

**Faculty of Engineering & Technology Electrical & Computer Engineering Department**

**APPLIED CRYPTOGRAPHY**

**ENCS4320**

**Assignment #2**

**"TEA with ECB and CBC”**

**Prepared by:**

**Student Name:** Mohammad Salem

**Student ID:** 1200651

**Instructor:** Dr. Ahmed Shawahna

**Section:** 1

**Date:** 3/6/2024

In our assignment we implement the TEA algorithm with two mode of operation

ECB (Electronic Code Bock)

CBC (Cipher text chaining)

I have two classes for ECB,CBC the first one is TEA\_CBC.java and the secand one is TEA\_CBC.java

Based on the attached document for the project, I worked to employ the method according to the attached encryption and decryption algorithm,

where the length of the key was 128 bits, and the data block 64 bit.

in TEA\_ECB.java as a primitive formate

public class TEA\_ECB {

// attribute

//constructes for key as array of 4 integer

encrypt(int[] p){

//encrypt function for ECB tacke palin text return cipher text

// after mack proccssing by xoring and shift

}

decrypt(int[] c){

// decreption function for ECB tacke cipher text return palin text

// after mack proccssing by xoring and shift

}

}

//////////////////////

in TEA\_CBC.java as a primitive formate

public class TEA\_CBC {

// attribute

//constructes for key as array of 4 integer

encrypt(int[] p, int[] prev){

// tack plain text the the previos plain text and return the cipher text after mack proccssing

// by xoring and shift

}

/////

decrypt(int[] c, int[] prev){

// decreption function for CBC tacke cipher text return palin text

//// after mack proccssing by xoring and shift

}

}

/////////Also,

Functions class with static attribute(parameters)

//empty constructe

readKey\_IV(){

// method to read from user

}

ENC\_DEC\_img\_ECB(int[] key, int mode){

// read image and mack ENC/DEC for the ECB (data in as a image)

}

ENC\_DEC\_img\_CBC(int[] key, int mode, int[] IV){

// chaining consept with IV as a previos for the first data in value (IV as a input from user)

// read image and mack ENC/DEC for the CBC (data in as a image)

}

////////////////////////////////////////

How to use my programe ? How to execute my implementatio?

Answer:

it is very simple

accourding of choice option from the case statment the operation is completly done

System.out.println("1. Encrypt and Decrypt the image with TEA ECB");

System.out.println("2. Encrypt and Decrypt the image with TEA CBC");

System.out.println("3. To Stop programme exit..");

System.out.print("Enter your choice: ");

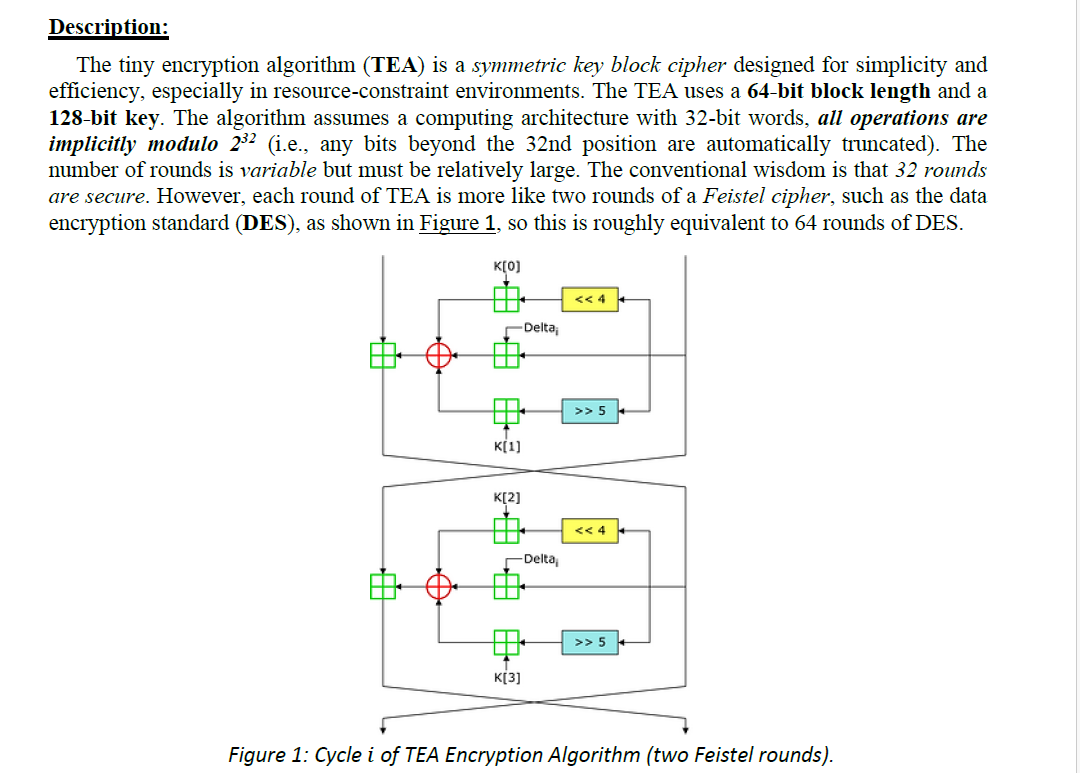
if you enter 1 , look at images file cipher text image and plain text image agin .... ECB mode

if you enter 2 , look at images file cipher text image and plain text image agin .... CBC mode

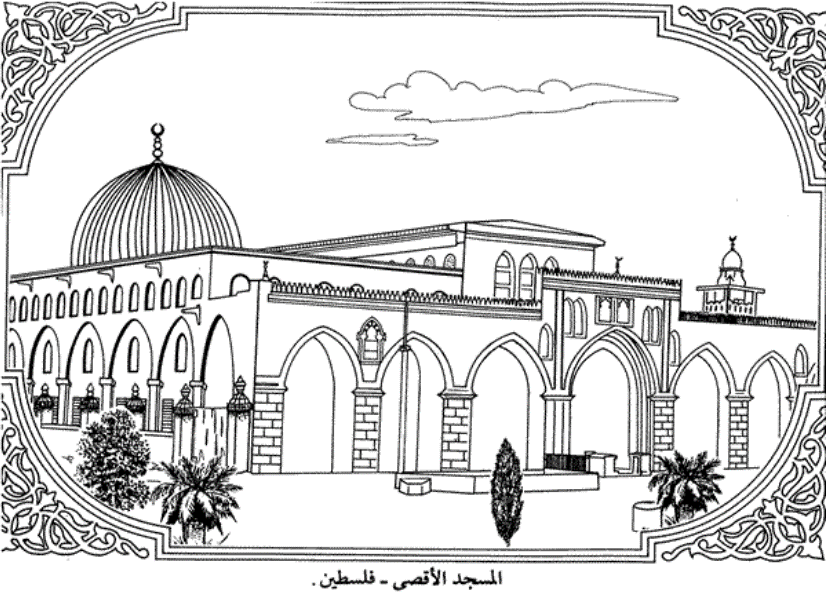
if you enter 3 stop

these choises in loop

as shown below one round for TEA:



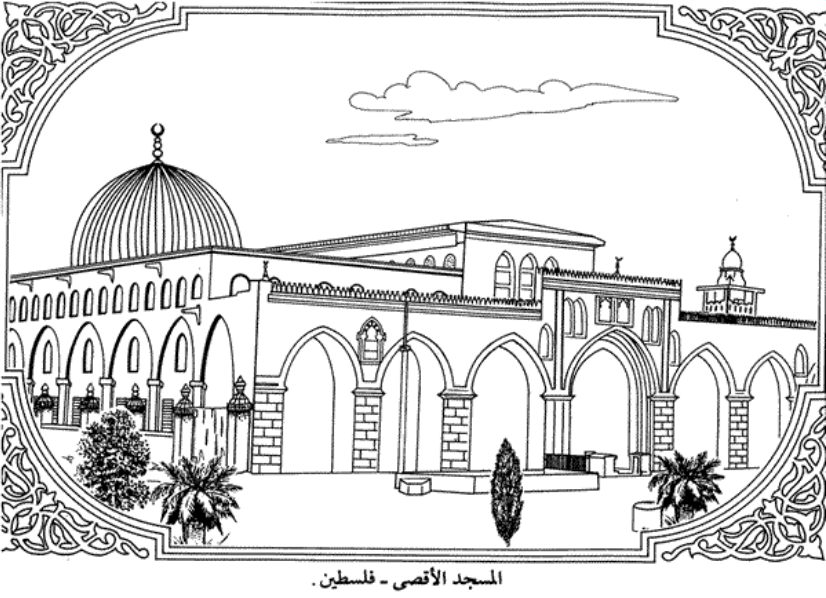
**input image on ECB:**



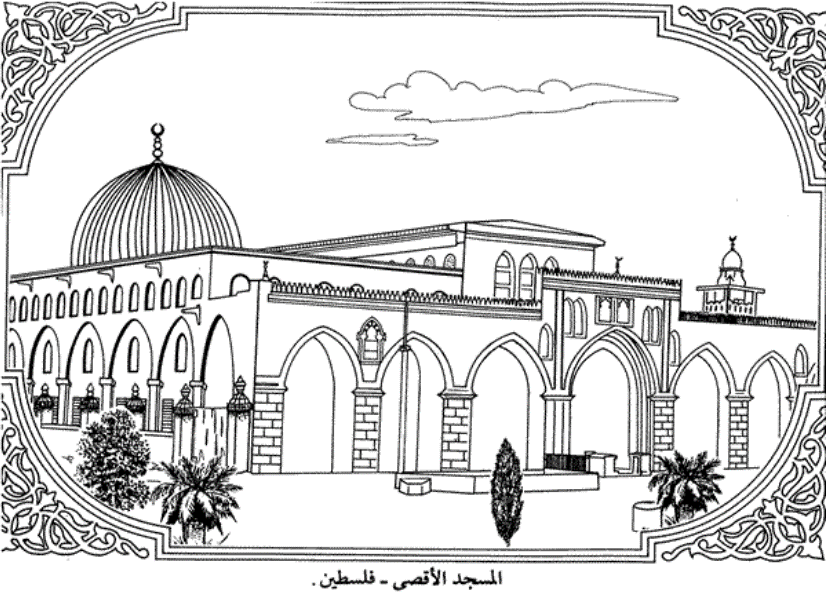
The cipher Text of ECB:



DEC the cipher text image on ECB:



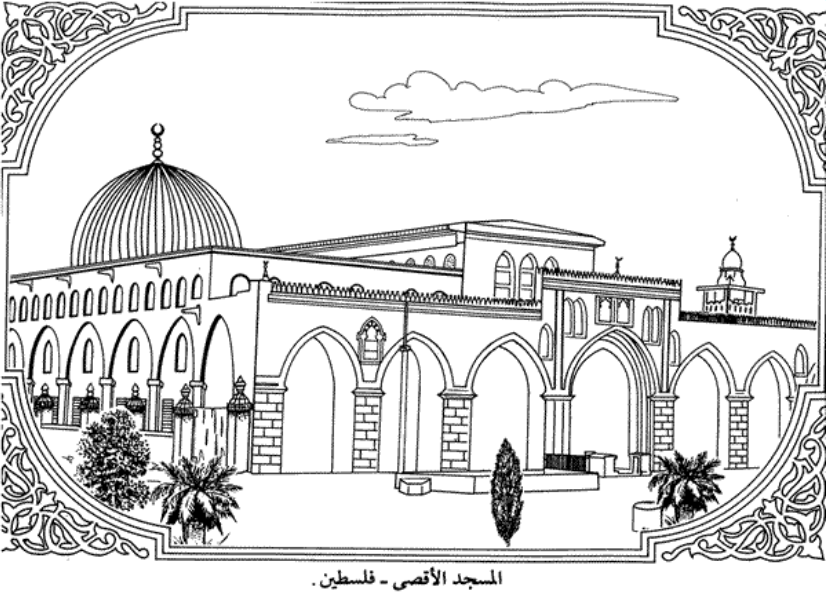
Input image on CBC:



Cipher Text for CBC mode:



Decrepit the cipher text in CBC mode:



Also, you can find Read me file and all files in attached.