

Владимир Утенков



6 класс

**Шифрование и расшифровывание
текстов с помощью компьютера**

учебный материал ко Всероссийскому уроку информатики

«Час кода 1017»



Шифрование методом сдвига

Если пронумеровать все буквы алфавита, а затем заменить каждую букву сообщения буквой, расположенной на три буквы вправо в нумерованном алфавите (например: А → Г; Ф → Ч), сообщение будет зашифровано. Для букв Э, Ю, Я сдвиг будет с начала таблицы (Э → А; Ю → Б; Я → В).

А	Б	В	Г	Д	Е	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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Пример шифрования: **ИНФОРМАТИКА** → **ЛРЧСУПГХЛНГ**

Расшифровывание производится путем обратного сдвига: на три буквы влево.

Пример расшифровывания: **ЫНСОГ** → **ШКОЛА**

Очевидно, что такой шифр легко разгадать, даже если производить сдвиг не на 3, а на другое число, количество вариантов всего 32. Компьютерная программа легко с этим справится, перебрав все 32 варианта. Ниже показаны программы для шифрования и расшифровывания текста.

```
C:\WINDOWS\system32\cmd.exe
Шифрование текста методом сдвига
Разработал: В. Утенков, Егорьевск, 2016 г.

Введите текст: Истас Шефу - за нами следит Айсан.
Введите величину сдвига 5
Гцццц Экшн - не теси цркийн Еоцсет.
Продолжить? Y/N _
```

Зашифровать

```
C:\WINDOWS\system32\cmd.exe
Расшифровывание текста методом сдвига
Разработал: В. Утенков, Егорьевск, 2016 г.

Введите шифротекст: Гунват сетиг оовло ввуц
Фцзсг вццщ цуц цуцц
Хвонд гцдх дзфоза фещ
Цсхце днечд бсхжб хжжц
Чзщфж ещцц вщцв цщз
Шсчхз жьзэш ггччаг ччим
Швщц зьнщ дшсбд шилц
Ыггвц ицв евшце шкз
Мдвшк йзкан жьььж ььло
Льмьцл кьлел зьмьдз мьн
Энжцн лмьз иццн цна
Юззьн нанго ийзэж эзоб
лмьл нбод кькьк вьлв
Ариэп овпеа ллил рг
Бскавр пгрже нмаин аасд
Вглес рдсзв ннбкн бете
Гунват сетиг оовло ввуц
Продолжить? Y/N
```

Расшифровать



Шифрование методом ключа

Более надежным считается метод ключа. Его смысл в следующем: берется произвольное слово (оно называется ключ), номера его букв будут использованы для сдвига шифруемого текста.

А	Б	В	Г	Д	Е	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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Пример: ключ: **ШКОЛА**, номера его букв: 25; 11; 15; 12; 1.

Зашифруем слово **ИНФОРМАТИКА** с помощью этого ключа:

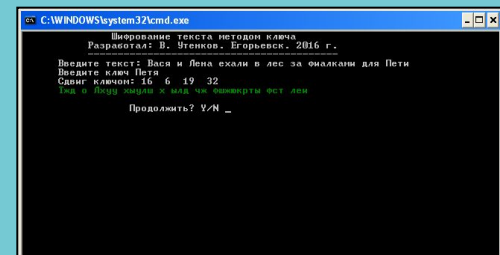
Букву И надо заменить буквой, сдвинутой по алфавиту на 25 букв, то есть буквой А, букву Н надо заменить буквой, сдвинутой по алфавиту на 11 букв, то есть буквой Ш и т. д. В результате получим: **АШГЬСЕЛБФЛЦ**.

Чтобы расшифровать такой текст, не зная ключа, надо перебрать все возможные сочетания букв в ключе. Например, в ключе **ШКОЛА** 5 букв, значит количество вариантов от **ААААА** до **ЯЯЯЯЯ** равно: $32^5 = 33\,554\,432$ – больше 33 миллионов! А если взять в качестве ключа более длинное слово (например **ЕГОРЬЕВСК** (9 букв) количество вариантов станет намного больше.

Программа
для расчета
вариантов
ключа

Введите ключ	Перетокино		
Количество букв	10	Вариантов	1.1259E+15

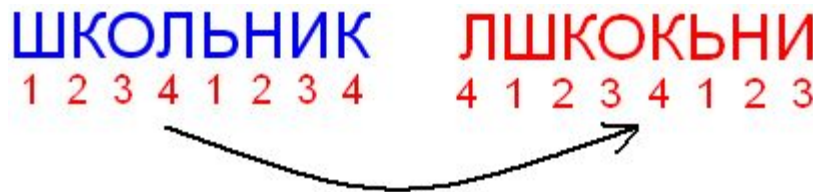
Зашифровать





Шифрованием перестановкой

Имеется еще один способ шифрования текстов. Принцип его следующий: текст разбивается на одинаковые отрезки и все символы в нем переставляются по определенному закону. Пример: В слове **ШКОЛЬНИК** 8 букв, разобьем его на две части по 4 буквы и переставим их по следующему правилу: 1; 2; 3; 4 → 4; 1; 2; 3. Мы получим текст: **ЛШКОКЪНИ**.



Ключом при этом способе будет последовательность номеров переставляемых букв. Количество ключей k определяется по формуле:

$$k = n!$$

где $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$. Для $n=4$: $n! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$. если отбросить тождественную перестановку 1; 2; 3; 4 получим 23 ключа. При длине ключа 10: $n! = 3\,628\,800$ (более трех миллионов ключей!).

Программа
шифрования
перестановкой

```
C:\WINDOWS\system32\cmd.exe
Шифрование текста методом перестановки
Разработал: В. Утенков. Егорьевск. 2016 г.

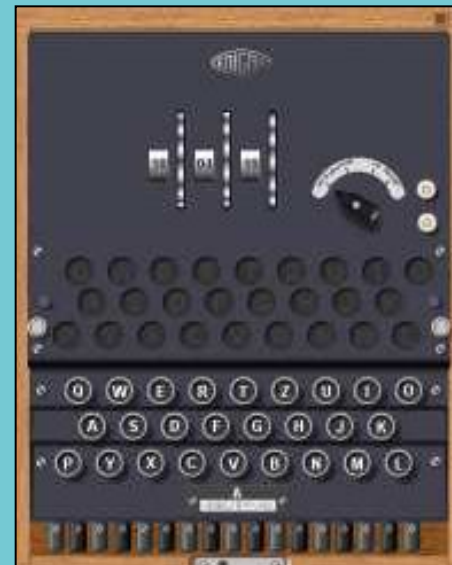
Введите длину ключа (число 2..10): 10
Количество возможных ключей: 3628800
Случайно выбрано ключ:
1 8421673519
2 1223761805
3 9366148172
4 3613112758
5 2594936118
6 8174329651
7 6812491132
8 9142638119
9 1317865249
10 1465232189
11 6913827415
12 1715834932
13 8461173592
14 1174236958
15 4719268153

Введите номер ключа: 5
Введите текст: Бвсд ефгх
```



Шифровальная машина Энигма

Во время Второй Мировой войны в немецких вооруженных силах применялась электромеханическая шифровальная машина «Энигма». Основой машины являются три соединенных проводами узла: клавиатура для ввода каждой буквы открытого текста, шифратор, который зашифровывает каждую букву открытого текста в соответствующую букву шифртекста, и индикаторное табло, состоящее из различных ламп для высвечивания букв шифртекста. Чтобы зашифровать букву открытого текста, оператор нажимает на клавиатуре клавишу с нужной буквой открытого текста, которая посылает электрический импульс через центральный шифратор на противоположную сторону, где на панели с лампочками высвечивается соответствующая буква шифртекста. Для любителей истории Второй Мировой войны в Интернете имеется компьютерная симуляция Энигмы. Она позволяет почувствовать себя немецким военным шифровальщиком на полях Второй Мировой войны.



Компьютерный
симулятор
Энигмы