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

CLASS: BE **SEMESTER: VII**
BRANCH: CSE **SESSION: MO/2018**

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) What are the following values in DES? [2]
1. Block size
2. Cipher key size
3. Round key size
4. Number of rounds (do not count IP, IP^{-1} and Swapper in number of rounds)

(b) Briefly explain the key generation procedure in DES with Diagram. [3]

Q2 (a) List all 4 types of cryptanalysis attacks? A security system asking for 4 digit hexadecimal PIN (Personnel Identification Number) to access the system. Maximum, how many trials an attacker have to perform to get access the system? [2]

(b) Explain different security services in network security given by ITU-T. [3]

Q3 (a) Hill cipher is block cipher or stream cipher, justify your answer with example. [2]

(b) Given a=161, and b= 28, find GCD(a,b) and the values of s and t such that [3]
a x s + b x t = GCD(a,b).

Q4 (a) Generate the elements of the field $GF(2^3)$ using the irreducible polynomial $f(x)= x^3+x+1$. [2]

(b) Use the extended Euclidean algorithm to find the inverse of polynomial x^2+x+1 using the modulus $\mathbf{x^3+x+1}$. [3]

Q5 (a) Encrypt the message "Enemy attacks tonight" using the transposition key [2]

3	1	4	5	2
1	2	3	4	5

(b) Use affine cipher to Decrypt the message "ZEBBW" with the key pair (K_1= 17, K_2= 5) in modulus 26. [3]

Q6 (a) Write an algorithm for pseudorandom number generation. [2]

(b) What are the modifications you can do to make DES even more complex and secure? Justify your answer. [3]

:::: 13/09/2018 M ::::::