

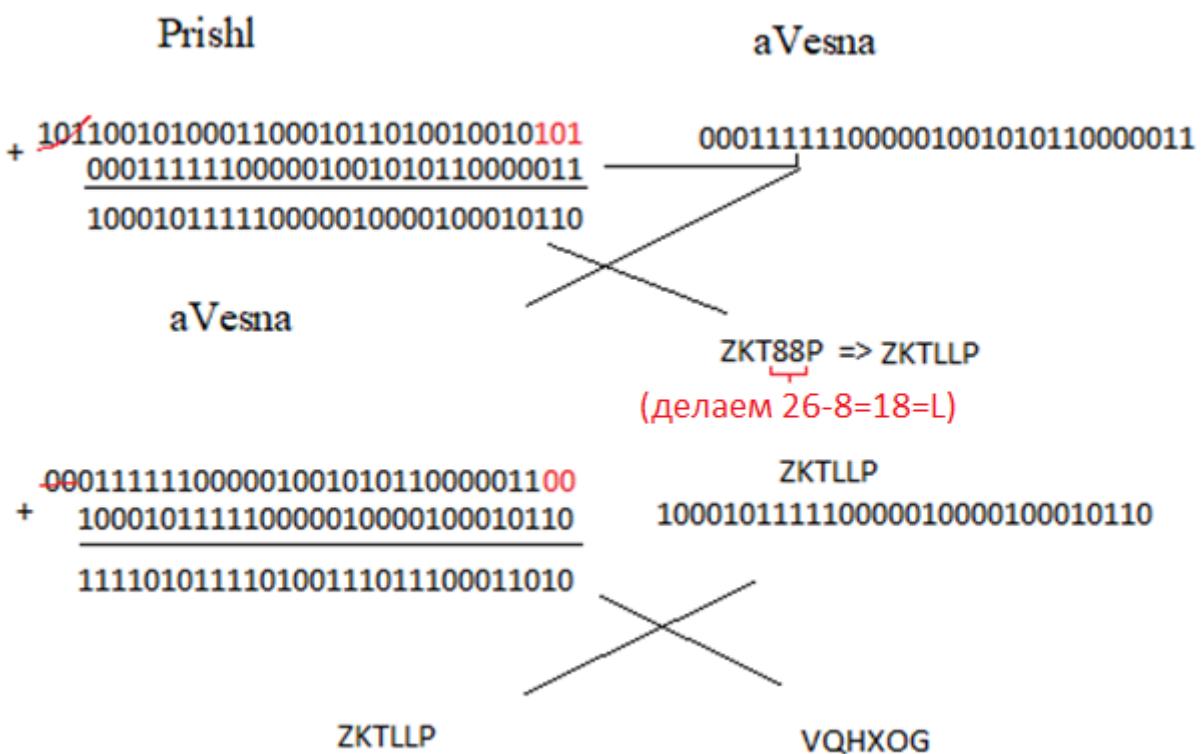
## Домашняя работа №2

### 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	В	Б	?
01110	14	С	Ц	:
01001	9	Д	Д	Кто там?
00001	1	Е	Е	3
01101	13	Ф	Ф	Э
11010	26	Г	Г	Ш
10100	20	Н	Х	Щ
00110	6	I	И	8
01011	11	J	Й	Ю

01111	15	К	К	(
10010	18	Л	Л	)
11100	28	М	М	-
01100	12	Н	Н	,
11000	24	О	О	9
10110	22	Р	П	0
10111	23	Q	Я	1
01010	10	Р	Р	4
00101	5	С	С	'
10000	16	Т	Т	5
00111	7	У	У	7
11110	30	Ж	=	
10011	19	В	В	2
11101	29	Ь	/	
10101	21	Ы	Ы	6
10001	17	З	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:**

Ну сколь  
↓  
по C3    рцвфнсоя  
k + сольсоль

16 22 02 20 13 17 14 31  
17 14 11 28 17 14 11 28  
33 36 13 48 30 31 25 59    по mod 33  
0 3 13 15 30 31 25 26    => АГНПЮЯЩЬ

ко можно

Это все изменение  
L блока при  
помощи функции  
и ключа

измененный L блок  
 АГНПЮЯЩЬ  
 + 0 3 13 15 30 31 25 26  
~~10 14 32 12 14 06 13 14~~ ←  
 10 17 45 27 44 37 38 40 по mod 33  
 10 17 12 27 11 4 5 7 => КСМЫЛДЕЗ  
 ко можно  
 R блок тот же  
 ко можно  
 КСМЫЛДЕЗ

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

ко можно  
 по СЗ НСВПСИРС  
 $k + \underline{\text{СОЛЬСОЛЬ}}$

$13\ 17\ 02\ 15\ 17\ 09\ 16\ 17$   
 $\underline{17\ 14\ 11\ 28\ 17\ 14\ 11\ 28}$   
 30 31 13 42 34 23 27 45 по mod 33  
 30 31 13 9 1 23 27 12 => ЮЯНЙБЧЫМ

### 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→ъ		
8	И→л	17	С→ф	26	Ъ→э		

### Поля Галуа:

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

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

**Задача 5:** Вычислить произведение 57·83, 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:  $f(x)=x^8 + x^7 + x^6 + x + 1 = 0$ .