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

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Marks** |
| **Q.1** | **(A)** | What is security Services? Explain any three types of security services. | **[5]** |
|  | **(B)** | Construct a playfair matrix with the key “occurrence”. Generate the cipher text for the plaintext “Tall trees” | **[5]** |
|  |  |  |  |
| **Q.2** | **(A)** | Define the terms threat and attack. List and briefly define categories of security attacks. | **[5]** |
|  | **(B)** | Explain Vegenere Cipher. | **[5]** |
|  |  | **OR** |  |
|  | **(A)** | Explain monoalphabetic cipher and polyalphabetic cipher by giving an example. | **[5]** |
|  | **(B)** | Explain the one time pad scheme. | **[5]** |
|  |  |  |  |
| **Q.3** | **(A)** | Define Block Cipher. Explain Design Principles of block cipher. | **[5]** |
|  | **(B)** | Write the Euclid’s algorithm and show the steps of Euclid’s algorithm to find gcd(1970,1066). | **[5]** |
|  |  | **OR** |  |
| **Q.3** | **(A)** | Explain the terms diffusion and confusion. | **[5]** |
|  | **(B)** | Explain single round function of DES with suitable diagram. | **[5]** |