Отчёт по лабораторной работе №3

Шифрование гаммированием

Еленга Невлора Люглеш

Содержание

[1. Цель работы 1](#_Toc209472256)

[2. Задание 1](#_Toc209472257)

[3. Теоретическое введение 1](#_Toc209472258)

[4. Выполнение лабораторной работы 3](#_Toc209472259)

[5. Выводы 5](#_Toc209472260)

[Список литературы 5](#_Toc209472261)

# 1. Цель работы

Изучить и реализовать шифрование гаммированием.

# 2. Задание

Реализовать алгоритм шифрования гаммированием конечной гаммой.

# 3. Теоретическое введение

В Гаммирование – процедура наложения при помощи некоторой функции $F$ на

исходный текст гаммы шифра, т.е. псевдослучайной последовательности (ПСП) с

выходов генератора G. Псевдослучайная последовательность по своим

статистическим свойствам неотличима от случайной последовательности, но

является детерминированной, т.е. известен алгоритм ее формирования. Чаще

Обычно в качестве функции F берется операция поразрядного сложения по

модулю два или по модулю $N$ ($N$ – число букв алфавита открытого текста).

Простейший генератор псевдослучайной последовательности

представить рекуррентным соотношением:

$ Yi = a Yi-1+ b mod(m), i = 1, m,$

можно

где $у - 1$-й член последовательности псевдослучайных чисел, $а, Y, b$ - ключевые

параметры. Такая последовательность состоит из целых чисел от $0$ до т - $1$. Если

элементы $Vi$ и у совпадут, то совпадут и последующие участки: $1+11-/j+1,

Vi+2= 1j+2$. Таким образом, ПСП является периодической. Знание периода гаммы

Сарущественно облегчает криптоанализ. Максимальная длина периода равна т. Для ее достижения необходимо удовлетворить следующим условиям:

1. Вит - взаимно простые числа;

2. а - 1 делится на любой простой делитель числа т;

3. а - 1 кратно 4, если т кратно 4.

Стойкость шифров, основанных на процедуре гаммирования, зависит от

характеристик гаммы — длины и равномерности распределения вероятностей

появления знаков гаммы.

При использовании генератора ПСП получаем бесконечную гамму. Однако,

возможен режим шифрования конечной гаммы. В роли конечной гаммы может

выступать фраза. Как и ранее, используется алфавитный порядок букв, т.е. буква

«а» имеет порядковый номер 1, «б» - 2 и т.д.

Например, зашифруем слово «ПРИКАЗ» $(«16 17 09 11 01 08»)$ ше гаммой

«ГАММА» $(«04 01 13 13 01»)$. Будем использовать операцию побитового

сложения по модулю $33 (mod 33)$. Получаем:

$c₁ = 16+ 4(mod 33) = 20$

$c2 = 17 +1(mod 33) = 18$

$C3 = 9+13(mod 33) = 22$

$C4 = 11 + 13(mod 33) = 24$

$Cg = 1+1(mod 33) = 2$

$C6=8+4(mod 33) = 12.$

Криптограмма: «УСХЧБЛ» $(«20 18 22 24 02 12»).$.

# 4. Выполнение лабораторной работы

- Код

- функция получения алфавита:

import numpy as np

def alphavit(choice):

if choice == 'eng':

return list(map(chr,range(ord('a'), ord('z')+1)))

elif choice == 'rus':

return list(map(chr,range(ord('а'), ord('я')+1)))

else :

print('Выбирайте eng или rus')

- функция Шифрование гаммированием :

def encrypt\_gamma(sms:str, gamma: str):

alphav = alphavit('eng')

if sms.lower() not in alphav :

alphav = alphavit('rus')

print(alphav)

mes = len(alphav)

def encrypt(letters: tuple):

idx = (letters[0]+1)+(letters[1]+1)%mes

if idx > mes:

idx = idx - mes

return idx-1

sms\_clear = list(filter (lambda s : s.lower() in alphav, sms))

gamma\_clear = list(filter (lambda s : s.lower() in alphav, gamma))

sms\_ind = list(map(lambda s : alphav.index(s.lower()), sms\_clear))

gamma\_ind = list(map(lambda s : alphav.index(s.lower()), gamma\_clear))

for i in range(len(sms\_ind)-len(gamma\_ind)):

gamma\_ind.append(gamma\_ind[i])

print(f'{sms.upper()} -> {sms\_ind}\n{gamma.upper()} -> {gamma\_ind}')

encrypted\_ind = list(map(lambda s : encrypt(s), zip(sms\_ind, gamma\_ind)))

print(f'encrypted form : {encrypted\_ind}\n')

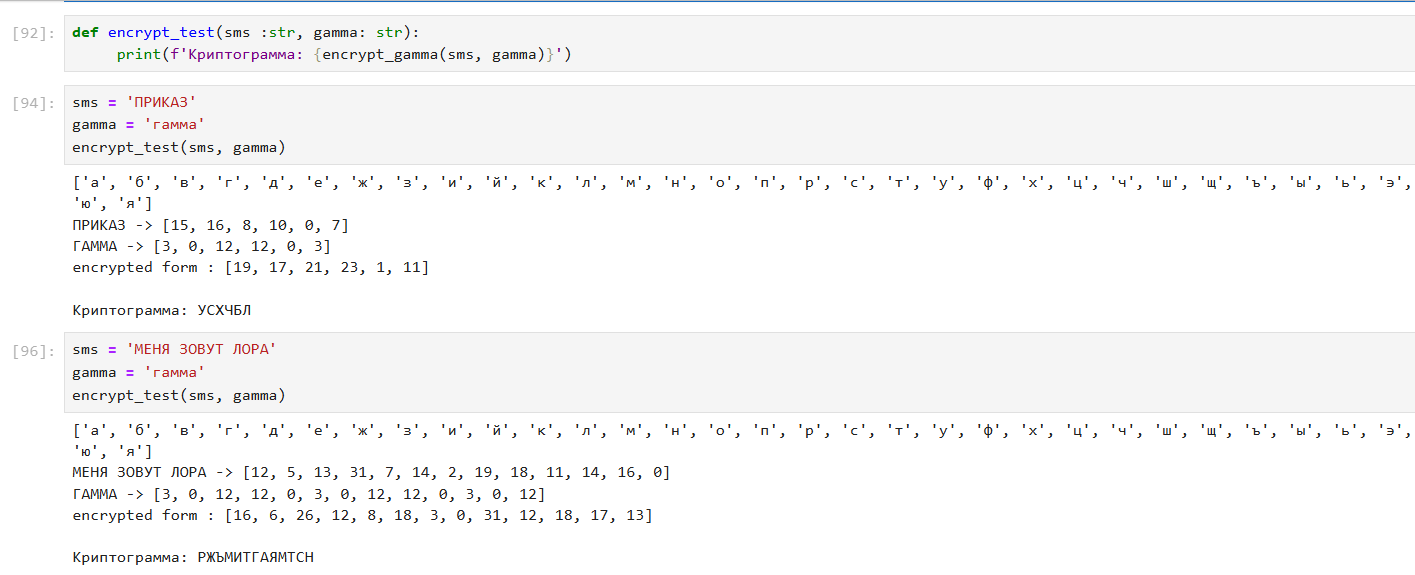
return ''.join(list(map(lambda s: alphav[s], encrypted\_ind))).upper()

- функция для тестирования :

def encrypt\_test(sms :str, gamma: str):

print(f'Криптограмма: {encrypt\_gamma(sms, gamma)}')

- Результаты:



# 5. Выводы

В ходе выполнения данной лабораторной работы изучили и реализовали шифрование гаммированием.

# Список литературы

::: {#Методические указания к лабораторной работе №3.}