Hw2

Jackson Mowry

Tue Sep 2 09:12:18 2025

Complete each question described below. When comparing blocks of ciphertext or plaintext, if corresponding blocks differ then mention which specific blocks differ. If they differ by only 1 bit, mention that fact specifically. If they differ by more than 1 bit, simply state the specific blocks that differ completely. If all blocks differ in the full ciphertext, simply state that there is no relationship. Be as precise as you can in your comparisons to illustrate that you understand the various modes.

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 ciphertext for each block cipher mode.

   - ECB
     - Only block 10 would differ, and the entire block differs completely
   - CBC
     - All blocks after and including block 10 differ
   - CTR
     - Only block 10 would differ, and it would differ by a single bit
   - CFB
     - Block 10 would differ by a single bit, then all following blocks would differ entirely
   - OFB

    - Block 10 would differ by a single bit, and all remaining blocks would match

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

   - ECB
     - No difference to the answer for #1 as there is no use of an IV
   - CBC
     - Every block differs
   - CTR
     - Every block differs
   - CFB
     - Every block differs
   - OFB
     - Every block differs

3. Suppose two ciphertext samples P and Q are decrypted using key K and the same IV (or nonce) when required. Suppose each ciphertext 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.

   - ECB
     - The entirety of plaintext block 25 would differ, with all other blocks matching exactly
   - CBC
     - The block 25 would differ by a bit
   - CTR
     - The block 25 would differ by a bit
   - CFB
     - The block 25 would differ by a bit, and all following blocks would be entirely different
   - OFB
     - The block 25 would differ by a bit

4. Assume each ciphertext 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 ciphertext must be accessed to obtain the plaintext for Block 50 for the following modes?
   - ECB
     - 50
   - CBC
     - 1-50
   - CTR
     - 50
   - CFB
     - 1-50
   - OFB
     - 50

5. Specify which of the following each mode allows: parallel encryption, parallel decryption, pre-computation of the key stream.
   - ECB
     - Parallel both, no need for pre-computation
   - CBC
     - Encryption serial, decryption parallel, cannot pre-compute
   - CTR
     - Parallel both, can pre-compute the key stream
   - CFB
     - Encryption serial, decryption parallel, cannot pre-compute
   - OFB
     - Both serial, can pre-compute the key stream