Câu 16: Tìm nghịch đảo của 3 trong Z8:

1. 1
2. 2
3. 3
4. 4

Câu 17: Tìm tập giá trị của Z11:

1. 1,2,3,4,5,6,7,8,9,10,11
2. 0,1,2,3,4,5,6,7,8,9,10
3. 0,2,4,6,8,10
4. 0,1,3,5,7,9,11

Câu 18: Tập giá trị của Z26 có bao nhiêu phần tử khả nghịch:

1. 10
2. 11
3. 12
4. 13

Câu 19: Tìm nghịch đảo của 7 trong Z11:

1. 3
2. 5
3. 7
4. 8

Câu 20: a = 6 có phải là phần tử khả nghịch trong Z8

1. Không
2. Có

Câu 21: Tập Z9 có bao nhiêu phần tử khả nghịch:

1. 4
2. 5
3. 6
4. 7

Câu 22: Tìm tập giá trị khả nghịch của Z10:

1. 1,3,5,7,9
2. 1,3,7,9
3. 3,7,9
4. 5,7,9

Câu 23: Trong các số sau số nào đồng dư với 9 khi modulo với 5:

1. -10
2. -11
3. -12
4. -13

Câu 24: Trong các số sau số nào đồng dư với -132 khi modulo với 5:

1. -10
2. -11
3. -12
4. -13

Câu 25: Tập Z13 có bao nhiêu phần tử khả nghịch?

1. 10
2. 11
3. 12
4. 13

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

1. NM
2. YT
3. NH
4. HN

Câu 27: Hãy mã hóa thông điệp P = BA với khóa a = 5; b = 7 sử dụng hệ mã khóa Affine: MH a\*x+b mod26

Câu 28: Hãy mã hóa thông điệp P = XK với khóa a =7; b =4 sử dụng hệ mã hóa Affine: JW

Câu 29: Hãy mã hóa thông điệp P = BO với khóa a = 11; b=2 sử dụng hệ mã hóa Affine: NA

Câu 30: Hãy giải mã thông điệp P = BY với khóa a = 3; b = 4 sử dụng hệ mã hóa Affine:

1. YZ
2. ZY
3. RI
4. IR

Câu 31: Hãy giải mã thông điệp P = AR với khóa a = 5; b = 3 sử dụng hệ mã hóa Affine: PI

Câu 32: Hãy giải mã thông điệp P = VI với khóa a = 7, b = 2 sử dụng hệ mã hóa Affine: ZM

Câu 33: Hãy giải mã thông điệp P = MB với khóa a = 11; b = 5 sử dụng hệ mã hóa Affine: DC

Câu 34:Hãy mã hóa sử dụng hệ mã Vigenere với thông điệp = BAOMAT, khóa K = TDC

1. VDFQDU
2. UDQFDV
3. QDUVDI
4. VDUVDI

Câu 35. Hãy mã hóa sử dụng hệ mã Vigenere với thông điệp = VANODO, khóa K = MIN

HIAALB

Câu 36. Hãy mã hóa sử dụng hệ mã Vigenere với thông điệp = BIANSO, khóa K = BOM

CWMOGA

37. Hãy mã hóa sử dụng hệ mã Vigenere với thông điệp = MATRAN, khóa K = BOM

NOFSOZ

38. Hãy giải mã sử dụng hệ mã Vigenere với thông điệp = ODPMKG, khóa K = TDC

1. THEVAN
2. MATRAN
3. VANTHE
4. TRANMA

39. Hãy giải mã sử dụng hệ mã Vigenere với thông điệp = MZNGZN, khóa K = TIN

1. THEVAN
2. MATRAN
3. VANTHE
4. TRANRA

40. Hãy mã hóa thông điệp HE sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (11-8;3-7) có thể hiểu là ( ): LG

41. Hãy mã hóa thông điệp LP sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (11-8;3-7) có thể hiểu là ( ): KL

42. Hãy mã hóa thông điệp XY sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (11-8;3-7) có thể hiểu là ( ): NO

43. Hãy mã hóa thông điệp AN sử dụng hệ mã Hill với khóa K là ma trận 2x2 = (11-8;3-7) có thể hiểu là ( ):NN

44. Trong các khóa sau của mã Hill khóa nào không thể giải mã được:

1. ( )
2. ( )
3. ( )
4. ( )

45. Trong các khóa sau của Hill khóa nào có Det bằng 13:

1. ( )
2. ( )
3. ( )
4. ( )

46. Hãy tính khóa đảo của khóa k trong hệ mã Hill biết

1. K = [3][3];[2][5] có thể hiểu là k = ( )
2. ( )
3. ( )
4. ( )
5. Không xác định

47. Hãy tính khóa đảo của khóa k trong hệ mã Hill biết

k = [5][2];[2][1] [1][24];[24][5]

48. Hãy tính khóa đảo của khóa k trong hệ mã Hill biết

k = [18][19];[1][7] [11][11];[17][6]

49. Hãy tính khóa đảo của khóa k trong hệ mã Hill biết

k = [5][2];[2][1] [1][24];[24][5]

50. Hãy tính khóa đảo của khóa k trong hệ mã Hill biết

k = [3][4];[2][6] ko xác định

51. Tìm khóa K của Hill với Det(k) = 5 ???????????????

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

M^e mod n

a. 171

b. 117

c. 46

d. Không xác định

27. Trong hệ mã RSA với n = 35, e = 11 hãy cho biết kết quả mã hóa x = 7 ?

a. 28

b. 11

c. 82

d. không xác định

28. Trong hệ mã RSA với n = 55, e = 19 hãy cho biết kết quả mã hóa x = 9 ?

a. 94

b. 29

c. 49

d. không xác định

29. Trong hệ mã RSA với n = 221, e = 11 hãy cho biết kết quả mã hóa x = 16 ?

a. 120

b. 102

c. 12

d. không xác định

30. Trong hệ mã RSA với n = 221, e = 11 hãy cho biết kết quả mã hóa x = 18 ?

a. 155

b. 86

c. 68

d. không xác định

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

(p,q)=(11,13)=>phi n=120 =>d=103

a. 72

b. 27

c. 53

d. không xác định

32. Hệ mã RSA với n = 253, e = 13 hãy cho biết kết quả giải mã bản mã 16: ?

(p,q)=(11,23)=> phi n=220 => d=17

a. 71

b. 36

c. 234

d. Không xác định

33. Hệ mã RSA với n = 253, e = 13 hãy cho biết kết quả giải mã bản mã 12: ?

(p,q)=(11,23)=> phi n=220 => d=17 KQ: 78

34. Hệ mã RSA với n = 253, e = 13 hãy cho biết kết quả giải mã bản mã 18: ?

(p,q)=(11,23)=> phi n=220 => d=17 KQ: 215

35. Hệ mã RSA với n = 55, e = 13 hãy cho biết kết quả giải mã bản mã 17: ?

(p,q)=(5,11) => phi n=40 =>d=37 KQ: 52

36. Hệ mã RSA với n = 221, e = 23 hãy cho biết khóa mật(p,q,d):

(p,q)=(13,17) =>phi n=192 =>d= 167

a. (17, 13, 167)

b. (17, 13, 173)

c. (16, 12, 167)

d. (16, 12, 173)

37. Hệ mã RSA với n = 85, e = 33 hãy cho biết khóa mật(p,q,d):

(p,q)=(5,17)=>phi n=65 => d=33

a. (4, 16, 37)

b. (5, 17, 67)

c. (4, 16, 73)

d. (5, 17, 33)

38. Hệ mã RSA với n = 299, e = 35 hãy cho biết khóa mật(p,q,d) ?

(p,q)=(13,23) => phi n=264 => d= 83

=> Khóa mật (13,23,83)

39. Hệ mã RSA với n = 161, e = 17 hãy cho biết khóa mật(p,q,d) ?

(p,q)=(7,23) => phi n=132 => d=101 => Khóa mật: (7,23,101)

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

b. 0.86

c. 0.30

d. 0.98

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

59. Hàm băm có số lượng giá trị băm là chuỗi 9 bit, nếu thám mã tìm khả năng đụng độ là 0.4 thì số lượng ít nhất văn bản khác nhau đem thử:

a. 26.64

b. 3.5322

c. 64.537

d. 15.07

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

a. 25

b. 30

c. 54

d. Không xác định

61. 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:

a. 216 bit

b. 16 byte

c. 32 byte

d. 232 bit

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

a. 7

b. 31

c. 100

d. Không xác định

63. 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 ?

64. Hàm băm có số lượng giá trị băm là 210, nếu thám mã tìm khả năng đụng độ là 0.5 thì số lượng ít nhất văn bản khác nhau đem thử:

a. 12

b. 38

c. 65

d. 84

65. Cho 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:

a. 80

b. 19

c. 51

d. 33

Câu 17 Hãy mã hóa thông điệp P = GT với khóa a=3;b=5 của hệ mã Affine

1. AN b. XK c. GA d. AJ

Câu 12 Hãy mã hóa thông điệp AB theo hệ mã Hill với khóa K = (5-10;6-13)

1. VN b. GN c. VD d. KT

Câu 18 Hãy tính khóa đảo trong hệ mã Hill biết khóa K = [24][13];[21][17]

a. [19][1];[13][10] b. [19][13];[1][10] c. [19][10];[13][1] d. Không tính được khóa đảo.

Câu 19 Hãy mã hóa thông điệp = THITIN với hệ mã Vigenere có khóa K =TDC

1. MKKMLP
2. MKKMLX
3. MKMKLX
4. MKLKLP

Câu 26 Hệ mã RSA với n= 221, e=31 hãy cho biết khóa mật

1. (16, 12, 31)
2. (17, 13, 13)
3. (17, 13, 31)
4. (16, 12, 13)

Câu 27 Hệ mã RSA với n= 145, e = 9 hãy cho biết kết quả mã hóa bản rõ 15

1. 55
2. 20
3. 15
4. 25

Câu 12 Hãy mã hóa thông điệp P = FE với khóa a=7;b=8 sử dụng hệ mã hóa Affine

a. RK

b. XK

c. GA

d. AJ

Câu 13 Hãy mã hóa thông điệp DE theo hệ mã Hill với khóa K = (15-6;23-19)

a. HQ

b. GQ

c. VH

d. KH

Câu 14 Hãy mã hóa thông điệp VO theo hệ mã Hill với khóa K = (18-13;21-22)

a. HW

b. JQ

c. WJ

d. KH

Câu 16 Hãy mã hóa thông điệp = KHOACN với hệ mã Vigenere có khóa K =VMU

a. FTIVOR

b. FTAVOX

c. FTIVOH

d. TFAVOX

Câu 17 Hệ mã RSA với n = 143, e=7 hãy cho biết kết quả giải mã bản mã 15

a. 141

b. 143

c. 140

d. 142

Câu 17 Hệ mã RSA với n = 143, e=7 hãy cho biết kết quả giải mã bản mã 15

11-13-120 d= 103

a. 141

b. 143

c. 140

d. 142

Câu 19 Hệ mã RSA với n= 145, e = 9 hãy cho biết sinh mã chữ ký số từ bản rõ 15

5-29-112 –d=25

a. 59

b. 15

c. 95

d. 25

Câu 20 Hàm băm có số lượng giá trị băm là 210, nếu thám mã tìm khả năng đụng độ là 0.5 thì số lượng văn bản thử

a. 30

b. 38

c. 35

d. 45