



Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Факультет інформатики та обчислювальної техніки
Кафедра інформаційні систем та технологій

Лабораторна робота №2
із дисципліни «Безпека інформаційних систем»
Тема: «Шифр DES»

Виконала:
Студент групи ІА-31
Самелюк А.С.

Перевірив:
Шимкович Л.Л.

Тема: Шифр DES.

Хід роботи:

1. Задаємо слово та ключ:

Слово: квіточка

Ключ: автобуси

Введення початкових даних

Для проходження тесту Ви повинні ввести шифроване повідомлення та ключ шифрування. Розмір повідомлення, що шифрується, і ключа повинен дорівнювати 8 байтам.

Повідомлення

квіточка EA E2 B3 F2 EE F7 EA E0

11101010 11100010 10110011 11110010 11101110 11110111 11101010 11100000

Ключ шифрування

автобуси E0 E2 F2 EE E1 F3 F1 E8

11100000 11100010 11110010 11101110 11100001 11110011 11110001 11101000

Вперед >>

2. Початкова перестановка:

Використовуючи таблицю та послідовність, отриману з вхідного слова, отримуємо початкову перестановку.

Тест N1 "Початкова перестановка"

Виконайте перестановку вхідної послідовності згідно з таблицею. Результат введіть у вікні редактора "Результат".

Натисніть кнопку "Демонстрація" для наочного навчання...

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Номер зазначеного біта

4

Вхідна послідовність

11101010 11100010 10110011 11110010 11101110 11110111 11101010 11100000

Результат

11111011001011000011000000100100111111111111110101000101111111

Демонстрація

Вперед >>

3. Отримання послідовностей $R(0)$ та $L(0)$:

Ділимо вхідну послідовність на дві($R(0)$ - перша половина, $L(0)$ - друга половина)

Тест N2 "Отримання послідовностей $R(0)$ та $L(0)$ "

Розділіть отриману в попередньому тесті послідовність на дві послідовності $L(0)$ та $R(0)$, згідно з таблицями 1,2 відповідно. Натисніть кнопку "Демонстрація" для одержання послідовності $L(0)$.

Номер зазначеного біта

Вхідна послідовність
 11111011 00101100 00110000 00100100 11111111 11111111 01010001 01111111

Послідовність $L(0)$

Послідовність $R(0)$

Демонстрація

Вперед >>

Таблиця 1

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24
25	26	27	28
29	30	31	32

Таблиця 2

33	34	35	36
37	38	39	40
41	42	43	44
45	46	47	48
49	50	51	52
53	54	55	56
57	58	59	60
61	62	63	64

4. Функція вибору та перестановки послідовності В:

Використовуючи таблицю та послідовність, отриману з ключа шифрування, отримуємо перестановку послідовності В.

Тест N3 "Функція вибору та перестановки послідовності В"

Виконайте перестановку вхідної послідовності згідно з таблицею. Результат введіть у вікні редактора "Результат". Для демонстрації прикладу натисніть кнопку "Демонстрація".

Номер зазначеного біта

Вхідна послідовність
 11100000 11100010 11110010 11101110 11100001 11110011 11110001 11101000

Результат

Демонстрація

Вперед >>

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

5. Отримання послідовностей $C(0)$ та $D(0)$:

Ділимо вхідну послідовність на дві($C(0)$ - перша половина, $D(0)$ - друга половина)

Тест N4 "Отримання послідовностей C0 та D0"

Розділіть отриману в попередньому тесті послідовність на дві послідовності C(0) та D(0), згідно з таблицями 1,2 відповідно. Натисніть кнопку "Демонстрація" для одержання послідовності C(0).

Номер зазначеного біга

Вхідна послідовність

11111111 11111111 11111111 01100010 11100000 10001000 10000100

Послідовність C(0)

11111111111111111111111110110

Послідовність D(0)

0010111000001000100010000100

Демонстрація

Вперед >>

Таблиця 1

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Таблиця 2

29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49
50	51	52	53	54	55	56

6. Отримання послідовності $C(i)$:

Всього є 16 ітерацій. Номер ітерації: $i = 14$. Додаємо всі зрушення з таблиці до даної ітерації ($1+1+2+2+2+2+2+2+1+2+2+2+2+2 = 24$). Щоб отримати $C(i) = C(14)$ робимо зсув вліво на 24 біти. Щоб отримати $C(i-1) = C(13)$, робимо зсув на ($1+1+2+2+2+2+2+2+1+2+2+2+2 = 22$) 22 біти вліво. Щоб отримати $C(i-2) = C(12)$, робимо зсув на ($1+1+2+2+2+2+2+2+1+2+2+2 = 20$) 20 бітів вліво.

Тест N5 "Отримання послідовності C(i)"

Отримайте послідовність C(i) з отриманої на попередньому кроці послідовності C(0), шляхом зсуву послідовності C(i-1) на кількість біт зазначених у таблиці. Для демонстрації отримання C(i-1) із C(i-2) натисніть кнопку "Демонстрація".

Для того щоб отримати послідовність C(13) зрушуємо на 2 біт(а) послідовність C(12)

Номер ітерації i

14

Вхідна послідовність C(0)

11111111 11111111 11111111 0110

Послідовність C(i-2)

111011011111111111111111111111

Послідовність C(i-1)

101101111111111111111111111111

Послідовність C(i)

110111111111111111111111111110

Демонстрація

Таблиця

N	Зруше
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Вперед >>

7. Отримання послідовності $D(i)$:

Всього є 16 ітерацій. Номер ітерації: $i = 5$. Додаємо всі зрушення з таблиці до даної ітерації ($1+1+2+2+2=8$). Щоб отримати $D(i) = D(14)$ робимо зсув вліво на 8 бітів. Щоб отримати $D(i-1) = D(4)$, робимо зсув на ($1+1+2+2=6$) 6 бітів вліво. Щоб отримати $D(i-2) = D(3)$, робимо зсув на ($1+1+2=4$) 4 біти вліво.

Тест N6 "Отримання послідовності $D(i)$ "

Отримайте послідовність $D(i)$ з отриманої на попередньому кроці послідовності $D(0)$, шляхом зсуву послідовності $D(i-1)$ на кількість біт зазначених у таблиці. Для демонстрації отримання $D(i-1)$ із $D(i-2)$ натисніть кнопку "Демонстрація".

Для того щоб отримати послідовність D (4) зрушуємо на 2 біт(а) послідовність $D(3)$

Номер ітерації i

Вхідна послідовність $D(0)$

Послідовність $D(i-2)$

Послідовність $D(i-1)$

Послідовність $D(i)$

Демонстрація

Вперед >>

N	Зрусь
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

8. Отримання послідовностей $K(i)$:

Для отримання $C(i)D(i)$, з'єднуємо дві послідовності поступово. Потім використовуючи таблицю та отриману послідовність, отримуємо $K(i)$.

Тест N7 "Отримання послідовностей $K(i)$ "

Для отримання послідовності $K(i)$ зробіть конкатенацію послідовностей $C(i)$ та $D(i)$. В отриманій послідовності $C(i)D(i)$ переставте біти згідно з таблицею. Для демонстрації натисніть кнопку "Демонстрація".

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Номер зазначеного біта

Послідовність $C(i)$

Послідовність $D(i)$

Послідовність $C(i)D(i)$

Послідовність $K(i)$

Демонстрація

Вперед >>

9. Функція E:

Використовуючи таблицю та послідовність R(i), отримуємо послідовність E.

Тест N8 "Функція E" ×

Використовуючи функцію E (дивись таблицю) провести перетворення послідовності R(i). Результат ввести у вікні редактора "Результат". Для демонстрації натискайте кнопку "Демонстрація".

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Номер зазначеного біта

Послідовність R(i)

Результат

10. Функція S(i):

Маємо вхідну послідовність: 111111 – b1b2b3b4b5b6. Номер рядка: b1b6 = 11 = 3. Номер стовпця: b2b3b4b5 = 1111 = 15. Елемент в таблиці з такими координатами - 14.

Тест N9 "Функції S(i)" ×

Виконайте перестановку вхідної послідовності згідно з таблицею. Результат введіть у вікні редактора "Результат".

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Номер стовпця Номер рядка Число

Вхідна послідовність

Результат

11. Функція шифрування.

$$L(i) = R(i-1) \Rightarrow L(16) = R(15)$$

$$R(i) = L(i-1) \text{ xor } F(R(i-1), K(i-1)) \Rightarrow R(16) = L(15) \text{ xor } F(R(15), K(15))$$

Для отримання $L(i)R(i)$, з'єднуємо дві послідовності поступово.

L(15)	0	1	0	0	0	1	1	0	1	0	1	0	1	1	0	1	1	1	1	0	1	0	0	1	1	1	1	1	1	0	0	0
F(R(15),K(15))	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	1	0	1	0	0	0	1	0	0
R(16)	0	0	0	0	0	1	0	1	1	0	1	0	1	1	0	0	1	1	0	0	1	0	0	0	1	0	1	1	1	1	0	0

Тест N10 "Функція шифрування"



Отримайте послідовність $L(16)R(16)$, використовуючи послідовності $L(15), R(15)$ і $F(R(15), K(16))$.
Для демонстрації натискайте кнопку "Демонстрація".

Послідовність L(15)

010001101010110110011111000

Послідовність R(15)

00100000010101011010101111000

Послідовність F(R(15),K(16))

01000011000000010010000101000100

Послідовність L(16)

00100000010101011010101111000

Послідовність R(16)

0000010110101100110010001011100

Послідовність L(16)R(16)

001000000101010110101011110000000101101011001100100010111100

Демонстрація

Вперед >>

12. Кінцева перестановка:

Використовуючи таблицю та вхідну послідовність, отримуємо кінцеву перестановку.

Тест N11 "Кінцева перестановка"



Виконайте перестановку послідовності, отриманої на попередньому кроці, згідно з таблицею. Результат введіть у вікні редактора "Результат".

Доведіть до кінця перестановку вхідної послідовності

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Номер зазначеного біта

Вхідна послідовність

Результат

Демонстрація

Вперед >>

13.Результат шифрування:

Результат шифрування



В результаті проведеного шифрування Ви отримали зашифрований текст

Вперед >>

Результати тесту:

Перегляньте результати тестування та оцініть свої знання !

Назва тесту	Кількість невірних бітів	Помилковість, %
Початкова перестановка	<input type="text" value="0"/>	<input type="text" value="0"/>
Отримання $L(0)$ та $R(0)$	<input type="text" value="0"/>	<input type="text" value="0"/>
Послідовність V	<input type="text" value="0"/>	<input type="text" value="0"/>
Отримання $C(0)$ та $D(0)$	<input type="text" value="0"/>	<input type="text" value="0"/>
Отримання $C(i)$	<input type="text" value="0"/>	<input type="text" value="0"/>
Отримання $D(i)$	<input type="text" value="0"/>	<input type="text" value="0"/>
Отримання $K(i)$	<input type="text" value="0"/>	<input type="text" value="0"/>
Отримання $S(i)$	<input type="text" value="0"/>	<input type="text" value="0"/>
Послідовність E	<input type="text" value="0"/>	<input type="text" value="0"/>
Функція шифрування	<input type="text" value="0"/>	<input type="text" value="0"/>
Кінцева перестановка	<input type="text" value="0"/>	<input type="text" value="0"/>

Вперед >>