|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Enrol. No. / ID** |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Marks** |
| **Q.1** | **(A)** | Draw & explain for single round DES Encryption Algorithm. | **[5]** |
|  | **(B)** | Explain the Rail-Fence Cipher with suitable example. | **[5]** |
|  |  |  |  |
|  |  |  |  |
| **Q.2** | **(A)** | Encrypt “CNS” with playfair using key “mendacious”. | **[5]** |
|  | **(B)** | Explain Triple DES for encryption & decryption. | **[5]** |
|  |  |  |  |
| **Q-2** | **(A)** | Explain any one block cipher mode of operation which is used to generate the stream cipher. | **[5]** |
|  | **(B)** | Find the decryption of “MATH” using Hill Cipher algorithm. The secret key which was used for encryption in Hill Cipher was :  K = | **[5]** |
|  |  |  |  |
| **Q.3** | **(A)** | Draw and explain the structure of AES Encryption and Decryption algorithm. | **[5]** |
|  | **(B)** | Calculate following using extended Euclidean algorithm.   * 20-1 mod 97 * 35-1mod 64 | **[5]** |
|  |  |  |  |
| **Q-3** | **(A)** | Write about fermat’s theorem and the concept of generators. | **[5]** |
|  | **(B)** | i) confussion  ii) dufission  iii) passive attack  iv) active attack  v) cryptography  vi) Find a number *n* such that 7**∙** n ≡ 1 mod 17. | **[5]** |