Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

SECOND SEMESTER M.Tech. (DEAC/ME) DEGREE END SEMESTER EXAMINATION - APRIL 2018

SUBJECT: CRYPTOGRAPHY AND NETWORK SECURITY (ECE - 5237)

TIME: 3 HOURS **MAX. MARKS: 50**

Instructions to candidates

- Answer **ALL** questions.
- Missing data may be suitably assumed.

1A. The intercepted message "**KYMVPD**" was enciphered using an affine map on digraphs in a 28-letter alphabet, in which A-Z have numerical equivalents 0-25, !=26 and ?=27. It is known that the plaintext "**BARN**" corresponds to "**MQUV**", find the enciphering keys and decrypt the message.

1B. Encrypt **BABY** using the linear Hill cipher with key $\begin{pmatrix} 3 & 2 \\ 13 & 9 \end{pmatrix}$. What is the de-crypting key?

1C. The ciphertext **DRZNUO** was produced by using a Vigenere cipher with keyword **BABY**. What is the plaintext?

(5+4+1)

2A. If the input to the AES S-box is 0x61, what is the output of the AES.

2B. Describe the DES key generation algorithm with relevant block diagram.

2C. gcd(970, 818)=…….

(5+4+1)

3A. The elliptic curve is represented by the following notation $E_{11}(2, 1)$. Write an equation and find all the points on the Elliptic curve.

3B. In an RSA system, the public key is {59, 3233}. Find the private key. Encrypt the plaintext "NO". The plaintext blocks are represented by diagraphs and ciphertext are by trigraphs. The alphabets A-Z have numerical equivalents 0-25.

3C. Solve the congruence: $x^2 \equiv 7 \bmod 11$

(5+4+1)

4A. Describe the Digital Signature Standard (DSS) in detail.

4B. What do you mean by message authentication? Describe the HMAC protocol with relevant block diagram.

4C. Find the number of primitive roots in $G = \langle Z_{17}*, \times \rangle$.

(5+4+1)

5A. Describe the following firewall systems.: Packet filters and Circuit level Firewalls with their advantages and disadvantages.

5B. Describe the following intrusion detection techniques: Signature based detection and Anomaly based detection.

5C. A straight permutation or a straight P-box has same number of inputs as …….

(5+4+1)