**چکیده:**

رمزهای قالبی نوعی رمزهای کلید متقارن هستند که از مهم‌ترین ابزارهای مورد استفاده در تأمین امنیت داده‌ها و شبکه‌ها محسوب می‌شوند. این رمزها امروزه در بسیاری از سرویس‌های مرتبط با امنیت همچون احراز و صحت و حتی در سایر ابزارهای رمزنگاری همانند رمزهای دنباله‌ای توابع درهم‌ساز و کدهای احراز اصالت پیام نیز مورد استفاده قرار می‌گیرند؛ اما هدف اصلی از بکار بردن آن‌ها، تأمین محرمانگی داده‌ها است. بنابراین برای اطمینان از برآورده شدن این هدف، باید امنیت رمزهای متقارن در برابر حملات مختلف مورد ارزیابی قرار گیرد. از جمله حمله­های مهم می­توان به حمله همبستگی صفر و همچنین حمله تفاضلی ناممکن اشاره کرد. در این ارائه سعی می­کنیم به معرفی این دو حمله پرداخته و روش­های جستجوی مشخصه­های تمایزگر مربوط به این نوع حمله­ها را مختصرا توضیح دهیم.

درباره سخنران:

صادق صادقی فارغ التحصیل دکتری رمز دانشکده علوم ریاضی و کامپیوتر دانشگاه خوارزمی تهران است. عنوان رساله دکتری وی، "تحلیل خودکار رمزهای متقارن سبک وزن" بود و تحت راهنمایی دکتر نصور باقری انجام شد. از جمله زمینه های پژوهشی مورد علاقه او رمزهای متقارن است.