

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

BSc DEGREE EXAMINATION DECEMBER 2024
(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 In which security model, system is secure simply because nobody knows about its existence and contents?
(i) No Security (ii) Security through Obscurity
(iii) Host Security (iv) Network Security
- 2 DES encrypts blocks of ____ bits
(i) 32 (ii) 56
(iii) 64 (iv) 128
- 3 Requesting for a certificate results into the creation of a ____ file.
(i) PKCS#7 (ii) PKCS#9
(iii) PKCS#10 (iv) PKCS#12
- 4 SSL layer is located between ____ and ____.
(i) transport layer, network layer (ii) application layer, transport layer
(iii) data-link layer, physical layer (iv) network layer, data-link layer
- 5 Firewall is a specialized form of a ____
(i) bridge (ii) disk
(iii) printer (iv) router

SECTION - B (15 Marks)

Answer ALL Questions

ALL Questions Carry EQUAL Marks (5 x 3 = 15)

- 6 a Explain the salient features of the modern nature of attacks.
OR
b Compare substitution and transposition ciphers.
- 7 a How does the one-time initialization step work in AES?
OR
b State the idea behind meet-in-the-middle attack.
- 8 a Describe the advantages and disadvantages of symmetric and asymmetric-key cryptography.
OR
b. Summarize the attacks are attempted by attackers on RSA digital signatures.
- 9 a Comparison between static web page and dynamic web page.
OR
b Classify the various types of Biometric techniques in detail.
- 10 a Sketch and explain the basic concepts of TCP/IP protocol suite.
OR
b Explain the application and advantages of IPSec.

Cont...

SECTION -C (30 Marks)

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

- 11 a Summarize the principles related to the security.
OR
b Highlight the steps involved in Play fair encryption scheme.
- 12 a Categorize the different types of algorithm mode in detail.
OR
b Explain the principles of the IDEA algorithm.
- 13 a Point out the idea and requirement of Message Digest.
OR
b. Outline the several steps involved in digital certificate creation process.
- 14 a Justify the various sub protocols constitute the overall working with SSL.
OR
b Identify the steps to clear the text password.
- 15 a Examine the different types of firewall in network.
OR
b Categorize the various types Audit records and Intrusion Detection Systems in detail.

Z-Z-Z

END