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

CLASS: BE **SEMESTER : VII**
BRANCH: CSE **SESSION : MO/19**

SUBJECT: CS7121 CRYPTOGRAPHY AND NETWORK SECURITY

TIME: 3:00 HOURS **FULL MARKS: 60**

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) Use the Vigenere cipher with the keyword "JOKER" to encipher the message "Why so serious". [2]

Q.1(b) Encrypt the message "This is an exercise" using [2+2]
(i) Additive cipher with key 20 (ii) multiplicative cipher with key 15.

Q.1(c) Explain with appropriate examples the attacks that threaten confidentiality and availability. [6]

Q.2(a) Determine whether the following P box are Expansion P box, Compression P box or straight P box: [1+1]
(i)

1	1	2	3	4	4

(ii)

1	3	5	6	7

Q.2(b) Highlight the difference between a strong key, weak key, a semi weak key and a possible weak key. [4]

Q.2(c) Discuss how chosen plaintext attack and known plaintext attacks are possible in DES. [6]

Q.3(a) Find the multiplicative inverse of x^3+x+1 modulo x^5+x^3+1 as polynomials with coefficients in GF(2). [2]

Q.3(b) Construct a Galois field of 16 elements, GF(2^4), using a primitive polynomial $f(x) = x^4+x+1$. [4]

Q.3(c) Discuss how is traffic confidentiality maintained in Link encryption techniques? Compare it with the traffic confidentiality technique used in End to End encryption. [6]

Q.4(a) Discuss why a random Initialization Vector (IV) is used in CBC mode encryption. What goes wrong if one uses a fixed IV? [2]

Q.4(b) Consider the "Plaintext Feedback" (PFB) mode where the encryption formula for ciphertext block C_i is: $C_i = E(K, P_i) \oplus C_{i-1}$, $C_0 = IV$ and E() can be any encryption function with key K and plaintext P_i. What is the formula for decrypting a cipher block C_i? Are there any security problems in PFB, if yes, briefly explain it. [4]

Q.4(c) (i) AES has a larger block size than DES. Is this an advantage or disadvantage? Explain. [3+3]
(ii) Discuss on the scope of performing a Brute Force attack on AES ciphers.

Q.5(a) To illustrate the RSA system, we use primes p = 23 and q = 17. As public encryption key we use e = 3. Compute the decryption key d. Show your computations. [2]

Q.5(b) (i) Find the result of 70^{-1} mod 101 [2+2]
(ii) Find the result of 16^{-1} mod 323

Q.5(c) Alice wants to send an encrypted message to Bob using RSA but doesn't know his public key. So, she sends Bob an email asking for the key. Bob replies with his RSA public key (e, N). However, the active adversary intercepts the message and changes one bit in e from 0 to 1, so Alice receives an email claiming that Bobs public key is (e', N), where e' differs from e in one bit. Alice encrypts m with this key and sends it to Bob. Of course, Bob cannot decrypt, since the message was encrypted with the wrong key. So, he resends his key and asks Alice to send the encrypted message again, which she does. The adversary eavesdrops to the whole communication without interfering further. Describe how he can now recover m illustrating the vulnerability of RSA. [6]

Q.6(a) Alice has an account with a server. The server makes her change her password every few months, to which Alice just increments a number in her password, e.g. pwd1, pwd2, pwd3,…. Why does the server not complain that the new password is very much like her old one? [2]

Q.6(b) Discuss the possibility of a Cryptanalytic Attack on a Hash function and MAC. [4]

Q.6(c) Discuss about the need for Mutual Authentication. Explain in detail a method through which Mutual Authentication can be achieved. [6]

Q.7(a) Can a Digital Signature be forged? [2]

Q.7(b) Distinguish between Direct and Arbitrated Digital Signatures. [4]

Q.7(c) Explain the working of the Secure Hash Algorithm. [6]