BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI
(END SEMESTER EXAMINATION MO2022)

CLASS:	**MCA/IMSC**	**SEMESTER: III/IX**
BRANCH:	**MCA/IMH**	**SESSION: MONSOON**

SUBJECT: CA529 NETWORK SECURITY AND CRYPTOGRAPHY

TIME:	**03 Hours**	**FULL MARKS: 50**

INSTRUCTIONS:
1. The question paper contains 5 questions each of 10 marks and total 50 marks.
2. Attempt all questions.
3. The missing data, if any, may be assumed suitably.
***4*. Tables/Data handbook/Graph paper etc., if applicable, will be supplied to the candidates**

Q.1(a) Explain the goals of Cryptography [2]
Q.1(b) If the message is “HELLOWORLD” and the key sequence is “TBFRGFARFM,” then what will be the cipher text if we use One Time Pad to encrypt the message. [3]
Q.1(c) Explain different types of attacks on a Cryptosystem. [5]

Q.2(a) Explain the procedure used for Verifying Keys. [2]
Q.2(b) What are the differences between Public Key Cryptography and Private Key Cryptography? [3]
Q.2(c) Write a short note on Steganography. [5]

Q.3(a) What do you mean by Double Encryption. [2]
Q.3(b) Find the GCD of (161, 28) using Extended Euclidean Algorithm. [3]
Q.3(c) Explain the detailed working of Data Encryption Standards (DES) using a block diagram. [5]

Q.4(a) Explain the MD5 algorithm. [2]
Q.4(b) What are the different characteristics of a Hash Function [3]
Q.4(c) Explain the working of SHA – 256 using a block diagram. [5]

Q.5(a) In RSA, suppose p = 7 and q = 11 and the plain text message is 9. What will be the cipher text? [2]
Q.5(b) In Diffie – Hellman Key Exchange algorithm, Alice and Bob have chosen prime value = 17 and primitive root = 5. If Alice’s secret key is 4 and Bob’s secret key is 6, what will be the secret key they exchanged? [3]
Q.5(c) Write a short note on any one of the following: [5]

- Elliptic Curve Cryptography (ECC)
- Digital Signature Algorithm (DSA)

:::::25/11/2022:::::E