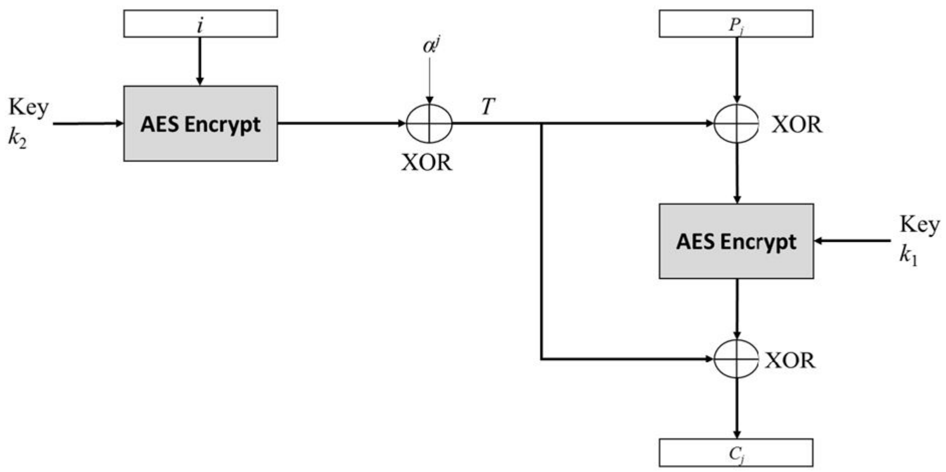
German University in Cairo
Faculty of MET (CSEN 1001 Computer and Network Security Course)
Dr. Amr El Mougy
Reham Ayman
Abdelrahman Osama

Practice Assignment 2 Solution

Discussion 15/02/2020 - 20/02/2020

1. The figure below shows the encryption diagram for the AES-XTS mode of encryption, which is used for data storage. In the figure, i, is a 128-bit value known as the tweak that is rarely changed, j is the number of the disk sector to be encrypted, α is a 128-bit fixed value, P_j is the data block in the j^th sector to be encrypted, and C_j is the resulting ciphertext. The system uses two symmetric keys k1 and k2 for the AES blocks.



   (a) Determine the formula for encryption (for calculating C_j).

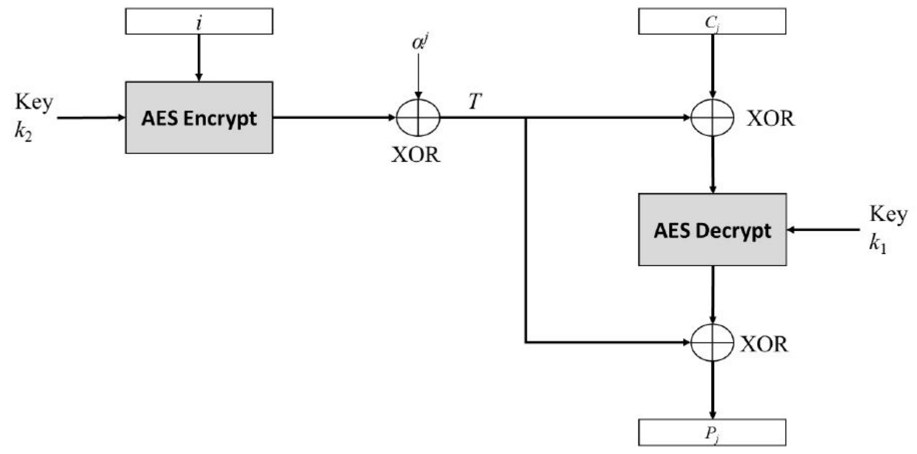
   (b) Determine the formula for decryption and draw the decryption algorithm.

   (c) If an error occurs in the j block of ciphertext (C_j, how many blocks will be affected in the decryption?

Solution:

(a) $T_J = E_{K2}(i) \oplus \alpha^j$
$C_j = E_{K1}(P_j \oplus T_j) \oplus T_j$

(b) $T_j = E_{K2}(i) \oplus \alpha^j$
$P_j = D_{K1}(C_j \oplus T_j) \oplus T_j$



(c) There is no chaining, errors do not propagate.

2. Assume a regular cipher block chaining encryption algorithm, which processes blocks of 16 bit length. If the last block is less than 16 bit, it will be padded with zeros on the right. The block cipher encryption consists of only a permutation given with the table below. The key defines how often the permutation is applied on a block. On the other hand, chaining is done using an XOR operation. Encrypt the following plaintext:

Plain Text: "ROCKNROLL"

Initialization Vector (IV): 0101 0101 0101 0101
Permutation table (indexes): 10 3 5 16 7 2 1 12 11 14 8 6 15 9 4 13
Key: K=1
Chain Operation: XOR
Convert letters into 8-bit blocks using ASCII conversion: A = 65, B=66, C=67 ...

Solution:

Letters	R	O	C	K	N	R	O
ASCII Dec	82	79	67	75	78	82	79
ASCII Bin	01010010	01001111	01000011	01001011	01001110	01010010	01001111

Letters	L	L
ASCII Dec	76	76
ASCII Bin	01001100	01001100

1. Group each two letters into 16-bit blocks

2. XOR the first 16 bits with the IV:
   0101010101010101
   0101001001001111 **RO**
   0000011100011010

3. One-time (K=1) permutation using the above key: 0000100100111001

4. XOR the next 16 bitsblocks:
   0000100100111001
   0100001101001011 **CK**
   0100101001110010

5. One time permutation: 1010110110001000

6. XOR the next 16 bitsblocks:
   1010110110001000
   0100111001010010 **NR**
   1110001111011010

7. One-time (K=1) permutation using the above key: 1100111100101101

8. XOR the next 16 bitsblocks:
   1100111100101101
   0100111101001100 **PL**
   1000000001100001

9. One-time (K=1) permutation using the above key: 1001001010000000

10. Last block needs to be padded:
    1001001010000000
    0100110000000000 **L + Padding**
    1101111010000000

11. One-time (K=1) permutation using the above key: 0010111000010110

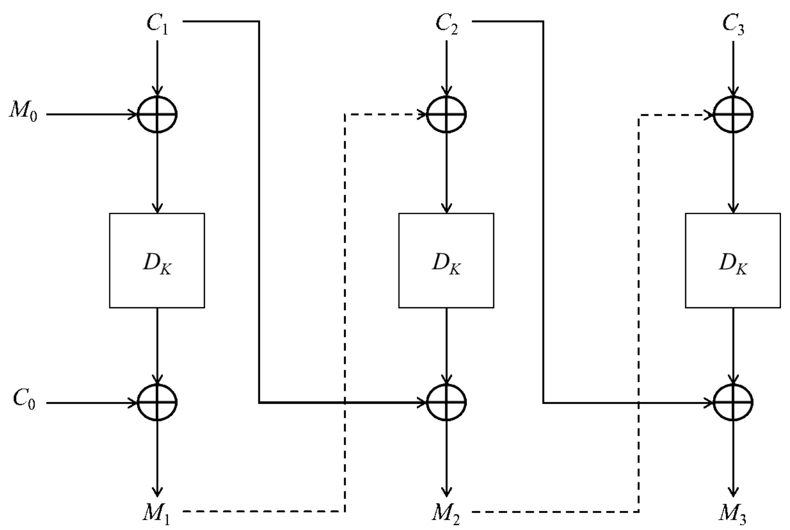
3. Let a block cipher with secret key K be chained in the following way:

$$C_i = M_{i-1} \oplus E((M_i \oplus C_{i-1}), K) \text{ for i} > 0$$

Where M_0 and C_0 are fixed public initialization vectors, K is the secret key known to both transmitter and receiver, and E and D represent encryption and decryption, respectively.

1. Determine the equation for decryption and draw the block diagram.
2. Suppose that ciphertext C_j is damaged in transmission, which plaintext blocks will be decrypted incorrectly?

Solution: $M_i = D(C_i \oplus M_{i-1}, K) \oplus C_{i-1}$



Chaining depends, not on the previous ciphertext, but on the previous message. Thus, an error C_j results in all subsequent blocks to be decrypted incorrectly.

4. (a) Suppose that we use DES in cipher block chaining (CBC) mode. The encryption rule for message M_i, key K and cipher C_i is:

$$C_i = DES(M_i \oplus C_{i-1,K}) \text{ i = 1,2,...}$$

where C_0 is an initial block and $\oplus$ is the XOR operation.

– What is the decryption rule (i.e. what is M_i=.........)? (You can alternatively draw a block diagram).

– Suppose an attacker changes C_i into $C_i' \neq C_i$. How many messages are then decrypted incorrectly?

(b) Suppose that we use DES in counter (CTR) mode. The encryption rule for key K and message M_i, at time i > 0 is

$$C_i = DES(R_i, K) \oplus M_i, \; R_i = R_i + 1$$

where R_0 = some starting value and $\oplus$ is the XOR operation..

– What is the decryption rule (i.e. what is M_i=........)? (You can alternatively draw a block diagram).

– Suppose an attacker changes C_i into $C_i' \neq C_i$. How many messages are then decrypted incorrectly?

Solution:

(a) $M_i = DES(C_i, K) \oplus C_{i-1}$ i = 1, 2, ... The messages decrypted incorrectly are i and the subsequent one.

(b) $M_i = DES(R_i, K) \oplus C_i$, $R_i = R_i + 1$ The message decrypted correctly is only i.

5. Alice and Bob agree to communicate privately via email using a scheme based on RC4, but want to avoid using the same secret key for each transmission. Alice and Bob privately agree on a 128-bit key k. to encrypt a message m, consisting of a string of bits, the following procedure is used:

   - Choose a random 80-bit key value v.
   - Generate the ciphertext c = RC4(v ∥ k) ⊕ m
   - Send the bit string (v ∥ c)

   1. Suppose Alice uses this procedure to send a message m to Bob. Describe how Bob can recover the message m from (v ∥ c) using k.
   2. If an adversary observes several values $(v_1 \parallel c_1)$, $(v_2 \parallel c_2)$....transmitted between Alice and Bob, how can he/she determine when the same key has been used to encrypt two messages?

Solution:

(a) By taking the first 80 bits of v ∥ c, we obtain the initialization vector, v. Since v, c, k are known, the message can be recovered (i.e., decrypted) by computing RC4(v ∥ k) ⊕ c.

(b) If the adversary observes that $v_i = v_j$ for distinct i, j then he/she knows that the same key stream was used to encrypt both m_i and m_j. In this case, the messages m_i and m_j may be vulnerable to the type of cryptanalysis carried out in part (a).

6. In a particular system, Alice wishes to send a message, M, to Bob using public key cryptography. Each time, Alice is going to desire to achieve some (or all) the objectives of Confidentiality, Integrity, and Non-repudiation. Alice's public and private keys are denoted by (PU_A, PR_A), while the keys of Bob are denoted by (PU_B, PR_B). An

encryption process in this system is denoted by E(K, M), where K is the key (could be a public or private key) and M is the plaintext. For each of the following situations, specify which of these objectives is achieved and explain why.

(a) Alice sends E(PU_B, M)

(b) Alice sends E(PR_A, M)

(c) Alice sends E(PU_B, E(PR_A, M))

(d) Alice sends E(PR_A, E(PU_B, M))

Solution:

(a) Confidentiality. Bob will decrypt with his private key

(b) Non-repudiation. No one could generate the message but Alice.

(c) Confidentiality and non-repudiation due to double encryption.

(d) Same as c), the order does not matter.