19ITU23

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

B.Sc DEGREE EXAMINATION MAY 2022
(Fourth Semester)

Branch – **INFORMATION TECHNOLOGY**

CRYPTOGRAPHY

Time: Three Hours Maximum: 75 Marks

SECTION-A (10 Marks)

Answer **ALL** questions
ALL questions carry **EQUAL** marks (10 x 1 = 10)

1 Which of the following is not a principle of data security?
(i) Data Confidentiality (ii) Data Integrity
(iii) Authentication (iv) None of the above

2 Which of the following attacks is a passive attack?
(i) Masquerade (ii) Modification of message
(iii) Denial of service (iv) quadratic ciphers

3 In cryptography, the order of the letters in a message is rearranged by _____.
(i) transposition ciphers
(ii) substitution ciphers
(iii) both transpositional ciphers and substitution ciphers
(iv) quadratic ciphers

4 Cryptanalysis is used_____
(i) to find some insecurity in a cryptographic scheme
(ii) to increase the speed
(iii) to encrypt the data
(iv) to make new ciphers

5. The first line of HTTP request message is called ____.
(i) Request line (ii) Header line
(iii) Status line (iv) Entity line

6 How many modes of operations are there in DES and AES?
(i) 4 (ii) 3
(iii) 2 (iv) 5

7 Which protocol is used to convey SSL related alerts to the peer entity?
(i) Alert protocol (ii) Handshake protocol
(iii) Upper – Layer protocol (iv) Change cipher spec protocol

8 The number of tests required to break the DES algorithm are _____.
(i) $2.8x10^{14}$ (ii) $4.9x10^{9}$
(iii) $1.84x10^{19}$ (iv) $7.2x10^{16}$

9 Network layer firewall has two sub- categories as _____.
(i) State full firewall and stateless firewall
(ii) Bit oriented firewall and packet firewall
(iii) Frame firewall and packet firewall
(iv) Network layer firewall and session layer firewall

10 Which of the statements are not true to classify VPN systems?
(i) Protocols used for tunneling the traffic
(ii) Whether VPNs are providing site-to-site or remote access connection.
(iii) Securing the network from bots and malwares.
(iv) Levels of security provided for sending and receiving data privately.

Cont...

SECTION - B (25 Marks)

Answer **ALL** questions
ALL questions carry **EQUAL** Marks (5 x 5 = 25)

11 a Discuss the needs of security in Cryptography.

OR

b Explain the principles of security.

12 a Evaluate Symmetric key Cryptography with example.

OR

b Enumerate the International Data Encryption Algorithm.

13 a Explain the RSA algorithm.

OR

b Discuss about Digital Certificate.

14 a Explain Time Stamping Protocol with example.

OR

b Discuss about Authentication Tokens.

15 a Write a brief note on Firewalls.

OR

b Explain Intrusion.

SECTION -C (40 Marks)

Answer **ALL** questions
ALL questions carry **EQUAL** Marks (5 x 8 = 40)

16 a Explain the security approach in cryptography.

OR

b Elaborate on Steganography.

17 a Trace out Data Encryption standard.

OR

b Explain AES.

18 a Briefly explain about Asymmetric key cryptography.

OR

b Trace out the Digital Signature with example.

19 a Compare and explain SSL vs SET.

OR

b Explain the biometric and token based authentication security.

20 a Explain the Virtual private networks in Cryptography.

OR

b Elucidate IP security with example.

Z-Z-Z END