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

CLASS: IMSC **SEMESTER : IX**
BRANCH: MATHS & COMP. **SESSION : MO/18**

SUBJECT: CS7121 CRYPTOGRAPHY AND NETWORK SECURITY
TIME: 3:00 HRS. **FULL MARKS: 50**

INSTRUCTIONS:
1. The question paper contains 7 questions each of 12 marks and total 84 marks.
2. Candidates may attempt any 5 questions maximum of 60 marks.
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) Categorize different types of network security attacks on the basis of security goals. [6]
Q.1(b) Encrypt the message “this is an exercise “using the affine cipher with key (15,20). Also decrypt the message to get the original plaintext. [6]

Q.2(a) Explain the different modes of operations for block cipher with suitable block diagram. [6]
Q.2(b) Describe the one round DES encryption process. [6]

Q.3(a) Write a short note on random number generation. [6]
Q.3(b) In the Diffie-Hellman key exchange algorithm, let the prime number be 353 and one of its primitive root be 3. Let the users A and B select their secret keys X_A = 97 and X_B =233. Compute: [6]
(i) The public keys of A and B
(ii) the common secret key

Q.4(a) Explain the meet-in-the-middle attack. [6]
Q.4(b) Describe the Advanced Encryption Standard algorithm. [6]

Q.5(a) Discuss the RSA cryptosystem with its weakness. [6]
Q.5(b) State and prove Fermat’s theorem. [6]

Q.6(a) What characteristics are needed in secure hash function. [6]
Q.6(b) Explain the MD5 algorithm with the help of a block diagram. [6]

Q.7(a) Describe the Digital signature standard approaches and its algorithm with proof. [6]
Q.7(b) In the RSA scheme, let p=3, q=11 and d=3. Calculate the public key. Now Suppose A wants to send a message M=107 to B. Sign and verify this message using the RSA digital signature scheme. [6]

:::::07/12/2018 M:::::