Chritopher LaJon Morgan
Sep 12, 2013

Homework 3

CS 465

Comparison of Block Cipher Modes

- 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 the plaintext blocks differ only by 1 bit in block 10, compare the corresponding ciphertext for each block cipher mode
  - ECB

    All blocks would be identical except for block 10.

  - CBC

    Blocks 1 through 9 would appear identical, but blocks 10-100 would be different.

  - CTR

    All blocks except for block 10 would appear identical. Block 10 would differ by 1 bit.

  - CFB

    Blocks 1-9 would appear identical; block 10 differs by 1 bit, blocks 10-100 would be different.

  - OFB

    All blocks but block 10 would be identical. Block 10 would differ by one bit.

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

    All blocks would be identical except for block 10.

  - CBC

All blocks would be different.

- CTR

  All blocks would be different.

- CFB

  All blocks would be different.

- OFB

  All blocks would be different.

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

    All blocks will be identical except for block 25.

  - CBC

    Block 25 would be different and block 26 would be different by one bit.

  - CTR

    Only block 25 will be different and it will differ by a bit.

  - CFB

    Blocks 1-24 would be identical, block 25 would be different by one bit, block 26 would be completely different, and blocks 27-100 would be different.

  - OFB

    Block 25 would be different by one bit.

- Assume each cipher text block is stored on a disk block that can be accessed independently. Suppose block 50 of an encrypted file needs to be accessed. Which specific blocks of ciphertext must be accessed to perform the decryption for the following modes?
  - ECB

    Just block 50.

  - CBC

    Blocks 49 and 50.

  - CTR

    Just block 50.

  - CFB

    Blocks 49 and 50.

  - OFB

    Just block 50.

- Which modes permit parallel encryption?

  ECB, CTR

- Which modes permit parallel decryption?

  ECB, CBC, CTR, CFB, OFB

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

  OFB, CTR