Блочний шифр – різновид симетричного шифру, який оперує із групами біт фіксованої довжини – блоками. Серед популярних блочних шифрів можна назвати шифри DES, AES, Lucifer, ГОСТ 28147-89. Як казав Нільс Фергюсон – «В нас є одне зауваження до шифру AES: ми не довіряємо його безпеці. Хвилює нас найбільше його проста алгебраїчна структура, чого немає в жодному шифрі. Ми не маємо поняття, веде це до атаки чи ні, але незнання це достатня причина, щоб скептично відноситись до шифру AES». Через це розглядатись в подальшому він не буде. ГОСТ був стандартом на СНГ просторі. Шифр DES використовували, як стандарт протягом багатьох десятиліть по всьому світу, тому він буде представником блочних шифрів.

DES має розмір блоку 64 біт та розмір ключа 56 біт. Через маленький розмір ключа існує можливість по дешифруванню цього алгоритму шифрування за допомогою повного підбору ключа. В основу роботи цього шифру була узята сітка Фейстеля. Перед початком шифрування потрібно сформувати ключ. Далі блок відкритого тексту проходить через 16 раундів шифрування, але на початку та у кінці своєї роботи текст проходить через початкову перестановку. На кожному раунді блок ділиться на дві частини по 32 біти в кожній, та права частина проходить через спеціальну функцію, після чого міняється місцями із лівою частиною.

Спеціальна функція працює за лінійний час, тому через те, що вона застосовується до кожного з блоків, увесь алгоритм працює за квадратний час, а якщо розглядається покращена версія DES-у – 3DES, то час роботи збільшується ще в три рази. Через велику асимптотику роботи цього шифру стає неможливо користуватися їм для шифрування великих рядків (порядку символів та більше).

Шифр DES має достатньо-гарну криптостійкість, бо для методів що до його дешифрування потрібно як найменш мати пар відкритого тексту та шифротексту. Але пошук такої кількості пар відкритого тексту та шифротексту досить складна задача.