

**COMP9337 - Securing Fixed and Wireless Networks**

**T1 2022**

**LAB 1**

**Group: T18B 7**

**Name:** Yuhua Zhao – **ZID:** Z5404443

**Name:** Yasin Khan – **ZID:** z5265047

**Environment:**

* **Programming Language:** Python
* **Version:** 3.9.2

## **Part A: DES Encryption and Decryption:**

* **Please run the following argument to test the Outcome**

python tempdes.py fecdba9876543210 0123456789abcdef test.txt mytest.des

**Argument Explanation:**

* + Argument 1: Initialization Vector (IV)
  + Argument 2: Key to be use for encryption
  + Argument 3: Input file path of the file that will be read
  + Argument 4: Encrypted file will be generated based on the argument 4 name.

### **Part A: Code Explanation:**

Text

Description automatically generated

* + DES encryption’s input shall be multiple of 8 octets. If the Length of the input is less than that, padding is required.
  + Firstly, line 14 will read the file according to Argument 3.
  + Secondly, the program will check whether the Length of the input is multiple of 8 bytes. If yes, will return the input itself. Else it will detect how many missing bytes are and add the Padding accordingly.

Text

Description automatically generated

* + “Encrypt\_DES” function is used to encrypt the plain text
  + “Decrypt\_DES” Function is used to decrypt the Cipher test that encrypt by the Encrypt\_DES function.

Text

Description automatically generated

* + Line 47: Detect arguments when this python script is being called and assigned to the Variable respectively.
  + Line 50: Call the Read File to get the text that needs to be encrypted and encode it with the selected Format.
  + Line 53 – 55: Record the time used for DES CBC encryption.
  + Line 57 – 59: Generate a file named by Argument 4 and write Ciphertext in.
  + Line 62 – 64: Record the time used for DES CBC decryption.
  + Line 67 – 73: Print the necessary value for Lab Part B.

## **Part B: Performance Measures for Various Algorithm:**

* **Please run the following argument to test the Outcome**

**python algPerformance.py**

The command above will run all the encryption algorithms that have specified on the requirement and print out the Encryption time and Decryption according to the Algorithm.