19SSP40A

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

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

Branch – **SOFTWARE SYSTEMS** (Five years integrated)

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 defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information?
   (i) Cyber attack (ii) Computer security
   (iii) Cryptography (iv) Digital hacking

2. Caesar Cipher is an example of
   (i) Poly-alphabetic Cipher (ii) Mono-alphabetic Cipher
   (iii) Multi-alphabetic Cipher (iv) Bi-alphabetic Cipher

3. The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key.
   (i) 12 (ii) 18 (iii) 9 (iv) 16

4. The 4×4 byte matrices in the AES algorithm are called?
   (i) States (ii) Words (iii) Transitions (iv) Permutations

5. In public key Cryptography _____ keys are used for encryption and decryption.
   (i) Same (ii) Different
   (iii) Encryption Keys (iv) None of the mentioned

6. Computation of the discrete logarithm is the basis of the cryptographic system.
   (i) symmetric cryptography (ii) asymmetric cryptography
   (iii) diffie-hellman key exchange (iv) secret key cryptography

7. When a hash function is used to provide message authentication, the hash function value is referred to as
   (i) Message Field (ii) Message Digest
   (iii) Message Score (iv) Message Leap

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

9. The intent of a _____ is to overkill the targeted server's bandwidth and other resources of the target website.
   (i) Phishing attack (ii) DoS attack
   (iii) Website attack (iv) MiTM attack

10. A firewall protects which of the following attacks?
    (i) Phishing (ii) Dumpster diving
    (iii) Denial of Service (DoS) (iv) Shoulder surfing

Cont...

SECTION - B (25 Marks)

Answer **ALL** questions

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

11 a. Appraise Various Security Mechanism that has to be followed in Computer Networks.

(OR)

b. Analyse Substitution Technique with suitable.

12 a. Discuss about Block Ciphers with an example.

(OR)

b. Determine the working concept of DES algorithm.

13 a. Explain the Principles of public key cryptosystems.

(OR)

b. Enumerate the operations of Cipher feedback mode and Counter Mode of Block Cipher Operation.

14 a. What is message authentication Code?

(OR)

b. Elucidate the working of Secure Hash Algorithm 512.

15 a. Appraise how Intrusion can be detected?

(OR)

b. Construct the purpose of installing a firewall in computer networks.

SECTION -C (40 Marks)

Answer **ALL** questions

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

(Q.No 16 Compulsory)

16 Mention the advantages and Disadvantages in using Transposition Techniques of encryption.

17 a. With neat sketch explain AES key expansion.

(OR)

b. Compare and contrast DES and AES.

18 a. Enumerate the advantages of RSA algorithm.

(OR)

b. Analyse Diffie-Hellman Key Exchange.

19 a. Assess HMAC algorithm.

(OR)

b. Determine the importance of Digital Signatures in maintain security.

20 a. Appraise any 10 malicious software and its attacks on computer system.

(OR)

b. Formulate password management process.

Z-Z-Z END