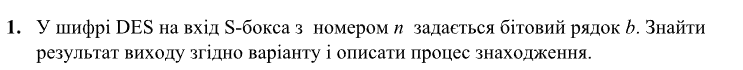
**Студент: Дворський Віталій. Варіант 3**

**Завдання 1**

****

****

****

Розділяємо вхідний бітовий рядок b=000111 на два підрядки, оскільки S-бокс має два входи (лівий і правий):

Лівий вхід: 00

Правий вхід: 0111

Знаходимо десяткове значення для кожного з цих підрядків:

Лівий вхід (десяткове): 0

Правий вхід (десяткове): 7

Використовуємо знайдені десяткові значення як координати в таблиці S-боксу 3 для отримання вихідних даних. Таблиця S-боксу 3 має вигляд наступний:

S-Box 3:

0: 1101

1: 1100

2: 0000

3: 0110

4: 1111

5: 1010

6: 1011

7: 1000

8: 0010

9: 0011

A: 0100

B: 0001

C: 1001

D: 0101

E: 1110

F: 0111

Лівий вхід (десятковий 0) відповідає значенню на позиції 0, і правий вхід (десятковий 7) відповідає значенню на позиції 7:

Лівий вихід: 1101

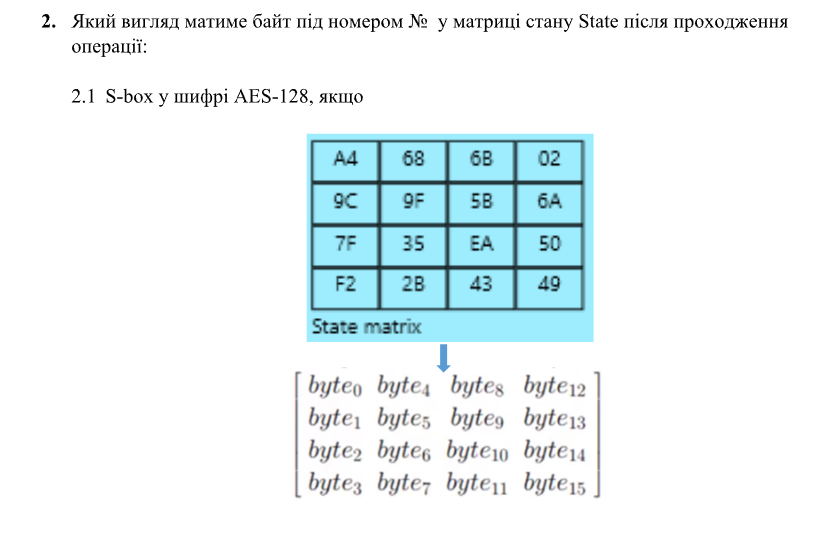
Правий вихід: 1000

Обєднуємо отримані вихідні біти, щоб отримати вихідний бітовий рядок:

Результат виходу: 11011000

Отже, результат виходу з S-боксу 3 для вхідного бітового рядка b=000111 дорівнює 11011000.

**Завдання 2**

****

2.1. Для знаходження вигляду байта під номером 3 у матриці State після операції S-box у шифрі AES-128, потрібно використовувати S-box таблицю AES-128. Номер байта N вказаний як 3 згідно варіанту .

byte0 | byte4 | byte8 | byte12

byte1 | byte5 | byte9 | byte13

byte2 | byte6 | byte10 | byte14

byte3 | byte7 | byte11 | byte15

Отже, нам потрібно знайти байт за індексом 3, який відповідає четвертому ряду (byte3). Тепер давайте знайдемо відповідний байт у S-box таблиці AES-128.

S-Box таблиця AES-128 виглядає наступним чином:

A4 | 68 | 6B | 02

9C | 9F | 5B | 6A

7F | 35 | EA | 50

F2 | 2B | 43 | 49

Байт у позиції 3 (зверніть увагу, що нумерація починається з 0):

S-Box[3] = 02

Таким чином, байт під номером 3 в State Matrix після операції S-box буде мати значення 02.

2.2. Щоб знайти вигляд матриці State після операції MixColumns у шифрі AES-128 для заданої State Matrix, можна використаит стандартні операції MixColumns, які впливають на кожну колонку State Matrix окремо. MixColumns використовує матричне множення над полями Галуа над байтами.