

Информатика

Златопольский Дмитрий Михайлович
*Кандидат технических наук, доцент,
 доцент кафедры информатики и прикладной математики
 Московского городского педагогического университета;
 организатор и директор Музея истории
 вычислительной техники*



Шифруем текст, разработав программу

В статье описывается методика шифрования текста тремя простейшими методами с помощью программы. Материалы статьи могут быть использованы при изучении темы «Информационная безопасность» или во внеурочной деятельности.

1. Шифр «атбаш»

«Атбаш» – один из самых древних методов шифрования. Шифрование заключается в замене каждой буквы исходного текста на «симметричную» ей букву алфавита, то есть первая алфавита заменялась на последнюю и наоборот, вторая буква – на предпоследнюю и наоборот и т. д. Шифр был, скорее всего, изобретен ессеями, иудейской сектой повстанцев. Они разработали множество различных кодов и шифров, которые использовались для сокрытия важных имен и названий, чтобы потом избежать преследования.

Можно так сформулировать схему алгоритма шифрования данным и двумя другими методами:

1. Ввод исходных данных

2. цикл для каждой буквы исходного текста

- 2.1. Определяется её порядковый номер в алфавите (*ном*)
- 2.2. Определяется номер в алфавите заменяющей её буквы (*ном_зам*)
- 2.3. Данная буква исходного текста заменяется на букву с найденным номером

конец цикла

3. Вывод ответа (зашифрованного сообщения)

Как, зная номер буквы *ном*, определить номер буквы *ном_зам* при шифровании методом «атбаш»? Для ответа составим таблицу:

Номер буквы в алфавите, <i>ном</i>	Номер заменяющей её буквы, <i>ном_зам</i>
1	33
2	32
...	...
32	2
33	1

Из неё следует, что

$$\text{ном_зам} = 33 - \text{ном} + 1$$

или

$$\text{ном_зам} = 34 - \text{ном}$$

Прежде чем представлять соответствующую программу (на школьном алгоритмическом языке), напомним, что к отдельному символу величина строкового типа можно обратиться следующим образом:

имя величины[*порядковый_номер_символа*]

Программа:

алг Шифрование_текста_методом_атбаш

нач лит текст, алфавит, **цел** к, ном, ном_зам

алфавит := "абвгдеёжзийклмнопрстуфхцчщъыьэя"

вывод нс, "Введите текст для шифрования"

ввод текст

нц для к **от** 1 **до** длин(текст) | Для каждой буквы заданного текста

| Определяем её порядковый номер в алфавите

ном := поз(текст[к], алфавит)

| Рассчитываем номер заменяющей буквы

ном_зам := 33 - ном + 1

| Заменяем к-ю букву

текст[к] := алфавит[ном_зам]

кц

вывод нс, "Зашифрованный текст", текст

кон

где:

длин – функция, возвращающая общее количество символов в строке;

поз – функция, возвращающая позицию (порядковый номер символа или подстроки символов в строке). В языке программирования Паскаль имя аналогичной функции Паскаль – Pos, в языке Python – find (она вызывается как метод).

Из программы видно также, что в ней используется переменная строкового типа *алфавит*, смысл которой ясен из её имени.

Можно переменную *ном_зам* не использовать, а букву, заменяющую к-ю, определять так:

текст[к] := алфавит[33 - ном + 1]

В программе решения задачи на языке Python возникает проблема, связанная с тем, что в этом языке величины строкового типа являются так называемым «неизменяемым объектом», то есть в них нельзя заменять отдельные символы. Решение такое: использовать переменную *text2* (зашифрованное сообщение), принять её начальное значение, равное «пустому» символу, а затем определить каждую букву, заменяющую буквы заданного текста, и «приклеивать» её к текущему значению переменной *text2*.

Задания для самостоятельной работы учащихся

1. Разработайте программы (на языке программирования, который изучаете) для шифрования текста методом «атбаш» и зашифруйте с её помощью текст:

ПОТЕНЦИАЛОЧЕНЬХОРОШИЙЖУРНАЛ

2. Опишите алгоритм расшифровки текста, зашифрованного методом «атбаш».

Шифр Цезаря

Метод шифрования носит имя римского императора Юлия Цезаря (I век до н. э.), который если и не сам изобрел его, то активно им пользовался. Этот метод основан на замене каждой буквы шифруемого текста на другую путем смещения в алфавите от исходной буквы на фиксированное количество символов, причем алфавит читается по кругу, т. е. после буквы *я* рассматривается *а*. Регистр символов не учитывается. Так, например, слово *БАЙТ* при смещении на два символа вправо кодируется словом *ГВЛФ*.

Как, выполняя этап 2.2 «тела» цикла, приведенного в схеме алгоритма шифрования (см. выше), и зная номер буквы *ном*, определить номер буквы *ном_зам* в данном случае? Ответ: следует учесть величину сдвига букв¹. Но можем ли мы сказать, что $ном_зам = ном + сдвиг$? – Нет, не можем, поскольку сумма $ном + сдвиг$ может быть больше 33.

Учитывая, что после буквы *я* рассматривается буква *а* и т.д., можем записать, что:

если $ном + сдвиг \leq 33$

то

$ном_зам = ном + сдвиг$

иначе

$ном_зам = ном + сдвиг - 33$

все

Соответствующая программа:

алг Шифрование_текста_методом_Цезаря

нач лит текст, алфавит, **цел** к, ном, ключ, ном_зам
алфавит := "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"

¹ Примем, что сдвиг происходит вправо.

```

Вывод нс, "Введите текст для шифрования"
Ввод текст
Вывод нс, "Введите ключ шифрования (величину сдвига букв)"
Ввод ключ
нц для к от 1 до длин(текст) | Для каждой буквы заданного
текста
    | Определяем её порядковый номер в алфавите
    ном := поз(текст[к], алфавит)
    | Рассчитываем номер заменяющей буквы
    если ном + ключ <= 33
        то
            ном_зам := ном + ключ
        иначе
            ном_зам := ном + ключ - 33
    все
    | Заменяем к-ю букву
    текст[к] := алфавит[ном_зам]
кц
Вывод нс, "Зашифрованный текст", текст
кон

```

Оказывается, можно не использовать полный условный оператор (команду **если**). Составим таблицу, в которой запишем значения суммы **ном** + **сдвиг**, большие 33:

Сумма <i>ном</i> + <i>сдвиг</i>	2	3	4	...	31	32	33	34	35	...	65	66
Номер <i>ном_зам</i>	2	3	4	...	31	32	33	1	2	...	32	33

Из неё следует, что

$ном_зам = ...$

Выражение в правой части для расчета определите самостоятельно².

Подсказка: используйте операцию определения остатка от деления одного целого числа на другое.

Задания для самостоятельной работы

1. Разработайте программу (на языке программирования, который изучаете) для шифрования методом Цезаря заданного текста при заданной величине ключа. Зашифруйте с её помощью текст:

ПОТЕНЦИАЛОЧЕНЬХОРОШИЙЖУРНАЛ

при ключе, равном 18.

2. Разработайте программу для расшифровки текста, зашифрованного методом Цезаря при известной величине ключа шифрования. При этом учтите, что при расшифровке возможен «выход» за начало алфавита.

² Указание адресовано учащимся.

Шифр Виженера

Сразу же скажем, что французский дипломат, криптограф и алхимик, живший в XVI веке, Блез Виженер, не является автором рассмотренного далее метода шифрования текста. Авторство было ошибочно приписано ему в XIX веке, хотя метод впервые описал Джовани Баттиста Белласо (Giovanni Battista Bellaso) в книге «La cifra del» в 1553 году.

Особенность шифрования методом Виженера (шифром Виженера) заключается в том, что каждая буква «сдвигается» не на одно и то же количество позиций, как в шифре Цезаря. Таких сдвигов – несколько. Размер этих сдвигов определяется некоторым ключом шифрования – словом. Например, пусть – ключевое слово *яблоко*. Его буквы в алфавите имеют порядковые номера, соответственно, 33, 2, 13, 16, 12 и 16. Так вот, первая буква исходного текста шифруется со сдвигом 33, вторая – 2, ..., шестая – 16, седьмая – опять 33 и т. д.

Особенности программы для шифрования методом Виженера: при определении номера буквы *ном_зам*, заменяющей ту или иную букву исходного текста (этап 2.2 «тела» цикла, приведенного в схеме алгоритма шифрования), надо прибавлять не одно и то же значение сдвига, как в шифре Цезаря, а разные. Какие именно? – Это значение зависит от того, какая буква ключевого слова «соответствует» той или иной букве исходного текста.

Рассмотрим пример:

Буквы исходного текста	В	С	Т	Р	Е	Ч	А	О	Т	М	Е
Номера букв исходного текста	1	2	3	4	5	6	7	8	9	10	11
Буквы ключа шифрования	В	И	Р	У	С	В	И	Р	У	С	В

Составим таблицу, в которой запишем номера букв исходного текста, для шифрования которых используется так или иначе буква ключевого слова:

Буква ключа	Номер буквы в ключе	Номер буквы исходного текста
В	1	1, 6, 11, ...
И	2	2, 7, 12, ...
Р	3	3, 8, 13, ...
У	4	4, 9, 14, ...
С	5	5, 10, 15,

Из нее можно установить, что

если остаток от деления номера буквы исходного текста
на 5 (длину ключа) больше нуля

то

используется буква ключа с номером, равным остатку

иначе | остаток равен нулю

используется буква ключа с номером 5 (длина ключа)

все

В программе понадобятся две дополнительные (по сравнению с программой шифрования методом Цезаря) переменные:

- 1) *буква_ключа* – отдельная буква ключевого слова;
- 2) *ном_буквы_ключа* – её порядковый номер в алфавите.

Соответствующая программа:

```
алг Шифрование_текста_методом_Виженера
нач лит текст, ключ, алфавит, сим буква_ключа
    цел к, ном, ном_буквы_ключа, ном_зам
    алфавит := "абвгдеёжзийклмнопрстуфхцчшщъзьёя"
    вывод нс, "Введите текст для шифрования"
    ввод текст
    вывод нс, "Введите слово - ключ шифрования"
    ввод ключ
    нц для к от 1 до длин(текст) | Для каждой буквы заданного
текста
        | Определяем её порядковый номер в алфавите
        ном := поз(текст[к], алфавит)
        | Определяем букву ключа, шифрующую данную к-ю
        если mod(к, длин(ключ)) > 0
            то
                буква_ключа :=  $\boxed{\dots}^3$ 
            иначе
                буква_ключа :=  $\boxed{\dots}$ 
        все
        | Определяем номер этой буквы в алфавите
        ном_буквы_ключа :=  $\boxed{\dots}$ 
        | Рассчитываем номер заменяющей буквы
        если ном + ном_буквы_ключа  $\boxed{\dots}$ 
             $\boxed{\dots}$ 
        все
        | Заменяем к-ю букву
        текст[к] := алфавит[ном_зам]
    кц
    вывод нс, "Зашифрованный текст", текст
```

³ Здесь и далее текст программы вместо многоточия в рамке учащиеся должны ввести самостоятельно.

Задания для самостоятельной работы

1. Разработайте программу (на языке программирования, который изучаете) для шифрования методом Виженера заданного текста при заданной величине ключа. Зашифруйте с её помощью текст:

ПОТЕНЦИАЛОЧЕНЬХОРОШИЙЖУРНАЛ

при ключевом слове, совпадающим с вашим именем.

2. Разработайте программу для расшифровки текста, зашифрованного методом Виженера при известном ключе шифрования. При этом учтите, что при расшифровке возможен «выход» за начало алфавита.

Дополнение

Оказывается, задачи шифрования описанными методами можно решить, не выписывая в программах весь алфавит, а используя коды букв. Дело в том, что в памяти компьютера каждый символ хранится в виде двоичного числа – его кода. Как правило, в современных системах программирования десятичные эквиваленты кодов букв идут подряд (приведены условные значения кодов):

Буква	А	Б	В	...	Ю	Я
Код	192	193	194		222	223

При шифровании методом «атбаш» с использованием кодов можно учесть тот факт, что, например, буква Г «отстоит» от буквы А на таком же «расстоянии», на каком шифрующая её буква Б «отстоит» от буквы Я. Это позволяет использовать коды «симметричных» букв, то есть буква, шифрующая *к*-ю букву, может быть определена как символ, код которого равен:

$\text{код}("Я") - (\text{код}(\text{текст}[к]) - \text{код}("А"))$

Напомним, что в языке программирования Паскаль код символа возвращает функция `ord`, а символ с заданным кодом – функция `chr`. Аналогичные по назначению функции с такими же именами предусмотрены и в языке программирования Python.

В программах шифрования текстов методами Цезаря и Виженера при определении кода буквы, шифрующей *к*-ю букву исходного текста, следует учесть возможный «переход за букву я»:

```
если код(текст[к]) + ключ <= код("я")
то | Используем сумму
    код_шифр_буквы := код(текст[к]) + ключ
иначе | Переход за букву я
    величина_перехода := (код(текст[к]) + ключ) - код("я")
    код_шифр_буквы := код("а") + величина_перехода - 1
все
```

Внимание! При использовании для шифрования кодов букв следует учесть, что в таблице кодировки русских букв нет буквы Ё.