# Шифрование с помощью операции «исключающее или»

Филатов Алексей Александрович,
учитель информатики и ИКТ
МАОУ «Лицей 44 » г. Липецка

# Свойства операции «исключающее или» (**XOR, ⊕**)

| A | B | A⊕B |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

**A ⊕B ⊕B=A**

# Задача

Зашифровать сообщение «A-b=c».

Маска: 27

**Используем 8-битную кодировку ASCII**

1. Переведем маску в двоичный вид:

$27_{10}=000\mathbf{11011}_2$

2. Для каждого символа из сообщения определим его код в десятичной и/или шестнадцатеричной форме из таблицы **ASCII**, затем переведем его в двоичный вид:

«**A**» $=65_{10}=41_{16}=0\mathbf{1000001}_2$

«**-**» $=45_{10}=2D_{16}=00\mathbf{101101}_2$

«**b**» $=98_{10}=62_{16}=0\mathbf{1100010}_2$

«**=**» $=61_{10}=3D_{16}=00\mathbf{111101}_2$

«**c**» $=99_{10}=63_{16}=0\mathbf{1100011}_2$

3. Выполним поразрядную операцию «**исключающее или**» между кодом каждого символа и маской.

«**A**» $\oplus$ 27=

$\oplus$ $01000001_2$

$00011011_2$

$0101\,1010_2 = 5A_{16}=90_{10}$

5 A

4. По таблице ASCII определим символ, код которого вычислили ранее.

**$5A_{16}=90_{10}$=«Z»,**

**Т.е. символ «А» кодируется символом «Z»**

«-» ⊕ 27=

⊕ $00101101_2$

$00011011_2$

$00110110_2 = 36_{16}=54_{10}=$«6»

3 6

Символ «-» кодируется символом«**6**».

«**b**» ⊕ 27=

⊕ $01100010_2$

$00011011_2$

$01111001_2 = 79_{16}=121_{10}=$«y»

7 9

Символ «**b**» кодируется символом«**y**».

Таким образом кодируем каждый символ. Зашифрованное сообщение будет иметь вид

«**Z6y&x**»

Для восстановления исходного сообщения нужно повторно применить операцию побитового «**исключающего или**» с закодированными символами и маской, которая использовалась при шифровании.

# Восстановление сообщения

Маска: $27_{10}=000\mathbf{11011}_2$

«**Z**» $=90_{10}=5A_{16}=0\mathbf{1011010}_2$

$$01011010_2 \oplus$$
$$\underline{00011011_2}$$
$$01000001_2 = 41_{16}=65_{10}=\text{«A»}$$

4 1

Данные действия проводим с каждым зашифрованным символом. В итоге мы получим исходное сообщение.