

Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Заболотная Кристина Александровна

Содержание

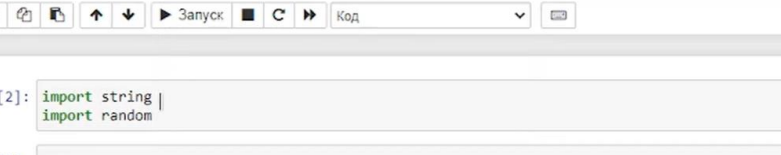
1	Цель работы	1
2	Выполнение лабораторной работы	1
3	Выводы.....	2
	Список литературы.....	2

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Выполнение лабораторной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: Определить вид шифротекста при известном ключе и известном открытом тексте.



```
File Edit View Insert Cell Kernel Widgets Help
[Icons] + % [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
Ввод [2]: import string
import random

Ввод [5]: def function1(text):
return ' '.join(function1(ord(i)[2:] for i in text))

def function2(size):
return ' '.join(random.choice(string.ascii_.letters+string.digits) for _ in range(size))

def function3(text,key):
return ' '.join(chr(a^b) for a,b in zip (text,key))

def function4(text,encrypt):
return ' '.join(chr(a^b) for a,b in zip (text, encrypt))

Ввод [ ]: message = 'С НОВЫМ ГОДОМ, ДРУЗЬЯ!'
key = function2(en(message))
```

Рис. 1: С Новым Годом, друзья!

The screenshot shows a Python IDE with a menu bar (File, Edit, View, Insert, Cell, Kernel, Widgets, Help) and a toolbar with icons for file operations, running, and search. The main editor area contains two code blocks. The first block, labeled 'Ввод [20]:', defines functions for message encryption and decryption. It uses a key 'zDgLIqM1zyRg6zxGluveI9' and a hex key '7a 44 67 4c 57 71 4d 31 7a 79 52 67 36 7a 78 47 4e 75 76 65 49 39'. The second block, labeled 'Ввод [23]:', demonstrates how to compute the key from the encrypted message and decrypt it back to its original form.

```
message = 'С новым Годом, друзья!'
key = function2(len(message))
hex_key = function1(key)
print("Используем ключ: ", key)
print("Ключ в шестнадцатиричном виде: ", hex_key)
encrypt = function3([ord(i) for i in message], [ord(i) for i in key])
hex_encrypt = function1(encrypt)
print("Зашифрованное сообщение: ", hex_encrypt)
decrypt = function3([ord(i) for i in encrypt], [ord(i) for i in key])
print("Расшифрованное сообщение: ", decrypt)
```

Используем ключ: zDgLIqM1zyRg6zxGluveI9
Ключ в шестнадцатиричном виде: 7a 44 67 4c 57 71 4d 31 7a 79 52 67 36 7a 78 47 4e 75 76 65 49 39
Зашифрованное сообщение: 45b 64 45a 472 465 43a 471 11 469 447 466 459 40a 56 58 473 40e 436 441 429 406 1f
Расшифрованное сообщение: С новым Годом, друзья!

```
compute_key = function4([ord(i) for i in message], [ord(i) for i in encrypt])
decrypt_compute_key = function3([ord(i) for i in encrypt], [ord(i) for i in key])
print("Исходный ключ: ", key)
print("Вариант прочтения открытого текста: ", decrypt_compute_key)
```

Исходный ключ: zDgLIqM1zyRg6zxGluveI9
Вариант прочтения открытого текста: С новым Годом, друзья!

3 Выводы

Список литературы