

Отчёт по лабораторной работе 7

Тейшейра Боа Морте Селмилтон

Содержание

4.1. Цель работы	1
4.2. Порядок выполнения работы.....	1
Выводы	2

4.1. Цель работы

Освоить на практике применение режима однократного гаммирования.

4.2. Порядок выполнения 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: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

```
Activities lab7.py (/home/celmi... Oct 20 21:06 en
Open lab7.py Save
/home/celmiltonbm

1 def pad_key(plaintext, key):
2     while len(key) < len(plaintext):
3         key += key
4     return key[:len(plaintext)]
5
6 def encrypt(plaintext, key):
7     key = pad_key(plaintext, key)
8
9     ciphertext = ""
10    for i in range(len(plaintext)):
11        ciphertext += chr(ord(plaintext[i]) ^ ord(key[i]))
12    return ciphertext
13
14 def decrypt(ciphertext, key):
15     key = pad_key(ciphertext, key)
16
17     plaintext = ""
18     for i in range(len(ciphertext)):
19         plaintext += chr(ord(ciphertext[i]) ^ ord(key[i]))
20     return plaintext
21
22 if __name__ == "__main__":
23     plaintext = "С новым годом, друзья!"
24     key = "11101001010" # Certifique-se de que a chave seja pelo menos tão longa quanto o texto
25
26     ciphertext = encrypt(plaintext, key)
27     print("Шифрованный Текст: ", ciphertext)
28

[celmiltonbm@localhost ~]$ su
Password:
[root@localhost celmiltonbm]# gedit lab7.py

(gedit:3912): dconf-WARNING **: 21:02:30.035: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
[root@localhost celmiltonbm]# python lab7.py
Шифрованный Текст: АКУГСКГЦЕЕИХV6ICW
Расшифрованный Текст: С новым годом, друзья!
[root@localhost celmiltonbm]#
```

Выводы

Научил как Освоил на практике применение режима однократного гаммирования.