Шифр Белазо

**1. Описание.**

В 1553 Джованни Баттиста Белазо предложил использовать для многоалфавитного шифра буквенный, легко запоминаемый ключ, который он назвал паролем. Паролем могло служить слово или фраза. Пароль периодически записывался над открытым текстом. Буква пароля, расположенная над буквой текста, указывала на алфавит таблицы, который использовался для зашифрования этой буквы. Например, это мог быть алфавит из таблицы Тритемия, первой буквой которого являлась буква пароля. Однако Белазо, как и Тритемий, использовал в качестве алфавитов шифра обычные алфавиты.

**2. Алгоритм шифра.**

Предположим, что исходное сообщение имеет следующий вид: «**ШИФРБЕЛАЗО**»

Человек, посылающий сообщение, записывает ключевое слово циклически до тех пор, пока его длина не будет соответствовать длине исходного текста: «**МЕХМЕХМЕХМ**»

Первый символ исходного текста «Ш» зашифрован последовательностью «М», которая является первым символом ключа. Первый символ зашифрованного текста находится на пересечении строки «Ш» и столбца «М» в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ зашифрованного текста получается на пересечении строки «И» и столбца «Е». Остальная часть исходного текста шифруется подобным способом.

Исходный текст: ШИФРБЕЛАЗО

Ключ: МЕХМЕХМЕХМ

Зашифрованный текст: ДНЙЬЖЪЧЕЬЪ

Расшифровывание 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.

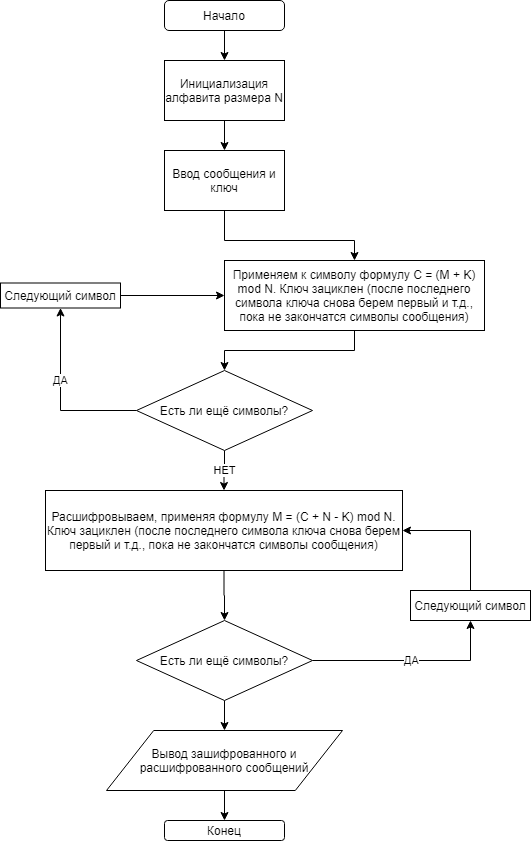
Если N{\displaystyle n}NNN — количество букв в алфавите,  — {\displaystyle m\_{j}} буквы открытого текста, {\displaystyle k\_{j}}— буквы ключа, то шифрование Белазо можно записать следующим образом:

Расшифрование:

Работа программы:

На вход подается исходное сообщение и ключ. Программа применяет к исходному сообщению формулу , «прокручивая» символы ключа от первого к последнему и заново, пока есть хоть один незашифрованный символ исходного сообщения. Пройдясь по всем символам сообщения, выводит на экран шифротекст. Расшифровка происходит аналогичным образом, к шифротексту применяется формула .

**3. Блок-схема.**



**4. Код программы.**

def pause():  
 programPause = input("Нажмите <ENTER> для продолжения...")  
   
alph = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'  
alph2 = alph.upper()  
print('Шифр Белазо')  
m1 = input('Введите сообщение: ')  
m2 = ''  
k = input("Введите ключ: ")  
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(k[ki].upper())) % len(alph2)]  
 # (С = М + К) mod N для больших букв  
 elif i.islower():  
 m2 += alph[(alph.find(i) + alph.find(k[ki])) % len(alph)]  
 else:  
 m2 += i  
 # Переход на следующий символ ключа. Модуль для того, чтобы зациклить над всем сообщением.   
 ki = (ki + 1) % len(k)  
print('Зашифрованное сообщение: ', m2)  
  
  
m1 = ''  
ki = 0  
# Блок расшифровки. Всё по аналогии с шифрованием  
for i in m2:  
 if i.isupper():  
 m1 += alph2[(alph2.find(i) - alph2.find(k[ki].upper())) % len(alph2)]  
 elif i.islower():  
 m1 += alph[(alph.find(i) - alph.find(k[ki])) % len(alph)]  
 else:  
 m1 += i  
 ki = (ki + 1) % len(k)  
   
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: сентябрь.**

Зашифрованное сообщение:

Ууя осшицх гсбвшщ ът улнрьа рйьюярыф. Ноя сарурояьъа нрзцтйьзк оцпюд, юлгнщткээк фыцфпфыкнц гмп ыеэдншхж чыфясюю з ъмухмюкя лбуьшнътф шзщ сэю эбтушочйе щтбапнртщуъяъц лджшъйбждъ. Ф уржяс ддлбоц эчглю таптду эяртч етпж хэз вмцъ таиртцз ъ псчиты нешй фыцжбукьупай. Йя щаеою щ очж эбфу. Мб омцмйт бдэзыэнг мцпыюдофкуеъа йблярйщнгрон ыцзо дьн цбб жьгдт й кхта йбаощта. Тъкьбча радэкэян бзяз ф ухжвчт мб омцмйт бдэзыэнг? Вчндзтвдые Фнсф аучтжьтьцч, цую гаюсцб гюечаб тжьгдтду ю цтую боя ьссэфбвдя змш хзтгсй ньуп рсхаюкц бжыдинън. Эк, тгкй гьуабнуабтрмды ямцйшавбьд, юаэирищ х гсгящсх цбборсх пжзд тн нешй ншъ еть цхюбпыь, яа люзщьтгсгю врыф охдшстямп юямэтрурбг. Ф люлщхнысжаныуц гжпоцрйянтвд фэъмавк цдъсбвш чигюшш в ьвнвхзссх змш ткф. Фзбг ьвнвхзяз ебжыдинптду ктятю ухжвчн осшицхъа ор вчы змш хзтгсй нщспакпт, зтцы шицтъа твкьбча срг си пбчацрмчл бзязн ргюэяйънл ямяцявяобоуущ. Тздгеяо ракткшн иржсмдъйй йц шраав, чнь лрж вяа ргнгут лжбоя. Агоржя ъчйпвкбат уйаим х айавщ пъгав вфэтбжфзщзию твьуняо твкщсыгсэ гс янразп цхюбпыку ю осюэцрнюз, нинятю яквртцмйх уеуяън щькщчмуюи пнйдтвюцтъавп юяцьвзавдр. Гндыьвнячрэ, инятсэ ньняяък оцпюд вхг ксъмпук фэаофбжс, язлвк тт аффбг. Ян скьбеъмтвюд ъееор зкът ир гаюсцф гюечаб сбш ьвнвхзяз.

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.