



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

Лабораторна робота №2

з дисципліни «Безпека інформаційних систем»

Виконав:
студент групи ІА-
23:
Лядський Д.С.

Перевірив:
Шимкович Л.Л.

Київ 2024

Шифр DES.

Хід роботи:

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

Ключ шифрування

Вперед >>

Тест N1 "Початкова перестановка"

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

Доведіть до кінця перестановку вхідної послідовності

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

Вхідна послідовність

Результат

Демонстрація

Вперед >>

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).

Доведіть до кінця одержання послідовності R(0)

Номер зазначеного біта

Вхідна послідовність

Послідовність L(0)

Послідовність R(0)

Демонстрація

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

Вперед >>

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

Доведіть до кінця перестановку вхідної послідовності

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

Номер зазначеного біта

Вхідна послідовність

Результат

Демонстрація

Вперед >>

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).

Доведіть до кінця одержання послідовності D(0)

Номер зазначеного біта

Вхідна послідовність

00000000 10001111 11111111 01110011 11001100 10100000 01010011

Послідовність C(0)

0000000010001111111111110111

Послідовність D(0)

0011110011001010000001010011

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

Демонстрація

Вперед >>

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 $C(3)$ зрушуємо на 2 біт(а) послідовність $C(2)$

Номер ітерації i

4

Вхідна послідовність $C(0)$

00000000 10001111 11111111 0111

Послідовність $C(i-2)$

000000100011111111111011100

Послідовність $C(i-1)$

0000100011111111111101110000

Послідовність $C(i)$

0010001111111111110111000000

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 >>

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 (10) зрушуємо на 2 біт(а) послідовність $D(9)$

Номер ітерації i

Вхідна послідовність $D(0)$

Послідовність $D(i-2)$

Послідовність $D(i-1)$

Послідовність $D(i)$

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 >>

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

Доведіть до кінця перестановку послідовності C(i)D(i)

Номер зазначеного біта

Послідовність C(i)

Послідовність D(i)

Послідовність C(i)D(i)

Послідовність K(i)

Демонстрація

Вперед >>

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

Доведіть до кінця перестановку послідовності R(i)

Номер зазначеного біта

Послідовність R(i)

Результат

Демонстрація

Вперед >>

Тест N9"Функції S(i)"



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

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

Номер стовпця

Номер рядка

Число

Вхідна послідовність

Результат

[Вперед >>](#)

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

Доведіть побудову послідовностей $L(16), R(16)$ і $L(16)R(16)$ до кінця.

Послідовність $L(15)$

01101111101000010000101000110011

Послідовність $R(15)$

01111100000110110101011011001001

Послідовність $F(R(15), K(16))$

11011001011110111000010011110010

Послідовність $L(16)$

01111100000110110101011011001001

Послідовність $R(16)$

10110110110110101000111011000001

Послідовність $L(16)R(16)$

0111110000011011010101101100100110110110110101000111011000001

Демонстрація

Вперед >>

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 >>

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="1"/>	<input type="text" value="1"/>
Послідовність B	<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 >>

Висновок: Отже, на цій лабораторній роботі ми розглянули Шифр DES та використали його на практиці.