Лабораторная работа №7

Основы информационной безопасности

Мишина А. А.

8 мая 2024

Докладчик

- Мишина Анастасия Алексеевна
- НПИбд-02-22

Выполнение лабораторной работы

Цель работы

- Освоить на практике применение режима однократного гаммирования.

Шифрование

```python
def encrypt(text: str, key: list = None):
    '''
    Выводит шифротекст для заданного текста.
    Если ключа нет, то генерируется случайный ключ
    '''

    text_16 = [char.encode(encoding='cp1251').hex().upper() for char in text]
    if not key:
        key = generate_key(length=len(text))

    print(f"Ключ шифрования:", ' '.join(str(s) for s in key))
    print(f"Исходный текст:", ' '.join(text_16))

    encrypted_text = []
    for i in range(len(text)):
        xor_char = int(text_16[i], 16) ^ int(key[i], 16)
        encrypted_text.append(int2hex(xor_char))

    encrypted_text = validate(encrypted_text)
    ciphertext = bytes.fromhex(''.join(encrypted_text)).decode('cp1251')
    print(f"Шифротекст: {ciphertext}\n\n")

    return {
        'key': key,
        'ciphertext': ciphertext
    }
```

Рис. 1: Функция encrypt()

Выполнение шифрования

```
encryption = encrypt('С Новым Годом, друзья!')
```

Рис. 2: Вызов функции encrypt()

```
[aamishina@aamishina Documents]$ python main.py
Ключ шифрования: 7A C0 EB A1 20 79 F5 71 68 75 32 8B 4C 52 F3 BE 3A C0 FF A3 CB 66
Исходный текст: D1 20 CD EE E2 FB EC 20 C3 EE E4 EE EC 2C 20 E4 F0 F3 E7 FC FF 21
Шифротекст: «a&OB,Q«›Це ~YZK3_4G
```

Рис. 3: Результаты работы функции encrypt()

Дешифровка

```python
def decrypt(ciphertext: str, key: list = None):
    ciphertext_16 = [char.encode('cp1251').hex().upper() for char in ciphertext]
    if not key:
        key = generate_key(length=len(ciphertext))

    print(f"Ключ шифрования:", ' '.join(str(s) for s in key))
    print(f"Исходный шифротекст:", ciphertext)

    decrypted_text = []
    for i in range(len(ciphertext)):
        xor_char = int(ciphertext_16[i], 16) ^ int(key[i], 16)
        decrypted_text.append(int2hex(xor_char))

    decrypted_text = validate(decrypted_text)
    decrypted_text = bytes.fromhex(''.join(decrypted_text)).decode('cp1251')

    print('Расшифрованный текст: ', decrypted_text)

    return {
        'key': key,
        'text': decrypted_text
    }
```

Рис. 4: Функция decrypt()

Выполнение дешифровки

```
encryption = encrypt('С Новым Годом, друзья!')
decrypt(encryption['ciphertext'], key=encryption['key'])

:wq
```

Рис. 5: Вызов функции denrypt()

```
[aamishina@aamishina Documents]$ python main.py
Ключ шифрования: 79 2E 70 29 28 2C 5C 21 0A 93 0A C4 F9 D5 51 98 27 1F 1F CD 10 FA
Исходный текст: D1 20 CD EE E2 FB EC 20 C3 EE E4 EE EC 2C 20 E4 F0 F3 E7 FC FF 21
Шифротекст: ËS3КЧ°Й}о*щq|Чмш1пы


Ключ шифрования: 79 2E 70 29 28 2C 5C 21 0A 93 0A C4 F9 D5 51 98 27 1F 1F CD 10 FA
Исходный шифротекст: ËS3КЧ°Й}о*щq|Чмш1пы
Расшифрованный текст:  С Новым Годом, друзья!
[aamishina@aamishina Documents]$
```

Рис. 6: Результаты работы функции denrypt()

Выполнение дешифровки

```
encryption = encrypt('С Новым Годом, друзья!')
decrypt(encryption['ciphertext'])
```

Рис. 7: Вызов функции denrypt()

```
[aamishina@aamishina Documents]$ python main.py
Ключ шифрования: 95 92 58 BA 93 89 23 79 F8 A9 E9 87 D7 4D 3B 9E 5E EB AC BE E8 BF
Исходный текст: D1 20 CD EE E2 FB EC 20 C3 EE E4 EE EC 2C 20 E4 F0 F3 E7 FC FF 21
i;a*KBhкст: DI•TqrNY;G


Ключ шифрования: 09 A8 81 3D 9E 0D D8 F0 2F 56 8F 8A 32 5D 6E 6D 6D 07 BA B6 F0 76
i;a*KBhй шифротекст: DI•TqrNY;G
Расшифрованный текст:  M?n©,r  <uГсфзи
[aamishina@aamishina Documents]$
```

Рис. 8: Результаты работы функции denrypt()

Поиск ключа

```
def find_key(text):
    '''
    Подбирает ключ, с помощью которого сообщение было зашифровано
    '''

    decrypted_text = ''
    encryption = encrypt(text)

    while decryption_text != text:
        decryption = decrypt(encryption['ciphertext'])
        decrypted_text = decryption['text']
        print(f'Полученный текст: {decrypted_text}')
    print(f"Ключ успешно подобран! {decryption['key']}")
```

Рис. 9: Функция find_key()

Вывод

- В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.