

# **Лабораторная работа №7**

**Элементы криптографии. Однократное гаммирование**

Панченко Денис Дмитриевич

# Содержание

1	Цель работы	3
2	Задачи	4
3	Выполнение лабораторной работы	5
4	Контрольные вопросы	7
5	Вывод	9

# **1 Цель работы**

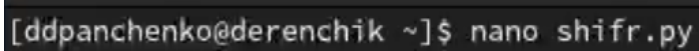
Освоить на практике применение режима однократного гаммирования.

## 2 Задачи

- Научиться применять режим однократного гаммирования.

### 3 Выполнение лабораторной работы

- 1) Создадим файл с программой (рис. 3.1).



```
[ddpanchenko@derenchik ~]$ nano shifr.py
```

Рис. 3.1: Файл с программой

- 2) Напишем саму программу для шифрования (рис. 3.2).

```

GNU nano 5.6.1 shifr.py
def generate_key(message_length):
    import secrets
    return bytearray(secrets.token_bytes(message_length))

def encrypt(message, key):
    encrypted = bytearray(len(message))
    for i in range(len(message)):
        encrypted[i] = message[i] ^ key[i]
    return encrypted

def decrypt(encrypted, key):
    decrypted = bytearray(len(encrypted))
    for i in range(len(encrypted)):
        decrypted[i] = encrypted[i] ^ key[i]
    return decrypted

def main():
    plaintext = "С Новым Годом, друзья!"
    plaintext_bytes = plaintext.encode('utf-8')

    key = generate_key(len(plaintext_bytes))

    ciphertext = encrypt(plaintext_bytes, key)

    print("Зашифрованный текст:")
    print(ciphertext)

    decrypted = decrypt(ciphertext, key)

    decrypted_text = decrypted.decode('utf-8')
    print("Дешифрованный текст:")
    print(decrypted_text)

if __name__ == "__main__":
    main()

```

Рис. 3.2: Программа

3) Выполним эту программу (рис. 3.3).

```

[ddpanchenko@derenchik ~]$ python shifr.py
Зашифрованный текст:
bytearray(b'RQ$xdf\xeazt.\xc4u\xc7NC\xec\xd5\x9fB2a+r\x10\xc5\xcd\x15z\x1c\xcb\xa4\xb0d\x13\x9b\xb5\xc73\xf5\x
d7\xbe')
Дешифрованный текст:
С Новым Годом, друзья!

```

Рис. 3.3: Выполнение программы

## 4 Контрольные вопросы

1. Поясните смысл одноразового гаммирования. Одноразовое гаммирование - это метод шифрования, при котором каждый символ открытого текста преобразуется путем выполнения операции XOR с соответствующим символом ключа. Этот метод получил свое название потому, что каждый ключ используется только один раз для шифрования определенного сообщения.
2. Перечислите недостатки одноразового гаммирования.
  - Необходимость в ключе такой же длины, как и открытый текст.
  - Необходимость генерации случайного ключа для каждого сообщения.
  - Уязвимость к атакам, основанным на повторном использовании ключа.
  - Ограничение на размер сообщения из-за необходимости ключа такой же длины.
3. Перечислите преимущества одноразового гаммирования.
  - При правильной реализации и использовании случайного ключа является абсолютно надежным методом шифрования.
  - Нельзя получить информацию о зашифрованном тексте без знания ключа.
  - Сложность криптоанализа возрастает с увеличением размера ключа и текста.
4. Почему длина открытого текста должна совпадать с длиной ключа? Поскольку для каждого символа открытого текста используется соответствующий символ ключа при операции XOR, длина ключа должна быть такой же, как

и длина открытого текста, чтобы обеспечить правильное шифрование и дешифрование.

5. Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется операция XOR (побитовое сложение по модулю 2). Особенность этой операции заключается в том, что она возвращает true (1), если только один из операндов true (1), и false (0) в противном случае.
6. Как по открытому тексту и ключу получить шифротекст? Шифротекст получается путем выполнения операции XOR между каждым символом открытого текста и соответствующим символом ключа.
7. Как по открытому тексту и шифротексту получить ключ? Ключ получается путем выполнения операции XOR между каждым символом шифротекста и соответствующим символом открытого текста.
8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра включают:
  - Полная случайность ключа.
  - Равенство длин ключа и открытого текста.
  - Однократное использование ключа.



## **5 Вывод**

Я освоил на практике применение режима однократного гаммирования.