BLOWFISH.
TWOFISH.

BLOWFISH

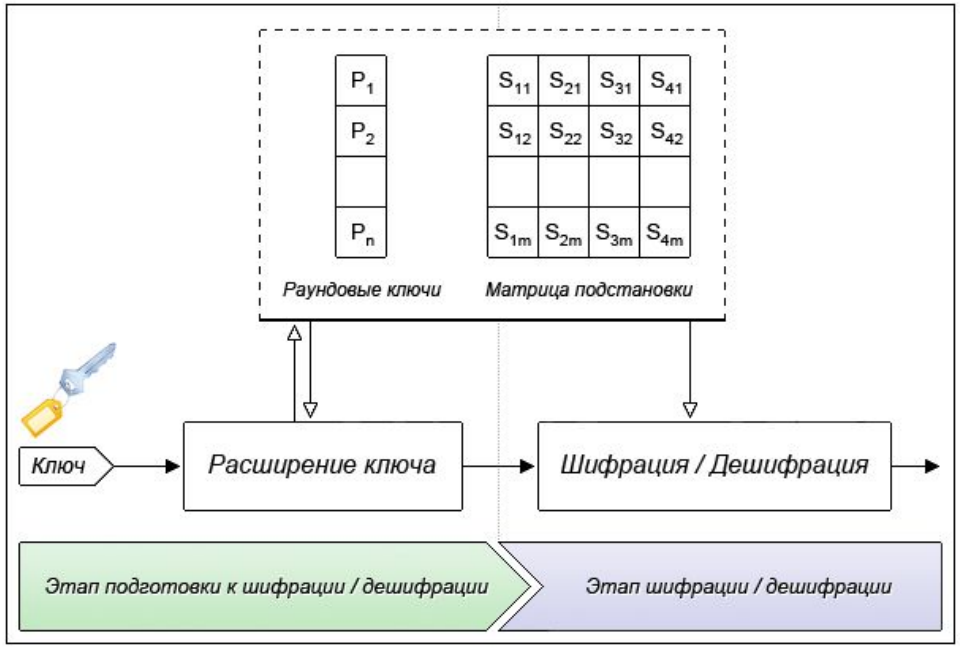
— криптографический алгоритм, реализующий блочное симметричное шифрование с переменной длиной ключа. Разработан Брюсом Шнайером в 1993 году. Представляет собой сеть Фейстеля.

Выполняется на простых и быстрых операциях: XOR, подстановка, сложение. Является незапатентованным и свободно распространяемым.

ОПИСАНИЕ АЛГОРИТМА **BLOWFISH**

Алгоритм состоит из двух частей: расширение ключа и шифрование данных. На этапе расширения ключа исходный ключ (длиной до 448 бит) преобразуется в 18 32-битовых подключей и в 4 32-битных S-блока, содержащих 256 элементов. Общий объём полученных ключей равен (18+256*4)*32=33344 бит или 4168 байт.

На этапе расширения ключа, исходный ключ преобразуется в матрицу раундовых ключей (P) и матрицу подстановки (S, Substitution-box) (или замены), общим объемом в 4168 байт. По всей вероятности, этим «расширением» (от 448 бит до 4168 байт) и объясняется выбор названия алгоритма Blowfish.



Blowfish показывает более высокие результаты при использовании кэша для хранения всех подключей. В этом случае он опережает алгоритмы DES, IDEA. На отставание IDEA влияет операция умножения по модулю 2^32+1 Скорость Twofish может быть близка по значению к Blowfish за счёт большего шифруемого блока.

Хотя Blowfish по скорости опережает некоторые свои аналоги, но при увеличении частоты смены ключа основное время его работы будет уходить на подготовительный этап, что в сотни раз уменьшает его эффективность.

TWOFISH

— симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа до 256 бит. Число раундов 16. Разработан группой специалистов во главе с Брюсом Шнайером. Алгоритм разработан на основе алгоритмов Blowfish, SAFER и SQUARE.

Отличительными особенностями алгоритма являются использование предварительно вычисляемых и зависящих от ключа узлов замены и сложная схема развёртки подключей шифрования. Половина n-битного ключа шифрования используется как собственно ключ шифрования, другая — для модификации алгоритма (от неё зависят узлы замены).

Алгоритм построен практически по классической схеме сетей Файстела, единственным отличием является наличие в схеме блоков циклического сдвига на 1 бит, однако они могут быть легко внесены внутрь основного преобразования, задаваемого функцией *F*

ОПИСАНИЕ АЛГОРИТМА **TWOFISH**

Twofish разбивает входной 128-битный блок данных на четыре 32-битных подблока, над которыми, после процедуры входного отбеливания (input whitening), производится 16 раундов преобразований. После последнего раунда выполняется выходное отбеливание (output whitening).

шифрование является обратимым процессом, где вы можете вернуть свои исходные данные.

хэширование-это односторонний процесс, который может свести все ваши данные к 20-байтному"*fingerprint*"