|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Hope Foundation’s,**  **Finolex Academy of Management and Technology, Ratnagiri** | | | | | | | | | |
| **Department of Information Technology** | | | | | | | | | |
| Subject name: SECURITY LAB | | | | | | | | Subject Code: ITL502 | | | |
| Class | | TE IT | | Semester – V (CBCGS) | | | | Academic year: 2018-19 | | | |
| Name of Student | |  | | | | | **QUIZ Score :** | | | | |
| Roll No | |  | | | Assignment/Experiment No. | | | | | 01 | |
| Title**: Design and Implementation of product cipher using Substitution and Transposition ciphers** | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. **Course objectives applicable:**   **LOB1**- To be able to apply the knowledge of symmetric cryptography to implement simple  Ciphers. | | | | | | | | | | | |
| 1. **Course outcomes applicable:**   **LO1**- Apply the knowledge of symmetric cryptography to implement simple ciphers. | | | | | | | | | | | |
| **3. Learning Objectives:**   * To conceal the context of some message from all , except the sender and recipient (privacy or secrecy) to prevent eavesdropping. * To verify the correctness of a message to the recipient (authentication) to prevent tampering. | | | | | | | | | | | |
| 1. **Practical applications of the assignment/experiment:**  * It helps to provide accountability, fairness, accuracy and confidentiality. * It can prevent fraud in electronic commerce and assure the validity of financial transactions. * It can prove one's identity and protect one's anonymity. | | | | | | | | | | | |
| **5. Prerequisites**: Understanding working of cryptosystem. | | | | | | | | | | | |
| **6. Hardware Requirements**:   1. PC with 4GB RAM, 500GB HDD,   **7. Software Requirements:**  1. Programming language C, C++, Java | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **8. Quiz Questions (if any): (Online Exam will be taken separately batch wise, attach the certificate/ Marks obtained)**   1. What is Symmetric Key cryptography? 2. What is Asymmetric Key cryptography? 3. Compare Substitution and Transposition ciphers. | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **9. Experiment/Assignment Evaluation:** | | | | | | | | | | | |
| **Sr. No.** | **Parameters** | | | | | | | | **Marks obtained** | | **Out of** |
| **1** | Technical Understanding (Assessment may be done based on Q & A **or** any other relevant method.) Teacher should mention the other method used - | | | | | | | |  | | 6 |
| **2** | Neatness/presentation | | | | | | | |  | | 2 |
| **3** | Punctuality | | | | | | | |  | | 2 |
| **Date of performance (DOP)** | | |  | | | **Total marks obtained** | | |  | | **10** |
| **Date of checking (DOC)** | | |  | | | **Signature of teacher** | | | | | |

**Results:**

**SOURCE CODE: PYTHON**a=str(input("Enter plain text:\n"))

l=len(a)

print("The ceaser cipher text is:")

for i in range(0,l):

o=ord(a[i])

s=0

s=o+3

c=chr(s)

print(c,end='')

**OUTPUT:**

Enter plain text:

Jawwad

The ceaser cipher text is:

Mdzzdg

**References** :

1. Build your own Security Lab, Michael Gregg, Wiley India.

2. CCNA Security, Study Guide, TIm Boyles, Sybex.