R A N - 5 8 3 5

RAN-5835

M.C.A. (Sem. IV) Examination

March / April - 2019

Paper : 404 Cryptography

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

સૂચના : / Instructions

નીચે દર્શાવેલ ☛ નિશાનીવાળી વિગતો ઉત્તરવહી પર અવશ્ય લખવી.
Fill up strictly the details of ☛ signs on your answer book

Name of the Examination:

☛ **M.C.A. (Sem. IV)**

Name of the Subject :

☛ **Paper : 404 Cryptography**

Subject Code No.: 5 8 3 5

Seat No.:

Student's Signature

Q-1. (A) Answer the following in brief (Any 2): [06]

1. List out the goals of Cryptography.
2. List out and explain different types of ciphers
3. The word "friends" is encrypted into "uirvmwh". What does "vwfxzgrlm" come out to?

Q-1. (B) Answer the following (Any 2): [08]

1. Explain LFSR sequence & compute it for IV = 100110
2. Explain Euler's Totient Theorem with example.
3. Write a short note on Finite fields.

Q-2. Answer the following: [14]

1. Explain Cipher Block Chaining Mode.
2. Difference between Symmetric Key Cryptography and Public Key Cryptography.

-- OR --

2. Explain Counter mode.

Q-3. Attempt any 2 of the following: [14]

1. Write a short note on RC4.
2. Write a short note on Differential Cryptanalysis.
3. Write a short note on DES.

Q-4. Attempt any 2 of the following: [14]

1. How does Diffie-Hellman differ from ElGamel? Discuss similarities as well.
2. Explain the importance of collision resistance in Hash Functions with example.
3. What are Digital Signatures? Explain with example.

Q-5. Attempt any 2 of the following: [14]

1. Write a short note on Shamir's Three Pass Protocol.
2. Write a short note on Kerberos.
3. Explain IBM Common Cryptographic Architecture.
