**ПРИМЕР ШИФРОВАНИЯ ГОСТ**

Шифруемое сообщение:

шифровка (64 бит) – 11111000111010001111010011110000 – N1(младшая)

11101110111000101110101011100000 – N2 (старшая)

Ключ (256 бит) – 1234567891011121314151617181920212223242526272829303132

1 блок 8 блок

Разбиваем на восемь 32-битных блоков

1|0011|0001|0011|0010|0011|0011|0011|0100|8

1|0011|0001|0011|0010|0011|0011|0011|0100|8

1|0011|0001|0011|0010|0011|0011|0011|0100|8

8|0100|0011|0011|0011|0010|0011|0001|0011|1

Берем N1 и X1 и складываем по модулю 232 (тоже самое, что и XOR):

11111000111010001111010011110000

00110001001100100011001100110100

11001001110110101100011111000100

Преобразуем при помощи таблицы замен:

S-блоки 1100|1001|1101|1010|1100|0111|1100|0100

12 9 13 10 12 7 12 4

Преобразуем: 7 3 0 6 0 13 6 5

Переводим: 0111|0011|0000|0110|0000|1101|0110|0101

Сдвигаем на 11 битов влево:

0011|0000|0110|1011|0010|1011|1001|1000

XOR со старшей частью N2:

0011|0000|0110|1011|0010|1011|1001|1000

1110|1110|1110|0010|1110|1010|1110|0000

1101|1110|1000|1001|1100|0001|0111|1000

Сдвиг по цепочки, младшая становится старшей, результат предыдущего шага – младшей:

11011110100010011100000101111000|11111000111010001111010011110000

N1 N2

Повторяем итерации 32 раза