**CEG 4750-01: Information Security**

**Amina Haq**

**David P. Wilson**

**Jean Pauline Arcita**

**Prof. Meilin Liu**

**18th March 2021**

**Project 2**

# Introduction

As an undergraduate group, our assignment for Project 2 included the following \_\_\_ tasks:

1. Develop a program to implement DES encryption and decryption in Cipher Block Chaining (CBC) mode and with PKCS #5 padding.
2. Verify successful encryption and decryption with the supplied text test files.
3. For bonus points, verify successful encrypt and decryption with the supplied binary file.
4. Examine the octal difference between two pairs of encrypted test files.
5. Demonstrate how changes in the key or input affect the ciphertext.

This report will explore our process and the results with evidence throughout each of these five tasks in order. It will conclude with a summary of functionality implemented in our program.

# Task 01: Develop a program to implement DES in CBC mode.

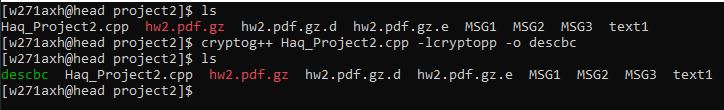
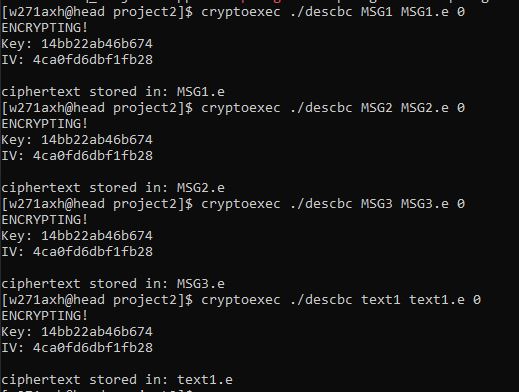
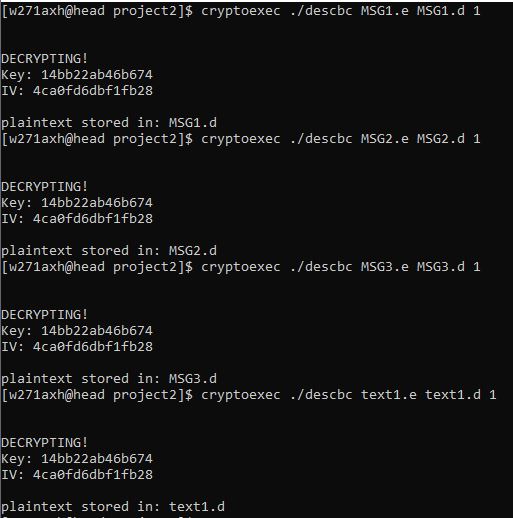
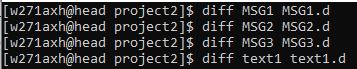


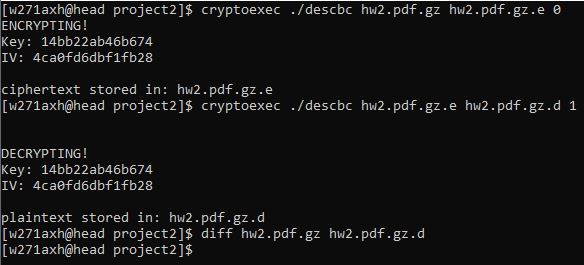
Figure : Successful compilation of the project source code.

# Task 02: Verify successful encryption and decryption with text files.

1. **Encryption**
2. **Decryption**
3. **Comparison of original files with plaintext files produced**

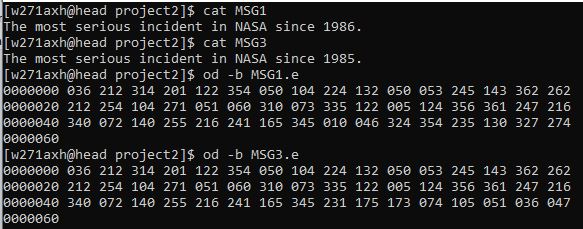


# Task 03: For bonus points, verify successful operation with a binary file.

**5: Binary file as input**

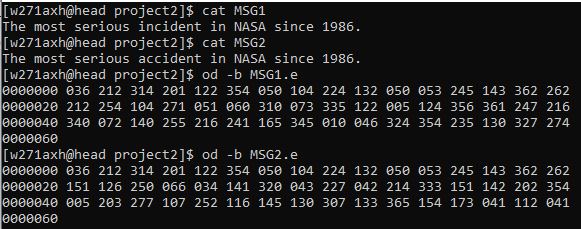
# Task 04: Examine the octal difference between two pairs of files.

**3: Octal difference in MSG1.e and MSG3.e and MSG1.e and MSG2.e**

1. **MSG1.e and MSG3.e  
   **

Between MSG1.e and MSG3.e there are 8 bytes that are different: byte 41-48

1. **MSG1.e and MSG2.e**

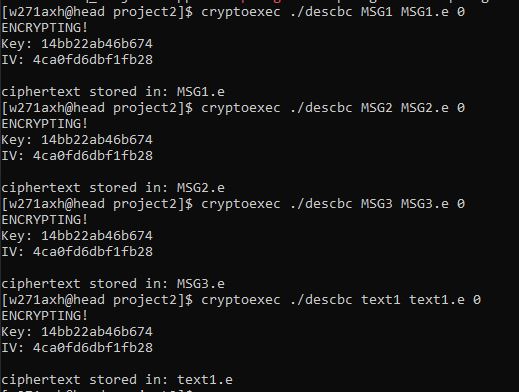
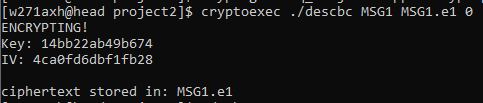
****

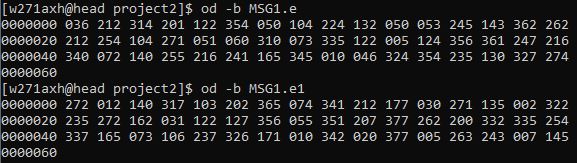
Between MSG1.e and MSG3.e there are 32 bytes that are different: byte 17-48

# Task 05: Demonstrate the effects of changes in the key and input.

**4: Effect of changing one bit in the key**

Changed key from **0x140bb22ab406b674** to **0x140bb22ab409b674**

1. ****Encrypted MSG1 to MSG1.e using key **0x140bb22ab406b674**
2. Encrypted MSG1 to MSG1.e1 using key **0x140bb22ab409b674**
3. Octal difference between MSG1.e to MSG1.e1



A difference of one bit in the key resulted in a completely different ciphertext

# Summary of Functionality

**6: A list of the functionality implemented by our program**

* Encrypt simple text files and write the ciphertext to an output file using hardcoded key and IV for DES in CBC mode
* Decrypt simple text files and write the plaintext to an output file using hardcoded key and IV for DES in CBC mode
* Encrypt and decrypt binary files and store ciphertext/plaintext to an output file using hardcoded key and IV for DES in CBC mode (bonus)