МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
“ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ”
(ФГБОУ ВПО “ВГУ”)
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ, ИНФОРМАТИКИ И МЕХАНИКИ
КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И ПРИКЛАДНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ОТЧЁТ

по лабораторной работе №4
“Шифр Вернама”
по специальности 01.03.02 Прикладная математика и информатика

Выполнил:
студент 4-го курса 6-ой группы
Козлуков С.В.
Проверил:
доц. Воронков Б. Н.

Воронеж
2017

Содержание

1 Постановка задачи

- Описать структуру шифра Вернама.
- Зашифровать и расшифровать исходный текст, используя шифр Вернама.
- Составить отчет о проделанной работе.

2 Общие сведения

Алгоритм шифрования Вернама был реализован в компьютерной программе на языке Python3.

3 Описание шифра Вернама

Шифр Вернама — потоковый one-time-pad шифр [2]. Пусть дан открытый текст $m : \{1, \ldots, N\} \to A : i \mapsto m_i$ длины N с элементами из алфавита $A = \{1, \ldots, M\}$. Для шифрования требуется pre-shared ключ k такой же длины N. Криптотекст определяется следующим образом:

$$c_i = m_i \oplus k_i.$$

Для дешифрования требуется повторить операцию:

$$m_i = c_i \oplus k_i.$$

4 Пример работы программы

```
import random
random.seed(42)

msg = """It must be the law of diminishing returns...
I feel the spell about to be broken.
(Energizing himself somewhat.
He takes out a coin, spins it high, catches it,
turns it over on to the back of his other hand,
studies the coin ---
and tosses it to ROS.
His energy deflates and he sits.)
Well, it was an even chance...
if my calculations are correct"""
key = [random.randint(1, 255) for m in msg]
enc = 'ascii'
c = vernam_enc(msg, key, enc=enc)

bytes(c)
```

```
    b"\xedi'\xd32LN\x04\xdf~\x8e\xca\x8d\xe97\xf4\x0c~(w^\x1c\xe6\xf2j\xf9]\xd1\xd4\xdc\xe5\
```

```
print(vernam_dec(c, key, decode=True))
```

```
    It must be the law of diminishing returns...
    I feel the spell about to be broken.
    (Energizing himself somewhat.
    He takes out a coin, spins it high, catches it,
    turns it over on to the back of his other hand,
    studies the coin ---
    and tosses it to ROS.
    His energy deflates and he sits.)
    Well, it was an even chance...
    if my calculations are correct
```

5 Выводы

В ходе работы был изучен и реализован алгоритм Вернама. Алгоритм обеспечивает идеальную криптостойкость, однако неприменим в реальности из-за сложности распределения ключей — ключ должен быть длины не меньшей длины открытого сообщения и должен использоваться лишь единожды. Также в реализации могут [2] возникнуть сложности с согласованием кодировок текста. Повторное использование ключа (в том числе, "зацикливание"короткого ключа для использования с длинным сообщением) компроментирует [1] безопасность.

6 Список использованных источников

[1] *Taking advantage of one-time pad key reuse?* URL: https://crypto.stackexchange.com/questions/59/taking-advantage-of-one-time-pad-key-reuse.

[2] Gilbert S Vernam. "Cipher printing telegraph systems: For secret wire and radio telegraphic communications". B: *Journal of the AIEE* 45.2 (1926), c. 109—115.

7 Код программы

```
import itertools

def vernam_enc(msg, key, enc='ascii', cycle_key=False, decode=False):
    if isinstance(msg, str):
        msg = msg.encode(enc)
    if isinstance(key, str):
        key = msg.encode(enc)
    N = len(msg)
    if len(key) < N and not cycle_key:
        raise ValueError('Vernam: `key` shall be as long as `msg`')
    key = itertools.cycle(key)
    msg = [m^k for m, k in zip(msg, key)]
    if decode:
        msg = bytes(msg)
        msg = msg.decode(enc)
    return msg

vernam_dec = vernam_enc
```