# **CPE 449: ENCRYPTION ASSIGNMENT**

**DAN OTIENO**

**09/01/2023.**

# **Task 1:**

**No submission required.**

# **Task 2:**

**A white paper with text

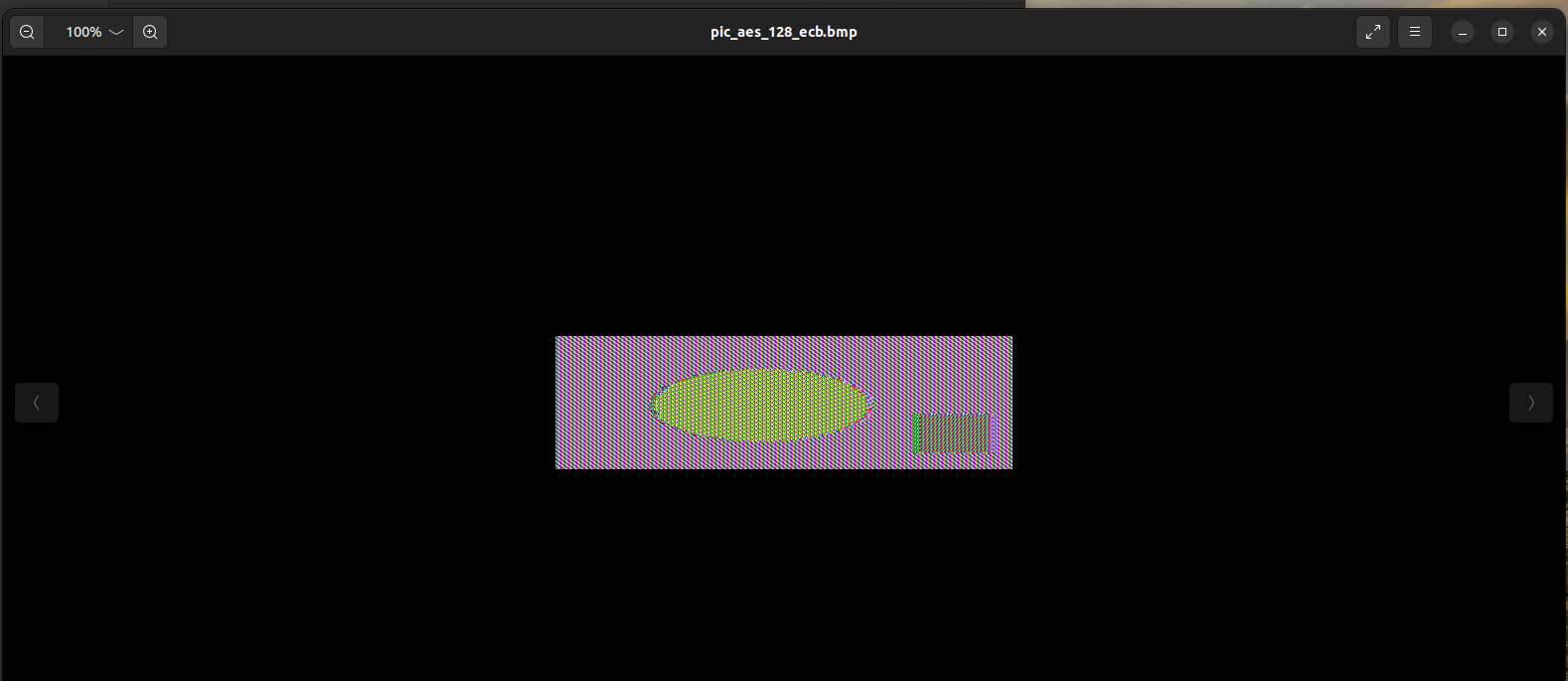
Description automatically generated**

1. **Original photo:**

**A screen shot of a computer

Description automatically generated**

**Encrypted photo (aes-128-ecb):**

****

**Encrypted photo (aes-128-cbc):**

**A screen shot of a computer

Description automatically generated**

1. **There’s not much information that can be derived when it comes to the colors from the original image. However, whether anything can be determined from the original image depends on the encryption method. When the ECB method is used, we can see the exact shapes from the original image, whereas, in the second encryption method, CBC, the original image is fully encrypted such that there is no visible data from the original. Because the CBC method carries over encryption information from the one block and uses it to encrypt the next block, whereas ECB encrypts each block independently, CBC is considered a more secure method between the two, and that is demonstrated in the exercise above.**

# **Task 3:**

**A screenshot of a computer

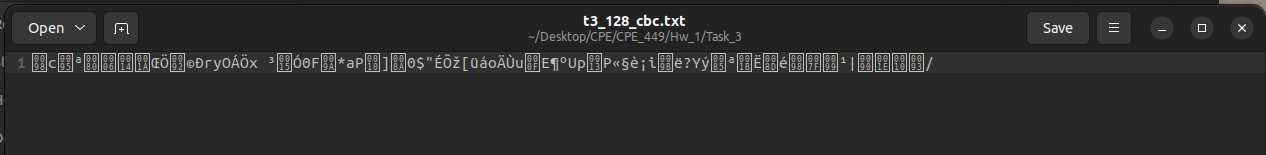
Description automatically generated**

**Original text:**

**A black screen with white text

Description automatically generated**

**Aes-128 Encryptions (CBC, CFB, ECB, OFB respectively):**

****

**A screen shot of a computer

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

**A black screen with white text

Description automatically generated**

**Aes-128 Decryptions after modifying 1 bit per file (CBC, CFB, ECB, OFB respectively):**

**A screen shot of a computer

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

1. **All the cypher files are modified in some way when decrypted. We get varying amounts of data recovered from the corrupted cypher files. 48 bytes of data is recovered from the CBC cypher, 46 bytes recovered from CFB cypher, 47 bytes recovered from the ECB cypher, and finally, 63 bytes recovered from the OFB cypher.**
2. **The most data recovered from the corrupted cypher is from the OFB-encrypted file. This is because the algorithm uses a stream of bits to encrypt subsequent data blocks, the decryption is completed one bit at a time, such that only the text corresponding to the corrupted bit is affected. The CBC and CFB modes are similar in that during decrypting of a ciphertext block, one should add XOR the output data received from the decryption algorithm to the previous ciphertext block. Because the receiver knows all the ciphertext blocks just after obtaining the encrypted message, he can decrypt the message using many threads simultaneously. So, if one bit is corrupted, then all the corresponding bits are affected when the file is decrypted. For the ECB method, each block of text/cyphertext is encrypted or decrypted separately, so all corresponding bits are affected if one is corrupted as well. (Source:** [**https://www.crypto-it.net/eng/theory/modes-of-block-ciphers.html**](https://www.crypto-it.net/eng/theory/modes-of-block-ciphers.html)**)**
3. **Because of the differences in how much of the original data can be retrieved from a corrupted cypher text file, the implications depend on the circumstances, in the case where bad actors are involved in decrypting the file, the method of encryption/decryption is important because less data can be recovered to prevent information ending up in the wrong hands. However, in the case where extremely important encrypted information ends up with the rightful receiver, the loss of data can lead to misinterpretation or misrepresentation of the original message, leading to detrimental outcomes.**

# **Task 4:**

**A white background with black text

Description automatically generated**

**Original text (with padding):**

**A screenshot of a computer

Description automatically generated**

**Hex view of original text:**

**A screenshot of a computer

Description automatically generated**

**Padded cypher:**

**A black and white photo frame

Description automatically generated with medium confidence**

**Hex view of padded cypher:**

**A screenshot of a computer

Description automatically generated**

**Hex view of modified bytes in padded cypher:**

**A screenshot of a computer

Description automatically generated**

**Decrypted cypher file after altering bytes such that only the padding is viewable:**

**A screen shot of a computer

Description automatically generated**

**Command line arguments for Task 4.**

**A screenshot of a computer

Description automatically generated**

1. **The Padding scheme used is PKCS#7.**
2. **See screenshot above.**
3. **12 Bytes are added for a 32-byte file.**
4. **See screenshot above.**