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

CLASS: M.TECH **SEMESTER : II**
BRANCH: ECE **SESSION : SP/19**

SUBJECT: IT504 APPLIED CRYPTOGRAPHY

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) What is the difference between a block cipher and a stream cipher? What is steganography? [5]
Q.1(b) What do you understand Zero Knowledge Protocol? Explain Zero-Knowledge Proofs of Identity [5]

Q.2(a) Explain the different methods of public key distribution with suitable diagrams and show how secret keys are exchanged using public keys. [5]
Q.2(b) Explain Diffie Hellman Algorithm with an example. [5]

Q.3(a) What are prime numbers and relatively prime numbers? State and Prove Fermat's theorem. [5]
Q.3(b) Explain the operation of DES algorithm using diagram. What is the strength of a DES algorithm? [5]

Q.4(a) What do you mean by pseudo random number generation? Explain. [5]
Q.4(b) Explain Secure Hash Algorithm using block diagram. [5]

Q.5(a) How elliptic curve cryptography can be used as key transfer, Encryption and Decryption of a message? [5]
Q.5(b) Assume a client C wants to communicate with a server S using Kerberos protocol. How can it be achieved? [5]

:::::01/05/2019:::::M