TOTAL PAGES: 2
19SSP40A

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

MSc DEGREE EXAMINATION MAY 2022
(Sixth Semester)

Branch – **SOFTWARE SYSTEMS (Five year 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 malicious software that runs its own code and modifies other programs.
   i) Virus ii) Spam iii) Spyware iv) Adware
2. Which of these is a part of network identification?
   i) UserID ii) Password iii) OTP iv) fingerprint
3. ___ encryption/decryption key known only to the party or parties that exchange secret messages.
   i) E-signature ii) Digital certificate iii) Private key iv) Security token
4. This is the inclusion of a secret message in otherwise unencrypted text or images.
   i) Masquerade ii) Steganography iii) Spoof iv) Eye-in-hand system
5. The DES algorithm has a key length of
   i) 128 Bits ii) 32 Bits iii) 64 Bits iv) 16 Bits
6. The 4×4 byte matrices in the AES algorithm are called
   i) States ii) Words iii) Transitions iv) Permutations
7. A digital signature is required ______
   i) for non-repudiation of communication by a sender
   ii) for all e-mail sending
   iii) for all DHCP server
   iv) for FTP Transactions
8. MAC is a __________
   i) one-to-one mapping ii) many-to-one mapping
   iii) onto mapping iv) none of the mentioned
9. Which of the following is not a type of peer-to-peer cyber-crime?
   i) Phishing ii) Injecting Trojans to a target victim
   iii) MiTM iv) Credit card details leak in deep web
10. In password protection, this is a random string of data used to modify a password hash.
    i) Sheepdip ii) Salt iii) Bypass iv) Dongle

SECTION – B (25 Marks)

Answer **ALL** questions
All Questions carry **EQUAL** marks (5 x 5 =25)

11. a. Compare security attacks and security services.

OR

b. Explain the outline of Specific security mechanisms.

12. a. Contrast the term Encryption and Decryption in detail.

OR

Cont...

b. Explain the various principles of Block Ciphers.

13. a. Specify the principles of public key cryptosystems.

OR

b. Explain Diffie-Hellman Key Exchange.

14. a. Write short notes on Digital Signatures.

OR

b. Explain HMAC algorithm.

15. a. Give a detailed note on Password Management.

OR

b. Give a brief note on Virus countermeasures.

SECTION – C (40 Marks)

Answer **ALL** questions

All Questions carry **EQUAL** marks (5 x 8 =40)

Question no.16 is compulsory

16. Explain Classical Encryption Techniques in detail.

17. a. Discuss Data Encryption Standard in detail.

OR

b. Explain AES Structure and Transformation Functions in detail.

18. a. Explain the working of RSA Algorithm.

OR

b. Analyze the properties of Stream Cipher and explain the working of stream cipher with a neat diagram.

19. a. Evaluate the properties of MAC and explain it.

OR

b. Discuss cryptographic hash functions in detail.

20. a. Explain Intrusion detection in detail.

OR

b. Outline in detail about Firewalls and its security evaluation.

Z-Z-Z END