TOTAL PAGES : 2

23ITU526

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

BSc DEGREE EXAMINATION MAY 2025
(Fifth Semester)

Branch – **INFORMATION TECHNOLOGY**

CRYPTOGRAPHY

Time: Three Hours | Maximum: 50 Marks

SECTION-A (5 Marks)
Answer **ALL** questions
ALL questions carry **EQUAL** marks (5 x 1 = 5)

1 The codified language can be termed
(i) clear text (ii) unclear text
(iii) code text (iv) cipher text

2 In IDEA, the key size is _____.
(i) 128 bytes (ii) 256 bytes
(iii) 128 bits (iv) 256 bits

3 The _____ of the user should never appear in a certificate.
(i) public key (ii) private key
(iii) organization name (iv) name

4 Determining the identity of a user is called _____.
(i) authentication (ii) authorization
(iii) confidentiality (iv) access control

5 Key management in IPSec is done by_____
(i) tunnel mode (ii)transport mode
(iii) IKE (iv) ESP

SECTION - B (15 Marks)
Answer **ALL** Questions
ALL Questions Carry **EQUAL** Marks (5 x 3 = 15)

6 a Explain the several approaches to implement its security model in organization.
OR
b Outline the Simple Columnar Transposition Technique.

7 a How can the same key be reused in triple DES?
OR
b Comparison between stream and block ciphers

8 a Outline the steps involved in working of AES.
OR
b Comparison between MAC and message digest

9 a Organize the various layers of TCP with neat diagram.
OR
b Describe the primary steps involved in Kerberos protocol.

10 a Sketch and explain the IP datagram formats and Fields.
OR
b Explain the architecture of VPN with neat diagram.

Cont...

SECTION -C (30 Marks)

Answer **ALL** questions

ALL questions carry **EQUAL** Marks (5 x 6 = 30)

11 a Discuss a few programs that attack computer systems to cause some damage.

OR

b Summarize the Diffie–Hellman key-exchange algorithm with an example.

12 a Sketch and Explain how does DES works with neat diagram.

OR

b Identify the objectives and operation involved in Blowfish algorithm.

13 a Analyze the some possible attack on RSA.

OR

b Elucidate the some important PKCS standards.

14 a Point out the technical details of SET process.

OR

b Categorize the various types of Authentication Token types in detail.

15 a Identify the possible configuration of Firewall

OR

b Elucidate the two main IPSec protocol in detail.

Z-Z-Z END