

рост

Шаг 0

Определяет исходные данные для основного шага криптопреобразования:

N – преобразуемый 64-битовый блок данных,

N_1 - младшая часть

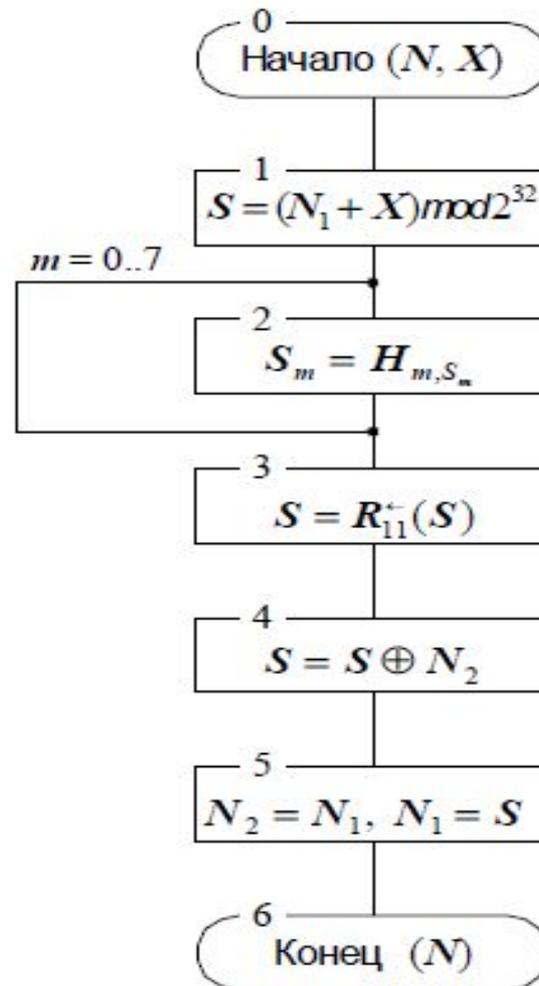
N_2 - старшая часть

$$N=(N1,N2).$$

Ключ

- Исходный 256-битный ключ разбивается на восемь 32-битных блоков: $x_1 \dots x_8$.
Ключи $x_9 \dots x_{24}$ являются циклическим повторением ключей $x_1 \dots x_8$ (нумеруются от младших битов к старшим). Ключи $x_{25} \dots x_{32}$ являются ключами $x_1 \dots x_8$, идущими в обратном порядке.
- **Ключ X** является массивом из восьми 32-битовых элементов кода,

Основной шаг



1. N_1 и X_1 складываются по модулю 2^{32}
2. Результат разбивается на восемь 4-битовых подпоследовательностей, каждая из которых поступает на вход своего узла *таблицы замен* (в порядке возрастания старшинства битов), называемого *S-блоком*.

Общее количество S-блоков ГОСТа — восемь. Каждый S-блок представляет собой перестановку чисел от 0 до 15. Первая 4-битная подпоследовательность попадает на вход первого S-блока, вторая — на вход второго и т. д.

3. Выходы всех восьми S-блоков объединяются в 32-битное слово, затем всё слово циклически сдвигается влево (к старшим разрядам) на 11 битов.

4. Побитовое сложение: значение, полученное на шаге 3, побитно складывается по модулю 2

со старшей половиной преобразуемого блока.

5. Сдвиг по цепочке: младшая часть преобразуемого блока сдвигается на место старшей, а на ее место помещается результат выполнения предыдущего шага.

6. Полученное значение преобразуемого блока возвращается как результат выполнения алгоритма основного шага криптопреобразования.

После выполнения всех 32 раундов алгоритма, блоки склеиваются.

Узлы замены (S-блоки)

| Номер S-блока | Значение |
|---------------|---------------------------------------|
| 1 | 4 10 9 2 13 8 0 14 6 11 1 12 7 15 5 3 |
| 2 | 14 11 4 12 6 13 15 10 2 3 8 1 0 7 5 9 |
| 3 | 5 8 1 13 10 3 4 2 14 15 12 7 6 0 9 11 |
| 4 | 7 13 10 1 0 8 9 15 14 4 6 12 11 2 5 3 |
| 5 | 6 12 7 1 5 15 13 8 4 10 9 14 0 3 11 2 |
| 6 | 4 11 10 0 7 2 1 13 3 6 8 5 9 12 15 14 |
| 7 | 13 11 4 1 3 15 5 9 0 10 14 7 6 8 2 12 |
| 8 | 1 15 13 0 5 7 10 4 9 2 3 14 6 11 8 12 |

- **Сравнение шифров ГОСТ 28147-89 и DES**

| Параметр | ГОСТ | DES |
|---|----------------|-------------|
| Размер блока шифрования | 64 бита | 64 бита |
| Длина ключа | 256 бит | 56 бит |
| Число раундов | 32 | 16 |
| Узлы замен (S-блоки) | не фиксированы | фиксированы |
| Длина ключа для одного раунда | 32 бита | 48 бит |
| Схема выработки раундового ключа | простая | сложная |
| Начальная и конечная перестановки битов | нет | есть |