RAN-2511000903022005

RAN-2511000903022005

S.Y. B.C.A (Sem. - III) Examination November - 2025

Cryptography and Secure Communication (TH) (MJ-2)

(Paper - 304-04)

Time: 1 Hour] **[Total Marks: 25**

સૂચના : / Instructions

(1) ઉપરોક્ત દર્શાવેલ વિગતો ઉત્તરવહી પર અવશ્ય લખવી.
Fill up strictly the above details on your answer book

Seat No.:

Student's Signature

SET- II

Q. 1 a) Do as Directed (Any Four) **[4]**

1) Which of these is a block cipher?
   i) RSA ii) AES
   iii) Diffie-Hellman iv) MD5
2) Which hashing algorithm produces a 160-bit output?
   i) SHA-1 ii) MD5
   iii) SHA-256 iv) AES
3) What does an SSL certificate contain?
   i) Private Key ii) Public Key
   iii) Shared Password iv) Hash Function
4) Collision attacks target _____ .
   i) Hash Function ii) RSA encryption
   iii) TLS Handshake iv) Digital Signature
5) The Caesar Cipher is an example of _____.
   i) Asymmetric encryption
   ii) Substitution cipher
   iii) Transposition cipher
   iv) Hashing

b) Answer in Short (Any Four) **[4]**

I. What is the main purpose of cryptography?
II. State one limitation of symmetric key encryption.
III. What is a man-in-the-middle (MITM) attack?
IV. Write two advantages of using TLS over SSL.
V. What is a hash function? Give one use.

Q. 2 Answer the Following. **[5]**

a) Discuss the architecture and importance of PKI in secure communications.

OR

a) Explain SSL/TLS protocols and their role in web security.

b) Discuss the role of cryptography in cyber security**.** **[4]**

Q. 3 **Write the following (Any Two)** **[8]**

a) Compare MD5 and SHA-256 hashing algorithms in terms of security and efficiency.
b) Write a Note on Brute Force Attack with an example.
c) How can end-to-end encryption be achieved in emails?

———