Reg. No.

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

A Constituent Institution of Manipal University

VII SEMESTER B.TECH. (COMPUTER AND COMMUNICATION ENGINEERING)

END SEMESTER EXAMINATIONS, NOVEMBER 2017

SUBJECT: CYBER SECURITY [ICT 4152]

REVISED CREDIT SYSTEM
(21/11/ 2017)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer ALL the questions.
- Missing data may be suitable assumed.

1A. Explain Kerberos operation with the help of a neat block diagram. [5]

1B. Apply the square-and-multiply fast exponentiation method to calculate 17^{22} mod 21. [3]

1C. Discuss Cross-Site Request Forgery with an example. [2]

2A. Elucidate the structure of one round of AES at the encryption site with the help of a suitable figure. [5]

2B. Apply Chinese Remainder Theorem to solve the following congruence equations. [3]
$x \equiv 2 \bmod 5$
$x \equiv 3 \bmod 4$
$x \equiv 6 \bmod 7$

2C. Using Fermat's little theorem, calculate 145^{102} mod 101. [2]

3A. How digital signatures are signed and verified in Digital Signature Standard (DSS)? Show the necessary steps for key generation, signing and verification. [5]

3B. Using Rabin Cryptosystem with $p = 3$ and $q = 7$, encrypt the message "MANIPAL" using 0 to 25 for letters A to Z. [3]

3C. Distinguish between chosen plaintext and chosen ciphertext attacks. [2]

4A. Decrypt the cipher text "**ZEBBW**" generated by affine cipher with encryption key pair (7,2). [5]

4B. Alice uses Bob's RSA public key (**e=3, n=35**) and sends the ciphertext 22 to Bob. Show how Eve(attacker) can find the plaintext using the cycling attack. [3]

4C. Differentiate between CMAC and HMAC. [2]

5A. Explain one round of Fiat-Shamir Protocol with a proper block diagram. [5]

5B. What do you understand by the term **same origin policy**? Enlist its key features. [3]

5C. If the key with parity bit (64 bits) is **0123 ABCD 2562 1456**, find the first round key in DES algorithm. Show the steps of working. Use the tables given in Table Q.5C1 and Table Q.5C2 for the computation. [2]

Table Q.5C1: Parity-bit drop table

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

Table Q.5C2: Key Compression table

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32