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

CLASS: BE **SEMESTER: VII**
BRANCH: CSE **SESSION : MO/2019**

SUBJECT : CS7121 CRYPTOGRAPHY AND NETWORK SECURITY

TIME: 1.5 HOURS **FULL MARKS: 25**

INSTRUCTIONS:
1. The total marks of the questions are 30.
2. Candidates may attempt for all 30 marks.
3. In those cases where the marks obtained exceed 25 marks, the excess will be ignored.
4. Before attempting the question paper, be sure that you have got the correct question paper.
5. The missing data, if any, may be assumed suitably.

Q1 (a) Identify the challenges associated with achieving security on a shared computer. [2]
(b) Describe the CIA triad in computer security. [3]

Q2 (a) Identify the cipher technique in which frequency analysis is difficult for a cryptanalyst. Also, mention how feature analysis becomes difficult. [2]
(b) Explain Caesar Cipher. Use it to decrypt HQFUBSWHG WHAW using key as 3. [3]

Q3 (a) Explain the use of the expansion permutation in DES. [2]
(b) Comment on the security and vulnerabilities of the DES technique. [3]

Q4 (a) Identify the parameter choices essential for designing a Feistel cipher technique. [2]
(b) Highlight the difference between confusion and diffusion in cryptography giving emphasis on the use of each. [3]

Q5 (a) Find the multiplicative inverse of 23 in Z_{100} using the Euclidean algorithm. [2]
(b) Explain a real scenario where the End to End encryption placement technique would be preferred. Also comment of the scope of this encryption technique in terms of the OSI layered architecture. [3]

Q6 (a) Explain what pseudorandom numbers are and how can they be generated? [2]
(b) Find the inverse of $(x^2 + 1)$ modulo $(x^4 + x + 1)$ in $GF(2^4)$. [3]

:::: 20/09/2019M ::::::