Reg. No.

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent institution of MAHE, Manipal)

VII SEMESTER B.TECH. (INFORMATION TECHNOLOGY)

MAKEUP EXAMINATIONS, DECEMBER 2018

SUBJECT: INFORMATION AND WEB SECURITY [ICT 4102]

REVISED CREDIT SYSTEM
(27/12/2018)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer ALL the questions.
- Missing data, if any, may be suitably assumed.

1A. Samantha uses the RSA signature scheme with primes p = 13 and q = 23 and public verification exponent e = 53.

i. What is Samantha's public modulus (n)? What is her private signing key?

ii. Samantha signs the digital document D = 100. What is the signature?

iii. Show the verification procedure. 5

1B. How can bank prevent guessing attacks and dictionary attacks on passwords? Explain. 3

1C. List the duties of a KDC. 2

2A. Using Symmetric key ciphers (Monoalphabetic and Polyalphabetic) perform the encryption for the text "SWARAJ IS MY BIRTH RIGHT"

i. Play Fair cipher using the keyword MONARCHY. Use X as blank space.

ii. Vigenere Cipher using keyword RHYTHM.

iii. Affine Cipher with key K_1 and K_2, 5 and 8 respectively.

iv. Columnar Transposition Cipher with Key = PHARAOH

v. Rail Fence Cipher with Key =4 5

2B. With a neat block diagram illustrate how HMAC is generated. 3

2C. Which security mechanism(s) are provided in the following scenarios?

i. A bank requires customer's signature for withdrawal.

ii. A school server disconnects a student if the student is logged into the system for more than three hours. 2

3A. Show that DES decryption is the inverse of DES encryption. **5**

3B. Explain the properties of cryptographic hash functions. **3**

3C. Answer the following using SHA-512 protocol.

i. Generate W_{45}.

ii. If the contents of the buffers are 0xF, 0xD and 0xB, calculate Majority and Conditional. **2**

4A. Explain S/MIME services with supported cryptographic algorithms used. Also compare and contrast the protocols PGP and S/MIME. **5**

4B. What is Cryptanalysis? Explain various cryptanalysis attacks possible with cryptography. **3**

4C. List the services provided by Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols. **2**

5A. Bob has to send a secret pin M= 24 to Alice using Rabin Cryptosystems. His private keys are p=23 and q=7. Calculate his public key and show how Bob encrypts the pin. Show how Alice decrypts the message to get back the plaintexts. **5**

5B. Elucidate with neat diagrams Cipher Block Chaining (CBC) and Output Feedback Mode (OFB) modes of operation. **3**

5C. Illustrate how digital signatures differ from conventional signatures. **2**