2.5. Скремблирование

Скремблерами называются программные или аппаратные реализации алгоритма, позволяющего шифровать побитно непрерывные потоки информации. Сам скремблер представляет из себя набор бит, изменяющихся на каждом шаге по определенному алгоритму. После выполнения каждого очередного шага на его выходе появляется шифрующий бит – либо 0, либо 1, который накладывается на текущий бит информационного потока операцией XOR.

Суть скремблирования заключается в побитном изменении проходящего через систему потока данных. Практически единственной операцией, используемой в скремблерах является XOR – "побитное исключающее ИЛИ". Параллельно прохождению информационного потока в скремблере по определенному правилу генерируется поток бит – кодирующий поток. Как прямое, так и обратное шифрование осуществляется наложением по XOR кодирующей последовательности на исходную.

Генерация кодирующей последовательности бит производится циклически из небольшого начального объема информации – ключа по следующему алгоритму. Из текущего набора бит выбираются значения определенных разрядов и складываются по XOR между собой. Все разряды сдвигаются на 1 бит, а только что полученное значение ("0" или "1") помещается в освободившийся самый младший разряд. Значение, находившееся в самом старшем разряде до сдвига, добавляется в кодирующую последовательность, становясь очередным ее битом (см. рис.1).

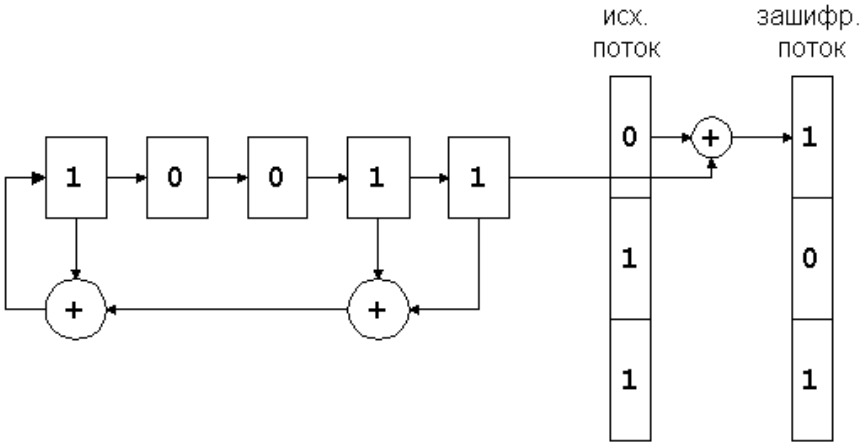

Рисунок 2.1 – Принцип работы скремблера

Из теории передачи данных криптография заимствовала для записи подобных схем двоичную систему записи. По ней изображенный на рисунке скремблер записывается комбинацией "10011_2" – единицы соответствуют разрядам, с которых снимаются биты для формирования обратной связи.

Рассмотрим пример кодирования информационной последовательности 010111_2 скремблером 101_2 с начальным ключом 110_2.

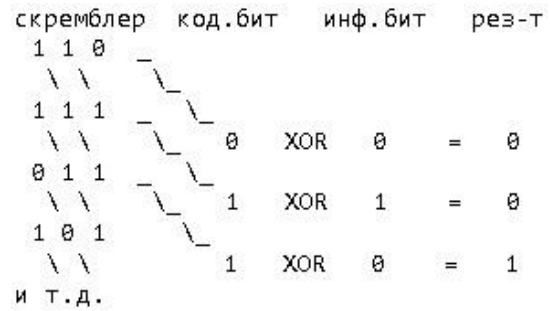

Рисунок 2.2 – Принцип работы скремблера

Декодирование заскремблированных последовательностей происходит по той же самой схеме, что и кодирование. Именно для этого в алгоритмах применяется результирующее кодирование по "исключающему ИЛИ" – схема, однозначно восстановимая при раскодировании без каких-либо дополнительных вычислительных затрат.