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 № 5

Тема: Шифрування методом гамування

Мета: вивчити шифрування методом гамування.

Порядок виконання роботи:

Завдання згруповані по парах. Непарні варіанти пишуть програму шифрування тексту із застосуванням зазначеного методу, парні варіанти програмують дешифратор.

Зашифрувати та розшифрувати текст, що знаходиться у файлі з ім’ям Source.txt. Закодований текст зберегти у файлі з ім’ям Coded.txt, розшифрований текст записати у файл DeCoded.txt.

Для генерації гами використовувати:

13–16 мультиплікативний датчик;

Варіант: 15

Скрипт програми:

```
import random

# Параметри мультиплікативного датчика
a = 7
m = 256
x0 = 5

def multiplicative_generator(length, a, m, x0):
    gamma = []
    x = x0
    for _ in range(length):
        x = (a * x) % m
        gamma.append(x)
    return gamma

def encrypt_bytes(data, gamma):
    encrypted = bytearray()
    for i, byte in enumerate(data):
        encrypted.append((byte * gamma[i % len(gamma)]) % m)
    return bytes(encrypted)

with open("Source.txt", "r", encoding="utf-8") as f:
    source_text = f.read()

source_bytes = source_text.encode("utf-8")
gamma = multiplicative_generator(len(source_bytes), a, m, x0)

encrypted_bytes = encrypt_bytes(source_bytes, gamma)
with open("Coded.txt", "wb") as f:
```

```
    f.write(encrypted_bytes)

print("Шифрування завершено.")
```

Результат:

```
C:\Python313\python.exe C:\Users\RoRHaT\Documents\GitHub\tzi-polynko-kn-23-1\5\python\script.py
Шифрування завершено.

Process finished with exit code 0
```

Рисунок 5.1 – Результат роботи програми

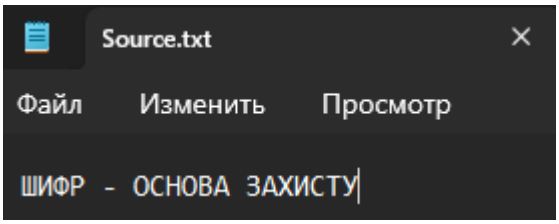

Рисунок 4.2 – Вміст файлу Source

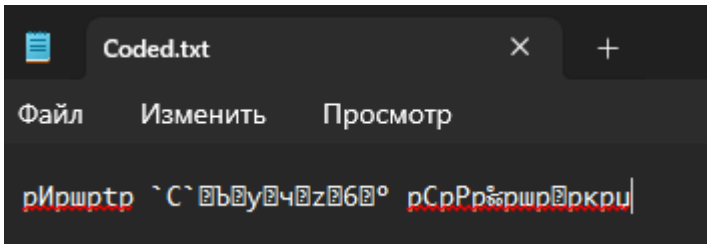

Рисунок 4.3 – Вміст файлу Coded

Висновок: на цій лабораторній роботі ми навчилися шифруванню методом гамування.

Контрольні питання:

1. Що таке гамування? Що розуміють під гамою шифру?

Гамування – це спосіб шифрування, за якого до елементів відкритого тексту послідовно додаються (накладаються) елементи спеціально згенерованої псевдовипадкової послідовності, що називається гамою шифру. Гама шифру – це послідовність чисел (символів), які утворюють ключовий потік і використовуються для перетворення повідомлення під час шифрування та розшифрування.

2. Які операції можна застосовувати для накладення гами? У чому полягає процес шифрування та дешифрування?

Для накладення гами можуть використовуватися такі операції:

– додавання за модулем m;

– побітова операція XOR (додавання за модулем 2);

– множення за модулем m.

Процес шифрування полягає в тому, що кожен елемент відкритого тексту комбінується з відповідним елементом гами за вибраною операцією. Процес дешифрування виконується аналогічно – за тією ж гамою, із застосуванням зворотної операції (або тієї ж самої, якщо це XOR).

3. Які переваги та недоліки має метод гамування?

Переваги:

– висока криптографічна стійкість за умови використання неповторюваної гами;

– простота реалізації алгоритму;

– можливість шифрування даних у потоковому режимі (поступово, без попереднього поділу на блоки).

Недоліки:

– необхідність синхронізації генераторів гами на стороні шифрування та дешифрування;

– у разі повторного використання тієї самої гами без зміни початкового стану шифр стає вразливим до криптоаналізу;

– складність забезпечення справді випадкової та довгої гами.

4. Які вимоги висувають до криптографічно стійкого генератора? Чому найбільш важлива довжина періоду гами?

Криптографічно стійкий генератор гами повинен забезпечувати:

– велику довжину періоду (послідовність не повинна повторюватися протягом шифрування всього повідомлення);

– рівномірний розподіл згенерованих значень;

– непередбачуваність наступних елементів навіть при знанні частини послідовності;

– стійкість до відновлення початкових параметрів (ключа, початкового стану).

Довжина періоду гами є найважливішою характеристикою, оскільки повторення гами призводить до періодичного повторення шифрованих фрагментів, що дає змогу криптоаналітику виявити закономірності й розкрити шифр.