Reg. No.

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL

III SEMESTER MCA END SEMESTER EXAMINATIONS, NOVEMBER 2017

SUBJECT: INFORMATION AND NETWORK SECURITY – (MCA-5013)

REVISED CREDIT SYSTEM

(22/11/2017)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer ALL FIVE FULL questions.
- Missing data may be suitable assumed.

1A.	Using Hill Cipher substitution technique, encrypt the plain text message "pay more money" with the key $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ (Use 3*3 matrix). Also explain the Hill Cipher substitution technique.	5
1B.	Explain various types of security attacks of OSI security architecture.	3
1C.	Differentiate SET and SSL.	2
2A.	What is authentication token? Explain how user authentication can be achieved using challenge based tokens and time based tokens?	5
2B.	With a suitable diagram, explain the working of HMAC.	3
2C.	Suppose an intruder has intercepted the message and message digest (K|M). What are the different possible ways to forge a message without knowing the secret key?	2

3A.	With a suitable example, explain RSA algorithm. Perform encryption and decryption using RSA algorithm for the following:- P = 5, q = 31 and plain text (M) = 5	5
3B.	Discuss different approaches of intrusion detection system.	3
3C.	Differentiate confusion and diffusion in cryptography	2
4A.	State Chinese remainder theorem and solve the simultaneous congruence using Chinese remainder theorem X = 6 mod 11 X = 13 mod 16 X = 9 mod 21 X = 19 mod 25	5
4B.	Explain how does digital signature algorithm provide authentication, integrity and non-repudiation?	3
4C.	Differentiate triple DES with two keys and three keys.	2
5A.	Why is Diffie – Hellman key exchange algorithm used? Write the steps of Diffie – Hellman key exchange algorithm. With suitable example, explain man-in-the-middle attack problem of the algorithm.	5
5B.	Explain how SET achieves its objectives?	3
5C.	Compare SHA-1 and MD5.	2