**TERNA ENGINEERING COLLEGE, NERUL**

**Department of Computer Engineering**

**Cryptography and System Security (CSS)**

**Assignment No 1**

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Question** | **CO -mapped** |
| **Q. 1** | Define Security goals, Services, Mechanisms with example and how each one can be achieved. | (CO-1) |
| **Q. 2** | Explain Substitution and transposition techniques, Vigenere cipher, Playfair cipher, Hill cipher with example. | (CO-1) |
| **Q. 3** | Explain Chinese Remainder theorem with example | (CO-2) |
| **Q. 4** | Explain the Euclid Algorithm, Fermat/Euler Algorithm | (CO-2) |
| **Q. 5** | A and B decide to use a Diffie Hellman key exchange algorithm. They choose p= 23 and g=5 as public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share. | (CO-3) |
| **Q. 6** | Explain the RSA algorithm with an example. | (CO-3) |

|  |
| --- |
| **CSS ASSIGNMENT - 1** |
| **AMEY THAKUR** |
| **COMPS TE B-50** |
|  |