Презентация к лабораторной работе №8

Цель работы

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

Выполнение работы

Начало кода

```
import random
from string import ascii_letters, digits

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

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))])
```

Написание кода для проверки текста 1 текста 2

```
text1: str = 'hey'
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)}')
```

```
text2: str = 'bye'
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)}')
```

Написание кода для потенциального ключа

```
potential_key: str = encrypt_and_decrypt(text=text1, key=text2)
print(f'Потенциальный ключ: {potential_key}')
print(f'Текст 1, расшифрованный с помощью нового ключа: {encrypt_and_decrypt(text=text1, key=potential_key)}')
print(f'Текст 2, расшифрованный с помощью нового ключа: {encrypt_and_decrypt(text=text2, key=potential_key)}')
```

Проверка результатов

```
Ключ: kUV
Исходный текст 1: hey
Зашифрованный текст 1: 0/
Текст 1, расшифрованный ключом: hey
Исходный текст 2: bye
Зашифрованный текст 2:  ,3
Текст 2, расшифрованный ключом: bye
Потенциальный ключ:

Текст 1, расшифрованный с помощью нового ключа: bye
Текст 2, расшифрованный с помощью нового ключа: hey
```

Вывод

В ходе выполнения лабораторной работы №8 я развил навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.