19SSP40A

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

MSc(SS) DEGREE EXAMINATION MAY 2023
(Sixth Semester)

Branch – **SOFTWARE SYSTEMS (Five Years Integrated)**

DISCIPLINE SPECIFIC ELECTIVE – II : CRYPTOGRAPHY

Time : Three Hours Maximum 75 Marks

SECTION-A (10 Marks)
Answer **ALL** questions
ALL questions carry **EQUAL** marks **(10 x 1 = 10)**

1. _____ is the science and art of transforming messages to make them secure and immune to attacks.
(i) Cryptography (ii) Calligraphy
(iii) Cryptanalysis (iv) None of the above

2. The _____Cipher reorders the plaintext characters to create a cipher text.
(i) Substitution (ii) Transposition
(iii) Either (i) or (ii) (iv) Neither (i) nor (ii)

3. Which of the following ciphers is a block cipher?
(i) Caesar Cipher (ii) Vernam Cipher
(iii) Playfair Cipher (iv) None of the above

4. AES uses a _____ bit block size and a key size of _____ bits.
(i) 128; 128 or 256 (ii) 64; 128 or 192
(iii) 256; 128, 192, or 256 (iv) 128; 128, 192, or 256

5. Which of the following is a mode of operation for the Block ciphers in cryptography?
(i) Electronic Code Book (ECB) (ii) Cipher Block Chaining (CBC)
(iii) Counter (CTR) mode (iv) All of the above

6. The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
(i) Authenticated (ii) Joined
(iii) Submit (iv) Separate

7. Public-key cryptography is also known as?
(i) Asymmetric cryptography (ii) Symmetric cryptography
(iii) Both (i) and (ii) (iv) None of the above

8. A digital signature is a mathematical technique which validates?
(i) Authenticity (ii) Integrity
(iii) Non-repudiation (iv) All of the above

9. What does the acronym Dos stands for?
(i) Distributed denial of software (ii) Denial of Service
(iii) Distribution of Services (iv) Denial of Software

10. Ideally, what characters should you use in a password to make it strong?
(i) Letters and Numbers only (ii) Mixed Case Characters
(iii) Special Characters (iv) All of the above

Cont...

SECTION - B (25 Marks)

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

11. a. Discuss about Security Attacks and Security services offered.
OR
b. Elucidate about Substitution Techniques with examples.

12. a. What is block Ciphers technique in cryptography?
OR
b. Explain the structure of Advanced Encryption Standard.

13. a. Discuss about Cipher Feedback Mode with diagram.
OR
b. Explain Public Key Cryptography and list its advantages.

14. a. Discuss about Message Authentication Functions.
OR
b. Enumerate the importance of Digital Signatures.

15. a. Mention the criteria for a good Password Management.
OR
b. Mention the necessity of Firewall in Network Security.

SECTION -C (40 Marks)

Answer **ALL** questions
ALL questions carry **EQUAL** Marks **(5 x 8 = 40)**
Question no. 16 is compulsory

16. Explain any two Symmetric Cipher model with examples.

17. a. What is the structure of Data Encryption Standard?
OR
b. Analyze the structure of Advanced Encryption Standards and comment on why it makes it so strong?

18. a. List the various phases of RSA algorithm.
OR
b. Elucidate about Diffie-Hellman Key Exchange with example.

19. a. Discuss about HMAC Algorithm.
OR
b. Elucidate NIST Digital signature algorithm.

20. a. Who are called Intruders and comment on how to detect intruders?
OR
b. What are Viruses and mention its threats. How to protect our systems from it?

Z-Z-Z END