SC

No. of printed pages : 02

(27) SEAT No._____ Sardar Patel University

External Examination (CBCS)

B. Sc. VIth Semester (Information Technology)

US06CINT05 : Information Security

3rd April, Wednesday - 2019

Time : 10:00 am to 01:00 pm Total Marks :70

Q.1 Select the appropriate option. 10

1. A process that designed to detect, prevent or recover from a security Attack is known as _____.
   (a) Security Service (b) Security Mechanism
   (c) Security Attack (d) None of these
2. The _____ attack attempts to alter system resources or affect their operation.
   (a) Passive (b) Active (c) Security (d) None of these
3. _____ is the original message or data that is involved into the algorithm as input.
   (a) Ciphertext (b) Simpletext (c) Plaintext (d) None of these
4. The full form of ECB is _____.
   (a) Electronic Codebook (b) Electronic Cipherbook
   (c) Elective Codebook (d) None of these
5. The key used in conventional encryption is referred as a _____.
   (a) Primary key (b) Public key (c) Secret key (d) None of these
6. If AES is designed with 128 bits size of data block and 12 no. of rounds then it requires _____ bits key size.
   (a) 128 (b) 192 (c) 256 (d) None of these
7. A _____ is one that is used only for the duration of one session.
   (a) secret key (b) private key (c) session key (d) none of these
8. In _____ signature there is a one-to-many relationship between a signature and documents.
   (a) Digital (b) Conventional (c) Fingerprint (d) None of these
9. In_____ IPSec protects the original IP header.
   (a) Tunnel mode (b) Active mode
   (c) Transport mode (d) None of these
10. A _____ firewall filters at the application layer.
    (a) packet filter (b) proxy (c) system (d) none of these

Q.2 Answer the following questions. **(Attempt any TEN)** 20

1. Define passive attack with its types.
2. Define security services. Also write down its categories.
3. List the fundamental principles of cryptography.
4. Explain in brief Triple DES.
5. Define: Logic Bomb and Backdoor.

6. List various types of attacks performed on encrypted message.
7. List the various security services.
8. How HMAC is generated?
9. List the various ways for public key distribution.
10. Draw the diagram for transport mode.
11. Explain IPSec protocol in brief.
12. Write a difference between Packet-filter firewall - Proxy firewall.

Q.3 [a] Write a detail note on Network Security Model. 5

[b] Explain transposition cipher in detail. 5

OR

Q.3 [a] Explain conventional encryption principles. 5

[b] What is cryptography? Specify the components of cryptography. Also define its categories. 5

Q.4 [a] Write a detail note on Data Encryption Standard. 5

[b] Explain Intruder Behavior Patterns with at least two examples. 5

OR

Q.4 [a] Explain different cipher modes in detail. 5

[b] Explain Virus Structure in detail. 5

Q.5 Explain Entity Authentication Methods in detail. 10

OR

Q.5 List the key management methods and explain any two of them in detail. 10

Q.6 [a] List and explain SSL protocols in detail. 5

[b] What is firewall? List the types of firewall and explain any one of them. 5

OR

Q.6 [a] Write a brief note on needs of firewall. 5

[b] Explain various services performed by Pretty Good Privacy protocol. 5

----- X ----- X -----

(2)