**Сеть Фейстеля**

Сеть Фе́йстеля или по другому – конструкция Фейстеля это один из активно используемых методов построения блочных шифров. Сеть состоит из ячеек, называемых ячейками Фейстеля. На вход каждой ячейки поступают данные и ключ. На выходе каждой ячейки получают изменённые данные и изменённый ключ. Все ячейки однотипны, и говорят, что сеть представляет собой определённую многократно повторяющуюся структуру. Ключ выбирается в зависимости от алгоритма шифрования/дешифрования и меняется при переходе от одной ячейки к другой. При шифровании и дешифровании выполняются одни и те же операции; отличается только порядок ключей. Ввиду простоты операций сеть Фейстеля легко реализовать как программно, так и аппаратно. Большинство современных блочных шифров (DES, RC6, Blowfish, FEAL, CAST-128, TEA, и др.) используют сеть Фейстеля в качестве основы.

**Шифрование**

Пусть требуется зашифровать некоторую информацию, представленную в двоичном виде (в виде последовательности нулей и единиц) и находящуюся в памяти компьютера или иного устройства.

Алгоритм шифрования :

Информация разбивается на блоки одинаковой (фиксированной) длины. Полученные блоки называются входными, так как поступают на вход алгоритма. В случае, если длина входного блока меньше, чем размер, который выбранный алгоритм шифрования способен зашифровать единовременно (размер блока), то блок удлиняется каким-либо способом. Как правило длина блока является степенью двойки, например, составляет 64 бита или 128 бит.

Далее будем рассматривать операции происходящие только с одним блоком, так как в процессе шифрования с другими блоками выполняются те же самые операции.

Алгоритм :

* Выбранный блок делится на два подблока одинакового размера — «левый» (L_0) и «правый» (R_0).
* «Левый подблок» L_0 изменяется функцией *f* с использованием [раундового](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%83%D0%BD%D0%B4_(%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8)) ключа K_0: x = f( L_0, K_0 ).
* Результат складывается по модулю 2 («xor») с «правым подблоком» R_0:

x = x \oplus R_0.

* Результат будет использован в следующем раунде в роли «левого подблока» L_1:

L_1 = x.

* «Левый подблок» L_0 текущего раунда будет использован в следующем раунде в роли «правого подблока» R_1:  R_1 = L_0. 
* По какому-либо математическому правилу вычисляется [раундовый](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%83%D0%BD%D0%B4_(%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8)) [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) K_1 — ключ, который будет использоваться в следующем раунде.

Перечисленные операции выполняются *N-1* раз, где *N* — количество [раундов](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%83%D0%BD%D0%B4_(%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8)) в выбраном алгоритме шифрования. При этом между переходами от одного раунда (этапа) к другому изменяются ключи: K_0 заменяется на K_1, K_1 — на K_2 и т. д.).

**Расшифрование**

Расшифровка информации происходит так же, как и шифрование, с тем лишь исключением, что ключи следуют в обратном порядке, то есть не от первого к N-ному, а от N-го к первому.

Сеть Фейстеля является обратимой даже в том случае, если функция F не является таковой, так как для дешифрования не требуется вычислять F-1. Для дешифрования используется тот же алгоритм, но на вход подается зашифрованный текст, и ключи используются в обратном порядке.

\_\_

**Другой технологией, широко используемой в блочном шифровании является подстановочно-перестановочная сеть – SP-сеть (AES и др.).**

**SP-сеть** (*Substitution-Permutation network*, подстановочно-перестановочная сеть) — один из алгоритмов блочного шифра, разработанный и впервые реализованный в 1971 году [Хорстом Фейстелем](https://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%80%D1%81%D1%82_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8C). В простейшем варианте представляет собой «сэндвич» из слоёв двух типов, используемых многократно по очереди. Первый тип слоя — P-слой, состоящий из P-блока большой разрядности, за ним идёт второй тип слоя — S-слой, представляющий собой большое количество S-блоков малой разрядности, потом опять P-слой, и такое действие повторяется циклом заданное количество раз. Первым криптографическим алгоритмом на основе SP-сети был [«Люцифер»](https://ru.wikipedia.org/wiki/Lucifer_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) ([1971](https://ru.wikipedia.org/wiki/1971)). В настоящее время из алгоритмов на основе SP-сетей широко используется [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard).

В современных алгоритмах вместо S- и P-блоков используются различные математические или логические функции. Любая двоичная функция может быть сведена к S-блоку, некоторые функции - к P-блоку. Например к P-блоку сводится [циклический сдвиг](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D1%81%D0%B4%D0%B2%D0%B8%D0%B3#.D0.A6.D0.B8.D0.BA.D0.BB.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.B8.D0.B9_.D1.81.D0.B4.D0.B2.D0.B8.D0.B3), сам P-блок является частным случаем S-блока. Такие функции, как правило, легко реализуются в аппаратуре, обеспечивая при этом хорошую [криптостойкость](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D1%82%D0%BE%D0%B9%D0%BA%D0%BE%D1%81%D1%82%D1%8C" \o "Криптографическая стойкость).

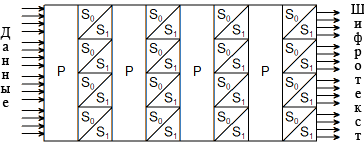


Рисунок . Упрощённая схема SP-сети

**S-блок**, «блок подстановок» — функция в коде программы или аппаратная система, принимающая на входе n бит, преобразующая их по определённому алгоритму и возвращающая на выходе m бит. n и m не обязательно равны.

Программная реализация s‑блока работает следующим образом:

* читается значение на входе (аргумент функции);
* выполняется поиск прочитанного значения по [таблице](https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D0%B0_%D0%BF%D0%BE%D0%B8%D1%81%D0%BA%D0%B0);
* по определённому правилу выбирается ячейка таблицы; из ячейки читается выходное значение; выходное значение возвращается из функции.

Используемая таблица называется «таблицей замен» или «таблицей подстановок». Таблица может:

* быть неизменной (фиксированной) (англ. *static*);
* генерироваться на основе [ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) (англ. *dynamic*).

Например, для шифра (алгоритма) DES используется фиксированная таблица, а для шифров [Blowfish](https://ru.wikipedia.org/wiki/Blowfish" \o "Blowfish) и [Twofish](https://ru.wikipedia.org/wiki/Twofish" \o "Twofish) таблица создаётся на основе ключа.

S-блоки используются в блочных шифрах при выполнении симметричного шифрования для сокрытия статистической связи между открытым текстом и шифротекстом.

Анализ n-разрядного s-блока при большом n крайне сложен, однако реализовать такой блок на практике очень сложно, так как число возможных соединений велико (2^n). На практике «блок подстановок» используется как элемент более сложных систем.

**P-блок** Блок перестановок (p-блок, [англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *p-box*) всего лишь изменяет положение цифр и является линейным устройством. Этот блок может иметь очень большое количество входов-выходов, однако в силу линейности систему нельзя считать криптоустойчивой.

Криптоанализ ключа для *n*-разрядного p-блока проводится путём подачи на вход *n-1* различных сообщений, каждое из которых состоит из *n-1* нуля («0») и 1 единицы («1») (или наоборот, из единиц и нуля).

В современных алгоритмах вместо S- и P-блоков используются различные математические или логические функции. Любая двоичная функция может быть сведена к S-блоку, некоторые функции - к P-блоку. Например к P-блоку сводится циклический сдвиг, сам P-блок является частным случаем S-блока. Такие функции, как правило, легко реализуются в аппаратуре, обеспечивая при этом хорошую криптостойкость.

<http://www.intuit.ru/studies/courses/28/28/lecture/20412?page=2>

<https://ru.wikipedia.org/wiki/SP-%D1%81%D0%B5%D1%82%D1%8C>

<https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D1%8C_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F>

<https://habrahabr.ru/post/140404/>