BCA III

Network security and Cryptography

Examination-2016

Model Paper 2

Time: 3hrs M.M:50

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

1. Input message in Cryptography is called;
   (a) Plain text (b) Cipher Text
   (c) Plain and cipher (d) None of the above ( )

2. Asymmetric key is also called:
   (a) Secret key (b) Public key
   (c) Private key (d) None of the above ( )

3. RSA stands for:
   (a) Rivest Shamir and Adleman
   (b) Rock Shane and Amozen
   (c) Rivest Shane and Amozen
   (d) Rock Shamir and Adleman ( )

4. A digital signature need a :
   (a) Public key system
   (b) Private key system
   (c) Public and private key system
   (d) None of the above ( )

5. Which layer filter the proxy firewall:
   (a) Application (b) Transport layer
   (c) Network Layer (d) None of the above ( )

6. Secure Hash function or algorithm developed by:
   (a) NIST (b) IEEE
   (c) ANSI (d) None of the above ( )

7. .....is an encryption method used to offer secure communication by e-mail:
   (a) Mail server (b) PGP
   (c) SSL (d) None of the above ( )

8. Network security ensures:

(a) Detecting attacks (b) Preventing attacks
(c) Recovering attacks (d) All of the above ( )

9. The process to discover plain text or key is known as:
(a) Cryptanalysis (b) Crypto design
(c) Crypto processing (d) Crypto graphic ( )

10. Hacking refers to:
(a) Data access without permission
(b) Data updation without permission
(c) Data deletion without permission
(d) All of the above. ( )

11. Encryption protects against:
(a) Attacks (b) Viruses
(c) Manipulation of data (d) All of the above ( )

12. Hash function is used to produce:
(a) Finger print of a file
(b) Useful for message authentication
(c) Both a and b
(d) None of the above ( )

13. Block cipher processes:
(a) 1000 bits at a time
(b) One bit block of data at a time
(c) Both a and b
(d) None of the above ( )

14. Decryption algorithm:
(a) Encrypts input data
(b) Decrypts the encrypted data
(c) Both a and b
(d) None of the above ( )

15. What is the name of the network attack that floods it with useless traffic?
(a) Virus (b) Trojan horse
(c) DOS attach (d) Spoofing ( )

16. RSA algorithm uses variable sized key that is usually between.....and bits.
(a) 256,1048 (b) 256, 2048
(c) 512, 1048 (d) 512, 2048 ( )

17. What is an advantage of RSA over DSS?
(a) It can provide digital signature and encryption functionality
(b) It uses fewer resources and encrypts quicker because it uses symmetric keys
(c) It is a block cipher versus a stream cipher
(d) It employs a one-time encryption pad ( )

18. The codified language can be termed as:
(a) Cleartext (b) Unclear text
(c) Codetext (d) Cipher text ( )

19. Cryptology means:
(a) Cryptology+ Cryptodesign
(b) Cryptology Cryptanalysis
(c) Cryptograph itself known as cryptology also

(d) None of the above ( )

20. The input block length in AES is:
(a) 56 bits (b) 64 bits
(c) 112 bits (d) 128 bits ( )

21. An attack on a cipher text message where the attacker attempts to use all possible permutations and combinations is called:
(a) Brute-Plaintext attack (b) Birthday attack
(c) Known-Plaintext attack (d) Chosen-plaintext attack ( )

22. Hash collision means:
(a) Two keys for one message
(b) One key for two message
(c) Two different keys for different message
(d) Always the same key ( )

23. Encryption strength is based on:
(a) Strength of algorithm
(b) Secrecy of key
(c) Length of key
(d) All of the above ( )

24. In an authentication using symmetric keys, if 10 people need to communicate, we need ..... Keys.
(a) 10 (b) 20
(c) 30 (d) 40 ( )

25. In an efficient algorithm for factoring large number is discovered, which of the following schemes will be known to be not secure?
(a) Diffle-Hellman (b) RSA
(c) AES (d) None of the above ( )

26. Session Key establishes:
(a) Logical connection (b) Physical Connection
(c) Both a and b (d) None of the above ( )

27. In the digital signature technique, the sender of the message uses.....to create cipher text:
(a) Own symmetric key
(b) Own private key
(c) The receiver's private key
(d) Receiver's public key ( )

28. The symmetric (Shared) key in the Diffle-Hellman protocol is:
(a) $k = g^{xy}$ and p (b) $K = g^{xy} \bmod q$
(c) K = (R2)x (d) All of the above ( )

29. Secure socket layer is designed to provide, security and compression services to data granted from.....
(a) Application Layer (b) Transport Layer
(c) Both (a) and (b) (d) None of the above ( )

30. Which of the following is not type of permutation in P-boxes?
(a) Plain permutation
(b) Straight permutation
(c) Expansion permutation
(d) Compression permutation ( )

31. Which of the following is not type of permutation in P-boxes?
(a) Plain permutation
(b) Straight permutation

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

32. SHA-1 is similar to:
(a) RSA (b) DES
(c) MDS (d) Rijndael ( )

33. Kerberos is an authentication scheme that can used to implement:
(a) Public key cryptography (b) Digital signature
(c) Hash function (d) Single sign on ( )

34. Transposition cipher involves:
(a) Replacement of blocks of text with other blocks
(b) Replacement of characters of text with other character
(c) Strict row to column replacement
(d) Some permutation on the input text to produce cipher text ( )

35. Which of the following is not a block cipher operating mode?
(a) ECB (b) CBF
(c) OFB (d) CBC ( )

36. If an efficient algorithm for factoring large number is discovered which of this following schemes will be known to be not secure?
(a) AES (b) Diffle-Hellman
(c) RSA (d) EI Gammal ( )

37. What are MD4 and MD5?
(a) Symmetric Encryption Algorithms
(b) Asymmetric encryption Algorithms
(c) Hashing algorithms
(d) Digital certificates ( )

38. TDES means:
(a) Triple digital encryption standard
(b) Triangular data encryption standard
(c) Triple data encryption standard
(d) Triangular digital encryption standard ( )

39. If an attacker stole a password file that contained one way encrypted passwords, what type of an attack would he/she perform to find the encrypted password?
(a) Man- in-the middle attack
(b) Birthday attack
(c) Denial of service attack
(d) Dictionary attack ( )

40. Masquerade attack is another name of:
(a) Virus attack (b) Spoofing
(c) DOS attack (d) Trojan Horse ( )

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

Q.1 (a) Explain the operation of DES algorithm using diagram. What is the strength of a DES algorithm?
(b) Write down AES parameter and explain AES key expansion.

Q.2 (a) Explain collision resistant has functions by taking suitable example.
(b) What do you mean by 'Birthday Attack"? Explain.

Q.3 (a) What do you mean by pseudo random number generation? Explain
(b) What is MAC? What is its use?

Q.4 (a) Describe various block cipher operating modes in brief.
(b) Differentiate symmetric and asymmetric encryption scheme.

Q.5 (a) What is the use of digital signature? What are the requirement of a digital Signature scheme?
(b) What is coin flipping? Explain briefly.

Q.6 Explain short notes on any three of the following:

(a) Proxy firewall
(b) One time pad scheme
(c) Triple DES
(d) SHA-1