Отчет по лабораторной работе № 7

По дисциплине Информационная безопасность

Выполнил: Максимов Алексей Александрович

Группа: НПИ-бд-01-20

Российский Университет Дружбы Народов #### г. Москва

Цель работы

Освоить на практике применение режима однократного гаммирования.

Задание

Создать программу для шифровки и поиска ключа.

Выполнение лабораторной работы

написал программу

main.py

```python
import itertools
# Составляем словарь
3 usages
def form_dict():
    ascii_dict = dict()
    ascii_in_number = range(0, 256)
    for i in ascii_in_number:
        ascii_dict[i] = chr(i)
    return ascii_dict

# Разбираем слово и ключ в ASCII
2 usages
def encode_val(word):
    d = form_dict()
    return [k for c in word for k, v in d.items() if v == c]
# Разбираем слово и ключ из ASCII
1 usage
def decode_val(value):
    d = form_dict()
    decode_v = ''
    for i in value:
        decode_v = decode_v + d[i]
    return decode_v
1 usage
def comparator(value, key):
    return dict([(index, list(character))
                 for index, character in enumerate(zip(value, itertools.cycle(key)))])
# сложение по модулю
2 usages
```

```
2 usages
def full_encode(value, key):
    d = comparator(value, key)
    l = len(form_dict())
    return [(v[0] ^ v[1]) % l for v in d.values()]

...

word = 'S novim godom, druzia!'
key = 'svnguervjttjvhkunuziiu'
print('Слово: ' + word, "; len:", len(word))
print('Ключ: ' + key, "; len:", len(key))
key_encoded = encode_val(key)
print('ключ в ASCII :', key_encoded, "; len:", len(key_encoded))
value_encoded = encode_val(word)
print('слово в ASCII :', value_encoded, "; len:", len(value_encoded))
encoded_text = full_encode(value_encoded, key_encoded)
print('закодированный текст :', encoded_text)
# получаем ключи из текста и закодированного текста
encoded_key = full_encode(value_encoded, encoded_text)
print('найденый ключ :', encoded_key)
decoded_val = decode_val(encoded_key)
print(decoded_val)
print(key)
```

смотрим результат

```
Run:  main
C:\Users\maksi\PycharmProjects\lab7_infoBez\venv\Scripts\python.exe C:\Users\maksi\PycharmProjects\lab7_infoBez\main.py
Слово: S novim godom, druzia! ; len: 22
Ключ: svnguervjttjvhkunuziiu ; len: 22
ключ в ASCII : [115, 118, 110, 103, 117, 101, 114, 118, 106, 116, 116, 106, 118, 104, 107, 117, 110, 117, 122, 105, 105, 117] ; len: 22
слово в ASCII : [83, 32, 110, 111, 118, 105, 109, 32, 103, 111, 100, 111, 109, 44, 32, 100, 114, 117, 122, 105, 97, 33] ; len: 22
закодированный текст : [32, 86, 0, 8, 3, 12, 31, 86, 13, 27, 16, 5, 27, 68, 75, 17, 28, 0, 0, 0, 8, 84]
найденый ключ : [115, 118, 110, 103, 117, 101, 114, 118, 106, 116, 116, 106, 118, 104, 107, 117, 110, 117, 122, 105, 105, 117]
svnguervjttjvhkunuziiu
svnguervjttjvhkunuziiu

Process finished with exit code 0
```

Выводы

Освоили на практике применение режима однократного гаммирования.