóa khối thường nhanh là do :** a. Hệ mã hóa khối sử dụng 1 khóa cho việc khóa và giải mã b. Dữ liệu được mã hóa theo khối nên việc xử lý nhanh hơn xử lý từng bit c. Cả 3 đáp án hiện có đều sai. d. Hệ mã hóa khối chủ yếu là các phép dịch bit và có thể được thiết kế bằng phần cứng.

### Trong hệ thống kết hợp giữa RSA và AES thì chức năng của các hệ mã hóa là

a. AES mã hóa thông điệp lần 1, RSA mã hóa lần 2 để tăng cường tính bảo mật  
b. RSA mã hóa thông điệp, AES mã hóa khóa của RSA  
c. AES mã hóa thông điệp, RSA mã hóa khóa của AES  
d. RSA mã hóa thông điệp lần 1. AES mã hóa thông điệp lần 2 để tăng cường tính bảo mật

### Thuật toán mã hóa khối được hiểu là :

a. Đầu vào dữ liệu là một chuỗi bit có độ dài tùy ý, đầu ra là các khối có kích thước quy ước

b. Dữ liệu đầu vào được đem đi mã hóa sẽ được chia thành các khối có độ dài qui ước

c. Đầu vào dữ liệu là chuỗi byte có độ dài tùy ý, đầu ra là các khối có kích thước bằng dữ liệu đầu vào

d. Dữ liệu sẽ được chạy qua các khối (hộp), mỗi khối có 1 chức năng mã hóa riêng.

## DES

### Số lượng bảng số sử dụng trong Des là

a. 13

b. 16

c. 14

d. 15

### Không sử dụng hệ mã hóa DES để xây dựng chữ ký số DES vì : a. DES là hệ mã hóa có độ phức tạp thấp b. DES là hệ mã hóa đối xứng c. DES là hệ mã hóa mà không gian khóa nhỏ, có thể dò được trong khoảng thời gian cho phép d. DES là hệ mã hóa hóa mà không gian từ mã nhỏ

### Trong sơ đồ sinh khóa của Des, kết luận nào sau là đúng:

a. 16 khóa con, mỗi khóa độ dài 48 bít.

b. 20 khóa con, mỗi khóa 32 bít

c. 16 khóa con, mỗi khóa độ dài 32 bít.

d. 12 khóa con, mỗi khóa 48 bít

### Giải thuật mã hóa và giải mã Des có đặc điểm

a. độ dài khóa có lựa chọn

b. cấu trúc đại số

c. của ba đáp án trên

d. sử dụng nhiều hàm phi tuyến

### Phát biểu nào sau đây là chính xác

a. Hệ mã hóa DES là hệ mã đối xứng vì không gian các từ tạo nên bản mã và không gian các từ tạo nên bản rõ là như nhau   
b. Hệ mã hóa DES là hệ mã đối xứng không gian bản mã và không gian bản rõ là như nhau  
c. Hệ mã hóa DES là hệ mã đối xứng vì khi có khóa để mã hóa ta dễ dàng suy ra được khóa để giải mã   
d. Hệ mã hóa DES là hệ mã đối xứng vì phương pháp mã hóa và giải mã là như nhau.

### Tăng độ an toàn của Des bằng cách

a. tăng số khóa con của giải thuật

b. tăng độ dài khóa của Des

c. tăng số vòng lặp của giải thuật

d. mã hóa nhiều khối Des nhưng không tăng độ dài khóa

### Giải thuật nào sau đây là không dùng khóa đối xứng

a. RC-2  
b. El-Gamal  
c. RC-4  
d. Des

## Giao thức có trọng tài

### Giao thức có người phân sử được hiểu a. Một trọng tài giám sát toàn bộ quá trình giao dịch và phân xử khi có tranh chấp xẩy ra b. Trọng tài giám sát mọi quá trình giao dịch, khi xẩy ra vi phạm, trọng tài sẽ mời đối tượng trung gian có đủ thẩm quyền đứng lên giải quyết mọi vi phạm c. Các qui tắc giao dịch được xây dựng từ trước, người trung gian chỉ được sử dụng khi có tranh chấp xẩy ra d. Khi có tranh chấp xẩy ra, một bên mời người trung gian vào để xác nhận toàn bộ quá trình giao dịch

### Những điều không đúng trong giao thức có trọng tài

a. Trọng tài được lợi nhất định trong quá trình giao dịch dù giao dịch tuy nhiên lợi ích này lại không đến trực tiếp từ quá trình giao dịch

b. Trọng tài chỉ thực hiện các qui tắc trong giao dịch theo đúng giao thức

c. Trọng tài là một đối tượng trung gian được tin tưởng của các bên tham gia, không có lợi ích trong giao dịch

d. Trọng tài là đối tượng đề ra qui tắc trong giao dịch và giám sát các bên tham gia

### Những điều nào đúng về giao thức có trọng tài

a. Trọng tài có quyền lợi cả hai phía khi giao dịch thành công

b. Trọng tài có quyền xử lý bất kỳ bên nào sai phạm trong quá trình giao dịch

c. Trọng tài chỉ có quyền giám sát các sai phạm trong quá trình giao dịch

d. Trọng tài là đối tượng không có quyền lợi trực tiếp trong giao dịch và được sự tin tưởng của các bên tham gia

### Kết luận nào sau là đúng cho những giao thức quản lý khóa

a. kết hợp các kết luận trên đều đúng

b. sinh khóa công khai và bí mật sử dụng trong hệ PKC

c. sinh và quản lý khóa phiên cho mỗi bên

d. luôn có sự tham gia của trọng tài

## Kerberos

### Sơ đồ phân phối khóa Kerberos, kết luận nào sau là sai:

a. mỗi bên có khóa riêng tạo thành với trung tâm TA

b. hai bên dùng khóa cũ để mã hóa và giải mã cho phiên truyền tin mới

c. TA tạo khóa bí mật dùng chung và gửi cho mỗi bên

d. hai bên trao đổi khóa bí mật dung chung

### Hệ phân phối khóa Kerberos có chức năng

a. Chống middle-attack  
b. Kết hợp 3 chức năng trên  
c. Xác nhận danh tính dựa trên chứng chỉ khóa công khai  
d. Chống thám mã gửi bản tin cũ

## KnapSack

### Phát biểu nào sâu đây đúng về hệ mã KnapSack

1. Dữ hiệu vào của hệ mã Knapsack là từng byte một
2. Dữ hiệu vào của hệ mã Knapsack là một khối có kích thước 128bit
3. Dữ hiệu vào của hệ mã Knapsack là một khối có kích thước 56 bit
4. Dữ hiệu vào của hệ mã Knapsack là số bit theo cài đặt riêng

## Mã khối

### Kết luận nào sau là đúng cho mã khối

a. bản mã và bản rõ có độ dài bằng nhau  
b. khối đơn vị mã hóa là 128 bít  
c. bản mã và bản rõ có độ dài khác nhau  
d. khối đơn vị mã hóa là 64 bít

### Chế độ sử dụng mã khối nào được ứng dụng chính

a. ECB bảng tra mã điện tử

b. CBC mã móc xích

c. CFB mã phản hồi

d. 3 chế độ trên

### Chứng chỉ khóa công khai dùng để

a. Cung cấp khóa công khai

b. Sử dụng khóa công khai tính khóa riêng

c. ứng dụng trong hệ mã khối

d. Cung cấp khóa bí mật

### **Các bảng hoán vị trong hệ mã khối được hiểu là :** a. Bảng thứ tự các bit đã được sắp xếp lại theo 1 thứ tự nào đó b. Bảng hoán vị thỏa mãn điều kiện có n bit đầu vào và có ít hơn n bit ở đầu ra c. Bảng hoán vị thỏa mãn điều kiện đảo ngược các bit đầu ra so với các đầu vào d. Bảng hoán vị thỏa mãn điều kiện có n bit đầu vào và có nhiều hơn n bit ở đầu ra

## RSA

### Phát biểu nào sau đây là chính xác

a. Tất cả các lý do trên đều không chính xác

b. Hệ mã hóa RSA là hệ mã hóa phi đối xứng vì khi biết được một khóa công khai ta rất khó khăn khi suy ra khóa bí mật

c. Hệ mã hóa RSA là hệ mã hóa phi đối xứng vì cách thức mã hóa và giải mã là hoàn toàn khác nhau

d. Hệ mã hóa RSA là hệ mã hóa phi đối xứng vì không gian bản mã và không gian bản rõ là không đối xứng

### Hệ mã RSA có thể bị giải mã theo định lý đồng dư TQ nếu

a. số mũ giải mã d nhỏ

b. số bản mã lặp lại nhiều từ bản rõ

c. số mũ sinh mã e nhỏ

d. kết hợp các trường hợp trên

### Nguyên nhân khiến tốc độ giải mã của RSA chậm là

a. Giải thuật mã hóa phức tạp

b. Độ dài khóa riêng p,q lớn

c. Số mũ sinh mã e lớn

d. Số mũ giải mã d lớn

### Phát biểu nào sau đây đúng về hệ mã RSA

a. Độ an toàn của hệ mã RSA phụ thuộc vào bài toán tính số nguyên tố p,q khi biết N=p\*q

b. Độ an toàn của hệ mã RSA phụ thuộc vào độ lớn của không gian khóa

c. Độ an toàn của hệ mã RSA phụ thuộc vào bài toán tìm k khi biết p,q trong phép Q=k\*p

d. Độ an toàn của hệ mã RSA phụ thuộc vào bài toán tìm số nghịch đảo của số e trong miền số cực lớn

## Các dạng khác

### Các yếu tố không ảnh hưởng đến sự an toàn của một hễ mã mật :

a. Kích thước dữ liệu đầu vào của hệ mã

b. Không gian từ mã và không gian thông điệp.

c. Phương pháp mã hóa/ giải mã.

d. Độ bí mật của khóa

### Hệ thống quản lý khóa công khai có chức năng chính ?

a. Thông báo khóa công khai khi thay đổi

b. Trung tâm hỏi đáp khóa công khai khi cần thiết

c. Trung tâp phân phối khóa (xây dựng và quản lý khóa) với cả hệ thống

d. Cấp lại khóa công khai khi bị lộ

### Trong mật mã khóa công khai, khóa công khai dùng để làm gì?

a. giải mã và tạo chữ ký

b. giải mã và sinh chữ ký

c. mã hóa và xác nhận chữ ký

d. mã hóa và sinh chữ ký

### Một trong những nhược điểm của hệ mã Merkle – Hellman ( bài toán xếp balo- đóng thùng)

a. bản mã lặp lại từ bản rõ

b. giải thuật sinh khóa siêu tăng đơn giản

c. độ dài khóa lớn

d. giải thuật có quá nhiều phép tính lũy thừa

### Trong các hệ mã sau, hệ mã hoá công khai là hệ mã

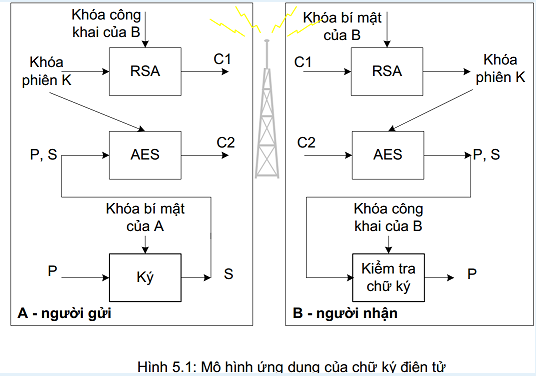
a. Thông điệp được mã hóa không cần khóa

b. Khoá được qui ước cho bên gửi và bên nhận là chung

c. Khóa chỉ cho những người trong nhóm truyền tin biết

d. Khóa được chia làm 2 phần, 1 phần được công khai và phần còn lại được giữ bí mật

### Câu hỏi không rõ ?



a. Ưu điểm của sơ đồ trên là có thể tận dụng được tốc độ xử lý nhanh của AES và tính phức tạp của RSA

b. Ưu điểm của sơ đồ trên là có thể tận dụng được khả năng xác minh thông điệp P ngay khi nhận dữ liệu

c. Ưu điểm của sơ đồ trên là sự an toàn cao do thông điệp được mã hóa nhiều hơn 1 lần

d. Ưu điểm của sơ đồ trên là có thể tận dụng được tốc độ xử lý nhanh của RSA và tính phức tạp của AES

### Phát biểu nào sau đây là chính xác

a. Hệ mã hóa cổ điển là hệ mã hóa đối xứng vì các ký tự để xây dựng lên không gian bản mã cũng chính là các ký tự xây dựng lên không gian bản rõ

b. Hệ mã hóa cổ điển là hệ mã hóa đối xứng vì không gian bản mã và không giai bản rõ có độ lớn bằng nhau

c. Hệ mã hóa cổ điển là hệ mã hóa đối xứng vì phương pháp mã hóa và phương pháp giải mã là như nhau

d. Hệ mã hóa cổ điển là hệ mã hóa đối xứng vì khi ta biết khóa để mã hóa sẽ dễ dàng suy ra được khóa để giải mã

### **Phương pháp nào dễ phát hiện nhất trong các phương pháp tấn công sau:** 1- Tấn công từ chối dịch vụ 2- Tấn công phá hủy dịch vụ 3- Tấn công sửa đổi quyền hạn 4- Tấn công truy cập dự liệu bất hợp pháp

a. Tấn công từ chối dịch vụ

b. Tấn công truy cập dự liệu bất hợp pháp

c. Tấn công phá hủy dịch vụ

d. Tấn công sửa đổi quyền hạn

### So sánh tốc độ mã và giải mã của hệ mật mã công khai với mật mã bí mật khối hiện đại (với cùng độ dài bản rõ và độ dài khóa)?

a. Mật mã công khai nhanh hơn

b. Mật mã công khai chậm hơn

c. Không xác định chính xác

d. Tốc độ như nhau

### Theo Kichoff, sự an toàn của hệ mật phụ thuộc vào

a. sự phức tạp của giải thuật mã hóa

b. sự phức tạp của giải thuật giải mã

c. sự bí mật của khóa và sự phức tạp của giải thuật mã hóa

d. sự bí mật của khóa

### **Mô hình mã hóa kết hợp giữa hệ mã hóa công khai và bí mật được sử dụng là:**

a. Sử dụng hệ mã hóa bí mật để mã hóa khóa công khai, sử dụng hệ mã hóa công khai để mã hóa thông điệp

b. Sử dụng hệ mã hóa công khai mã hóa thông điệp, hệ mã hóa bí mật mã hóa thông điệp lần 2

c. Sử dụng hệ mã hóa công khai để mã hóa khóa bí mật, thông điệp được mã hóa bằng hệ mã hóa khóa bí mật

d. Sử dụng hệ mã hóa bí mật mã hóa thông điệp, hệ mã hóa công khai mã hóa thông điệp lần 2.

e. Sử dụng hệ mã hóa bí mật mã hóa thông điệp, hệ mã hóa công khai mã hóa khóa bí mật và cùng truyền

f. Sử dụng hệ mã hóa công khai mã hóa thông điệp, hệ mã hóa bí mật mã hóa khóa bí mật và cùng truyền

### **Trong hệ thống có n thành viên tham gia, nếu sử dụng hệ mã hóa bí mật mỗi thành viên cần nắm số khóa là :**

a. n-1

b. n\*(n-1)/2

c. (n-1)/2

d. n\*(n-1)

### Phát biểu nào sau đây đúng về độ an toàn của hệ mã hóa trên đường cong Elliptic

a. Phụ thuộc vào bài toán tính số nguyên tố p,q khi biết N=p\*q

b. Phụ thuộc vào bài toán tìm số nghịch đảo của số e trong miền số cực lớn

c. Phụ thuộc vào độ lớn của không gian khóa

d. Phụ thuộc vào bài toán tìm k khi biết Q,p trong phép Q=k\*p với Q,p là 2 điểm trên đường cong

### Hình thức tấn công giao thức thụ động được hiểu a. Đối tượng thứ 3 nghe lén các giao dịch, khi phát hiện kẽ hở sẽ lợi dụng tấn công phiêu giao dịch b. Đối tượng thứ 3 nghe lén các giao dịch, phát hiện đặc trưng và tung các giao dịch giả mạo nhằm thu lợi c. Đối tượng thứ 3 nghe lén các giao dịch, tìm hiểu các qui tắc và sau đó tham gia sửa đổi giao dịch d. Đối tượng thứ 3 nghe lén các giao dịch, thu thập thông tin về các giao dịch

### Hình thức tấn công giao thức chủ động được hiểu

a. Đối tượng thứ 3 nghe lén các giao dịch, thu thập thông tin về các giao dịch

b. Đối tượng thứ 3 nghe lén các giao dịch, khi phát hiện kẽ hở sẽ lợi dụng thay đổi nội dung phiên giao dịch đó

c. Đối tượng thứ 3 nghe lén các giao dịch, tìm hiểu các qui tắc và sau đó can thiệp các phiên giao dịch

d. Đối tượng thứ 3 nghe lén các giao dịch, thu lợi từ việc nắm được các thông tin giao dịch

### Phát biểu nào sau đây đúng về hình thức tấn công giao thức thụ động

a. Đối tượng tấn công là người ngoài hệ thống, thu thập thông tin về các giao dịch trong hệ thống

b. Đối tượng tấn công là người trong hệ thống, thu thập thông tin về một giao dịch có chủ đích trong hệ thống

c. Đối tượng tấn công là người trong hệ thống, thu thập thông tin về các giao dịch trong hệ thống

d. Đối tượng tấn công là người trong hệ thống, thu thập các thông tin về mọi giao dịch trong hệ thống

### Mã hóa là

a. Giấu thông tin để không nhìn thấy

b. Nén thông tin

c. Giữ bí mật thông tin

d. Biến đổi thông tin từ dạng đọc được sang dạng không đọc được

### Giải mã là

a. biến đổi thông tin từ dạng đọc được sang dạng không đọc được

b. biến đổi thông tin từ dạng không đọc được sang dạng đọc được

c. tấn công hệ mật mã để tìm bản rõ và khóa bí mật

d. giải nén thông tin

### Ưu điểm của hệ mã khóa bí mật so với hệ mã hóa khóa công khai là

a. Tốc độ xử lý của hệ mã khóa bí mật cao hơn hệ mã khóa công khai

b. Độ lớn khóa của hệ mã khóa bí mật cao hơn độ lớn khóa của hệ mã hóa khóa công khai

c. Độ an toàn của các thuật toán mã hóa khóa bí mật cao hơn hệ mã hóa khóa công khai

d. Không gian bản mã của hệ mã khóa bí mật cao hơn hệ mã khóa công khai

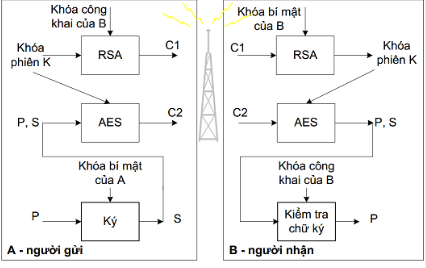
### Giải thuật Oclit dùng để

a. Kiểm tra số nguyên tố

b. Tìm giá trị nghịch đảo của số nguyên và tìm ước số chung lớn nhất giữa hai số nguyên   
c. Tìm lũy thừa nhanh trên trường số nguyên

d. Tìm số đồng dư trên trường số nguyên

### Câu hỏi không rõ?



1. Trong sơ đồ trên,P và S sử dụng AES để mã hóa vì kích thước của P và S là không đáng kể
2. Trong sơ đồ trên,P và S sử dụng AES để mã hóa vì tốc độ AES nhanh và kích thước của S lại lớn ( thông điệp sau khi được kí sẽ chứa 1 lượng chữ ký = độ dài thông điệp)
3. Trong sơ đồ trên,P và S sử dụng AES để mã hóa vì độ an toàn của AES cao
4. Trong sơ đồ trên,P và S sử dựng AES để mã hóa vì AES sử dụng khóa K và khóa công phai của B nên độ an toàn cao

### Khi ký lên một nội dung số có kích thước lớn ta thường thực hiện

a. Ký ở đầu và cuối của văn bản số

b. Ký trên đại diện của nội dung số

c. Ký trên toàn nội dung số

d. Ký trên những phần quan trọng của nội dung số

d. giải thuật mã hóa thực hiện chậm

### Giải thích nào là đúng về tấn công thụ động trong các ý dưới đây

a. Tấn công thụ động là việc đối tượng tấn công chờ đợi sự cố của hệ thống qua đó để lộ những kẻ hở để lợi dụng kẽ hở đó tấn công vào hệ thống

b. Tấn công thụ động là việc đối tượng tấn công chờ đợi sự sơ xuất của chủ thể để lợi dụng kẽ hở đó tấn công vào hệ thống

c. Tấn công thụ động là việc đối tượng tấn công bằng nhiều phương pháp và cách thức khác nhau nhưng không biết cách thức, phương pháp nào là chính xác và chỉ chờ đợi xác xuất thành công.

d. Tấn công thụ động là việc đối tượng tấn công chờ đợi quá trình truyền dữ liệu giữa các bên để qua đó đọc dữ liệu trên đường truyền

### Giao thức trao đổi khóa sử dụng chứng chỉ khóa công khai nhằmmục tiêu

a. chống giả mạo danh tính

b. mã hóa văn bản

c. giải mã văn bản đã mã hóa

d. kết hợp các mục tiêu trên

## New

### Khi ký lên một nội dung số có kích thước lớn ta thường thực hiện

a. Ký ở đầu và cuối của văn bản số

b. Ký trên đại diện của nội dung số

c. Ký trên toàn nội dung số

d. Ký trên những phần quan trọng của nội dung số

### Sự an toàn của hệ mã Diffie - Hellman dựa trên

a. kênh an toàn

b. dựa vào độ tin cậy của trọng tài

c. bí mật của khóa phiên dùng chung

d. độ khó bài toán logarith rời rạc

### Một trong những nhược điểm của hệ mã El Gamal

a. bản mã lặp từ bản rõ

b. không an toàn so với rsa

c. độ dài bản mã tăng so với bản rõ

d. giải thuật mã hóa thực hiện chậm

### Độ khó của giải thuật mã hóa El Gamal dựa trên

a. giải thuật sinh khóa phức tạp

b. độ khó của giải thuật phân tích số nguyên tố

c. độ khó của giải thuật logarith rời rạc

d. độ khó của bản mã độ dài lớn

### Nếu đưa một văn bản qua hàm băm sau 2 lần liên tiếp ta thu được kết quả

a. Kích thước đầu ra giảm so với việc sử dụng hàm băm 1 lần

b. Ta thu lại kết quả chính bằng văn bản đầu vào đưa vào bảng băm

c. Kích thước đầu ra không thay đổi so với việc sử dụng hàm băm 1 lần

d. Giá trị đầu ra sau 2 lần không thay đổi so với việc sử dụng hàm băm 1 lần

### Hàm một chiều sử dụng trong

1. Hệ mã Khóa bí mật
2. Giải thuật hàm băm
3. Giải thuật chữ ký số
4. Hệ mã khóa công khai

### Việc sử đưa văn bản qua hàm băm nhiều lần liên tiếp phục vụ mục đích

a. Xây dựng đại diện là duy nhất

b. Giảm kích thước của đại diện

c. Tăng độ an toàn cho đại diện

d. Tăng tính phức tạp của thuật toán xây dựng đại diện

### Ành 5.1 ( ảnh đâu?)

a. Trong sơ đồ trên, chữ ký S có kích thước tỉ lệ mã hóa của văn bản P.

b. Trong sơ đồ trên, chữ ký S có kích thước bằng đúng văn bản P.

c. Trong sơ đồ trên, chữ ký S có kích thước lớn hơn kích thước văn bản P

d. Trong sơ đồ trên, chữ ký S có kích thước bằng đại diện của văn bản P.

### Phát biểu nào sau đây đúng về chữ ký điện tử

a. Một chữ ký điện tử tiêu chuẩn sẽ có kích thước khác nhau khi sử dụng với các văn bản có độ dài khác nhau nếu ký văn bản đó trên đại diện của chúng qua cùng một hàm băm

b. Một chữ ký điện tử tiêu chuẩn sẽ có kích thước như nhau khi sử dụng với các văn bản có độ dài khác nhau nếu ký văn bản đó trên đại diện của chúng qua cùng một hàm băm

c. Một chữ ký điện tử tiêu chuẩn sẽ có kích thước như nhau khi sử dụng với các văn bản có độ dài khác nhau

d. Một chữ ký điện tử tiêu chuẩn sẽ có kích thước khác nhau khi sử dụng với các văn bản có độ dài khác nhau

### Phương pháp nào dễ dàng bị tấn công nếu đối tượng tấn công là người bên ngoài hệ thống

a. Tấn công sửa đổi quyền hạn

b. Tấn công truy cập dự liệu bất hợp pháp

c. Tấn công phá hủy dịch vụ

d. Tấn công từ chối dịch vụ

### Phát biểu nào sau đây dúng với hệ mã Vigenere

a. Hệ mã này yêu cầu khóa mã hóa phải có độ dài bằng cả nội dung bản rõ

b. Hệ mã này có yêu cầu để mã hóa 1 từ cần khóa có độ dài m bất kỳ

c. Hệ mã này đảm bảo trong 1 khối dữ liệu 1 từ được mã hóa bằng 1 khóa riêng

d. Hệ mã này có thể được dò bằng phương pháp tính xác suất

### hệ mã Affine và Vigenere có đặc điểm chung:

a. mã hóa đơn vị bít

b. hệ mã khối

c. số khóa bằng nhau

d. giữ nguyên tần suất xuất hiện chữ mã của bản mã

### Khóa trong cài đặt Aes được lựa chọn

a. 64, 128, 192 bít

b. 64, 192, 256 bít

c. 64, 128, 192, 256 bít

d. 128, 192, 256 bít

### Trong chuẩn mã hóa Aes, kết luận nào sau là sai:

a. độ dài khóa có thể thay đổi

b. khối đơn vị dữ liệu mã hóa có thể thay đổi

c. số vòng có thể thay đổi

d. độ an toàn tương đương Des

### Trong các phát biểu dưới đây, phát biểu nào là chính xác

a. Ta có thể tăng độ an toàn dữ liệu cho đại diện bằng phương pháp băm nhiều lần liên tiếp

b. Mỗi dữ liệu chỉ có duy nhất một đại diện và mỗi đại diện chỉ đại diện duy nhất một dữ liệu

c. Ta có thể giảm thiểu kích thước đại diện dữ liệu bằng cách sử dụng phương pháp băm nhiều lần liên tiếp

d. Đại diện dữ liệu được sử dụng để xác minh sự thay đổi dữ liệu

### Một chức năng mã hóa của hệ mã khóa công khai là

a. mã hóa khóa mật của giải thuật mã khối

b. mã hóa chữ ký số

c. mã hóa văn bản có độ an toàn cao như mã khối

d. mã hóa giá trị băm

### Một trong những khác biệt giữa giải thuật Aes và giải thuật Des là

a. Aes là hệ mã khóa đối xứng còn Des là hệ mã khóa bí mật

b. Aes cải thiện tốc độ so với Des

c. Aes không cần chế độ sử dụng mã khối còn Des vẫn sử dụng chế độ sử dụng mã khối

d. Aes giảm bớt số lượng bảng thế so với Des

### Hàm phi Ơle của n là

a. Số các số nguyên tố cùng nhau với n và nhỏ hơn n

b. Số các số nguyên dương nhỏ hơn n

c. Số các số nguyên tố nhỏ hơn n

d. Số các số nguyên tố cùng nhau với n

### Phát biểu nào sau đây đúng về hệ mã Knapsack

a. Mã hóa chính là giải bài toán xếp ba lô với các giá trị 0-9

b. Giải mã chính là giải bài toán xếp ba lô với các giá trị 0-9

c. Mã hóa chính là giải bài toán xếp ba lô với các giá trị 0-1

d. Giải mã chính là giải bài toán xếp ba lô với các giá trị 0-1

### Khi kết hợp giữa hệ mã hóa khóa công khai và hệ mã hóa khóa bí mật, kịch bản được sử dụng là

a. Sử dụng hệ mã hóa khóa công khai để truyền khóa bí mật và hệ mã hóa khóa bí mật để mã hóa thông điệp

b. Sử dụng hệ mã hóa khóa công khai để mã hóa dữ liệu, sử dụng hệ mã hóa khóa bí mật để mã hóa khóa bí mật và công khai

c. Sử dụng hệ mã hóa khóa bí mật để mã hóa và truyền khóa công khai

d. Sử dụng hệ mã hóa khóa bí mật để mã hóa và truyền khóa bí mật

### Cho kết luận đúng về SHA-1

a. Hàm băm được dùng trong hệ chữ ký số Merkle - Hellman

b. Hàm băm được dùng trong hệ chữ ký số El -Gammal

c. Hàm băm được dùng trong hệ chữ ký số RSA

d. Hàm băm được dùng trong hệ chữ ký số tiêu chuẩn @

### Kết luận nào sau là đúng cho Triple Des

a. Có 3 khóa, mỗi khóa độ dài 112 bít

b. Có 3 khóa, mỗi khóa có độ dài 128 bít

c. Có 3 khóa, mỗi khóa có độ dài 64 bít

d. Có 3 khóa, mỗi khóa có độ dài 192 bít

### Giải thuật nào sau không dùng để mã hóa và giải mã thông tin

a. Giải thuật EI-Gamal

b. Giải thuật Diffie-Hellman

c. Giải thuật RC-2

d. Giải thuật RSA

### Steganorgraphy là gì?

a. Mã hóa công khai

b. Ẩn đi nội dung của tin bằng cách mã hoá chúng

c. Mã hóa cổ điển

d. bảo vệ thông tin khỏi truy cập trái phép bằng cách ẩn đi sự tồn tại các thông tin mật

### Message digest là gì?

a. chữ ký số

b. giá trị băm

c. bản rõ

d. bản mã