Scott Christensen

09/10/16

CS. 465

H.W. #3

* 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: The small alteration in plaintext in block 10 will result in a large deviation in the ciphertext in block 10 only.
  + CBC: Because CBC encrypted plaintext is XOR-ed with subsequent plaintext blocks, an alteration in the 10th plaintext block will result in alterations between P and Q in block 10 and all subsequent blocks.
  + CTR: The small alteration in plaintext in block 10 will result in a large deviation in the ciphertext in block 10 only. It only differs by 1 bit.
  + CFB: Because CBC plaintext is encrypted and XOR-ed in subsequent blocks, an alteration in the 10th plaintext block will result in alterations between P and Q in block 10 by 1 bit and all subsequent blocks very much different.
  + OFB: The small alteration in plaintext in block 10 will result in a 1 bit difference in the ciphertext in block 10 only.
* Same as #1, except assume P and Q are encrypted with a different IV (nonce) as recommended by cryptographers.
  + ECB: There will be no difference in the results, as ECB doesn’t use a IV in its implementation. The small alteration in plaintext in block 10 will result in a large deviation in the ciphertext in block 10 only.
  + CBC: No relationship.
  + CTR: No relationship.
  + CFB: No relationship.
  + OFB: No relationship.
* 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 small alteration in the ciphertext in block 25 will result in a large deviation in the plaintext in block 25 only.
  + CBC: Because CBC ciphertext is XOR-ed with subsequent plaintext blocks, an alteration in the 25th plaintext block will result in alterations between P and Q in block 25 and block 26 differs by 1 bit.
  + CTR: The small alteration in ciphertext in block 25 will result in a 1 bit difference in the ciphertext in block 25 only.
  + CFB: There will be a 1 bit difference in block 25 and a large change in each subsequent block.
  + OFB: There is a 1 bit alteration in ciphertext in block 25 will result in a large deviation in the plaintext in block 25 only.
* 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: Only the ciphertext at block 50 would be needed in order to obtain the plaintext for block 50.
  + CBC: You would need the ciphertext from blocks 49 and 50 in order to get the plaintext in block 50.
  + CTR: Only the ciphertext at block 50 would be needed in order to obtain the plaintext for block 50.
  + CFB: You’d need the ciphertext from block 49 and 50 in order to obtain the plaintext for block 50.
  + OFB: Only the ciphertext at block 50 would be needed in order to obtain the plaintext for block 50.
* Which modes permit parallel encryption?

ECB, CTR

* Which modes permit parallel decryption?

ECB, CBC, CFB, CTR

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

CTR, OFB