Задание 1

Дано:

1. 8 х 32 = 256 бит ключа (см. таблицу №1).
2. 8 х (16х4) = 512 бит узла замены (см.таблицу №2).
3. Схема алгоритма (слайд).
4. Сообщение длиной 64 бита: в виде ГNГN ГNГN,

где Г- две цифры номера группы, N - Ваш номер по журналу (две цифры);

Выполнить:

1. Операции криптографических преобразования для двух раундов алгоритма шифрования согласно ГОСТ 28147-89.
2. Представить результаты промежуточных вычислений и результат шифрования после второго раунда в двоичной и шестнадцатиричной формах.

Указания:

- указать номер варианта и фамилию;
- сообщение, ключ, перестановки, представленные одно или двухразрядными десятичными числами записать 4-х разрядными двоичными числами;
- первые 32 бита сообщения записать в регистр N1, вторые в N2, запись осуществлять справа налево.

Таблица 1.

Ко	7	15	1	5	4	12	11	10
К1	3	14	5	0	9	7	5	4
К2	11	4	6	10	7	1	12	3
К3	2	1	8	4	12	9	7	5
К4	5	3	13	10	9	6	4	1
К5	1	0	4	8	5	9	3	14
К6	13	11	5	2	1	6	9	8
К7	8	12	9	7	6	3	2	1

Таблица 2.

Адрес	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**
0	7	1	11	9	15	8	10	7
1	12	6	5	14	4	2	5	0
2	0	10	7	0	12	4	0	9
3	5	5	14	13	11	11	12	5
4	14	7	4	15	5	7	13	12
5	3	9	3	3	8	12	2	6
6	9	12	13	5	2	13	7	10
7	10	3	0	8	1	1	9	3
8	1	13	8	6	10	5	4	8
9	11	8	6	11	9	15	3	11
10	15	0	2	10	6	3	11	15
11	6	15	9	7	0	6	6	2
12	4	14	15	1	3	14	14	1
13	8	2	10	4	14	9	8	13
14	2	11	1	12	13	0	1	4
15	13	4	12	2	7	10	15	14

Пример:

Исходное сообщение

11.6.5.3.0.9.12.15. 13.8.10.4.7.14.1.2.

0010 0001 1110 0111 0100 1010 1000 1101 N2

2 1 14(E) 7 4 10(A) 8 13(D)

1111 1100 1001 0000 0011 0101 0110 1011 N1

15(F) 12(F) 9 0 3 5 6 11(B)

[+] mod 2^{32}

0111 1111 0001 0101 0100 1100 1011 1010 Ко

7 15(F) 1 5 4 12(C) 11(B) 10(A)

0111 1011 1010 0101 1000 0010 0010 0101 на вых. СМ mod2^{32}

7 11(B) 10(A) 5 8 2 2 5

1010 1111 0010 0011 1010 0010 0000 0110 из узла замены

10 15(F) 2 3 10 4 0 6

0001 1101 0010 0000 0011 0101 0111 1001 на вых.рег. сдвига на 11 разрядов

(+) mod2

0010 0001 1110 0111 0100 1010 1000 1101 N2

0011 1100 1100 0111 0111 1111 1111 0100 на вых. СМ mod2 и в N1

1111 1100 1001 0000 0011 0101 0110 1011 N2

2-й раунд аналогично