(FOR THE CANDIDATES ADMITTED   SUBJECT CODE 21UIT517

DURING THE ACADEMIC YEAR 2021 ONLY)   REG.NO. :

N.G.M.COLLEGE (AUTONOMOUS) : POLLACHI
END-OF-SEMESTER EXAMINATIONS : NOVEMBER 2023

B.Sc-INFORMATION TECHNOLOGY   MAXIMUM MARKS: 70

SEMESTER : V   TIME : 3 HOURS

PART - III
21UIT517- INFORMATION SECURITY
SECTION - A   (10 X 1 = 10 MARKS)

ANSWER THE FOLLOWING QUESTIONS.
MULTIPLE CHOICE QUESTIONS.   **(K1)**

1. The principle of _____ ensure that only the sender and the intended receipts have access to the contents of a message.

  (a) Confidentiality   (b) Authentication   (c) Integrity   (d) Access control

2. DES encrypts blocks of _____ bits.

  (a) 32   (b) 56   (c) 64   (d) 128

3. In asymmetric key cryptography, _____ keys are required per communicating parties.

  (a) 2   (b) 3   (c) 4   (d) 5

4. A _____ can issue digital certificates.

  (a) government   (b) Shopkeeper   (c) bank   (d) CA

5. SSL works between _____ and _____.

  (a) web browser, application server   (b) web server, application server

  (c) web browser, web server   (d) network layer, data link layer

ANSWER THE FOLLOWING IN ONE (OR) TWO SENTENCES   **(K2)**

6. What is denial of service attack?

7. Define: Stream cipher.

8. What is meant by collision?

9. Expand: (i) CSR   (ii) PKCS

10. What is electronic money?

SECTION – B **(5 X 4 = 20 MARKS)**

ANSWER EITHER (a) OR (b) IN EACH OF THE FOLLOWING QUESTIONS. (K3)

11. a) Describe the security attacks in general view.

(OR)

b) Examine the possible types of attacks.

12. a) Discuss key aspects of "Blowfish'.

(OR)

b) Describe the working principles of DES.

13. a) Discuss in detail about RSA algorithm.

(OR)

b) Write a note on knapsack algorithm.

14. a) Describe digital certificates. Explain the concept of digital certificates.

(OR)

b) Examine the public key cryptography standards.

15. a) Show the functionality of time stamping protocol.

(OR)

b) List and explain the types of electronic money.

SECTION - C **(4 X 10 = 40 MARKS)**

ANSWER ANY FOUR OUT OF SIX QUESTIONS
(16th QUESTION IS COMPULSORY) **(K4 (Or) K5)**

16. Distinguish between symmetric and asymmetric key cryptography.

17. Summarise the transposition techniques in detail.

18. Elaborate the IDEA. How IDEA works?

19. Discuss briefly the of asymmetric key cryptography.

20. Explain about private key management.

21. Determine the E-mail security with examples.

****

21UIT517

ETHICAL PAPER