



A Charutar Vidya Mandal's Institution
V. P. & R. P. T. P. SCIENCE COLLEGE

(AUTONOMUS) (Grant-in-Aid)

Affiliated to Sardar Patel University

VALLABH VIDYANAGAR-388120



Bachelor of Science (Semester V) Internal Examination-2025

US05SEMTH02: Basics of Cryptography

Date: 26-09-2025, (Friday)

Time: 10:45 am to 11:45 am

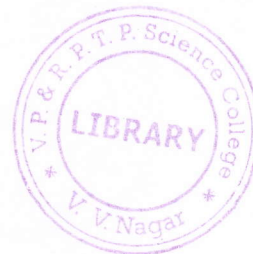
Total marks: 20

NOTE: The symbols used in this paper have usual meaning unless specified.

Q. 1 Choose the most appropriate answer.

[05]

- (1) What does cryptanalysis refer to?
 - (a) Generating random numbers
 - (b) Breaking cryptographic codes
 - (c) Encrypting data
 - (d) Storing large data sets
- (2) Hill Cipher is based on:
 - (a) Prime factorization
 - (b) Matrix multiplication
 - (c) Polynomial equations
 - (d) Random number generation
- (3) What is the main idea of a permutation cipher?
 - (a) Replace letters with numbers
 - (b) Rearranging the order of letters in plaintext
 - (c) Add a fixed key to each letter
 - (d) Use random numbers for encryption
- (4) What is the value of $15 \times 7 \text{ mod } 26$?
 - (a) 3
 - (b) 1
 - (c) 25
 - (d) 27
- (5) What is the key difference between a TRNG and a PRNG?
 - (a) TRNG is faster than PRNG
 - (b) TRNG is based on physical processes; PRNG is algorithmic
 - (c) PRNG uses quantum physics
 - (d) There is no difference
- (6) One-Time Pad key = 11010110, plaintext = 10110011. What is the ciphertext?
 - (a) 01100101
 - (b) 11100101
 - (c) 11110101
 - (d) 00100100



Q. 2 (A) Define encryption and decryption process of Shift cipher. Let the key be $k = 6$, and the plaintext is "computer" then encrypt the plaintext using shift cipher. [3]

(B) Encrypt the following plaintext using Hill Cipher. Plaintext: "MONDAY". Use matrix $\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$. After finding ciphertext decrypt the ciphertext using the same cipher. [4]

OR

Q. 2 (P) Define encryption and decryption process of Affine cipher. Let the key be $k = (a, b) = (3, 5)$, and the plaintext is "cipher" then encrypt the plaintext using Affine cipher. [4]

(Q) Encrypt the following plaintext using permutation cipher. Plaintext: "Everything you can imagine is real" Use permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}$. [3]

Q. 3 (A) Introduce Stream and Block ciphers. Write the difference between them. [4]

(B) Discuss the relation between Modulo 2 addition and XOR operation corresponding to stream cipher. [3]

OR

Q. 3 (P) Explain encryption and decryption process of stream cipher. Also prove that encryption and decryption function of stream cipher are same function. [4]

(Q) Explain Random Number Generators. [3]

ALL THE BEST

Seat No:

Supervisor's sign

Bachelor of Science (Semester V) Quiz-2025
US05SEMTH02: Basics of Cryptography

Date: 26-09-2025 (Friday)

Time: 10 minutes

Total marks: 05

NOTE: The symbols used in this paper have usual meaning unless specified.

Check whether the following statements are true or false. Write your answer in the box. [05]

- (1) In symmetric cryptography, the same key is used for both encryption and decryption. []
- (2) Affine Cipher combines both multiplication and addition in its encryption formula. []
- (3) Stream ciphers encrypt data one bit or byte at a time, rather than in blocks. []
- (4) Pseudorandom Number Generators (PRNGs) are completely unpredictable without knowledge of the seed. []
- (5) The One-Time Pad is perfectly secure only if the key is reused multiple times. []

All The Best

