

TILAK MAHARASHTRA VIDYAPEETH, PUNE
MASTER OF SCIENCE (M.Sc) in COMPUTER APPLICATIONS
EXAMINATION : MAY/JUNE - 2026

SEMESTER – III

Sub : Cryptography and Network Security (MSC24-307)

Date : 4/06/2026

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 Caesar cipher?
2. What is transposition technique?
3. Define the term confusion?
4. What is feistel round?
5. What is P-Box operation?
6. What is prime number?
7. What are Trapdoor one-way functions?

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

(20)

1. How Digital Signature Works?
2. Explain in detail Elliptic Curve Cryptography.
3. How does HMAC work?
4. Does Euler's theorem hold true for $a=10$ and $n=11$?
5. Explain Fermat's little theorem.
6. Explain the working of A-Symmetric key cryptography.

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

(30)

1. Explain the the Chinese Remainder Theorem.
 2. What is significance of Euler's Totient Function?
 3. Explain the AES structure in detail.
 4. Explain in detail working of Tripple DES.
 5. Explain the block cipher principals.
-