MIT-WPU

॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

SY B.Tech Semester-IV (AY 2022-23)

Computer Science and Engineering (Cybersecurity and Forensics)

Information and Cyber Security Lab

Assign No.	List of Assignments
1.	Write a program using JAVA or Python or C++ to implement any classical cryptographic technique
2.	Write a program using JAVA or Python or C++ to implement Feistal Cipher structure
3.	Write a program using JAVA or Python or C++ to implement S-AES symmetric key algorithm
4.	Write a program using JAVA or Python or C++ to implement RSA asymmetric key algorithm
5.	Write a program using JAVA or Python or C++ to implement integrity of message using MD5 or SHA
6.	Write a program using JAVA or Python or C++ to implement Diffie Hellman Key Exchange Algorithm
7.	Write a program using JAVA or Python or C++ to implement Digital signature using DSA
8.	Demonstrate Email Security using - PGP or S/MIME for Confidentiality, Authenticity and Integrity
9.	Demonstration of secured web applications system using SSL certificates and its deployment in Apache tomcat server
10.	Configuration and demonstration of Intrusion Detection System using Snort
11.	Configuration and demonstration of NESSUS tool for vulnerability assessment

LCA Marks Distribution

Examination	Marks
Practical Performance	10
Active Learning/Mini Project/ Additional implementation/On paper design	10
End term practical	10
Total	**30**

Assignment No. 1 : Write a program using JAVA or Python or C++ to implement any classical cryptographic technique.

Objectives: Conceal the context of some message from all except the sender and recipient (privacy or secrecy).

Classical Cryptography

Basic Terminology

- Plaintext- the original message
- Ciphertext - the coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering ciphertext from plaintext
- Cryptography - study of encryption principles/methods
- Cryptanalysis (codebreaking) - the study of principles/ methods of deciphering ciphertext without knowing key
- Cryptology - the field of both cryptography and cryptanalysis

Cryptography Classification

- By type of encryption operations used
  - Substitution
  - Transposition
  - Product
- By number of keys used By number of keys used
  - Single-key or private key or private
  - Two-key or public key or public
- By the way in which plaintext is processed
  - Block
  - Stream

Caesar Cipher

- Earliest known substitution cipher. Invented by Julius Caesar
- replace each letter of message by a letter a fixed distance away eg use the 3rd letter on
- Each letter is replaced by the letter **three** positions further down the alphabet.

Example: **mit pune** → plw sxqh

- Mathematically, map letters to numbers:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Then the general Caesar cipher is:

c = EK(p) = (p + k) mod 26

p = DK(c) = (c – k) mod 26

Monoalphabetic Cipher

monoalphabetic - only one substitution/transposition is used, or

polyalphabetic - where several substitutions/transpositions are used

- Shuffle the letters and map each plaintext letter to a different random ciphertext letter:

  Plain letters: abcdefghijklmnopqrstuvwxyz

  Cipher letters: DKVQFIBJWPESCXHTMYAUOLRGZN

  Plaintext: ifwewishtoreplaceletters

  Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

Input:

Enter the string (Plaintext):

Enter the key position :

Output:

1. Cipher text:

Rail Fence Cipher Algorithm

- The **rail fence cipher** is a form of transposition cipher.
- The plain text is written downwards and diagonally on successive “rails” of an imaginary fence, then moving up when the bottom rail is reached.
- When the top rail is reached, the message is written downwards again until the whole plaintext is written out.
- The message is then read off in rows.

INPUT:

line 1: message

line 2: key

OUTPUT:

line 1: Encrypted message

```
H . . . O . . . L .
. E . L . W . R . D
. . L . . . O . . .
```

- Rails or depth or key = 3

HOLELWRDLO