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

CLASS: M.Tech **SEMESTER : II**
BRANCH: IS **SESSION : SP/19**

SUBJECT: IT514 CRYPTOGRAPHY

TIME: 3 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) Suppose a customer buys a product online worth Rs 10,000 from a merchant and makes the payment for the same. Identify and discuss on the type of attack in the following situations: [5]
- (i) An attacker intercepts the message containing the payment details and modifies the amount to Rs 20,000.
- (ii) An attacker obtains a copy of the transaction message. After the payment is made, the attacker again sends the same (copied) message to the payment portal.

Q.1(b) Illustrate the use of the Extended Euclidean Algorithm to find the gcd of 161 and 28. [5]

Q.2(a) Use Vigenere cipher to encrypt the text "NOTWELLTODAY" using the key "HEAL". How does Vigenere cipher differ from other polyalphabetic ciphers? [5]

Q.2(b) Assess the significance of SubBytes transformation, key expansion, key length and the number of rounds in the AES encryption technique. [5]

Q.3(a) Analyze the robustness of the RSA cryptosystem in terms of factorization attack and broadcast attack. [5]

Q.3(b) Review the security mechanism of ElGamal Cryptosystem. [5]

Q.4(a) Explain the MD4 Hash function. [5]

Q.4(b) Design a digital signature technique based on RSA cryptosystem. [5]

Q.5(a) Distinguish between message authentication and entity authentication. [5]

Q.5(b) Differentiate between the two different Biometric techniques. [5]

:::::24/04/2019 M:::::