COMP-424 Classwork April 5, 2016

BLOCK CIPHER OPERATION

TRUE OR FALSE

T F 1. A mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application.

T F 2. Given the potential vulnerability of DES to a brute-force attack, an alternative has been found.

T F 3. A number of Internet based applications have adopted two-key 3DES, including PGP and S/MIME.

T F 4. The sender is the only one who needs to know an initialization Vector (IV) in the CBC mode of operation.

MULTIPLE CHOICE

1. Triple DES makes use of _________ stages of the DES algorithm, using a total of two or three distinct keys.

   A. nine B. six

   C. twelve D. three

2. _________ modes of operation have been standardized by NIST for use with symmetric block ciphers such as DES and AES.

   A. Three B. Five

   C. Nine D. Seven

3. The simplest form of multiple encryption has _________ encryption stages and _________ keys.

   A. four, two B. two, three

   C. two, two D. three, two

4. The _________ algorithm will work against any block encryption cipher and does not depend on any particular property of DES.

   A. cipher block chaining B. meet-in-the-middle attack

   C. counter mode attack D. ciphertext stealing

5. The _________ method is ideal for a short amount of data and is the appropriate mode to use if you want to transmit a DES or AES key securely.

   A. cipher feedback mode B. counter mode

   C. output feedback mode D. electronic codebook mode

SHORT ANSWER

1. The_________ is a technique in which an encryption algorithm is used multiple times.

2. The most significant characteristic of _________ is that if the same b-bit block of plaintext appears more than once in the message, it always produces the same ciphertext.

3. A _________ is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream.

4. Five modes of operation have been standardized by NIST for use with symmetric block ciphers such as DES and AES: electronic codebook mode, cipher block chaining mode, cipher feedback mode, _________, and counter mode.

5. One of the most widely used multiple-encryption scheme is _________ .

6. The simplest mode of operation is the __________ mode, in which plaintext is handled one block at a time and each block of plaintext is encrypted using the same key.

Problems

1. With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C_1 obviously corrupts P_1 and P_2.

a. Are any blocks beyond P_1 and P_2 affected?
b. Suppose that there is a bit error in the source version of P_1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?

2. Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? How about decryption?

3. CBC-Pad is a block cipher mode of operation used in the RC5 block cipher, but it could be used in any block cipher. CBC-Pad handles plaintext of any length. The ciphertext is longer than the plaintext by at most the size of a single block. Padding is used to assure that the plaintext input is a multiple of the block length. It is assumed that the original plaintext is an integer number of bytes. This plaintext is padded at the end by from 1 to bb bytes, where bb equals the block size in bytes. The pad bytes are all the same and set to a byte that represents the number of bytes of padding. For example, if there are 8 bytes of padding, each byte has the bit pattern 00001000.Why not allow zero bytes of padding? That is, if the original plaintext is an integer multiple of the block size, why not refrain from padding?

4. For the ECB and CBC modes, the plaintext must be a sequence of one or more complete data blocks. In other words, the total number of bits in the plaintext must be a positive multiple of the block size. One common method of padding, if needed, consists of a 1 but followed by as few 0 bits, possibly none, as are necessary to complete the final block. It is considered good practice for the sender to pad every message, including messages in which the final message block is already complete. What is the motivation for including a padding block when padding is not needed?

5. What happens when two plaintexts are encrypted with the same key using a stream cipher?