Anekant Education Society's

Tuljaram Chaturchand College of Arts, Science and Commerce, Baramati

(Autonomous)

Department of Computer Science

Class : M.Sc.(Comp.Sci.) – I Semester : I Paper Code : COMP4102 (Paper – II)

Title : Cryptography & Network Security

Question Bank

Type of Question : MCQ

1. The _________ attack is related to confidentiality.
   a) Interception b) fabrication c) modification d) interruption
2. The _________ attack is related to authentication.
   a) Interception b) fabrication c) modification d) interruption
3. The _________ attack is related to integrity.
   a) Interception b) fabrication c) modification d) interruption
4. The _________ attack is related to availability.
   a) Interception b) fabrication c) modification d) interruption
5. In _______ attacks, there is no modification to message contents.
   a) Passive b) active c) both of the above d)none of the above
6. In _______ attacks, the message contents are modified.
   a) Passive b) active c) both of the above d)none of the above
7. Interruption attacks are also called as _______ attacks.
   a) masquerade b) alteration c) denial of service d) replay attacks
8. DOS attacks are caused by __________.
   a) Authentication b) alteration c) fabrication d) replay attacks
9. Virus is a computer _______.
   a) File b) program c) database d) network
10. A worm ___________ modify a program.
    a) Does not b) does c) may or may not d) may
11. Applets and ActiveX controls are __________ side programs.
    a) Client b) server c) database d) none of the above
12. ActiveX Controls are ________secure as compared to applets.
    a) More b) equally c) far more d) less
13. The language that we commonly used can be termed as ___________.
    a) Pure text b) simple text c) Plain text d) normal text
14. The codified language can be termed as __________.
    a) Pure text b) simple text c) Plain text d) normal text
15. Caesar Cipher is an example of _______________.
    a) Substitution Cipher b)Transposition Cipher
    c) Substitution as well as Transposition d) none of the above
16. Vernam Cipher is an example of _____________.
    a) Substitution Cipher b)Transposition Cipher
    c) Substitution as well as Transposition d) none of the above

17. The Process of writing the text as diagonals and reading it as sequence of rows is called as _______.

a) Rail Fence Technique b) One Time Pad

c) Mono alphabetic Cipher d) Homophonic substitution Cipher

18. Book Cipher is also called as ________.

a) Rail Fence Technique b) One Time Pad

c) Mono alphabetic Cipher d) Running Key Cipher

19. Vernam Cipher is also called as _________.

a) Rail Fence Technique b) One Time Pad

c) Book Cipher d) Running Key Cipher

20. There are ________ rounds in DES.

a) 8 b) 10 c) 14 d) 16

21. In _________ , one bit of plain text is encrypted at a time.

a) Stream Cipher b) Block Cipher c) Both a & b d) None of the above

22. In _________ , one block of plain text is encrypted at a time.

a) Stream Cipher b) Block Cipher c) Both a & b d) None of the above

23. In IDEA, the key size is _________

a) 128 bytes b) 128 bits c) 256 bytes d) 256 bits

24. ____________ increases the redundancy of plain text.

a) Confusion b) Diffusion c) Both a & b d) Neither confusion nor diffusion

25. DES encrypts blocks of ___________ bits.

a) 32 b) 56 c) 64 d) 128

26. _________ works on block mode.

a) CFB b) OFB c) CCB d) CBC

27. To decrypt a message encrypted using RSA, we need the ___________.

a) Senders private key b) senders public key c) receivers private key d) receivers public key

28. To verify a digital signature, we need the _________

a) Senders private key b) senders public key c) receivers private key d) receivers public key

29. RSA _______ be used for digital signature.

a) Must not b) cannot c) can d) should not

30. ________ is a message digest algorithm.

a) DES b) IDEA c) MD5 d) RSA

31. When two different message digests have the same value, it is called as ________

a) Attack b) collision c) hash d) none of the above

32. A _______ is used to verify the integrity of message.

a) Message digest b) decryption algorithm c) digital envelop d) none of the above

33. The private key _________

a) must be distributed b) must be shared with everyone

c) must remain secret with an individual d) none of the above

34. In asymmetric key cryptography, _________ keys are required per communicating party.

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

35. We trust a digital certificate because it contains _________

a) owner's public key b) CA's public key c) CA's signature d) Owners signature

36. OCSP is _____________

a) online b) online and offline c) offline d) not defined

37. CRL is _____________

a) online b) online and offline c) offline d) not defined

38. To solve the problem of trust, the _____________ is used.

a) public key b) self signed certificate c) private key d) digital signature

39. The ___________ standard defines the structure of a digital certificate.

a) X.500 b) TCP/IP c) ANSI d) X.509

40. A ______ can issue digital certificates.

a) CA b) Government c) shopkeeper d) bank

41. SSL works between ________ and _________

a) Web browser, Web Server b) Web browser, application server

c) Web Server, application server d) application server , database server

42. SSL layer is located between ________ and ________

a) transport layer, network layer b) application layer, transport layer

c) data link layer, physical layer d) network layer, data link layer

43. The __ ______ Protocol is similar to SSL.

a) HTTP b) HTTPS c) TLS d) SHTTP

44. SET uses the concept of ___________.

a) Double Signature b) Dual signature c) Multiple signature d) Single signature

45. Electronic money is made up of ________ in physical form.

a) floppy disk b) computer files c) hard disks d) Credit card

46. The security layer in WAP is between ________ layer and the ________ layer.

a) Transaction , Transport b) application, transport

c) Transport, physical d) session, transport

47. Kerberos provides for _________

a) encryption b) SSO c) Remote Login d) local login

48. In _________ authentication mechanism, only one party authenticates the other.

a) one way b) mutual c) timestamp-based d) mutual with public keys

49. Biometric authentication works on the basis of __________

a) human characteristics b) passwords c) smart card d) PINs

50. In certificate based authentication, the user needs to enter password for accessing _________

a) public key file b) private key file c) seed d) random challenge

51. ______ is the most common authentication mechanism.

a) Smart Card b) PIN c) Biometrics d) Password

52 Firewall should be situated _________

a) Inside a corporate Network b) outside a corporate Network

c) Between a corporate Network and the outside world d) None of these

53. Firewall is a specialized form of a _________

a) Bridge b) disk c) printer d) router

54. Application gateways are _________ than packet filters.

a) less secure b) more secure c) equally secure d) slower

55. _______ allows reuse of IP addresses.

a) Firewalls b) IPSec c) NAT d) VPN

56. IPSec provides security at the _________ layer

a) Application b) transport c) network d) data link

57. ISAKMP/Oakley is related to _________

a) SSL b) SET c) SHTTP d) IPSec

58. Encryption in IPSec is done by __________

a) Tunnel mode b) transport mode c) IKE d) ESP

59. A packet filters examines ________ packets.

a) All b) no c) some d) alternate

60. The trap set to attract potential attackers is called as _________.

a) VPN b) trapdoor c) proxy d) honeypot

Type of Questions : Short answer Questions

1. List the principles of security.
2. List the types of active attacks.
3. Define active and passive attacks
4. Define Phishing.
5. Define cryptanalysis.
6. What are the two basic ways of transforming plain text into cipher text ?
7. Define encryption and decryption.
8. Define plain text and cipher text.
9. Write down the steps of algorithm of Rail Fence Technique.
10. Define Stegnography.
11. Define Stream Cipher and Block Cipher.
12. List different algorithm modes
13. Define symmetric key cryptography
14. Define asymmetric key cryptography.
15. Define Collision.
16. Define Public Key and Private Key.
17. List four steps in the creation of a digital certificate.
18. What is RA ?

19. What is CA ?
20. What is the use of X.509 ?
21. Which features provide by Java to create and work with digital certificates.
22. On which layer SHTTP works?
23. In which layer SSL works?
24. Which mechanism used by SET to achieve its objectives?
25. What is Kerberos ?
26. What are the main types of authentication tokens ?
27. What is SSO?
28. What is reflection attack?
29. Define security handshake pitfalls.
30. List the characteristics of a good firewall implementation ?
31. What are the limitations of firewall?
32. What is the significance of tunnel mode?
33. What is VPN?
34. What is honeypot?

Type of Questions: Long answer questions/write note on:

1. What are the key principles of security ?
2. What is access control ? How different is it from availability ?
3. Discuss Passive attack.
4. Explain in brief types of attacks.
5. What is worm ? What is the significant difference between a worm and a virus ?
6. Discuss the concepts of phishing and pharming.
7. Discuss ActiveX Controls and contrast them with applets.
8. Explain substitution Cipher and Transposition Cipher.
9. What is encryption and decryption ? Draw a block diagram showing plain text, cipher text, encryption and decryption.
10. Distinguish between Symmetric and Asymmetric Key Cryptography.
11. Discuss Vernam Cipher with suitable example.
12. How does Simple Columnar Transposition technique works ? state with suitable example.
13. What would be the transforming of a message “Happy birth day to you” using Rail Fence Technique ?
14. What would be the cipher text of the message “HOW ARE YOU” , Using Vernam Cipher, use one time pad “NCBTZQARX”.
15. How would we transform the message “ Come Home Tomorrow” using Rail Fence Technique ?

16. State and explain different algorithm modes.

17. Write a note on Symmetric Key Cryptography.

18. Discuss How DES Works ?

19. Write a note on Blowfish.

20. Explain the principles of the IDEA algorithm.

21. Explain AES technique in detail.

22. Given two prime numbers P= 7 and Q =17. Find out N,E, and D in an RSA encryption Process.

23. Explain RSA algorithm in brief

24. Discuss the history of asymmetric key cryptography in brief.

25. Describe the advantages and disadvantages of symmetric and asymmetric key cryptography.

26. State the difference between symmetric and asymmetric key cryptography.

27. Write a note Digital Signature.

28. Write a note on Message Digest.

29. What are the key requirements of message digest?

30. In RSA, given N = 187 and the encryption key (E) as 17. Find out the corresponding private key (D).

31. What is the role of a CA & RA. (Certification Authority & Registration Authority).

32. State the four key steps in the creation of a digital certificate.

33. What are the typical contents of a digital certificate?

34. Why is a self signed certificate needed?

35. Describe how cross certification is useful.

36. Discuss XML security concepts in brief.

37. Why do we trust a digital certificate?

38. What is the purpose of the SSL Protocol?

39. What is the significance of the time stamping protocol?

40. How is 3-D secure different from SET?

41. What is electronic money?

42. What is the security concern in WAP?

43. How does Kerberos Work?

44. How does Biometrics work?

45. How does certificate-based Authentication Work?

46. What is the difference between challenge/response tokens and time based tokens?

47. How does something derived from a password work?

48. Write a note on mutual authentication mechanism with its advantages and drawbacks.

49. Explain how NAT works with an example.

50. What are the two main attacks on corporate network?
51. What are the three main actins of a packet filters?
52. How is circuit gateway different from an application gateway?
53. Write a note on Firewall.
54. Write a note on VPN.

Type of Questions : Questions related with syllabus

- ✓ Explain how cookies can be misused to invade people’s privacy.
- ✓ What is Trojan horse ? What is the principle behind it ?
- ✓ Write a C program to implement the DES algorithm logic.
- ✓ Write a program to implement the RSA algorithm in a suitable language.
- ✓ What are the important features provided by .NET for certificate related areas?
- ✓ It is said that 2-factor authentication is not necessarily better. Why ?
- ✓ Do you think a mobile phone can be made a part of user authentication? How?
- ✓ What is Phishing? How is it related to authentication? How would you prevent possible phishing attacks?
- ✓ What is the difference between software and hardware firewalls?
- ✓ Would you ever propose leased line as a better approach than VPN? Why?

==
==