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:

```
Введіть текст для шифрування (тільки українські літери та пробіли): АВТОМОБІЛІ ЇДУТЬ ЗРАНКУ
Введіть числовий ключ: 04132

Зашифрований текст:
АҐУСООЕЇОЖ КЕЦФЬГИУВНОФ
```

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.

2. 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.

3. 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.

4. 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 k – на скільки позицій зміщувати літери.

3. Для кожної літери відкритого тексту з номером ttt обчислюємо номер шифротексту:

$$C = (t + k)\ mod\ m \quad (1)$$

4. Замість літери з номером ttt ставимо літеру з номером C.

5. 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».