VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT
EXERCISE – 11

DATE: 08.10.2020

IMPLEMENTATION OF CRYPTOGRAPHY ALGORITHMS

Perform the following tasks,

1. **Symmetric Key Encryption/Decryption**
    a. Perform Encryption and Decryption
    b. In a separate word file, show the input, output of encryption and decryption algorithm. Show that you are retrieving the Plain Text at the end.
    c. Show the algorithm-pseudo code, flow-chart diagram
    d. Describe the algorithm
    e. Upload the word file and program file
2. **Asymmetric Key Encryption/Decryption**
    a. Perform Encryption and Decryption
    b. In a separate word file, show the input, output of encryption and decryption algorithm. Show that you are retrieving the Plain Text at the end.
    c. Show the algorithm-pseudo code, flow-chart diagram
    d. Describe the algorithm
    e. Upload the word file and program file
3. **Hashing**
    a. Perform Hashing on the input (text & file)
    b. Show the Message and its Hash.
    c. Introduce a very small modification in the input. Show the change in the hash code.
    d. Show the algorithm-pseudo code, flow-chart diagram
    e. Describe the algorithm
    f. Upload the word file and program file
4. **Digital Signature**
    a. Affix digital signature to your input (Text & File)

  b. In a separate word file, show the input, output of double time encryption and double time decryption algorithm. Show that you are retrieving the Plain Text at the end.

  c. Show the algorithm-pseudo code, flow-chart diagram

  d. Describe the algorithm

  e. Upload the word file and program file

5. Ensure the presence of CIA (Confidentiality, Integrity, Authentication) triad

  a. Perform Digital Signature and Hashing in a single program (Text 7 File input)

  b. In a separate word file, show the input, output of your complete algorithm. Show that you are retrieving the Plain Text at the end and proving the hash code match also.

  c. Show the algorithm-pseudo code, flow-chart diagram

  d. Describe the algorithm

  e. Upload the word file and program file

<u>Execute the algorithms on the following input types:</u>

Case 1 : A simple input with numerals, alphabets, alphanumeric. Eg., 12345, hello, TrueFriend7

Case 2 : A File input – Word, pdf, text file etc.

Note :

- You can choose any Programming Language
- You can use the inbuilt functions available within the packages
- You can choose any algorithm for each task