Отчёт по лабораторной работе №3. Шифрование гаммированием

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Лапшенкова Любовь Олеговна 1032217633

Группа: НФИмд-02-21

Преподаватель: д-р.ф.-м.н., проф. Кулябов Дмитрий Сергеевич

27 ноября, 2021, Москва

Цели и задачи работы

Цель лабораторной работы

Целью данной лабораторной работы является ознакомление с шифрованием гаммированием, – а так же реализация шифра на произвольном языке программирования.

Задание

Реализовать алгоритм шифрования гаммированием конечной гаммой.

Ход выполнения и результаты

Реализация

Гаммирование Реализация

```
alphabet="АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"#задаем алфавит
alphabet_list=list(alphabet)#сделали алфавит списком
N=len(alphabet)#ввели размер алфавита
slovo="ПРИКАЗ"
key="ГАММА"
index_slovo=[]#ввели списки для индексов
index_key=[]#ввели списки для индексов
'''
Находим индексы в соответствии с алфавитом
'''
for i1 in slovo:
  index_slovo.append(alphabet.find(i1))
for i2 in key:
  index_key.append(alphabet.find(i2))
'''
Находим индексы в соответствии с алфавитом (+смещение на 1 (из-за питона))
'''
index_slovo_1=[]
index_key_1=[]
for j1 in range (0,len(index_slovo)):
  index_slovo_1.append(index_slovo[j1]+1)

for j2 in range (0,len(index_key)):
  index_key_1.append(index_key[j2]+1)
```

Figure 1: 1 часть программного кода реализации гаммирования конечной гаммой

Гаммирование. Реализация

```
'''
Нахождение индексов букв будущего шифра (первые k символов, где k-длина ключа)
'''
ciphered_text_indexes=[]#ввели список для индексов будущего шифра
for l in range(len(index_key_1)):
  ciphered_text_indexes.append(index_slovo_1[l]+(index_key_1[l])%N)
'''
Поиск новых индексов для шифра
'''
difference=len(index_slovo_1)-len(index_key_1)#ввели разницу в длине
index_key_2=0#ввели индекс символа ключа, с которого будем начинать
index_slovo_2=len(index_key_1)#ввели индекс символа слова, с которого будем начинать
while difference>0:
  ciphered_text_indexes.append(index_slovo_1[index_slovo_2]+(index_key_1[index_key_2])%N)
  difference=difference-1
  index_key_2+=1
  index_slovo_2=index_slovo_2-1
  if index_key_2==len(index_key_1):
    index_key_2=0
#ВНИМАНИЕ! ДЛЯ ТОГО, ЧТОБЫ СХОДИЛОСЬ С ОТВЕТОМ,
#ДАННЫМ В ЛАБОРАТОРНОЙ РАБОТЕ НЕОБХОДИМО ВЗЯТЬ АЛАВИТ БЕЗ БУКВЫ Ё (т.е. 32 символа)
'''
Поиск шифра с помощью полученных индексов и алфавита
'''
cipered_text=[]
for i in range(len(ciphered_text_indexes)):
  cipered_text.append(alphabet_list[ciphered_text_indexes[i]-1])#вспомнили что в питоне индексация с 1!
print(ciphered_text_indexes)
print('Криптограмма:"',"".join(cipered_text),'"')
```

Figure 2: 2 часть программного кода реализации гаммирования конечной гаммой

Гаммирование. Результаты

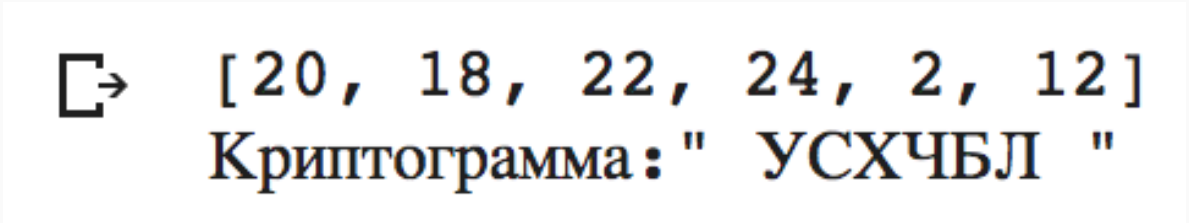

Figure 3: Результат шифрования сообщений с использованием гаммирования конечной гаммой

Спасибо за внимание