**Homework - 3**

**1. Suppose two plaintext samples P and Q are encrypted using a block cipher with the same secret key K and the same initialization vector IV (or nonce) for those modes that require it. Suppose each plaintext sample is divided into 100 blocks (including padding). If all the plaintext blocks of P and Q are the same, except for block 10, in which they differ by 1 bit, compare the corresponding cipher text for each block cipher mode**

**- Electronic Codebook**

Each block is encrypted with the secret key, K.

Identical Blocks - All, except 10.

Different blocks - Block 10.

**- Cipher Block Chaining**

Identical blocks - 1, 2, 3, 4, 5, 6, 7, 8, 9.

Different Blocks - 10, 11, 12, ……. , 100.

**- Counter Mode:** Turns a block cipher into a stream cipher.

Identical blocks - All, except 10.

Different blocks - Block 10.

**- Cipher Feedback Mode**

Identical blocks - 1, 2, 3, 4, 5, 6, 7, 8, 9.

Different Blocks - 10, 11, 12, ……. , 100.

**- Output Feedback Mode**

Identical blocks - 1, 2, 3, 4, 5, 6, 7, 8, 9.

Different Blocks - 10, 11, 12, ……. , 100.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2. Same as #1, except assume P and Q are encrypted with a different IV (nonce) as recommended by cryptographers.**

**- Electronic Codebook**

ECB doesn’t make use of IV.

Each block is encrypted with the secret key, K.

Identical Blocks - All, except 10.

Different blocks - Block 10.

**- Cipher Block Chaining**

Identical blocks - None.

Different Blocks - The first block (different IV). Each block takes the output from the previous block, and hence, all blocks differ.

**- Counter Mode:** Turns a block cipher into a stream cipher.

Identical blocks - None.

Different blocks - All, as nonce is different for each.

**- Cipher Feedback Mode**

Identical blocks - None.

Different Blocks - The first block (different IV). Each block takes the output from the previous block, and hence, all blocks differ.

**- Output Feedback Mode**

Identical blocks - None.

Different Blocks - The first block (different IV). Each block takes the output from the previous block, and hence, all blocks differ.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3. Suppose two cipher text samples P and Q are decrypted using key K and the same IV (or nonce) when required. Suppose each cipher text sample of 100 blocks differs by 1 bit in block 25 only. Compare the corresponding plaintext blocks following decryption of P and Q for each block cipher mode.**

**- Electronic Codebook**

Identical blocks - 1, 2, 3, 4, ……… , 24, 26, 27 …… 100.

Different Blocks - 25

**- Cipher Block Chaining**

Identical blocks - 1, 2, 3, 4, …… , 24

Different blocks - 25, 26, 27, 28, …… 100.

**- Counter Mode:**Turns a block cipher into a stream cipher.

Identical blocks - 1, 2, 3, 4, ……… , 24, 26, 27 …… 100.

Different Blocks - 25

**- Cipher Feedback Mode**

Identical blocks - 1, 2, 3, 4, …… , 24

Different blocks - 25, 26, 27, 28, …… 100.

**- Output Feedback Mode**

Identical blocks - 1, 2, 3, 4, ……… , 24, 26, 27 …… 100.

Different Blocks - 25

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4. Assume each cipher text block is stored on a separate disk block that can be accessed independently. Suppose only block 50 of an encrypted file of 100 blocks needs to be accessed. Which specific blocks of cipher text must be accessed to obtain the plaintext for block 50 for the following modes?**

**- Electronic Codebook:** Block 50.

**- Cipher Block Chaining:** Block 49 and 50.

**- Counter Mode:** Block 50.

**- Cipher Feedback Mode:** Block 49 and 50.

**- Output Feedback Mode:** Block 50.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**5. Which modes permit parallel encryption?**

Electronic Codebook and Counter Mode permit parallel encryption.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6. Which mode permits parallel decryption?**

Electronic Codebook, Counter Mode, Cipher Feedback Mode, Cipher Block Chaining and Output Feedback Mode permit parallel decryption.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**7. Which modes permit pre-computation of key stream?**

Output Feedback Mode and Counter Mode permit pre-computation of key stream.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_