الگوریتم Data Encryption Standard (DES)

یک الگوریتم رمزنگاری متقارن است یعنی در رمزنگاری DES فرستنده و گیرنده از یک کلید مشترک استفاده می کنند.رمزنگاری DES شامل چندین تكرار است که از هر دو تكنیك جابه‌جایی و جایگزینی است. در این الگوریتم حفظ كلید بین فرستنده و گیرنده پیغام به صورت محرمانه بسیار مهم است زیرا الگوریتم در اختیار همگان است و در صورت لو رفتن كلید، هر كسی می‌تواند پیغام محرمانه را ببیند. به همین جهت در رمزنگاری DES معمولاً عمر كلید به اندازه عمر تراكنش است.

کلید در این الگوریتم یك توالی هشت بایتی است كه هر بایت شامل یك كلید هفت بیتی و یك بیت توازن (Parity) است. پس این کلید ۶۴ بیتی می باشد. تنها از ۵۶ بیت این کلید استفاده مؤثر می شود و ۸ بیت آن بیت parity می باشد.

لگوریتم رمزنگاری DES متن اصلی را به بلوکهای ۶۴ بیتی میشکند و در هر زمانبر روی یکی از این بلوکها کار میکند.کلید DES دارای ۶۴ بیت می باشد که ۸ بیت آن توازن و ۵۶ بیت آن کلید است.در این مرحله کلید ۵۶ بیتی به دو نیمه تقسیم میشود (دو نیمه ۲۸ بیتی) و به چپ شیفت داده میشوند.بلوک ۶۴ بیتی داده خام به دو نیمه راست و چپ شکسته میشود و نیمه راستبا نتایج مرحله دوم XOR می شود.نیمه چپ داده خام و نتیجه حاصل شده از XOR در مرحله سوم برای رمزنگاری وارد این مرحله می شوند.در این مرحله دو نیمه راست و چپ جدید ساخته می شوند تا به عنوان ورودی دور (Round) بعدی مورد استفاده قرار گیرند.

نتایج مرحله پنجم به عنوان داده های ورودی وارد دور بعدی می شود و نتایج مرحله دوم نیز یه عنوان کلیدهای دور بعدی وارد می شوند و این مراحل ۱۵ مرتبه دیگر (جمعا ۱۶ مرتیه) تکرار میشوند.پس از ۱۶ دور تکرار مراحل بالا، متن رمزشده ۶۴ بیتی از الگوریتم خارج می شود.