Fundamentals of Cryptography

Homework 2

Dr. Mohammad Dakhilalian

Fall 2023

Theory Part

Question 1

A DES key K_w is called *a weak key* if encryption and decryption are identical operations:

$$DES_{K_w}(x) = DES^{-1}_{K_w}(x) \text{ , for all } x$$

1. Describe the relationship of the subkeys in the encryption and decryption algorithm that is required so that the equation above is fulfilled.
2. There are four weak DES keys. What are they?
3. What is the likelihood that a randomly selected key is weak?

Question 2

We want to show that

$$y = DES_k(x) \Longrightarrow y' = DES_{k'}(x')$$

Try to prove this property using the following steps:

1. Show that for any bit strings A, B of equal length:

$$A' \oplus B' = A \oplus B$$
$$A' \oplus B = (A \oplus B)'$$

2. Show that

$$PC-1(k') = (PC-1(k))'$$

3. Show that

$$LS_i(C'_{i-1}) = (LS_i(C_{i-1}))'$$

4. Using the two results from above, show that if k_i are the keys generated from k, then k'_i are the keys generated from k', where i = 1,2,...,16.
5. Show that

$$IP(x') = (IP(x))'$$

6. Show that

$$E(R'_i) = (E(R_i))'$$

7. Using all previous results, show that if R_{i-1}, L_{i-1}, k_i generate R_i, then R'_{i-1}, L'_{i-1}, k'_i generate R'_i.
8. Show that $y = DES_k(x) \Longrightarrow y' = DES_{k'}(x')$ is true.

Question 3

It is desirable for good block ciphers that a change in one input bit affects many output bits, a property that is called diffusion or the avalanche effect. Now we want to inspect the avalanche property of DES. We apply an input word that has a "1" at bit position 57 and all other bits as well as the key are zero.
(Note that the input word has to run through the initial permutation.)

1. How many S-boxes get different inputs compared to the case when an all-zero plaintext is provided?
2. What is the minimum number of output bits of the S-boxes that will change according to the S-box design criteria?
3. What is the output after the first round?
4. How many output bits after the first round have changed compared to the case when the plaintext is all zero?
   (Note that we only consider a single round here. There will be more and more output differences after every new round.)

Question 4

Consider the irreducible polynomial $P(x) = x^4 + x + 1$:

1. Compute $A(x) + B(x) \bmod P(x)$ in $GF(2^4)$.
2. Compute $A(x) * B(x) \bmod P(x)$ in $GF(2^4)$.
   - $A(x) = x^2 + 1$, $B(x) = x^3 + x^2 + 1$
   - $A(x) = x^2 + 1$, $B(x) = x + 1$

Question 5

Find all irreducible polynomials

1. of degree 3 over $GF(2)$.
2. of degree 4 over $GF(2)$.

(The best approach for doing this is to consider all polynomials of lower degree and check whether they are factors. Please note that we only consider monic irreducible polynomials, i.e., polynomials with the highest coefficient equal to one.)

Question 6

We consider AES with 128-bit block length and 128-bit key length. What is the output of the first round of AES if the plaintext consists of 128 ones, and the first subkey also consists of 128 ones?
You can write your final results in a rectangular array format if you wish.

Question 7

We consider known-plaintext attacks on block ciphers by means of an exhaustive key search where the key is k bits long. The block length counts n bits with $n > k$.

1. How many plaintexts and ciphertexts are needed to successfully break a block cipher running in ECB mode? How many steps are done in the worst case?
2. Assume that the initialization vector IV for running the considered block cipher in CBC mode is known. How many plaintexts and ciphertexts are now needed to break the cipher by performing an exhaustive key search? How many steps need now maximally be done?

3. How many plaintexts and ciphertexts are necessary if you do not know the IV?

4. Is breaking a block cipher in CBC mode by means of an exhaustive key search considerably more difficult than breaking an ECB mode block cipher?

Question 8

Sometimes error propagation is an issue when choosing a mode of operation in practice. In order to analyze the propagation of errors, let us assume a bit error in a ciphertext block y_i.
(i.e., a substitution of a "0" bit by a "1" bit or vice versa)

1. Assume an error occurs during the transmission in one block of ciphertext, let's say y_i. Which cleartext blocks are affected on Bob's side when using the ECB mode?

2. Again, assume block y_i contains an error introduced during transmission. Which cleartext blocks are affected on Bob's side when using the CBC mode?

3. Suppose there is an error in the cleartext x_i on Alice's side. Which cleartext blocks are affected on Bob's side when using the CBC mode?

4. Assume a single-bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode. How far does the error propagate? Describe exactly how each block is affected.

Programming Part

Question 9

Here you have to implement an AES in CBC mode with Python. What are the advantages and disadvantages of this mode?
(Note that you can use the Crypto library)