Biyani's Group of Girls' Colleges

BCA III

Network security and Cryptography

Examination-2016

Model Paper 1

Time: 3hrs M.M:50

The question paper contains 40 multiple choice questions with four choices and student will have to pick the correct one. (Each carrying ½ marks.).

1. Cryptography means:
   (a) Secret writing (b) Word processing
   (c) Parallel processing (d) All of the above ( )
2. In cryptography:
   (a) Information is transmitted from sender to receiver
   (b) No information is transmitted
   (c) Information is damaged
   (d) None of the above ( )
3. Input message in cryptography is called:
   (a) Plain text
   (b) Cipher text
   (c) Both a and b
   (d) None of the above ( )
4. Output message in cryptography is called:
   (a) Plain text (b) Cipher text
   (c) Both a and b (d) None of the above ( )
5. The process to discover plain text or key is known as:
   (a) Cryptanalysis
   (b) Crypto design
   (c) Crypto processing
   (d) Crypto graphic ( )
6. Block cipher process:
   (a) 1000 bits at a time (b) Secure Hash Function
   (c) Both a and b (d) None of the above ( )
7. SHF stands for:
   (a) Symmetric Hash Function
   (b) Secure Hash Function
   (c) Simulated Hash Function
   (d) None of these
8. One way authentication is:
   (a) Single transfer of information (b) Duplex transfer of information
   (c) Half duplex transfer of information (d) None of the above ( )
9. Two way authentication is:
   (a) Double transfer of information (b) No transfer of information
   (c) Half duplex transfer of information (D) None of the above ( )

10. Authentication is:
    (a) Verification of user's identification
    (b) Verification of the data
    (c) Both a and b
    (d) None of the above ( )
11. DES stand for:
    (a) Data Encryption standard
    (b) Data Encryption source
    (c) Data encryption system
    (d) None of these ( )
12. What is size of data block in AES configuration:
    (a) 128
    (b) 64
    (c) 256
    (d) None of these ( )
13. Which of the following is not a block cipher operating mode:
    (a) ECB
    (b) CBC
    (c) CFB
    (d) None of these ( )
14. Who was designed RC5:
    (a) Ron
    (b) Rivent
    (c) Ron & Rivent
    (d) None of these ( )
15. RSA stands for:
    (a) Rivest
    (b) Shamir
    (c) Rivest Shamir & Adleman
    (d) None of these ( )
16. IDEA developed by:
    (a) Xuijla Lai & James Massey
    (b) Xaija
    (c) James Massey
    (d) None of these ( )
17. Blowfish was developed by Bruce Schneier. The block size is:
    (a) 64
    (b) 32
    (c) 48
    (d) None of these ( )
18. The symmetric (Shared) key in the Diffie - Hellman Protocol is:
    (a) $k = g^{xy}$ and p
    (b) $K = g^{xy} \bmod q$
    (c) $K = (R_2)^x$
    (d) All of the above ( )
19. Triple DES was designed to increase the size of teh DES key for better security:
    (a) 56 bits
    (b) 112
    (c) 256 bits
    (d) None of these ( )
20. Which of the following is not a type of permutation in P-boxes:
    (a) Plain permutation
    (b) Straight permutation

(c) Expansion permutation
(d) Compression permutation ( )

21. A digital signature needs a:
(a) Plain permutation (b) Straight permutation
(c) Expansion permutation (d) compression permutation ( )

22. SHA-1 algorithm process data in block length of .....bits.
(a) 128 (b) 256
(c) 512 (d) 1024 ( )

23. The codified languages can be termed as:
(a) Clear text
(b) Unclear text
(c) Code text
(d) Cipher text ( )

24. To preserve the integrity of a message, the message is passed through an algorithm called a:
(a) Hash function (b) Finger Print Function
(c) N Hash function (d) None of these ( )

25. Secure socket layer is designed to provide security and compression services to data granted from.....
(a) Application layer
(b) Transport layer
(c) Application layer & transport layer
(d) None of these ( )

26. .....is an encryption method used to offer secure communication by e-mail:
(a) Mail Server (b) PGP
(c) SSL (d) None of these ( )

27. Which of the following is not a property of a packet filtering firewall :
(a) Network layer and transport layer
(b) Uses ACLs
(c) Considered first generation firewall
(d) None of these ( )

28. Which layer filter the proxy firewall:
(a) Application layer
(b) Transport layer
(c) Network layer
(d) None of these ( )

29. Which of the following is not a criteria of a hash function:
(a) Two-wayness
(b) Weak collision resistance
(c) Strong collision
(d) One - Wayness ( )

30. Network security:
(a) Data is protected during transmission
(b) Data is not protected at all
(c) Data is changed
(d) All of the above ( )

31. CBCM stands for:
(a) Cipher block chaining mode

(b) Cipher block changing mode
(c) Cipher block chaining method
(d) Cipher block changing method ( )

32. Cryptograph ensures:
(a) Confidentiality of data
(b) Authentication of data
(c) Integrity of data
(d) All of the data ( )

33. Secure hash function or algorithm developed by:
(a) National Institute of Standard & Technology
(b) IEEE
(c) ANSI
(d) Nose of these ( )

34. Deffie - Hellman protocol that provides a session key:
(a) One time
(b) Two time
(c) One time & two time
(d) None of these ( )

35. X.509 include which of the following authentication procedure:
(a) One way authentication
(b) Two way authentication
(c) Three way authentication
(d) None of these ( )

36. Which of the following is not provided by digital signature:
(a) Message integrity
(b) Authentication
(c) Non repudiation
(d) KDC ( )

37. PKI stands for:
(a) Public key infrastructure
(b) Public Key interface
(c) Public key internet
(d) None of these ( )

38. The most widely used public key algorithm are:
(a) RAS
(b) Diffie-Hellman
(c) RAS & Diffie-Hellman
(d) None of these ( )

39. ESP stands for:
(a) Encryption Security Protocol
(b) Entity Secure Protocol
(c) Encapsulating Security payload
(d) None of these ( )

40. Which of the following is not provided by ESP:
(a) Source authentication (b) Data integrity
(c) Privacy (d) Padding ( )

Attempt any four descriptive types of questions out of the six. All questions carry 7½ marks each.

Q.1 (a) Explain the RSA Crypto System. Also explain how decryption be made fast.
(b) What are the different types of attacks on double DES and triple DES?

Q.2 (a) Explain about block cipher principles and modes of operations.

(b) What are the uses of authentication protocols?

Q.3 (a) What is the use of digital signature? What are the requirements of the digital signature scheme?

(b) What is MAC? Explain its use?

Q.4 (a) Explain the Diffie-Hellman Key Exchange Algorithm with an example.

(b) Describe the data encryption algorithm.

Q.5 (a) What is a hash function? What are the requirements for a hash function? Also list the basic uses of a hash function.

(b) Explain about Kerberos.