Theo Shannon, để che giấu sự dư thừa thông tin bản rõ:

Select one:

Kết hợp các đáp án trên

Nén thông tin

Giải thuật mã hóa phức tạp

Khóa độ dài lớn

Microsoft Word sử dụng giải thuật mật mã nào để mã hóa văn bản

Select one:

a. Mật mã khóa công khai

b. Mật mã khóa phi đối xứng

c. Mật mã cổ điển

d. Mật mã khóa đối xứng

Hệ mã RSA với n= 115, e = 19 hãy cho biết khóa mật (p,q,d):

Select one:

(23, 5, 19)

(22, 4, 51)

(23, 5, 51)

(22, 4, 19)

Hệ mã RSA với n = 69, e = 23 hãy cho biết kết quả mã hóa bản rõ 15:

Select one:

23

15

51

60

Hệ mã RSA với n = 121, e = 27 hãy cho biết sinh mã chữ ký số từ bản rõ 23:

Select one:

111

23

Không xác định

27

Chữ ký số:

Select one:

Bảo mật khóa của văn bản

Bảo mật nội dung văn bản

Xác nhận tính sở hữu của văn bản

Không cho phép thay đổi nội dung văn bản

Hệ mã RSA với n = 143, e = 7 hãy cho biết kết quả mã hóa bản rõ 100:

Select one:

100

200

300

50

Hệ mã RSA với n = 169, e = 7 hãy cho biết kết quả mã hóa bản rõ 15:

Select one:

63

15

37

Không xác định

Kết luận nào đúng:

Select one:

Tốc độ mã hóa và giải mã trong hệ mã PKC là tương đương

Hệ mã PKC cho phép mã hóa khóa của hệ mã SKC

PKC là viết tắt của cụm từ Private key cryptography

PKC có giải thuật mã hóa và giải mã giống nhau

Kết luận nào đúng:

Select one:

Hệ mã hóa Merkle – Hellman có độ an toàn kém so với RSA

Hệ mã hóa Merkle - Hellman dựa trên độ khó bài toán logarith rời rạc

Hệ mã hóa Merkle - Hellman được ứng dụng rộng rãi

Hệ mã hóa Merkle - Hellman có độ dài khóa nhỏ

Hãy tính khóa đảo trong hệ mã Hill biết khóa K = [11][16];[10][21]:

Select one:

Không tính được khóa đảo

[23][6];[17][20]

[23][6];[20][17]

[23][7];[20][17]

Chế độ sử dụng mã khối OFB hay CFB ứng dụng chủ yếu trong

Select one:

a. Mật mã khóa công khai

b. Mạng viễn thông

c. Mật mã khối Aes

d. Mật mã khối Des

Hãy tính khóa đảo trong hệ mã Hill biết khóa K = [25][10];[15][19]:

Select one:

Không tính được khóa đảo

[1][17];[14][15]

[25][15];[15][19]

[1][14];[17][15]

Hãy tính khóa đảo trong hệ mã Hill biết khóa K = [11][19];[4][23]:

Select one:

Không tính được khóa đảo

[11][9];[6][13]

[11][19];[6][3]

[11][9];[6][3]

Hãy tính khóa đảo trong hệ mã Hill biết khóa K = [24][13];[21][17]:

Select one:

Không tính được khóa đảo

[19][10];[13][1]

[19][1];[13][10]

[19][13];[1][10]

Kết luận nào sau là đúng cho DES:

Select one:

DES là hệ mã hóa dựa trên Lucipher

DES là hệ mã hóa có không gian khóa nhỏ

DES là hệ mã hóa PKC

DES là hệ mã hóa có độ phức tạp thấp

Kết luận nào đúng:

Select one:

Hệ mã khóa công khai an toàn tương đương mã khối

Hệ mã khóa công khai an toàn cao hơn mã khối

Hệ mã khóa công khai dùng trong mạng Internet

Hệ mã khóa công khai có tốc độ tính toán nhanh hơn mã khối

Kết luận nào đúng với hệ mã khóa công khai:

Select one:

Mỗi thành viên có một cặp khóa

Khóa riêng xác nhận chữ ký, khóa công khai sinh chữ ký

Khóa riêng mã hóa, khóa công khai giải mã

Không tồn tại trường hợp lộ bản rõ

Kết luận nào đúng cho hàm băm:

Select one:

Phi đụng độ của MD-5 tương đương so với SHA-1

Hàm băm chỉ được áp dụng trong chữ ký số

Phi đụng độ của MD-5 hơn so với SHA-1

Hàm băm được dùng tạo tài khoản người dùng trên mạng

Middle – Attack là hình thức thám mã:

Select one:

Sao chép bản tin

Gửi bản tin cũ

Chủ động

Thụ động

Hệ thống phân phối khóa Blom thực hiện:

Select one:

Phân phối từng cặp khóa bí mật một cho từng người dùng trong hệ thống

Phân phối một hàm số riêng, người dùng tự xây dựng khóa dùng chung nhờ kết hợp hàm số riêng với khóa công khai

Phân phối một khóa chung dùng cho cả nhóm người dùng

Phân phối khóa bí mật và công khai của từng người dùng, khóa công khai được thông báo chung cho cả nhóm

Kết luận nào đúng cho hàm băm:

Select one:

Phi đụng độ của MD-5 hơn so với SHA-1

MD-5 không có phi đụng độ

Phi đụng độ của MD-5 tương đương so với SHA-1

Phi đụng độ của MD-5 kém so với SHA-1

Ứng dụng chữ ký số có nhãn thời gian:

Select one:

a. Quy định thời gian ký

b. Ký và xác minh thông tin chỉ 1 lần.

c. Chống sửa đổi thông tin hoặc chữ ký

d. Quy định thời gian xác minh chữ ký

Chữ ký số RSA khác với hệ mã hóa RSA ở các điểm:

Select one:

Sử dụng chung cặp khóa nhưng thứ tự sử dụng khóa ngược nhau

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

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

Trong chữ ký số vai trò của khóa bí mật và công khai không rõ rang

Chữ ký số RSA giống với hệ mã hóa RSA ở các điểm:

Select one:

Sử dụng khóa bí mật và công khai

Sử dụng khóa bí mật và công khai, khóa bí mật được sử dụng để mã hóa và công khai để giải mã

Sử dụng chung các thuật toán mã hóa và giải mã như nhau

Sử dụng khóa bí mật và công khai theo thứ tự thực hiện giống nhau

Kết luận nào đúng:

Select one:

Chữ ký có kích thước bằng chính văn bản cần ký

Chữ ký số có thể dùng nhãn thời gian

Chữ ký trên văn bản khác nhau sẽ có kích thước khác nhau

Chữ ký trên văn bản có độ dài bằng giá trị băm

Giao thức Diffie – Hellman sử dụng chứng chỉ loại trừ thám mã:

Select one:

Giải mã bản tin

Giả mạo danh tính

Gửi bản tin cũ

Sử dụng khóa cũ

Replay – Attack là hình thức thám mã:

Select one:

Sử dụng thông tin cũ

Sao chép bản tin

Thụ động

Chủ động

Giao thức thỏa thuận khóa:

Select one:

Có trung tâm thứ ba tham gia tạo, gửi khóa cho hai bên

Hai bên thực hiện quản lý, trao đổi khóa

Có bên thứ ba tham gia tạo, gửi khóa cho hai bên

Tối đa 2 thành viên

Giải thuật lũy thừa nhanh được áp dụng cho:

Select one:

Hệ chữ ký số

Hệ mã khóa công khai

Hệ mã khóa bí mật

Hệ mã khóa công khai và chữ ký số

Giải thuật đoán số nguyên tố:

Select one:

Cho phép thám mã có thể giải mã hệ mã khối

Cho phép thám mã có thể giải mã RSA

Xác định đúng một số là số nguyên tố

Cho phép thám mã có thể giả mạo chữ ký số

Kết luận nào sau là đúng

Select one:

a. Mã Vigenere là trường hợp riêng từ mã Hill.

b. Mã cộng là trường hợp riêng từ mã Hill

c. Mã Caesar là trường hợp riêng từ mã cộng

d. Mã cộng là mật mã khác xa mã Caesar

Số nghịch đảo được dùng cho:

Select one:

Hệ mã Aes

Hệ mã Vigenere

Hệ mã Aes và PKC

PKC

Hệ mã Aes có mấy bảng thế S – box cho quá trình mã hóa:

Select one:

3

2

1

4

Mật mã PKC nào có thể cho nhiều hơn một bản mã từ một cặp khóa bí mật-công khai và một bản rõ biết trước:

Select one:

a. RSA

b. El-gamal

c. Không tồn tại

d. Merkle-Hellman

Hãy cho biết đặc điểm hàm băm:

Select one:

Tạo giá trị đầu ra có độ dài không đổi

Mã hóa được bản rõ

Tạo giá trị đầu ra có độ dài thay đổi

Với cùng một giá trị đầu vào sẽ thu được các giá trị đầu ra khác nhau

Cấu trúc của một hệ chữ ký số gồm:

Select one:

Chữ ký trên đại diện

Đại diện thông điệp và chữ ký

Chữ ký trên thông điệp

Thông điệp và chữ ký

Kết luận nào sai:

Select one:

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

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

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

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

Hình thức tấn công chủ động được hiểu:

Select one:

Thám mã nghe lén các giao dịch, tìm hiểu các qui tắc và sau đó can thiệp các phiên giao dịch

Thám mã nghe lén các giao dịch, khi phát hiện kẽ hở sẽ lợi dụng thay đổi nội dung phiên giao dịch đó

Thám mã nghe lén các giao dịch, khi phát hiện kẽ hở sẽ lợi dụng thay đổi nội dung phiên giao dịch đó

Thám mã nghe lén các giao dịch, thu thập thông tin về các giao dịch

Hình thức tấn công thụ động được hiểu:

Select one:

Thám mã nghe lén các giao dịch, thu thập thông tin về các giao dịch

Thám mã nghe lén các giao dịch, phát hiện đặc trưng và tung các giao dịch giả mạo nhằm thu lợi

Thám mã nghe lén các giao dịch, khi phát hiện kẽ hở sẽ lợi dụng tấn công phiêu giao dịch

Thám mã nghe lén các giao dịch, tìm hiểu các qui tắc và sau đó tham gia sửa đổi giao dịch

Mật mã khóa phi đối xứng được hiểu là:

Select one:

a. Mật mã khóa cổ điển

b. Mật mã khóa bí mật

c. Mật mã khóa khối

d. Mật mã khóa công khai

Giải thuật Lehman có thể được áp dụng cho:

Select one:

Giải mã hệ RSA

Giải mã hệ mã Merkle – Hellman

Giải mã hệ mã DES

Giải mã hệ El – gamal

Kết luận nào sau là sai

Select one:

a. Giải thuật lũy thừa đồng dư ứng dụng cho chữ ký số

b. Giải thuật lũy thừa đồng dư ứng dụng cho giao thức quản lý khóa

c. Giải thuật lũy thừa đồng dư ứng dụng nhiều cho mật mã cổ điển

d. Giải thuật lũy thừa đồng dư áp dụng nhiều cho mật mã khối

Kết luận nào sau là đúng:

Select one:

a. Microsoft Word chỉ mã hóa cho văn bản

b. Microsoft Word chỉ sinh chữ ký số cho văn bản

c. Microsoft Word không hỗ trợ mã hóa và không hỗ trợ chữ ký số cho văn bản

d. Microsoft Word cho phép mã hóa và sinh chữ ký số cho văn bản

Hệ mã RSA với n= 221, e=31 hãy cho biết kết quả mã hóa bản rõ 10:

Select one:

114

31

141

10

Hệ mã RSA với n= 221, e=31 hãy cho biết khóa mật (p,q,d):

Select one:

(17, 13, 31)

(16, 12, 31)

(16, 12, 13)

(17, 13, 13)

Hệ mã nào khác loại so với các hệ mã còn lại:

Select one:

RSA

El – gamal

Merkle – Hellman

Aes

Hàm one – way:

Select one:

Mã hóa chậm nếu không có khóa

Giải mã chậm nếu không có khóa

Ứng dụng trong hệ SKC

Ứng dụng trong mã khối

Trong giải thuật mã khối, sử dụng bảng thế số liệu thay cho biểu thức tính toán:

Select one:

Tạo thuận tiện cho lập trình

Tăng tốc độ tính toán

Kết hợp các đặc điểm trên

Giải mã khó

Chế độ sử dụng mã khối nào không sử dụng giá trị IV:

Select one:

CBC

ECB

CFB

OFB

Hệ mã nào khác loại so với các hệ mã còn lại:

Select one:

RSA

Affine

Merkle – Hellman

El – gamal

Hệ mã nào khác loại so với các hệ mã còn lại:

Select one:

Affine

Vigenere

Hill

Des

Mạng có n thành viên, nếu sử dụng hệ mã hóa bí mật thì số lượng tối đa khóa sinh ra:

Select one:

a. 2n

b. n(n+1)/2

c. n

d. n(n-1)/2

Khóa riêng (p,q) nào sau là sai đối với mật mã RSA

Select one:

a. (17, 19)

b. (19, 17)

c. (31, 31)

d. (11, 13)

???

Kết luận nào sai:

Select one:

Hệ mã hóa RSA luôn tồn tại hiện tượng bản rõ trùng bản mã

Hệ mã hóa Merkle - Hellman có độ dài khóa lớn

Hệ mã hóa Merkle - Hellman có độ an toàn thấp

Hệ mã hóa Elgamal luôn tồn tại hiện tượng bản rõ trùng bản mã

Hàm băm có số lượng giá trị băm là 216, nếu thám mã tìm khả năng đụng độ là 0.5 thì số lượng ít nhất văn bản khác nhau đem thử:

Select one:

210

450

302

390

Chứng chỉ chữ ký số của một cá nhân

Select one:

a. Không chứa thông tin giải thuật chữ ký số

b. Cho phép nhiều người xác minh được danh tính chủ sở hữu

c. Được tạo bởi bất kỳ ai

d. Chỉ cá nhân đó có thể xác minh danh tính

Kết luận nào đúng cho chứng chỉ X.509:

Select one:

Chuẩn mã hóa

Chuẩn chữ ký số

Chuẩn mã hóa, chuẩn chữ ký số, và chuẩn chứng chỉ khóa công khai

Chuẩn chứng chỉ khóa công khai

Để ký lên một nội dung số có kích thước lớn, thực hiện:

Select one:

Ký trên toàn nội dung số

Ký trên những phần quan trọng của nội dung số

Ký tại cuối văn bản

Ký trên đại diện của nội dung số

Kết luận nào sau là sai

Select one:

a. Chữ ký số RSA và DSA được ứng dụng

b. Chỉ có chữ ký số DSA là được ứng dụng

c. Chữ ký số Merkle-Hellman không được ứng dụng phổ biến

d. Chữ ký số El-gamal không được ứng dụng phổ biến

Giao thức có người phân xử được hiểu:

Select one:

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

Khi có tranh chấp xẩy ra, một bên mời người trung gian vào để xác nhận toàn bộ quá trình giao dịch

Các qui tắc giao dịch được xây dựng từ trước, người trung gian chỉ được sử dụng khi có tranh chấp xẩy ra

Một trọng tài giám sát toàn bộ quá trình giao dịch và phân xử khi có tranh chấp xẩy ra

Nhãn thời gian trong giao thức Kerberos loại bỏ trường hợp thám mã:

Select one:

Giả mạo danh tính

Sử dụng khóa cũ và giả mạo danh tính

Sử dụng khóa cũ

Middle attach

Ưu điểm của mật mã El-gamal:

Select one:

a. Tốc độ thực hiện nhanh

b. An toàn vượt trội

c. Không có rắc rối bản quyền sử dụng

d. Cài đặt dễ

Sử dụng chữ ký số lên đại diện nội dung số:

Select one:

Tăng tính bảo mật của chữ ký số trên nội dung số

Tăng tính bảo mật của nội dung số

Tạo và xác nhận chữ ký nhanh chóng

Sinh chữ ký số giống chữ ký tay

Giao thức thỏa thuận khóa:

Select one:

Tạo khóa cho hệ chữ ký số

Tạo khóa cho hệ mã khóa đối xứng

Tạo khóa cho hệ mã khóa phi đối xứng

Tạo khóa cho hệ mã khóa đối xứng, khóa phi đối xứng, và hệ chữ ký số.

Chứng chỉ khóa công khai được dùng cho:

Select one:

Mã hóa khóa công khai, chữ ký số

Giao thức quản lý trao đổi khóa, chữ ký số

Mã hóa khóa công khai, chữ ký số và giao thức quản lý khóa

Giao thức quản lý trao đổi khóa , mã hóa khóa công khai

Mật mã nào sau không sử dụng phép tính nghịch đảo đồng dư

Select one:

a. Rsa

b. Hill

c. Des

d. Aes

Kết luận nào sai cho hệ mã khóa công khai PKC:

Select one:

PKC có cửa bẫy khiến giải mã khó

PKC được dùng cho mã hóa khóa của hệ mã đối xứng

PKC có giải thuật mã hóa và giải mã tương tự nhau

PKC là một loại hệ mã khóa phi đối xứng

Kết luận nào sai:

Select one:

Hệ mã Merkle – Hellman không được ứng dụng rộng rãi trong mạng Internet

Hệ mã Merkle – Hellman được ứng dụng rộng rãi trong chữ ký số

Mật mã El-gamal được ứng dụng trong mô hình thỏa thuận khóa

Hệ mã RSA được ứng dụng rộng rãi trong mạng Internet

Cơ sở của giải thuật chữ ký số tiêu chuẩn DSA:

Select one:

Giải thuật chữ ký số El - gamal

Giải thuật chữ ký số Merkle – Hellman

Giải thuật chữ ký số RSA

Giải thuật mật mã Des

Chứng chỉ khóa công khai có mô tả:

Select one:

Khóa và giải thuật chữ ký

Khóa, giải thuật băm, giải thuật chữ ký

Khóa, giải thuật mã hóa và giải mã văn bản

Khóa và giải thuật mã hóa văn bản

Mệnh đề nào sau đây là sai:

Select one:

DES có các khóa con độ dài 56 bít

DES có 4 khóa yếu

DES có các khóa con độ dài 48 bít

DES có 6 cặp khóa nửa yếu

Chế độ sử dụng mã khối nào là phổ thông:

Select one:

OFB

ECB

CFB

CBC

Chế độ sử dụng mã khối được ứng dụng cho

Select one:

a. Sinh mã xác thực

b. Mã hóa cổ điển

c. Mã hóa khóa phi đối xứng

d. Sinh chữ ký số

Kết luận nào đúng:

Select one:

Hệ mã Merkle – Hellman an toàn kém so với RSA

Hệ mã Merkle – Hellman có khóa siêu tăng là khóa công khai

Hệ mã Merkle – Hellman an toàn cao

Hệ mã Merkle – Hellman có cửa bẫy chứa trong khóa công khai

Kết luận nào đúng:

Select one:

Hệ mã Merkle – Hellman được ứng dụng rộng rãi trong mạng Internet

Hệ mã El – Gamal được ứng dụng rộng rãi trong mạng Internet

Hệ mã Merkle – Hellman được ứng dụng rộng rãi trong chữ ký số

Mật mã RSA được ứng dụng trong chữ ký số

Kết luận nào sau là sai

Select one:

a. Hàm băm Md-5 có thể dùng cho chữ ký số

b. Hàm băm Sha an toàn hơn Md-5

c. Chỉ các hàm băm Sha được dùng cho chữ ký số

d. Hàm băm Md5 tồn tại đụng độ

Hãy tính khóa đảo trong hệ mã Hill biết khóa K = [20][13];[21][16]:

Select one:

[2][13];[27][22]

Không tính được khóa đảo

[2][25];[13][22]

[2][13];[25][22]

Hệ mã RSA với n= 143, e = 25 hãy cho biết kết quả giải mã bản mã 7:

Select one:

7

17

98

Không xác định

Kết luận nào đúng:

Select one:

Hệ mã Merkle – Hellman có khóa kích thước nhỏ

Hệ mã Merkle – Hellman không tính toán số nghịch đảo

Hệ mã Merkle – Hellman có cửa bẫy là khóa siêu tăng

Hệ mã Merkle – Hellman có cửa bẫy là khóa công khai

Hệ mã RSA với n = 91, e =27 hãy cho biết sinh mã chữ ký số từ bản rõ 23:

Select one:

13

32

Không xác định

23

Chữ ký số của một cá nhân:

Select one:

a. Độ dài thay đổi nhưng nội dung không đổi

b. Độ dài và nội dung tương đương văn bản ký

c. Độ dài cố định nhưng nội dung biến đổi theo văn bản ký

d. Độ dài và nội dung cố định

Kết luận nào đúng cho hàm băm SHA-I:

Select one:

Có 2\*160 giá trị băm

Có 160 giá trị băm

Có 1602 giá trị băm

Không gian băm độ dài 160 bit

Hệ mã RSA với n= 55, e=19 hãy cho biết khóa mật (p,q,d):

Select one:

(5,11, 19)

(4,10, 91)

(4,10, 19)

(5,11, 91)