МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КРЕМЕНЧУЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ МИХАЙЛА ОСТРОГРАДСЬКОГО

КАФЕДРА АВТОМАТИЗАЦІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ЗВІТ

ЗВІТ З ЛАБОРАТОРНИХ РОБІТ

З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**«ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»**

Виконав студент групи КН-23-1

Полинько Ігор Миколайович

Перевірив: викладач Рилова Н. В.

Кременчук 2025

**ЛАБОРАТОРНА РОБОТА № 1**

**Тема:** Шифрування методами перестановки

**Мета:** навчитися розроблювати програми для шифрування методами

перестановок.

**Порядок виконання роботи:**

Для непарних варіантів (1, 3, ..., 13) пропонується реалізувати процедуру шифрування, для парних (2, 4, ..., 14) – дешифрування з використанням зазначених методів. Потрібно передбачити вибір ключа шифрування.

Написати програму шифрування (дешифрування).

1, 2. Вхідну послідовність поділіть на групи по чотири символи, потім у кожній групі символи потрібно переставити з використанням підстановки, яку виберіть самостійно.

**Варіант: 15**

**Скрипт програми:**

# функція шифрування  
def encrypt(text, key):  
 # Довжина блоку (4 символи)  
 block\_size = len(key)  
 # Доповнення пробілами, якщо не ділиться  
 while len(text) % block\_size != 0:  
 text += " "  
 result = ""  
 # Обробка блоками  
 for i in range(0, len(text), block\_size):  
 block = text[i:i+block\_size]  
 new\_block = [""] \* block\_size  
 for j, pos in enumerate(key):  
 new\_block[j] = block[pos-1]  
 result += "".join(new\_block)  
 return result  
  
  
text = input("Введіть текст для шифрування: ")  
key\_input = input("Введіть ключ довжиною в 4 символи (наприклад: 3 1 4 2): ")  
  
# перетворюємо рядок ключа у список  
key = list(map(int, key\_input.split()))  
  
# перевірка, щоб ключ не був довший за 4  
if len(key) > 4:  
 print("Помилка: довжина ключа не може бути більше 4!")  
else:  
 encrypted = encrypt(text, key)  
 print("Вхідний текст: ", text)  
 print("Зашифрований: ", encrypted)

**Результат:**

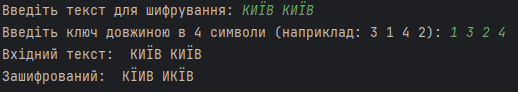
****

Рисунок 1.1 – Результат шифрування програми

**Висновок:** на цій лабораторній роботі ми навчилися розроблювати програми для шифрування методами перестановок.

**Контрольні питання:**

1. **У чому полягає метод шифрування перестановкою?**

Метод шифрування перестановкою полягає у зміні порядку символів відкритого тексту відповідно до певного ключа-перестановки. При цьому самі символи не змінюються, а секретність забезпечується саме за рахунок переставлення їх позицій.

1. **Що таке маршрутна перестановка?**

Маршрутна перестановка — це спосіб шифрування, при якому символи повідомлення записуються у таблицю визначеної форми (прямокутник, квадрат тощо), після чого символи зчитуються не за рядками, а за заданим «маршрутом» (наприклад, по стовпцях, по діагоналі, спіраллю).

1. **Який «маршрут» можна використовувати для реалізації шифру «Сцитала»?**

У шифрі «Сцитала» маршрут відповідає порядку зчитування символів з поверхні циліндра: текст записується по колу, уздовж циліндра — рядками, а для шифрування він зчитується по вертикалі (стовпцями). Таким чином формується нова послідовність символів.

1. **Оцініть кількість ключів шифру вертикальної перестановки. У скільки разів ця кількість ключів збільшується з використанням подвійної перестановки?**

Для вертикальної перестановки ключем є довжина рядка (кількість стовпців у таблиці). Якщо в таблиці m стовпців, то кількість можливих ключів дорівнює m! (факторіал від m).

При використанні подвійної перестановки (двох незалежних ключів) кількість можливих ключів збільшується у m! × m! = (m!)² разів.

1. **Наведіть приклад використання магічного квадрата для шифрування повідомлення «ВИПРОБОВУВАТИ\_НА».**

Візьмемо магічний квадрат 4×4:

|  |  |  |  |
| --- | --- | --- | --- |
| 16 | 2 | 3 | 13 |
| 5 | 11 | 10 | 8 |
| 9 | 7 | 6 | 12 |
| 4 | 14 | 15 | 1 |

Запишемо повідомлення «ВИПРОБОВУВАТИ\_НА» (16 символів, включно з підкресленням) у клітинки квадрата відповідно до чисел:

|  |  |  |  |
| --- | --- | --- | --- |
| В | И | П | Р |
| О | Б | О | В |
| У | В | А | Т |
| И | \_ | Н | А |

1→А, 2→И, 3→П, 4→И, 5→О, 6→А, 7→В, 8→В, 9→У, 10→О, 11→Б, 12→Т, 13→Р, 14→\_, 15→Н, 16→В

Отримане зашифроване повідомлення (зчитування по рядках):  
АИПИОАВВУОБТР\_НВ

1. **Що таке шифрування перестановкою біт?**

Шифрування перестановкою біт — це метод, коли переставляються не символи повідомлення, а окремі біти у їх двійковому поданні. Таким чином формується нова послідовність бітів, яка змінює вигляд символів, хоча їхня кількість залишається сталою.

1. **Запропонуйте порядок розкриття шифру перестановки. Яка складність виникає при цьому, і які «помилки» шифрувальників можна використовувати?**

Порядок розкриття:

1. Визначити довжину ключа (кількість стовпців або переставних позицій).
2. Скласти таблицю можливих перестановок.
3. Поступово перевіряти перестановки, намагаючись отримати осмислений текст.

Складність: кількість можливих ключів дорівнює факторіалу довжини (m!), що швидко зростає і ускладнює повний перебір.

Можливі помилки шифрувальників:

* використання коротких ключів (невелике m);
* застосування простих або «природних» перестановок (напр., зсув на 1–2 позиції);
* збереження пробілів та пунктуації, що допомагає відновити структуру тексту.