DES یک الگوریتم رمز رمز بلوک متقارن است. DES مخفف Standard Encryption Standard است. طبق استانداردهای امروزی این الگوریتم منسوخ است. DES بر اساس شبکه Feistel ساخته شده است. الگوریتم DES از اندازه بلوک 64 بیت و اندازه کلید 56 بیت استفاده می کند. کلید 56 بیتی از طریق عملکرد کششی Key PRG به 16 کلید هر کدام از 48 بیت کشیده می شود.

*K -> (k0, k1, k3, …. k15)*

فرض کنید ما یک پیام M به طول دلخواه داریم. پیام ابتدا به بلوک های 64 بیتی تقسیم می شود

*M -> (m0, m1, m2, m3, ….mn)*

سپس هر بلوک از طریق تابع round برای 16 تکرار اجرا می شود. هر دور شامل مراحل مختلفی است که در زیر توضیح داده شده است. اگر بلوک m0 را انتخاب کنیم ، می توان آن را به یک بلوک سمت چپ 32 بیتی L0 و بلوک راست 32 بیتی R0 تقسیم کرد. مراحل زیر بر روی پارتیشن L0 اعمال می شود.

مرحله 1: برخی از تابع های توسعه f0 برای گسترش 32 بیت به 48 بیت اعمال می شود.

مرحله 2: 48 بیت حاصل با کلید k0 XOR شده و مقدار 48 بیت دیگر بدست می آید.

مرحله 3: 48 بیت حاصل به صورت منطقی در 6 بلاک تقسیم می شود.

مرحله 4: برخی از تابع های کوچک کننده s0 برای هر بلوک 6 بیتی اعمال می شود تا به بلوک های 4 بیتی تبدیل شود.

مرحله 5: این 4 بیت بلاک با هم یک بلاک 32 بیتی تشکیل می دهند که برای تکرار بعدی به R1 تبدیل می شود.

مرحله 6: R0 برای تکرار بعدی به L1 تبدیل می شود.

مرحله 7: مراحل 1-6 دوباره برای L1 و R1 با کلید k1 تکرار می شوند تا آخرین تکرار برای k15 انجام شود.

مرحله 8: 32 بیت L15 و 32 بیت R15 با هم بلوک رمزگذاری خروجی c0 حاصل برای بلوک پیام m0 را تشکیل می دهند

مرحله 9: مراحل 1-8 برای تمام بلوک های پیام m0 ، m1 ، .m ..mn تکرار می شود تا رمز c0 ، c1 ، c3 ، c ..cn حاصل شود.