# Information Security

## SET-2

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. Cryptanalysis is used**

A. to find some insecurity in a cryptographic scheme
B. to increase the speed
C. to encrypt the data
D. to make new ciphers

**2. The procedure to add bits to the last block is termed as**

A. decryption
B. hashing
C. tuning
D. padding

**3. In same keys are implemented for encrypting as well as decrypting the information.**

A. symmetric key encryption
B. asymmetric key encryption
C. asymmetric key decryption
D. hash-based key encryption

**4. An attack in which the user receives unwanted amount of e- mails.**

A. Smurfing
B. denial of service
C. e-mail bombing
D. ping storm

**5. Study of creating a d using encryption and decryption techniques.**

A. Cipher
B. Cryptography
C. Encryption
D. decryption

**6. A unique piece of information that is used in encryption.**

A. Cipher
B. plain text
C. key
D. cipher

**7. The information that gets transformed in encryption is .....**

A. plain text
B. parallel text
C. encrypted text
D. decrypted text

**8. If communication between 2 people is overheard by a third person without extraction of any data, it is called as:**

A. release of message content-passive attack
B. traffic analysis -passive attacks
C. release of message content- active attacks
D. traffic analysis -active attacks

**9. If communication between 2 people is overheard by a third person without manipulation of any data, it is called as:**

A. release of message content-passive attack
B. traffic analysis -passive attacks
C. release of message content- active attacks
D. traffic analysis -active attacks

**10. Compromising confidential information comes under**

A. Bug
B. Threat

(C) Vulnerability
(D) Attack

**11. From the options below, which of them is not a threat to information security?**

A. Disaster
B. Eavesdropping
C. information leakage
D. unchanged default password

**12. ……is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction.**

A. network security
B. database security
C. information security
D. physical security

**13. Data integrity gets compromised when and are taken control off.**

A. access control, file deletion
B. network, file permission
C. access control, file permission
D. network, system

**14. Data is used to ensure confidentiality.**

A. Encryption
B. Locking
C. Deleting
D. Backup

**15. SET stands for**

A. set electronic transaction
B. secure electronic transaction
C. simple electronic transaction

(D) none of the above

**16. PGP is abbreviated as**

A. pretty good privacy
B. pretty good policy
C. policy good privacy
D. pretty good protection

**17. Internet Key Exchange has .... phases and modes of operations**

A. 4
B. 3
C. 2
D. 5

**18. Pretty good privacy (PGP) is used in _____ .**

A. browser security.
B. email security
C. wifi security
D. ftp security

**19. SSL primarily focuses on _____ .**

A. integrity and authenticity
B. integrity and non-repudiation
C. authenticity and privacy
D. confidentiality and integrity

**20. An attempt to make a computer resource unavailable to**

its intended users is called _____.

A. denial-of-service attack
B. virus attack
C. worms attack
D. botnet process

**21. HTTPS is abbreviated as _____ .**

A. hypertexts transfer protocol secured
B. secured hyper text transfer protocol
C. hyperlinked text transfer protocol secured
D. hyper text transfer protocol secure

**22. RSA algorithm is best example of_____ .**

A. asymmetric key cryptography
B. symmetric key cryptography
C. elliptic curve cryptography
D. all of the above

**23. Hash function is used for_____ .**

A. message authentication
B. digital signature
C. both a and b
D. only a

**24. Diffie-Hellman algorithm is widely known as_____ .**

A. key exchange algorithm
B. key agreement algorithm
C. only a
D. both a and b

**25. ECC stands for**

A. elliptic curve cryptography
B. elliptic cryptography curve
C. error correcting code
D. none of the above

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