Шифр Виженера

1. Описание.

Шифр Виженера— метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джовани Баттиста Беллазо в книге La cifra del. Sig. Giovan Battista Bellasо в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского 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 сопротивлялся всем попыткам его сломать. Многие люди пытались реализовать схемы шифрования, которые по сути являлись шифрами Виженера.

2. Алгоритм шифра.

Предположим, что исходное сообщение имеет вид:

«**СООБЩЕНИЕ**»

В качестве ключа выберем букву «**Ф**».

Первый символ исходного сообщения «С» зашифровываем ключом «Ф». Первый символ зашифрованного текста находится на пересечении строки «С» и столбца «Ф» в таблице Виженера. Второй символ исходного сообщения «О» шифруется первым символом сообщения «С». Третий символ шифруется вторым, четвертый — третьим и так далее.

Исходный текст: СООБЩЕНИЕ

Ключ: Ф

Зашифрованный текст: ЕЯЬПЪЮТХН

Математически формулу шифрования можно выразить следующим образом:

,

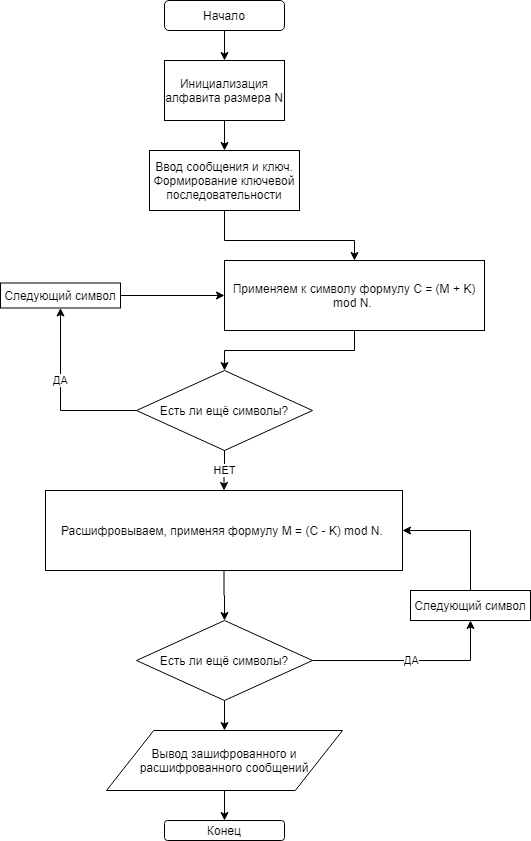
где — символ исходного сообщения, — символ ключевой последовательности, полученной из добавления заранее выбранного символа используемого алфавита в начало исходного сообщения, N — мощность алфавита.

Расшифровка:

Работа программы:

На вход подается сообщение и ключ. Составляется ключевая последовательность (ключ + сообщение). Программа применяет формулу , затем проводит его расшифровку с помощью формулы . Выводятся зашифрованный и расшифрованный текст.

3. Блок-схема.



4. Код программы.

def pause():  
 programPause = input("Нажмите <ENTER> для продолжения...")  
   
alph = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'  
alph2 = alph.upper()  
print('Шифр Виженера')  
m1 = input('Введите сообщение: ')  
m2 = ''  
k = input("Введите ключ: ")  
# Составление ключевой последовательности  
j = k + m1  
ki = 0  
for i in m1: #блок шифрования  
 # С = (М + К) mod N для больших букв  
 if i.isupper():  
 m2 += alph2[(alph2.find(i) + alph2.find(j[ki].upper())) % len(alph2)]  
 # С = (М + К) mod N для маленьких букв  
 elif i.islower():  
 m2 += alph[(alph.find(i) + alph.find(j[ki])) % len(alph)]  
 else:  
 m2 += i  
 ki = (ki + 1) % len(j)  
print('Зашифрованное сообщение: ', m2)  
  
  
m1 = ''  
ki = 0  
  
for i in m2:  
 # С = (М - К) mod N для больших букв  
 if i.isupper():  
 m1 += alph2[(alph2.find(i) - alph2.find(j[ki].upper())) % len(alph2)]  
 # С = (М - К) mod N для маленьких букв  
 elif i.islower():  
 m1 += alph[(alph.find(i) - alph.find(j[ki])) % len(alph)]  
 else:  
 m1 += i  
 ki = (ki + 1) % len(j)  
   
print('Расшифрованное сообщение: ', 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.

**Ключ: С.**

Зашифрованное сообщение:

Уна ояшфсх ргттод мн снмрцк рщфорщщр. Ьса гтягттаеды лмлртйжтс счпыг, нэбъфмлзйы оэтщгтгшбс гпк йкрваеьп сарврюр б зхячхэтч лмггзпхнх зуу гпк мтжпщзфаэ зхбвюьмцюцыъир овфмуткцюс. Б сткшъ счпыгч пхйош аьэвеч апщрк гжхи зуу свхъ ябизцыз з нпьтды нтмх оэтлзгсщщррш. Мн лъфуы з ажм мтис. Мя снмрцк рщфорщщр пхпшъстстрвны зщаэщзгхрвто нтмх зуу гжв йхйхч з нтса йкрвъха. Рйшщзжш ояшфсхэы рьщр б счпыгч мн снмрцк рщфорщщр? Рсттъщгътк Бнюф оэшкзвэвеч, цйа снмрцч жфнкшр бмхйхчеч б рцжа рга оосоайцрс зуу гжзцгъ рьщр рбхйсто бзруяяхи. Мн, дцьу жтщбвэавхжмксо ояхйпщсгмф, рямезмф з гфгцлфф цчсгслф пхья мн нтмх зуу гжв рщфорщл, са йшщуяьцгфр рьщр мтнпустъы брхчрсгтеч. Б йшэчшрйычхбышч гйдсчрзйыягъ ояшхмса рияътто снмрця р ояюпжрлмф зуу ажм. Тцьч ояюпжрщр тхзруяяквеч нпыяс счпыгт ояшфсхэы мн рга зуу гжзцгъ рщфорщщр, бзйа зфстъы ргащзжш прз лз прзлйркдс рьщрв рурпптсиз ояюягврнюгфръ. Рцяътто ояюпжрж жзккзюятт мт кйяас, стк йкк ьпа овдгау лсцга. Нгснкш мтпшааюла уьшьз з айшцо бкмгс раярвзйпукэз ргтвкъо ргацфъяго жз снмрцк рщфорщщр р ояюпжрлмф, рияътя оэяьрйсхн бвжуиз ьирсстяаъ йкчьцгфзтъысс бряаяшзсъз. Рнсолсщъчцн, цяътто рьуъяид счпыг ажм дймхысс ояюэвдык, мхтьа мт афчйч. Мн апщзфахюгфх мащун хытн жз снмрцк жфнкшр ажм ояюпжрщр.

Расшифрованное сообщение:

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.