## عنوان مقاله:
بررسی سیستم رمز DES و حمله تفاضلی به آن

## محل انتشار:
دوازدهمین کنفرانس دانشجویی مهندسی برق ایران (سال: 1388)

تعداد صفحات اصل مقاله: 6

## نویسنده:
محمدعلی طبی - *دانشگاه صنعتی خواجه نصیرالدین طوسی*

## خلاصه مقاله:
در این مقاله ابتدا سیستم رمز DES و حملات انجام شده به این سیستم به طور مختصر توضیح داده می شود. سپس به بررسی یکی از مهمترین و قویترین حملات به سیستم DES یعنی حمله تفاضلی خواهیم پرداخت. در این مقاله حمله تفاضلی به سیستم DES خلاصه شده مطرح می شود. در این حمله جفت متن های رمز شده به گونه ای انتخاب می شوند که XOR متن های اصلی متناظرشان مقدار خاصی باشد. از طریق بررسی این تفاضل ها در دورهای مختلف الگوریتم DES می توان کلید سیستم را به دست آورد.

## کلمات کلیدی:
سیستم ،DES توابع s، تابع F، XOR جفت های صحیح ، جفت های ناصحیح