دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

نام دانشجو: **مریم اسلاملو**		**نام استاد راهنما:** **جناب آقای دکتر علی جهانیان**
مقطع: کارشناسی ارشد	**گرایش: معماری سیستم‌های کامپیوتری**	**رشته: مهندسی کامپیوتر**
نوع دفاع: • **دفاع پروپوزال** □ • **دفاع پایان نامه** ■ • **دفاع رساله دکترا** □		**تاریخ: یکشنبه ۲۹ آبان‌ماه ۱۴۰۱** **ساعت: ۱۷-۱۸** **مکان: دانشکده مهندسی و علوم کامپیوتر – کلاس ۱۱۷**

عنوان: ارائه یک مد رمزنگاری بلوکی جدید با استفاده از کدگذاری مبتنی بر دی اِن اِی

داوران خارجی: جناب آقای دکتر هادی سلیمانی	**داوران داخلی: سرکار خانم دکتر راضیه سالاری‌فرد**

چکیده:

امروزه با گسترش فناوری شاهد رشد روزافزون اطلاعات هستیم. از آنجایی که اطلاعات نیز همانند هر دارایی دیگری مهم است نیازمند راه‌های مطمئنی برای نگهداری و انتقال ایمن آن هستیم. یکی از بهترین راه‌ها برای انتقال امن اطلاعات، رمزنگاری است. با گسترش فناوری و دانش بشری شاهد قوی‌تر شدن راه‌های حمله به الگوریتم‌های رمزنگاری نیز هستیم؛ بنابراین تقویت الگوریتم‌های رمزنگاری نیازی اجتناب‌ناپذیر است. در این پایان‌نامه قصد داریم با استفاده از کدگذاری دی ان ای نوعی مد رمزنگاری توأم با احراز اصالت برای پیام ایجاد کنیم. با انتساب دو بیت به نام یک باز آلی می‌توان ۲۴ روش برای کدگذاری پیام دودویی به دست آورد. ما این روش‌ها را قانون نامیده و از ۱۶ قانون برای کدگذاری خود استفاده کرده ایم. هر بایت را با یکی از این قوانین کدگذاری می‌کنیم. قانون مربوط به هر بایت با توجه به قانون بایت قبلی و مقدار بایت مورد نظر محاسبه می‌شود. آخرین قانون محاسبه شده را به عنوان کد احراز اصالت پیام در انتهای پیام ذخیره کرده و همراه با پیام توسط الگوریتم رمزنگاری AES با یکی از مدهای ECB، CBC، CFB یا OFB رمز خواهیم کرد. بدون دانستن آخرین قانون، برای پیامی به طول b بایت نیاز به بررسی 16^b حالت متفاوت از رشته قوانین برای کل بایت‌های پیام است و احتمال حدودی موفقیت در حدس رشته قوانین معتبر چیزی در حدود $(85/256^b)$ خواهد بود.

بدین‌ترتیب قبل از انجام رمزگذاری، پیام را کدگذاری کرده و برای پیام ایجاد پیچیدگی می‌کنیم. پیچیدگی ایجاد شده باعث می‌شود سطح اعتماد سامانه رمزنگاری بالا رود و متن عادی لزوماً به به صورت یک به یک به متن رمزی نگاشت نشود (البته بدون در نظر گرفتن بلوک آخر متن رمزی). لازم به ذکر است که با متغیر در نظر گرفتن قوانین کدگذاری دنا، $24!/8!$ جایگشت متفاوت از قوانین را خواهیم داشت.