Information Security

SET-3

By

BHARAT BHUSHAN @ B. K. NAL
Assistant Professor (Computer Science)
Director, BSTI, Kokar

&

SUPRIYA BHARATI
Assistant Professor (Computer Science)
Asst. Director, BSTI, Kokar

Buddha Science and Technical Institute (BSTI), Kokar
www.bharatsir.com

1. Public key cryptography also called as_____ .

A. asymmetric key cryptography
B. symmetric key cryptography
C. both a and b
D. none of the above

2. PGP makes use of which cryptographic algorithm?

A. Rsa
B. Aes
C. Des
D. robin

3. USENET falls under which category of public key sharing?

A. public announcement
B. publicly available directory
C. public key authority
D. public key certificate

4. In Asymmetric-Key Cryptography, the two keys, e and d, have a special relationship to

A. Other
B. Data
C. Keys
D. each other

5. In Asymmetric-Key Cryptography, although RSA can be used to encrypt and decrypt actual messages, it is very slow if the message is

A. Short
B. Flat
C. Long
D. thin

6. An asymmetric-key (or public-key) cipher uses

A. 1 key
B. 2 key
C. 3 key
D. 4 key

7. In cryptography the original message before being transform is called

A. simple text
B. plain text
C. empty text
D. filled text

8. In asymmetric key cryptography, the private key is kept by_____ .

A. sender
B. receiver
C. sender and receiver
D. none of these

9. _____is the practice of concealing a message within another message, image or file.

A. steganography
B. cryptography
C. cipher
D. receiver

10. The_____is a polygraphic substitution cipher based on linear algebra.

A. hill cipher
B. playfair cipher
C. affine cipher
D. none of these

11. The message which is not understandable is called as?

A. cipher text
B. plain text
C. hidden text
D. both a & c

12. Which of them is type of Cipher?

A. stream cipher
B. block cipher
C. both of them
D. none of these

13. AES stands for?

A. authorized encryption standard
B. advance encryption standard
C. advance encryption strategy
D. none of these

14. In AES in which Round Subkeys are Generated from Original key for each round?

A. key expansion
B. initial round
C. finale round
D. none of these

15. What is the 4th step in DES Algorithm?

A. key transformation
B. s-box substitution
C. p-box permutation
D. expansion permutation

16. In DES step both LPT and RPT undergoes in how much key Rounds?

A. 8

B. 16
C. 32
D. 64

17. Blum Blum Shub Generator is based on which Algorithm?

A. private key
B. public key
C. both a & b
D. none of these

18. In Symmetric schemes requires both parties to share how many secret key?

A. One
B. Two
C. Three
D. four

19. Conversion of plain text into Cipher text is called as_____.

A. Encryption
B. Decryption
C. hidden text
D. none of above

20. The technique in which when one character is replaced by another character is called as?

A. Transposition
B. Substitution
C. Combinational
D. none of these

21. A way to ensure that the entity is indeed what it claims to be

A. authentication
B. accountability
C. identification
D. security

22. An act of protecting information from unauthorized disclosure to an entity

A. integrity
B. avability
C. confidentiality
D. none of these

23. _____is used to create the organization's overall security program.

A. program policy
B. purpose
C. security
D. none of these

24. Conversion of Cipher text to plain text?

A. Encryption
B. Decryption
C. simple text
D. none of these

25. Symmetric key encryption is also called as?

A. public key encryption
B. private key encryption
C. both of these
D. none of these

ANSWER						
1.	A		11.	A	21.	A
2.	A		12.	C	22.	C
3.	A		13.	B	23.	A
4.	D		14.	A	24.	B
5.	C		15.	C	25.	B
6.	A		16.	B		
7.	B		17.	B		
8.	B		18.	A		
9.	A		19.	A		
10.	A		20.	B		