M.Sc. - II (Computer Science) (NEP Pattern) Semester-IV

04MSCCS05 - Elective-I Paper-V : Advanced Cryptography

P. Pages : 2 **GUG/S/25/16334**

Time : Three Hours * 3 9 2 8 * Max. Marks : 80

Notes : 1. All questions are compulsory and carry equal marks.
2. Draw neat and labelled diagram wherever necessary.
3. Avoid vague answer and write specific answers related to questions.

Either :

1. a) Explain Data Encryption Standard (DES). in detail. **8**

b) Write a note on – **8**

i) Rotor Machine

ii) Steganography.

OR

c) What are the fundamental security design principles? Explain. **8**

d) Write about Polynomial Arithmetic. **8**

Either :

2. a) Explain AES structure. Also write about AES implementation. **8**

b) Write a note on – **8**

i) Multiple Encryption

ii) Triple DES

OR

c) Write about Cipher Block Chaining Mode & Counter Mode. **8**

d) Explain : **8**

i) Electronic Codebook

ii) RAC.

Either :

3. a) Write and Explain RSA algorithm. **8**

b) Write the principles of public-key cryptosystems. **8**

OR

c) Explain pseudorandom number generation based on an asymmetric cipher. **8**

d) Explain **8**

i) Elliptic Curve Arithmetic

ii) Elliptic Curve Cryptography.

Either :

4. a) List and explain application of cryptographic hash function. **8**

b) Explain authenticated encryption GCM in detail. **8**

OR

c) Write about NIST Digital signature algorithm. **8**

d) What are the requirement for message authentication code (MACs). **8**

5. All are compulsory.

a) Write a short note on Security Attacks. **4**

b) Explain True Random Number Generators. **4**

c) What are the block cipher modes of operation. **4**

d) What is Kerberos? Explain. **4**

****