Uka Tarsadia University (Diwaliba Polytechnic)
Diploma in Computer Engineering
Objective Type Questions (Information Security- 020040608)

Unit 1: Introduction to Information Security

1. 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
2. Which of the following is not the primary objective of cryptography?
   a) Confidentiality
   b) Data Integrity
   c) Data Redundancy
   d) Authentication
3. Which of the following is a principle of data security?
   a) Data Confidentiality
   b) Data Integrity
   c) Authentication
   d) All of the above
4. Which of the following attack is a passive attack?
   a) Masquerade
   b) Modification of message
   c) Denial of service
   d) Traffic analysis
5. Which of the following options correctly defines the Brute force attack?
   a) Brutally forcing the user to share the useful information like pins and passwords.
   b) Trying every possible key to decrypt the message.
   c) One entity pretends to be some other entity.

d) The message or information is modified before sending it to the receiver.

6. "A key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text." Which of the following is capable of becoming a key in a cryptographic algorithm?
   a) An integer values
   b) A square matrix
   c) An array of characters (i.e. a string)
   d) All of the above
7. In general how many key elements constitute the entire security structure?
   a) 1 b) 2 c) 3 d) 4
8. According to the CIA, which of the below-mentioned element is not considered in the triad?
   a) Confidentiality
   b) Integrity
   c) Authenticity
   d) Availability
9. This is the model designed for guiding the policies of Information Security within a company, firm or organization. What is "this" referred to here?
   a) Confidentiality
   b) Non-repudiation
   c) CIA
   d) Authenticity
10. When you use the word _____ it means you are protecting your data from getting disclosed.
   a) Confidentiality
   b) Integrity
   c) Authentication
   d) Availability
11. _____ means the protection of data from modification by unknown users.
   a) Confidentiality
   b) Integrity

c) Authentication

d) Non-repudiation

12. When integrity is lacking in a security system, _____ occurs.

a) Database hacking

b) Data deletion

c) Data tampering

d) Data leakage

13. _____ of information means, only authorized users are capable of accessing the information.

a) Hiding

b) Integrity

c) Non-repudiation

d) Availability

14. Why these 3 elements (confidentiality, integrity, availability) are considered fundamental?

a) They help understanding hacking better

b) They help to understand the cyber-crime better

c) They help understanding security and its components better

d) None of the above

15. This helps in identifying the origin of information and authentic user. This referred to here as _____.

a) Confidentiality

b) Integrity

c) Authenticity

d) Availability

16. Data _____ is used to ensure confidentiality.

a) Encryption

b) Locking

c) Deleting

d) Backup

17. Which of these is not a proper method of maintaining confidentiality?
    a) Biometric verification
    b) ID and password based verification
    c) 2-factor authentication
    d) Switching off the phone
18. Data integrity gets compromised when _____ is not done properly.
    a) Data hiding
    b) Access control
    c) Network management
    d) None of the above
19. One common way to maintain data availability is _____
    a) Data clustering
    b) Data backup
    c) Data recovery
    d) Data Altering
20. _____ 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
21. From the options below, which of them is not a threat to information security?
    a) Disaster
    b) Eavesdropping
    c) Information leakage
    d) Unchanged password
22. Compromising confidential information comes under _____
    a) Bug
    b) Threat
    c) Vulnerability
    d) None of the above

23. Lack of access control policy is a _____

a) Data backup

b) Security

c) Vulnerability

d) None of the above

24. Which is not an objective of network security?

a) Integrity

b) Authentication

c) Access control

d) Lock

25. Which of the following security feature controls who can access resources in the OS?

a) Authentication

b) Identification

c) Validation

d) Access control

26. The information that gets transformed in encryption is _____

a) Plain text

b) Parallel text

c) Encrypted text

d) Decrypted text

27. The process of transforming plain text into unreadable text.

a) Decryption

b) Encryption

c) Network Security

d) Information Hiding

28. A process of making the encrypted text readable again is _____.

a) Decryption

b) Encryption

c) Network Security

d) Information Hiding

29. A unique piece of information (readable) that is used in encryption is _____.
    a) Cipher text
    b) Plain Text
    c) Key
    d) None of the above
30. A cryptosystem is also termed as _____.
    a) secure text
    b) cipher system
    c) cipher text
    d) secure algorithm
31. Study of creating and using encryption and decryption techniques is called
    a) Cipher
    b) Cryptography
    c) Encryption
    d) Decryption
32. 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) Cryptanalysis
33. _____ assures that individuals control what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
    a) Availability
    b) System Integrity
    c) Confidentiality
    d) Data Integrity
34. _____ assures that a system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system.
    a) System Integrity
    b) Data Integrity

c) Availability
d) Confidentiality

35. A loss of _____ is the unauthorized disclosure of information.
    a) confidentiality
    b) integrity
    c) authenticity
    d) availability
36. A _____ is an attempt to learn or make use of information from the system that does not affect system resources.
    a) passive attack
    b) inside attack
    c) outside attack
    d) active attack
37. Masquerade is an example of _____ attack.
    a) unauthorized disclosure
    b) active
    c) passive
    d) none of the above
38. An example of _____ is an attempt by an unauthorized user to gain access to a system by posing as an authorized user.
    a) masquerade
    b) interception
    c) repudiation
    d) inference
39. The _____ prevents the normal use or management of communications facilities.
    a) passive attack
    b) traffic encryption
    c) denial of service
    d) masquerade

40. A _____ is any action that compromises the security of information owned by an organization.

a) security mechanism
b) Security attack
c) security policy
d) Security service

41. The assurance that data received are exactly as sent by an authorized entity is _____.

a) authentication
b) data confidentiality
c) access control
d) data integrity

42. 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) none of the above

43. _____ 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

44. _____ 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

45. The “A” in the CIA triad stands for _____.

a) Availability

b) Access control

c) Authentication

d) None of the above

46. _____ 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

47. State true or false: Availability assures that systems works promptly and service is not denied to authorize users.

48._____ is the art and science of cracking the cipher-text without knowing the key.

a) Cracking

b) Cryptanalysis

c) Cryptography

d) Crypto-hacking

49. The OSI security architecture focuses on security attacks, _____, and services.

a) Mechanism

b) policy

c) technique

d) none of the above

50. Data which is easily readable and understandable without any special algorithm or method is called _____

a) cipher-text

b) plain text

c) raw text

d) encrypted text

Unit 2: Encryption Techniques

1. Use Caesar's Cipher to decipher the following using key=3.
   HQFUBSWHG WHAW
   a) ABANDONED LOCK
   b) ENCRYPTED TEXT
   c) ABANDONED TEXT
   d) ENCRYPTED LOCK
2. State true or false: Symmetric encryption is used primarily to provide confidentiality.
3. Caesar Cipher is an example of
   a) Polyalphabetic Cipher
   b) Monoalphabetic Cipher
   c) Multialphabetic Cipher
   d) Bi-alphabetic Cipher
4. State true or false: The secret key is input to the encryption algorithm.
5. Which is the largest disadvantage of the symmetric encryption?
   a) More complex and therefore more time-consuming calculations.
   b) Problem of the secure transmission of the Secret Key.
   c) More secure encryption function.
   d) None of the above
6. In cryptography, the order of the letters in a message is rearranged by _____
   a) transposition ciphers
   b) substitution ciphers
   c) both transposition ciphers and substitution ciphers
   d) quadratic ciphers
7. If the sender and receiver use same key, the system is referred to as _____ cipher system.
   a) Symmetric
   b) asymmetric
   c) public key cryptosystem
   d) None of the above

8. A symmetric encryption scheme has ___ingredients.
    a) 5
    b) 6
    c) 7
    d) 8
9. State true or false: Public-key cryptography is asymmetric.
10. Which one of the following is correct equation to find cipher text using caeser cipher?
    a) C = (p + Key) mod 26
    b) C = (p * Key) mod 26
    c) C = (p + Key) mod 36
    d) C = (p + Key) mod 6
11. Which one of the following algorithm is based on 5x5 matrix of letters?
    a) Playfair cipher
    b) Polyalphabetic cipher
    c) Railfence cipher
    d) Caeser cipher
12. The plain text “balloon” can be written in playfair cipher as
    a) Ba ll oo nx
    b) Ba ll oo n
    c) Ba lx lo on
    d) None of the above
13. The plain text “following” can be written in playfair cipher as
    a) Fo lx lo wi ng
    b) Fo ll ow in g
    c) Fo ll ow in gx
    d) None of the above
14. The plain text “wrapping” can be written in playfair cipher as
    a) Wr ap pi ng
    b) Wr ax pp in g
    c) Wr ax pp in gx
    d) None of the above

15. The plain text “bitter” can be written in playfair cipher as
    a) Bi tt er
    b) Bi tx te rx
    c) Bi tx te r
    d) None of the above
16. The plain text “letter” can be written in playfair cipher as
    a) Le tt er
    b) Le tx te rx
    c) Le tx tx er
    d) None of the above
17. The plain text “three” can be written in playfair cipher as
    a) Th re e
    b) Th re ex
    c) Th rx ee
    d) None of the above
18. The plain text “access” can be written in playfair cipher as
    a) Ac ce ss
    b) Ac ce sx sx
    c) Ac cx es sx
    d) None of the above
19. The plain text “enroll” can be written in playfair cipher as
    a) En ro lx lx
    b) En ro ll
    c) En rx ol lx
    d) None of the above
20. Which of the following algorithm uses matrix multiplication to obtain cipher text?
    a) Hill cipher
    b) Columnar
    c) Caeser cipher
    d) Playfair cipher
21. Polyalphabetic cipher is also known as _____ cipher

a) Vigenere cipher
b) Hill cipher
c) Playfair cipher
d) Columnar

22. The scheme in which each new message requires a new key of the same length as the new message, is called _____.
    a) Steganography
    b) One time pad
    c) Hill cipher
    d) None of the above
23. Which one of the following is major drawback of one time pad?
    a) Problem of making large number of random keys
    b) Problem of key distribution and protection
    c) Both a) and b)
    d) None of the above
24. _____ technique performs permutations on the plain text letters.
    a) Transposition
    b) Substitution
    c) Both a) and b)
    d) None of the above
25. Which of the following is not a transposition technique?
    a) Railfence
    b) Columnar
    c) Hill cipher
    d) All of the mentioned
26. Which of the following is a transposition technique?
    a) Columnar
    b) Playfair cipher
    c) Caeser cipher
    d) All of the mentioned
27. _____ hides the existence of the actual message.

a) Steganography
b) Security
c) Rotor machine
d) None of the above

28. _____ is the technique in which selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
    a) Invisible ink
    b) Character marking
    c) Pin punctures
    d) None of the above
29. _____ is the technique in which a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
    a) Invisible ink
    b) Character marking
    c) Pin punctures
    d) None of the above
30. _____ is the technique in which small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.
    a) Invisible ink
    b) Character marking
    c) Pin punctures
    d) None of the above
31. _____ is the technique in which the results of typing with the correction tape are visible only under a strong light.
    a) Invisible ink
    b) Character marking
    c) Typewritter correction ribbon
    d) None of the above
32. Use Caesar's Cipher to encipher the following using key=2.
    hello

a) jgnnq

b) ifmmp

c) khoor

d) None of the above

33. Use Caesar's Cipher to encipher the following using key=4.

world

a) xpsme

b) asvph

c) yqtnf

d) None of the above

34. Use Caesar's Cipher to encipher the following using key=3.

corona

a) dpspob

b) eqtqpc

c) frurqd

d) gsvsre

35. Use Caesar's Cipher to encipher the following using key=5.

covid

a) dpwje

b) eqxkf

c) frylg

d) htani

36. Use Caesar's Cipher to encipher the following using key=1.

better

a) cfuufs

b) dgvvgt

c) ehwwhu

d) fixxiv

37. Use Caesar's Cipher to encipher the following using key=6.

shelter

a) ynkrzkx

b) zolsaly

c) apmtbmz

d) bqnucna

38. Use Caesar's Cipher to encipher the following using key=2.

color

a) eqnqt

b) froru

c) gspsv

d) htqtw

39. Use Caesar's Cipher to encipher the following using key=10.

hope

a) ryzo

b) ipqf

c) gnod

d) fmnc

40. Which of the following is fed as an input to the encryption algorithm?

a) Plain text

b) Secret key

c) Both a) and b)

d) None of the above

41. Which of the following function does an encryption algorithm perform?

a) Substitution

b) Transposition

c) Both a) and b)

d) None of the above

42. Which of the following is an independent dimension of a cryptographic system?

a) The type of operations used for transforming plaintext to ciphertext.

b) The number of keys used.

c) The way in which the plaintext is processed.

d) All of the above

43. How many general approaches are there to attack a conventional encryption scheme?

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

44. Use Caesar's Cipher to decipher the following using key=3.
PHHW PH DIWHU WKH WRJD SDUWB
a) meet me after the toga party
b) meet me after the yoga party
c) meet me after our toga party
d) meet me before the toga party

45. Which of the following statement is correct for playfair cipher?
a) The letters I and J count as one letter.
b) Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
c) Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x.
d) All of the above

46. Which of the following is the correct equation for hill cipher?
a) C = PK mod 26
b) C = P+K mod 26
c) C = PK mod 6
d) C = PK mod 25

47. Find out the cipher text for the plain text "attack postponed until two am" using columnar technique and key = 4312567.
a) TTNAAPTMTSUOAODWCOIKNLPET
b) TNTAAPTMTSUOAODWCOIKNLPET
c) TTNAPATMTSUOAODWCOIKNLPET
d) TTNAATPMTSUOAODWCOIKNLPET

48. The sequence of first letters of each word of the overall message spells out the hidden message. This is an example of _____.
a) Encryption

b) Steganography
c) One time pad
d) None of the above

49. Which of the following letter has the highest occurrence frequency in English text?
    a) X
    b) Z
    c) E
    d) Q
50. State true or false: Stream ciphers process one bit at a time.
51. State true or false: Symmetric encryption is also known as conventional encryption.
52. In single-key encryption, how many numbers of key are used?
    a) 1
    b) 2
    c) 3
    d) 4
53. _____ means original intelligible message.
    a) Plaintext
    b) Ciphertext
    c) Private key
    d) Encrypted message
54. _____means encrypted message.
    a) Plaintext
    b) Ciphertext
    c) Private key
    d) None
55. State true or false: The key is a value dependent of the plaintext and the algorithm.
56. What is the input of decryption algorithm?
    a) Ciphertext
    b) Secret Key
    c) Both
    d) None

57. State true or false: Decryption means encryption algorithm run in reverse.
58. In conventional encryption two different keys produces _____.
    a) Same output
    b) Different output
    c) Both
    d) None
59. Let the plaintext be X, key be K and the ciphertext produced by Y, then encryption is performed as _____.
    a) X= E(K,Y)
    b) Y=E(K,X)
    c) Y=E(X,K)
    d) X= E(Y,K)
60. How many letters are encrypted at a time in playfair cipher?
    a) 2
    b) 4
    c) 1
    d) 3
61. How many number of alternative keys are possible in monoalphabetic substitution cipher?
    a) 26
    b) 25
    c) 26!
    d) 25!
62. If cipher text = DIFVE, key = 4 than find plaintext using caeser cipher.
    a) ZEBRA
    b) HMJZI
    c) PLAIN
    d) GTYU
63. If cipher text = EXXEGO, key = 4 than find plaintext using caeser cipher.
    a) Attack
    b) Cipher

c) String

d) Letter

64. If the opponent is interested in only this particular message, then the focus of the effort is_____.

a) to recover message from ciphertext

b) to recover key value

c) to recover ciphertext

d) None

65. If opponent is interested in being able to read future messages as well, in which case an attempt is made_____.

a) to recover message from ciphertext

b) to recover key value

c) to recover ciphertext

d) None

66. In_____, each element in the plaintext is mapped into another element.

a) Transposition

b) Substitution

c) Both a) and b)

d) None of the above

67. In_____, the attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

a) Brute-force attack

b) Traffic analysis attack

c) DoS attack

d) Replay attack

68. Which one of the following is correct equation to find plian text using caeser cipher?

a) P = (C - Key) mod 26

b) P = (C* Key) mod 26

c) P = (C+ Key) mod 36

d) P = (C - Key)

69. In caeser cipher,b applying Brute Force attack there are only _____possible keys.

a) 26
b) 26!
c) 25
d) 25!

70. _____works on binary data (bits) rather than letters.
    a) Vernam cipher
    b) Auto key system
    c) Vigenère cipher
    d) None
71. State true or false: In Vigenère cipher, to encrypt a message, a key is needed that is as long as the message.
72. In which encryption involves writing plaintext letters diagonally over a number of rows, then read off cipher row by row?
    a) Rail fence technique
    b) Transposition technique
    c) Both
    d) None
73. If plaintext= come home, find cipher text using rail fence method where key = 2.
    a) CMHMOEOE
    b) CEOMMEHO
    c) EOEOMHMC
    d) EOCMCMHE
74. If plaintext= meet me, find cipher text using rail fence method where key = 2.
    a) MEMETE
    b) MEEMTE
    c) TEETME
    d) METEME
75. State true or false: Symmetric key encryption is faster than asymmetric key.
76. State true or false: Plaiyfair cipher is transposition technique.
77. In vernam cipher, ciphertext is generated by performing _____.

a) the bitwise XOR of the plaintext and the key

b) the bitwise OR of the plaintext and the key

c) the bitwise NOR of the plaintext and the key

d) None

78. In which technique Vigenere table is used to generate ciphertext?

a) Monoalphabetic

b) Polyalphabetic

c) Playfair

d) Caeser cipher

79. If plaintext= Example, find cipher text using rail fence method where key = 3142.

a) XL MX EP AE

b) EP XL AE ME

c) XL AE MX EP

d) EP ME XL AE

80. If plaintext=Security, find cipher text using rail fence method where key = 3142.

a) EI UY SR CT

b) EI SR CT UY

c) UY CT SR EI

d) UY SR EI CT

Unit 3: Block cipher principles

1. Which cipher encrypts a data stream one bit or one byte at a time?

   a) Stream cipher
   b) Block cipher
   c) A and b both
   d) None of above

2. In which cipher a block of plaintext is treated as a whole and used to produce a cipher text block of equal length?

   a) Stream cipher
   b) Block cipher
   c) A and b both
   d) None of above

3. Which is the example of stream cipher?

   a) DES
   b) Vigenere cipher
   c) A and b both
   d) None of above

4. Which is the example of block cipher?

   a) DES
   b) Vigenere cipher
   c) A and b both
   d) None of above

5. In _____, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext.

   a) Diffusion
   b) Confusion
   c) Stream cipher

d) Block cipher

6. In _____seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible.

a) Diffusion
b) Confusion
c) Stream cipher
d) Block cipher

7. DES follows_____.

a) Hash Algorithm

b) Caesars Cipher

c) Feistel Cipher Structure

d) SP Networks

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

a) 12

b) 18

c) 9

d) 16

9. The DES algorithm has a key length of

a) 128 Bits

b) 32 Bits

c) 64 Bits

d) 16 Bits

10. What is the size of the key in the SDES algorithm?

a) 24 bits

b) 16 bits

c) 20 bits

d) 10 bits

11. What is the size of the plaintext in the SDES algorithm?

a) 24 bits

b) 16 bits

c) 20 bits

d) 8 bits

12. How many rounds used in SDES algorithm?

a) 2
b) 3
c) 4
d) 16

13. SDES is _____ cipher.

a) Symmetric
b) Asymmetric
c) A and b both
d) None of above

14. “A small change in either the plaintext or the key should produce a significant change in the ciphertext” this property is known as _____.

a) The Avalanche effect
b) The Avalanche update
c) The significant effect
d) None of above

15. In which attack, the attacker exploits the fact that any algorithm takes different amount of time for different data?

a) Brute force attack
b) Ciphertext attack
c) Timing attack
d) None of above

16. Assume input 10-bit key, K: 1010000010, P10 = 1000001100, P8 = 0000111000 for the SDES algorithm. What is K1?

a) 10100100

b) 01011011

c) 01101000

d) 10100111

17. Which are the parameters on which feistel network depends?

a) Block size
b) Key size
c) Number of rounds
d) All of above

18. Which are the strength of DES algorithm?

a) Use of 56 bit key
b) The nature of DES algorithm
c) A and b both
d) None of above

19. How many number of s-box are used in DES algorithm?

a) 7
b) 8
c) 10
d) 12

20. What is the input to the S-box in DES algorithm?

a) 4 bits
b) 2 bits
c) 5 bits
d) 6 bits

21. What is the output of the S-box in DES algorithm?

a) 4 bits
b) 2 bits
c) 5 bits
d) 6 bits

22. _____ is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream.

a) S-box
b) P-box
c) T-box
d) none of the above

23. DES is _____ method adopted by the U.S. government.

a) symmetric-key

b) asymmetric-key

c) Both (a) or (b)

d) None of above

24. What values we get after applying one round shift circulate (LS-1) on each half of the bits? Where,

Left half: 10000, Right half: 01100

a) Left half: 00100, Right half: 00011
b) Left half: 00010, Right half: 10001

c) Left half: 00001, Right half: 11000

d) Left half: 00010, Right half: 00011

25. What values we get after applying one round shift circulate (LS-2) on each half of the bits? Where,

Left half: 10101, Right half: 10001

a) Left half: 11100, Right half: 00011

b) Left half: 01011, Right half: 00011

c) Left half: 01101, Right half: 10001

d) Left half: 11010, Right half: 00011

26. The _____ is obtained from plaintext by iterating a function F over some number of rounds.

a) Key value

b) Ciphertext

c) Original message

d) None of above

27. In block cipher, fixed-length groups of bits is called _____

a) blocks

b) Group

c) Byte

d) None of above

28. In a block cipher, the function F which depends on the output of the previous round and the key K is known as a _____

a) Round function.

b) Merry-go-round.

c) Ring function.

d) Round algorithm

29. Which of the following encryption algorithms is based on the Fiestal struture?

a) Advanced Encryption Standard

b) RSA public key cryptographic algorithm

c) Data Encryption Standard

d) RC4

30. SDES stands for_____.

a) Simple Data Encryption Standard
b) Simplified Data Encryption Standard
c) Secret Data Encryption Standard
d) Structure Data Encryption Standard

31. If value of master key is 1010000010 and P10 = 3 5 2 7 4 10 1 9 8 6 then what is value generated after permutation?

a) 0100100010
b) 1000001100
c) 1000101100
d) 1000001110

32. If value of master key is 0111010001 and P10 = 3 5 2 7 4 10 1 9 8 6 then what is value generated after permutation?

a) 1001100010
b) 1000100110
c) 1010110001
d) 1010010001

33. If value of master key is 1011000110 and P10 = 3 5 2 7 4 10 1 9 8 6 then what is value generated after permutation?

a) 1000101110
b) 1000111111
c) 1100110011
d) 1100111110

34. In feistel cipher _____ key is used for each round.

a) Same
b) Separate
c) Encrypted
d) None of above

35. How many keys are generated using SDES key generation algorithm?

a) 2
b) 3
c) 8
d) 16

36. SDES key generation algorithm a ____bit key as input and produces an ____bit block of ciphertext as output.

a) 8, 10
b) 8, 8
c) 10, 8
d) 10 ,10

37. IP stands for _____.

a) Initial Partition
b) Initial Permutation
c) Inverse Permutation
d) Inverse Partition

38. What values we get after applying two round shift circulate (LS-2) on each half of the bits? Where,

Left half: 00001, Right half: 11000

a) Left half: 00100, Right half: 00011
b) Left half: 00010, Right half: 10001
c) Left half: 00001, Right half: 10001

d) Left half: 00010, Right half: 00011

39. What values we get after applying two round shift circulate (LS-2) on each half of the bits? Where,

Left half: 00011, Right half: 11101

e) Left half: 01100, Right half: 10111
f) Left half: 00110, Right half: 11011
g) Left half: 01100, Right half: 11011
h) Left half: 11000, Right half: 10111

40. What values we get after applying two round shift circulate (LS-2) on each half of the bits? Where,

Left half: 01011, Right half: 00011

a) Left half: 01101, Right half: 01100
b) Left half: 10110, Right half: 00110
c) Left half: 01101, Right half: 00110
d) Left half: 10110, Right half: 01100

41. What is the output of 00111100 $\oplus$ 10100100?

a) 00100100
b) 10011000
c) 00100101
d) 10001001

42. What is the output of 00010100 $\oplus$ 10100100?

a) 10010000
b) 10110001
c) 10110000
d) 100010001

43. If we have string of 4 bit = 0110, what is the value we get after applying expansion/permutation (E/P)? where,

E/P							
4	1	2	3	2	3	4	1

a) 00101110
b) 00101001
c) 00111100
d) 11000011

44. If we have string of 4 bit = 0010, what is the value we get after applying expansion/permutation (E/P)? where,

E/P							
4	1	2	3	2	3	4	1

a) 00101110
b) 00101001
c) 00010100
d) 00010010

45. What is the heart of the DES algorithm?

a) Round function
b) Swapping function
c) Initial permutation
d) Inverse initial permutation

46. Feistel structure is based on _____

a) DES algorithm
b) substitution-permutation network
c) A and b both
d) None of above

47. In feistel cipher plaintext in divided into _____

a) Two equal parts
b) Three equal parts

c) Two different parts
d) Three different parts

48. What is the input of the decryption algorithm in feistel structure?

a) Plaintext
b) Ciphertext
c) Original text
d) None of above

49. In fesitel structure _____ key size, _____ security and _____ encryption/decryption speed.

a) Less, greater, less
b) Large, less, greater
c) Large, greater, less
d) Less, less, less

50. In fesitel structure _____ block size, _____ security and _____ encryption/decryption speed.

a) Less, greater, less
b) Large, less, greater
c) Large, greater, less
d) Less, less, less

Unit 4: Public Key Cryptography

1. How many keys are used in public key cryptosystems?

   a) Two
   b) One
   c) A and b both
   d) None of above

2. What are the value of n and ⌀(n), when p = 7 and q = 13?

   a) n = 72, ⌀(n) = 91
   b) n = 84, ⌀(n) = 72
   c) n = 91, ⌀(n) = 84
   d) n = 91, ⌀(n) = 72

3. What are the value of n and ⌀(n), when p = 3 and q = 11?

   a) n = 14, ⌀(n) = 33
   b) n = 14, ⌀(n) = 20
   c) n = 33, ⌀(n) = 20
   d) n = 33, ⌀(n) = 14

4. Which one of the following is not a public key distribution means?

   a) Public-Key Certificates

   b) Hashing Certificates

   c) Publicly available directories

   d) Public-Key authority

5. Which of the following public key distribution systems is most secure?

   a) Public-Key Certificates

   b) Public announcements

   c) Publicly available directories

d) Public-Key authority

6. Which system uses a trusted third party interface?

a) Public-Key Certificates
b) Public announcements
c) Publicly available directories
d) Public-Key authority

7. Publicly Available directory is more secure than which other system?

a) Public-Key Certificates
b) Public announcements
c) Public-Key authority
d) None of the mentioned

8. RSA stands for:

a) Rock, Shane and Amazon
b) Rivest, Shane and Adleman
c) Rivest, Shamir and Adleman
d) Rock, Shamir and Adleman

9. If Bob wants to send an encrypted message to Alice using a public key cryptosystem, which key does he use to encrypt the message?

a) Bob's public key
b) Bob's private key
c) Alice's public key
d) Alice's private key

10. If Richard wants to send an encrypted message to Sue using a public key cryptosystem, which key does he use to encrypt the message?

a) Richard's public key
b) Richard's private key
c) Sue's public key

d) Sue's private key

11. If plaintext (M) = 88, e = 7 and n = 187 than find Ciphertext (C) using RSA algorithm.

a) 10
b) 11
c) 12
d) 13

12. Which key pairs are used to achieve authenticity?

a) Sender’s private key for encryption and sender’s public key for decryption
b) Sender’s private key for encryption and receiver’s public key for decryption
c) Receiver’s private key for encryption and receiver’s public key for decryption
d) Receiver’s private key for encryption and sender’s public key for decryption

13. Which key pairs are used to achieve confidentiality?

a) Sender’s public key for encryption and sender’s public key for decryption
b) Sender’s private key for encryption and receiver’s public key for decryption
c) Receiver’s public key for encryption and receiver’s private key for decryption
d) Receiver’s private key for encryption and sender’s public key for decryption

14. When Alice receive message from Bob and decrypted with her private key then message was encrypted with _____.

a) Bob's public key
b) Bob's private key
c) Alice's public key
d) Alice's private key

15. For RSA to work, the value of p must be less than the value of _____.

a) p
b) q
c) n
d) r

16. In asymmetri-key cryptography, although RSA can be used to encrypt and decrypt actual messages, it is very slow if the message is_____

a) Short
b) Long
c) Flat
d) Thin

17. What is the meaning of Y = E (PU, X)

a) Message X is encrypted using public key
b) Message Y is encrypted using public key
c) Message E is encrypted using public key
d) Message PU is encrypted using public key

18. Which equation is used to find ciphertext using RSA algorithm?

a) $M = C^n \bmod e$
b) $C = M^e \bmod n$
c) C = M mod n
d) M = C mod e

19. Which equation is used to find plaintext using RSA algorithm?

a) $M = C^n \bmod e$
b) $C = M^e \bmod n$
c) C = M mod n
d) M = C mod e

20. Communication between end systems is encrypted using a key, often known as

a) temporary key

b) section key

c) line key

d) session key

21. Session keys are transmitted after being encrypted by

a) make-shift keys

b) temporary keys

c) master keys

d) section keys

22. How many handshake rounds are required in the Public-Key Distribution Scenario?

a) 7

b) 5

c) 3

d) 4

23. Which should be kept as a secret in public key cryptosystem?

a) Encryption key

b) Decryption key

c) Encryption & Decryption key

d) None of the mentioned

24. In RSA, $\Phi(n)$ = _____ in terms of p and q.

a) (p)/(q)

b) (p)(q)

c) (p-1)(q-1)

d) (p+1)(q+1)

25. In public key cryptosystem _____ keys are used for encryption and decryption.

a) Same

b) Different

c) Encryption Keys

d) None of the mentioned

26. In public key cryptosystem which is kept as public?

a) Encryption keys

b) Decryption keys

c) Encryption & Decryption keys

d) None of the mentioned

27. Which algorithm can be used to sign a message?

a) Public key algorithm

b) Private key algorithm

c) Public & Private key algorithm

d) None of the mentioned

28. One commonly used public-key cryptography method is the _____ algorithm.

a) RSS

b) RAS

c) RSA

d) RAA

29. The secret key between members needs to be created as a _____ key when two members contact KDC.

a) public

b) session

c) complimentary

d) none of the above

30. _____ is a trusted third party that assigns a symmetric key to two parties.

a) KDC

b) CA

c) KDD

d) None of the above

31. What is the use of nonce?

a) To Send message
b) To identify this transaction uniquely
c) To generate message
d) None of above

32. In which method man-in-the-middle attack is possible?

a) Public announcement
b) Publicly available directories
c) Simple Secret Key Distribution
d) None of above

33. A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key is known as _____.

a) key certificate
b) Key Certificate
c) Session key certificate
d) None of above

34. In which cryptographic algorithm that uses two related keys, a public key and a private key?

a) Asymmetric Cryptographic Algorithm
b) Symmetric Cryptographic Algorithm
c) a and b both
d) None of above

35. If plaintext (M) = 6, e = 7 and n = 33 than find ciphertext (C) using RSA algorithm.

a) 29
b) 30
c) 31
d) 32

36. If ciphertext (C) = 30, d = 3 and n = 33 than find plaintext (M) using RSA algorithm.

a) 6
b) 7
c) 8
d) 9

37. If ciphertext (C) = 11, e = 7 and n = 187 than find plaintext (M) using RSA algorithm.

a) 87
b) 88
c) 12
d) 13

38. What are the value of n and ⌀(n), when p = 3 and q = 7?

a) n = 21, ⌀(n) = 10
b) n = 10, ⌀(n) = 21
c) n = 21, ⌀(n) = 12
d) n = 10, ⌀(n) = 12

39. If values of e = 5 and ⌀(n) = 12, than d using RSA algorithm.

a) 5
b) 6
c) 7
d) 8

40. If values of e = 7 and ⌀(n) = 20, than find d using RSA algorithm.

a) 3

b) 4

c) 7

d) 8

41. 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 and q should be divisible by Φ(n)

b) p and q should be co-prime

c) p and q should be prime

d) p/q should give no remainder

42. Which of the following Ciphertext is true for RSA?

a) $M=C^d \bmod N$

b) $M=e^C \bmod N$

c) M=N mod Ce

d) M=N mod eC

43. In which of the following algorithm two large prime numbers must be selected?

a) DES

b) RSA

c) Caeser cipher

d) Playfair cipher

44. Which of the following Ciphertext is true for RSA?

a) $C=M^e \bmod n$

b) $C=e^M \bmod n$

c) $C=n \bmod M^e$

d) $C=n \bmod e^M$

45. CAs stands for_____

a) Certificate authorities

b) Controlled activities
c) Certification authority
d) Certificate anomaly

46. What is the meaning of X = D (PU, Y)?

a) Message X is decrypted using public key
b) Message Y is decrypted using public key
c) Message D is encrypted using public key
d) Message PU is encrypted using public key

47. What are the value of p and q, when n = 187 and ⌀(n) = 160?

a) p = 11, q = 17
b) p = 10, q = 16
c) p = 11, q = 18
d) p = 12, q = 17

48. What are the value of p and q, when n = 55 and ⌀(n) = 40?

a) p = 10, q = 4
b) p = 10, q = 11
c) p = 11, q = 5
d) p = 11, q = 4

49. What are the value of p and q, when n = 35 and ⌀(n) = 24?

a) p = 12, q = 2
b) p = 8, q = 3
c) p = 6, q = 4
d) p = 5, q = 7

50. What condition is used to select the value of e in RSA algorithm?

a) i < e < ⌀(n)
b) ⌀(n) < e < i
c) ⌀(n) < I < e

d) None of above

51. In public key cryptosystem which key is kept as private?

a) Public key
b) Private key
c) Both
d) None

52. Public key cryptography is also known as _____.

a) Symmetric key cryptography
b) Asymmetric key cryptography
c) Secret key cryptography
d) None

53. RSA is example of _____.

a) Substitution technique
b) Transposition technique
c) Asymmetric key cryptography
d) Symmetric key cryptography

54. If message is encrypted with receiver's public key, _____ key is used for decryption.

a) Receiver's private key
b) Sender's public key
c) Sender's private key
d) None

55. If message is encrypted with sender's private key, _____ key is used for decryption.

a) Receiver's public key
b) Sender's public key
c) Sender's private key

d) None

56. _____ is the valid pair of input to encryption algorithm.

a) E(Key,Text)
b) E(Text,Key)
c) D(Key,Text)
d) D(Text,Key)

57. Which of the following is not ingredient of public key cryptosystem?

a) Plaintext
b) Ciphertext
c) Hash function
d) Key

58. User A decrypt message Y using PUb then what will be the generated plaintext X?

a) X=D(X,PUb) b) X=D(PUb, Y) c) X=Y(PUb, E) d) X=PUb(D,X)

59. Which of the followings are applications of public key crypto system?

a) Encryption/Decryption b) Digital signature c) Key exchange d) All of above

60. What is the equation of euler's totient function?

a) pq b) (1-p)(1-q) c) (p-1)(q-1) d) p(p-q)

61. If n=35 then what will be the value of euler's totient function?

a) 7 b) 12 c) 35 d) 24

62. If n=6 then what will be the value of euler's totient function?

a) 6 b) 2 c) 5 d) 8

63. _____ is gcd of 54 and 888.

a) 5 b) 6 c) 4 d) 3

64. _____ is gcd of 55 and 22.

a) 11 b) 12 c) 13 d) 14

65. _____ is gcd of 590 and 45.

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

66. _____ is gcd of 270 and 192.

a) 6 b) 7 c) 8 d) 9

67. In RSA algorithm, if p=17, q=11 then n=_____.

a) 17 b) 11 c) 160 d) 187

68. In RSA algorithm, if p=17, q=31 then n=_____.

a) 480 b) 840 c) 257 d) 527

69. If n=21 then what will be the value of euler's totient function?

a) 21 b) 12 c) 13 d) 22

70. If n=77 then what will be the value of euler's totient function?

a) 40 b) 50 c) 60 d) 77

71. Which of the followings are the attacks on RSA algorithm?

a) Brute-force b) Timing c) Mathematical d) All of the above

72. In _____, any participant can broadcast the key to the community at large.

a) Public-Key Certificates

b) Public announcements

c) Publicly available directories

d) Public-Key authority

73. In directory, authority maintain _____ entry for each participant.

a) {name, public key}

b) {name, private key}

c) {public key, time stamp}

d) {private key, time stamp}

74. _____Scheme ensures both confidentiality and authentication in the exchange of a secret key.

a) Public-Key Certificates

b) Public announcements

c) Publicly available directories with Confidentiality and Authentication

d) Secret Key Distribution with Confidentiality and Authentication

75. Secrecy means _____.

a) Confidentiality
b) Authentication
c) Decryption
d) None

76. Any cryptosystem are designed to meet which goal?

a) Secrecy
b) Authentication
c) Both
d) None

77. Counter measure against brute force attack is _____.

a) Use of large key
b) Use of public key
c) Share private key
d) None

78. In _____ attack, the opponent has some idea about the plaintext and he uses this information to find the private key.

a) Probable message attack
b) Brute force attack
c) DoS attack
d) None

79. Counter measure against probable message attack is _____.

a) Use of large key
b) Appending some random bits to message
c) Share private key
d) None

80. In RSA, d satisfies the equation _____.

a) $d*e \equiv 1 \pmod{\Phi(n)}$
b) $d \equiv 1 \pmod{\Phi(n)}$
c) $e \equiv 1 \pmod{d}$
d) $d \equiv 1 \pmod{e}$

Unit 6: Digital signatures and Authentication protocols

1. Which of the following is true for digital signature _____.

   i) It must verify the author and the date and time of the signature.

   ii) It must authenticate the contents at the time of the signature.

   a) i) b) ii) c) i) & ii) d) none of above

2. What are the essential things that are necessary for the digital signature?

   a) Source b) Destination c) a & b d) None of above

3. In public key encryption system if A encrypts a message using his private key and sends it to B

   a) if B knows it is from A he can decrypt it using A's public key

   b) Even if B knows who sent the message it cannot be decrypted

   c) It cannot be decrypted at all as no one knows A's private key

   d) A should send his public key with the message.

4. The method of access which uses key transformation is known as …

   a) Direct b) Hash c) Random d) Sequential

5. What is digital signature?

   a) A scanned signature

   b) A Signature in binary form

   c) Encrypting information

   d) Handwritten signature

6. Why digital signature is required?

   i) To tie an electronic message to the senders identity

   ii) For non-repudiation of communication by a sender

iii) To prove that a message was sent by the in a court of law

iv) In all e-mail transactions

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

7. What do you mean by computationally infeasible to forge?

a) new message for existing digital signature

b) fraudulent digital signature for given message

c) none

d) a & b

8. Why digital signature is an important in public - key cryptosystem?

a) it protects two parties who exchange messages from any third party

b) none

c) a & d

d) it protect the two parties against each other

9. From below which is true for digital signature

a) must use information unique to sender

b) input function

c) output function

d) b & c

10. Which are the necessary in the aspect of the DDS (Direct Digital Signature)

a) time stamp

b) none

c) timely key revocation

d) a & c

11. Which of the followings are true for Arbitrated Digital Signature?

    a) requires suitable level of trust in arbiter

    b) can be implemented with either private or public-key algorithms

    c) arbiter may or may not be able to see message

    d) all of above

12. What do you mean by Direct Digital Signature?

    a) important that sign first then encrypt message & signature

    b) authenticate message contents

    c) security depends on sender's private-key

    d) a & c

13. Which scheme of the digital signature is more secure?

    a) Arbitrated Digital Signature

    b) Direct Digital Signature

    c) a and b both

    d) None

14. How confidentiality will be given in direct digital signature?

    a) encrypting the entire message

    b) signature using either public or private key schemes

    c) a & b

    d) none

15. Which are the key issues in Authentication Protocol?

    a) Timeliness

    b) Confidentiality

c) None

d) a & b

16. Why Authentication Protocol is used?

a) convince parties of each other's identity and to exchange session keys

b) none

c) perform signature function

d) a & c

17. What is true for Replay attack?

a) none

b) threat of message replay

c) b & d

d) valid signed message is copied and later resent

18. What are the countermeasure for Replay attack?

a) use of sequence numbers (generally impractical)

b) timestamps (needs synchronized clocks)

c) challenge/response (using unique nonce)

d) all

19. Which of the following is true for Replay attack?

a) repetition that cannot be detected

b) all

c) backward replay without modification

d) repetition that can be logged

20. Why symmetric encryption is used?

a) provide confidentiality for communication in a distributed environment

b) provide integrity in distributed environment

c) provide confidentiality for communication in a non-distributed environment

d) none

21. What are the components of the Replay attack using symmetric encryption?

a) plain text, cipher text

b) encryption and decryption algorithm

c) secret key

d) all

22. What are the functions of KDC (Key Distribution Center)?

a) each party shares own master key with KDC

b) KDC generates session keys used for connections between parties

c) master keys used to distribute these to them

d) all of above

23. A digital signature is ….

a) A bit string giving identity of a correspondent

b) A unique identification of sender

c) An authentication of an electronic record by tying it uniquely to a key only a sender knows

d) An encrypted signature of a sender

24. The central system is also known as?

a) Authentication Server

b) Key Distribution Center

c) Nonce

d) None

25. When One- way authentication is required?

a) sender & receiver are not in communications at same time

b) sender & receiver are in communications at same time

c) None

d) A and b both

26. What is the purpose of using symmetric encryption in one way authentication?

a) intended recipient of a message will be able to read the message

b) all recipient of a message will be able to read

c) none of above

d) a & b

27. How we can achieve the authentication?

a) signature can be encrypted with the recipient's public key

b) signature can be encrypted with the recipient's private key

c) signature can be encrypted with the recipient's secret key

d) none of above

28. How we can achieve the confidentiality?

a) message is encrypted with a one-time public key

b) message is encrypted with a one-time private key

c) message is encrypted with a one-time secret key

d) None of above

29. The advanced version of DSS by using the Secure Hash Algorithm is known as?

a) Digital Signature Algorithm

b) Advanced Digital Signature Standard

c) A & b

d) None

30. What is the size of signature in Digital Signature Algorithm?

a) 128 bit

b) 256 bit

c) 320 bit

d) 512 bit

31. What are the variants of Digital Signature Algorithm?

a) ElGamal

b) Schnorr

c) a & b

d) none

32. Digital Signature Algorithm uses…

a) message hash

b) global public values

c) private key & random k

d) all

33. What is the value of public key derived from Digital Signature Algorithm?

a) $y = gx \pmod p$

b) $y = hx \pmod p$

c) $y = gx \pmod h$

d) None of above

34. What is the necessary condition for generating random signature key in Digital Signature Algorithm?

a) k<q

b) k<=q

c) k>q

d) k=q

35. What is the formula to compute signature pair in Digital Signature Algorithm?

a) r = (hk(mod p))(mod q)

s = (k-1.H(M)+ x)(mod g)

b) r = (hk(mod p))(mod g)

s = (k1.H(M)+ x)(mod q)

c) r = (gk(mod p))(mod g)

s = (p-1.H(M)+ x.r)(mod g)

d) r = (gk(mod p))(mod q)

s = (k-1.H(M)+ x.r)(mod q)

36. What is the essential to ensure that signature is verified?

a) v!=r

b) v>r

c) v<r

d) v=r

37. A digital signature needs a _____.

a) Private key system

b) Shared key system
c) Public key system
d) All of above

38. Digital signature provides _____.

a) Authentication
b) Integrity
c) A and b both
d) None of above

39. What is the full form of DDS?

a) Direct Digital Signature
b) Direct Digital Sign
c) Direct Digital Standard
d) Direct Digital System

40. What is the full form of DSS?

a) Direct Signature Standard
b) Digital Signature Standard
c) Digital Signature Scheme
d) Digital Signature System

41. What is the full form of DSA?

a) Digital Signature Algorithm
b) Digital System Algorithm
c) Digital Security Algorithm
d) Digital Structure Algorithm

42. Which are the types of digital signature?

a) Direct Digital Signature
b) Arbitrated Digital Signature
c) A and b both

d) None of above

43. RSA signature encrypt the message hash with _____

a) Public key to create a signature
b) Private key to create a signature
c) A and b both
d) None of above

44. Digital signature is encrypted using _____.

a) Using symmetric encryption
b) Using public key encryption
c) A and b both
d) None of above

45. The digital signature standard uses the _____.

a) SAH hash algorithm
b) SHA hash algorithm
c) A and b both
d) None of above

46. Digital Signature Algorithm creates a _____ signature

a) 320 bit
b) 230 bit
c) 20 bit
d) 30 bit

47. DSA algorithm is _____ and _____ than RSA algorithm.

a) Smaller, slower
b) Smaller, faster
c) Larger, faster
d) Larger, slower

48. A digital signature may be formed by encrypting the entire message with the _____

a) sender’s private key
b) sender’s public key
c) Receiver’s private key
d) None of above

49. A digital signature may be formed by encrypting _____of the message with the sender’s private key.

a) a hash code
b) a hash function
c) a MAC
d) None of above

50. Digital signature must be _____ by third parties, to resolve disputes.

a) generated
b) Verifiable
c) A and b both
d) None of above

51. State the following statement is true or false: The signature must be a bit pattern that depends on the message being signed.

52. To achieve synchronization of clock of all parties, _____ is used.

a) Timestamp
b) Timeclock
c) Timesync
d) None