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

CLASS: MTECH **SEMESTER : I**
BRANCH: IS **SESSION : MO/19**

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)	What do you understand by Secure Communication? List and briefly define categories of Security Services.	5]
Q.1(b)	Explain the different types of network security attack on the basis of security principles.	[5]
Q.2(a)	Encrypt the plaintext message "The key is hidden under the door pad" by using a 6 character key "CENTER" with the Vigenere Cipher.	[5]
Q.2(b)	Distinguish between symmetric and asymmetric key cryptography.	[5]
Q.3(a)	Compare the round keys in DES and AES. In which cipher is the size of the round key the same as the size of the block?	[5]
Q.3(b)	Illustrate the RSA algorithm with suitable example.	[5]
Q.4(a)	Explain the steps involved in creation of digital certificate. What are the common causes for revoking a digital certificate?	[5]
Q.4(b)	Discuss the various services offered by PGP to secure e-mails.	[5]
Q.5(a)	Describe the SSL architecture. How it works?	[5]
Q.5(b)	What is block chain and why is it important? Are crypto currencies a currency or an asset?	[5]

:::::04/12/2019:::::E