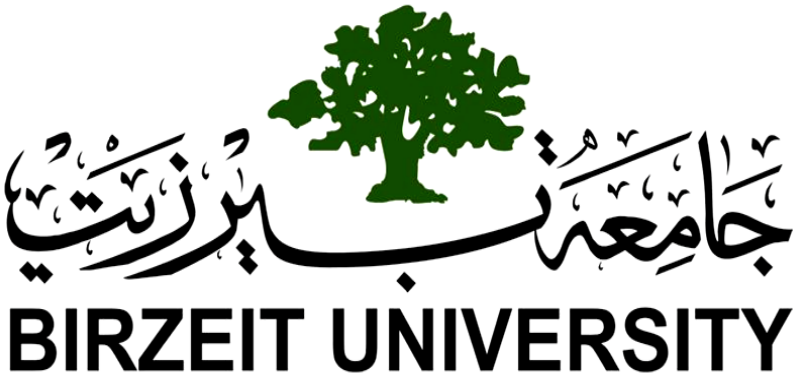


Faculty of Engineering & Technology
Electrical & Computer Engineering Department

Applied Cryptography
ENCS4320
Homework#2

Image Encryption and Decryption Using TEA-ECB and TEA-CBC

Prepared by: Ahmad Ismail 1202450

Instructor: Dr. Mohammed Hussein

Section: 2

Date: 05/06/2024

Table of Contents

TEA Encryption and Decryption

Description:

The tiny encryption algorithm (TEA) is a symmetric key block cipher designed for simplicity and efficiency, especially in resource-constraint environments. The TEA uses a 64-bit block length and a 128-bit key. The algorithm assumes a computing architecture with 32-bit words, all operations are implicitly modulo 2^(32) (i.e., any bits beyond the 32nd position are automatically truncated)

Requirements

Make sure **Python3** is downloaded.
Before you can run this script, you need to install the following Python libraries:

- `Pillow`
- `numpy`
- `matplotlib`
- `pyinstaller` (for creating the executable)

- Installation

You can install the required libraries using pip. Open a command prompt and run the following command:

- pip install Pillow numpy matplotlib pyinstaller

  OR
- pip3 install Pillow numpy matplotlib pyinstaller

Procedure for Using the Image Encryption and Decryption Script:

1- make sure all previous requirements are downloaded.

2- Download the Script.

3- Run the script using Python3:
   - Open a Command Prompt: Open a command prompt or terminal.
     i. -Navigate to the Script Directory: Use the cd command to navigate to the directory where the script is saved. For example:
     cd path/to/your/script
   - -Run the Script: Execute the script using Python:
     python3 main.py

4- Provide Inputs: Follow the prompts to enter the image path, key, and IV.
   a. Image Path: Enter the full path to your image file (e.g., C:\Users\YourName\Desktop\image.png).
   b. Key: Enter the key as four 32-bit hexadecimal numbers separated by spaces (e.g., 0x11223344 0x55667788 0x99AABBCC 0xDDEEFF00).

c. IV: Enter the IV as two 32-bit hexadecimal numbers separated by a space (e.g., 0xAABBCCDD 0xEEFF0011).

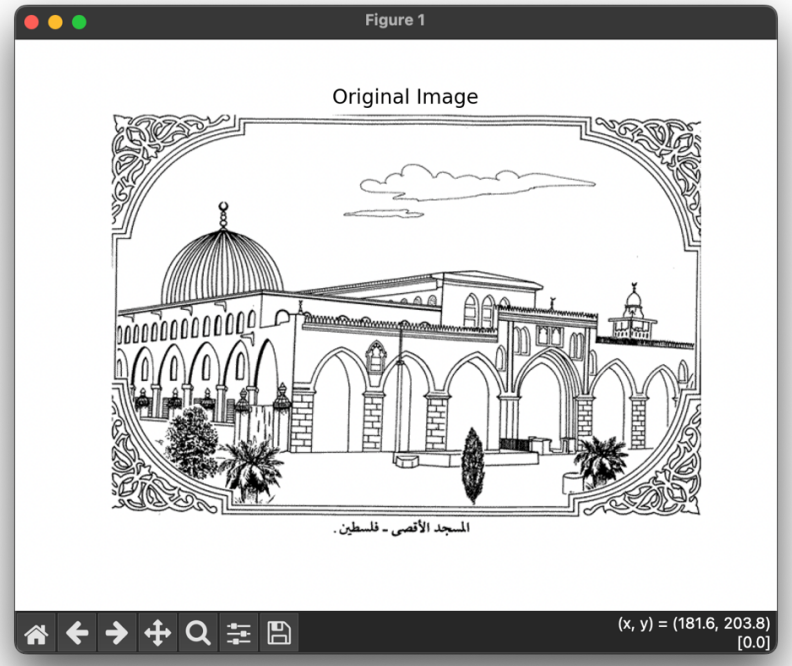
5- View Results: The script will display the original image, encrypted image, and decrypted image for both ECB and CBC modes.

Troubleshooting

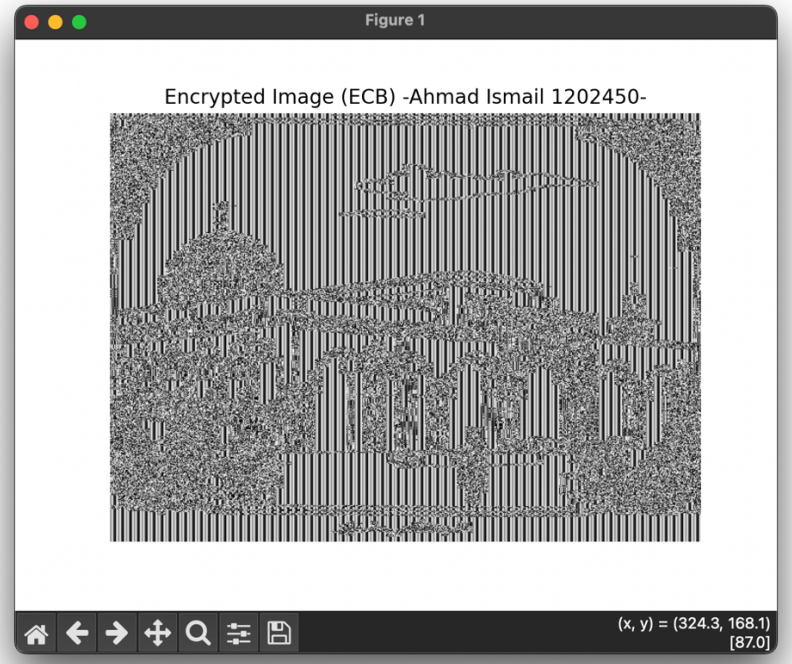
- File Not Found Error: Ensure the path to the image file is correct.
- Invalid Key/IV Format: Ensure the key and IV are entered in the correct hexadecimal format.
- Library Installation Issues: Ensure all required libraries are installed using the pip install command.

Results:

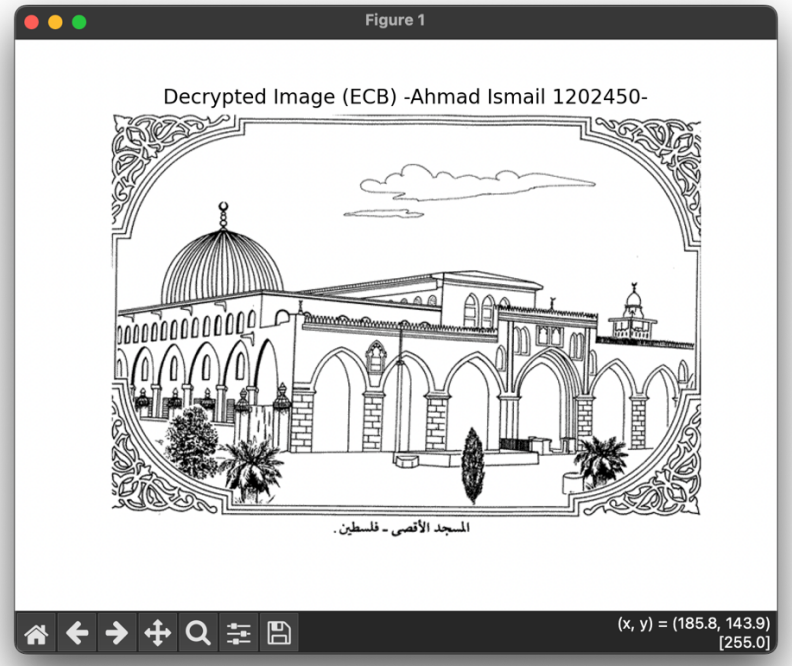
Original Image



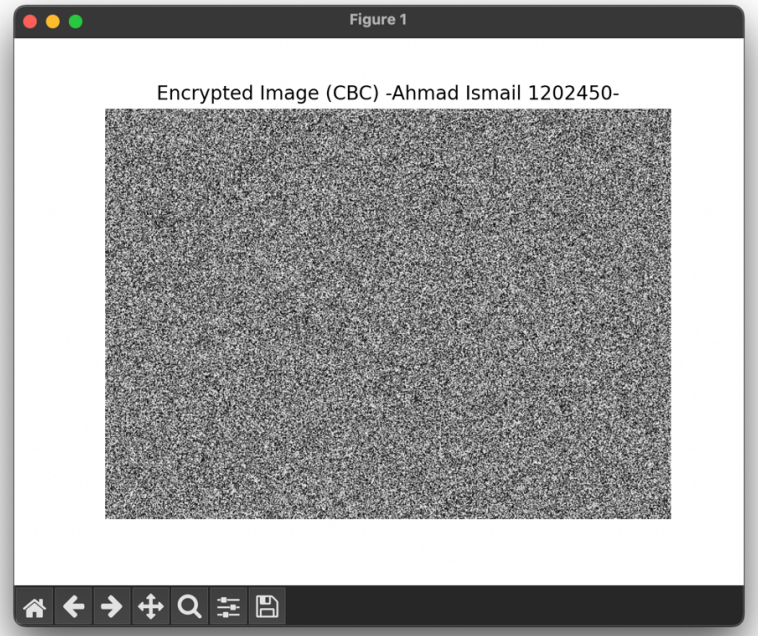
Encrypted Image (TEA-ECB)



Decrypted Image (TEA-ECB)



Encrypted Image (TEA-CBC)



Decrypted Image (TEA-CBC)