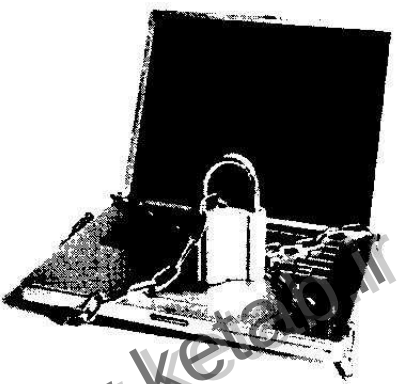
رمزنگاری اطلاعات



نویسندگان

محمدحسین روزبهانی

رضا اقدامی کلید بری

جواد خباز

سرشناسه : روزبهانی، محمدحسین، ۱۳۷۸-
عنوان و نام پدیدآور : رمزنگاری اطلاعات/نویسندگان محمدحسین روزبهانی، رضا اقدامی‌کلیدبری، جواد خباز.
مشخصات نشر : تهران: نشر بهداد، ۱۴۰۱.
مشخصات ظاهری : ۲۱۴ص.: مصور (بخشی رنگی).
شابک : ۱۵۰۰۰۰۰ریال :978-600-8203-34-6
وضعیت فهرست نویسی : فیپا
یادداشت : کتابنامه.
موضوع : رمزنگاری
Cryptography
رمزگذاری داده‌ها
Data encryption (Computer science)
شناسه افزوده : اقدامی کلیدبری، رضا، ۱۳۶۸-
شناسه افزوده : خباز، جواد، ۱۳۵۳-
رده بندی کنگره : Z۱۰۳
رده بندی دیویی : ۸/۶۵۲
شماره کتابشناسی ملی : ۸۸۵۱۵۳۳
اطلاعات رکورد کتابشناسی : فیپا

عنوان کتاب: رمزنگاری اطلاعات
مولفان : محمدحسین روزبهانی - رضا اقدامی کلیدبری - جواد خباز
ناشر: انتشارات بهداد
قطع و تیراژ: وزیری / ۱۰۰ جلد
قیمت: ۱۵۰/۰۰۰ تومان
تعداد صفحات : ۲۱۴
چاپخانه : دیانا
صحافی : دیانا
نوبت چاپ: اول
سال چاپ: ۱۴۰۱
شابک: ۹۷۸-۶۰۰-۸۲۰۳-۳۴-۶

چکیده:
امروزه در دنیای دیجیتال حفاظت از اطلاعات رکن اساسی و مهمی در تبادلات پیام ها ومبادلات تجاری ایفا می نماید. یکی از متداولترین روشهای حفاظت اطلاعات، رمز نمودن آنها است. با توجه به اهمیت این موضوع و گذار از مرحله سنتی به مرحله دیجیتال آشنایی با روش های رمز گذاری ضروری به نظر می رسد. دستیابی به اطلاعات رمز شده رشد و گسترش روزافزون شبکه های کامپیوتری، خصوصا اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، سازمانها و موسسات شده است. از این رو امنیت اطلاعات یکی از مسائل ضروری ومهم در این چرخه گردیده است. با اتصال شبکه داخلی سازمانها به شبکه جهانی، داده های سازمان ها در معرض دسترسی افراد و میزبان های خارجی قرار می گیرد. اطمینان از عدم دستیابی افراد غیر مجاز به اطلاعات حساس از مهمترین چالش های امنیتی در رابطه با توزیع اطلاعات در اینترنت است. با توجه به کاربرد روز افزون کامپیوتر حفظ امنیت و تایید صحت تصاویر نیز روز به روز اهمیت بیشتری می یابد.تصاویر مخابره شده ممکن است کاربرد هایی چون کاربرد تجاری، نظامی و یا حتی کاربرد های پزشکی داشته باشند که در صورت حفظ امنیت آنها و جلوگیری از دسترسی های غیر مجاز به این تصاویر رمز نگاری آنها را قبل از ارسال روی شبکه ضروری می کند ولی به دلیل ویژگی های تصاویر خصوصا حجم زیاد داده های تصویری و وید ئویی استفاده از الگوریتم های کلاسیک رمز نگاری متن مانند DES , RSAو.... در این موارد نا کار آمد است. چون اولا رمز کردن حجم زیاد داده های تصویری به این طریق بسیار وقت گیر خواهد بود و خصوصا در کاربرد های بلادرنگ عملی نیست و دومین مشکلی که این الگوریتمها دارند طول کلید آنهاست که با توجه به حجم داده های رمز شده استفاده از کلید های با طول محدود باعث ضربه پذیری روش در برابر حملات متن رمز شده می گردد. امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم های اطلاعاتی از فعالیت های غیرمجاز. این فعالیت ها عبارتند از دسترسی، استفاده، افشا، خواندن، نسخه برداری

یا ضبط، خراب کردن، تغییر، دستکاری. در این کتاب ضمن بررسی الگوریتم های رمز نگاری کلید عمومی(نامتقارن) و کلید خصوصی(متقارن)، جنبه های گوناگون کلید عمومی مورد بررسی قرار می گیرد و ویژگی های هر کدام بیان می گردد.

فهرست مطالب