Guiding Question for Security

1. _____ is the process or mechanism used for converting ordinary plain text into garbled non-human readable text & vice-versa.
   a) Malware Analysis
   b) Exploit writing
   c) Reverse engineering
   d) Cryptography

2. _____ is a means of storing & transmitting information in a specific format so that only those for whom it is planned can understand or process it.

   a) Malware Analysis
   b) Cryptography
   c) Reverse engineering
   d) Exploit writing

3. Cryptographic algorithms are based on mathematical algorithms where these algorithms use _____ for a secure transformation of data.

   a) **secret key**
   b) external programs
   c) add-ons
   d) secondary key

4. Cryptography can be divided into _____ types.

   a) 5
   b) 4
   c) 3
   d) 2

5. Data which is easily readable & understandable without any special algorithm or method is called _____

   a) cipher-text
   b) plain text
   c) raw text
   d) encrypted text

6. There are _____ types of cryptographic techniques used in general.

   a) 2

b) 3
c) 4
d) 5

7. Conventional cryptography is also known as _____ or symmetric-key encryption.

a) secret-key
b) public key
c) protected key
d) primary key

8. Data Encryption Standard is an example of a _____ cryptosystem.

a) Conventional
b) public key
c) hash key
d) asymmetric-key

9. _____ cryptography deals with traditional characters, i.e., letters & digits directly.

a) Modern
b) Classic
c) Asymmetric
d) Latest

10. _____ cryptography operates on binary-bit series and strings.

a) Modern
b) Classic
c) Traditional
d) Primitive

11. _____ cryptography has always been focussing on the concept of 'security through obscurity'.

a) Modern
b) Asymmetric
c) Classic
d) Latest

12. _____ cryptography is based on publicly known mathematically designed algorithms to encrypt the information.

a) Modern
b) Classic
c) Traditional
d) Primitive

13. _____ is a mono-alphabetic encryption code wherein each & every letter of plain-text is replaced by another letter in creating the cipher-text.

a) Polyalphabetic Cipher
b) Caesar Cipher
c) Playfair Cipher
d) Monoalphabetic Cipher

14. _____ is the concept that tells us about the replacement of every alphabet by another alphabet and the entire series gets 'shifted' by some fixed quantity.

a) Rolling Cipher
b) Shift Cipher
c) Playfair Cipher
d) Block Cipher

15. _____ is a cipher formed out of substitution where for a given key-value the cipher alphabet for every plain text remains fixed all through the encryption procedure.

a) Polyalphabetic Cipher
b) Caesar Cipher
c) Playfair Cipher
d) Monoalphabetic Cipher

16. In Playfair cipher, at first, a key table is produced. That key table is a 5 by 5 grid of alphabets which operates as the key to encrypt the plaintext.

a) Rolling Cipher
b) Shift Cipher
c) Playfair Cipher

d) Block Cipher

17. _____ employs a text string as a key that is implemented to do a series of shifts on the plain-text.

a) Vigenere Cipher
b) Shift Cipher
c) Playfair Cipher
d) Block Cipher

18. The _____ has piece of the keyword that has the same length as that of the plaintext.

a) Block Cipher
b) One-time pad
c) Hash functions
d) Vigenere Cipher

19. In _____ a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits.

a) Block Cipher
b) One-time pad
c) Hash functions
d) Vigenere Cipher

20. In _____ the plain-text is processed 1-bit at a time & a series of actions is carried out on it for generating one bit of cipher-text.

a) Block Cipher
b) One-time pad
c) Stream cipher
d) Vigenere Cipher

21. Which of the following is not an example of a block cipher?

a) DES

b) IDEA
c) Caesar cipher
d) Twofish

22. AES is at least 6-times faster than 3-DES.

a) True
b) False

23. _____ is another data hiding technique which can be used in conjunction with cryptography for the extra-secure method of protecting data.

a) Cryptography
b) Steganography
c) Tomography
d) Chorography

24. _____ is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

a) Cryptography
b) Tomography
c) Steganography
d) Chorography

25. A _____ tool permits security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

a) Cryptography
b) Tomography
c) Chorography
d) Steganography

26. AES uses a _____ bit block size and a key size of _____ bits.
a) 128; 128 or 256
b) 64; 128 or 192
c) 256; 128, 192, or 256
d) 128; 128, 192, or 256

27. Like DES, AES also uses Feistel Structure.
a) True
b) False

28. How many rounds does the AES-192 perform?
a) 10
b) 12
c) 14
d) 16

29. How many rounds does the AES-256 perform?
a) 10
b) 12
c) 14
d) 16

30. What is the expanded key size of AES-192?
a) 44 words
b) 60 words
c) 52 words
d) 36 words
View Answer

31. The 4×4 byte matrices in the AES algorithm are called
a) States
b) Words
c) Transitions
d) Permutations

32. In AES the 4×4 bytes matrix key is transformed into a keys of size _____
a) 32 words
b) 64 words
c) 54 words
d) 44 words

33. For the AES-128 algorithm there are _____ similar rounds and _____ round is different.
a) 2 pair of 5 similar rounds ; every alternate
b) 9 ; the last
c) 8 ; the first and last
d) 10 ; no

34. Which of the 4 operations are false for each round in the AES algorithm
i) Substitute Bytes
ii) Shift Columns
iii) Mix Rows
iv) XOR Round Key

a) i) only
b) ii) iii) and iv)
c) ii) and iii)
d) only iv)

35. There is an addition of round key before the start of the AES round algorithms.

a) True
b) False

36. Conversion of the Plaintext MANIPALINSTITUTE to a state matrix leads to

a)

M	A	N	I
P	A	L	I
N	S	T	I
T	U	T	E

b)

M	P	N	T
A	A	S	U
N	L	T	T
I	I	I	E

c)

M	A	I	L
N	P	I	T
A	N	I	U
S	T	T	E

d)

E	U	T	L
T	I	I	L
T	N	P	A
S	A	N	M

37. In AES, to make the s-box, we apply the transformation

b'_i = b_i XOR b_(i+4) XOR b(i+5) XOR b_(i+6) XOR b_(i+7) XOR c_i
What is c_i in this transformation?
a) c_i is the ith bit of byte c with value 0x63
b) c_i is the ith bit of byte c with value 0x25
c) c_i is the ith bit of byte c with value 0x8F
d) c_i is the ith bit of byte c with value 0x8A

38. The S-box value for byte stored in cell (6,D)

a) 0x3C
b) 0x7F
c) 0xFD
d) 0x4A

39. The inverse s-box permutation follows, b'_i = b_(i+2) XOR b(i+5) XOR b_(i+7) XOR d_i Here d_i is

a) d_i is the ith bit of a byte 'd' whose hex value is 0x15
b) d_i is the ith bit of a byte 'd' whose hex value is 0x05
c) d_i is the ith bit of a byte 'd' whose hex value is 0x25
d) d_i is the ith bit of a byte 'd' whose hex value is 0x51

40. The Inverse S-box value for byte stored in cell (3,3)\

a) 0xC3
b) 0x66
c) 0x1F
d) 0x9B

41. What is the Shifted Row transformation for the matrix bellow?

FE	72	2B	D7
6B	77	A4	6B
AD	01	F0	63
30	D7	AF	FE

a)

FE	72	2B	D7

6B	77	A4	6B
AD	01	F0	63
30	D7	AF	FE

b)

72	2B	D7	FE
A4	6B	6B	77
63	AD	01	F0
30	D7	AF	FE

c)

FE	72	2B	D7
77	A4	6B	6B
F0	63	AD	01
FE	30	D7	AF

d)

D7	FE	72	2B
A4	6B	6B	77
01	AD	63	F0
30	D7	AF	FE

42. How many computation rounds does the simplified AES consists of?

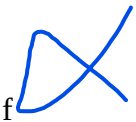
a) 5
b) 2
c) 8
d) 10

43. For an inputs key of size 128 bits constituting of all zeros, what is w(7) ?

a) {62 63 63 63}
b) {62 62 62 62}
c) {00 00 00 00}

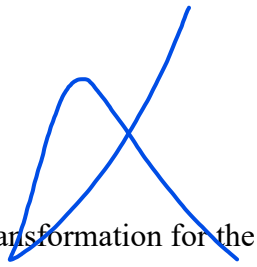
d) {63 63 63 62}

44. On comparing AES with DES, which of the following functions from DES does not have an equivalent AES function?
    a) f function
    b) permutation p
    c) swapping of halves
    d) xor of subkey with function f



45. On perform the Mix Columns transformation for the sequence of bytes “77 89 AB CD” we get output

    a) {01 55 EE 4A}
    b) {0A 44 EF 4A}
    c) {08 55 FF 3A}
    d) {09 44 DD 4A}



46. On perform the Mix Columns transformation for the sequence of bytes “67 89 AB CD” we get output

    a) {08 55 FF 18}
    b) {28 45 EF 08}
    c) {28 45 FF 18}
    d) {25 35 EF 08}

47. Is the following matrix the inverse matrix of the matrix used in the mix columns step?

    $x^3 + 1$ x
    x $x^3 + 1$

    a) Yes
    b) No
    c) Can’t say
    d) Insufficient Information

48. For the cipher text 0000 0111 0011 1000 and Key 0110 1111 0110 1011, apply the Simplified AES to obtain the plaintext. The plain text is

a) 0110 1001 0111 0001
b) 0110 1111 0110 1011
c) 0010 1001 0110 1011
d) 1111 0101 0111 1111

49. What is the block size in the Simplified AES algorithm?

a) 8 bits
b) 40 bits
c) 16 bits
d) 36 bits

50. What is the key size in the S-AES algorithm?

a) 16 bits
b) 32 bits
c) 24 bits
d) None of the mentioned

51. . How many step function do Round 1 and 2 each have in S-AES?

a) 4 and 3
b) Both 4
c) 1 and 4
d) 3 and 4

52. Which of the following are true

i) In the AES key expansion algorithm, the function g() operates on w i+3
ii) Perform a one-byte right circular rotation on the argument 4-byte word
iii) The round constant follows the formula RC[j] = RC[j − 1]

a) i) ii)
b) ii) only
c) i) only
d) All

53. How many round keys are generated in the AES algorithm?

a) 11
b) 10
c) 8
d) 12

54. How many modes of operation are there in in DES and AES?

a) 4
b) 3
c) 2
d) 5

55. Which one of the following modes of operation in DES is used for operating short data?

a) Cipher Feedback Mode (CFB)
b) Cipher Block chaining (CBC)
c) Electronic code book (ECB)
d) Output Feedback Modes (OFB)

56. Which of the following is false for ECB mode of operation

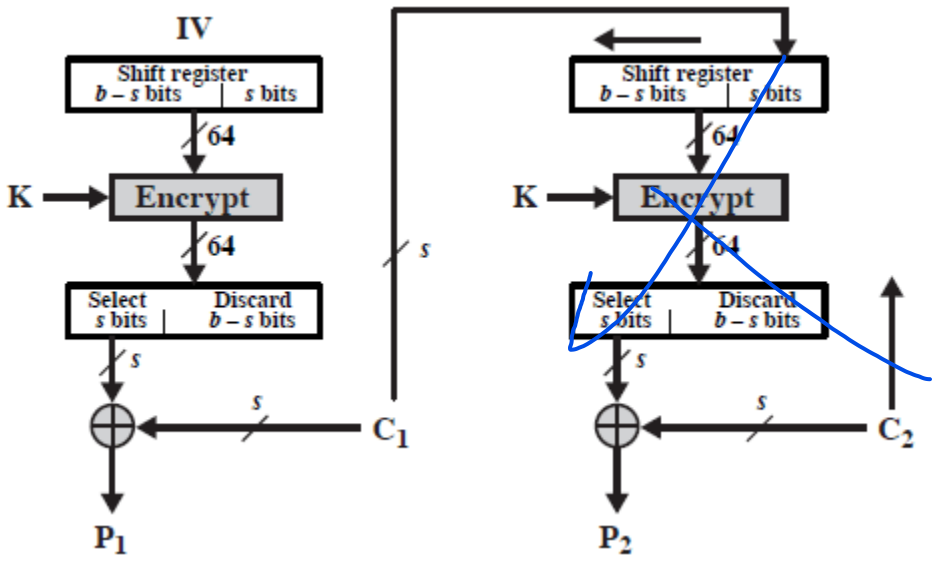
i) The Plain text is broken into blocks of size 128 bytes
ii) Blocks can be swapped, repeated, replaced without recipient noticing
iii) Good for short data
iv) Encryption of each block is done separately using a randomly generated key for each block

a) i) only
b) ii) and iii)
c) i) and iv)
d) i) ii) and iv)

57. There is a dependency on the previous ‘s’ bits in every stage in CFB mode. Here ‘s’ can range from ___

a) 8-16 bits
b) 8-32 bits
c) 4-16 bits
d) 8-48 bits

58. What is the fault in the above figure?



a) The output of the XOR is sent to the next stage
b) The “Encrypt” Box should be replaced by “Decrypt Box
c) b-s bits are selected for the XOR operation
d) No fault

59. DES follows

a) Hash Algorithm
b) Caesars Cipher
c) Feistel Cipher Structure
d) SP Networks

60. The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key

a) 12
b) 18
c) 9
d) 16

61. The DES algorithm has a key length of

a) 128 Bits
b) 32 Bits
c) 64 Bits
d) 16 Bits

62. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.

a) True
b) False

63. In the DES algorithm the round key is _____ bit and the Round Input is _____bits.
a) 48, 32
b) 64,32
c) 56, 24
d) 32, 32
View Answer
64. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
a) Scaling of the existing bits
b) Duplication of the existing bits
c) Addition of zeros
d) Addition of ones

65. The Initial Permutation table/matrix is of size
a) 16×8

b) 12×8
c) 8×8
d) 4×8

66. The number of unique substitution boxes in DES after the 48 bit XOR operation are
a) 8
b) 4
c) 6
d) 12
View Answer

67. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.
a) True
b) False

68. During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.
a) True
b) False

69. A preferable cryptographic algorithm should have a good avalanche effect.
a) True
b) False

70. The number of tests required to break the DES algorithm are
a) 2.8×10^{14}
b) 4.2×10^{9}
c) 1.84×10^{19}
d) 7.2×10^{16}

71. The number of tests required to break the Double DES algorithm are
a) 2112
b) 2111
c) 2128
d) 2119

72. How many keys does the Triple DES algorithm use?
a) 2
b) 3
c) 2 or 3
d) 3 or 4

73. Using Differential Crypt-analysis, the minimum computations required to decipher the DES algorithm is
a) 2^{56}
b) 2^{43}
c) 2^{55}

d) 2^{47}

74. Using Linear Crypt-analysis, the minimum computations required to decipher the DES algorithm is
    a) 2^{48}
    b) 2^{43}
    c) 2^{56}
    d) 2^{64}

75. What is the size of the key in the SDES algorithm?
    a) 24 bits
    b) 16 bits
    c) 20 bits
    d) 10 bits

76. Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K1?
    a) 10100100
    b) 01011011
    c) 01101000
    d) 10100111

77. Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K2?
    a) 10100111
    b) 01000011
    c) 00100100
    d) 01011010

78. The Ciphertext for the Plaintext 01110010, given that the keys K1 is 10100100 and K2 is 01000011 is
    a) 01110111
    b) 10010110
    c) 01010110
    d) 01000101

79. The Ciphertext for the Plaintext 11010101, given that the key is 0111010001 is
    a) 00010001
    b) 10110010
    c) 11010010
    d) 01110011

80. Assume input 10-bit key, K: 0010010111 for the SDES algorithm. What is K1?
    a) 00101111
    b) 01011011
    c) 01101000
    d) 10100111

81. The Plaintext for the Ciphertext 00001111, given that the key is 1111111111 is
a) 01100111
b) 00001010
c) 11111111
d) 01101101

82. Assume input 10-bit key, K: 0010010111 for the SDES algorithm. What is K2?
a) 11101010
b) 11011011
c) 01101000
d) 10101111

83. Cryptography offers a set of required security services. Which of the following is not among that 4 required security services?
a) Encryption
b) Message Authentication codes
c) Hash functions
d) Steganography

84. A cryptosystem is also termed as _____

a) secure system
b) cipher system
c) cipher-text
d) secure algorithm

85. _____ is the mathematical procedure or algorithm which produces a cipher-text for any specified plaintext.

a) Encryption Algorithm
b) Decryption Algorithm
c) Hashing Algorithm
d) Tuning Algorithm

86. _____ takes the plain text and the key as input for creating cipher-text.

a) Decryption Algorithm
b) Hashing Algorithm
c) Tuning Algorithm
d) Encryption Algorithm

87. _____ is a mathematical algorithm that produces a unique plain text for a given cipher text along with a decryption key.

a) Decryption Algorithm
b) Hashing Algorithm
c) Tuning Algorithm
d) Encryption Algorithm

88. A set of all probable decryption keys are collectively termed as _____

a) key-stack
b) key bunch
c) key space
d) key pack

89. Encryption-decryption in cryptosystem is done in _____ ways.

a) 4
b) 3
c) 5
d) 2

90. In _____ same keys are implemented for encrypting as well as decrypting the information.

a) Symmetric Key Encryption
b) Asymmetric Key Encryption
c) Asymmetric Key Decryption
d) Hash-based Key Encryption

91. In _____ 2 different keys are implemented for encrypting as well as decrypting that particular information.

a) Symmetric Key Encryption
b) Asymmetric Key Encryption
c) Asymmetric Key Decryption
d) Hash-based Key Encryption

92. A set of all probable decryption keys are collectively termed as key space.
a) True
b) False

93. _____ is the art & science of cracking the cipher-text without knowing the key.

a) Cracking
b) Cryptanalysis
c) Cryptography
d) Crypto-hacking

94. The process of disguising plaintext in such a way that its substance gets hidden (into what is known as cipher-text) is called _____

a) cryptanalysis
b) decryption
c) reverse engineering
d) encryption

95. The method of reverting the encrypted text which is known as cipher text to its original form i.e. plain text is known as _____

a) cryptanalysis
b) decryption
c) reverse engineering
d) encryption

96. Which of the following is not the primary objective of cryptography?
a) Confidentiality
b) Data Integrity
c) Data Redundancy
d) Authentication