

***Faculty of Engineering and Technology***

***Department of Electrical and Computer Engineering***

***ENCS4320 - Applied Cryptography***

***Homework # 2 (Programming Assignment)***

***Student: Maisam Alaa***

***ID: 1200650***

***Section:1***

***Abstract:***

***The Tiny Encryption Algorithm (TEA) is a symmetric key block cipher known for its simplicity and efficiency, especially in resource-constrained environments, utilizing a 64-bit block size and a 128-bit key. TEA operates on 32-bit words with operations modulo \(2^{32}\) and typically uses 32 rounds, where each round is roughly equivalent to two rounds of the Data Encryption Standard (DES), necessitating a large number of rounds due to its simple round function. This project implements TEA in both Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes, with 32 rounds for encryption and decryption, leaving the first 10 blocks unencrypted. The program prompts for user input for the key, plaintext/ciphertext, and initialization vector (IV), and demonstrates the implementation by encrypting and decrypting a BMP image file, showcasing the functionality through visual output.***

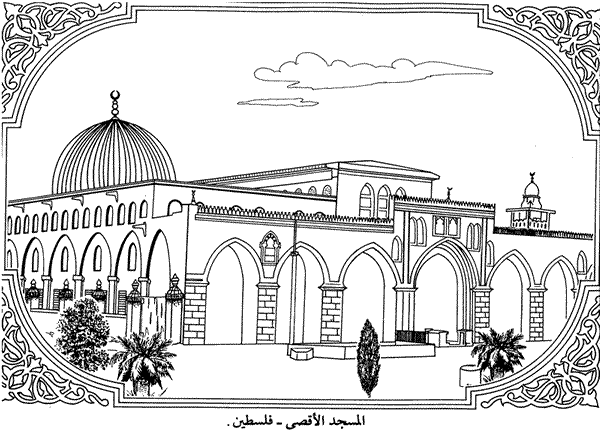
******

Figure 1 Original Photo

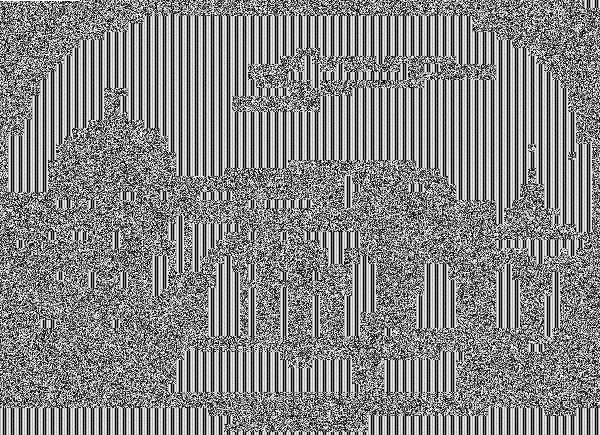
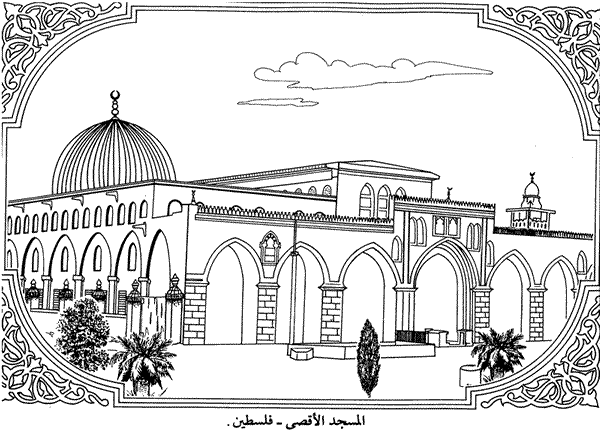
******

Figure 2 Encryption and Decryption using TEA-CBC of the Origianl photo

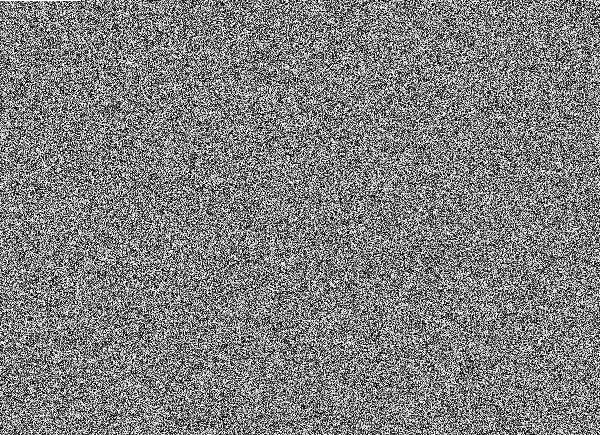
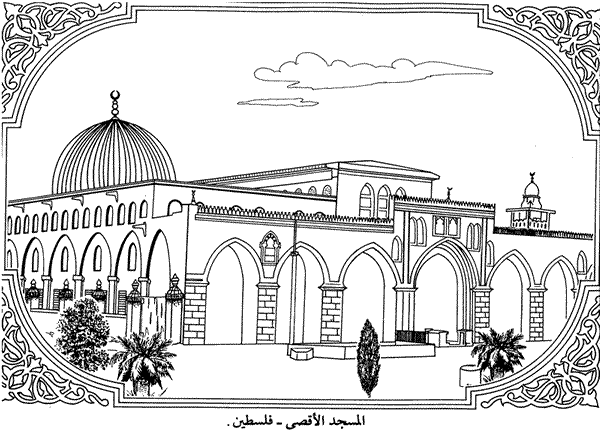
******

Figure 3 Encryption and Decryption using TEA-ECB of the Origianl photo