ST.XAVIER’S COLLEGE

(Affiliated to Tribhuvan University)

Maitighar, Kathmandu



**Cryptography Lab Assignment #5**

**SUBMITTED BY:**

Pradeep Dahal

017BSCIT029

3rd Year/5th Sem

|  |  |
| --- | --- |
| **SUBMITTED TO:** |  |

|  |  |  |
| --- | --- | --- |
|  | **Signature** | **Remarks** |
| **Er. Anil Kumar Shah**  **Lecturer, Dept. of Computer Science** |  |  |

**TITLE: WRITE A PROGRAM TO ENCRYPT AND DECRYPT A MESSAGE USING ONE-TIME PAD**

**ALGORITHM**

**Theory**

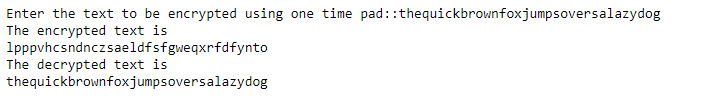
One-time pad is a traditional and potentially unbreakable cipher technique where a onetime pad of random keys is generated as long as of the input text.

**Procedure**

1. Input the data to be encrypted or decrypted.
2. Generate a pad of random number as long as of the input text.
3. Add those random number in each letter to encrypt and subtract to decrypt.
4. End

**SOURCE CODE**

**OBSERVATION**

****

**CONCLUSION**

Thus, one-time pad was implemented in the python programming language.