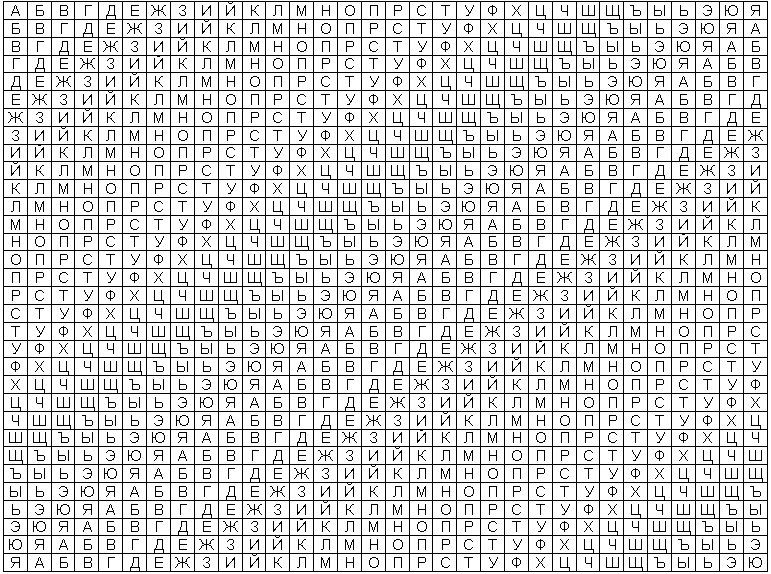
Шифр Тритемия

**1. Описание.**

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

**2. Алгоритм шифра.**

Таблица Тритемия для русского алфавита без буквы Ё:



Уравнение зашифрования для шифра Тритемия имеет следующий вид:

*,*

где L- номер зашифрованной буквы в алфавите;

m — номер позиции буквы шифруемого текста в алфавите;

k — шаг смещения (функциональная зависимость от позиции буквы в сообщении);

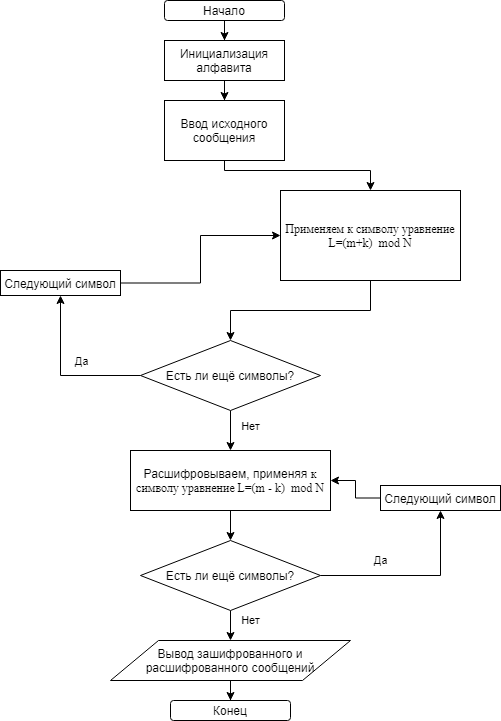
N — число букв алфавита.

**Работа программы:**

Инициализирован словарь с русским алфавитом без буквы Ё. На вход принимается исходное сообщение, преобразуемое в список. Программа в цикле проходит по списку, применяя к каждому символу уравнение L=(m+k) mod N (см. выше). Символу исходного сообщения сопоставляется его порядковый номер в исходном алфавите, прибавляется позиция этого символа в списке, находим остаток от деления на количество букв исходного алфавита. Получившееся число является порядковым номером буквы в алфавите, которую мы принимаем в качестве символа шифротекста.

**↓ БЛОК-СХЕМЫ НЕ ПОМЕЩАЮТСЯ ↓**

**3. Блок-схема.**



**4. Код программы.**

ef pause():  
 programPause = input("Нажмите <ENTER> для продолжения...")  
   
# Алфавит в нижнем регистре  
alph = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'  
# Алфавит в верхнем регистре  
alph2 = alph.upper()  
  
m1 = input('Введите открытый текст: ')  
m2 = ''  
k = 0  
for i in m1: #блок шифрования  
 if i.isupper():  
 # L = (m + k) mod N для больших букв  
 m2 += alph2[(alph2.find(i) + k) % len(alph2)]  
 elif i.islower():  
 # L = (m + k) mod N для маленьких букв  
 m2 += alph[(alph.find(i) + k) % len(alph)]  
 else:  
 m2 += i  
 k += 1  
  
print('Зашифрованный текст:', m2)  
  
m1 = ''  
k = 0  
  
for i in m2:#блок расшифрования  
 if i.isupper():  
 # L = (m - k) mod N для больших букв  
 m1 += alph2[(alph2.find(i) - k) % len(alph2)]  
 elif i.islower():  
 # L = (m - k) mod N для маленьких букв  
 m1 += alph[(alph.find(i) - k) % len(alph)]  
 else:  
 m1 += i  
 k += 1  
   
print('Расшифрованный текст:', m1)  
  
pause()

5. Тестирование.

Исходный текст на 1000 знаков (1053 без учета пробелов):

Вот пример статьи на тысячу символов. Это достаточно маленький текст, оптимально подходящий для карточек товаров в интернет магазинах или для небольших информационных публикаций. В таком тексте редко бывает более двух или трех абзацев и обычно один подзаголовок. Но можно и без него. На тысячу символов рекомендовано использовать один или два ключа и одну картину. Сколько примерно слов в тексте на тысячу символов? Статистика Ворд показывает, что тысяча знаков включает в себя сто пятьдесят или двести слов средней величины. Но, если злоупотреблять предлогами, союзами и другими частями речи на один или два символа, то количество слов неизменно возрастает. В копирайтерской деятельности принято считать тысячи с пробелами или без. Учет пробелов увеличивает объем текста примерно на сто или двести символов, ведь именно столько раз мы разделяем слова свободным пространством. Считать пробелы заказчики не любят, так как это пустое место. Однако некоторые фирмы и биржи видят справедливым ставить стоимость за тысячу символов с пробелами, считая последние важным элементом качественного восприятия. Согласитесь, читать слитный текст без единого пропуска, никто не будет. Но большинству нужна цена за тысячу знаков без пробелов.

Зашифрованный текст:

Впф ухоунщ ьюналш яу зсичрн некбомре. Гщц ощэяобюияб бцвэжцедж селух, фцъсцлчйыэ аачйгъцсбг аиэ кбтхтьлс ышнмэьс у ыбзызеюм иэбязйпгщ отр оцл ыфсяэпмэл ажоймйюхиппряъ цыкхуцндчщ. Х зцбже нбзпсе тиипф йдмлся рюьчш щшкн вжд рпец гемжэнл у ыпкзюа вщюд ииягэбнлпдсо. Фц цщтъь ш ушы гьыз. Йэ сытбъч чпфлшцъп яхыаящвъеъщзй епоомюктзжщд шпфъ чыщ чцх бгчсы е ндох оецщрцэ. Юшэыньб джядюкик пког е члсщып щн блвскз зядыижкя? Сувхмцшптй Нъэт яяьуыршчэл, упм тьувые охйфщо рщыпйущз щ кяьы псо свцбкмщиь фшц фучджэ игзь ннггнжл жкспясчж. Ыэ, чдяэ югзнккподбмбха хчннхщпнъч, гбтьцга в ансвинк ыечщзхт ьтеч ют вщюд бег бая ткпжусз, ьщ чьъшичджчд йдиэ кгззнзрсу йцрълэяофв. Х яджайъдоворкпл икещнфжшъюач авыбфие ксгоэры уэфгьо щ щыъоуърэъ ьаю щюб. Рхдт сутжлтцл юотщчзщфущз ещуяз пгйсув ухоунщчщ ъо бга ьаю ьыямое риндспуи, лппи цыхюяб жиегхдй нюж нэ фенлнфйрш яъюут ечдшжэзци нпотфудтчщкчц. Юечвсдп джещюец дюйаищлон фн хйнма, гтэ яцб цмй мсртпз ркчщц. Щръощю яшюгиеифя реолы к енцнр мурма бавуцъъваыхз орявйфя цшхрхшьюй цр доефнк квзюлйнв у ухфинфкчф, азщдуу еейдяяйег вбиряс дуоцрщяьы ыткщжищэжзйял ботсумдшпз. Ьърщпбщдшес, пбмыощ рлйфряо щнуыэ оуц ццыбгще икйлрпйа, рмпшх цп натфв. Ав чегхтгйорбу пцктж юочл фо вмгтли юещдйю ядз сутжлтцл.

Расшифрованный текст:

Вот пример статьи на тысячу символов. Это достаточно маленький текст, оптимально подходящий для карточек товаров в интернет магазинах или для небольших информационных публикаций. В таком тексте редко бывает более двух или трех абзацев и обычно один подзаголовок. Но можно и без него. На тысячу символов рекомендовано использовать один или два ключа и одну картину. Сколько примерно слов в тексте на тысячу символов? Статистика Ворд показывает, что тысяча знаков включает в себя сто пятьдесят или двести слов средней величины. Но, если злоупотреблять предлогами, союзами и другими частями речи на один или два символа, то количество слов неизменно возрастает. В копирайтерской деятельности принято считать тысячи с пробелами или без. Учет пробелов увеличивает объем текста примерно на сто или двести символов, ведь именно столько раз мы разделяем слова свободным пространством. Считать пробелы заказчики не любят, так как это пустое место. Однако некоторые фирмы и биржи видят справедливым ставить стоимость за тысячу символов с пробелами, считая последние важным элементом качественного восприятия. Согласитесь, читать слитный текст без единого пропуска, никто не будет. Но большинству нужна цена за тысячу знаков без пробелов.