**DES:**

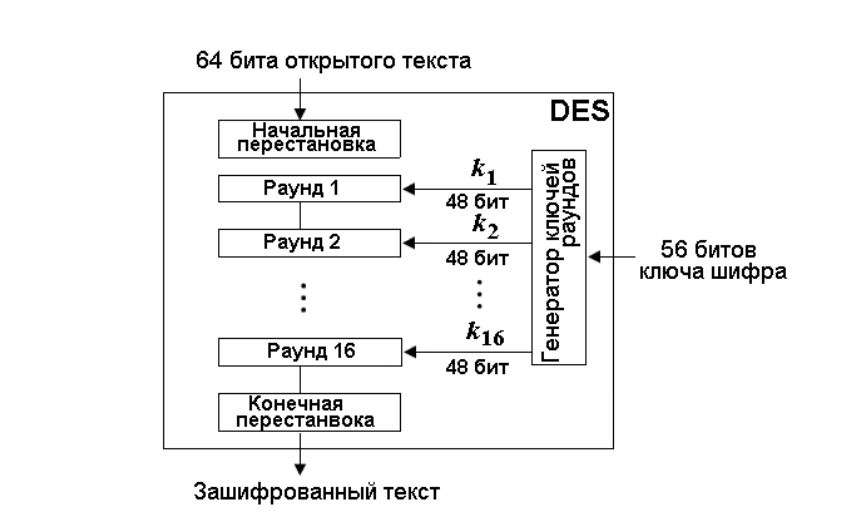
DES (англ. Data Encryption Standard) — алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3). Размер блока для DES равен 64 битам. В основе алгоритма лежит сеть Фейстеля с 16 циклами (раундами) и ключом, имеющим длину 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. Для DES рекомендовано несколько режимов:

* ECB (англ. electronic code book) — режим «электронной кодовой книги» (простая замена);
* CBC (англ. cipher block chaining) — режим сцепления блоков;
* CFB (англ. cipher feed back) — режим обратной связи по шифротексту;
* OFB (англ. output feed back) — режим обратной связи по выходу;
* Counter Mode (CTR) — режим счётчика.

Прямым развитием DES в настоящее время является алгоритм Triple DES (3DES). В 3DES шифрование/расшифровка выполняются путём троекратного выполнения алгоритма DES.

**Общие положения**

Для шифрования DES принимает 64-битовый открытый текст и порождает 64-битовый зашифрованный текст и наоборот, получив 64 бита зашифрованного текста, он выдает 64 бита расшифрованного. В обоих случаях для шифрования и дешифрования применяется один и тот же 56-битовый ключ.



**Структура DES**

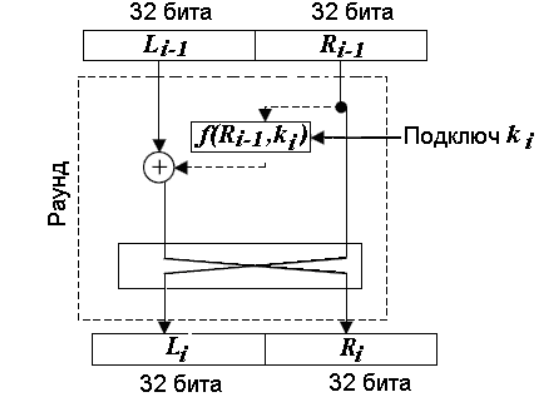
Процесс шифрования состоит из двух перестановок, которые называют начальной и финальной (конечной) перестановками, и 16 раундов Фейстеля. Каждый раунд использует различные сгенерированные 48-битовые ключи.

**Начальная IP и конечная IP-1 перестановки**

На вход каждой из них поступает 64 бита, которые затем переставляются в соответствии с заданными таблицами. Эти перестановки взаимно обратны. Другими словами, 58-й бит на входе начальной перестановке переходит в 1-ую позицию на выходе из нее. А финальная перестановка 1-ый входной бит переведет в 58-ую позицию на выходе. 

**Раунды DES**

DES использует 16 раундов. Каждый раунд DES применяет шифр Фейстеля, как это показано на рисунке



Раунд принимает полублоки Li−1 и Ri−1 от предыдущего раунда (или начального блока перестановки) и создает полублоки Li и Ri для входа в следующий раунд (или конечный блок перестановки). Все необратимые элементы сосредоточены в функции ƒ(*Ri-1,ki*)

**Генерация ключей**

DES создает 16 раундовых ключей i k по 48 битов из ключа k шифра на 56 битов. Однако, чтобы задать ключ шифра надо среди 56 битов ключа дополнительно вписать 8 битов в позиции 8,16,...,64 для проверки четности таким образом, чтобы каждый байт содержал нечетное число единиц. С помощью этой операции выявляют ошибки при обмене и хранении ключей. Ключевое расписание состоит из этапов: 1). Перестановка сжатия для удаления битов проверки – из 64- битового ключа удаляют биты 8,16,24, 32,…,64 и переставляет остальные биты согласно таблице (в ходе перестановки сохраняется нумерация битов расширенного ключа).



2) После перестановки 56 битов ключа делятся на два блока C0 и D0 по 28 бит каждый. Дале для генерации раундовых ключей из блоков C0 и D0 с помощью операции циклического сдвига влево на 1-2 бита строятся блоки Ci и Di , *i* =1,2,...,16 . В раундах 1,2,9 и 16 смещение – на 1 бит, в других раундах — на 2 бита. После определения блоков Ci и Di биты этих блоков объединяются в один ключ на 56 битов.



3) Перестановка сжатия (P-бокс, таблица) изменяет 56 битов на 48 битов, которые образуют раундовый ключ.

