RAN-1911000701030002

RAN-1911000701030002

M.Sc.(ICT) (Sem. - I) Examination November - 2025

Information Security and Applications (Paper - 103)

Time: 3 Hours] **[Total Marks: 70**

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

Q.1. Answer the following questions in short. (Any Seven) **[14]**

1) Differentiate between active and passive attacks.
2) What is S/MIME?
3) Encrypt "EDUCATION" by using playfair cipher with key "MONARCHY".
4) What is the encryption formula in RSA?
5) Explain concept of rotor machine.
6) What is the purpose of a digital signature?
7) Explain with an example how the transposition cipher works.
8) What is the difference between threat and vulnerability?
9) What is authentication? Explain any two biometric techniques of authentication.

Q.2. Answer following questions. (Any Two) **[14]**

1) Explain functionality of HTTPS protocol with diagram.
2) Explain various key distribution scenario in detail.
3) Differentiate between transport and tunnel mode of operation in IPSec.

Q.3. Answer following questions. (Any Two) **[14]**

1) Explain in brief classical cryptography. Write a note on stagnography.
2) Compare and contrast symmetric and asymmetric key cryptography. Explain one public key cryptography algorithms.
3) Explain AES algorithm in detail. Compare its performance with DES.

Q.4. (A) Write short notes. (Any 2) **[10]**

1) Digital Signature
2) Firewall
3) SHA

Q.4. (B) Explain in brief the concept of hashing for message authentication with example. **[04]**

Q.5. (A) Write Short Notes (Any 2) **[10]**

1) Email Security.
2) Web security challenges and solutions.
3) Kerberos.

Q.5 (B) Explain in brief the concept of DMZ. **[04]**