

Лабораторная работа № 8

Элементы криптографии. Шифрование (кодирование)
различных исходных текстов одним ключом

Сухарев Кирилл

Цель работы

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

Генерация ключа

```
import random
import string

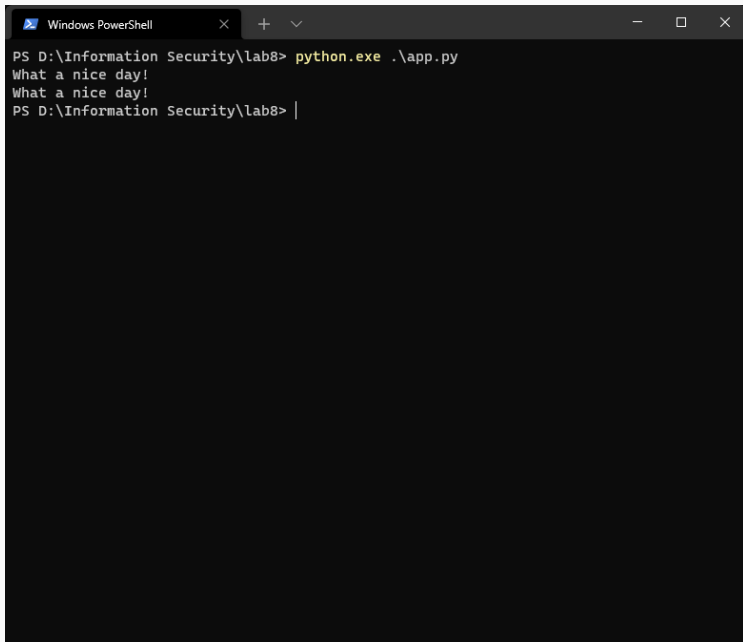
def generate_key(length):
    return ''.join(random.choice(string.ascii_letters + string.digits)
                    for _ in range(length))
```

Шифрование

```
def single_gamming(message, key):  
    return ''.join(chr(ord(m) ^ ord(k)) for m, k in zip(message, key))
```

Проверка работоспособности

Проверка работоспособности



```
Windows PowerShell
PS D:\Information Security\lab8> python.exe .\app.py
What a nice day!
What a nice day!
PS D:\Information Security\lab8> |
```

Листинг программы

```
import random
import string

def generate_key(length):
    return ''.join(random.choice(string.ascii_letters + string.digits) \
                    for _ in range(length))

def single_gamming(message, key):
    return ''.join(chr(ord(m) ^ ord(k)) for m, k in zip(message, key))
```

```
visible = "You are at home!"  
hidden = "What a nice day!"  
key = generate_key(25)  
encrypted1 = single_gamming(visible, key)  
encrypted2 = single_gamming(hidden, key)  
prediction = single_gamming(single_gamming(encrypted1, encrypted2  
print(hidden)  
print(prediction)
```