(NO. OF PAGES: 2)

(FOR THE CANDIDATES ADMITTED **22UIT514**

DURING THE ACADEMIC YEAR 2022 ONLY) **REG.NO. :**

N.G.M.COLLEGE (AUTONOMOUS) : POLLACHI

END-OF-SEMESTER EXAMINATIONS : NOVEMBER 2024

B.Sc. (IT) **MAXIMUM MARKS: 50**

SEMESTER: V **TIME : 3 HOURS**

PART - III

INFORMATION SECURITY

SECTION – A (10 X 1 = 10 MARKS)

ANSWER THE FOLLOWING QUESTIONS.
(Objective Questions with four Multiple Choices) **(K1)**

1. Caesar cipher is an example of

(a) Substitution cipher (b) Transposition cipher

(c) Substitution as well as transposition (d) Vernam cipher

2. DES encrypts blocks of _______bits.

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

3. MAC is ________ a message digest.

(a) same as (b) different from (c) subset of (d) not a

4. The _____ standard defines the structure of a digital certificates.

(a) X.500 (b) TCP/IP (c) ASN.1 (d) X.509

5. SET uses the concept of _________.

(a) Double signature (b) Dual signature

(c) Multiple signature (d) Single signature

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

6. Define: Virus.

7. Expand: IDEA.

8. What is a birthday attack?

9. Give any two services of a registration authority.

10. What is electronic money?

(CONTD …. 2)

ETHICAL PAPER

SECTION – B (5 X 3 = 15 MARKS)

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

11. a) Examine the plain text and cipher text.

(OR)

b) Explain stegnography.

12. a) Summarize the types of symmetric key algorithms.

(OR)

b) Write a short note on RC5.

13. a) Discuss the history of asymmetric key cryptography in brief.

(OR)

b) Give an insight on Elliptic curve cryptography.

14. a) What is the role of a CA and a RA?

(OR)

b) Investigate the PKIX services.

15. a) What is the significance of the time stamping protocol?

(OR)

b) Compare SSL versus SET.

SECTION – C (5 X 5 = 25 MARKS)

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

(K4 (Or) K5)

16. a) Describe in detail about substitution techniques.

(OR)

b) Discuss on symmetric and asymmetric key cryptography.

17. a) Explain the working principle of DES encryption algorithm.

(OR)

b) Examine the Blowfish encryption algorithm.

18. a) Determine the working principle of RSA algorithm.

(OR)

b) Illustrate the concept of message digests.

19. a) Explain the typical contents of a digital certificate.

(OR)

b) Describe the mechanisms of protecting the private key of a user.

20. a) Explain the SSL handshake protocol.

(OR)

b) Discuss about Preety Good Privacy.

****