Отчет по лабораторной работе №3.

Шифрование гаммированием

Alexander O. Vorobyov[1]

12 October, 2023

[1]RUDN University, Moscow, Russian Federation

Прагматика выполнения

Прагматика выполнения

Лабораторная работа выполняется для получения знаний о шифровании гаммированием.

Цель работы

Цель работы

Целью данной работы является приобретение практических навыков реализации Шифрования гаммированием.

Задачи выполнения

Задачи выполнения

1. На языке Python реализовал выбор алфавита и его генерацию.

```
[1]  import numpy as np
```

```
[2]  def get_alph(option):
       if option=="eng":
         return list(map(chr, range(ord("a"), ord("z") + 1)))
       elif option=="rus":
         return list(map(chr, range(ord("a"), ord("я") + 1)))
       else:
         print("введите eng или rus")
```

Задачи выполнения

2. Далее реализовал алгоритм шифрования гаммированием.

```python
def gamma_encrypt(message: str, gamma: str):
  alph = get_alph("eng")
  if message.lower() not in alph:
    alph = get_alph("rus")
  print(alph)
  m = len(alph)
  def encrypt(letters_pair: tuple):
    idx = (letters_pair[0] + 1) + (letters_pair[1] + 1) % m
    if idx > m:
      idx = idx - m
    return idx - 1

  message_clear = list(filter(lambda s: s.lower() in alph, message))
  gamma_clear = list(filter(lambda s: s.lower() in alph, gamma))
  message_ind = list(map(lambda s: alph.index(s.lower()), message_clear))
  gamma_ind = list(map(lambda s: alph.index(s.lower()), gamma_clear))

  for i in range(len(message_ind) - len(gamma_ind)):
    gamma_ind.append(gamma_ind[i])
  print(f'{message.upper()} -> {message_ind}\n{gamma.upper()} -> {gamma_ind}')
  encrypted_ind = list(map(lambda s: encrypt(s), zip(message_ind, gamma_ind)))
  print(f'encrypted form: {encrypted_ind}\n')
  return ''.join(list(map(lambda s: alph[s], encrypted_ind))).upper()
```

Figure 1: Код 2

2. Ввел данные для проверки.

```
[4] def test_encryption(message: str, gamma:str):
      print(f'encryption result: {gamma_encrypt(message, gamma)}')
```

```
message = "приказ"
gamma = "гамма"
test_encryption(message, gamma)
```

```
['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р
ПРИКАЗ -> [15, 16, 8, 10, 0, 7]
ГАММА -> [3, 0, 12, 12, 0, 3]
encrypted form: [19, 17, 21, 23, 1, 11]

encryption result: УСХЧБЛ
```

Figure 2: Код 3

Результаты выполнения

Результаты выполнения

В результате проделанной работы я приобрел практические навыки шифрования гаммированием.