ریاضیات

در

نظریه رمزگذاری

مرضیه راعی

سرشناسه : راعی، مرضیه، ۱۳۶۲-
عنوان و نام پدیدآور : ریاضیات در نظریه رمزگذاری
مشخصات نشر : تهران: آرنا، ۱۳۹۴.
مشخصات ظاهری : ۱۶۳ ص.
شابک : 978-600-356-254-7
وضعیت فهرست نویسی : فیپای مختصر
یادداشت : فهرستنویسی کامل این اثر در نشانی: http://opac.nlai.ir قابل دسترسی است
شماره کتابشناسی ملی : ۳۸۰۳۳۷۸

عنوان : ریاضیات در نظریه رمزگذاری
مولف : مرضیه راعی
ناشر : آرنا
ناظر چاپ : مهدی اکبری
چاپ : اول ۱۳۹۴
شمارگان : ۱۰۰۰ نسخه قیمت: ۱۱۰۰۰ تومان
شابک : ۹۷۸-۶۰۰-۳۵۶-۲۵۴-۷

www.a r n a p u b.com

فهرست مطالب

مقدمه مؤلف

چندین دلیل برای این که چرا اطلاعات به رمزگذاری نیاز دارند، وجود دارد. یک دلیل پنهان کردن اطلاعات یا غیر قابل دسترس نمودن اطلاعات برای کاربران غیر مجاز است. این قبیل رمزها موضوع رمزشناسی هستند. دلیل دیگر فشرده سازی اطلاعات برای کاهش مقدار فضایی است که برای حفظ آن‌ها نیاز است. مثلاً رمزهای موسوم به *'ZIP'* برای فشرده‌سازی فایل‌ها روی هارد دیسک کامپیوتر به کار می‌روند. این نوع رمزگذاری‌ها با *نظریه‌ی اطلاعات* پوشش داده می‌شوند. سومین و در حقیقت جالب‌ترین دلیل کاربرد رمزها، افزایش ایمنی در ارسال اطلاعات است. تجهیزات الکترونیکی مورد استفاده در ارسال اطلاعات و پردازش داده‌ها مستعد انواع گوناگونی از خطا هستند. به عنوان مثال یک نوع از این خطاها هنگام ارسال از یک مکان به مکان دیگر رخ می‌دهد و در نتیجه موجب می‌شود که اطلاعات اشتباه تفسیر شده یا مفقود شوند. از این‌رو تمایل داریم راه‌هایی برای تشخیص و در صورت امکان تصحیح این خطاها بیابیم.

نظریه‌ی رمزگذاری در سال ۱۹۴۸ توسط ریچارد همینگ پایه ریزی شد. هنگامی‌که همینگ در آزمایشگاه بل روی یک دستگاه مکانیکی متصل به کامپیوتر کار می‌کرد، دریافت که اغلب زمان‌های از دست رفته بر اثر ناتوانی کامپیوتر مربوط به خطاهاست. یک خطای منفرد می‌تواند تشخیص داده شود، اما هنگامی‌که کامپیوتر از یک عمل رایج نسخه برداری می‌کند و با عمل دیگری شروع به کار می‌کند، هرگز نمی‌تواند به حالت اولیه باز گردد.

همینگ تحقیقات در این رابطه را شروع کرد و یک مدل ریاضی برای تصحیح خطای منفرد دودویی را مطرح کرد. ایده‌ی مطرح شده، ساده و ظریف بود؛ با جایگزینی هوشمندانه‌ی رقم‌های بررسی توازن در بین رقم‌های پیام رمز شده، دنباله ای از بررسی‌های توازن شامل اعدادی که در آن‌ها خطا رخ داده بود، تولید می‌کرد. دیگر ریاضیدانان و دانشمندان علوم کامپیوتر به طور همزمان با مشکلات مشابهی مواجه شدند. در برابر گروهی از رمزها که در آن‌ها به تصحیح خطاهای منفرد و چندگانه پی برده بودند، ایده های همینگ را اتخاذ کردند. رمزهای متفاوت نیاز به شرایط مختلفی دارند. رمزهای پیچیده اطلاعات را بهتر ارائه می‌کنند، اما سبب کاهش کارآیی می‌شوند. اگر

خسارت سبب مفقود شدن کمی از اطلاعات شود، یا احتمال رخ دادن خطا بزرگ نباشد، رمزهای ساده نیز می‌توانند مورد استفاده قرار گیرند.

نظریه‌ی رمزگذاری مثال قابل توجهی از کاربرد ریاضیات محض در حل مسائل علمی است. اگر چه برخی از رمزهای ساده دارای ساختاری هستند که نیاز زیادی به ریاضیات ندارد، با این حال ویژگی رمزها از کشفیات ریاضیات است. مانند هسته‌ی ارسال خطی که اثبات فعالیت های واقعی را ممکن می‌سازد و بدون این گونه برهان‌ها، رمزها در حقیقت بدون استفاده می‌باشند. علاوه بر این، ریاضیات موجب ایجاد رمزها در ابعاد دیگر می‌شود و با افزایش قابلیت تصحیح خطا، اثبات‌هایی را برای موجودیت یا عدم موجودیت رمزها ارائه داده است.

مطلب دیگری که تا حدی مورد نظر می‌باشد، کدهای کامل است. کدهای کامل دارای ویژگی‌های هندسی هستند که به وسیله‌ی بسته هایی معین می‌شوند؛ مجموعه‌ی نقاط S در فضای n ـ بعدی را در نظر می‌گیریم، که هر رمز (کامل) زیر مجموعه‌ای از گوی های n ـ بعدی مجزایی حول هر عنصر رمز است که می‌تواند تمامی نقاط S را در برگیرد. در حقیقت هر نقطه در یک گوی قرار دارد. این مطلب از آن جهت جالب است که ریاضیدانانی که بر روی بسته‌ی گوی‌ها تحقیق می‌کنند، با بسته‌های گوناگونی مواجه می‌شوند که در این صورت می‌توانند بهترین بسته را برای ابعاد مشخصی تشخیص دهند.

در حالت کلی، مسئله‌ی اساسی نحوه‌ی بسته بندی گوی‌های n ـ بعدی مجزا به فضای n ـ بعدی می‌باشد به طوری که مقدار فضای غیر قابل استفاده مینیمم شود. این مسئله هنوز برای فضاهای با بعد $n > 3$ غیر قابل حل باقی مانده است.

در این مبحث سعی شده است مفهوم اطلاعات، رمز، رمزگذاری بدون اختلال و همچنین رمزگذاری همراه با اختلال و متعاقب آن رمزگشایی از این گونه سیستم‌ها از نقطه نظر ریاضیات مورد بررسی قرار گیرد. در نظریه‌ی رمزگذاری به طور کاملاً مشخص از ریاضیات محض و به ویژه جبر و به طور جزئی تر جبر خطی و میدان های دودویی استفاده شده است. قضایا و احکام اساسی نظریه‌ی رمزگذاری دارای اثبات‌های ریاضی‌گونه با کاربرد اصول ریاضیات می‌باشند.

از نظریه‌ی رمزگذاری به طور تخصصی و کاربردی در مخابرات، صنایع الکترونیکی، کامپیوتر، سیستم‌های کامپیوتری و صنایع دفاع استفاده می‌شود.

مجموعه‌ی حاضر شامل مباحثی از نظریه‌ی رمزگذاری و رمزگشایی سیستم‌های رمزی و کاربرد مستقیم ریاضیات در این علم نوین می‌باشد. ریاضیات و به خصوص ریاضیات محض کاربرد زیادی در این موضوع دارند، و به دلیل نقش بنیادی علم ریاضی در پیشبرد فنون رمزگذاری، آشنایی علاقمندان و صاحب نظران در زمینه‌ی ریاضیات با نظریه‌ی رمزگذاری مفید به نظر می‌رسد.

همچنین کمبود مراجع فارسی در رابطه با نظریه‌ی رمزگذاری اینجانب را بر آن داشت هر چه مصمم‌تر در رابطه با این موضوع فعالیت نموده و مجموعه‌ای حتی الامکان مختصر و مفید را فراهم آورم. امید است حاصل این تلاش برای خوانندگان محترم مثمر ثمر واقع شود.