

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 IA-31 Самелюк А.С. Перевірив: Шимкович Л.Л. Tema: 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

ЕА Е2 В3 F2 ЕЕ F7 EA E0

11101010 11100010 10110011 11110010 11101110 11110111 11101010 11100000

Ключ шифрування

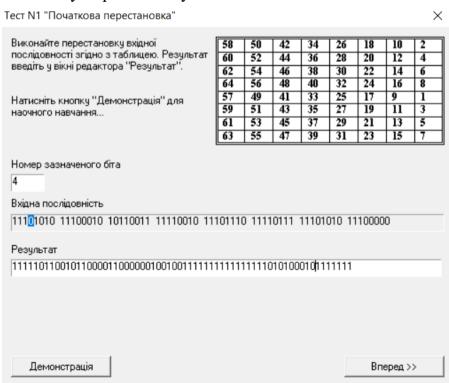
автобуси

Е0 Е2 F2 ЕЕ Е1 F3 F1 E8

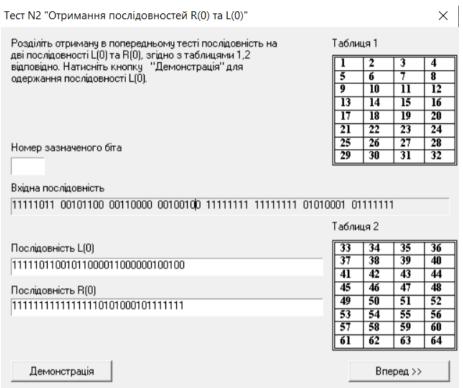
11100000 11100010 11110010 11101110 11110001 11110011 11110000

### 2. Початкова перестановка:

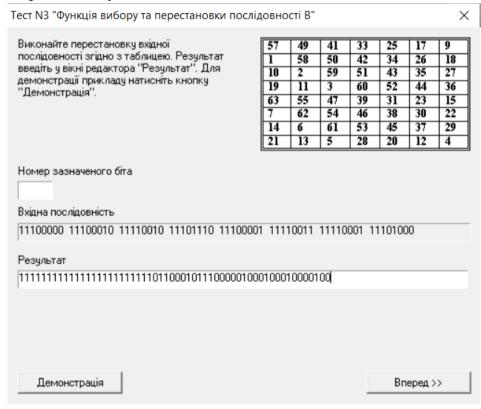
Використовуючи таблицю та послідовність, отриману з вхідного слова, отримуємо початкову перестановку.



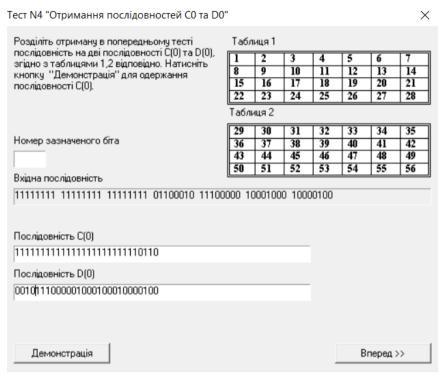
Отримання послідовностей R(0) та L(0):
 Ділимо вхідну послідовність на дві(R(0) - перша половина, L(0) - друга половина)



4. Функція вибору та перестановки послідовності В: Використовуючи таблицю та послідовність, отриману з ключа шифрування, отримуємо перестановку послідовності В.



Отримання послідовностей C(0) та D(0):
 Ділимо вхідну послідовність на дві(C(0) - перша половина, D(0) - друга половина)

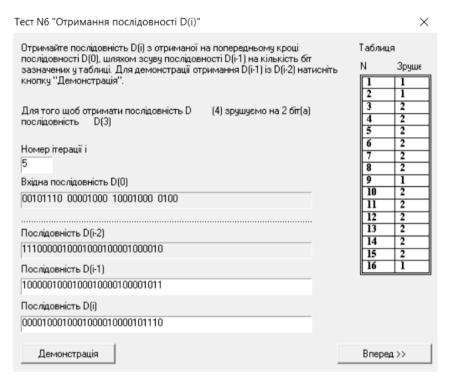


### 6. Отримання послідовності С(і):

Тест N5 "Отримання послідовності C(i)"	×
Отримайте послідовність С(і) з отриманої на попередньому кроці послідовності С(0), шляхом зсуву послідовності С(і-1) на кількість біт	Таблиця
зазначених у таблиці. Для демонстрації отримання C(i-1) із C(i-2) натисніть кнопку "Демонстрація".	N Зрушє 1 1
Для того щоб отримати послідовність С(13) зрушуємо на 2 біт(a)	2 1 3 2
послідовність С(12)	4 2 5 2
Номер ітерації і	6 2 7 2 8 2
Вхідна послідовність С(0)	9 1 1 10 2
11111111 11111111 11111111 0110	11 2 12 2
Послідовність С(i-2)	13 2 14 2
Послідовність С(i-1)	15 2 16 1
101101111111111111111111111111111111111	
Послідовність C(i) 1101111111111111111111111111111111111	
Демонстрація	Вперед>>

### 7. Отримання послідовності D(i):

Всього  $\epsilon$  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.



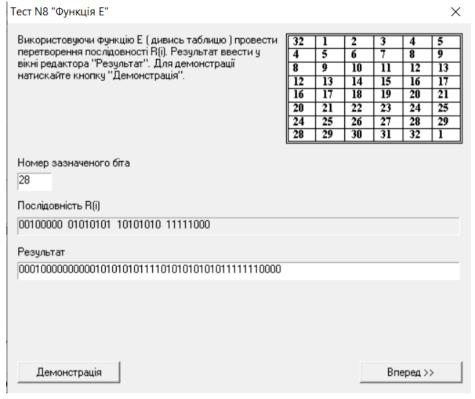
## 8. Отримання послідовностей К(і):

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 К(і) зробіть конкетанацію послідовностей С(і) та D(і). В отриманій послідовності С(і)D(і) переставте біти згідно з таблицею. Для демонстрації натисніть кнопку "Демонстрація".	14 3 23 16 41 30 44 46	17 28 19 7 52 40 49	11 15 12 27 31 51 39 50	24 6 4 20 37 45 56 36	1 21 26 13 47 33 34 29	5 10 8 2 55 48 53 32
Номер зазначеного біта						
Послідовність С(і)						
10110111111111111111111111						
Послідовність D(i)						
0010000101110000010001000100						
Послідовність C(i)D(i)						
101101111111111111111111111110010000101111	010001	00				
Послідовність К(і)						
111110111111111111111110001000010000000						
Демонстрація			L	Bne	еред>	>

## 9. Функція Е:

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



### 10. Функція S(i):

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

Тест N9"Функції S(i)"											X				
Виконайте перестановку вхідної послідовності згідно з таблицею. Результат введіть у вікні редактора "Результат".															
7	13	14 11	3	6	6 15	9	10 3	1 4	7	8	5	11	12 10	14	15 9
13 10	ó	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	Ó	6	10	1	13	8	9	4	5	11	12	7	2	14
15	на пос		3	омер р	ядка	14	СЛО								
111	111														
Рез	ультат														
111	ol .														
													Впер	ед >>	

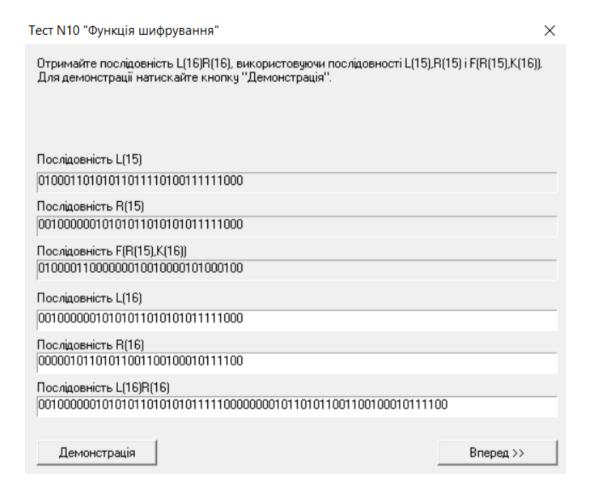
## 11. Функція шифрування.

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

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

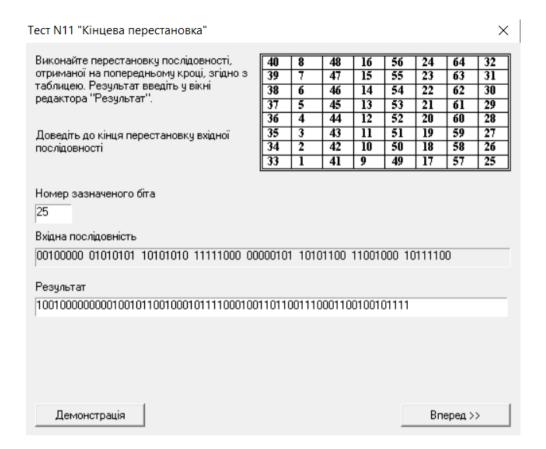
Для отримання L(i)R(i), з'єднуємо дві послідовності поступово.

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

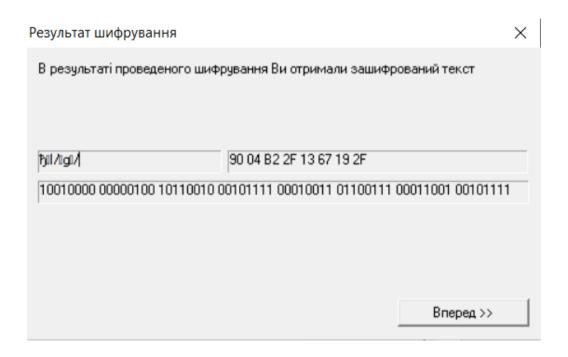


## 12. Кінцева перестановка:

Використовуючи таблицю та вхідну послідовність, отримуємо кінцеву перестановку.



## 13. Результат шифрування:



#### Результати тесту:

Результати тест	y >	<

Перегляньте результати тестування та оцініть свої знання !								
Назва тесту	Кількість не	евірних бітів	Помилковість, %					
Початкова перестано	овка	0	0					
Отримання L(0) та R(I	0)	0	0					
Послідовність В		0	0					
Отримання C(0) та D(	0)	0	0					
Отримання С(і)		0	0					
Отримання D(i)		0	0					
Отримання К(і)		0	0					
Отримання S(i)		0	0					
Послідовність Е		0	0					
Функція шифрування	l	0	0					
Кінцева перестановк	a	0	0					
			Вперед >>					