Лабораторна робота №4
Система блокового шифрування S-DES

Мета:

Створити просту криптографічну систему на основі спрощеного блочного алгоритму Simple DES (S-DES) та дослідити її роботу.

Обладнання:

- персональний комп'ютер з встановленою операційною системою;
- будь-яка мова програмування.

Завдання:

1. Створити просту криптографічну систему на основі спрощеного блочного алгоритму S-DES.
2. Перевірити її роботу.

Література:

1. В.Столлингс. Криптография и защита сетей. М.: «Вільямс», 2001. – 672 с.
2. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные коды на языке С. 1996.

Теоретичні відомості

Спрощений DES – це алгоритм шифрування, який має, скоріше, навчальне, ніж практичне значення. За своїми властивостями він подібний до DES, але має значно менше параметрів [1].

Цей алгоритм приймає на вході 8-бітний блок відкритого тексту та 10-бітний ключ, а на виході генерує 8-бітний блок шифрованого тексту. При розшифруванні на вхід алгоритму подається 8-бітний блок шифротексту і 10-бітний ключ, а на виході генерує 8-бітний блок відкритого тексту.

Алгоритм шифрування передбачає послідовне виконання п'яти операцій: початкової перестановки *IP*; циклової функції, що складається з перестановок та підстановок; перестановки *SW*, коли дві половинки блоку по 4 біти переставляється місцями; ще одного застосування циклової функції; і, нарешті, перестановки IP^{-1}, оберненої до початкової. Послідовне використання кількох перестановок та підстановок, як це показано у [1-2], значно ускладнюють криптоаналіз.

Циклова функція приймає на вході не лише блок тексту, а й 8-бітний цикловий підключ, який утворюється з 10-бітного ключа.

Блок-схему алгоритму подано на рис. 1. З цього рисунку видно, що, оскільки це симетричний криптоалгоритм, він використовує для шифрування та розшифрування один і той самий ключ. Тому ключ має бути як на передавальній, так і на приймальній стороні. З цього ключа на певних етапах шифрування та розшифрування генерується два 8-бітних циклових підключа.

Процедура генерування циклових підключів

1. Спочатку переставляються біти ключа таким чином. Якщо 10-бітний ключ уявити у вигляді $k_1,k_2,\ldots,k_{10}$, то перестановка P10 задається формулою:

$$P(k_1,k_2,k_3,k_4,k_5,k_6,k_7,k_8,k_9,k_{10}) = (k_3,k_5,k_2,k_7,k_4,k_{10},k_1,k_9,k_8,k_6).$$

Можна також зобразити перестановку P10 у вигляді таблиці:

P10									
3	5	2	7	4	10	1	9	8	6

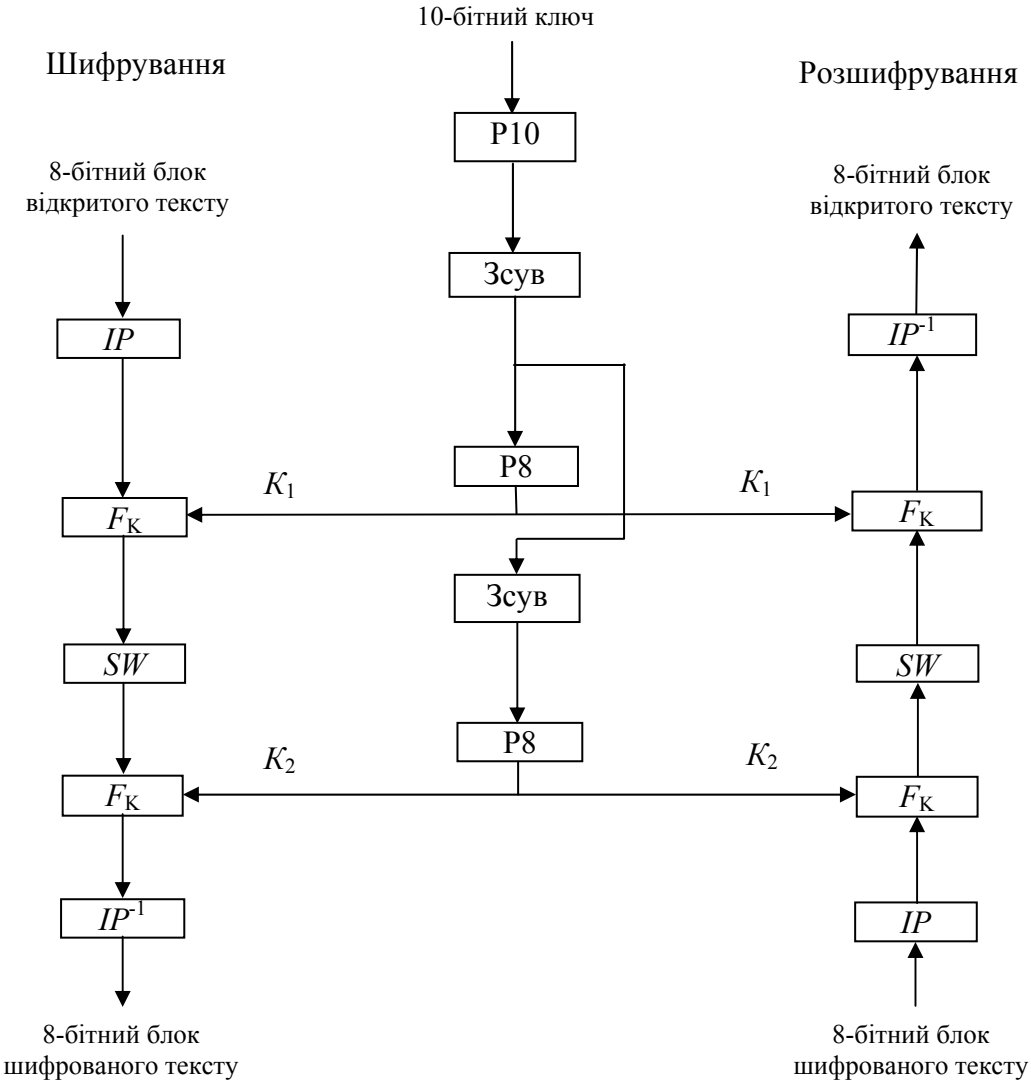

Рис. 1. Схема спрощеного алгоритме DES

Ця таблиця символізує позицію біту вхідних даних у вихідній послідовності: першм стає 3-й біт, другим – 5-й, третім – 2-й і т.д. Наприклад, ключ (1010000010) у відповідності з цією перестановкою перетворюється у послідовність (1000001100).

2. Ключ розділяється на дві половинки по п‘ять бітів кожна. Окремо перша половина і окремо друга піддаються циклічному зсуву ліворуч на одну позицію. У нашому прикладі в результаті буде отримана послідовність (00001 11000).

3. Отримана послідовність піддається перестановці P8, в результаті якої з 10-бітного ключа обираються 8-бітова послідовність за таким правилом:

P8							
6	3	7	4	8	5	10	9

В результаті цієї операції ми отримаємо перший цикловий підключ (K_1). У нашому прикладі він буде мати вигляд (10100100).

4. Для генерування другого циклового підключа K_2 необхідно повернутися на крок назад, до двох 5-бітових рядків до застосування P8 та виконати для кожного з цих рядків циклічний зсув ліворуч на дві позиції. У нашому прикладі значення підключів (00001 11000) перетворяться у (00100 00011).

5. Нарешті, застосувавши до цієї послідовності перестановку P8, отримаємо другий цикловий підключ K_2. Для нашого прикладу результатом буде (01000011).

Шифрування S-DES

1. *Початкова і кінцева перестановки (IP та IP^{-1}).* На вхід алгоритму подається 8-бітний блок відкритого тексту, до якого застосовується початкова перестановка IP:

IP							
2	6	3	1	4	8	5	7

На завершальній стадії алгоритму виконується обернена перестановка IP^{-1}:

IP^{-1}							
4	1	3	5	7	2	8	6

Можна пересвідчитися, що ці дві таблиці дійсно обернені одна до другої тобто $IP^{-1}(IP(M))=M$.

2. *Циклова функція* F_K. Розіб‘ємо вхідний блок тексту після IP-перестановки на два 4-бітні підблоки. Лівий 4-бітний блок позначимо через L, а правий - через R. Тоді циклову функцію можна записати у вигляді такої формули:

$$F_K(L,R) = (L \oplus F(R,K_i),R). \qquad (1)$$

Тут K_i означає цикловий підключ, K_1 або K_2; $\oplus$ - побітове XOR.

Тепер опишемо саму циклову функцію. На вході вона отримує 4-бітне значення (n_1,n_2,n_3,n_4), тобто праву половину вхідного блоку. Перша операція – операція розширення та перестановки. Її можна також зобразити табличкою:

Розширення з перестановкою							
4	1	2	3	2	3	4	1

Зручніше цю операцію зобразити у вигляді такої матриці:

$$\begin{matrix} n_4 & n_1 & n_2 & n_3 \\ n_2 & n_3 & n_4 & n_1 \end{matrix}$$

До цього значення додається 8-бітний підключ за допомогою операції XOR. Це можна зобразити наступним чином:

$$\begin{matrix} n_4+k_1 & n_1+k_2 & n_2+k_3 & n_3+k_4 \\ n_2+k_5 & n_3+k_6 & n_4+k_7 & n_1+k_8 \end{matrix}$$

Перейменуємо отримані елементи наступним чином:

$$\begin{matrix} p_{00} & p_{01} & p_{02} & p_{03} \\ p_{10} & p_{11} & p_{12} & p_{13} \end{matrix}$$

Перші чотири біти (тобто перший рядок цієї матриці) далі подаються на вхід модуля заміни (S-матриці), S_0, на виході якого отримується 2-бітна послідовність. Другий рядок матриці подається на вхід другого модуля заміни, S_1, на виході якого також отримується 2-бітна послідовність.

Модулі S_0 та S_1 задаються наступним чином:

$$S_0 = \begin{matrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 1 \end{matrix}; \quad S_1 = \begin{matrix} 1 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{matrix}$$

Рядки та стовпчики нумеруються, починаючи з нуля.

Ці модулі заміни працюють наступним чином. Перший і четвертий біти вхідної послідовності вважаються за двійкове представлення номера рядка, а другий та третій – номера стовпчика. Елемент, що знаходиться на перетині цих рідка і стовпчика задає двобітне вихідне значення. Наприклад, якщо (p_{00}, p_{03}) = (00) та (p_{01}, p_{02})=(10), то вихідні два біти задаються значенням, яке знаходиться на перетині 0-го рядка та 3-го стовпчика, тобто буде числом 3, а у двійковому представленні –11.

Аналогічну операцію виконують і з другим рядком p_{10} p_{11} p_{12} p_{13}.

Після застосування матриць заміни результат піддають перестановці P4 за таким законом:

P4			
2	4	3	1

Результат перестановки P4 і буде результатом функції F_K. Отримана послідовність бітів додається за модулем 2 з лівою половиною L вхідного блоку і буде новою лівою половинкою. Права половина передається на вихід циклу без змін.

3. *Перестановка підблоків*. Як бачимо, за один цикл цикловою функцією обробляється лише ліва половина відкритого тексту, права половина залишається без змін. Для того, щоби зашифрувати й праву половину, використовується другий цикл, однак на його вхід треба подати переставлені підблоки: L і R поміняти місцями. Для цього й служить функція SW – перемикач блоків.

Після переставляння підблоків один цикл алгоритму закінчено.

До переставлених підблоків знову застосовується циклова функція, як це описано вище. При другому виклику циклової функції розширення з перестановкою, модулі S_0 та S_1 та P4 залишаються тими ж, тільки використовується підключ K_2.

По закінченні другого циклу виконується IP^{-1}-перестановка і роботу алгоритму закінчено, тобто на виході маємо зашифрований текст.

Розшифрування зашифрованого тексту

Як видно з рисунку 1, розшифрування зашифрованого тексту виконується аналогічно шифруванню за винятком того, що ключі подаються у зворотному порядку.

Практична частина

1. Використовуючи будь-яку мову програмування створіть програму, яка б шифрувала та розшифровувала текстові повідомлення за допомогою криптосистеми S-DES.

2. Перевірте правильність функціонування криптосистеми, зашифрувавши та розшифрувавши текст. Порівняйте отриманий результат з відкритим текстом.

3. Здійсніть шифрування та розшифрування двох інших текстів на різних криптографічних ключах та зробіть висновок про правильність функціонування створеної програми.

4. Зробіть висновок з лабораторної роботи.

Підготуйте звіт з лабораторної роботи. Звіт повинен містити: а) протокол Ваших дій; б) код програми; в) відкриті та зашифровані тексти, а також криптографічні ключі, на яких виконувалося шифрування; г) результати порівняння розшифрованих текстів з відкритими; д) висновки з лабораторної роботи; е)відповіді на контрольні запитання.

Контрольні запитання:

1. До якого класу криптоалгоритмів належить спрощений DES, розглянутий у цій роботі?
2. Які особливості цього алгоритму?
3. Чим він відрізняється від алгоритму DES?
4. Особливості обробки криптографічного ключа у S-DES.
5. Опишіть структуру циклової функції у S-DES.
6. Чи не можна було би зробити S-DES з одним циклом? Чому?
7. Для чого потрібні перестановки IP та IP^{-1}?