Домашняя работа №2

Сеть Фейстеля:

Задача 1: При помощи таблицы кода Бодо зашифруйте сообщение «ZimABlizko» со сдвигом влево на секретный ключ [2,3] по сети Фейстеля. Ответ представьте в текстовом виде. Сделайте 2 раунда для всего текста (не нужно делить еще на пополам).

Пример: При помощи таблицы кода Бодо зашифруйте сообщение «PrishlaVesna» со сдвигом влево на секретный ключ [3,2]. Ответ представьте в текстовом виде.

Решение:

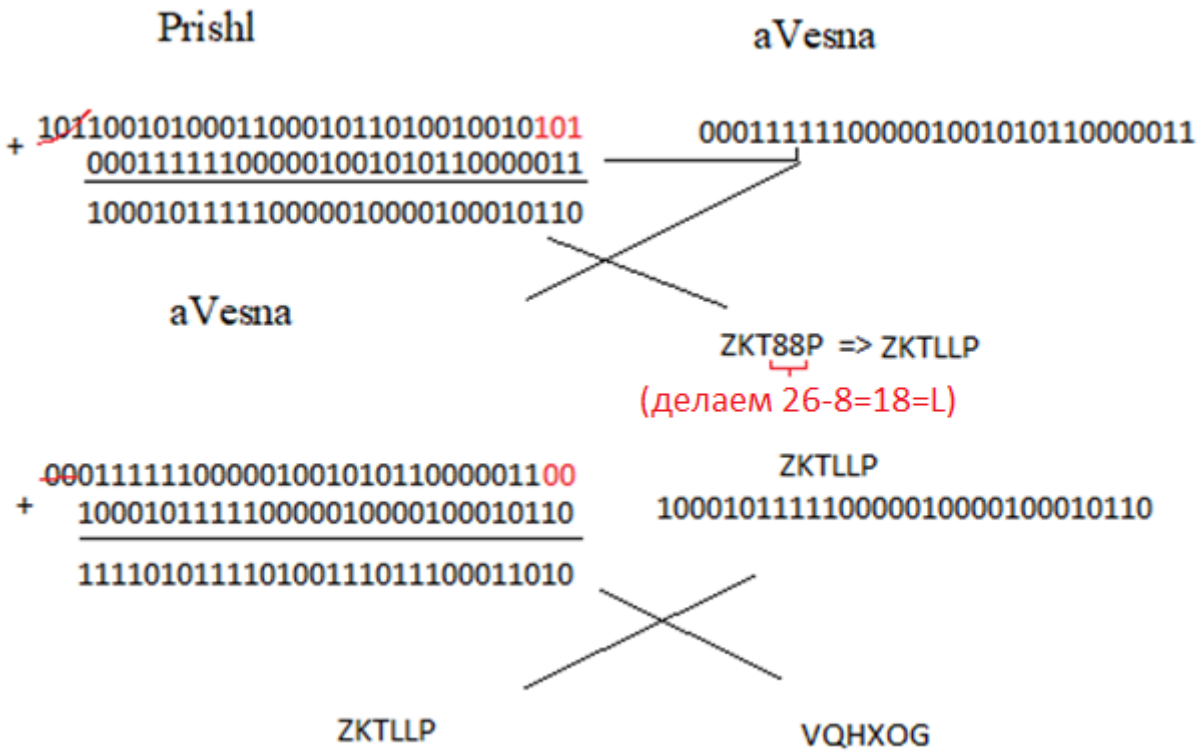


Таблица Код Бодо:

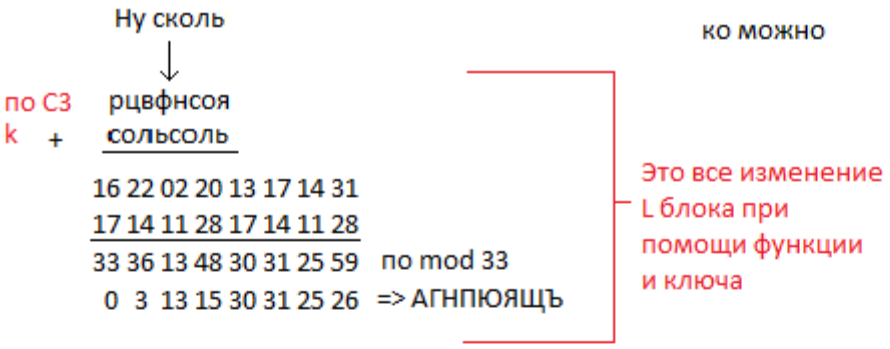
Управляющие символы		
Двоичный код	Десятичный код	Назначение
01000	8	Возврат каретки
00010	2	Перевод строки
11111	31	Буквы латинские
11011	27	Цифры
00100	4	Пробел
00000	0	Буквы русские

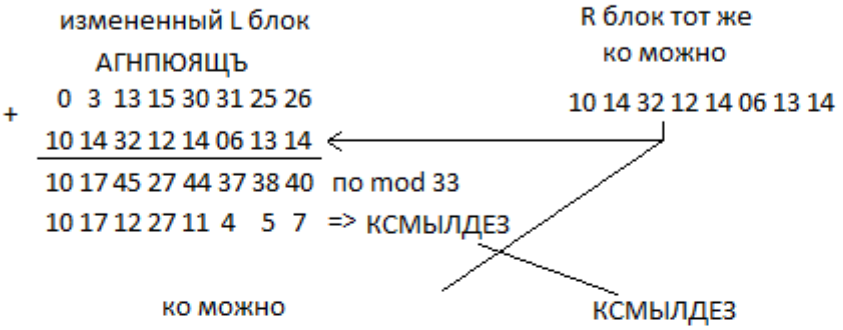
Буквы, цифры и остальные символы				
Двоичный код	Десятичный код	Латинская буква	Русская буква	Цифры и прочие символы
00011	3	A	А	-
11001	25	B	Б	?
01110	14	C	Ц	:
01001	9	D	Д	Кто там?
00001	1	E	Е	З
01101	13	F	Ф	Э
11010	26	G	Г	Ш
10100	20	H	Х	Щ
00110	6	I	И	8
01011	11	J	Й	Ю
01111	15	K	К	(
10010	18	L	Л	)
11100	28	M	М	.
01100	12	N	Н	,
11000	24	O	О	9
10110	22	P	П	0
10111	23	Q	Я	1
01010	10	R	Р	4
00101	5	S	С	'
10000	16	T	Т	5
00111	7	U	У	7
11110	30	V	Ж	=
10011	19	W	В	2
11101	29	X	Ь	/
10101	21	Y	Ы	6
10001	17	Z	З	+

Задача 2: При помощи таблицы ниже зашифруйте сообщение «Я не хочу выживать Я хочу жить» с использованием шифра цезаря C_3 и секретным ключом «ручка» по сети Фейстеля. Ответ представьте в текстовом виде. Пробелы учитывать!

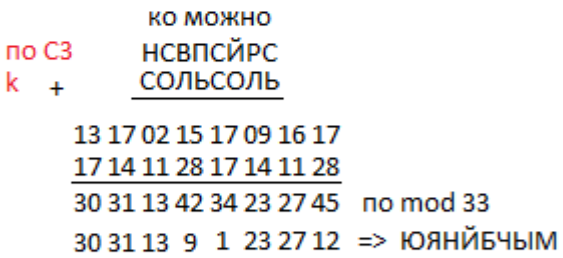
Пример: При помощи таблицы ниже зашифруйте сообщение «Ну сколько можно» с использованием шифра цезаря C_3 и секретным ключом «соль». Ответ представьте в текстовом виде. Пробелы учитывать!

Решение:





теперь тоже самое еще раз, что
изменить весь текст, а не часть



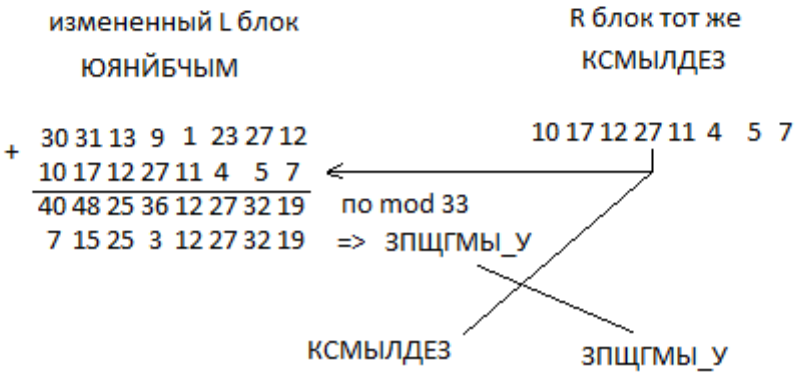


Таблица со сдвигом по С3:

0	А→г	9	Й→м	18	Т→х	27	Ы→ю
1	Б→д	10	К→н	19	У→ц	28	Ь→я
2	В→е	11	Л→о	20	Ф→ч	29	Э→_
3	Г→ж	12	М→п	21	Х→ш	30	Ю→а
4	Д→з	13	Н→р	22	Ц→щ	31	Я→б
5	Е→и	14	О→с	23	Ч→ъ	32	_→в
6	Ж→й	15	П→т	24	Ш→ы		
7	З→к	16	Р→у	25	Щ→ь		
8	И→л	17	С→ф	26	Ъ→э		

Поля Галуа:

Задача 3: Решить полином: $\left(x^3 + x^4 + x^2\right) \bullet \left(x^5 + x\right) + \left(x^2 + x^5\right) \bullet x^5$. Ответ представить в десятичной системе счисления. Порождающий полином: $f(x)=x^3 + x + 1 = 0$.

Задача 4: Решить полином: $\left(x^2 + x^3 + x\right) \bullet \left(x^3 + x\right) + \left(x^2 + x^3 + 1\right) \cdot x$. Ответ представить в шестнадцатеричной системе счисления. Порождающий полином: $f(x)=x^3 + x + 1 = 0$.

Задача 5: Вычислить произведение $57 \cdot 83$, где полиномиальное представление 57 есть $x^6 + x^4 + x^2 + x + 1$, а полиномиальное представление 83 есть $x^7 + x + 1$. Ответ представить в шестнадцатеричной системе счисления. Порождающий полином: $f(x)=x^8 + x^7 + x^6 + x + 1 = 0$.