**Задание №1. Шифр Цезаря**

Исходный текст:

«ДАКУКИН ИВАН ЕВГЕНИЕВИЧ»

Используем алфавит, содержащий 33 буквы и пробел, стоящий после буквы Я:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯпробел

Ключом в шифре Цезаря является число 3. Каждая буква в исходном тексте сдвигается по алфавиту на 3 позиции. Таким образом, получаем:

|  |  |
| --- | --- |
| Исходный текст | ДАКУКИН ИВАН ЕВГЕНИЕВИЧ |
| Зашифрованный текст | ЖГНЦНЛРВЛЕГРВЗЕЁЗРЛЗЕЛЪ |

**Задание №2. Алгоритм шифрования ГОСТ 28147-89.**

Исходные данные для зашифрования: ДАКУКИН\_

Для ключа возьмем последовательность, состоящую из 32 букв:

ИВАН евгениевич криптография это

Исходный текст

Д 11000100

А 11000000

К 11001010

У 11110011

К 11001010

И 11001000

Н 11101101

пробел 00010000

Первый подключ X0

И 11001000

В 11000010

А 11000000

Н 11101101

Таким образом, первые 64 бита определяют входную последовательность

L0: 11000100 11000000 11001010 11110011

R0: 11001010 11001000 11101101 00010000

следующие 32 бита определяют первый подключ

X0: 11001000 11000010 11000000 11101101

1). Вычисление суммы R0 и X0 по mod 2 32

R0: 1100 1010 1100 1000 1110 1101 0001 0000

X0: 1100 1000 1100 0010 1100 0000 1110 1101

1001 0011 1000 1011 1010 1101 1111 1101

2). Преобразование в блоке подстановки

Результат суммирования R0+X0 по mod 2 32

1001 0011 1000 1011 1010 1101 1111 1101

номера блоков

8 7 6 5 4 3 2 1

1001 0001 1000 1011 1010 1101 1111 1101

номера строк в таблице подстановки

9 1 8 11 10 13 15 13

заполнение

2 11 3 14 6 0 9 15

результат

0010 1011 0011 1110 0110 0000 1001 1111

3). Циклический сдвиг результата п.2 на 11 бит влево

1111 0011 0000 0100 1111 1001 0101 1001

f(R0,X0):

1111 0011 0000 0100 1111 1001 0101 1001

II. Вычисляем R1= f(R0,X0) ⊕ L0.

Результат преобразования функции f(R0,X0) складываем с L0 по mod2:

L0: 1100 0100 1100 0000 1100 1010 1111 0011

f(R0,X0): 1111 0011 0000 0100 1111 1001 0101 1001

R1: 1011 0111 1100 0100 0011 0011 1010 1010