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

CLASS: M.TECH **SEMESTER : I**
BRANCH: IS **SESSION : MO/18**

SUBJECT: IT504 APPLIED 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) Explain the key principles of security with examples. [5]
Q.1(b) Explain Zero-Knowledge proof along with the properties. [5]

Q.2(a) Explain symmetric key exchange algorithm with example. [5]
Q.2(b) Explain Run Length encoding scheme with an example. [5]

Q.3(a) What a prime numbers and relatively prime numbers? State and Prove Fermat's theorem. [5]
Q.3(b) Explain the steps in the various rounds of DES. [5]

Q.4(a) What is the difference between a block cipher and a stream cipher? [5]
Q.4(b) What is a Message Authentication code? What is the difference between MAC and Message digest? [5]

Q.5(a) Briefly explain elliptic curve cryptography. [5]
Q.5(b) What us the important aspect that establishes trust in digital signatures? Explain MD5 algorithm. [5]

:::::05/12/2018:::::M