عنوان مقاله:
ارائه نظام های رمزنگاری نوین

محل انتشار:
همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات (سال: 1393)

تعداد صفحات اصل مقاله: 12

نویسندگان:
زهرا پارسیان - *دانشجوی مقطع کارشناسی ارشد گروه آموزشی فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه شاهد، تهران*

محمدعلی دوستاری - *استادیار گروه آموزشی فناوری اطلاعات، داانشکده فنی و مهندسی، دانشگاه شاهد، تهران*

مسعود مومنی تزنگی - *دانشجوی مقطع کارشناسی ارشد گروه آموزشی فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه شاهد، تهران*

خلاصه مقاله:
امروزه جاسوسی و کسب غیر مجاز اطلاعات و اخبار به یکی از مسائل مهم جهان سیاست تبدیل گردیده است. به همین دلیل ابداع روش های مقابله با این پدیده حائز اعتبار و اهمیت است و نقش بسیار مهمی در رشد و توسعه کشورها و جوامع بشری دارد. ارسال رمز گونه اطلاعات یکی از روش هایی است که می تواند در این راستا مورد استفاده قرار گیرد. در این مقاله، ضمن اشاره به برخی نظام های رمزنگاری موجود، به حاسبه احتمال گشایش تصادفی هر یک از آنها می پردازیم. سپس چند روش رمزنگاری جدید را ارائه می دهیم. آنگاه با محاسبه احتمال گشایش رمز این روش ها نشان می دهیم که هر یک، در جهت افزایش امنیت نظام های رمزنگاری موجود صورت بندی شده اند.

کلمات کلیدی:
روش هم نهشتی، روش تبدیل خطی، روش جانشینی ساده، روش هیل، احتمال