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 № 3

Тема: Шифрування методом Вернама

Мета: навчитися писати програми для шифрування (дешифрування) методом Вернама

Порядок виконання роботи:

Розробити програмний код застосування бібліотеки шифрування даних методом Вернама. При цьому:

Змоделювати кодер з послідовністю ключів із 17 елементів.

Варіант: 15

Скрипт програми:

```
import random

KEY_LENGTH = 17
key = [random.randint(0, 255) for _ in range(KEY_LENGTH)]
print("Згенерований ключ (17 елементів):", key)

plaintext = input("Введи текст для шифрування: ")

plain_bytes = plaintext.encode("utf-8")

cipher_bytes = bytearray()
for i, byte in enumerate(plain_bytes):
    cipher_byte = byte ^ key[i % KEY_LENGTH]
    cipher_bytes.append(cipher_byte)

cipher_hex = cipher_bytes.hex()
print("\nШифртекст (у hex):", cipher_hex)
```

Результат:

```
Згенерований ключ (17 елементів): [73, 90, 140, 211, 168, 64, 120, 171, 120, 193, 250, 222, 14, 214, 138, 184, 17]
Введи текст для шифрування: Hello World!

Шифртекст (у hex): 013fe0bfc7602fc40aad9eff
```

Рисунок 3.1 – Результат шифрування програми

Висновок: на цій лабораторній роботі ми навчилися писати програми для шифрування (дешифрування) методом Вернама.

Контрольні питання:

1. Що таке шифрування, дешифрування?

1) Шифрування – це процес перетворення відкритого тексту у зашифрований, щоб зробити його незрозумілим для сторонніх.

2) Дешифрування – це зворотний процес: перетворення зашифрованого тексту назад у початковий, зрозумілий вигляд.

– У шифруванні завжди беруть участь два основні елементи: повідомлення (що шифрується) і ключ (за допомогою якого воно шифрується).

2. Що таке алфавіт, текст?

1) Алфавіт – це множина всіх можливих символів, які можуть входити до тексту.

– Наприклад: для англійського тексту – A–Z, a–z, пробіл, пунктуація тощо.

– Для комп'ютера алфавіт – це просто набір чисел (байтів) від 0 до 255, бо будь-який символ має свій код у таблиці ASCII або UTF-8.

2) Текст – це послідовність символів із певного алфавіту.

– У нашому випадку ми кодуємо його в байти, щоб виконувати математичні операції над ними.

3. Що таке ключ:\?

– Ключ – це секретна послідовність даних, за допомогою якої виконується шифрування та дешифрування.

– Без правильного ключа отримати початковий текст практично неможливо.

– У нашому прикладі ключ – це набір випадкових чисел від 0 до 255, який ми генеруємо ось так:

– key = [random.randint(0, 255) for _ in range(17)]

4. У чому полягає шифрування методом Вернама?

1) Кожен байт відкритого тексту XOR'иться (тобто додається за модулем 2) із байтом ключа.

2) Формула:

3) $y = x \oplus k$

де

x – байт відкритого тексту,

k – байт ключа,

$\oplus$ – операція XOR (виключне "АБО"),

y – байт зашифрованого тексту.

– Якщо виконати ту ж саму операцію ще раз, то ми отримаємо початковий байт:

– $(x \oplus k) \oplus k = x$

Тобто XOR сам себе «знищує» при повторному застосуванні.

– Ідея: якщо ключ абсолютно випадковий і ніколи не повторюється, такий шифр неможливо зламати – це ідеально стійке шифрування.

5. Як можна реалізувати нескінченну послідовність ключів?

– Один із способів – повторювати ключ циклічно, як у нашому коді:

– key[i % KEY_LENGTH]

Тобто якщо текст довший за ключ, програма починає використовувати ключ заново з початку.

– Інший спосіб – генерувати ключ динамічно, наприклад, із генератора псевдовипадкових чисел (PRNG), який видає нескінченну послідовність байтів.

6. Яким має бути текст перед безпосереднім шифруванням?

Текст повинен бути:

– перетворений у байти (через .encode("utf-8")),

– без «сирих» символів, які не входять до алфавіту (наприклад, нечитабельні юнікодні знаки без підтримки у шифрі),

– чітко визначений – без додаткових пробілів або невидимих символів, щоб результат був відтворюваним.