

TILAK MAHARASHTRA VIDYAPEETH, PUNE
MASTER OF SCIENCE (M.Sc) in COMPUTER APPLICATIONS
EXAMINATION : DECEMBER - 2025
SEMESTER – III

Sub : Cryptography and Network Security (MSC24-307)

Date : 29/12/2025

Total Marks : 60

Time: 2.00 pm to 4.30 pm

Instruction:

1. All questions are compulsory unless and otherwise stated.
2. Bold figures to the right of every question are the maximum marks for that question.
3. Candidates are advised to attempt questions in order.
4. Answers written illegibly are likely to be marked zero.
5. Use of scientific calculators, Log tables, Mollier Charts is allowed.
6. Draw neat and labelled diagram wherever necessary.

Q. 1. Answer the following in 2 - 3 lines. (Any 5)

(10)

1. What is stream cipher?
2. Define the term diffusion?
3. What is S-Box operation?
4. What is co-prime number?
5. Write a short note on CMAC.
6. Explain the working of playfair cipher.
7. What is circular left shift?

Q. 2. Answer the following in short. (Any 4)

(20)

1. Explain various types of security attacks.
2. Explain the working of symmetric key cryptography.
3. Explain in detail Fistel Cipher structure with the help of neat diagram.
4. Explain the working on AES algorithm.
5. Explain the Euler's Theorem.
6. Explain in detail RSA algorithm.

Q. 3. Answer the following in detail. (Any 3)

(30)

1. Explain in detail model for network security with neat diagram.
2. Explain in detail Blowfish algorithm.
- Solve the following equations using CRT
3. a. $4X \equiv 5 \pmod{9}$
b. $2X \equiv 6 \pmod{20}$
4. What are the advantages and disadvantages of a digital certificate?
5. What are the different types of authentication used in wireless security?
