Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

I SEMESTER M.TECH. COMPUTER SCIENCE AND INFORMATION SECURITY

END SEMESTER EXAMINATIONS, FEBRUARY 2022

SUBJECT: ADVANCED CRYPTOGRAPHY [CSE 5171]

REVISED CREDIT SYSTEM
14. 02. 2022

Time: 75 minutes MAX. MARKS: 20

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitably assumed.

1A. Find all the elements of $<Z^*_{15},*>$ and generate all the cyclic subgroups of the group $<Z^*_{15},*>$. Also, find order of each element. **5M**

1B. Find the primality of 1917 and 117 using Miller-Rabin test with all intermediate results assuming the base as 2. **3M**

1C. Compare and contrast the flat key distribution center based and hierarchical key distribution center based key management techniques. **2M**

2A. Compare and contrast the symmetric key cipher based, asymmetric key cipher based and keyed-hash function based challenge response authentication approaches with neat diagrams. **5M**

2B. Illustrate elliptic curve cryptography key generation, encryption and decryption process for the following. Consider the curve $y^2=x^3+7$ (mod 17) in GF(17) and e1={5,8}, d=2, and plaintext {5,8}. **3M**

2C. Compare and contrast the OAEP and RSA operations. **2M**

****