عنوان مقاله:
شکستن الگوریتم رمزنگاری طاهر الجمالی با استفاده از الگوریتم پلینگ هلمن

محل انتشار:
چهارمین کنفرانس ملی تحقیقات کاربردی در مهندسی برق،مکانیک،کامپیوتر و فناوری اطلاعات (سال: 1397)

تعداد صفحات اصل مقاله: 7

نویسنده:
یاشار سلامی - *دانشگاه آزاد اسلامی، تبریز، ایران،*

خلاصه مقاله:
دانش رمزنگاری بیشتر بر پایه مقدمات از قبیل تئوری اطلاعات، نظریه اعداد، لگاریتم گسسته و آمار بنا شده است. عمل تحلیل رمز به مطالعه روش ها و اصولی می پردازد که بر اساس آنها می توان بدون در اختیار داشتن کلید رمز، داده های رمزنگاری شده را از رمز خارج کرد، یا کلید رمز را به دست آورد. یک از مسئله های مورد استفاده در رمزنگاری لگاریتم گسسته است که یکی از معروف ترین این الگوریتم های الگوریتم تبادل کلید دیفی هلمن که بر این اساس طراحی شده است و سپس الگوریتم رمزنگاری طاهر الجمالی سپس آن امضا دیجیتال الجمال معرفی و طراحی گردید. با این حال رمزشکنی نیز با پیشرفت رمزنگاری از طرف محققان در حال توسعه هست. ما در این مقاله با فرض اینکه پیچیدگی زمانی الگوریتم دیفی هلمن در زمان تولید بسیار زیاد بود و برای کامپیوترهای آن زمان بسیار دشوار بوده و همین اساس الگوریتم الجمال که بر اساس دیفی هلمن طراحی شده با خیال راحت سه عدد (P,?,β) را در اختیار عموم قرار میدهد که این امر با وجود کامپیوترهای کوانتومی یک ضعف اساسی در طراحی رمزنگاری اجمال می باشد؛ زیرا می توان با استفاده از الگوریتم پلینگ هلمن که با پیچیدگی زمانی به مراتب کمتر با استفاده از یک کامپیوتر کوانتومی می توان این شکست را برای الگوریتم رمزنگاری الجمالی مطرح کرد. در این مقاله به دلیل عدم وجود کامپیوتر کوانتومی مسئله مطرح شده بر روی پردازنده معمولی اجرا شده نتایج به دست آمد نشان می دهد که الگوریتم پلینگ هلمن عملکردی بسیار خوبی به نسبت حملات جستوجوی فراگیر برای شکستن الگوریتم الجمال نشان داده است.

کلمات کلیدی:
رمزنگاری، رمزشکنی، لگاریتم گسسته