VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CSE1011 – Cryptography Fundamentals

Fall Semester 2021-2022

Lab Experiments:

Instructions:

- Students are advised to use any language for lab experiments.
- Students are strictly advised to follow the submission deadline.
- No Built in / library functions
- Students are strictly advised not to copy from other students

Activity - 1 (10 Marks) ---------- 30-Sep-2021

ClassicalEncryption

1.Encode and decode a message Using

a. Playfair cipher
b. Hill cipher
c. Vigenere cipher
d. Vernam Cipher

2. Use single letter frequency attack to decipher the following message. You know that it has been created with an additive (Shift) cipher.

PXPXKXENVDRUXVTNLXHYMXGMAXYKXJNXGVRFXMAHWGXXWLEHGZXKVBIAXKMXQM

Activity - 2 (10 Marks) ---------- 15-Oct-2021

Modern Cryptosystems:

1. Encode a message using DES when encrypted. Try the following experiments and note how they change the output:

a) Change one character at the end of the message. How much of the encoded message changes?
b) Change one character at the beginning of the message. How much of the encoded message changes?
c) Delete one character at the end of the message. How much of the encoded message changes?
d) Change one character in the key. How much of the encoded message changes?
e) Decrypt a message using a key with one character changed. Does it look anything like the original?

2. Create text file sample.txt; encrypt the file sample.txt using a symmetric key. The first time when code is run, a folder is created. You will be asked to enter a key. The key used is "infosec". An encrypted file is now created in the same location as the plaintext file with the name "sample1.txt" and sees difference in file. And also perform the Decryption also. (**Use AES algorithm**)

Activity – 3 (10 Marks) ---------- 31-Oct-2021
Asymmetric Cryptosystems:

1.RSA & ElGamal cryptosystems:
(a) Generate Public and private keys of two communicating parties
(b) Encrypt a short text message of your choice with their RSA /ElGamal key and send them the encrypted message (as a number, or as a sequence of numbers if your message is longer than the block size for their n).
(c) Decrypt the encrypted message you receive from your partner.

2.
Diffie- Hellman:
Simulate the Man- in the -Middle Attack.

Activity -4 (10 Marks) ---------- 15-Nov-2021
SHA-1 is a popular heuristic hash function that is currently in trend. In this experiment, we shall familiarize ourselves with SHA-1 as well as look at one important application of hashing, namely, the HMAC algorithm which is currently used in the Internet to achieve data integrity.

Activity - 5 (10 Marks) ---------- 30-Nov-2021
Digital Signature and Elliptic curve cryptography (ECC)

1. **Digital Signature (DSA signature)**

Generate the digital Signature for the specific document. Modify the content of the document and verify the signature.

2. Design and Implementation of a Secure Instant Messaging Service based on Elliptic-Curve Cryptography. (secure communication using Standard Libraries)

Activity – 6 (10 Marks) ---------- 09-Dec-2021
-
Simulate the Secure payment systems./ innovative application