Semester Project

Cryptography & Data Security

Implementation of
Advanced Modes of AES

Team

i170519 Nasir Iqbal

i140233 M. Ahsan Mehdi

Supervised by

Sir Jawad Hassan Nisar

Department of Computer Science

National University of Computer and Emerging Sciences

Islamabad, Pakistan

Introduction

In this project we have implemented the Advanced Modes of AES Algorithm. It includes the encryption and decryption of messages to make data secure. The AES is very popular algorithm which has not been broken yet.

AES Algorithm:

It has 10 rounds each has four steps except the last round. Last round has 3 steps excluding mix column operation.

Rounds Operation:

Following are 4 operations in each round of AES:

- Byte Substitution
- Shift Rows
- Mix Column
- Adding Round Key – not in last round

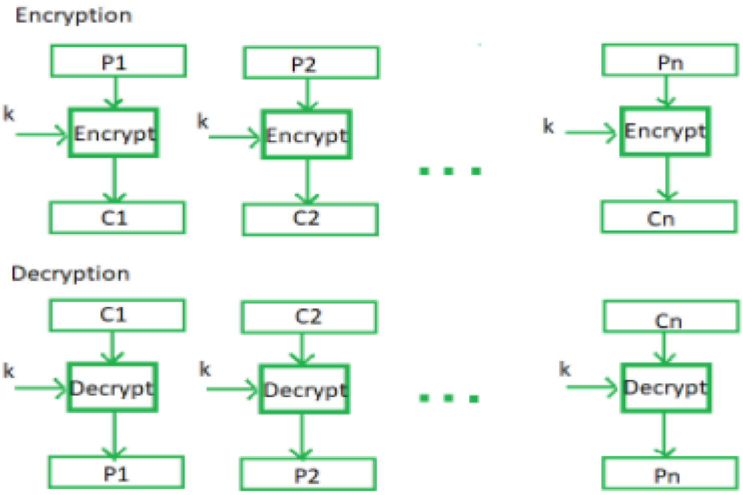
Advanced Modes of AES

Following are five advanced Modes of AES:

- ECB mode: Electronic Code Book mode.
- CBC mode: Cipher Block Chaining mode.
- CFB mode: Cipher FeedBack mode.
- OFB mode: Output FeedBack mode.
- CTR mode: Counter mode.

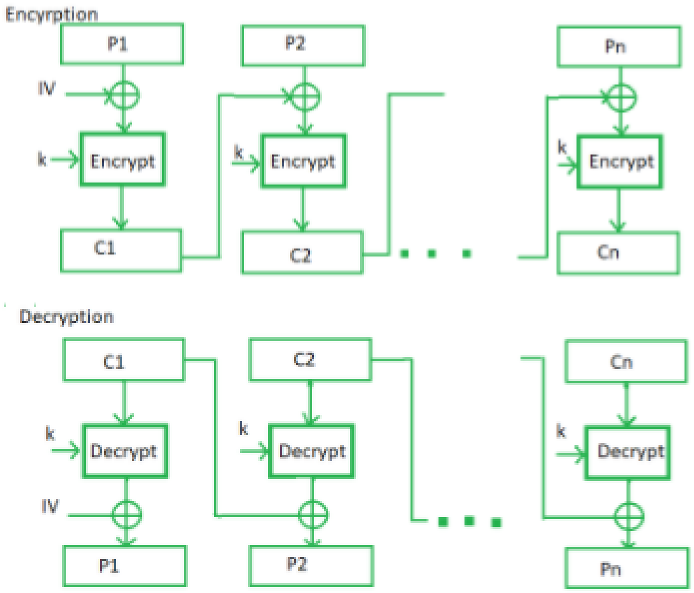
ECB:

Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted ciphertext. Generally, if a message is larger than *b* bits in size, it can be broken down into bunch of blocks and the procedure is repeated.



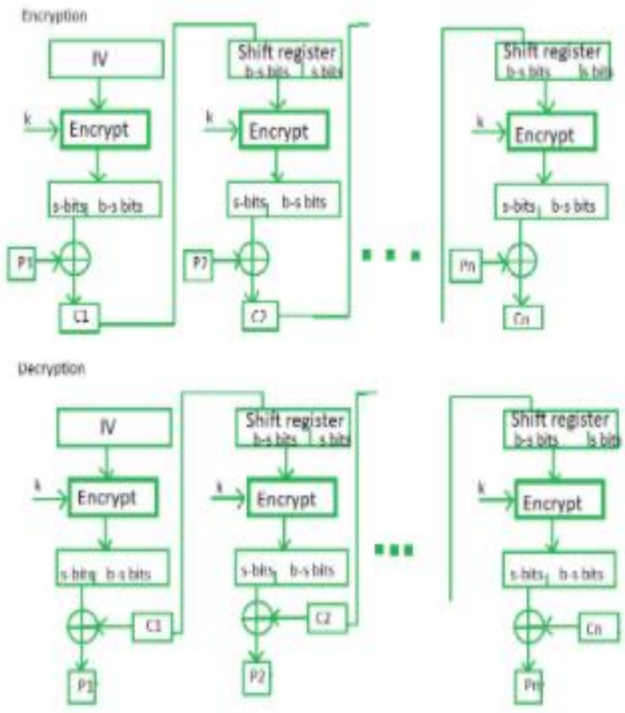
CBC:

Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, previous cipher block is given as input to next encryption algorithm after XOR with original plaintext block. In a nutshell here, a cipher block is produced by encrypting a XOR output of previous cipher block and present plaintext block.



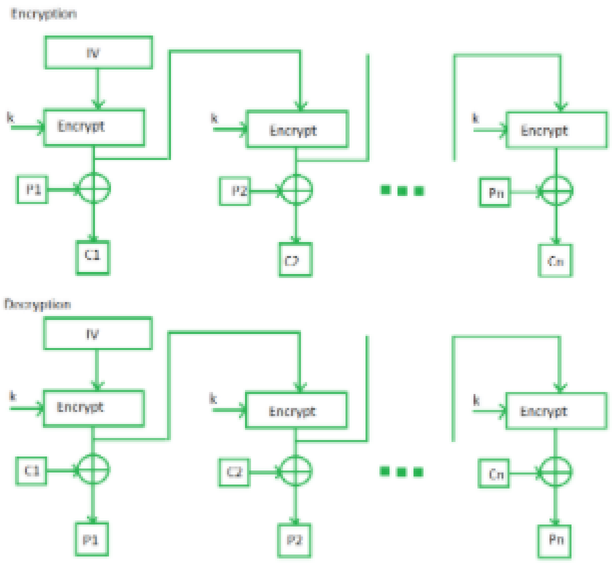
CFB:

In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first an initial vector IV is used for first encryption and output bits are divided as set of *s*and*b*-*s* bits the left hand side *s*bits are selected and are applied an XOR operation with plaintext bits. The result given as input to a shift register and the process continues. The encryption and decryption process for the same is shown below, both of them use encryption algorithm.



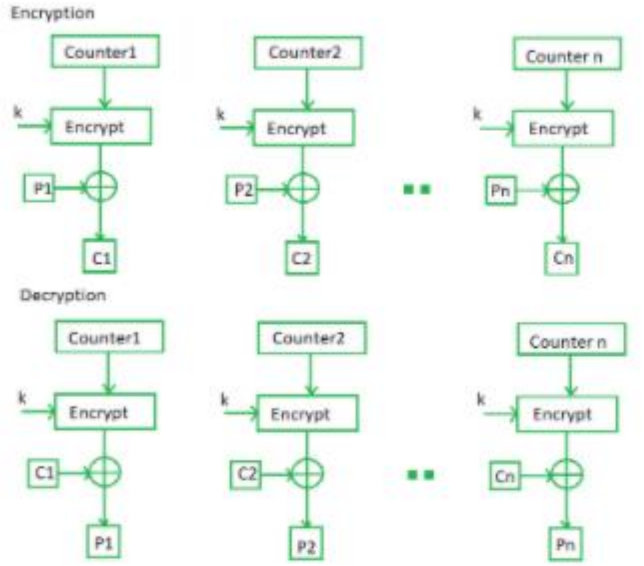
OFB:

The output feedback mode follows nearly same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are send instead of sending selected *s* bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases dependency or relationship of cipher on plaintext.



CTR:

The Counter Mode or CTR is a simple counter based block cipher implementation. Every time a counter initiated value is encrypted and given as input to XOR with plaintext which results in ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.



Encoding & Decoding Scheme

We receive the key and message as a text and then covert that text into string hexa. While for decoding we convert the hexa values into string or characters.

Padding Scheme

Plaintext Padding

Add zero B to right end until it becomes multiple of 128 bits. Stops padding when it becomes 128 bits.

Key Padding

Add zero B to right end until it becomes multiple of 128 bits. Stops padding when it becomes 128 bits.

Encryption

For encryption of the message we have used the byte substitution, shift row, mix column, and add round key.

Note: first we have calculated the round key from given key and message.

Decryption

For Decryption of the message we have used the byte substitution, shift row, mix column, and add round key but all these steps are used as inverse.

Architecture Overview

Main class initialize the GUI and the main controller make communication possible between AES and USER by using user interface.

We have following classes:

- Main
- MainController
- AES
- Utility

- ECB
- CFB
- CBC
- CTR
- OFB

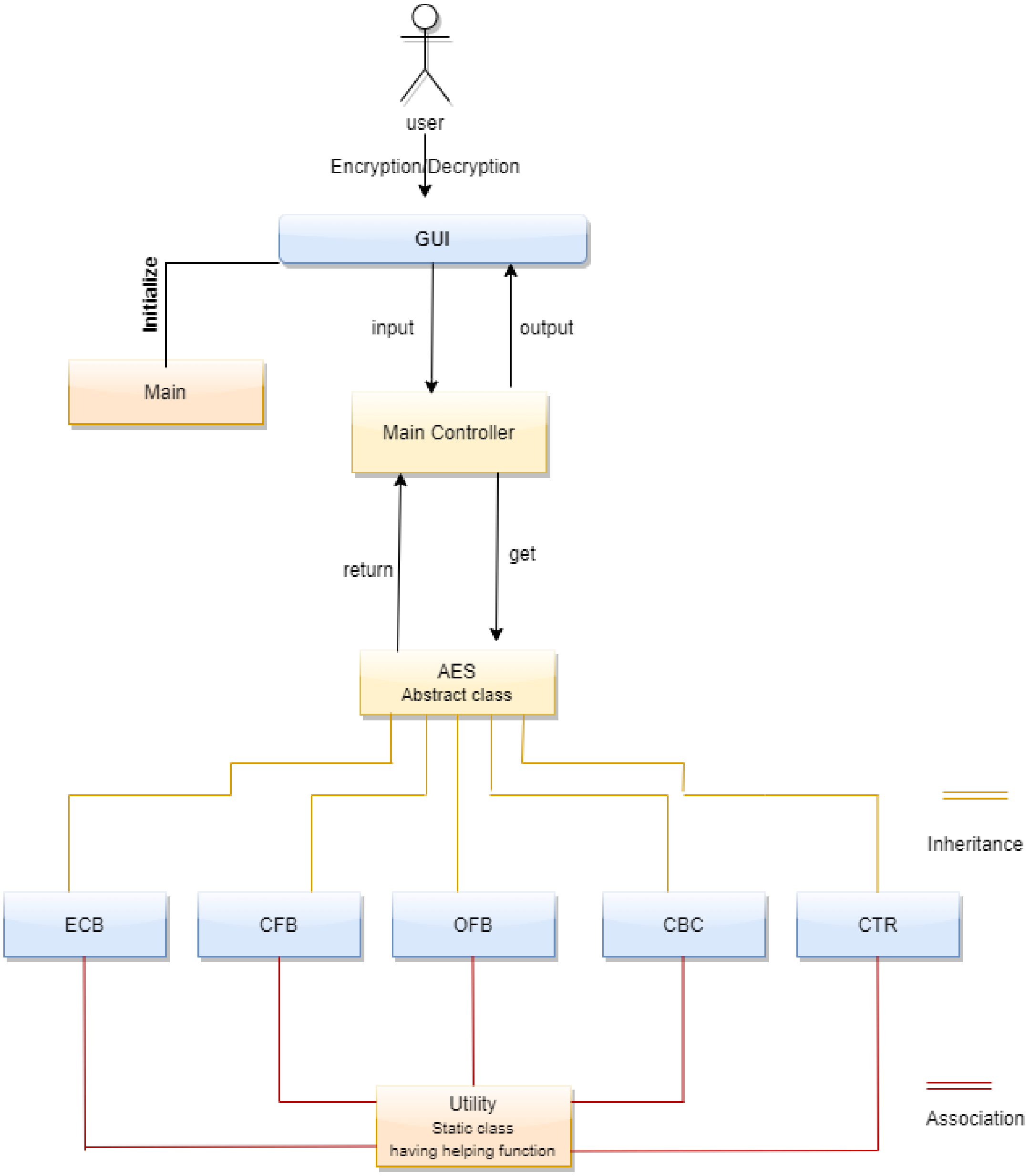
Abstract Class & Inheritance

AES is an abstract class there is inheritance between modes of AES.

Association

There is association between utility class and modes of AES. All other classes use the helping functions implemented in Utility.

Architecture Diagram



References

https://computing-concepts.cs.uri.edu/wiki/Cyber_Security_and_Cryptography

https://www.geeksforgeeks.org/block-cipher-modes-of-operation/

https://www.atpinc.com/blog/what-is-aes-256-encryption#:~:text=Data%20Encryption&text=Encryption%20works%20by%20taking%20plain,to%20cipher%20and%20decipher%20information.

https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

https://github.com/kokke/tiny-AES-c

https://github.com/boppreh/aes

https://medium.com/quick-code/aes-implementation-in-python-a82f582f51c2

https://www.researchgate.net/publication/236656798_MODES_OF_OPERATION_OF_THE_AES_ALGORITHM#:~:text=AES%20is%20an%20algorithm%20for,)%20and%20CTR%20(Counter).