Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

V SEMESTER B.TECH.
(Computer and Communication Engineering)
END SEMESTER EXAMINATIONS, DEC 2021/JAN 2022
SUBJECT: INFORMATION SECURITY [ICT 3172]
REVISED CREDIT SYSTEM
23/12/2021

Time: 3 Hours MAX. MARKS: 20

Instructions to Candidates:

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

1A. David uses ElGamal for creating a secure system. Given the prime p=23, primitive root e_1 = 5, random number r=9 and private key d =3. **5**

i. Encrypt the message "7".
ii. Decrypt the cipher text to get back the plain text.
iii. Calculate the two signatures S_1 and S_2.
iv. Show the verification process for the above calculated signatures.
v. Differentiate based on the security service, offered by the above two security mechanisms presented in the scenario, with suitable examples.

1B. Eve gains access to sender's PC for a brief period of time. She encrypts her plain text using the 2 algorithms in the PC and obtains the following answers **3**

Algorithm 1 -> Input: WR; Output: JS
Algorithm 2 -> Input: ET; Output: WC
Using the given scenario answer the following questions:

i. Name and exemplify on the attack launched.
ii. Which amongst the two algorithms gives the ideal keypair for Affine cipher? Justify
iii. Decrypt the message "DHBDUEKDSMVFHS" using the ideal keypair obtained above by employing Affine cipher.

1C. You are hired as a security engineer in an IT organization. Address the following issues with suitable examples. **2**

i. The importance of having accountability in a system.
ii. Difference between threat, attack and vulnerability.
iii. The importance of having multifactor authentication.
iv. Effect of active and passive attack on system resources.

2A. How Challenge Response protocols are different from Zero Knowledge protocols? Elucidate how symmetric and asymmetric key ciphers are helpful in entity authentication by providing various services? **5**

2B. Suppose, an organization is using RSA with modulus *n* and public exponent *e*. One day they are hacked, and their private key *d* becomes known to the attackers. Bob, the security consultant, suggests that instead of regenerating the new keys completely from the scratch, only the new exponents *e', d'* need to be re-computed, leaving the modulus *n* unchanged. Is this safe or not? Explain. **3**

2C. Which are the three cases, where the security of the MAC is vulnerable to threat and attacks? **2**