Лабораторная работа №1: Шифр Цезаря

Введение

Шифр Цезаря — это моноалфавитный шифр подстановки, в котором каждая буква открытого текста заменяется на букву, находящуюся на фиксированное число позиций (ключ) дальше в алфавите. Этот шифр назван в честь Юлия Цезаря, который использовал его для защиты своей переписки.

Математическая модель

Шифрование описывается формулой:

$$C = (P + k) \mod m$$

где:

- P — номер буквы открытого текста,
- C — номер буквы шифртекста,
- k — ключ (сдвиг),
- m — количество букв в алфавите (например, 26 для латинского алфавита).

Расшифрование выполняется по формуле:

$$P = (C - k) \mod m$$

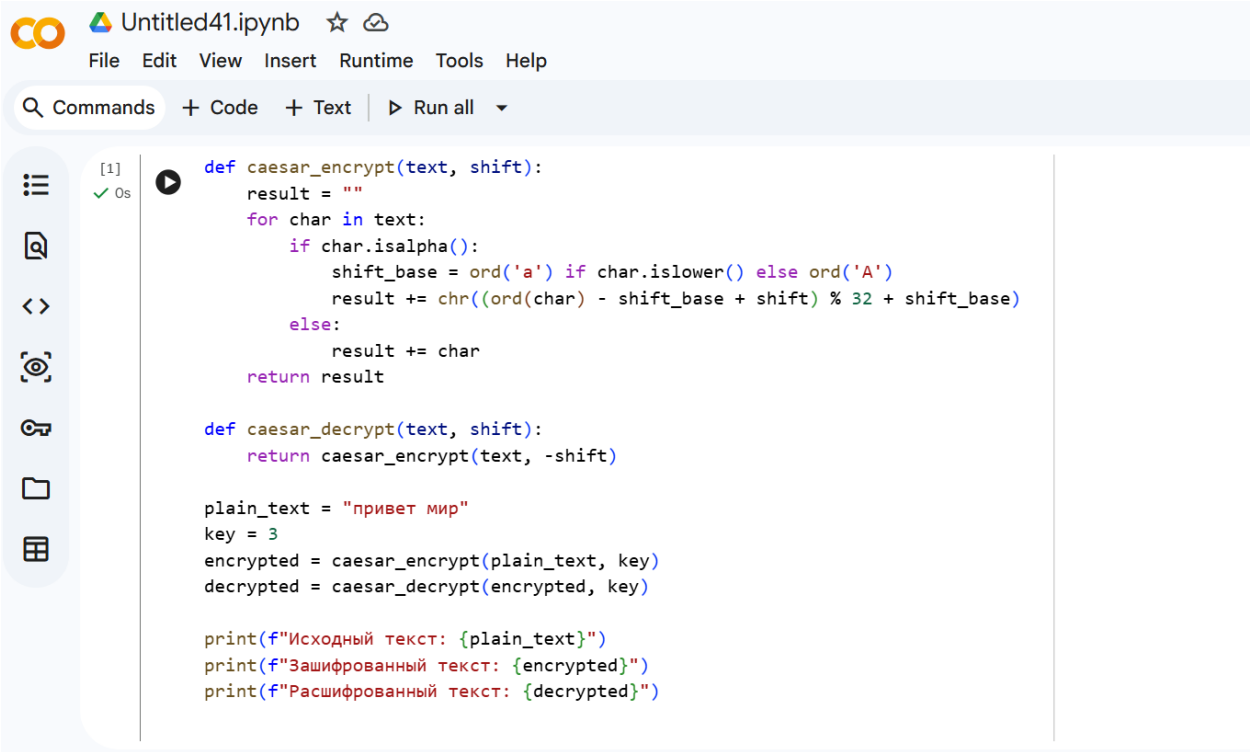
Реализация на Python

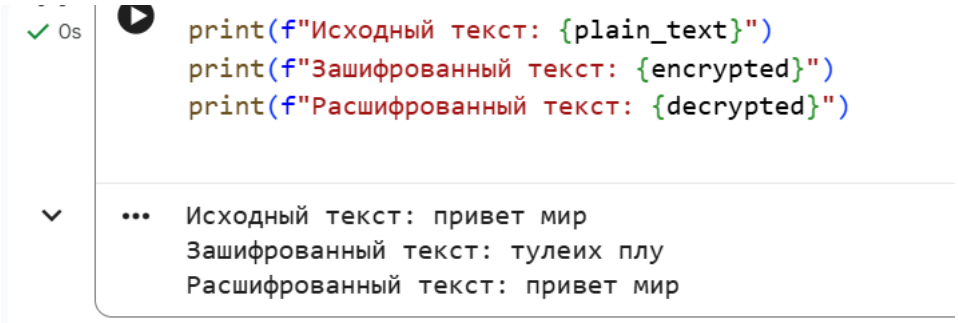
python

```python
def caesar_encrypt(text, shift):
    result = ""
    for char in text:
        if char.isalpha():
            shift_base = ord('a') if char.islower() else ord('A')
            result += chr((ord(char) - shift_base + shift) % 32 + shift_base)
        else:
            result += char
    return result

def caesar_decrypt(text, shift):
    return caesar_encrypt(text, -shift)
```

```
plain_text = "привет мир"
key = 3
encrypted = caesar_encrypt(plain_text, key)
decrypted = caesar_decrypt(encrypted, key)

print(f"Исходный текст: {plain_text}")
print(f"Зашифрованный текст: {encrypted}")
print(f"Расшифрованный текст: {decrypted}")
```

Пример работы программы





Вывод

Шифр Цезаря является простым и исторически значимым методом шифрования, но он не обеспечивает достаточного уровня безопасности для современных применений из-за уязвимости к частотному анализу и атакам методом brute force.

Список литературы

1. Цезарь Ю. Записки о Галльской войне.
2. Шнайер Б. Прикладная криптография. — М.: Триумф, 2002.
3. Алферов А.П. и др. Основы криптографии. — М.: Гелиос АРВ, 2002.
4. https://ru.wikipedia.org/wiki/Шифр_Цезаря