Презентация к лабораторной работе №8

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Выполнение работы

Использование функций из предыдущей лабораторной работы

In [1]:
```
import random
from string import ascii_letters, digits
```

In [2]:
```
def generate_key(key_length: int) -> str:
    return ''.join([random.choice(ascii_letters + digits) for _ in range(key_length)])
```

In [3]:
```
def encrypt_and_decrypt(text: str, key: str) -> str:
    if len(key) != len(text):
        raise ValueError('!!! text and key length must be equal !!!')
    return ''.join([chr(ord(text[i]) ^ ord(key[i])) for i in range(len(text))])
```

Проверка корректности равботы функций

In [4]:
```
text1: str = 'bober kurwa'
key: str = generate_key(key_length=len(text1))
print(f'Ключ: {key}')
encrypted_text1: str = encrypt_and_decrypt(text=text1, key=key)
print(f'Исходный текст 1: {text1}')
print(f'Зашифрованный текст 1: {encrypted_text1}')
print(f'Текст 1, расшифрованный ключом: {encrypt_and_decrypt(text=encrypted_text1, key=key)}')
```

```
Ключ: spsXPQC76tj
Исходный текст 1: bober kurwa
Зашифрованный текст 1: ▯▯▯="q(BD▯▯
Текст 1, расшифрованный ключом: bober kurwa
```

In [5]:
```
text2: str = 'ja pierdole'
encrypted_text2: str = encrypt_and_decrypt(text=text2, key=key)
print(f'Исходный текст 2: {text2}')
print(f'Зашифрованный текст 2: {encrypted_text2}')
print(f'Текст 2, расшифрованный ключом: {encrypt_and_decrypt(text=encrypted_text2, key=key)}')
```

```
Исходный текст 2: ja pierdole
Зашифрованный текст 2: ▯▯S(941SY▯▯
Текст 2, расшифрованный ключом: ja pierdole
```

Дешифрование сообщений, зашифрованных одним ключом

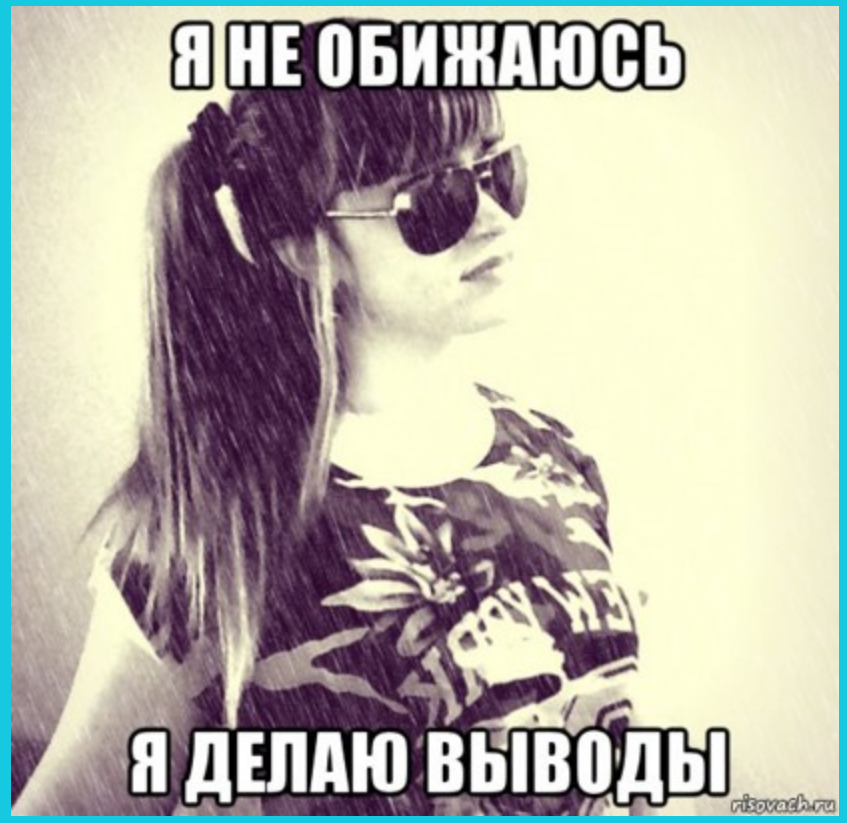
In [6]:

```
potential_key: str = encrypt_and_decrypt(text=text1, key=text2)
print(f'Потенциальный ключ: {potential_key}')
print(f'Текст2, расшифрованный с помощью нового ключа: {encrypt_and_decrypt(text=text1, key=potential_key)}')
print(f'Текст1, расшифрованный с помощью нового ключа: {encrypt_and_decrypt(text=text2, key=potential_key)}')
```

```
Потенциальный ключ:□B□□E□□□□□
Текст2, расшифрованный с помощью нового ключа: ja pierdole
Текст1, расшифрованный с помощью нового ключа: bober kurwa
```

Вывод

В рамках выполнения работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом



Финал