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: ассистент кафедри АІС Андреєв П. І.

Кременчук 2025

**ЛАБОРАТОРНА РОБОТА № 2**

**Тема:** Шифрування методами заміни

**Мета:** вивчити методи шифрування заміною.

**Порядок виконання роботи:**

Реалізувати алгоритми шифрування (для непарних варіантів) і дешифрування (для парних) файлів за допомогою методу, зазначеного у варіанті.

15–16. Шифр Гронсфельда.

**Варіант: 15**

**Скрипт програми:**

ALPHABET = "АБВГДЕҐІЇЖЗИКЛМНОПРСТУФХЦЧШЩЬЄЮЯ "  
M = len(ALPHABET)  
  
  
def encrypt\_gronsfeld(plain\_text, key):  
 cipher\_text = ""  
 key\_digits = [int(k) for k in key]  
  
 for i, char in enumerate(plain\_text):  
 if char not in ALPHABET:  
 cipher\_text += char  
 continue  
 P = ALPHABET.index(char)  
 K = key\_digits[i % len(key\_digits)]  
 C = (P + K) % M  
 cipher\_text += ALPHABET[C]  
 return cipher\_text  
  
  
def main():  
 plain\_text = input("Введіть текст для шифрування (тільки українські літери та пробіли): ").upper()  
  
 for c in plain\_text:  
 if c not in ALPHABET:  
 print(f"Помилка: недопустимий символ '{c}' у тексті!")  
 return  
  
 key = input("Введіть числовий ключ: ")  
 if not key.isdigit():  
 print("Помилка: ключ повинен складатися лише з цифр!")  
 return  
  
 cipher\_text = encrypt\_gronsfeld(plain\_text, key)  
 print("\nЗашифрований текст:")  
 print(cipher\_text)  
  
  
if \_\_name\_\_ == "\_\_main\_\_":  
 main()

**Результат:**

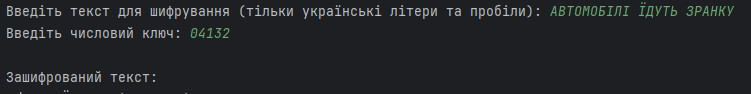
****

Рисунок 2.1 – Результат шифрування програми

**Висновок:** на цій лабораторній роботі ми вивчили методи шифрування заміною.

**Контрольні питання:**

1. **Які шифри називають шифрами заміни?**

Шифри заміни – це такі шифри, в яких кожен символ відкритого тексту замінюється на інший символ (шифрозображення), при цьому порядок символів у шифротексті збігається з порядком символів відкритого повідомлення.

1. **Що таке ключ шифру заміни?**

Ключ шифру заміни – це таблиця або набір правил, за якими відбувається заміна кожного символу відкритого тексту на символ шифру. Знаючи ключ, можна як шифрувати, так і дешифрувати повідомлення.

1. **Що називають множиною шифрозображень?**

Множина шифрозображень для символу α – це сукупність всіх символів, на які можна замінити α під час шифрування.

* Якщо в множині лише один елемент, такий шифр називають простою заміною.

1. **Наведіть приклади шифрів простої заміни. Опишіть алгоритм одного з них.**

Приклади:

* Цезар (зсув)
* Афінний шифр
* Шифр Атбаш

Алгоритм шифрування Цезаря:

1. Визначаємо алфавіт і його розмір mmm.
2. Вибираємо ключ – на скільки позицій зміщувати літери.
3. Для кожної літери відкритого тексту з номером ttt обчислюємо номер шифротексту:

(1)

1. Замість літери з номером ttt ставимо літеру з номером .
2. **Які основні недоліки шифрів простої заміни?**

* Легко піддаються частотному аналізу (частоти букв у шифротексті збігаються з частотами в мові).
* Мала стійкість до криптоаналізу, особливо при коротких алфавітах.
* Для великих текстів і постійного ключа шифр швидко «розкривається».