Лабораторная работа 7

Элементы криптографии. Однократное гаммирование

Панченко Д. Д.

11 мая 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Панченко Денис Дмитриевич
- Студент 2 курса факультета физико-математических наук.
- Российский университет дружбы народов
- derenchikde@gmail.com

Цели и задачи

- Цель: Освоить на практике применение режима однократного гаммирования.
- Задачи:
  - Научиться применять режим однократного гаммирования.

Выполнение лабораторной работы

1) Создадим файл с программой.

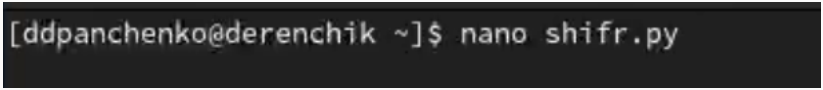

Рис. 1: Файл с программой

2) Напишем саму программу для шифрования.

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:")
```

3) Выполним эту программу.

```
[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: Выполнение программы

Вывод

Вывод

Я освоил на практике применение режима однократного гаммирования.