

۱۳۸۲۹۹



پرتکا اشتراک از

گردآوری

دکتر علی نخعی امروودی، دکتر علیرضا شجاعی فرد، محمد رستمی

گروه ریاضی و آمار، دانشگاه جامع امام حسین (ع)

پاییز ۱۳۹۶

سرشناسه : نخعی امرودی، علی، ۱۳۶۴ -
 عنوان و نام پدیدآور : پروتکل اشتراک راز / گردآوری علی نخعی امرودی، علیرضا شجاعی فرد، محمد رامشینی.
 مشخصات نشر : کرج: پیدار، ۱۳۹۶.
 مشخصات ظاهری : ۱۵۶ ص.
 شابک : ۹۷۸-۶۰۰-۴۹۹-۲۰۱-۳
 وضعیت فهرست نویسی : فیبا
 موضوع : شبکه‌های کامپیوتری — تدابیر ایمنی
 موضوع : Security measures — Computer networks
 موضوع : سامانه‌های امنیتی — نرم‌افزار
 موضوع : Security systems — Software
 موضوع : رمزنگاری
 موضوع : Cryptography
 شناسه افزوده : شجاعی فرد، علیرضا، ۱۳۶۴ -
 شناسه افزوده : رامشینی، محمد، ۱۳۶۰ -
 رده بندی رنگره ۵ K ۵۹/۵۱ / ۳۹۶۴ پ
 رده بندی دیویی : ۸/۰۱
 شماره کتابشناسی : ۵۱۱۰۳۹



پروتکل اشتراک راز

مولفان: محمد رامشینی / علیرضا شجاعی فرد / علی نخعی امرودی

چاپ: پیشگام | نوبت چاپ: اول ۱۳۹۶ | شمارگان: ۱۰۰۰ جلد | قیمت: ۱۵۰۰ تومان

مرکز پخش: انتشارات پیدار

آدرس: رجایی شهر خ هفتم غربی فاز ۲- پلاک ۹۰ | تلفن: ۳۴۲۱۰۵۰۳-۳۴۲۱۰۵۰۷-۲۶

کلیه حقوق برای ناشر محفوظ است.

از انواع پروتکل‌ها می‌توان به موارد زیر اشاره نمود: الف) پروتکل‌های شناسایی و احراز اصالت موجودیت‌ها^۱؛ ب) پروتکل‌های انسانی^۲ (قوانینی که از اثر فعل و انفعالات انسانی پیروی می‌کند. مانند: سوال کردن در کلاس درس)؛ ج) پروتکل‌های شبکه‌ای (مجموعه قوانینی که در شبکه‌های ارتباطی استفاده می‌شود. مانند: *HTTP, FTP*).

همواره ارتباط امن و خصوصی داشتن به نحوی که دیگران هیچ اطلاعاتی از آن بدست نیاورند، یکی از مده‌تاس‌ها و تحقیقات مراکز نظامی را به خود اختصاص داده است. در گذشته برای داشتن ارتباط امن، سیستم رمزهای ساده‌ای ابداع شده بود که به کمک آن می‌توانستند یک ارتباط تقریباً امن داشته باشند. با ظهور رایانه‌ها که عملیات زیادی را در کسری از ثانیه انجام می‌دهند سیستم رمز قبلی عملاً شکسته شدند و نیاز به سیستم رمزهای جدید به وجود آمد به طوری که امروزه تقریباً هر ارتباطی دارای نوعی رمزنگاری است.

پروتکل‌های امنیتی^۳ یکی از مباحث مهم در رمزنگاری می‌باشد. پروتکل اشتراک راز یا به عبارتی طرح اشتراک راز یکی از پروتکل‌های مهم در رمزنگاری است. در سال‌های اخیر محققان بسیاری از جمله محققانی از کشور عزیز ایران، بر روی طرح‌های اشتراک راز کار کرده‌اند. در این کتاب ابتدا مقدماتی درباره انواع پروتکل‌ها بیان خواهیم کرد

^۱ Identification and entity authentication protocols

^۲ Human protocols

^۳ Security Protocols

سپس به معرفی پروتکل تسهیم راز خواهیم پرداخت. امید آن می‌رود که این کتاب بتواند راهی نو در تحقیقات رمزنگاری، برای محققان جوان بازگشاید.

دکتر علی نخعی امروزی، دکتر علیرضا شجاعی فرد، محمد رامشینی

پاییز ۱۳۹۶

www.ketab.ir

فهرست مطالب

۱	فصل اول: مقدمه
۲	۱-۱ پروتکل
۲	۱-۱-۱ مفهوم پروتکل
۹	۲-۱-۱ پروتکل ارتباطات
۱۲	۳-۱-۱ مقدمه ای بر پروتکل های شبکه
۲۴	۴-۱-۱ پروتکل بارز
۲۵	۵-۱-۱ پروتکل اینترنت
۲۷	۶-۱-۱ پروتکل اینترنت
۲۸	۷-۱-۱ پروتکل اینترنت سریع
۲۸	۸-۱-۱ پروتکل اینترنت گیگابیت
۲۹	۹-۱-۱ پروتکل صحبت محلی
۳۰	۱۰-۱-۱ پروتکل حلقه علامت
۳۱	۱۱-۱-۱ پروتکل FDDI
۳۱	۱۲-۱-۱ پروتکل ATM
۳۲	۱۳-۱-۱ دیگر پروتکل های شبکه
۳۴	۱۴-۱-۱ پروتکل اینترنت
۳۹	۲-۱ مفاهیم اولیه رمزنگاری

۳-۱ رمزنگاری متقارن ۴۹

۴-۱ رمزنگاری نامتقارن ۵۰

۵-۱ تابع درهم ساز ۵۸

۶-۱ انواع حملات ۶۲

۷-۱ ادغامی دیجیتال ۶۵

فصل سوم: طرح اشتراک راز کلاسیک ۷۲

۱-۲ بررسی اشتراک راز شمشیر ۷۴

۲-۲ اشتراک راز مبتنی بر دستگاه معادلات ۸۲

۳-۲ اشتراک راز مبتنی بر درونمایی ۹۱

۴-۲ اشتراک راز وزن دار ۱۰۰

۵-۲ اشتراک راز بلکلی ۱۰۶

فصل سوم: طرح اشتراک راز پساکوانتومی ۱۰۸

۱-۳ اشتراک راز مبتنی بر سیستم رمز *GGH* ۱۰۹

۲-۳ اشتراک راز مبتنی بر سیستم رمز *NTRU* به کمک توابع چندمتغیره ۱۱۱

۳-۳ تحلیل امنیت و پیچیدگی محاسباتی طرحهای معرفی شده ۱۱۵

۱۱۶

مراجع