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

CLASS: BTECH **SEMESTER : V**
BRANCH: CSE **SESSION : MO/2022**

SUBJECT: IT330 CRYPTOGRAPHY AND NETWORK SECURITY

TIME: 3:00 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*. Before attempting the question paper, be sure that you have got the correct question paper.**
5. Tables/Data hand book/Graph paper etc. to be supplied to the candidates in the examination hall.

Q.1(a)	Define cryptanalysis.	[2]
Q.1(b)	Explain OSI security architecture in details.	[3]
Q.1(c)	Explain all types of active and passive attacks with example.	[5]
Q.2(a)	Define Euler's theorem and it's application.	[2]
Q.2(b)	Using Playfair cryptographic algorithm, encrypt this message: " BTECH FIFTH SEMESTER". Here key is "CRYPTOGRAPHY".	[3]
Q.2(c)	What is the purpose of the S-boxes in DES? Show that DES decryption is, in fact, the inverse of DES encryption.	[5]
Q.3(a)	Find the multiplicative inverse of each nonzero element in Z_5.	[2]
Q.3(b)	Explain Euclidean algorithm. Using this algorithm, determine gcd(24140,16762) .	[3]
Q.3(c)	With the help of an example, explain Diffie-Hellman Key Exchange.	[5]
Q.4(a)	Write short notes on SSL handshake protocol.	[2]
Q.4(b)	Differentiate between SSL (Security Socket Layer) and SET (Secure Electronic Transaction).	[3]
Q.4(c)	With the help of an example, explain RSA algorithm.	[5]
Q.5(a)	Explain all the types of Intrusion Detection System.	[2]
Q.5(b)	Differentiate between Virus and Worm.	[3]
Q.5(c)	Explain the importance of Firewall in network security. Compare all the types of firewall with each other.	[5]

:::::28/11/2022:::::M