Міністерство освіти і науки України

КПІ ім. Ігоря Сікорського

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій (ІСТ)

Звіт до комп’ютерного практикуму №2

З дисципліни

«Алгоритми та математичні методи захисту інформації»

Підготував:

Студент групи ІК-02

Талько Ярослав

Перевірив:

Нестерук А.

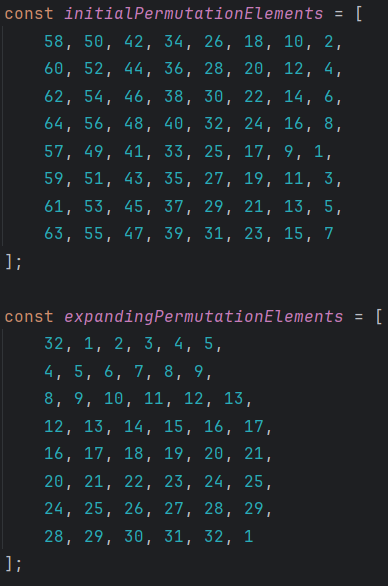
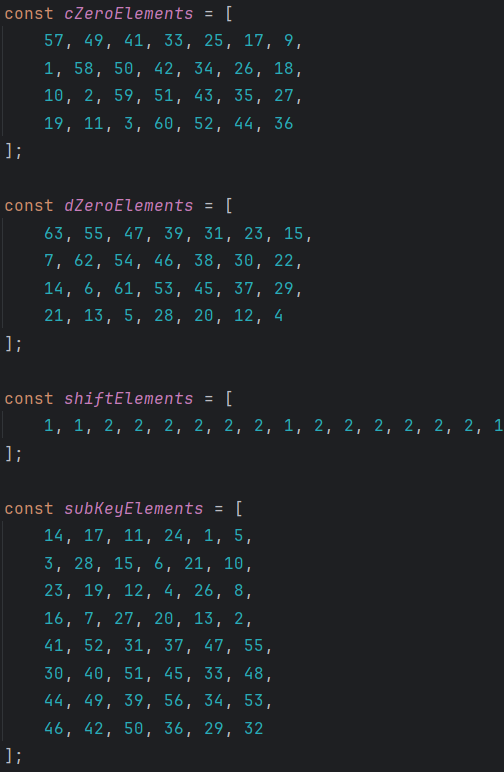
Київ 2024

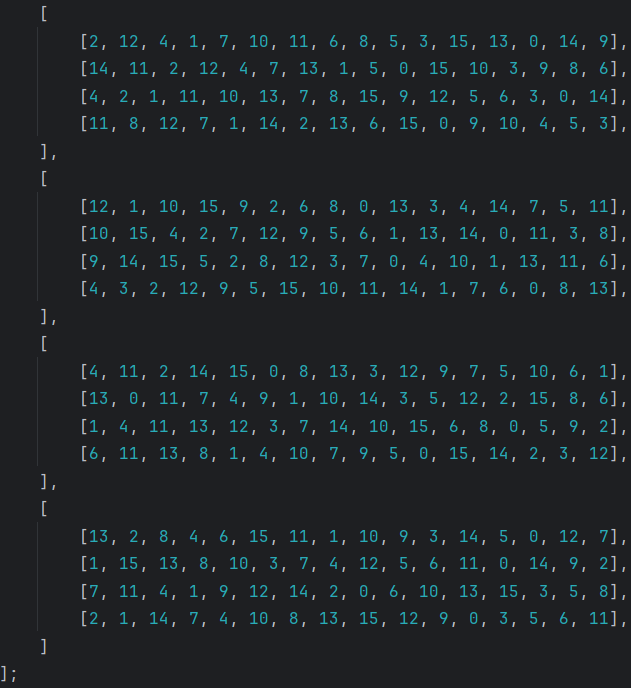
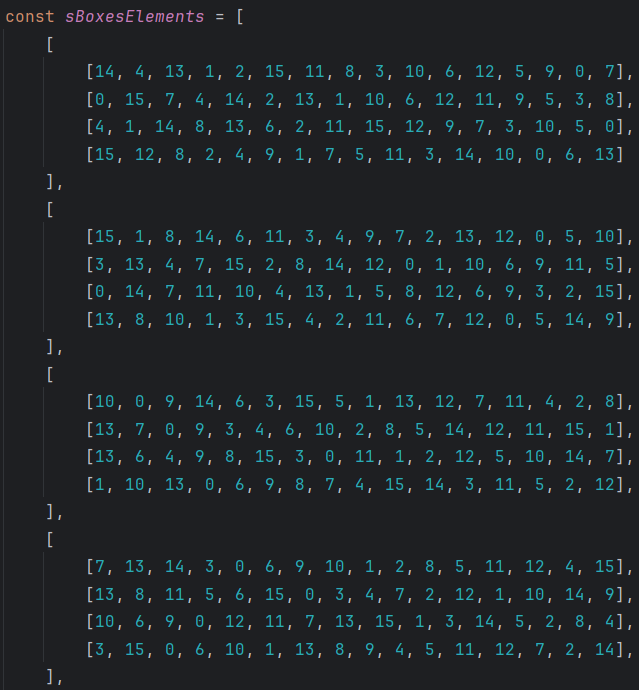
**Тема:** Симетричні блочні шифрування DES та ГОСТ 28147-89.

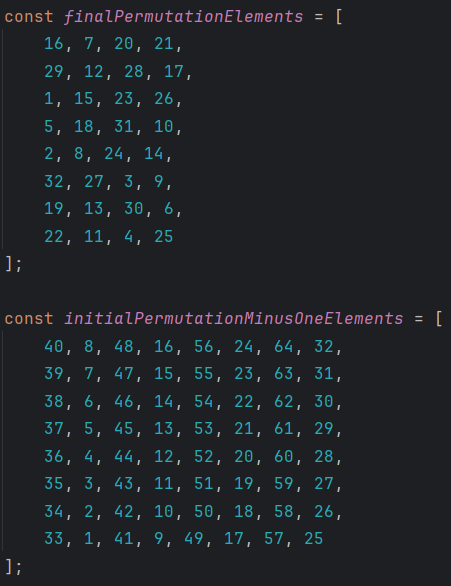
**Мета:** Навчитися шифрувати та розшифровувати інформацію за допомогою симетричних блочних шифрів DES та ГОСТ 28147-89.

**Хід роботи**

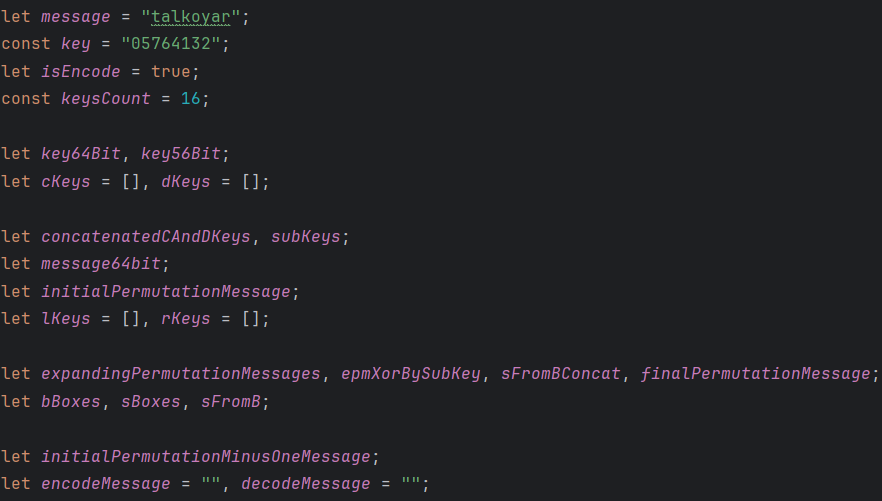
Так, як я маю 41 номер в списку, тоді я повинен виконувати перше завдання. Перейдемо до коду, написаного мовою JS:



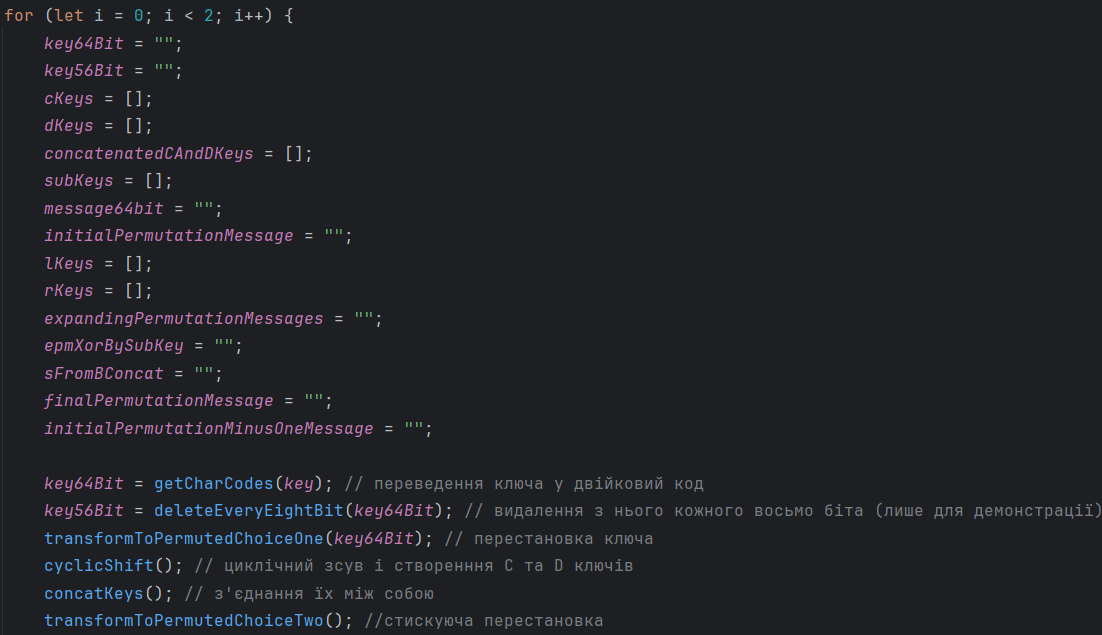




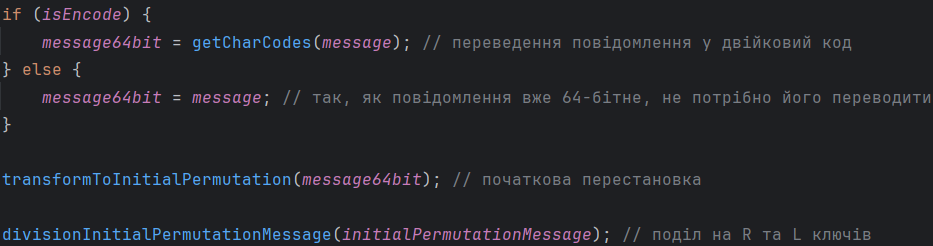
Дані блоки коду призначені для правильного розташування бітів по позиціям. sBoxes призначений для зберігання чисел, які потім будуть шукатися в ньому за рядком та стовпчиком.



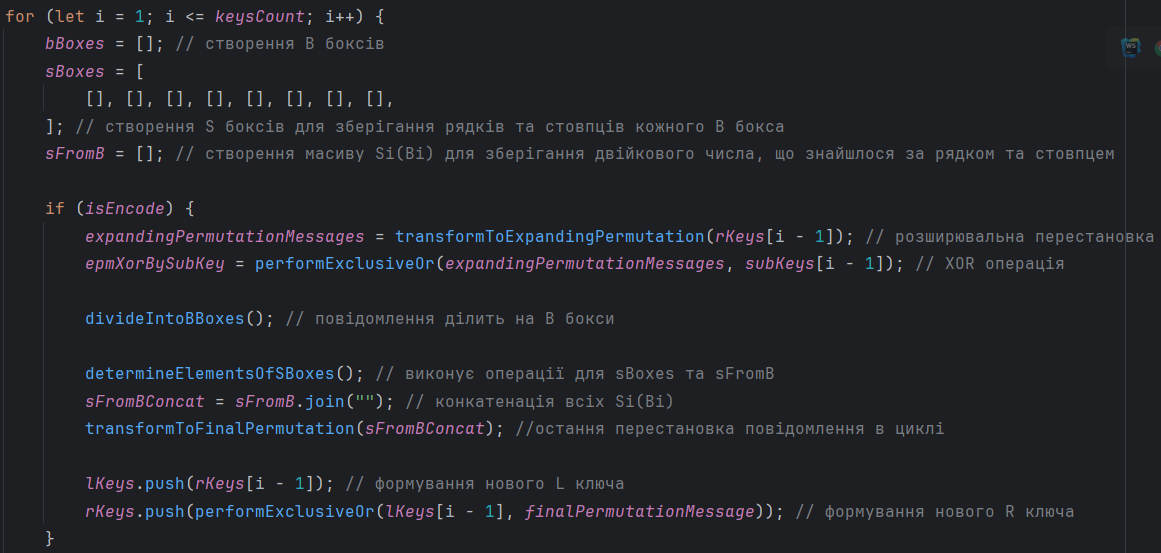
Всі ці змінні призначені для зберігання даних, які ми будемо отримувати внаслідок роботи програми.

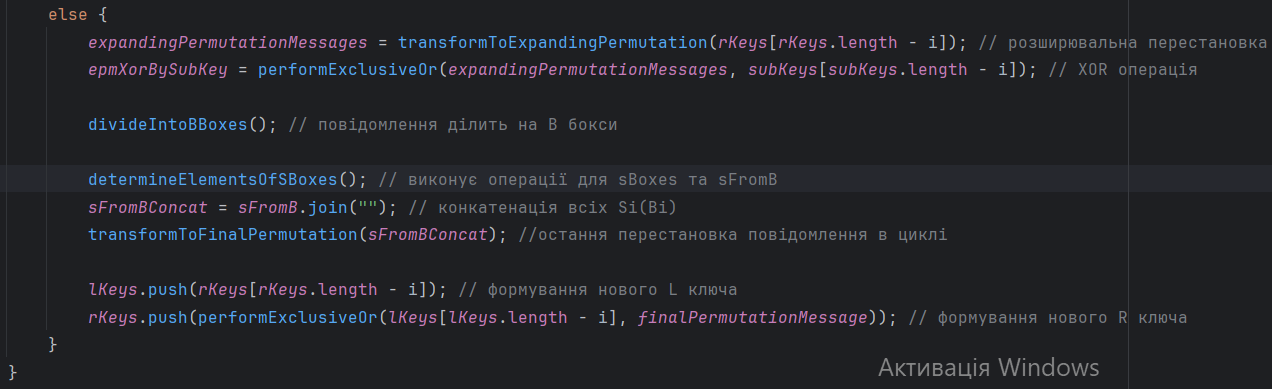


Далі ми розпочинаємо цикл, що складається з двох ітерацій, перша з яких відповідає за шифрування, а друга за розшифрування. Подальші дій в коді описуються в коментарях до нього, тому дублювати їх немає сенсу. Важливо зазначити, що в кожній ітерації значення обнуляються, адже програма використовує при шифруванні та розшифруванні майже одні й ті ж значення та функції.

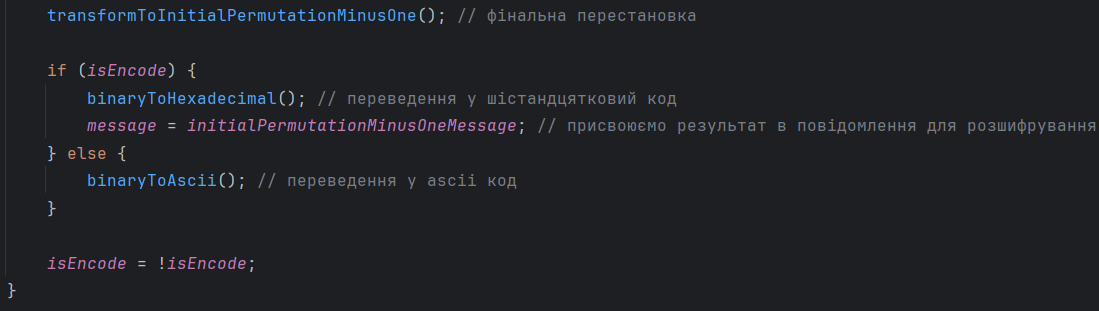


isEncode тут якраз і позначає місця, де повинні використовуватися різні підходи під час процесів шифрування та розшифрування.





В цьому випадку для шифрування ключі використовуються в своєму звичайному порядку, тоді як для розшифрування в оберненому.



Тут відбувається завершення циклу, і тому ми при шифруванні ми перероблюємо результат у 16-ий код для відображення і присвоюємо повідомленню результат останньої перестановки, аби в наступному циклі вже могло почати його розшифровувати. У випадку із розшифруванням переводимо результат останньої перестановки в текст.

Нижче описані всі функції, які я написав для роботи програми. До них я коментарів я не писав, адже в основному коді основна їхня робота була описана.





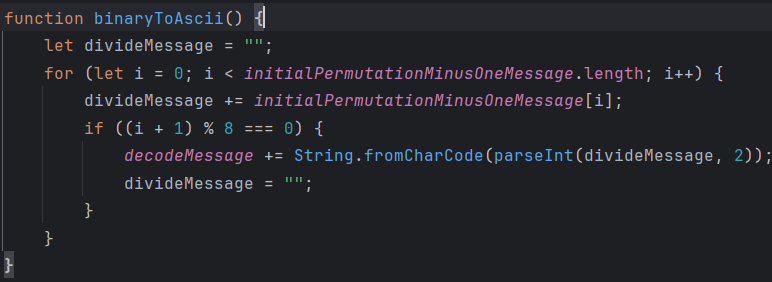












Також нижче наведений код програми:

Результат роботи програми:



**Висновок:** На цій лабораторій роботі я навчився шифрувати та розшифровувати інформацію за допомогою симетричних блочних шифрів DES та ГОСТ 28147-89.