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 - All the blocks are the same except for block 10 which are randomly different.
   * CBC - Block 1 to 9 are the same, and from block 10 to 100 are randomly different.
   * CTR - All the blocks are the same except for block 10 which are randomly different.
   * CFB - Block 1 to 9 are the same, and from block 10 to 100 are randomly different.
   * OFB - All the blocks are the same except for block 10 which are randomly different.
2. Same as #1, except assume P and Q are encrypted with a different IV (nonce) as recommended by cryptographers.
   * ECB - All the blocks are the same except for block 10 which are randomly different.
   * CBC - All the blocks are randomly different.
   * CTR - All the blocks are randomly different.
   * CFB - All the blocks are randomly different.
   * OFB - All the blocks are randomly different.
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 - All the blocks are the same except for block 25 which are randomly different.
   * CBC - Block 1 to 24 are the same, and from block 25 to 100 are randomly different.
   * CTR - All the blocks are the same except for block 25 which are randomly different.
   * CFB - Block 1 to 24 are the same, and from block 25 to 100 are randomly different.
   * OFB - All the blocks are the same except for block 25 which are randomly different.
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 - Block 50.
   * CBC - Block 49 and 50.
   * CTR - Block 50.
   * CFB - Block 49 and 50.
   * OFB - Block 50.
5. Which modes permit parallel encryption?

ECB, CTR

1. Which modes permit parallel decryption?

ECB, CBC, CTR, CFB

1. Which modes permit pre-computation of the key stream?

CTR, OFB