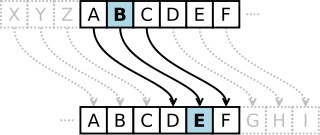
**Шифр Цезаря**



Шифр Цезаря со сдвигом на 3:  
**A** заменяется на **D**  
**B** заменяется на **E**  
и так далее  
**Z** заменяется на **C**

**Шифр Цезаря**, также известный как шифр **сдвига**, **код Цезаря** или **сдвиг Цезаря** — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и всё ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.

**Пример**

Шифрование с использованием ключа k =3. Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее. :

Исходный алфавит: А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Шифрованный: Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В

Оригинальный текст:

Съешь же ещё этих мягких французских булок, да выпей чаю.

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:

Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб.

Для шифровки и расшифровки удобно пользоваться двумя дисками разного диаметра на одной оси с нарисованными по краям дисков алфавитами. Шифр Цезаря легко взламывается: например, для этого можно использовать заранее заготовленные полоски с алфавитом.



**Взлом шифра**

Шифр Цезаря может быть легко взломан даже в случае, когда взломщик знает только зашифрованный текст. Можно рассмотреть две ситуации:

1. Взломщик знает (или предполагает), что использовался простой шифр подстановки, но не знает, что это — схема Цезаря.
2. Взломщик знает, что использовался шифр Цезаря, но не знает значение сдвига.

В первом случае шифр может быть взломан, используя те же самые методы что и для простого шифра подстановки, такие как частотный анализ и т. д. Используя эти методы, взломщик, вероятно, быстро заметит регулярность в решении и поймёт, что используемый шифр — это шифр Цезаря.

Одним из методов является *частотный анализ*. Распределение букв в криптотексте сравнивается с распределением букв в алфавите исходного сообщения. Буквы с наибольшей частотой в криптотексте заменяются на букву с наибольшей частотой из алфавита. Вероятность успешного вскрытия повышается с увеличением длины криптотекста. Существуют множество различных таблиц о распределении букв в том или ином языке, но ни одна из них не содержит окончательной информации - даже порядок букв может отличаться в различных таблицах. Распределение букв очень сильно зависит от типа теста: проза, разговорный язык, технический язык и т.п.

|  |  |
| --- | --- |
| Таблицы распределения букв | |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | В русском языке | | | | | | | Буква | Частота | Буква | Частота | Буква | Частота | | а | 0.062 | л | 0.035 | ц | 0.004 | | б | 0.014 | м | 0.026 | ч | 0.012 | | в | 0.038 | н | 0.053 | ш | 0.006 | | г | 0.013 | о | 0.090 | щ | 0.003 | | д | 0.025 | п | 0.023 | ы | 0.016 | | е | 0.072 | р | 0.040 | ъ, ь | 0.014 | | ж | 0.007 | с | 0.045 | э | 0.003 | | з | 0.016 | т | 0.053 | ю | 0.006 | | и | 0.062 | у | 0.021 | я | 0.018 | | й | 0.010 | ф | 0.002 | разделитель | 0.174 | | к | 0.028 | х | 0.009 |  |  | | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | В английском языке | | | | | | | Буква | Частота | Буква | Частота | Буква | Частота | | a | 0.0804 | b | 0.0154 | c | 0.0306 | | d | 0.0399 | e | 0.1251 | f | 0.0230 | | g | 0.0196 | h | 0.0549 | i | 0.0726 | | j | 0.0016 | k | 0.0067 | l | 0.0414 | | m | 0.0253 | n | 0.0709 | o | 0.0760 | | p | 0.0200 | q | 0.0011 | r | 0.0612 | | s | 0.0654 | t | 0.0925 | u | 0.0271 | | v | 0.0099 | w | 0.0192 | x | 0.0019 | | y | 0.0173 | z | 0.0009 |  |  | |

Хотя нет таблицы, которая может учесть все виды текстов, но есть вещи общие для всех таблиц, например, в английском языка буква E всегда возглавляет список частот, а T идет на второй позиции. A и O почти всегда третьи. Кроме того девять букв английского языка E, T, A, O, N, I, S, R, H всегда имеют частоту выше, чем любые другие. Эти девять букв заполняют примерно 70% английского текста. Ниже приведены соответствующие таблицы для различных языков.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Русский | | | Буква | Частота | | о | 0.1090 | | е | 0.0872 | | а | 0.0751 | | и | 0.0751 | | н | 0.0642 | | т | 0.0642 | | с | 0.0545 | | р | 0.0484 | | в | 0.0460 | | Всего | 0.6235 | | |  |  | | --- | --- | | Английский | | | Буква | Частота | | e | 0.1251 | | t | 0.0925 | | a | 0.0804 | | o | 0.0760 | | i | 0.0726 | | n | 0.0709 | | s | 0.0654 | | r | 0.0612 | | h | 0.0549 | | Всего | 0.6990 | | |  |  | | --- | --- | | Немецкий | | | Буква | Частота | | e | 0.1846 | | n | 0.1142 | | i | 0.0802 | | r | 0.0714 | | s | 0.0704 | | a | 0.0538 | | t | 0.0522 | | u | 0.0501 | | d | 0.0494 | | Всего | 0.7263 | | |  |  | | --- | --- | | Французский | | | Буква | Частота | | e | 0.1587 | | a | 0.0942 | | i | 0.0841 | | s | 0.0790 | | t | 0.0726 | | n | 0.0715 | | r | 0.0646 | | u | 0.0624 | | l | 0.0534 | | Всего | 0.7405 | | |  |  | | --- | --- | | Итальянский | | | Буква | Частота | | e | 0.1179 | | a | 0.1174 | | i | 0.1128 | | o | 0.0983 | | n | 0.0688 | | l | 0.0651 | | r | 0.0637 | | t | 0.0562 | | s | 0.0498 | | Всего | 0.7500 | | |  |  | | --- | --- | | Финский | | | Буква | Частота | | a | 0.1206 | | i | 0.1059 | | t | 0.0976 | | n | 0.0864 | | e | 0.0811 | | s | 0.0783 | | l | 0.0586 | | o | 0.0554 | | k | 0.0520 | | Всего | 0.7359 | |

Заметим, что буквы I, N, S, E, A (И, Н, С, Е, А) появляются в высокочастотном классе каждого языка! Также есть таблицы частоты появления букв в начале и конце слова.

**ЗАДАНИЕ 1.**

Дан текст на английском алфавите, ключ (целое число) (ввод текста, ключа из консоли).

Зашифровать текст шифром Цезаря с данным ключом.

**ЗАДАНИЕ 2.**

**Постановка задачи**

Попытайтесь расшифровать фразы.

1. Г хсуяъж бав бвъ улцщхц у хцвцуяп гдарэ гдаэт г бвътъдаы ь яцюе хагьаы: «Хцв. Юаващауьс». Ъ уад ахясшхм гъэнямы уцдцв баусэъэ гдаэт, ъ хагьс всгьаэаэсгн.

2. У чыущдысж бучфд Ъцнльщчауи лчычксфиъе чанце чъцчкиынфецч. Кдхдфи к уфиъън шчфд с чуци, шчкнъсфи цчкдн бычщд, щиъъыиксфи к буиэию уцслс с ьанйцдн шчъчйсз.

3. Мпьж мпвпы шкхкшюшп люоюдкй ювуэпцжшубк ьщьэкмцйцк ыкьъуькшуп юыщхщм, ткъщцшйцк хцкььшёф сюышкц, шкоъуьёмкцк эпэыкоу… Ок экх у юьшюцк шк хуъп эпэыкощх.

4. Стыуш писнщям мяыич. Яытр цяшюцщям ын яьщыдт. Ц яьщытеыит хнчецшц эюирнщц аба ц анъ, ытшьаьюит снфт эюманщцяй п ншшбюнаыь юняеуяныыьч оьюьст Стсн Ъьюьхн.

5. Фбыш яюбьювафвл эп ъпавг, вю ьюцэю гсшуфвл эп эфщ уфбовъш, п ьюцфв рквл, ш бювэш апчэке Ьюаючюсюъ. Сюв ш аюуюспо уфафсэо Уфуп Ьюаючп б эфчпяпьовэке сафьхэ эпчкспыпбл Ьюаючюсъющ.

Частоты можно взять из файла «Частоты.txt».

Пример кода для чтения данных из файла в массив.

fso = new ActiveXObject ("Scripting.FileSystemObject");

fh = fso.OpenTextFile("d:\\11.txt");

i=0

arr=new Array()

while (!fh.AtEndOfStream){

s = fh.Readline();

arr[i] = s.split(' ');

i++;

}

fh.Close();

Пояснения.

Известны частоты букв pi, i=1,2,…,n в языке сообщения (n – число букв в алфавите). Определяем частоты букв fi в зашифрованном сообщении. Затем необходимо делать перебор по сдвигам (разным ключам). Минимум величины говорит о том, что сдвиг N наиболее вероятный ключ к расшифровке текста, зашифрованного кодом Цезаря.

Указание к программе.

Строку, которую будете расшифровывать преобразуйте, чтобы были одни маленькие буквы.

Введите строку русский алфавит alphrus=’абвгдеёжзийклмнопрстуфхцчшщъыьэюя’

Создайте массив, где будете хранить частоты из файла «Частоты.txt», типа chast[alphrus.charAt(i)]=….

Создайте массив, где будете хранить частоту букв из введенной строки, типа strch[alphrus.charAt(i)]=….

Дальше пробегаем по всем значениям сдвига, ищем минимум величины .

Т.е.

Min=

Сдвиг\_min=0

Сдвиг\_i от 1 до 32

Начало цикла

D=

Если Min>D

Начало\_если

Min=D

Сдвиг\_min= Сдвиг\_i

Конец\_если

Конец цикла

// Составляем расшифрованную строку.

Str\_nov=’’

J от 0 до длины\_строки-1 // Пробегаем по зашифрованной строке

Начало цикла

Если символ\_J принадлежит строке alphrus

Начало\_если

Символ\_замены= alphrus.charAt((Место\_ символ\_J\_в\_alphrus + Сдвиг\_min)%33)

Str\_nov= Str\_nov+ Символ\_замены

Конец\_если

Иначе

Str\_nov= Str\_nov+ символ\_J

Конец цикла