1 **An algorithm in encryption is called _____.**

A Algorithm
B Procedure
C Cipher
D Module

Ans. **C**

2 **The information that gets transformed in encryption is _____.**

A Plain text
B Parallel text
C Encrypted text
D Decrypted text

Ans. **A**

3 **In brute force attack, on average half of all possible keys must be tried to achieve success.**

A True
B False

Ans. **A**

4 **A (n) _____ algorithm transforms ciphertext to plaintext.**

A Encryption
B Decryption
C Either (a) or (b)
D Neither (a) nor (b)

Ans. **B**

5 **The _____ is the message after transformation.**

A Ciphertext
B Plaintext
C Secret-text
D None of the above

Ans. **A**

6 **Which of the following is not a type of virus?**

A Boot sector
B Polymorphic
C Multipartite
D Trojans

Ans. **D**

7 **A computer _____ is a malicious code which self-replicates by copying itself to other programs.**

A Program
B Virus
C Application
D Worm

Ans. B

8 **_____ infects the master boot record and it is challenging and a complex task to remove this virus.**

A Boot Sector Virus
B Polymorphic
C Multipartite
D Trojans

Ans. A

9 **_____ infects the executable as well as the boot sectors.**

A Non-resident virus
B Boot Sector Virus
C Polymorphic Virus
D Multipartite Virus

Ans. D

10 **Trojan creators do not look for _____.**

A Deleting Data
B Protecting Data
C Modifying Data
D Copying Data

Ans. B

11 **Once activated _____ can enable _____to spy on the victim, steal their sensitive information & gain backdoor access to the system.**

A Virus, Cyber-Criminals
B Malware, Penetration Testers
C Trojans, Cyber-Criminals
D Virus, Penetration Testers

Ans. C

12 **During a DOS attack, the regular traffic on the target _____ will be either dawdling down or entirely interrupted.**

A Network
B System
C Website

D Router

Ans. C

13 The intent of a _____ is to overkill the targeted server's bandwidth and other resources of the target website.

A Phishing attack
B DoS attack
C Website attack
D MiTM attack

Ans. B

14 In _____ some cyber-criminals redirect the legitimate users to different phishing sites and web pages via emails, IMs, ads and spyware.

A URL Redirection
B DOS
C Phishing
D MiTM attack

Ans. C

15 Trojan creators do not look for _____.

A Credit card information
B Confidential data
C Important documents
D Securing systems with such programs

Ans. D

16 When one participant in a communication pretends to be someone else, it is called _____?

A Virus Attacks
B Fire Attacks
C Data Driven Attacks
D Masquerade

Ans. D

17 _____ is a term used to describe a phishing attack that is specifically aimed at wealthy, powerful, or prominent individuals. Generally CEO's and important celebrities.

A Message Authentication Code
B Steganography
C Whale phishing
D A cipher

Ans. C

18 Message_____means that the sender and the receiver expect privacy.

A Confidentiality

B Integrity
C Authentication
D None of the above

Ans.

19 Compromising confidential information comes under _____.

A Bug
B Threat
C Vulnerability
D Attack

Ans. B

20 When an attacker sends unsolicited communication, it is an example of_____.

A Spoofing
B Spamming
C Crackers
D Sniffers

Ans. A

21 Masquerading is _____.

A Attempting to hack a system through backdoors to an operating system or application.
B Pretending to be an authorized user
C Always done through IP spoofing
D Applying a subnet mask to an internal IP range

Ans. B

22 Integrity is protection of data from all of the following except _____.

A Unauthorized changes
B Accidental changes
C Data analysis
D Intentional manipulation

Ans. C

23 A security program cannot address which of the following business goals?

A Accuracy of information
B Change control
C User expectations
D Prevention of fraud

Ans. A

24 The absence of a fire-suppression system would be best characterized as_____.

A Exposure
B Threat
C Vulnerability

D Risk

Ans. C

25 Asymmetric key cryptography is used for all of the following except_____.

A Encryption of data
B Access control
C Nonrepudiation
D Steganography

Ans. D

26 Firewalls are to protect against_____.

A Virus Attacks
B Fire Attacks
C Data Driven Attacks
D Unauthorized Attacks

Ans. D

27 The first computer virus is_____.

A The famous
B HARLIE
C PARAM
D Creeper

Ans. D

28 _____ is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction.

A Network Security
B Database Security
C Information Security
D Physical Security

Ans. C

29 From the options below, which of them is not a vulnerability to information security?

A Without deleting data, disposal of storage media
B Latest patches and updates not done
C Flood
D Unchanged default password

Ans. C

30 Compromising confidential information comes under _____.

A Bug
B Threat
C Vulnerability
D Attack

Ans. **B**

31 **Possible threat to any information cannot be _____.**
- A Ignored
- B Protected
- C Transferred
- D Reduced

Ans. **A**

32 **A _____ can gain access illegally to a system if the system is not properly tested in scanning and gaining access phase.**
- A Security officer
- B Malicious hacker
- C Security auditor
- D Network analyst

Ans. **B**

33 **_____ 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

Ans. **D**

34 **When plain text is converted to unreadable format, it is termed as _____.**
- A Rotten text
- B Raw text
- C Cipher-text
- D Cipher

Ans. **C**

35 **_____ 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

Ans. **B**

36 **Cryptography can be divided into _____ types.**
- A 5
- B 2
- C 7
- D 3

Ans. **B**

37 **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

Ans. **B**

38 **Plain text are also called _____.**

A Encrypted text
B Clear-text
C Raw text
D Cipher-text

Ans. **C**

39 **There are _____ types of cryptographic techniques used in general.**

A 2
B 3
C 4
D 5

Ans. **B**

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

A Secret-key
B Public key
C Protected key
D Primary key

Ans. **A**

41 **Data Encryption Standard is an example of a _____ cryptosystem.**

A Conventional
B Public key
C Hash key
D Asymmetric-key

Ans. **A**

42 **_____ Cryptography deals with traditional characters, i.e., letters & digits directly.**

A Latest
B Asymmetric
C Classic
D Modern

Ans. **C**

43 **_____ Cryptography operates on binary-bit series and strings.**

A Modern
B Classic
C Traditional
D Primitive

Ans. **A**

44 **_____ 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

Ans. **B**

45 **_____ 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

Ans. **B**

46 **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

Ans. **C**

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

A Shift Cipher
B Block Cipher
C Playfair Cipher
D Vigenere Cipher

Ans. **D**

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

A One-time pad
B Hash functions
C Vigenere Cipher

D Block Cipher

Ans. A

49 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 Vigenere Cipher
B Block Cipher
C Stream cipher
D One-time pad

Ans. C

50 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 Hash functions
B Vigenere Cipher
C One-time pad
D Block Cipher

Ans. D

51 The procedure to add bits to the last block is termed as _____.

A Padding
B Hashing
C Tuning
D Decryption

Ans. A

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

A DES
B Caesar cipher
C Twofish
D IDEA

Ans. A

53 DES stands for _____.

A Device Encryption Standard
B Data Encrypted Standard
C Data Encryption Security
D Data Encryption Standard

Ans. D

54 _____ carries out all its calculations on bytes rather than using bits and is at least 6-times faster than 3-DES.

A Twofish
B IDEA
C DES

D AES

Ans. D

55 AES stands for _____.

A Active Encryption Standard
B Advanced Encrypted Standard
C Advanced Encryption Standard
D Advanced Encryption Security

Ans. C

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

A True
B False

Ans. A

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

A Chorography
B Tomography
C Steganography
D Cryptography

Ans. C

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

A Steganography
B Cryptography
C Chorography
D Tomography

Ans. A

59 Steganography follows the concept of security through obscurity.

A True
B False

Ans. A

60 The word _____is a combination of the Greek words 'steganos' which means "covered or concealed", and 'graphein' which means "writing".

A Tomography
B Chorography
C Steganography
D Cryptography

Ans. C

61 **Which of the following is not a steganography tool?**

A Steghide
B ReaperExploit
C Image steganography
D Xaio steganography

Ans. **B**

62 **Which of the following is not a steganography tool?**

A rSteg
B Crypture
C SteganographX Plus
D Burp Suite

Ans. **D**

63 **The main motive for using steganography is that hackers or other users can hide a secret message behind a _____.**

A Program file
B Special file
C Ordinary file
D Encrypted file

Ans. **C**

64 **People will normally think it as a normal/regular file and your secret message will pass on without any _____.**

A Cracking
B Encryption
C Suspicion
D Decryption

Ans. **C**

65 **By using _____ you can diminish the chance of data leakage.**

A Steganography
B Chorography
C Tomography
D Cryptography

Ans. **A**

66 **Which mode of operation has the worst "error propagation" among the following?**

A ECB
B CBC
C CBC
D OFB

Ans. **A**

67 **Which block mode limits the maximum throughput of the algorithm to the reciprocal of the time for one execution?**

A ECB
B CBC
C CTR
D OFB

Ans. **C**

68 **Which mode requires the implementation of only the encryption algorithm?**

A OFB
B CTR
C CBC
D ECB

Ans. **B**

69 **Which of the following modes of operation does not involve feedback?**

A OFB
B CTR
C CBC
D ECB

Ans. **A**

70 **Which of the following is a natural candidates for stream ciphers?**

A OFB
B ECB
C CBC
D CFB

Ans. **A**

71 **Which one of the following is not a cryptographic algorithm- JUPITER, Blowfish, RC6, Rijndael and Serpent?**

A Rijndael
B Serpent
C Blowfish
D JUPITER

Ans. **D**

72 **Which algorithm among- MARS, Blowfish, RC6, Rijndael and Serpent -was chosen as the AES algorithm?**

A Rijndael
B RC6
C Blowfish
D MARS

Ans. **D**

73 **How many rounds does the AES-192 perform?**
- A 16
- B 12
- C 14
- D 10

Ans. **B**

74 **What is the expanded key size of AES-192?**
- A 60 words
- B 32 words
- C 52 words
- D 44 words

Ans. **C**

75 **The 4×4 byte matrices in the AES algorithm are called_____.**
- A Permutations
- B Transitions
- C Words
- D States

Ans. **D**

76 **In AES the 4×4 bytes matrix key is transformed into a keys of size _____.**
- A 60 words
- B 32 words
- C 52 words
- D 44 words

Ans. **D**

77 **For the AES-128 algorithm there are _____ similar rounds and _____ round is different.**
- A 9 ; the last
- B 8 ; the first and last
- C 10 ; no
- D 2 pair of 5 similar rounds ; every alternate

Ans. **A**

78 **There is an addition of round key before the start of the AES round algorithms.**
- A True
- B False

Ans. **A**

79 **How many computation rounds does the simplified AES consists of?**
- A 10
- B 8
- C 2

D 5

Ans. C

80 On comparing AES with DES, which of the following functions from DES does not have an equivalent AES function?

A Permutation P
B Swapping of halves
C XOR of subkey with function f
D F function

Ans. B

81 What is the block size in the Simplified AES algorithm?

A 36 bits
B 16 bits
C 40 bits
D 8 bits

Ans. C

82 What is the key size in the S-AES algorithm?

A 32 bits
B 24 bits
C 16 bits
D None of the mentioned

Ans. C

83 Which of the following is a faulty S-AES step function?

A Mix Columns
B Add round key
C Byte substitution
D Shift rows

Ans. C

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

A 1 and 4
B 3 and 4
C Both 4
D 4 and 3

Ans. D

85 The inverse transformation matrix times the forward transformation matrix equals the identity matrix.

A True
B False

Ans. A

86 **How many round keys are generated in the AES algorithm?**

A 12
B 11
C 10
D 8

Ans. **B**

87 **DES follows_____.**

A SP Networks
B Feistel Cipher Structure
C Caesars Cipher
D Hash Algorithm

Ans. **B**

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

A 16
B 9
C 12
D 18

Ans. **A**

89 **The DES algorithm has a key length of _____.**

A 16 Bits
B 32 Bits
C 64 Bits
D 128 Bits

Ans. **C**

90 **In the DES algorithm the round key is _____ bit and the Round Input is _____bits.**

A 48, 32
B 32, 32
C 56, 24
D 64,32

Ans. **A**

91 **In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____.**

A Addition of ones
B Addition of zeros
C Duplication of the existing bits
D Scaling of the existing bits

Ans. **D**

92 **The Initial Permutation table/matrix is of size _____.**

A 4×8
B 8×8
C 12×8
D 16×8

Ans. **B**

93 **The number of unique substitution boxes in DES after the 48 bit XOR operation are___.**

A 4
B 8
C 12
D 16

Ans. **B**

94 **What is the number of possible 3 x 3 affine cipher transformations?**

A 840
B 168
C 1344
D 1024

Ans. **C**

95 **The S-Box is used to provide confusion, as it is dependent on the unknown key.**

A True
B False

Ans. **A**

96 **For p = 11 and q = 17 and choose e=7. Apply RSA algorithm where PT message=88 and thus find the CT.**

A 64
B 11
C 54
D 23

Ans. **B**

97 **For p = 11 and q = 17 and choose e=7. Apply RSA algorithm where Cipher message=11 and thus find the plain text.**

A 122
B 143
C 111
D 88

Ans. **D**

98 **In an RSA system the public key of a given user is e = 31, n = 3599. What is the private key of this user?**

A 1023
B 2432
C 2412
D 3031

Ans. D

99 Compute private key (d, p, q) given public key (e=23, n=233 ´ 241=56,153).

A 32432
B 19367
C 12543
D 35212

Ans. B

100 RSA is also a stream cipher like Merkel-Hellman.

A True
B False

Ans. A

101 In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'?

A p/q should give no remainder
B p and q should be prime
C p and q should be co-prime
D p and q should be divisible by Φ(n)

Ans. B

102 In RSA, Φ(n) = _____ in terms of p and q.

A (p+1)(q+1)
B (p-1)(q-1)
C (p)(q)
D (p)/(q)

Ans. B

103 For p = 11 and q = 19 and choose e=17. Apply RSA algorithm where message=5 and find the cipher text.

A C=23
B C=56
C C=92
D C=80

Ans. D

104 For p = 11 and q = 19 and choose d=17. Apply RSA algorithm where Cipher message=80 and thus find the plain text.

A 5
B 12

C 43
D 54
Ans. A

105 **Perform encryption on the following PT using RSA and find the CT. p = 3; q = 11; M = 5.**
A 18
B 12
C 26
D 28
Ans. C

106 **Perform encryption on the following PT using RSA and find the CT. p = 5; q = 11; M = 9.**
A 43
B 14
C 112
D 54
Ans. B

107 **Perform encryption on the following PT using RSA and find the CT. p = 7; q = 11; M = 8.**
A 58
B 34
C 123
D 57
Ans. D

108 **Perform encryption on the following PT using RSA and find the CT. p = 11; q = 13; M = 7.**
A 78
B 45
C 124
D 25
Ans. C

109 **Perform encryption on the following PT using RSA and find the CT. p = 17; q = 31; M = 2.**
A 128
B 124
C 127
D 167
Ans. A

110 **n = 35; e = 5; C = 10. What is the plaintext (use RSA)?**

A 2
B 4
C 5
D 6

Ans. C