عنوان مقاله:
رمزگشایی با استفاده از حملات تحلیل توان

محل انتشار:
اولین کنفرانس سراسری توسعه محوری مهندسی عمران، معماری،برق و مکانیک ایران (سال: 1393)

تعداد صفحات اصل مقاله: 10

نویسندگان:
محمدمهدی غفارنسب - *دانشجوی مهندسی مخابرات رمز دانشکده و پژوهشکده مهندسی فناوری اطلاعات وارتباطات گروه رمزوامنیت دانشگاه جامع امام حسین (ع)*

پویا حبیبی ارباستان - *دانشجوی مهندسی مخابرات رمز دانشکده و پژوهشکده مهندسی فناوری اطلاعات وارتباطات گروه رمزوامنیت دانشگاه جامع امام حسین (ع)*

سیدسبحان موسوی - *دانشجوی مهندسی مخابرات رمز دانشکده و پژوهشکده مهندسی فناوری اطلاعات وارتباطات گروه رمزوامنیت دانشگاه جامع امام حسین (ع)*

خلاصه مقاله:
یکی ازموضوعات مهم و موردنیازدرحوزه جنگ الکترونیک آگاهی ازداده های دشمن است وقطعا این داده ها بایکی ازالگوریتم های رمزنگاری بصورت رمز درامده است ازاین رو مسئله رمزگشایی ازجمله نیازهای اصلی جهت دستیابی به محتوای داده هاست مدل متداول سنتی درارزیابی سیستم های رمزنگاری امنیت سیستم رمزنگاری را ازمنظرتوابع ریاضی به کاررفته درآن مورد ارزیابی و بررسی قرارمیدهد و دراین روش رمزگشایی کاری بس دشوار است این روش تاثیر فیزیکی جانبی استفاده ازاین توابع را دردنیای واقعی درنظر نمیگیرد یک مدل واقعی ترامنیت ابزار رمزنگاری راازدید حملات کانال جانبی نیز موردتوجه قرارمیدهد کانال جانبی منبعی ازاطلاعات مرتبط با پیاده سازی فیزیکی توابع رمزنگاری است که استفاده ازحملات کانال جانبی یک راه میان بردرامر رمز گشایی است دراین مقاله درابتدا تعاریف موردنیاز درحوزه رمزنگاری و رمزگشایی بیان خواهد شد درادامه به معرفی حملات سخت افزاری و انواع آنها می پردازیم سپس حملات کانال جانبی معرفی میشود و ادامه با روش رمزگشایی توسط حمله تحلیل توان اشنا خواهیم شد

کلمات کلیدی:
رمزگشایی ، حملات کانال جانبی ، حملات سخت افزاری ، حملات تحلیل توان ، پیاده سازی الگوریتم های رمزنگاری