**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**ОТЧЁТ**

**по лабораторной работе №1**

**«Простые шифры»**

*дисциплина: Математические основы защиты информации и информационной безопасности*

Вариант 3

Студент: Хиссен Али Уэддей

Группы: НПМмд-02-20

Ст/б: 10322009306

**МОСКВА**

**2021**

Оглавление

[Цель работы 3](#_Toc58934138)

[Ход работы 3](#_Toc58934139)

[История: 3](#_Toc58934140)

[a) Шифрование: 5](#_Toc58934141)

[b) Дешифрование: 6](#_Toc58934142)

[c) Применение 6](#_Toc58934143)

[Программная реализация: 7](#_Toc58934144)

[a) Псевдокод программы: 7](#_Toc58934145)

[b) Листинг программы: 8](#_Toc58934146)

[c) Результат выполнения программы: 9](#_Toc58934147)

[Вывод 9](#_Toc58934148)

[Ответы на контрольные вопросы 10](#_Toc58934149)

# Цель работы

Целью работы является ознакомление с простыми симметричными криптографическими шифрами на основе методов подстановок, перестановок и гаммирования.

Определила вариант с помощью формулы , где — номер студ.билета, N— количество заданий. Так как Sn=1032209306, а N=8, то номер варианта лабораторной работы 3.

# Ход работы

**Шифр Виженера (**метод шифрования буквенного текста с использованием ключевого слова) является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джованни-Баттиста Беллазо (Giovan Battista Bellaso) в книге La cifra del. Sig. Giovan Battista Bellasо в 1553 году, однако в 19 веке получил имя Блеза Виженера, швейцарского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

Хотя шифр легко понять и реализовать, на протяжении трех столетий он противостоял всем попыткам его сломать; чем и заработал название le chiffre indéchiffrable (с французского “неразгаданный шифр”). Многие люди пытались реализовать схеме шифрования, которые по сути являлись шифрами Виженера.

# История:

По сути дела, Виженер объединил подходы Тритемия, Беллазо, Порта к шифрованию открытых текстов, по существу, не внеся в них ничего оригинального. В наше время «шифр Виженера», состоящий в периодическом продолжении ключевого слова по таблице Тритемия, вытеснил имена его предшественников. Дэвид Кан в своей книге «Взломщики кодов» отозвался об этом осуждающе, написав, что история «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то что он ничего не сделал для его создания».

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон ([Льюис Кэрролл](https://ru.wikipedia.org/wiki/%D0%9B%D1%8C%D1%8E%D0%B8%D1%81_%D0%9A%D1%8D%D1%80%D1%80%D0%BE%D0%BB%D0%BB)) назвал шифр Виженера невзламываемым в своей статье «Алфавитный шифр» англ. The Alphabet Cipher, опубликованной в детском журнале в 1868 году. В 1917 году Scientific American также отозвался о шифре Виженера как о не поддающемся взлому. Это представление было опровергнуто после того, как Касиски полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.

Шифр Виженера достаточно прост для использования в полевых условиях, особенно если применяются шифровальные диски. Например, «конфедераты» использовали медный шифровальный диск для шифра Виженера в ходе Гражданской войны. Послания Конфедерации были далеки от секретных, и их противники регулярно взламывали сообщения. Во время войны командование Конфедерации полагалось на три ключевых словосочетания: «Manchester Bluff», «Complete Victory» и — так как война подходила к концу— «Come Retribution».

Гилберт Вернампопытался улучшить взломанный шифр (он получил название шифр Вернама-Виженера в 1918 году), но, несмотря на его усовершенствования, шифр так и остался уязвимым для криптоанализа. Однако работа Вернама в конечном итоге всё же привела к получению шифра Вернама, который действительно невозможно взломать.

# Шифрование:

Квадрат Виженера или таблица Виженера, может быть использована для заширования и расшифрования.

Изображение выглядит как стрела

Автоматически созданное описание

Рисунок 1: Квадрат Виженера.

В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например, в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифрования может использоваться таблица алфавитов, называемая квадрат Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На разных этапах кодировки шифр Виженера использует различные алфавиты из этой таблицы. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Например, предположим, что исходный текст имеет вид:

ATTACKATDAWN

Человек, посылающий сообщение, записывает ключевое слово("LEMON") циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE

Первый символ исходного текста A зашифрован последовательностью L, которая является первым символом ключа. Первый символ L шифрованного текста находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; т.е. второй символ шифрованного текста X получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

# Дешифрование:

Расшифрование производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если количество букв в алфавите, — буквы открытого текста, — буквы ключа, то шифрование Виженера можно записать следующим образом:

И расшифровывание:

# Применение

В XIX в. большое распространение получил так называемый метод блокнотного шифрования. Им пользовались революционеры-[народники](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B8%D0%BA%D0%B8), шпионы и т.п. Шифр использует фразы, взятые из языка, как ключ шифрования.

Например, фраза: **«14 июля — Mary’s birthday».** Если использовать принятую для примеров нумерацию букв английского алфавита, то **Marysbirthday** означает **12,0,17,24,18,1,8,17,19,7,3,0,24.** Для шифровки фразы **Iamgoing ↔ 8,0,12,6,14,8,13,6** производится сложение mod 26 текста с ключом, в роли которого выступает записанная фраза. Получается **20, 0, 3, 4, 6, 9, 21, 23 ↔ U A D E G J V X.**

Как видно, в данном случае это обыкновенное гаммирование. Французский криптограф Виженер предложил использовать ключ такого типа и в тех случаях, когда текст длиннее ключа, накладывая его столько раз, сколько нужно. При этом совсем необязательно, чтобы ключ получался из осмысленной фразы. Более того, это даже нежелательно, так как осмысленность может помочь взломщику шифра.

# Программная реализация:

Описанный шифр был реализован на языке программирования Python 3. Далее будут приведен псевдокод и код программ.

# Псевдокод программы:

**Шифрование:**

START: Задание функции шифрования текста, которая получает на вход текст и ключ.

INPUT: текст, ключ

READ: считаем длину ключа

CALCULATE: преобразовываем символ в ключе, в юникод (цифровое значение для каждого символа), тоже самое делаем для текста

SET: задаем пустое значение для зашифрованного текста

FOR количество символов в тексте

Вычисляем посимвольный сдвиг, задаваемый ключом

Записываем зашифрованный текст

ENDFOR

END: вывод зашифрованного текста

**Дешифрование:**

START: Задание функции дешифрования текста, которая получает на вход текст и ключ.

INPUT: текст, ключ

READ: считаем длину ключа

CALCULATE: преобразовываем символ в ключе, в юникод (цифровое значение для каждого символа), тоже самое делаем для текста

SET: задаем пустое значение для расшифрованного текста

FOR количество символов в тексте

Вычисляем посимвольный сдвиг, задаваемый ключом

Записываем расшифрованный текст

ENDFOR

END: вывод расшифрованного текста

# Листинг программы:

**Шифрование:**

def encrypt(plaintext, key):

key\_length = len(key)

key\_as\_int = [ord(i) for i in key]

plaintext\_int = [ord(i) for i in plaintext]

ciphertext = ''

for i in range(len(plaintext\_int)):

value = (plaintext\_int[i] + key\_as\_int[i % key\_length]) % 26

ciphertext += chr(value + 65)

return ciphertext

**Дешифрование:**

def decrypt(ciphertext, key):

key\_length = len(key)

key\_as\_int = [ord(i) for i in key]

ciphertext\_int = [ord(i) for i in ciphertext]

plaintext = ''

for i in range(len(ciphertext\_int)):

value = (ciphertext\_int[i] - key\_as\_int[i % key\_length]) % 26

plaintext += chr(value + 65)

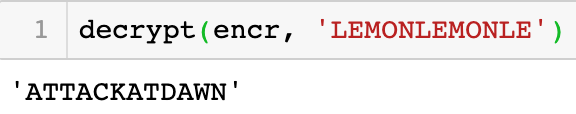
return plaintext

# Результат выполнения программы:

**Шифрование:**

****

**Дешифрование:**

****

# Вывод

В ходе выполнения лабораторной работы были изучены простые симметричные криптографические шифрамы на основе методов подстановок, перестановок и гаммирования. Также реализован алгоритм шифрования/дешифрования Шифр многоалфавитной замены (Вижинера).

# Ответы на контрольные вопросы

1. **Какой шифр называется шифром подстановки?**

Подстановочным шифром называется шифр, который каждый символ открытого текста в шифротексте заменяет другим символом. Получатель инвертирует подстановку шифротекста, восстанавливая открытый текст.

1. **Какой шифр называется шифром перестановки?**

Шифр, преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется шифром перестановки (ШП). Рассмотрим преобразование из ШП, предназначенное для шифрования сообщения длиной n символов.

1. **Какой шифр называется поворотной решёткой?**

Для использования шифра, называемого поворотной решёткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера 2𝑚 × 2𝑘 клеток. В трафарете вырезано 𝑚 × 𝑘 клеток так, что при наложении его на лист чистой бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа. Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

1. **Какой шифр называется шифром вертикальной перестановки?**

Шифром вертикальной перестановки (ШВП) называется широко распространенная разновидность шифра маршрутной перестановки. В нем используется прямоугольник, в котором сообщение вписывается обычным способом (по строкам слева направо). Выписываются буквы по вертикали, а столбцы при этом берутся в порядке, определяемом ключом.

1. **К какому классу шифров относится шифр Цезаря?**

Знаменитый шифр Цезаря, в котором каждый символ открытого текста заменяется символом, находящегося тремя символами правее по модулю 26 («A» заменяется на «D,» «B» — на «E», «W» — на «Z», «X» — на «A», «Y» — на «B», «Z» — на «C»), представляет собой простой подстановочный фильтр. Он действительно очень прост, так как алфавит шифротекста представляет собой смещённый, а не случайно распределённый алфавит открытого текста.

Таким образом, шифр Цезаря относится к классу подстановочных шифров.