**ЛАБОРАТОРНА РОБОТА №3**

**МОДЕЛЮВАННЯ ПРОЦЕСІВ ШИФРУВАННЯ ЗА ДОПОМОГОЮ ОПЕРАЦІЇ XOR. АЛГОРИТМ DES**

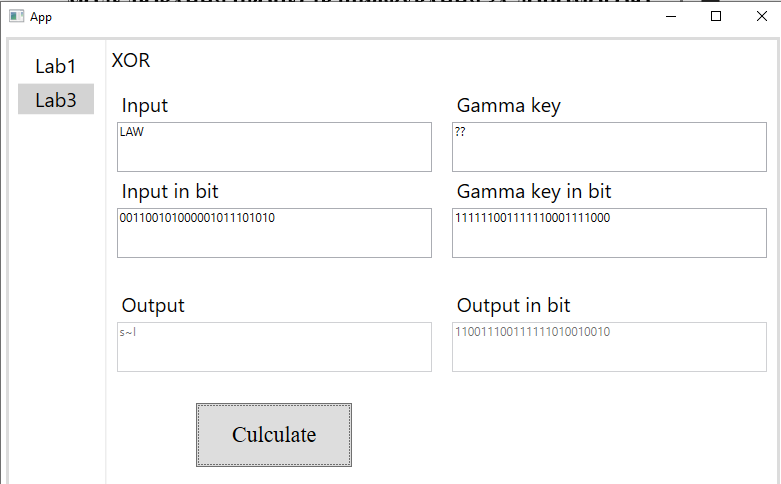
**Мета:** набути вміння шифрування повідомлень із використанням операції побітового додавання за модулем 2, дослідити процеси шифрування за допомогою алгоритму DES на основі навчальної програми CrypТool 2.

**Хід роботи:**

Завдання №1: Реалізувати в середовищі MS Excel або на будь-якій мові програмування перетворення текстового повідомлення у двійкову послідовність, що додається 10 за модулем 2 (XOR) із ключовою гамою. Перевірити роботу програми для вхідних даних згідно варіанту (англійській алфавіт). Кроки алгоритму шифрування зі скріншотами описати у звіті.

Табл. 1

|  |  |  |
| --- | --- | --- |
| Варіант № | Відкритий текст | Ключова гама |
| 2 | LAW | 111111001111110001111000 |



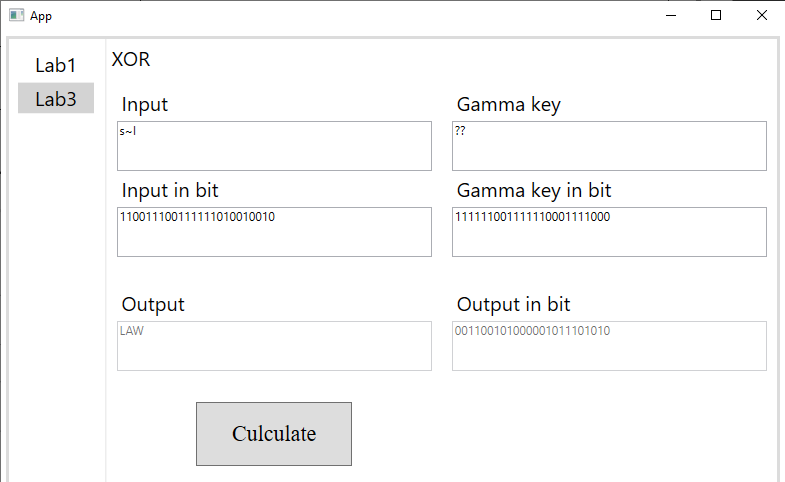


Рис. 1. Результат роботи програми

LAW2 = 001100101000001011101010

KEY = 111111001111110001111000

Res = 110011100111111010010010

Result to chars = s~I

Бачимо, що результати програми співпали.

Перетворюємо кожну букву відкритого тексту у двійкову послідовність. І потім виконуємо додавання бітів за модулем 2 (XOR). Після цього перетворюємо отримано послідовність у літери.

Завдання №2: Виконати зашифрування блоку повідомлення за допомогою алгоритму DES на основі навчальної програми CrypТool 2 (Templates⇒Cryptography⇒Modern⇒Symmetric⇒DES Visualization). Ключ **обрати самостійно** (64 бітова послідовність символів), не використовувати ключ за замовчуванням. У звіті описати зі скріншотами нижчезазначені кроки алгоритму.

Табл. 2

|  |  |
| --- | --- |
| Варіант № | Відкритий текст |
| 2 | TOMORROW |

Спочатку перетворимо відкритий текст і ключ (TOMORROW) у шістнадцяткову систему числення.

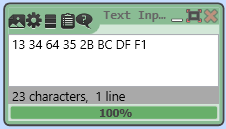


Рис. 2. Ключ (64 біти) у 16-ій системі числення

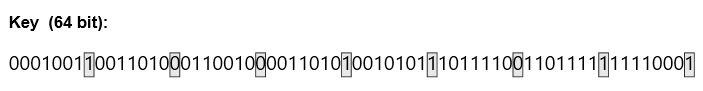


Рис. 3. Ключ (64 біти) у 2-ій системі числення

(з позначенням бітів контролю парності)

Ключ шифрування складається з 56 випадкових бітів; додається ще 8 біт в позиціях 8, 16,…, 64, таким чином, щоб кожен байт містив непарну кількість одиниць. (використовується при знаходженні помилок при обміні та зберіганні ключів).

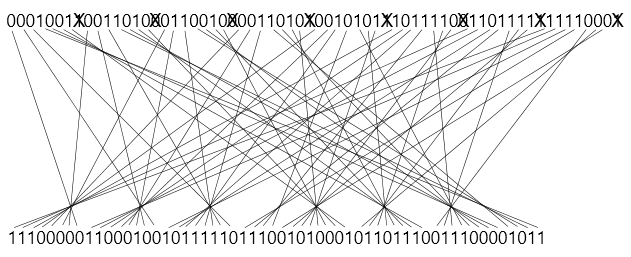


Рис. 4. Ключ (56 біт) у 2-ій системі числення і

перестановка початкового 56-бітного ключа

Перестановка здійснюється за допомогою матриці початкової перестановки Initial Permutation.

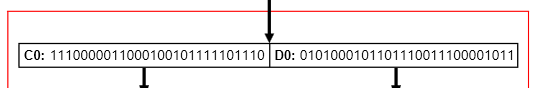
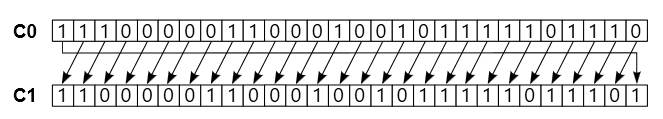


Рис. 5. Поділ ключа на дві частини C0 та D0



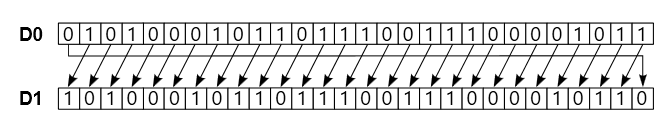


Рис. 6. Зсув C0 та D0

Довжина зсуву визначається матрицею зсуву для обчислення ключів.

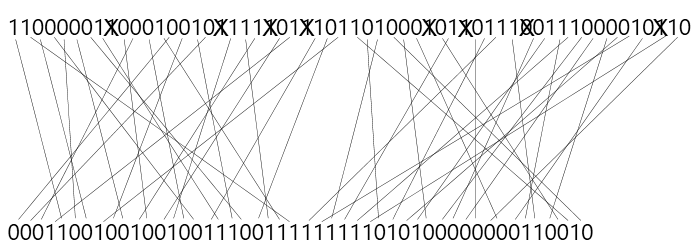


Рис. 7. Перестановка зі стисненням

Для перестановки вибирається 48 бітів з 56 бітів та міняється їх порядок за допомогою матриці перестановки зі стисненням.

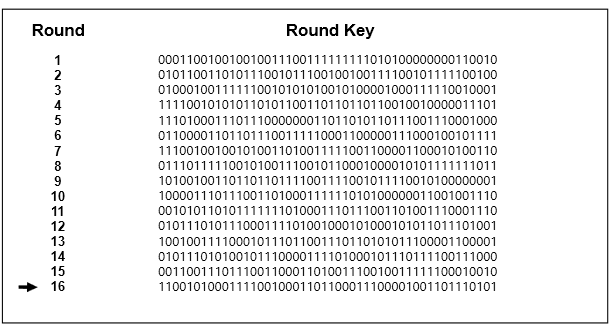


Рис. 8. Таблиця усіх раундових ключів

TOMORROW

Рис. 9. Початковий блок повідомлення у вигляді тексту

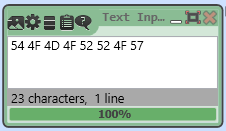


Рис. 10. Початковий блок повідомлення (64 біти) у 16-ій системі числення

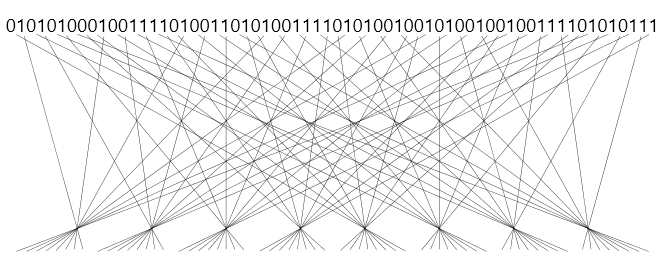


Рис.11. Початковий блок повідомлення (64 біти) у 2-ій системі числення і початкова перестановка



Рис. 12. Поділ блоку на дві половини L0 та R0 (1 раунд)

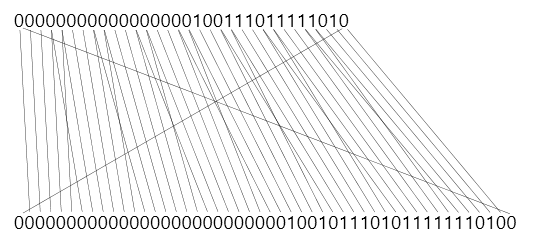


Рис. 13. Перестановка з розширенням R0

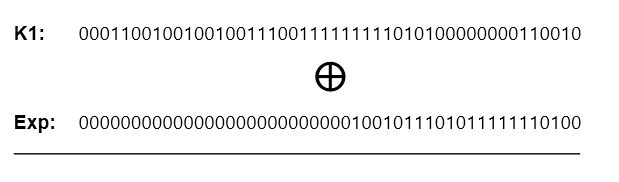


Рис. 14. Додавання R0 з раундовим ключем K1

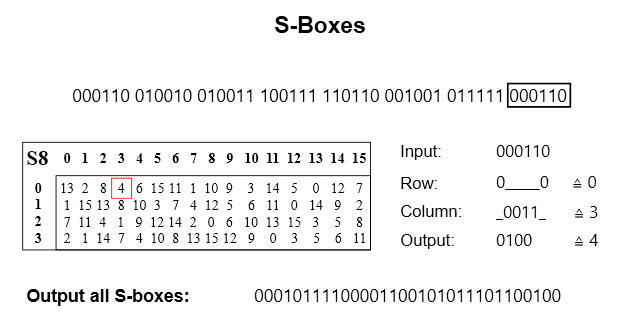


Рис. 15. Перетворення з використанням S-боксів (з поясненням)

Обираємо перший 6-бітний блок. Далі записуємо окремо перший і останній розряди блоку та середні чотири розряди. Після чого шукаємо число на перетині отриманих двох чисел, представлених у десятковій системі числення. Після знаходження числа подаємо його у двійковому представленні. Аналогічні дії виконуємо над всіма іншими 6-бітними блоками.

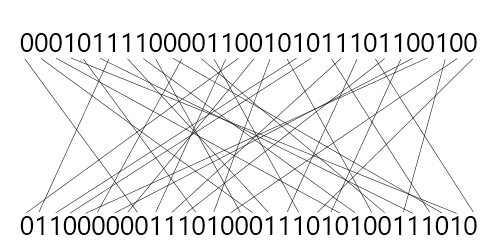


Рис. 16. Перестановка P

Отриманий блок в попередній дії перетворюється за допомогою матриці перестановки P.

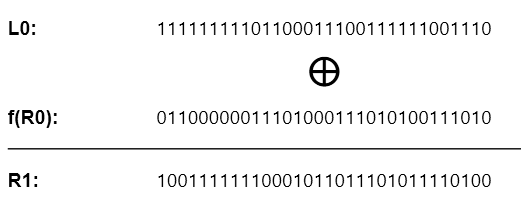


Рис. 17. Додавання L0 та f (R0, K1)

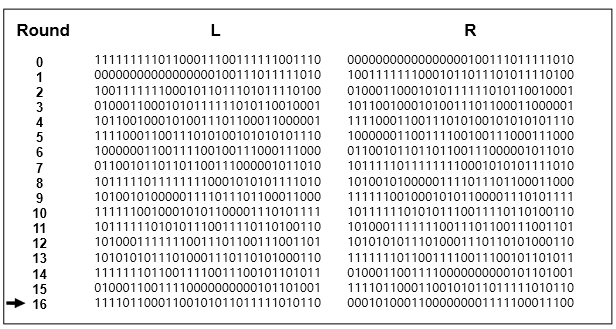


Рис. 18. Таблиця лівих та правих половин кожного раунду

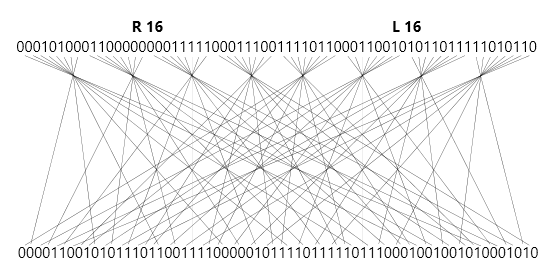


Рис. 19. Кінцева перестановка

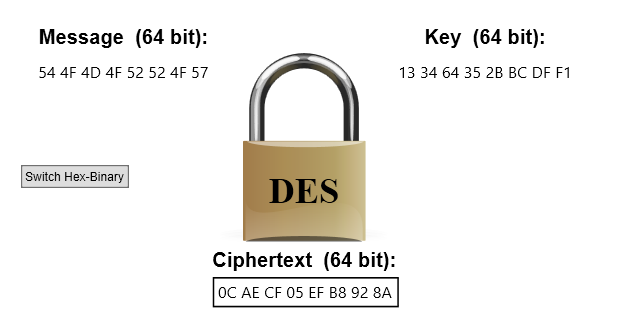


Рис. 20. Результат шифрування блоку

**Висновок:** ми набули вміння шифрування повідомлень із використанням операції побітового додавання за модулем 2, дослідили процеси шифрування за допомогою алгоритму DES на основі навчальної програми CrypТool 2.