**Міністерство освіти і науки України**

**Національний університет «Львівська політехніка»**

**Кафедра СКС**

****

# Звіт

до лабораторної роботи №2

# з дисципліни: «Захист інформації в комп’ютерних системах»

На тему: «Перестановочний шифр»

# Варіант №3

Виконав:

ст.гр. КІ-307

Ващишин І.І.

Прийняв:

Морозов Ю.В.

Львів 2025

**Мета:** ознайомитись з основами класичної техніки шифрування – перестановочний шифр.

**Теоретичні відомості**

Розглянутий вище метод ґрунтувався на заміщенні символів відкритого тексту різними символами шифрованого тексту. Принципово інший клас перетворень будується на використанні перестановок букв відкритого тексту. Шифри, створені за допомогою перестановок, називають перестановочними шифрами.

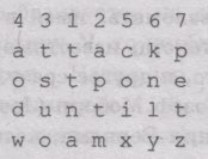
Найпростіший з таких шифрів використає перетворення "драбинки", що полягає в тім, що відкритий текст записується уздовж похилих рядків певної довжини ("сходів"), а потім зчитується построчно по горизонталі. Наприклад, щоб шифрувати повідомлення "meet me after the toga party" по методу драбинки зі сходами довжиною 2, запишемо це повідомлення у вигляді:



Шифроване повідомлення буде мати такий вигляд:



Такий "шифр" особливої складності для криптоаналізу не представляє. Більше складна схема припускає запис тексту повідомлення в горизонтальні рядки однакової довжини й наступне зчитування тексту стовпець за стовпцем, але не один по одному, а відповідно до деякої перестановки стовпців. Порядок зчитування стовпців при цьому стає ключем алгоритму. Розглянемо наступний приклад.

Ключ:

Відкритий текст:

Шифрований текст: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Простий перестановочный шрифт дуже легко розпізнати, тому що букви в ньому зустрічаються з тією же частотою, що й у відкритому тексті. Наприклад, для тільки що розглянутого способу шифрування з перестановкою стовпців аналіз шифру виконати досить просто - необхідно записати шифрований текст у вигляді матриці й перебрати можливі варіанти перестановок для стовпців. Можна використати також таблиц і значень частоти биграм і триграм.

**Завдання лабораторної роботи**

1. Створити програму, що реалізує довільний перестановочний шифр.
2. Підготувати і захистити звіт, в якому обов’язково навести алгоритм роботи даного перестановочного шифру.

**Хід виконання роботи:**

Програма реалізована на мові Python

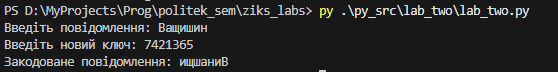
**Код програми:**

class Encryption:  
 def \_\_init\_\_(self):  
 self.key\_char = ['1', '2', '3', '4', '5', '6', '7',  
 '8', '9']  
 self.message = ""  
 self.key = ""  
  
 def input\_data(self):  
 # Просимо користувача ввести повідомлення та новий ключ  
 self.message = input("Введіть повідомлення: ")  
 self.key = input("Введіть новий ключ: ")  
  
 def encryption(self, message):  
 result\_message = ""  
 for i in range(len(self.key)):  
 # Для кожного символу ключа обчислюємо зміщення та додаємо відповідні символи повідомлення до результату  
 for j in range(self.key.index(self.key\_char[i]), len(message), len(self.key)):  
 result\_message += message[j]  
 return result\_message  
  
 def run(self):  
 self.input\_data()  
 # Зашифруємо повідомлення та виведемо результат  
 encrypted\_message = self.encryption(self.message)  
 print("Закодоване повідомлення:", encrypted\_message)  
  
  
def main():  
 # Створимо екземпляр класу шифрування та запустимо програму  
 enc = Encryption()  
 enc.run()  
  
  
if \_\_name\_\_ == "\_\_main\_\_":  
 main()

**Алгоритм роботи програми:**

1. Створення класу Encryption.
2. У конструкторі класу ініціалізується список key\_char з цифрами від 1 до 9, а також змінні message і key.
3. Метод input\_data запитує користувача ввести повідомлення та новий ключ.
4. Метод encryption приймає повідомлення як аргумент, потім перебирає ключ і шифрує повідомлення, додаючи до result\_message символи з повідомлення у порядку, що визначається ключем.
5. Метод run викликає метод input\_data, а потім застосовує метод encryption до введеного повідомлення і виводить результат.
6. Функція main створює екземпляр класу Encryption і викликає його метод run.
7. При запуску програми викликається функція main, яка виконує основну логіку програми.

**Результат виконання програми:**



**Висновок:** на цій лабораторній роботі, я користуючись методичними вказівками навчився працювати з шифрами і програмами, що реалізують довільний перестановочний шифр, також навчився виправляти помилки , які можуть появитись при їх виконанні.