|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |

**E Reg. No. :**

**Question Paper Code: 55P21**

M.E. DEGREE EXAMINATION, NOV 2017

Elective

Communication Systems

15PCM509- COMMUNICATION NETWORK SECURITY

(Regulation 2015)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART - A (5 x 20 = 100 Marks)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | (a) | Convert “MEET ME” using Hill cipher with the key matrixConvert the cipher text back to plaintext.$$\left[\begin{matrix}17&17&5\\21&18&21\\2&2&19\end{matrix}\right]$$ | CO1- U | (20) |
|  |  | Or |  |  |
|  | (b) | (i) Briefly explain the design principles of block cipher.  | CO1- U | (10) |
|  |  | (ii) Discuss in detail block cipher modes of operation. | CO1- U | (10) |
|  |  |  |  |  |
| 2. | (a) | (i) Explain the generation sub key and S Box from the given 32-bit  key by Blowfish. | CO2- U | (10) |
|  |  | (ii) In AES, hoe the encryption key is expanded to produce keys for  the 10 rounds | CO2- U | (10) |
|  |  | Or |  |  |
|  | (b) | (i) Describe about RC4 algorithm. | CO2- U | (10) |
|  |  | (ii) Explain the Miller-Rabin Algorithm | CO2- U | (10) |
|  |  |  |  |  |
| 3. | (a) | (i) Compare the Features of SHA-1 and MD5 algorithm. | CO3-Ana | (10) |
|  |  | (ii) Discuss about the objectives of HMAC and it security features.  | CO3-Ana | (10) |
|  |  | Or |  |  |
|  | (b) | Describe the MD5 message digest algorithm with necessary block diagrams. | CO3-Ana | (20) |
|  |  |  |  |  |
| 4. | (a) | (i) Describe the SSL Specific protocol – Handshake action in detail.  | CO4- U | (10) |
|  |  | (ii) Explain Secure Electronic transaction with neat diagram.  | CO4 -U | (10) |
|  |  | Or |  |  |
|  | (b) | Explain the architecture of IP Security. | CO4- U | (20) |
|  |  |  |  |  |
| 5. | (a) | (i) Explain any two approaches for intrusion detection.  | CO5- U | (10) |
|  |  | (ii) Identify a few malicious programs that need a host program for  their existence. | CO5-Ana | (10) |
|  |  | Or |  |  |
|  | (b) | Describe the familiar types of firewall configurations.  | CO5- U | (20) |
|  |  |  |  |  |