**Задание.**

Программа, реализующая алгоритм симметричного шифрования ГОСТ 28147-89 для одного блока сообщения. Необходимо зашифровать и дешифровать, например, текстовый документ.

**Пояснения.**

1. Алгоритм шифрует только один блок размером 64 бита.
2. В программе рекомендуется оформить алгоритм в виде отдельной функции с передаваемыми ей параметрами и возвращаемым значением.
3. Интерфейс программы должен предусматривать возможность изменения ключа шифрования (в том числе перед дешифрованием), открытого текста и шифротекста (в самой программе или как отдельные файлы).

**Общие сведения.**

Алгоритм шифрования ГОСТ 28147-89 является симметричным, блочным алгоритмом. Преобразование осуществляется над блоком размером 64 бита, размер секретного ключа 256 бит, в алгоритме 32 раунда преобразований.

Необходимые определения и обозначения:

 – блок открытого текста размером 64 бита;

 – блок зашифрованного текста размером 64 бита;

 – секретный ключ (256 бит);

 – раундовый ключ.

В алгоритме ГОСТ используются следующие операции:

S-блок или S-box – табличная подстановка, при которой группа бит отображается в другую группу бит;

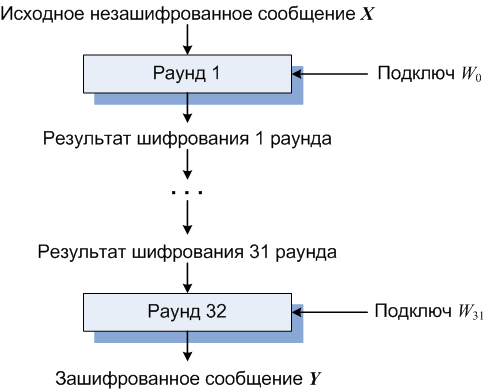
– операция сложения по модулю 232;

или XOR – операция сложения по модулю 2 (или побитовое «исключающее или»);

11 – циклический сдвиг влево на 11 бит.

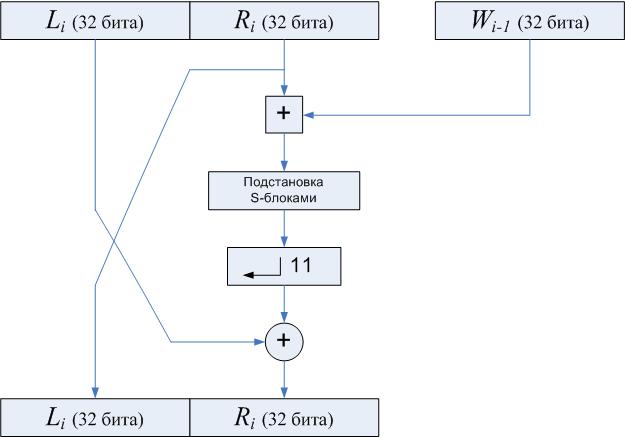
Эти операции циклически повторяются в алгоритме, образуя так называемые раунды. Входом каждого раунда является выход предыдущего раунда и раундовый подключ , который получен из секретного ключа шифрования  следующим образом. Рассмотрим секретный ключ  (256 бит), состоящий из восьми слов по 32 бита: . На их основе строим раундовый ключ :

.



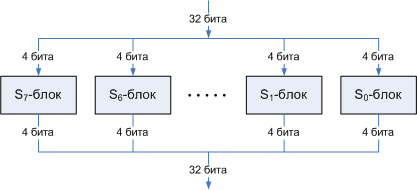
*Рис. 3. Основная схема алгоритма ГОСТ*

Для шифрования блок открытого текста сначала разбивается на две одинаковые части, правую *R* (младшее слово) и левую *L* (старшее слово).



*Рис. 4. Схема одного раунда алгоритма ГОСТ*

На *i*-м раунде используется подключ . Правая часть  складывается по модулю 232 с раундовым подключом . Над получившимся результатом выполняется операция табличной подстановки.



*Рис. 5. Подстановка S-блоками*

Для этого результат разбивается на восемь 4-битовых кусочков, каждый из которых подается на вход своего S-блока: первые четыре бита в S0-блок, вторые – в S1-блок и так далее. Каждый S-блок содержит 16 четырехбитовых элементов, нумеруемых с 0 по 15. ГОСТ рекомендует заполнять каждую из восьми таблиц различными числами множества {0, 1, 2, …, 15}, переставленными случайным образом.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S0-блок** | | | | | | | | | | | | | | | | |
| № | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Элемент | 4 | 10 | 9 | 2 | 13 | 8 | 0 | 14 | 6 | 11 | 1 | 12 | 7 | 15 | 5 | 3 |
| **S1-блок** | | | | | | | | | | | | | | | | |
| № | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Элемент | 14 | 11 | 4 | 12 | 6 | 13 | 15 | 10 | 2 | 3 | 8 | 1 | 0 | 7 | 5 | 9 |
| **S2-блок** | | | | | | | | | | | | | | | | |
| № | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Элемент | 5 | 8 | 1 | 13 | 10 | 3 | 4 | 2 | 14 | 15 | 12 | 7 | 6 | 0 | 9 | 11 |
| **S3-блок** | | | | | | | | | | | | | | | | |
| № | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Элемент | 7 | 13 | 10 | 1 | 0 | 8 | 9 | 15 | 14 | 4 | 6 | 12 | 11 | 2 | 5 | 3 |
| **S4-блок** | | | | | | | | | | | | | | | | |
| № | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Элемент | 6 | 12 | 7 | 1 | 5 | 15 | 13 | 8 | 4 | 10 | 9 | 14 | 0 | 3 | 11 | 2 |
| **S5-блок** | | | | | | | | | | | | | | | | |
| № | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Элемент | 4 | 11 | 10 | 0 | 7 | 2 | 1 | 13 | 3 | 6 | 8 | 5 | 9 | 12 | 15 | 14 |
| **S6-блок** | | | | | | | | | | | | | | | | |
| № | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Элемент | 13 | 11 | 4 | 1 | 3 | 15 | 5 | 9 | 0 | 10 | 14 | 7 | 6 | 8 | 2 | 12 |
| **S7-блок** | | | | | | | | | | | | | | | | |
| № | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Элемент | 1 | 15 | 13 | 0 | 5 | 7 | 10 | 4 | 9 | 2 | 3 | 14 | 6 | 11 | 8 | 12 |

*Рис. 6. Набор S-блоков Центрального банка РФ*

По входным четырем битам определяется номер элемента в S-блоке, который поступает на выход. Выходы всех восьми S-блоков объединяются в 32-битовое слово, затем все слово циклически сдвигается влево на 11 бит. Наконец, результат объединяется с помощью XOR с левой половиной, и получается новая правая половина, а правая половина становится левой половиной. Эти операции выполняются 32 раза. После этого левая и правая части меняются местами.

Запишем базовый цикл алгоритма ГОСТ.

Вход: Блок , , раундовый ключ .

Выход: Преобразованный блок , .

FOR TO 31 DO

;

FOR TO 7 DO

RETURN

Для шифрования и дешифрования сообщения используется один алгоритм. Единственным различием является генерация раундового ключа. Чтобы дешифровать блок, строим раундовый ключ

,

подаем на вход  и на выходе получаем .