Cryptography Project Report
(CIE 582)-Fall 2021

University:Zewail City of Science and Technology

Department:Communications and Information Engineering Program

Members:

Student Name
Rahma Hassan

Abstract:

The purpose of this project is to get familiar with some Cryptographic concepts and tools.The goal is to implement block cipher modes ECB and CBC.In addition encrypt and decrypt bitmap image using AES algorithm.Finally,we evaluate our implementation of encryption and decryption of these modes by calculating time of each operation and each mode.This file is a documentation of the project.

Code:

Python Code is implemented but it isn't published for the public here.

Design and Implementation:

First Mode:ECB mode:

MODE_ECB Encryption:

I-The image is opened and read.
II-It is padded with zeros,divided into parts consisting of 16 bytes (128 bits),which is the block size of the AES encryption algorithm and finally stored into a list of 16-bytes parts.
III-Now these parts are ready for the encryption step,AES encryption python built in library will be used.Therefore:Crypto.Cipher is imported and AES.new(key, AES.MODE_ECB) function is used.
AES.new(key, AES.MODE_ECB) :
This function needs a key,which will be generated randomly.It also needs the mode value which will not be given because It will be implemented.
IV-Base on the mode will be chosen ,the implementation of each mode will differ so:
After having a list of 16-bytes parts,Looping on it is required using the encrypt function in python.
V-Time of encryption is calculated in python by subtracting end time from start time.After that,The encrypted message is being saved in file.

MODE_ECB Decryption:

The decryption is a reversed mode of encryption.Therefore,The decryption process goes as following:
I-The Encrypted file will be read and divided into 128 bits(16 bytes) parts and appended to a list.
II-Th (decrypt) function in python from the AES module is used for decryption of each part of the list.
III-Final thing,The decrypted message will be written in a decrypted file and saved.
V:Time for the decryption process is calculated in python.

Second Mode:CBC mode:

MODE_CBC Encryption:

I-The image is opened and read.
II-It is padded with zeros,divided into parts consisting of 16 bytes (128 bits),which is the block size of the AES encryption algorithm and finally stored into a list of 16-bytes parts.
III-Now these parts are ready for the encryption step,**AES.new(key, AES.MODE_CBC),**this python statement is used,Here,CBC mode will be implemented not used directly.In CBC mode,Key is needed to be generated so 16 bytes length key is used.Also,Initial vector is generated,We will loop on each 16 bytes part of the list and make bitwise xoring it with initial vector (IV).(encrypt) function from the AES module will be used for the encryption purpose.
IV-All cipher_texts are appended to get the whole final ciphertext.
V-We will calculate the time of encryption and save the encrypted message.

MODE_CBC Decryption:

The decryption is a reversed mode of encryption.Therefore,The decryption process goes as following:
I-The Encrypted file will be read and divided into 128 bits(16 bytes) parts and looped over them to be appended to a list to be used in decryption which AES encryption should take 16 bytes blocks only.
II-Th (decrypt) function in python from the AES module is used for decryption of each part of the list.Bitwise XOring is done on each block with the IV.All decrypted parts are appended to get the whole decrypted message.
III-Time for the decryption process is calculated in python.
V-Final thing,The decrypted message will be written in a decrypted file and saved.

Standards:

AES standard is to take 128 bits of block of plaintext.There are different modes like ECB and CBC.ECB is the easiest mode to implement.CBC mode can take 3 different possible keys like 128 bits key,192 bits key and 256 bits key.In addition,CBC needs initial vector to be XORed with the plaintext.All of these modes can AES in encryption.CBC mode is more secure than ECB mode and has more operations.

Output:

We find that encryption time of ECB mode is 480.61766958236694 and encryption time of CBC mode is 505.10883045196533.
We find that the decryption time of ECB mode is 156.57949662208557 and decryption time of CBC mode is 160.73358249664307.
Therefore,We find that encryption and decryption of CBC takes more time than ECB mode because It is more complex and has more operations. But,on the other hand,CBC mode is more secure than ECB mode and it gives better results because if we have the same inputs repeatedly,we will get different output unlike ECB mode.