Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

V SEMESTER B.TECH.
(Computer and Communication Engineering)
MAKE-UP EXAMINATIONS, JAN-FEB 2022
SUBJECT: INFORMATION SECURITY [ICT 3172]
REVISED CREDIT SYSTEM
22/2/2022

Time: 3 Hours MAX. MARKS: 20

Instructions to Candidates:

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

1A. Decrypt the message "HDSIOEYQOCAA" using 3*3 Hill cipher with the Key: "CIPHERING". Encrypt the text decrypted above using Columnar Transposition cipher with key- "BENIGN". Also comment on the differences observed in the two ciphering techniques used. **5**

1B. Suppose that the two parties A and B wish to set up a common Diffie-Hellman Key. Users agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and Party B chooses 5 as their respective secrets. Compute the shared secret key. Using the shared secret key obtained above decrypt the message "ISNNIMUTDAYORICY" using Rail fence Cipher. **3**

1C. Answer with respect to block ciphers. **2**

i. Explain that the Electronic Code Book (ECB) mode is not a secured mode of encryption and highlight the problems with this mode.

ii. Differentiate between Linear and Differential cryptanalysis attacks on block ciphers.

2A. Compare the Message Authentication Code computation and Master Secret Generation in SSL and TLS with respect to efficiency. Also elucidate how TLS produces variable length key material? List the cryptographic secrets needed to be recomputed after session resumption with suitable reasoning. **5**

2B. What are third and fourth generation firewalls? How fourth generation firewalls are different from their predecessor? **3**

2C. What is the role of a Certification Authority? Mention the different reasons for revoking a digital certificate. **2**