# Câu 1. Mục tiêu chung của an toàn bảo mật thông tin ?

A. Tính bí mật

B. Tính toàn vẹn

C. Tính sẵn sàng

**D. Cả ba phương án trên**

# Câu 2. Theo luật của Kirchoff thì độ an toàn của hệ mã phụ thuộc vào yếu tố nào :

A. **Khóa**

B Giải thuật mã hóa

C. Giải thuật giải mã

D. Kết hợp các đáp án trên

# Câu 3. Các chiến lược an toàn hệ thống

A. Giới hạn quyền hạn tối thiểu

B. Bảo vệ theo chiều sâu

C. Nút thắt

D. Điểm nối yếu nhất

E. Tính toàn cục :

F. Tính đa dạng bảo vệ

**G. Tất cả các phương án trên**

# Câu 4. Ứng dụng của mật mã bao gồm :

A. Mã hóa , toàn vẹn thông tin , sinh chữ ký số , thỏa thuận khóa

**B. Bảo mật dữ liệu , xác thực toàn vẹn thông tin , chữ ký số và quản lý khóa**

C Bảo mật dữ liệu , xác thực thông tin , xác nhận chữ ký số , phân phối khóa

D. Mã hóa dữ liệu , tạo hàm băm , chữ ký số , quản lý khóa

# Câu 5. Các cách tăng sự an toàn của bản rõ trong hệ mã là :

A. Nên bản rõ

B. Che giấu mối quan hệ giữa bản rõ và bản mã

C. Tăng sự phụ thuộc giữ bản mã và bản rõ

**D Nén bản rõ , che giấu mối quan hệ giữa bản rõ và bản mã , tăng sự phụ thuộc giữ bản mã và bản rõ**

# Câu 6. Các yếu tố không ảnh hưởng đến sự an toàn của một hệ mã mật :

A. Bí mật của khóa

B. Giải thuật mã hóa và giải mã

**C. Độ dài bản mã**

D. Độ phức tạp tính toán của hệ mã

# Câu 7. Lược đồ của một hệ mật mã có mấy thành phần :

A. 3 tập khác nhau

B. 4 tập khác nhau

C.5 tập khác nhau

D.6 tập khác nhau

# Câu 8. SKC được hiểu là :

A**. Hệ mã khóa đối xứng**

B. Hệ mã khóa phi đối xứng

C. Hệ mã khóa dòng

D. Hệ mã khóa cổ điển

# Câu 9. PKC được hiểu là :

A. Hệ mã khóa đối xứng

**B. Hệ mã khóa phi đối xứng**

C. Hệ mã khóa dòng

D. Hệ mã khóa cổ điển

# Câu 10. Có mấy phương pháp chính cho việc mã hoá và giải mã

A. Hai ( mã hóa khóa đối xứng , mã hóa khóa công khai )

**B. Ba ( mã hóa khóa đối xứng , mã hóa khóa công khai , hàm băm )**

C. Bốn ( mã hóa khóa đối xứng , mã hóa khóa công khai , hàm băm , mã hóa dòng )

# Câu 11. Hệ mã khóa dòng được biết là một :

**A. Hệ mã khóa đối xứng**

B. Hệ mã khóa phi đối xứng

C. Hệ mã khóa công khai

D. Hệ mã khóa cổ điển

# Câu 12. Theo Shannon , để che giấu sự dư thừa thông tin bản rõ :

A. Giải thuật mã hóa phức tạp

B. Khóa độ dài lớn

C. Kết hợp các đáp án trên

**D. Bản mã có sự lộn xộn và sự rườm rà**

# Câu 13. Theo Shannon , hệ mã an toàn tuyệt đối nếu :

A. Giải thuật mã hóa phức tạp

B. Khóa thay đổi liên tục

**C. Khoá có độ dài tối thiểu là tương đương độ dài thông báo**

D. Kết hợp các đáp án trên

# Câu 14. Theo Shannon , entropy được hiểu là gì :

**A. Đo khối lượng thông tin của thông điệp**

B. Đo độ an toàn thông báo

C. Đo độ dài bản mã của thông báo

D. Kết hợp các đáp án trên

# Câu 15. Nghịch đảo của một số nguyên a trong tập Z là số :

A. Tồn tại với mọi điều kiện

**B. Tồn tại theo điều kiện**

C. Là số thực

D Là số chẵn

# Câu 16. Tìm nghịch đảo của 3 trong 48

a . 1

b . 2

**c . 3** vì 3\*3 mod 8 = 1

d . 4

# Câu 18. Tập giá trị của Z16 có bao nhiêu phần tử khả nghịch

A. 10

B. 11

**C. 12**

D. 13

# Câu 19. Tìm nghịch đảo của 7 trong Z1

a . 3

b . 5

c . 7

**d . 8 V**i 7 \* 8 mod 11 = 56 mod 11 = 1

# Câu 21. Tập Z9 , có bao nhiêu phần tử khả nghịch

A. 4

B. 5

**C. 6**

D. 7

# Câu 23. Trong các số sau số nào đồng dự với 9 khi modulo với 5

A. -10

**B. -11**

c . -12

D. -13

# Câu 26. Hãy mã hóa thông điệp P = KE với khóa a = 1 ; b = 3 sử dụng hệ mã hóa Affine

A. NM

B. YT

**C. NH**

D. HN

Câu 34. Hãy mã hóa sử dụng hệ mã Vigenere với thông điệp = BAOMAT , khóa K = TDC A. VDFQDU **B. UDQFDV** C. QDUVDI D. VDUVDI B + T mod 26 = 1 + 19 = 20 → U A + D → 3D O + C → 16 → Q M + T + 12 + 19 m 26 = 5 → F A + D → 3D T + C → 21 → V

Câu 40. Hãy mã hóa thông điệp HE sử dụng hệ mã Hill với 8 ) khóa K là ma trận 2x2 = ( 11-8 ; 3-7 ) có thể hiểu là ( 3 A. FX B. XF C. GL **D. LG**

Câu 44. Trong các khóa sau của mã HILL khóa nào không thể giải mã được

# Câu 1. Trong hệ mã khối , sử dụng bảng thay thế số liệu ( s - box ) cho biểu thức tính toán để :

**A. Tăng tốc độ tính toán**

B. Giải mã khó

C. Tạo thuận tiện cho lập trình

D. Kết hợp các đặc điểm trên

# Câu 2. Các hộp mật ( S - Box ) của giải thuật Des

A. Đầu vào chuỗi bịt độ dài 32 và sinh các chuỗi 32 bit

B. Đầu vào bịt độ dải 48 và sinh các chuỗi 40 bit

C. Đầu vào chuỗi bit độ dài 32 và sinh các chuỗi 40 bít

**D.Đầu vào cuỗi bit có độ dài 48 và sinh các chuỗi 32 bit**

# Câu 3 : Kết luận nào sau là đúng cho DES :

A. là hệ mã hóa có độ phức tạp thấp

B. là hệ mã hóa PKC

C. là hệ mã hóa có không gian khóa nhỏ

**D. là hệ mã hóa dựa trên mã Lucipher**

# Câu 4. AES có mấy khóa chính ( khóa chủ ) :

A. 2

**B.** 3

C. 4

D. 5

# Câu 5. Có mấy chế độ sử dụng mã khối :

A. 2

B. 3

**C.** 4

D. 5

# Câu 7. Mệnh đề nào sau đây là SAI :

A. DES có các khóa con độ dài 48 bit

B. DES có 4 khóa yếu

C. DES có 6 cặp khóa nửa yếu

**D. DES có các khóa con độ dài 32 bit**

# Câu 8. Số lượng hộp mật ( S - box ) của giải thuật Des :

A. 6

**B**. 8

C. 10

D. 12

# Câu 9. Các hệ mã hóa cổ điển là hệ mã :

A. Mã hóa dãy bit

B. Có khóa độ dài lớn

**C. Mã hóa một hoặc cụm ký tự rời rạc**

D. Có khóa được sinh theo giải thuật

# Câu 10. Trong hệ mã VIGENERE , nếu áp dụng bộ ký tự ASCII cho không gian bản rõ và bản mã thì với khóa độ dài 10 sẽ có số lượng khóa :

**A 256^10**

B , 2610

C. 10256

D. 256 \* 10

# Câu 11. Với hệ mã hóa AES có số vòng lặp :

1. 8 , 12 , hoặc 14
2. 8 , 10 hoặc 32
3. 10 , 16 , hoặc 32
4. 10 , 12 , hoặc 14

# Câu 12. Giải thuật mã hóa AES sử dụng khóa chủ độ dài 192 có số vòng lặp :

A. 8

**B**. 10

C. 12

D. 14

# Câu 13. Chế độ sử dụng mã khối nào là phổ thông :

• ECB

• **CBC**

• CFB

• OFB

# Câu 14. Chế độ sử dụng mã khối nào không sử dụng giá trị V ( Initialization Vector ) :

A. **ECB**

B. CBC

C. CFB

D. OFB

# Câu 15. Hệ mã Aes có mấy bảng thế S– box cho quá trình mã hóa :

A. 4

B. 3

**C.** 1

D. 2

# Câu 16. Cấu trúc đại số của DES khiến :

**A. Độ phức tạp không tăng nếu mã hóa lặp nhiều lần với các khóa cùng kích thước .**

# Câu 17. Trong hệ mã hóa khóa công khai nhận định nào sau đây là ĐÚNG ?

A. Sử dụng khóa mật để MÃ HÓA , sử dụng khóa công khai để GIẢI MÃ .

**B. Sử dụng khóa công khai để MÃ HÓA , khóa bí mật để GIẢI MÃ**

C. Sử dụng hai khóa do người gửi sinh ra

D. Sử dụng một khóa mật chung cho cả hai hệ mã

# Câu 18. Nhận định nào là SAI trong hệ mã hóa PKC ?

A. Sử dụng khóa mật để MÃ HÓA , sử dụng khóa công khai để GIẢI MÃ .

B. Sử dụng khóa công khai để MÃ HÓA , khóa bí mật để GIẢI MÃ

C. Hệ mã sử dụng hai khóa

**D. Sử dụng một khóa mật chung cho cả hai hệ mã**

# Câu 19. Ý tưởng của hệ mã hóa Knapsack ( Merkle – Hellman ) là

A. Tính khó giải của bài toán Logarit rời rạc

**B. Bài toán đóng thùng**

C. Tính khó giải của bài toán phân tích một số thành hai thừa số nguyên tố

D. Hệ mã hóa khóa bí mật .

# Câu 20. Ý tưởng của hệ mã hóa RSA

A. Tính khó giải của bài toán Logarit rời rạc

B. Bài toán đóng thùng

**C. Tính khó giải của bài toán phân tích một số thành hai thừa số nguyên tó**

D. Hệ mã hóa khóa bí mật .

# Câu 21. Ý tưởng của hệ mã hóa Elgama

**A. Tính khó giải của bài toán Logarit rời rạc**

B. Bài toán đóng thùng

C. Tính khó giải của bài toán phân tích một số thành hai thừa số nguyên tố

D. Hệ mã hóa khóa bí mật .

# Câu 22. Trong các hệ mã hóa sâu hệ mã nào không phải hệ mã hóa khóa công khai

A. Trapdoor

B. RSA

**C. DES**

D. Elgama

# Câu 23. Trong các hệ mã hóa sau hệ mã nào không phải hệ mã hóa khóa bí mật

A. **Trapdoor**

B. Hill

C. Affine

D. Caesar

# Câu 24. Trong các hệ mã hóa sau hệ mã nào không phải hệ mã hóa khóa khối

A. Trapdoor

B. DES

C. AES

D. **DSA**

# Câu 25. Chữ ký số là gì ?

A. Sử dụng khóa mật để kiểm tra chữ ký , khóa công khai để ký

B. Sử dụng chung một khóa vừa ký và kiểm tra chữ ký

C. Một hệ mã hóa khóa bí mật

**D. Sử** dụng khóa bí mật để ký , khóa công khai để kiểm tra chữ ký

# Câu 26. Trong hệ mã RSA với n = 143 , e = 7 hãy cho biết kết quả mã hóa x = 13 ?

A. 171

**B. 117**

C. 46

D. Không xác định

# Câu 31. Hệ mã RSA với n = 143 , e = 7 hãy cho biết kết quả giải mã bản mã 14 : ?

A. 72

B. **27**

C. 53

D. Không xác định

N = 143 = 11x13 ,p = 11 , q = 13

Phj = 10x12 = 120 và e = 7=>d = 103

Vậy giải mã 14 được x = 144103 m 143 = 27

# Câu 36. Hệ mã RSA với n = 221 , e = 23 hãy cho biết khóa mật ( P.4 , d ) :

**A. ( 17 , 13 , 167** )

B. ( 17,13,173 )

C. ( 16,12 , 167 )

D. ( 16,12 , 173 ) Gợi ý N = 17 \* 13 Phi = 1612 D là nghịch đảo của e đối với phi.d = 167

# Câu 40. Nhận định nào sau đây ĐÚNG về chữ ký số ?

A. Một bản mã hóa khóa công khai

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

C. Một phép kiểm tra trong đó những người biết khóa mật mới có thể kiểm tra được

**D. Một phép kiểm tra trong đó nhiều người có thể kiểm tra nhưng chỉ một người được tạo chữ ký**

# Câu 41. Nhược điểm của các hệ mật mã khóa công khai :

A. Khóa công khai nên nội dung thông điệp dễ dàng bị giải mã

B. Phương pháp mã hóa công khai nên không an toàn

**C. Tốc** độ xử lý của thuật toán chậm

D. Không gian khóa hẹp dễ bị thám mã

# Câu 42. 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 mã hóa thông điệp , hệ mã hóa công khai mã hóa khóa bí mật** và cùng truyền

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

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

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

# Câu 43. Hiện tượng lộ bản rõ trong thuật toán RSA được hiểu :

A. Thông điệp gốc dễ dàng bị suy luận ngược trở lại từ thông điệp mã hóa

**B. Kết qu**ả mã hóa không thay đổi so với thông điệp gốc

C. Nội dung thông điệp sau mã hóa có thể dễ dàng được suy luận từ thông điệp gốc

D. Thông điệp gốc dễ dàng bị sử dụng các phương pháp thám mã đề suy luận

# Câu 44. Kết luận nào đúng cho hệ mã hóa trên đường cong Elliptic :

**A. Khóa riêng là** một điểm trên đường cong

B. Độ phức tạp tính toán phân tích số nguyên tố

C. Không gian khóa rất lớn

D. Độ phức tạp tính toán lũy thừa

# Câu 45. Kết luận nào ĐÚNG cho hệ mã hóa trên đường cong Elliptic :

A. Độ dài bản mã bằng độ dài bản rõ

B. Giải thuật tính toán với các phép lũy thừa

**C. Độ** dài khóa nhỏ hơn RSA nhưng đáp ứng độ an toàn

D. Kết hợp các đáp án trên

# Câu 46. Trong hệ thống kết hợp giữa RSA và AES thì chức năng của các hệ mã hóa là :

**A**. AES mã hóa thông điệp , RSA mã hóa khóa của AES

B. RSA mã hóa thông điệp , AES mã hóa khóa của RSA

C. AES mã hóa thông điệp lần 1 , RSA mã hóa lần 2 để tăng cường tính bảo mật

D. RSẠ mã hóa thông điệp lần 1. AES mã hóa thông điệp lần 2 để tăng cường tính bảo mật

# Câu 47. Kết luận nào ĐÚNG :

A. Hệ mã Merkle - Hellman có của bấy là khóa công khai

B. Hệ mà Merkle – Hellman không tính toán số nghịch đảo

C. Hệ mã Merkle - Hellman có khóa kích thước nhỏ

**D. Hệ mã Merkle - H**ellman có của bạn là khóa siêu tăng

# Câu 48. Kết luận nào sai

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

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

C. Hệ mã hóa Merkle - Hellman có độ dài khóal

D. Hệ mã hóa ECC có độ dài khóa nhỏ hơn RSA

# Câu 49. Kết luận nào SAI :

A. Hệ mã hóa Elgamal dựa trên độ khó bài toán logarithm rời rạc

B. Hệ mã hóa Elgamal cho bản mã có kích thước lớn hơn bản rõ

C. Hệ mã hóa Elgamal cho bản mã có kích thước gấp đôi bản rõ

**D. Hệ mã hóa Elgama**l được ứng dụng rộng rãi

# Câu 50. Kết luận nào sai :

A. Hệ mã hóa Merkle - Hellman độ an toàn thấp

**B. Hệ mã hóa Merkle - Hellman có độ dài khóa nhỏ**

C. Hệ mã hóa Merkle Hellman không được ứng dụng rộng rãi

D. Hệ mã hóa Merkle - Hellman dựa trên độ khó bài toán đặt đồ vật vào thùng

# Câu 51. Kết luận nào sai với hệ mã khóa ECC :

**A. ECC dễ triển khai cà**i đặt

B. ECC có khóa là điểm trên đường cong Elliptic

C. ECC thực hiện các phép tính các điểm trên đường cong Elliptic

D. ECC có kích thước khóa nhỏ hơn RSA

# Câu 52. Kết luận nào sai :

A. Mật mã ECC được ứng dụng trong mô hình thỏa thuận

B. Hệ mã Merkle - Hellman không được ứng dụng rộng rãi trong mạng Internet

**C. Hệ mã Merkl**e – Hellman được ứng dụng rộng rãi trong chữ ký số

D. Hệ mã RSA được ứng dụng rộng rãi trong mạng Internet

# Câu 53. So với hệ mã khối , hệ mã mật khóa công khai có đặc tính gì :

A. Có khóa được công khai nên nội dung thông điệp dễ dàng bị giải mã

B. Giải thuật mã hóa công khai nền không an toàn

C. Không gian khóa nhỏ dễ bị thám mã

D**. Có tốc độ tính toán c**hậm

# Câu 54. Kết luận nào đúng :

**A. Mật mã ECC đượ**c ứng dụng trong chữ ký số

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

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

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

# Câu 55. Kết luận nào đúng :

A. PKC là viết tắt của cụm từ Private key cryptography

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

**C. Hệ mã PKC cho phép mã hóa khóa của hệ mã SKC**

D. PKC có giải thuật mã hóa và giải mã giống nhau

# Câu 56. Kết luận nào đúng :

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

**B. Hệ mã Merkle – Hellman an toàn kém so với RSA**

C. Hệ mã Merkle Hellman có khóa siêu tăng là khóa công khai

D. Hệ mã Merkle – Hellman an toàn cao

# Câu 57. Hàm băm có số lượng giá trị băm là 216 , nếu thám mã thử 512 văn bản khác nhau thì khả năng đụng độ :

A. 0.60

D. 0.98

**B. 0.86**

**C**. 0.30

# Câu 58. Hàm băm có số lượng giá trị băm là chuỗi 16 bit , nếu thám mã tìm khả năng đụng độ là 0.5 thì số lượng ít nhất văn bản khác nhau đem thử :

A. 5,385,596.70

B. 4.7096

**C**. **301.4144**

D. Không xác định

# Câu 58 Chữ ký số được hiểu là:

1. Một bản mã hóa khóa công khai –
2. Một phép kiểm tra trong đó 1 người có thể mã hóa và duy nhất 1 người có thể kiểm tra –
3. Một phép kiểm tra trong đó những người biết khóa mật mới có thể kiểm tra được –
4. Một phép kiểm tra trong đó nhiều người có thể kiểm tra nhưng chỉ một người được tạo chữ ký

# Câu 59 Sử dụng chữ ký số lên đại diện nội dung số: -

1. Tạo và xác nhận chữ ký nhanh chóng –
2. Sinh chữ ký số giống chữ ký tay –
3. Tăng tính bảo mật của nội dung số -
4. Tăng tính bảo mật của chữ ký số trên nội dung số

# Câu 60 Để ký lên một nội dung số có kích thước lớn, thực hiện:

1. Ký tại cuối văn bản –
2. Ký trên những phần quan trọng của nội dung số -
3. Ký trên đại diện của nội dung số -
4. Ký trên toàn nội dung số

# Câu 61 Chữ ký số RSA giống với hệ mã hóa RSA ở các điểm:

1. Sử dụng khóa bí mật và công khai, khóa bí mật được sử dụng để mã hóa và công khai để giải mã –
2. sử dụng khóa bí mật và công khai –
3. Sử dụng khóa bí mật và công khai theo thứ tự thực hiện giống nhau –
4. Sử dụng chung các thuật toán mã hóa và giải mã như nhau

# Câu 62 Chữ ký số RSA khác với hệ mã hóa RSA ở các điểm:

1. Sử dụng khóa bí mật và công khai nhưng 2 khóa được định nghĩa khác nhau hoàn toàn –
2. Sử dụng khóa bí mật và công khai hoàn toàn khác nhau –
3. Sử dụng chung cặp khóa nhưng thứ tự sử dụng khóa ngược nhau –
4. Trong chữ ký số vai trò của khóa bí mật và công khai không rõ ràng

# Câu 63 Hãy cho biết đặc điểm hàm băm:

1. Tạo giá trị đầu ra có độ dài không đối -
2. Tạo giá trị đầu ra có độ dài thay đổi –
3. Với cùng một giá trị đầu vào sẽ thu được các giá trị đầu ra khác nhau –
4. Mã hóa được bản rõ

# Câu 64 Kết luận nào đúng cho hàm băm:

1. Một hàm băm được qui ước một khóa bí mật và người dùng có thể thay đổi –
2. Một hàm băm được qui ước một khóa bí mật và người dùng không thể thay đổi –
3. Một hàm băm có số lượng đầu ra tương đương với số lượng đầu vào –
4. Giá trị băm là đại diện của đầu vào

# Câu 65 Kết luận nào đúng cho hàm băm:

1. Hàm băm mạnh là hàm băm phi đụng độ cao –
2. Hàm băm mạnh là hàm băm không có đụng độ -
3. Hàm băm mạnh là hàm băm đụng độ cao –
4. Hàm băm mạnh là hàm băm có tỷ số nén cao

# Câu 66 Cấu trúc của một hệ chữ ký số gồm:

1. Đại diện thông điệp và chữ ký –
2. Thông điệp và chữ ký –
3. Chữ ký trên thông điệp –
4. Chữ ký trên đại diện

# Câu 67 Chữ ký số tiêu chuẩn DSS sinh chữ ký độ dài:

1. 160 bit
2. 128 bit
3. 320 bit
4. 512 bit

# Câu 68 Kết luận nào đúng cho hàm băm MD-5:

1. Có 2^128 giá trị băm-
2. Có 128 giá trị băm –
3. Có 2\*128 giá trị băm –
4. Có 128^2 giá trị băm

# Câu 69 Kết luận nào đúng cho hàm băm SHA-I:

1. Có 160^2 giá trị băm –
2. Có2\*160 giá trị băm -
3. Có 160 giá trị băm –
4. Không gian băm độ dài 160 bit

# Câu 70 Một thông điệp có độ lớn là 1024 byte. Sau khi qua hàm băm lần 1 thu được kết quả 16 byte. Hỏi nếu qua 2 lần hàm băm liên tiếp ta thu được kết quả bao nhiêu:

1. 2^16 bit –
2. 16 byte –
3. 32 byte –
4. 2^32 bit

# Câu 71 Cơ sở của giải thuật chữ ký số tiêu chuẩn DSA:

1. Giải thuật chữ ký số Merkle — Hellman -
2. Giải thuật chữ ký số RSA -
3. Giải thuật chữ ký số ECC -
4. Giải thuật chữ ký số El-gamal

# Câu 72 Kết luận nào đúng cho hàm băm:

1. Phi đụng độ của MD-5 kém so với SHA-1 –
2. Phi đụng độ của MD-5 tương đương so với SHA-1 –
3. Phi đụng độ của MD-5 hơn so với SHA-1 –
4. MD-5 không có phi đụng độ

# Câu 73 Kết luận nào đúng cho hàm băm:

1. Phi đụng độ của MD-5 kém so với SHA-1 –
2. Phi đụng độ của MD-5 tương đương so với SHA-1 –
3. Hàm băm được dùng tạo tài khoản người dùng trên mạng –
4. Hàm băm chỉ được áp dụng trong chữ ký số

# Câu 74 Hệ mã RSA với n = 121, e = 31 hãy cho biết sinh mã chữ ký số từ bản rõ 7:

1. 7 –
2. 31 –
3. 100 –
4. Không xác định

# Câu 75 Hàm băm có số lượng giá trị băm là 10 bit, nếu thám mã thử 120 văn bản khác nhau thì khả năng đụng độ:0.99906

# Câu 76 Hàm băm có số lượng giá trị băm là 2^10, nếu thám mã tìm khả năng đụng độ là 0.5 thì số lượng ít nhất văn bản khác nhau đem thử:

1. 12 –
2. 38 –
3. 65 –
4. 84

# Câu 77 Hàm băm có không gian băm 10 bit, nếu thám mã tìm khả năng đụng độ là 0.4 thì số lượng ít nhất văn bản khác nhau đem thử:

1. 80 –
2. 19 –
3. 51 –
4. 33

# Câu 78 Hệ thống phân phối khóa Blom thực hiện:

1. Phân phối một hàm số riêng, người dùng tự xây dựng khóa dùng chung nhờ kết hợp hàm số riêngvới khóa công khai –
2. Phân phối từng cặp khóa bí mật một cho từng người dùng trong hệ thống –
3. Phân phối một khóa chung dùng cho cả nhóm người dùng –
4. Phân phối khóa bí mật và công khai của từng người dùng, khóa công khai được thông báo chung cho cả nhóm

# Câu 79 Nhãn thời gian trong giao thức Kerberos loại bỏ trường hợp thám mã:

1. Middle attach -?
2. Sử dụng khóa cũ –
3. Giả mạo danh tính –
4. Sử dụng khóa cũ và giả mạo danh tính

# Câu 80 Giao thức Diffie - Hellman sử dụng chứng chỉ loại trừ thám mã:

Gửi bản tin cũ –

Giải mã bản tin –

Sử dụng khóa cũ -?

Giả mạo danh tính

# Câu 81 Giao thức thỏa thuận khóa Diffie - Hellman sinh khóa phiên dựa trên:

1. Mật mã Des –
2. Mật mã Aes - ?
3. Mật mã trên đường cong Elliptic –
4. Mật mã Affine

# Câu 82 Giao thức phân phối khóa được hiểu là gì:

1. Có trung tâm phân phối khóa –
2. Có trung tâm phân phối khóa tham gia tạo, gửi khóa –
3. Không có trung tâm phân phối khóa –
4. Tối đa 2 thành viên

# Câu 83 Giao thức thỏa thuận khóa:

1. Hai bên thực hiện quản lý, trao đổi khóa–
2. Có bên thứ ba tham gia tạo, gửi khóa cho hai bên –
3. Có trung tâm thứ ba tham gia tạo, gửi khóa cho hai bên –
4. Tối đa 2 thành viên

Câu 84 Hệ thống phân phối khóa Blom trường hợp đơn giản chỉ an toàn cho nhóm có tối đa:

1. **2** –
2. 3 –
3. 4 –
4. 5

# Câu 85 Middle — Attack là hình thức thám mã:

1. Chủ động-
2. Thụ động -
3. Saochép bản tin –
4. Gửi bản tin cũ

# Câu 86 Kết luận nào đúng cho X.509:

1. Chuẩn chứng chỉ khóa công khai -
2. Chuân mã hóa –
3. Chuẩn chữ ký số -
4. Chuẩn mã hóa, chuẩn chữ ký số, và chuẩn chứng chỉ khóa công khai

# Câu 87Giao thức có người phân xử được hiểu:

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

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

C. 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

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

# Câu 88 Giao thức tự phân xử được hiếu:

1. Các bên thống nhất giao dịch trong từng bước. Sau khi thống nhất một bước thì mới chuyển sang bước tiếp theo
2. Các bên giao dịch có đủ thẩm quyền để xử lý các bên vi phạm giao thức
3. Trọng tài giám sát giao dịch, nếu thấy có dấu hiệu vi phạm sẽ thông báo cho cả 2 phía liên quan để tự sửa đổi quá trình
4. Các bên tự giám sát lẫn nhau, khi thấy có dấu hiệu vi phạm quá trình giao dịch sẽ bị dừng để xác minh

# Câu 89 Hình thức tấn công thụ động được hiểu:

1. Thám mã nghe lén các giao dịch, phát hiện đặc trưng và tung các giao dịch giả mạo nhằm thu lợi
2. Thám mã nghe lén các giao dịch, thu thập thông tin về các giao dịch
3. Thám mã nghe lén các giao dịch, khi phát hiện kẽ hở sẽ lợi dụng tấn công phiêu giao dịch
4. Thám mã nghe lén các giao dịch, tìm hiểu các qui tắc và sau đó tham gia sửa đổi giao dịch

# Câu 90 Hình thức tấn công chủđộng được hiểu:

1. Thám mã nghe lén các giao dịch, tìm hiểu các qui tắc và sau đó can thiệp các phiên giao dịch
2. Thám mã nghe lén các giao dịch, thu thập thông tin về các giao dịch
3. Thám mã nghe lén các giao dịch, khi phát hiện kẽ hở sẽ lợi dụng thay đổi nội dung phiên giao dịch đó
4. Thám mã nghe lén các giao dịch, khi phát hiện kẽ hở sẽ lợi dụng thay đổi nội dung phiên giao dịch đó

# Câu 91 Giải thuật Lehman có thể được áp dụng cho:

1. Giải mã hệ RSA –
2. Giảimã hệ El- gamal –
3. Giải mã hệ mã mã ECC –
4. Giải mã hệ Merkle - Hellman

# Câu 92 Định lý phần dư Trung hoa dùng cho:

1. Giải hệ mã AES –
2. Giảhệ mã DES –
3. Giải hệ mã El-Gamal –
4. **Giải hệ mã RSA**

# Câu 93 Giải thuật lũy thừa nhanh được áp dụng cho:

1. **Hệ mã khóa công khai và chữ ký số** -
2. Hệ mã khóa bí mật –
3. Hệ mã khóa công khai –
4. Hệ chữ ký số