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.

Київ-2025

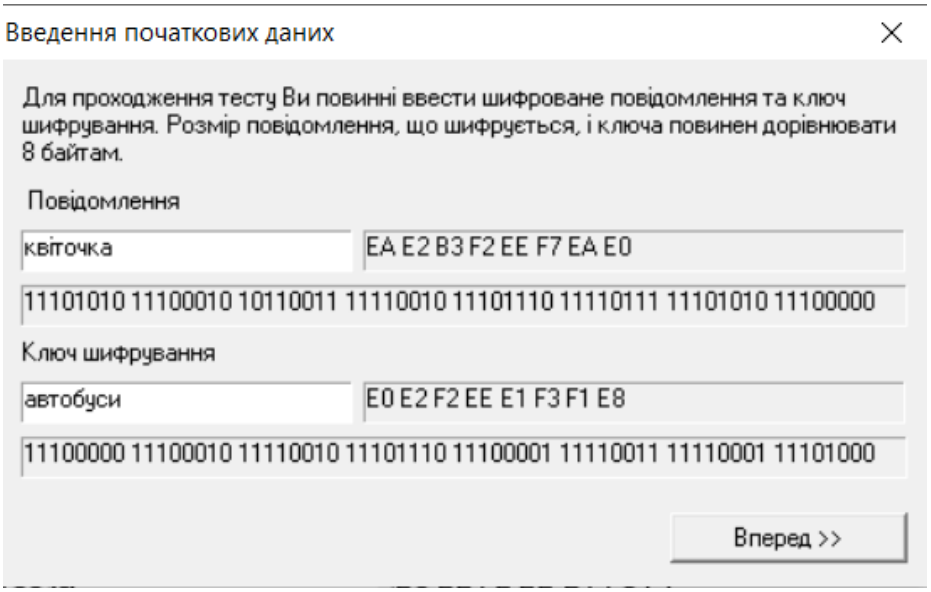
Тема: Шифр DES.

Хід роботи:

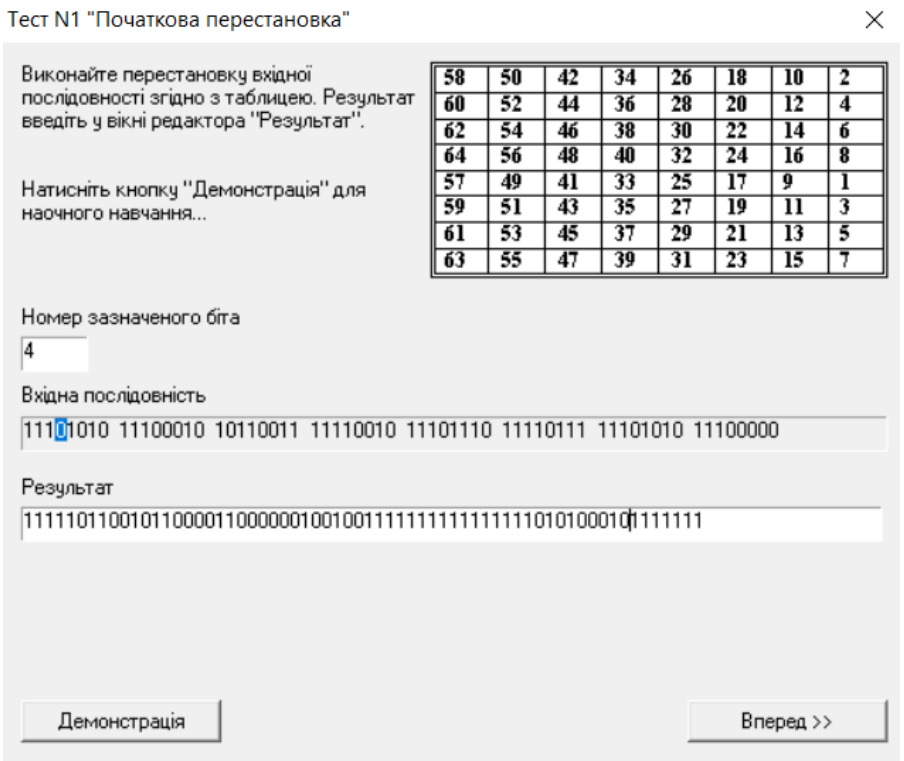
1. Задаємо слово та ключ:

   Слово: квіточка

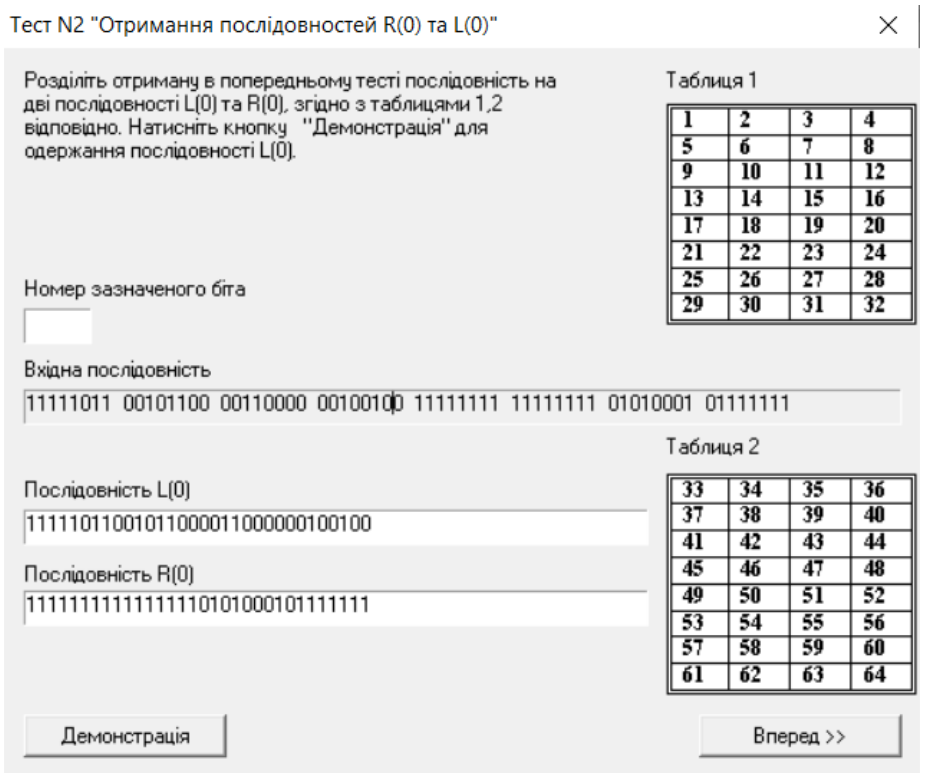
   Ключ: автобуси



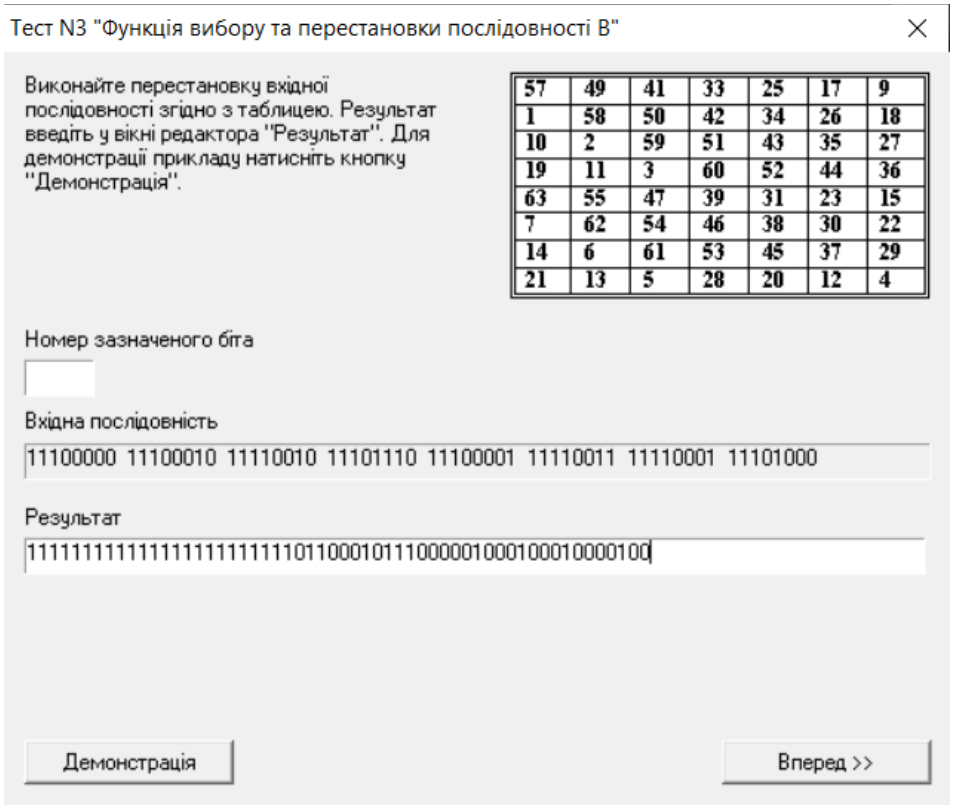
2. Початкова перестановка:
   Використовуючи таблицю та послідовність, отриману з вхідного слова, отримуємо початкову перестановку.



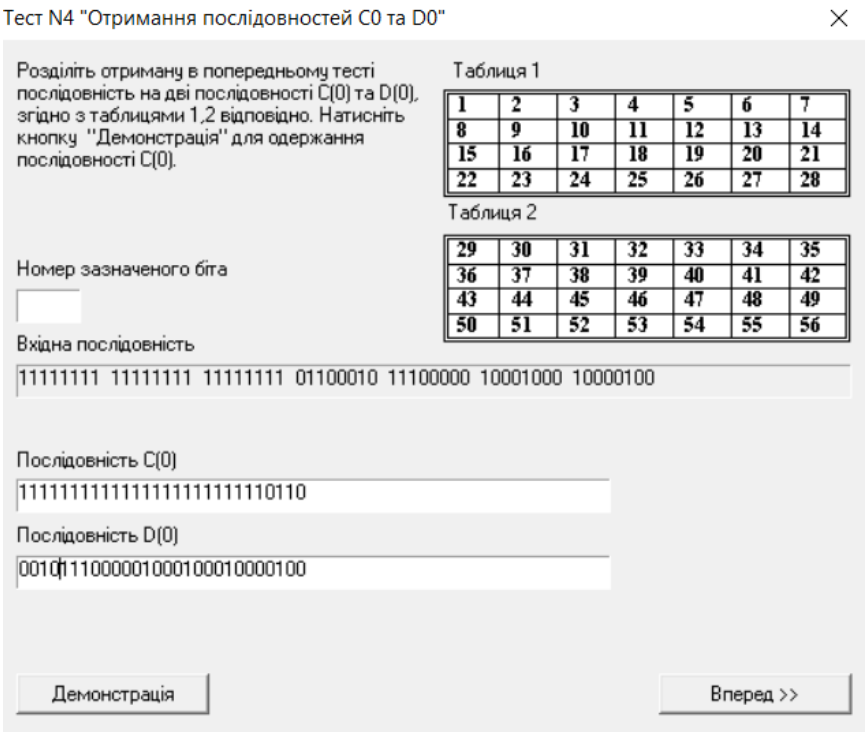
3. Отримання послідовностей R(0) та L(0):
   Ділимо вхідну послідовність на дві(R(0) - перша половина, L(0) - друга половина)



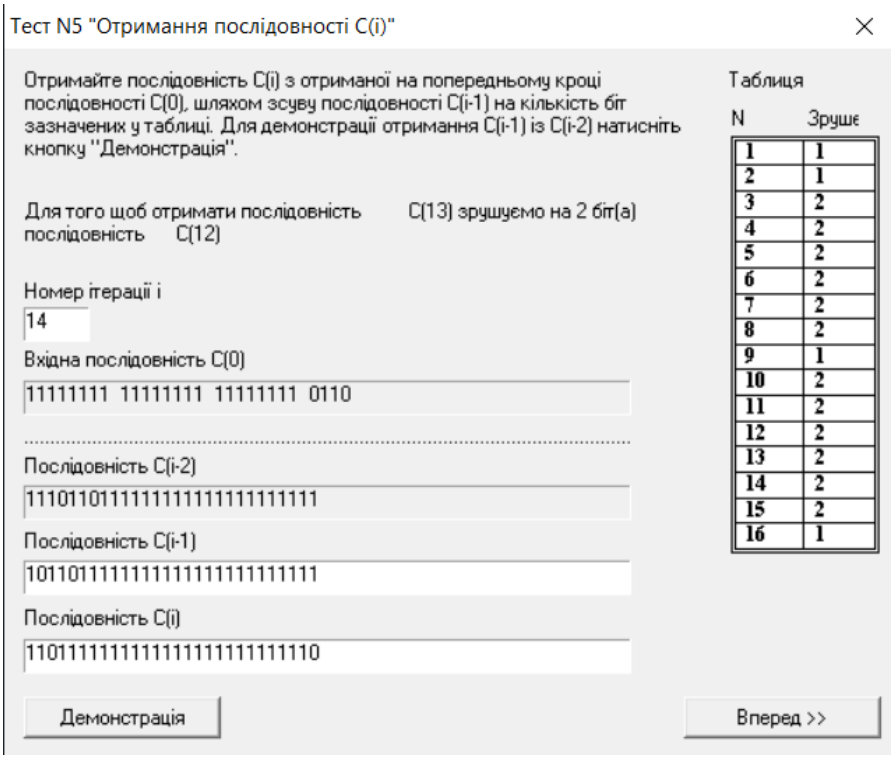
4. Функція вибору та перестановки послідовності B:
   Використовуючи таблицю та послідовність, отриману з ключа шифрування, отримуємо перестановку послідовності B.



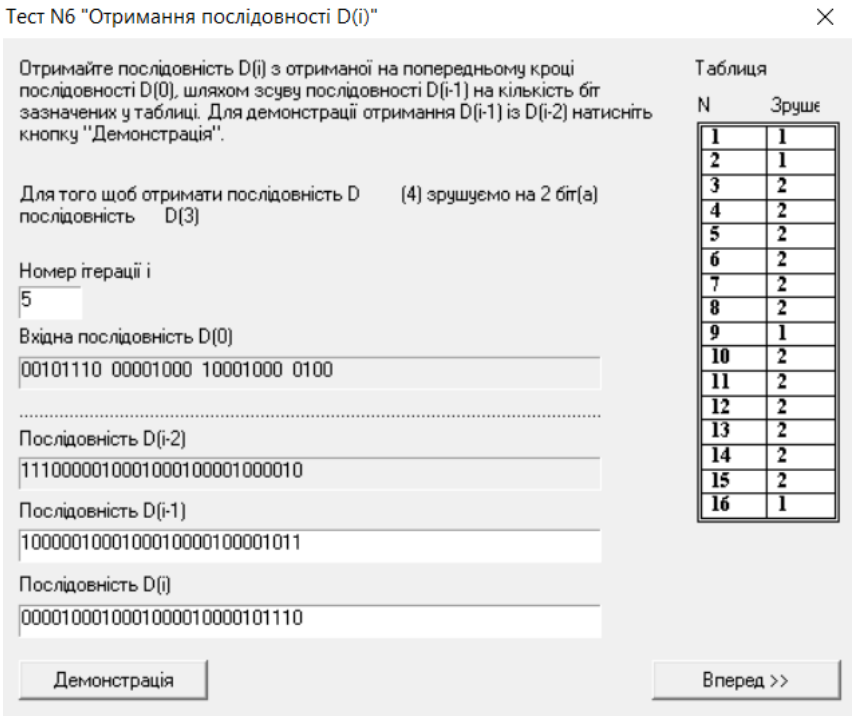
5. Отримання послідовностей C(0) та D(0):
   Ділимо вхідну послідовність на дві(C(0) - перша половина, D(0) - друга половина)



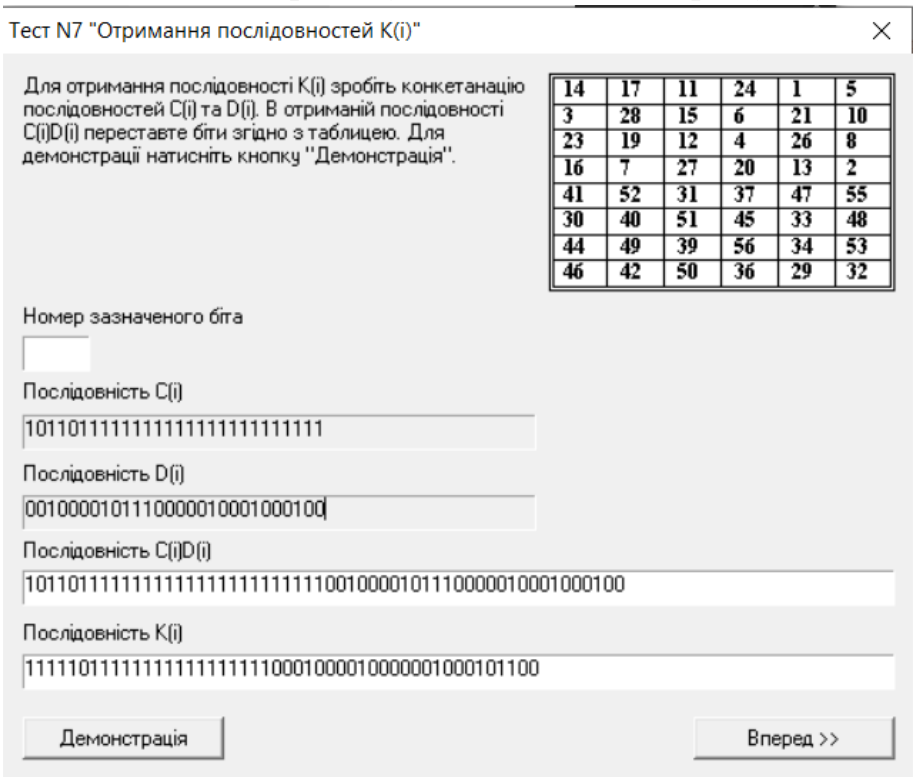
6. Отримання послідовності C(i):
   Всього є 16 ітерацій. Номер ітерації: i = 14. Додаємо всі зрушення з таблиці до даної ітерації (1+1+2+2+2+2+2+2+1+2+2+2+2+2 = 24). Щоб отримати C(i) = C(14) робимо зсув вліво на 24 біти. Щоб отримати C(i-1) = C(13), робимо зсув на (1+1+2+2+2+2+2+2+1+2+2+2+2 = 22) 22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



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.

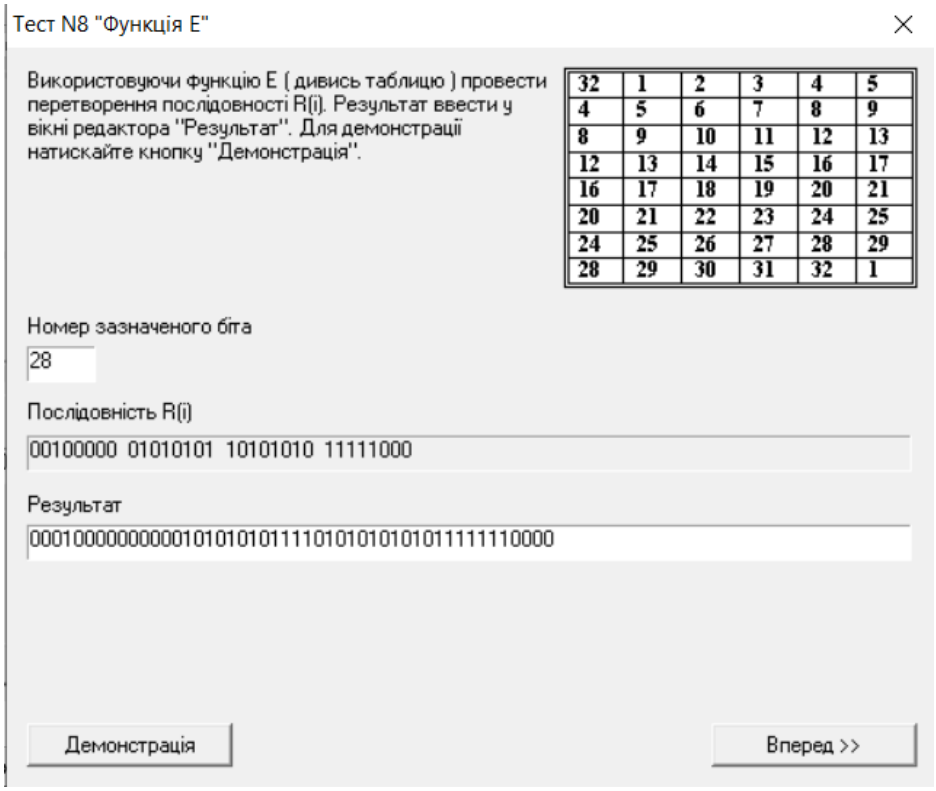


8. Отримання послідовностей K(i):
   Для отримання C(i)D(i), з'єднуємо дві послідовності поступово. Потім використовуючи таблицю та отриману послідовність, отримуємо K(i).



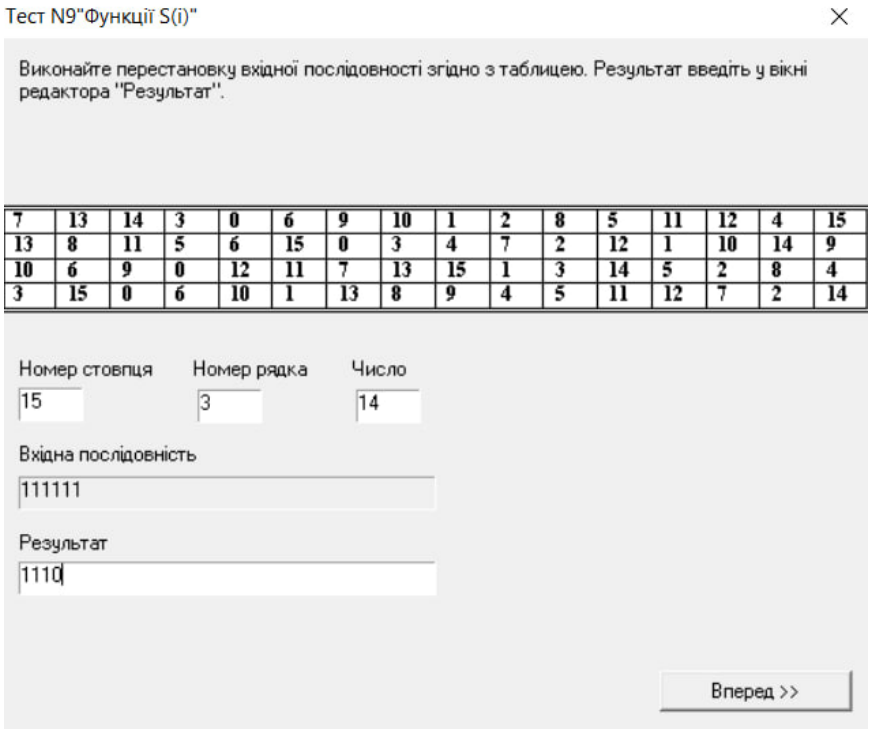
9. Функція E:

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



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.



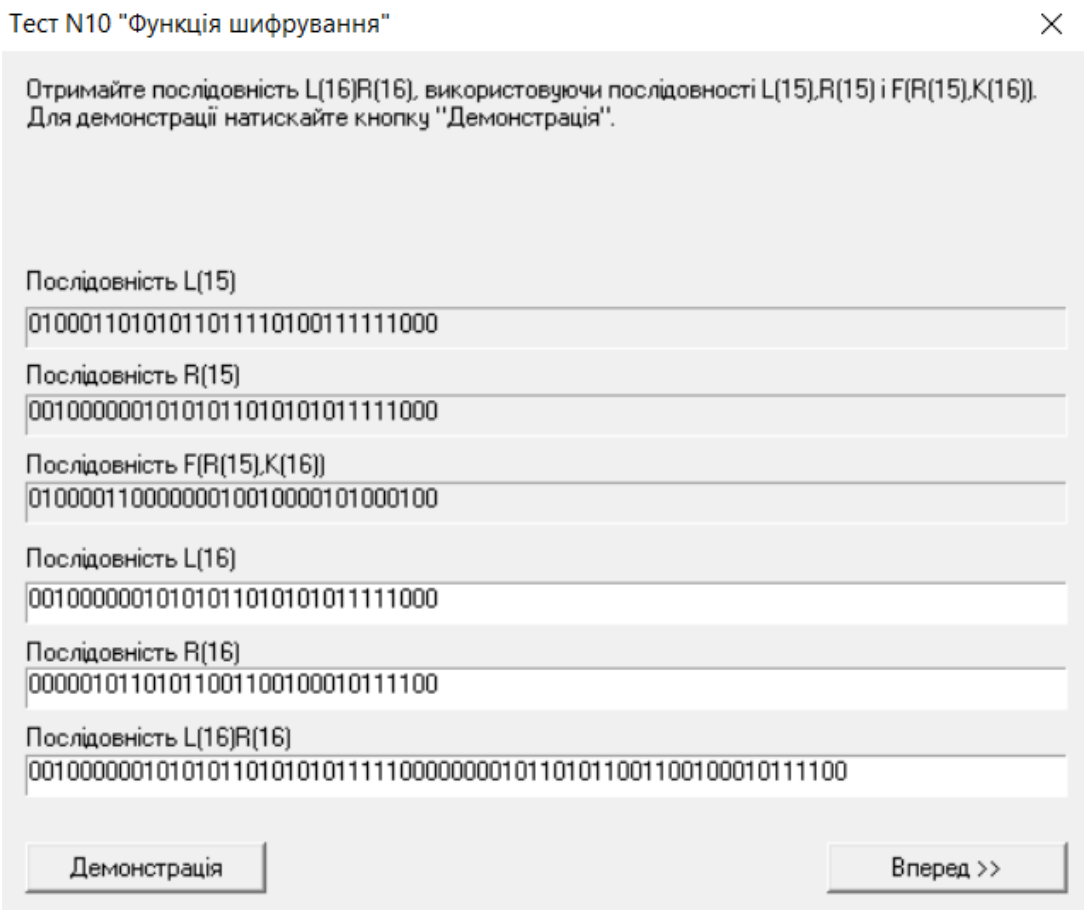
11.Функція шифрування.

L(i) = R(i-1) => L(16) = R(15)

R(i) = L(i-1) xor F(R(i-1),K(i-1)) => R(16) = L(15) xor F(R(15),K(15))

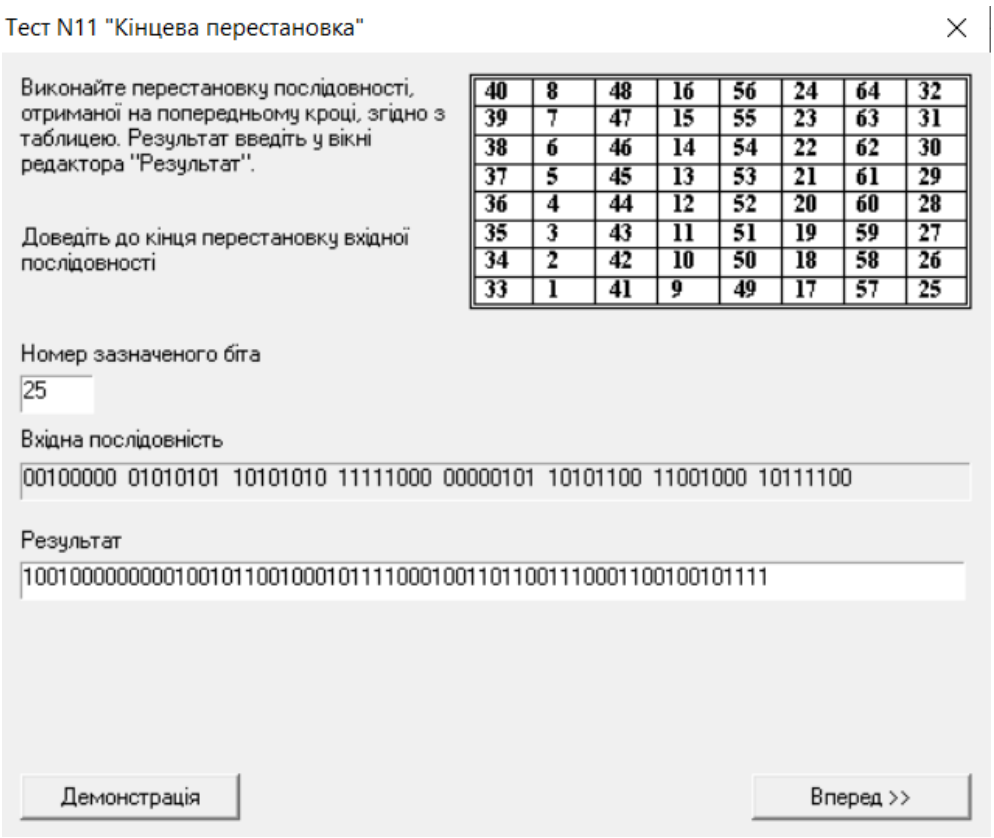
Для отримання L(i)R(i), з’єднуємо дві послідовності поступово.

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

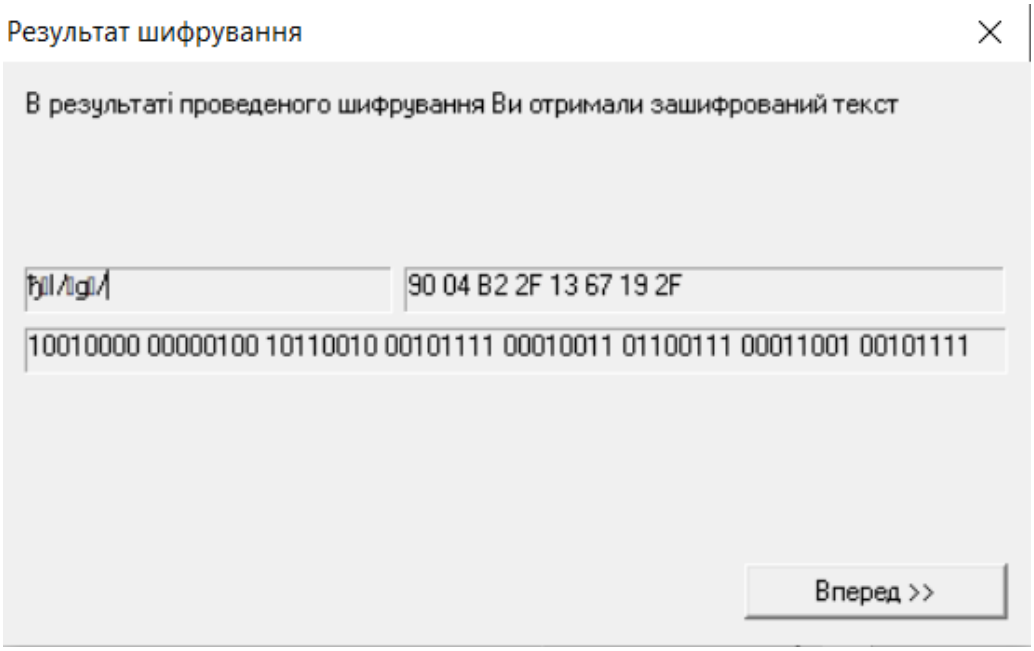


12. Кінцева перестановка:

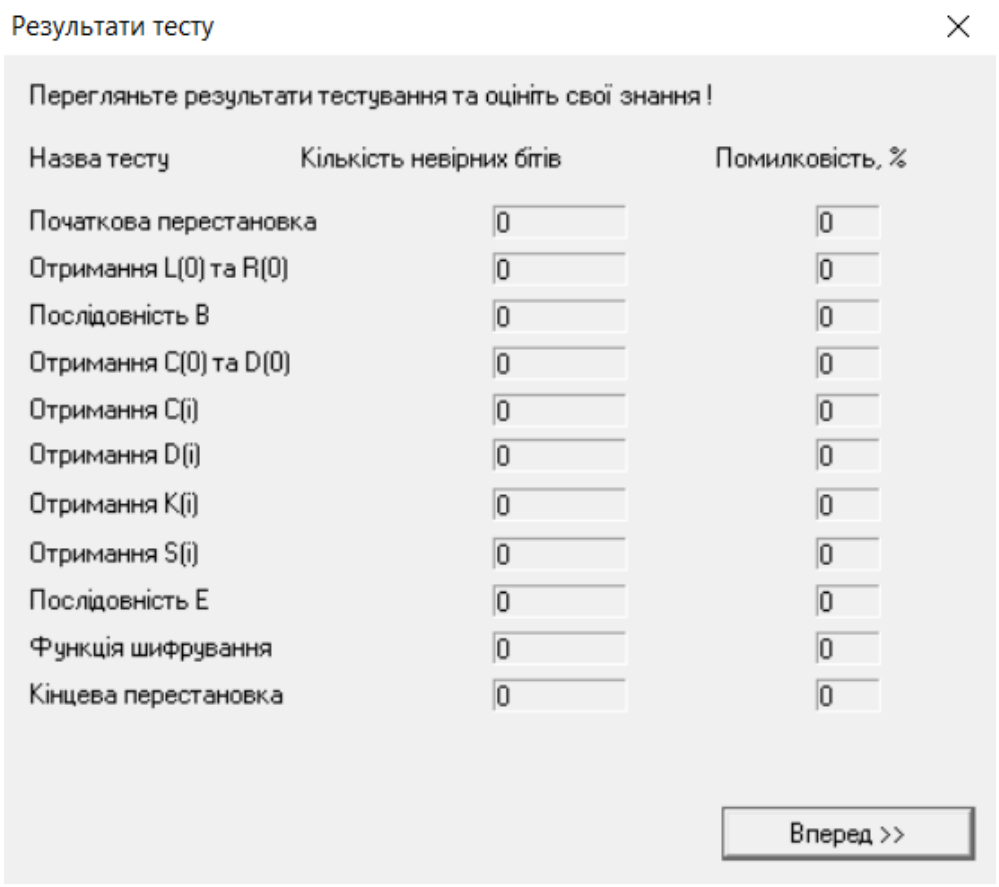
Використовуючи таблицю та вхідну послідовність, отримуємо кінцеву перестановку.



13.Результат шифрування:



Результати тесту:


Результати тесту
Перегляньте результати тестування та оцініть свої знання !
Назва тесту
Кількість невірних бітів
Помилковість, %
Початкова перестановка
Отримання L(0) та R(0)
Послідовність B
Отримання C(0) та D(0)
Отримання C(i)
Отримання D(i)
Отримання K(i)
Отримання S(i)
Послідовність E
Функція шифрування
Кінцева перестановка
0
Вперед >>