CS323: Information Security Lab

Computer Science and Engineering

T.Y. Trimester VIII (2020-21)

Assign No.	Name of Assignment
A	**Core Level security (Any two)**
1	Implement any classical cryptographic technique using java or python or C++
2	Implement simple DES symmetric key algorithm using python or java or C++
3	Implement simple RSA asymmetric key algorithm using python or java or C++
B	**API Level - (Using Libraries) (Any two)**
1	To program asymmetric key cryptography such as RSA cryptography using JAVA API, Python or C++ API.
2	To program basic cryptography hash algorithm SHA1 or MD5 Use Java or Python or C++ API. Additionally demonstrate client server authentication using socket programming.
3	Write program for demonstration of digital signature and its verification using Java or Python or C++.
C	**Security Tools Level – (Any two)**
1	Demonstrate use of PGP open source security tool for Confidentiality, Authentication and Integrity.
2	Demonstrate secured web applications system using SSL certificates and its deployment in Apache tomcat server
3	Implement Intrusion Detection System using Snort IDS tool
4	Install and configure and demonstrate NESSUS tool of vulnerability assessment

LCA Marks Distribution

Examination	Weightage	Marks
Understanding, Practical Implementation and Demonstration Skills	30%	15
Timely Submission and Ethics	30%	15
Understanding (End Term Oral)	40%	20
Total		**50**

1. Implement any classical cryptographic technique using java or python or C++

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:

$$c = EK(p) = (p + k) \bmod 26$$

$$p = DK(c) = (c - k) \bmod 26$$

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: