Reg. No.										

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

DEPARTMENT OF MECHATRONICS

VII SEMESTER B.TECH. (MECHATRONICS)

END SEMESTER EXAMINATIONS, NOVEMBER 2022

SUBJECT: PRINCIPLES OF CRYPTOGRAPHY [MTE 4058]

(Date: November 28, 2022)

Time: 3 Hours **MAX. MARKS: 50**

Instructions to Candidates:

- Answer **ALL** the questions.

Q. No		M	CO	PO	LO	BL
1(a).	Explain in detail how a "meet-in-the-middle" attack with a two-bit key is feasible with the 2DES (Double Data Encryption Standard) encryption technique.	4	1	2	2	5
1(b).	Employ Euler's theorem to find a solution to the problem $3^{401} mod\ 11$ to use the RSA cryptosystem for internet communications.	3	2	1	1	3
1(c).	In an RSA cryptosystem, a participant uses two prime numbers $p = 5$ and $q = 7$ to generate his public and private keys. Evaluate the private key d if the public key $e = 11$. Also generate the ciphertext C if the plaintext $M = 2$.	3	3	2	4	5
2(a).	List the various primitive functions that can be applied in each round of MD5 hash algorithm. Use different combinations of the binary values of the word buffers $'a', 'b', 'c', and\ 'd'$ to evaluate each primitive function.	4	4	1	1	5
2(b).	Find the GCD of two numbers, such as $a = 129171816$ and $b = 31343824$, using the Euclidean algorithm.	3	2	1	1	3
2(c).	Examine the security threats that provide a "threat to confidentiality," "threat to integrity," and "threat to availability."	3	1	2	2	4
3(a).	Solve $3^{30} mod\ 13$ by applying the following property of Modular arithmetic. $$[(a\ mod\ n) \times (b\ mod\ n)] mod\ n = (a \times b) mod\ n$$	4	2	1	1	3
3(b).	If the plaintext is "COLLEGE WILL OPEN ON MONDAY" and the key is "STUDENTS WILL GO TO COLLEGE," then generate the ciphertext and then the decoded text using the One Time Pad technique. Prove that the plaintext and the decoded text are identical.	3	1	1	1	5
3(c).	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 7 and primitive root = 3. If Alice's secret key is 3 and Bob's secret key is 4, prove that both Alice and Bob exchanged the same secret key.	3	3	2	4	5
4(a).	Develop a message authentication system that provides confidentiality and authenticity. The designed authentication should be performed in two levels such as authentication tied to plaintext and authentication tied to ciphertext.	4	4	4	6	6
4(b).	If the plaintext is "KILL CORONA VIRUS AT ELEVEN AM TOMORROW" and the key is (4 3 1 2 5 6 7), then create the ciphertext	3	1	1	1	5

	and subsequently the decoded text using the Columnar Transposition technique. Compare the decoded text to the plaintext.					
4(c).	Classify AES-128 and AES-192 with respect to "Key size", "Plaintext block size", "Number of Rounds", "Round Key Size", and "Expanded Key Size".	3	2	2	2	4
5(a).	Draw a model for the AES-256 encryption, decryption, and key generation. Also mention the plaintext block size, number of rounds, expanded key size, and round key size for the AES-256 model as well.	4	2	2	2	3
5(b).	Draw a model for the S-DES (Simplified Data Encryption Standard) encryption algorithm's key generation operation and explain the operation of each of the blocks using an appropriate example. P10 permutation = (3, 5, 2, 7, 4, 10, 1, 9, 8, 6) P8 permutation = (6, 3, 7, 4, 8, 5, 10, 9)	3	1	2	2	3
5(c).	Discuss the hardware and software efficiency of CTR (Counter) mode. Why, CTR mode is simpler than ECB (Electronic Code Book) and CBC (Cipher Block Chaining) modes?	3	1	2	2	6