

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:

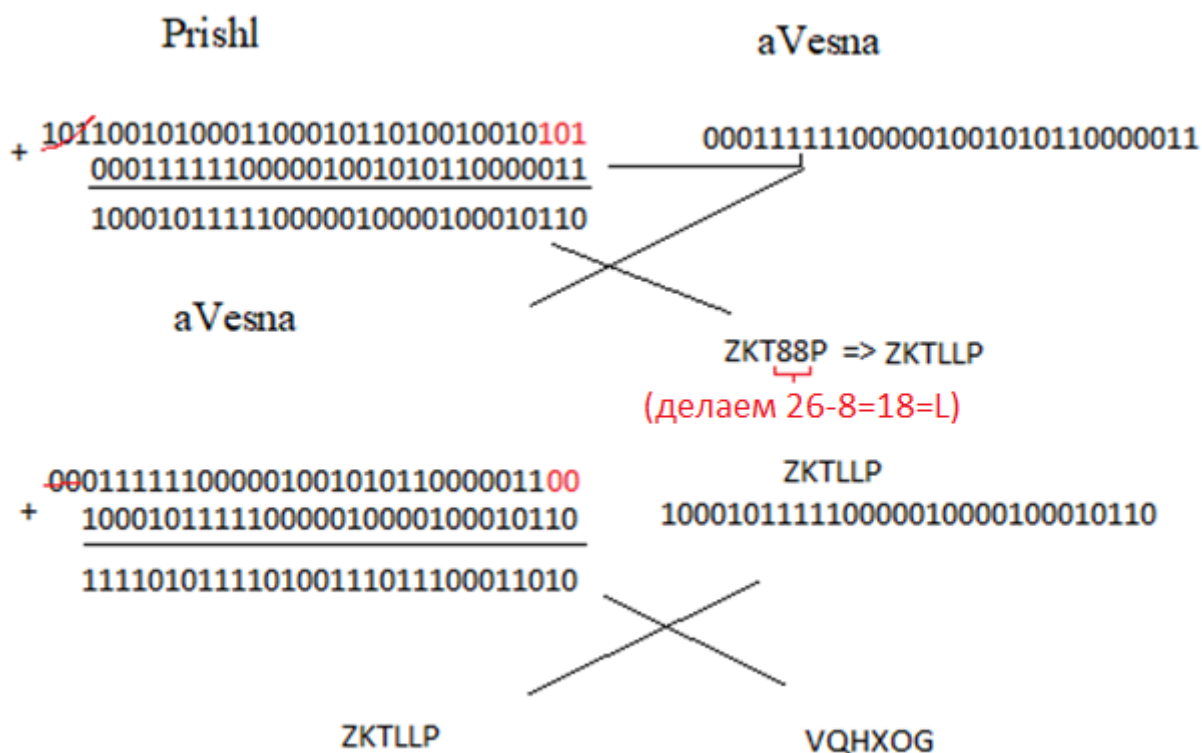


Таблица Код Бодо:

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	3
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:

Ну сколь
↓
по СЗ
k + рцвфнся
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
0	3	13	15	30	31	25	26

по mod 33
=> АГНПЮЯЩЪ

ко можно

Это все изменение
L блока при
помощи функции
и ключа

измененный L блок
АГНПЮЯЩЪ

ко можно

по СЗ
k + 0 3 13 15 30 31 25 26

10	14	32	12	14	06	13	14
10	17	45	27	44	37	38	40
10	17	12	27	11	4	5	7

по mod 33
=> КСМЫЛДЕЗ

ко можно

КСМЫЛДЕЗ

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

КСМЫЛДЕЗ

по СЗ
k + ко можно
НСВПСЙРС
СОЛЬСОЛЬ

13	17	02	15	17	09	16	17
17	14	11	28	17	14	11	28
30	31	13	42	34	23	27	45
30	31	13	9	1	23	27	12

по mod 33
=> ЮЯНЙБЧЫМ

измененный L блок
ЮЯНЙБЧЫМ

ко можно

по СЗ
k + 30 31 13 9 1 23 27 12

10	17	12	27	11	4	5	7
40	48	25	36	12	27	32	19
7	15	25	3	12	27	32	19

по mod 33
=> зпщгмы_у

КСМЫЛДЕЗ

зпщгмы_у

Таблица со сдвигом по СЗ:

0	$A \rightarrow \Gamma$	9	$\Upsilon \rightarrow \mathcal{M}$	18	$\mathcal{T} \rightarrow \mathcal{X}$	27	$\mathcal{Y} \rightarrow \mathcal{Y}_o$
1	$\mathcal{B} \rightarrow \mathcal{D}$	10	$\mathcal{K} \rightarrow \mathcal{H}$	19	$\mathcal{Y} \rightarrow \mathcal{C}$	28	$\mathcal{B} \rightarrow \mathcal{Y}$
2	$\mathcal{V} \rightarrow \mathcal{E}$	11	$\mathcal{L} \rightarrow \mathcal{O}$	20	$\Phi \rightarrow \mathcal{C}$	29	$\mathcal{E} \rightarrow _$
3	$\mathcal{G} \rightarrow \mathcal{J}$	12	$\mathcal{M} \rightarrow \mathcal{P}$	21	$\mathcal{X} \rightarrow \mathcal{H}$	30	$\mathcal{Y}_o \rightarrow \bar{a}$
4	$\mathcal{D} \rightarrow \mathcal{Z}$	13	$\mathcal{H} \rightarrow \mathcal{P}$	22	$\mathcal{C} \rightarrow \mathcal{H}$	31	$\mathcal{Y} \rightarrow \mathcal{B}$
5	$\mathcal{E} \rightarrow \mathcal{H}$	14	$\mathcal{O} \rightarrow \mathcal{C}$	23	$\mathcal{C} \rightarrow \mathcal{B}$	32	$_ \rightarrow \mathcal{V}$
6	$\mathcal{J} \rightarrow \mathcal{Y}$	15	$\mathcal{P} \rightarrow \mathcal{T}$	24	$\mathcal{H} \rightarrow \mathcal{Y}$		
7	$\mathcal{Z} \rightarrow \mathcal{K}$	16	$\mathcal{P} \rightarrow \mathcal{Y}$	25	$\mathcal{H} \rightarrow \mathcal{B}$		
8	$\mathcal{H} \rightarrow \mathcal{L}$	17	$\mathcal{C} \rightarrow \mathcal{F}$	26	$\mathcal{B} \rightarrow \mathcal{E}$		

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 $57 \cdot 83$, 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: $f(x) = x^8 + x^7 + x^6 + x + 1 = 0$.