Лабораторная № 3
Шифр гаммированием

Баранов Иван Юрьевич
2022 Москва
RUDN University, Moscow, Russian Federation

ЦЕЛЬ РАБОТЫ

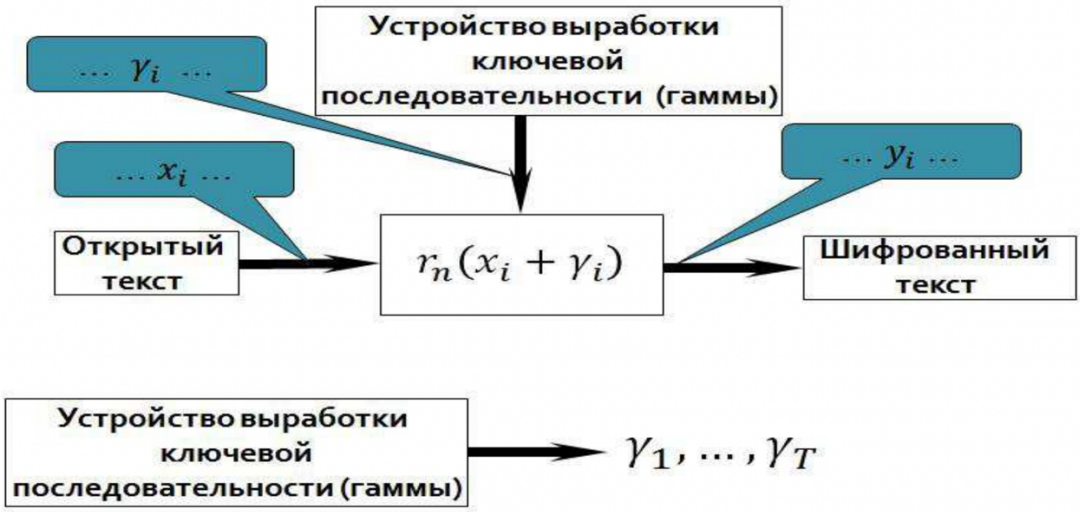
- Ознакомиться с шифрами гаммирования;
- Реализовать шифр гаммированием конечной гаммы при помощи языка программирования PYTHON

Ход работы

- Для реализации алгоритмов использовались средства языка Python.
- Были реализованы шифраторы, рассматриваемых алгоритмов.

Описание

- Гамми́рование (gamma xoring) — метод шифрования, основанный на «наложении» гамма-последовательности на открытый текст. Обычно это суммирование в каком-либо конечном поле (например, в поле GF(2) такое суммирование принимает вид обычного «исключающего ИЛИ»). При расшифровании операция проводится повторно, в результате получается открытый текст.



1 задача шифр гаммированием конечной гаммы

Реализация кода шифрование гамированием конечной гаммой

[101]:
```
def enccrypt(text_1, text_2):

    def alphabet_position(text):
        text = ''.join(text)
        alphabet = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'
        res = ''
        for j in text.lower():
            if j in alphabet:
                res += str(alphabet.index(j)+1) + ', '
            else:
                res += ' '
        return res


    alphabeth = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'
    textLen = len(text_1)
    gammaLen = len(text_2)

    keyText = []
    for i in range(textLen // gammaLen):
        for symb in text_2:
            keyText.append(symb)
    for i in range(textLen % gammaLen):
        keyText.append(text_2[i])

    num_alp_1 = alphabet_position(text_1)
    num_alp_2 = alphabet_position(keyText)
    num_alp_1 = num_alp_1.strip().split(',')
    num_alp_2 = num_alp_2.strip().split(',')

    num_alp_1 = list(map(lambda x: int(x.strip()) if x != '' else None , num_alp_1))
    num_alp_1 = list(filter(None, num_alp_1))

    num_alp_2 = list(map(lambda x: int(x.strip()) if x != '' else None , num_alp_2))
    num_alp_2 = list(filter(None, num_alp_2))

    sum_count = list(map(sum, zip(num_alp_1, num_alp_2)))

    alphabet = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'
    alphabet = list(alphabet)
    length = len(alphabet)
    keys = [i for i in range(1, length+1)]
    dict_ = dict(zip(keys, alphabet))
    final_word = []
    for let in sum_count:
        final_word.append(dict_[let])
    final_word = ''.join(final_word)
    final_word

    return final_word
```

[102]:
```
text_1 = 'приказ'
text_2 = 'гамма'
fin = enccrypt(text_1, text_2)
fin
```

[102]: 'усхчбл'

Вывод

- Ознакомились с шифрами гаммирования;
- Реализовали шифр гаммированием конечной гаммы.