

Отчёт по лабораторной работе №8

Режим однократного гаммирования

Вакутайпа Милдред

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	9
	Список литературы	10

Список иллюстраций

2.1	Расшифрованные тексты	6
-----	---------------------------------	---

Список таблиц

1 Цель работы

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


```

import string
import random

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

def crypt(text, key):
    return ''.join(chr(ord(c) ^ ord(k)) for c, k in zip(text, key))

def find_keys(cipher, fragment):
    return [ ''.join(chr(ord(cipher[i+j])^ord(f)))
              for i in range(len(cipher)-len(fragment)+1)
              for j, f in enumerate(fragment)]

bland1 = 'НаВашисходящийот1204'
key1 = generate_key(bland1)
ciphered1 = crypt(bland1, key1)
decrypted1 = crypt(ciphered1, key1)

bland2 = 'ВСеверныйфилиалБанка'
ciphered2 = crypt(bland2, key1)
decrypted2 = crypt(ciphered2, key1)

print(f"orig:{bland1}, \nkey:{key1}, \nciphered:{ciphered1}")
print(f"orig:{bland2}, \nkey:{key1}, \nciphered:{ciphered2}")

unknown = crypt(ciphered1, ciphered2)

```

```
print(f"decrypt with unknown key: {crypt(bland1, unknown)}")  
print(f"decrypt with unknown key: {crypt(bland2, unknown)}")
```


3 Выводы

При выполнении данной работы я освоила на практике применение режим однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Список литературы