

3.6. Алгоритм ГОСТ 28147

Алгоритм ГОСТ 28147 является отечественным стандартом для алгоритмов симметричного шифрования. ГОСТ 28147 разработан в 1989 году, является блочным алгоритмом шифрования, длина блока равна 64 битам, длина ключа равна 256 битам, количество раундов равно 32. Алгоритм представляет собой классическую сеть Фейштеля.

$$L_i = R_{i-1}$$

$$R_i = L_i \oplus f(R_{i-1}, K_i)$$

Функция F проста. Сначала правая половина и *i*-ый подключ складываются по модулю 2^{32} . Затем результат разбивается на восемь 4-битовых значений, каждое из которых подается на вход S-box. ГОСТ 28147 использует восемь различных S-boxes, каждый из которых имеет 4-битовый вход и 4-битовый выход. Выходы всех S-boxes объединяются в 32-битное слово, которое затем циклически сдвигается на 11 битов влево. Наконец, с помощью XOR результат объединяется с левой половиной, в результате чего получается новая правая половина.



Рисунок 3.11 – I-ый раунд ГОСТ 28147

Генерация ключей проста. 256-битный ключ разбивается на восемь 32-битных подключей. Алгоритм имеет 32 раунда, поэтому каждый подключ используется в четырех раундах по следующей схеме:

Раунд	1	2	3	4	5	6	7	8
Подключ	1	2	3	4	5	6	7	8
Раунд	9	10	11	12	13	14	15	16
Подключ	1	2	3	4	5	6	7	8
Раунд	17	18	19	20	21	22	23	24
Подключ	1	2	3	4	5	6	7	8

Раунд	25	26	27	28	29	30	31	32
Подключ	8	7	6	5	4	3	2	1

Считается, что стойкость *алгоритма ГОСТ 28147* во многом определяется структурой *S-boxes*. Входом и выходом *S-box* являются 4-битные числа, поэтому каждый *S-box* может быть представлен в виде строки чисел от 0 до 15, расположенных в некотором порядке. Тогда порядковый номер числа будет являться входным значением *S-box*, а само число - выходным значением *S-box*.