

Докладчик

- Тейшейра Боа Морте Селмилтон
- Студент Группы НКНбд-01-20
- Факультет Физико-Математических и Естественных Наук
- Российский Университет Дружбы Народов
- <https://github.com/Celmilton>

Цель работы

Освоить на практике применение режима однократного гаммирования.

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:

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.

The screenshot shows a Linux desktop environment. At the top, there's a taskbar with 'Activities', a file manager icon, and a terminal icon. The terminal window is open, showing the command prompt [celmiltonbm@localhost ~]\$ su, followed by Password:, and then [root@localhost celmiltonbm]# gedit lab7.py. The gedit editor is open, displaying a Python script named lab7.py. The script defines three functions: pad_key, encrypt, and decrypt. It also includes a main block that sets a plaintext, a key, and prints the encrypted and decrypted texts. The terminal output shows the execution of the script, displaying the encrypted text 'АКЎҒСКҒҮЄҒҲХV6IC0' and the decrypted text 'С новым годам, Друзья!'.

```

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 годам, Друзья!"
24     key = "11101001010" # Certifigue-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 cre
dentials: Error sending message: Broken pipe
[root@localhost celmiltonbm]# python lab7.py
Шифрованный Текст: АКЎҒСКҒҮЄҒҲХV6IC0
Расшифрованный Текст: С новым годам, Друзья!
[root@localhost celmiltonbm]#

```

Выводы

Научил как Освоить на практике применение режима однократного гаммирования.