**بسم الله الرحمن الرحیم**

الگوریتم DES  
رمز نگاری  
رمز نگاری در این روش براساس تغیر در قطعه ای از اطلاعات ورودی صورت میگیرد برای رمزنگاری مراحل زیر انجام میشود.   
1 - پیام اولیه به صورت قطعات 64 بیتی از ورودی اخذ میشود. درصورتی که پیام ورودی کمتر از 64 بیت باشد باقیمانده پیام تاسقف 64 بیت با بیت های تصادفی پرخواهد شد.   
2 - با استفاده از [جدول جایگزینی اولیه](https://ircrypt.com/des.php#initialpermutation) (Initial Permutation) مکان بیت های رشته ورودی جابجا خواهد شد.   
3 - در جایگشت اول, پیام به دو بخش L0,R0 تقسیم میشود   
4 - مقدار R0 به بخش L1 در مرحله بعد انتقال می یابد L1 = R0   
5 - مقدار R1 بر اساس ترکیب R1=L0 XOR F(R0,K1) تولید میشود . وظیفه تابع F در این بخش انجام عملیات اصلی رمزنگاری می باشد.   
6 - مراحل چهارم و پنجم تا 15 مرحله تکرار خواهد شد.   
7 - در مرحله شانزدهم از فرمول زیر برای محاسبه استفاده می شود:   
L16=R15   
R16=L15 XOR F(R15,K16)   
7 - در مرحله نهایی رشته بدست امده از مرحله شانزدهم, با استفاده از [جدول جایگزینی معکوس](https://ircrypt.com/des.php#inverseinitialpermutation)(Inverse Initial Permutation) مکان بیت های رشته خروجی جابجا خواهد شد   
8 - مراحل اول تا هفتم تا اتمام رشته ورودی ادامه خواهد یافت   
وظیفه تابع F در این بخش انجام عملیات اصلی رمزنگاری می باشد که که در بخش جداگانه ای توضیح داده شده است. . 

**رمزگشایی:**

برای رمزگشایی از یک متن رمزشده مانند فرایند رمزنگاری شانزده چرخه محاسباتی خواهیم داشت. چرخه های مورد استفاده به ترتیب عکس فرایند رمزنگاری اجرا خواهند شد   
R15=L16   
L15=R16 xor F(L16, K16) 