Shivaji University , Kolhapur
Question Bank For Mar 2022 (Summer) Examination

Subject Code : 80798 **Subject Name** : B.Tech.CBCS Part 3 Semester 5 - Information Security

Common subject Code (if any) _____

Multiple Choice Questions

1. ..... Is To Protect Data And Passwords

   A. Encryption

   B. Authentication

   C. Authorization

   D. Non Repudiation

2. . …….Prevents Either Sender Or Receiver From Denying A Transmitted Message

   A. Non Repudiation

   B. Data Integrity

   C. Active Attack

   D. Passive Attack

3. In Playfair cipher technique combining i&j, if PT = MYNAMEISATUL and Keyword = PLAYFAIREXAMPLE, CT=_____

   A. XFOLXRMKPVLR

   B. XFOLIXMKPVLR

   C. XFOLXRMKPVRL

   D. XFOLIXMKPVRL

4. In which intruder observe pattern of message from sender to receiver.

   A. Replay

   B. Denial of service

C. Masquerade

D. Traffic analysis

5. In Rail fence of depth 2, the ciphertext of PT :- we are TE students is_____

A. **WAEETDNSERTSUET**
B. WREUNEESDTATTES
C. WAEETDNSERTSUTE
D. None of these

6. A process that is designed to detect, prevent or recover is called as_____

A. **Security Mechanism**
B. None of these
C. Security Attack
D. Security Service

7. Protection of all user data in single data block is done by which service.

A. Repudiation
B. Integrity
C. **Connectionless confidentiality**
D. Both a&b

8. The Vernam Cipher is also called as_____

A. polyalphabetic
B. Caesar
C. Hill cipher
D. **One time Pad**

9. In pervasive mechanism_____is refered to data collected and potentially used to facilitate a security audit.

A. security recovery
B. event detection
C. **security audit trail**
D. all the above

10. ---------- integrity provide selective fields within user.

A. **selective field connection integrity**
B. connectionless integrity
C. connetion connection integrity

D. all the above

11.In data encryption standard ,S boxes each of which accepts _____bits as input and produces _____bits as output.

A. 3,2
B. 2,2
C. 6,4
D. 8,8

12 .In data encryption algorithm ___bit key is used as input.

A. 32
B. 48
C. 8
D. 64

13.In case of avalanche effect a change in one bit of the plain text or one bit of the key should produce a change in …… bits of the ciphertext.

A. many
B. three
C. two
D. one

14. In DES algorithm ,Each row of an S box defines general_____ substitution

A. irreversible
B. none of the above
C. both a&b
D. reversible

15. In data encryption standard algorithm _____is produced by the combination of left circular shift and permutation.

A. subkey(ki)
B. private key
C. public key
D. secrete key

16.Public key encryption is currently confined to key management and _____

A. Digital signature
B. Encryption decryption
C. signature applications
D. None of these

17. _____ key is not used in public key cryptosystem.

A. Public Key
B. Private Key
C. Secret Key
D. None of these

18.The two keys used for asymmetric encryption are referred to as the _____ and _____.

A. public key and private key
B. shared key and secret key
C. public key and shared key
D. secret key and private key

19. In RSA algorithm If two prime numbers are 17 and 11 then value of n will be_____

A. 187
B. 160
C. 178
D. 198

20. _____ is used on sender side for encryption for getting authentication.

A. Public Key
B. **Private Key**
C. Secret key
D. symmetric key

21. CA stands for_____

A. Certified Auditing
B. Certification Authorities.
C. Cyper Abuses.
D. Certified Automation.

22.A hash function guarantees integrity of a message. It guarantees that message has not be _____ .

A. Replaced
B. Over view

C. **changed**
D. Left

23.MAC stands for _____ .

A. **message authentication code**
B. message authentication connection
C. message authentication control
D. message authentication cipher

24.if any participant can send his or her public key to any other participant or broadcast the key to the community at large then this technique of key distribution is called as _____ .

A. Publicly available directory
B. **Public announcement**
C. Public-key authority
D. Public-key certificates

25.Maintenance and distribution of the public directory would have to be the responsibility of some trusted entity or organization in this technique of key distribution is called _____ .

A. **Publicly available directory**
B. Public announcement
C. Public-key authority
D. Public-key certificate

26.Hash function is a _____ .

A. A function that maps a message of any length into a variable-length hash value, which serves as the authenticator

B. **A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator**

C. Both A & B.
D. None of the above.

27.MAC = C(K, M), where K = _____ .

A. **shared secret key**
B. shared public key.
C. Shared private key.
D. None of the above

28.A variety of approaches has been proposed for the digital signature function. These approaches fall into two categories _____ .

A. **direct and arbitrated**
B. Indirect and arbitrated
C. Direct and indirect
D. None of the above

29. A digital signature needs a(n) _____ system.
A. symmetric key
B. **asymmetric key**
C. public key
D. None of the above

30.Digital signature provides _____.
A. authentication
B. nonrepudiation
C. **both a and b**
D. neither a nor b

31. A _____ signature is included in the document; a _____ signature is a separate entity.
A. conventional; digital
B. **digital; digital**
C. either a or b
D. either a or b

32.. In Kerberos ,AS referred as _____ .

A. Authorization Service
B. Authentication Service
C. **Authentication Server**
D. None of the above

33. In Kerberos ,TGS referred as _____ .

A. **Ticket granting Server**
B. Token getting Server
C. Target getting Service
D. None of the above

34. In Kerberos ,AS requests _____ from user.

A. **Ticket granting ticket**
B. Token gaining ticket
C. Ticket granting Token
D. None of the above

35..Kerberos , TGS requests _____ from user.

A. **Service granting ticket**
B. Ticket granting ticket
C. Ticket granting token
D. Token gaining ticket

36. In X.509 certificate , _____ Consists of two dates: the first and last on which the certificate is valid.

A. Signature algorithm identifier
B. **Period of validity**
C. Issuer unique identifier
D. Subject unique identifier

37. in X.509 certificate _____ do the following task that , An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.

A. Signature algorithm identifier
B. Period of validity
C. **Issuer unique identifier**
D. Subject unique identifier

38. Pretty Good Privacy (PGP) provides……

A. confidentiality, integrity, and authenticity.
B. integrity, availability, and authentication
C. availability, authentication, and non-repudiation.
D. authorization, non-repudiation, and confidentiality

39. In ……. mode, a common technique in packet-switched networks consists of wrapping a packet in a new one.

A. Tunneling
B. Encapsulation
C**. Both A and B**
D. None of the above

40. The components of IP security includes …….

A. Authentication Header (AH)
B. Encapsulating Security Payload (ESP)
C. Internet key Exchange (IKE)
D. **All of the above**

41. In ……. Mode, the authentication header is inserted immediately after the IP header.

A. Tunnel
B**. Transport**
C. Authentication
D. Both A and B

42. Which e-mail standard relies on "Web of Trust"?

A. **Pretty Good Privacy (PGP)**
B. Privacy Enhanced Mail (PEM)
C. MIME Object Security Services (MOSS)
D. Secure Multipurpose Internet Mail Extensions (S/MIME)

43. IPSec is designed to provide the security at the _____

A. transport layer
B. **network layer**
C. application layer
D. session layer

44. _____ uniquely identifies the MIME entities uniquely with reference to multiple contexts.

A. Content description.
B**. Content -id.**
C. Content type.
D. Content transfer encoding

45. Which one is the application of IPSec?

A. Secure Remote access
B. Secure branch office connectivity
C. Secure E-Commerce
D. **all of the above**

11. IPSec is implement in _____.

A. firewall
B. router
C. **either a or b**
D. none of the above

46. IPSec is below the _____ layer.

A. network layer

B**. transport layer**
C. application layer
D. session layer

47.Which one of the following is not IPSec services?

A. access control
B**. connection integrity**
C. confidentiality
D. limited traffic flow confidentiality

48. The use of S/MIME ___.

A. commercial
B. organization
C. **both a and b**
D. none of the above

49.PGP can be used for ___.

A. email
B. file storage application
C. **both a and b**
D. none of the above

50.The primary goal of the …….. protocol is to provide a private channel between communicating application, which ensures privacy of data authentication of the partners, and integrity.

A**. SSL**
B. ESP
C. TSL
D. PSL

51. At the lower layer of SSL, a protocol for transferring data using a variety of predefined cipher and authentication combinations called the …….

A**.** SSL handshake protocol
B. SSL authentication protocol
C. **SSL record protocol**
D. SSL cipher protocol

52. Which of the following is / are the types of firewall?

A. Packet Filtering router.
B. Application level gateway.

C. Circuit level gateway

D**. All of the above**

53. The primary goal of the …….. protocol is to provide a private channel between communicating application, which ensures privacy of data authentication of the partners, and integrity.

A**. SSL**

B. ESP

C. TSL

D. PSL

54. Firewalls operate by _____.

A. The pre-purchase phase

B. Isolating intranet from extranet

C. **Screening packets to/from the network and provide controllable filtering of network traffic**

D. None of the above.

55. A fundamental tool for intrusion detection is ……

A. **Audit record.**

B. Password management.

C. Both A & B

D. None of the above.

56. …….designed to protect credit card transactions on the Internet.

A. SSL(Secure socket layer)

B. **SET(secure electronic transaction)**

C. Both A & B

D. None of the above

57. Intrusion detection systems have been developed to provide…….

A. **Early warning of an intrusion so that defensive action can be taken to prevent or minimize damage.**

B. Only detecting the intrusion.

C. Only prevent the damage.

D. None of the above.

58. …… is a collection facility can be implemented that generates audit records containing only that information required by the intrusion detection system.

A. Native audit records
B. **Detection-specific audit records.**
C. Both A & B
D. None of the above

59. Point out the correct statement.
A) Parameterized data cannot be manipulated by a skilled and determined attacker
B) Procedure that constructs SQL statements should be reviewed for injection vulnerabilities
C)The primary form of SQL injection consists of indirect insertion of code
D)None of the mentioned

60. When people send you phony emails, pop-up messages, social media messages, texts, calls, or links to fake websites in order to hook you into giving out your personal and financial information.
A.Plagiarizing
B.Skimming
C.Phishing
D.Identity Theft

61. What is one of the most common and simplest attacks on a system?

A. Denial of service

B. Buffer overflow

C. Session hacking

D. Password cracking

62. What is a buffer-overflow attack?

A. Overflowing a port with too many packets

B. Putting more email in an email system than it can hold

C. Overflowing the system

D. Putting more data in a buffer than it can hold

63. SQL injection is based on what?

A. Having database admin privileges

B. Creating an SQL statement that is always true

C. Creating an SQL statement that will force access

D. Understanding web programming

Descriptive Questions

Chapter 1

Q1. Explain different types of attacks with example ?

Q.2 Explain X.800 Security services?

Q.3 Explain X.800 Security Mechanisms.?

Q4. Explain model of conventional cryptosystem?

Q.5 Explain Play fair cipher with example?

Q6. Explain Transposition Techniques with Examples?

Q7. Explain single round of DES algorithm?

Q8 .Explain Hill Cipher with Example ?

Q.9 Explain a model for network security with neat diagram ?

Q.10 What is substitution technique? Explain Caesar, monoalphabetic cipher ?

Chapter 2

Q11. Explain applications and requirements of public key cryptography?

Q.12 Explain RSA algorithm with example ?

Q.13 Write and explain Diffie-Helman Keyexchange algorithm?

Q.14 *Explain the distribution of public keys using public-key certificates?*

Q.15 what is message authentication code ? What are basics of MAC?

Q16.How message authentication achieved using Hash functions?

Q.17 *Explain Man-in-middle attack ?*

Q.18 *Consider Diffie-Helman Scheme with common prime q=11 and primitive* root alpha =2

A. show that 2 is primitive root of 11.

B. If user A has public key YA=9,W hat is A's private key XA ?

C. If user B has public key YB=3, What is shared secret key ?

Q.19 Explain principals of public key cryptosystems?

Q.20 5How Encryption can be used for message authentication ?

Chapter 3

Q.21 Explain arbitrated and direct digital signature?

Q.22 Exlain RSA and DSS approaches to digital signature?

Q.23 Explain DSA algorithm?

Q.24 Give the overview of kerberos?

Q.25 Explain Difference between kerberos 4 and kerberos 5 ?

Q.26 Explain X.509 certification formats?

Q.27 Define Digital signature? Explain Propertities of Digital Signature?

Q.28 Mention Differences between arbitrated and direct digital signature?

Q.29 Define Kerberos? Explain the Reqirements of Kerberos?

Chapter 4

Q.30 Explain 5 services of PGP ?

Q.31 What is MIME And S/MIME ?

Q.32 Explain Tunnel and Transport mode of IP Security?

Q.33 Explain antireplay service?

Q.34 Explain Cryptographic keys and keyrings?

Q.35 Explain Applications and Benefits of Ipsec ?

Q.36 Explain overview of IP Security Architecture?

Q.37 Explain AH in Detail.

Q.38 Explain ESP in Detail.

Q.39 Write Short Note on PGP?

Chapter 5

Q.40 Explain SSL Architecture?

Q.41 Explain SSL Record Protocol ?

Q.42 Explain SSL Handshake Protocol?

Q.43 What is SET ? Explain SET Participants and Requirements?

Q.44 What are different classes of intruders and explain with example?

Q.45 Explain Different approaches used for Intrusion detection?

Q.46 What are audit records ? Which fields are present in detection specific audit records.

Q.47 Describe the architecture for distributed intrusion detection system.

Q.48 Explain Different Types of firewalls?

Q.49 Write a short note on trusted systems?

Q.50 Explain different Password Selection Strategies ?

Chapter 6

Q.51 Explain DOS and DDOS attack?

Q.52 Explain ARP Spooing with neat diagram?

Q.53 Explain Pharming Attacks?

Q.54 Write a short note on Phishing?

Q.55 Explain Buffer over flow in detail?

Q.56 Explain Format string attack?

Q.57 Describe SQL injection attack is detail.