

رمزنگاری اطلاعات



نویسندگان

محمد حسین روزبهانی

رضا اقدامی کلید بری

جواد خباز

سرشناسه : روزبهانی، محمدرحیم، ۱۳۷۸-
عنوان و نام پدیدآور : رمزنگاری اطلاعات/نویسندگان محمدرحیم روزبهانی، رضا اقدامی کلیدیری، جواد خباز.
مشخصات نشر : تهران: نشر بهداد، ۱۴۰۱.
مشخصات ظاهری : ۲۱۴ص: مصور (بخشی رنگی).
شابک : ۹۷۸-۶۰۰-۸۲۰۳-۳۴-۶: ۱۵۰۰۰۰۰ ریل
وضعیت فهرست نویسی : فیفا
یادداشت : کتابنامه.
موضوع : رمزنگاری
Cryptography
رمزگذاری داده‌ها

Data encryption (Computer science)

شناسه افزوده

عنوان کتاب: رمزنگاری اطلاعات
مؤلفان: محمدحسین روزبهانی - رضا قدامی 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

حق چاپ برای ناشر و مولفان محفوظ است

چکیده:

امروزه در دنیای دیجیتال حفاظت از اطلاعات رکن اساسی و مهمی در تبادلات پیام ها و مبادلات 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 و مهم 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 ویدئویی استفاده از الگوریتم های کلاسیک رمز نگاری متن مانند **DES , RSA** و... در این موارد نا کار آمد است، چون اولاً 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.

www.ketab.ir

فهرست مطالب

۱	فصل اول
۱	رمزنگاری اطلاعات
۲	مقدمه :
۵	بخش ۱
۵	مفاهیم رمز نگاری
۶	مقدمه
۶	مفاهیم پایه
۱۷	سیستمهای کلید متقارن
۱۹	سیستمهای کلید نامتقارن
۲۳	بخش ۲
۲۳	الگوریتمهای کلاسیک: مثالهایی ساده
۲۴	مقدمه
۲۴	رمز سزار
۳۰	رمزهای جانشینی ساده
۳۶	آمار زبان انگلیسی
۴۰	رمز Play fair
۴۴	کدگذاری همنوا
۴۸	رمزهای چند الفبایی
۴۹	رمزهای دیگر
۵۷	رمزهای ترانهشی
۵۹	رمز گذاری سطح بالا (Super-encryption)
۶۱	نتایج

پیوست	۶۲
مقدمه	۶۲
اعداد دودویی	۶۲
حساب پیمانه ای	۶۴
بخش ۳	۶۹
رمزهای غیرقابل شکست	۶۹
امنیت کامل	۷۲
One-time pad	۷۶
بخش ۴	۸۱
الگوریتمهای مدرن	۸۱
مقدمه	۸۲
رشته های بیتی	۸۲
رمزهای جریانی	۸۶
رمزهای بلاکی (روش ECB)	۹۰
توابع در همازی	۹۶
سیستمهای کلید عمومی	۹۷
فصل دوم	۱۰۳
اتوماتای سلولی	۱۰۳
مقدمه	۱۰۴
بخش ۱	۱۰۵
بخش ۲	۱۲۱
انواع CA	۱۲۲
- اتوماتای سلولی با صفر بعد ۱ - مقدمات	۱۲۲
- آنتروپی شانن	۱۲۳

۱۲۵	- اتوماتای سلولی دو بعد
۱۲۶	- اتوماتای سلولی مصرفی نوع خاصی از CA
۱۲۷	- اتوماتای سلولی ژنتیکی
۱۲۹	- اتوماتای سلولی ژنتیکی
۱۳۱	- مدل یادگیری Q سلولی
۱۳۲	- یادگیری Q
۱۳۳	- سلولی Q یادگیرنده
۱۳۷	بخش ۳
۱۳۸	مدل‌های ساده CA
۱۳۸	- مدل رشد
۱۳۹	- مدل رقابتی
۱۴۰	- مدل ترافیکی یک بعدی
۱۴۵	بخش ۴
۱۴۶	کاربرد CA
۱۴۶	- CA به عنوان فیلتر تصاویر دیجیتالی
۱۴۷	- CA به عنوان مدلی برای شناسایی مرزها در تصاویر دیجیتالی
۱۴۸	- مدل‌های ترافیک دو بعدی
۱۵۵	- شبیه‌سازی فرآیند نفوذ سموم شیمیایی در خاک به کمک اتوماتای یادگیر سلولی
۱۶۵	- شبیه‌سازی تبخیر آب در حضور محلول با استفاده از اتوماتای سلولی
۱۷۵	بخش ۵
۱۷۵	نتیجه‌گیری
۱۷۶	نتیجه‌گیری
۱۷۷	فصل سوم
۱۷۷	رمزنگاری به کمک اتوماتای سلولی