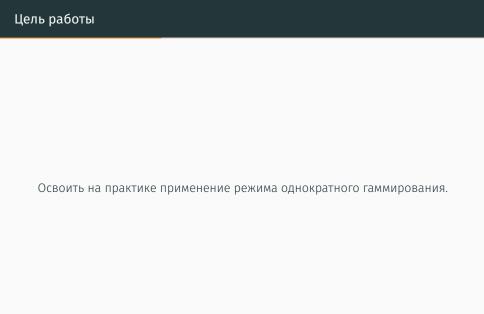
Элементы криптографии. Однократное гаммирование

Гебриал Ибрам 1

2021 Moscow, Russia

¹RUDN University, Moscow, Russian Federation

Цель работы



Результаты

1.Написал блок функции для расчетов. (рис. 1)

```
In [8]: import string import random

In [9]: imengeded & unconsultant unconsultant
```

Figure 1: Блок функции для расчетов

Определил вид шифротекста при известном ключе и известном открытом тексте. (рис. 2)

```
In [10]: message= 'C Homme Fodom, друзья!'

keyvgem key/len(message))

hex_key/menx(key)

print("Knewsayemak rune: ", key)

print("Knewsayemak rune: ", key)

print("Knewsayemak rune: ", key)

print("Snewsayemak rune: ", key)

print("Snewsayemak rune: ", key)

print("Saumehpodamanee coofugemue: ", hex_encrypt)

decryptt = encrypted([ord(i) for i in mersynt], [ord(i) for i in key])

print("Saumehpodamanee coofugemue: ", hex_encrypt)

Mcnomsayemak rune: AlTournetsTrotogliMixTx

Knews a mechangamanee coofugemue: ", decryptt)

Mcnomsayemak rune: AlTournetsTrotogliMixTx

Knews a mechangamanee coofugemue: ", decryptt )

Augustypodamanee coofugemue: ", decryptt )

Saumehpodamanee coofugemue: do 6 cs day 51 af 7 d34 d52 d5 d67 d64 d66 d74 d8a 58 67 445 d2c 47a 479 436 437 75

Pocumphypodamanee coofugemue: Tough rune; source s
```

Figure 2: Задание 1. Получение шифротекста

Определил ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. (рис. 3)

```
In [27]: compute_key = compute_key([ord(i) for i in message], [ord(i) for i in encrypt])

decrypt_compute_key= encrypted([ord(i) for i in encrypt], [ord(i) for i in key])
print("Исходный клем", key)
print("Вариант прочения ликрытого текста: ", decrypt_compute_key)

Исходный клем Fыйнопи_Uehvcp3rvaOcUuc
Вариант прочения ликрытого текста: С Новым Годом, друзья!
```

Figure 3: Один из вариантов прочения открытого текста:



Освоил на практике применение режима однократного гаммирования.

