بسم الله الرحمن الرحیم

آشنایی با رمزنگاری

کریستف پار و جان پلت‌سُل

مترجم:

دکتر ناصر زمانی

عضو هیأت علمی دانشگاه محقق اردبیلی

سرشناسه	:	پار، کریستف، ۱۹۶۳ - م. Paar, Christof
عنوان و نام پدیدآور	:	آشنایی با رمزنگاری
مشخصات نشر	:	تهران : کتاب دانشجو، ۱۳۹۴.
مشخصات ظاهری	:	۴۲۶ص.
شابک	:	۲۰۰۰۰۰ریال: 978-600-5061-45-1
وضعیت فهرست نویسی	:	فیپای مختصر
یادداشت	:	فهرستنویسی کامل این اثر در نشانی: http://opac.nlai.ir قابل دسترسی است
شناسه افزوده	:	پلت سل، جان
شناسه افزوده	:	زمانی، ناصر، ۱۳۴۹ - ، مترجم
شماره کتابشناسی ملی	:	۳۸۲۸۴۶۲

کتاب دانشجو

محل فروش: نشر کتاب دانشجو

تهران، خیابان انقلاب، نبش خیابان فخر رازی، پلاک ۱۳۵۲

تلفن: ۶۶۴۹۳۱۶۵

عنوان کتاب: آشنایی با رمزنگاری

ناشر: انتشارات کتاب دانشجو

مترجم - ناصر زمانی

ویراستار: حسین نوین

نوبت چاپ: اول ۱۳۹۴

شمارگان: ۵۰۰ جلد

چاپ: مبتکران

صحافی: مبتکران

شابک: ۱-۴۵-۵۰۶۱-۶۰۰-۹۷۸

قیمت: ۲۰،۰۰۰ تومان

پیش‌گفتار مترجم

رمزنگاری علم پنهان‌نویسی، تبادل و نگه‌داری محرمانه اطلاعات است. پیشرفت سریع فناوری اطلاعات و انجام الکترونیکی بسیاری از داد و ستدها، بر اهمیت و نقش کلیدی این علم افزوده است. می‌توان گفت که امروزه الگوریتم‌های رمز آنچنان عمومی و فراگیر شده‌اند که افراد زیادی باید از نحوه کارکرد و کاربرد عملی آنها در زندگی روزمره آشنایی داشته باشند. الگوریتم‌های رمزنگاری براساس نظریهٔ اعداد، ساختارهای جبری، توابع ریاضی، و به طور خاص توابع یک طرفه بیان می‌شوند. بر این اساس کتاب حاضر ضمن اشاره‌ای مختصر به زمینه‌های ریاضی، بیش‌تر به جنبه‌های کاربردی رمزنگاری می‌پردازد. این کتاب را می‌توان به عنوان یک منبع اصلی در درس رمزنگاری در مقطع کارشناسی رشته‌های علوم ریاضی، کامپیوتر و برق در نظر گرفت. افزون بر این با توجه به نحوهٔ ارائهٔ مطالب و اجتناب نویسندگان از درگیری با مطالب فنی ریاضی، تمام شاغلان و کاربران حوزه فناوری اطلاعات و صنعت اینترنت می‌توانند از آن استفاده نمایند.

با عنایت به آن‌چه ذکر شد، ترجمهٔ این اثر را تقدیم به همهٔ علاقه‌مندان و دانشجویان می‌نمایم و امیدوارم مورد استفاده قرار گیرد.

در معادل‌یابی واژگان فنی و تخصصی سعی کافی شده است. لکن در مواردی ممکن است لغت‌ها و واژگان تازه مطابق سلیقهٔ اهل فن نبوده و یا هنوز رایج نباشند. تذکر هر نوع انحراف و لغزش از بهترین معادل فارسی مورد استقبال اینجانب است.

از حوزه معاونت پژوهشی دانشگاه محقق اردبیلی به خاطر پی‌گیری فرآیند داوری کتاب و حمایت‌های مالی، از آقای حسن قربان‌زاد به‌خاطر انجام امور تایپی و صفحه‌آرایی کتاب و از همکار محترم آقای دکتر حسین نوین که کار ویراستاری کتاب را انجام دادند، تقدیر می‌کنم.

انجام این کار، بدون تشویق‌ها و حوصلهٔ خانوادهٔ صبورم ممکن نبود و لازم است از حمایت‌های آنها نیز به طور ویژه سپاسگزاری کنم.

ناصر زمانی

دانشگاه محقق اردبیلی

بهار ۹۳

پیش‌گفتار

پژوهش‌های دانشگاهی در رمزشناسی از اواسط دهه ۱۹۷۰ شروع شد که امروزه یک شاخهٔ پژوهشی بالغ، توأم با سازمان تخصصی ثابت (IACR، موسسه بین‌المللی پژوهش‌های رمزشناسی)، هزاران پژوهش‌گر و کنفرانس‌های بین‌المللی متعددی است. هر ساله بیش از هزار مقاله علمی در مورد رمزشناسی و کاربردهای آن چاپ می‌شوند.

تا دهه ۱۹۷۰، رمزنگاری اغلب در کاربردهای سیاسی، نظامی و دولتی یافت می‌شد. در طول دهه ۱۹۸۰، شرکت‌های مالی و ارتباطی، ابزارهای رمزنگاری را مستقر نمودند. اولین بازار بزرگ برای کاربردهای رمزنگاری، سیستم گوشی‌های موبایل دیجیتالی در اواخر دهه ۱۹۸۰ بود. امروزه هر فردی رمزنگاری را به طور دائم به کار می‌برد. باز کردن درب خودرو یا پارکینگ با ابزار کنترل ریموت، اتصال به یک بی‌سیم LAN، خرید کالا با کارت اعتباری یا کارت حساب شخصی در فروشگاه مصالح ساختمانی یا از طریق اینترنت، نصب به‌روز رسانی نرم‌افزار، تلفن از طریق IP، یا پرداخت هزینه حمل و نقل در یک سیستم مسافرتی عمومی نمونه‌هایی از آن هستند. تردیدی وجود ندارد که حوزه‌های کاربردی ضروری، مانند کنترل الکترونیکی سلامت، سیستم مکان‌یابی سراسری خودرو و ساختمان‌های هوشمند، رمزنگاری را فراگیرتر نیز خواهند ساخت.

رمزشناسی یک شاخه پرجاذبهٔ میان رشته‌ای بین علوم کامپیوتر، ریاضی و مهندسی الکترونیک است. از آنجا که رمزشناسی سریع رشد می‌کند، سروکار داشتن با تمام پیشرفت‌های آن کاری دشوار است. در ۲۵ سال اخیر، پایه‌های نظری این حوزه قوی‌تر شده‌اند. به طوری که اکنون آشنایی کاملی از تعاریف ایمنی و روش‌های اثبات ایمنی ساختارها داریم. همچنین، در حوزه رمزنگاری کاربردی شاهد پیشرفت‌های خیلی سریعی بوده‌ایم: الگوریتم‌های قدیمی شکسته شده، کنار می‌روند و الگوریتم‌ها و پروتکل‌های جدید پدید می‌آیند.

گرچه در دههٔ گذشته چندین کتاب درسی عالی در زمینهٔ رمزشناسی چاپ شده‌اند، ولی عمده تمرکز آنها روی خوانندگانی بوده است که دارای زمینهٔ قوی ریاضی باشند. به‌علاوه، پیشرفت‌های جدید زیبا و پروتکل‌های پیشرفته، وسوسهٔ افزودن موضوعات ذهنی بیش‌تری را به وجود می‌آورند. مزیت بزرگ این کتاب درسی این است که خود را به مباحثی محدود می‌کند که با شاغلان امروزی مرتبط هستند. در ضمن پیش‌نیازهای ریاضی به موارد به‌طور کامل ضروری محدود است که به طور دقیق در مواقع لازم معرفی شده‌اند. این رهیافت "کم بیش‌تر است" برای شناساندن نیازهای

تازه‌واردها در این حوزه خیلی مناسب است. زیرا که با مفاهیم اصلی و الگوریتم‌ها و پروتکل‌های مدبرانه انتخاب شده، مرحله به مرحله آشنایی پیدا می‌کنند. هر فصل راهنمایی‌های مفیدی را برای مطالعه اضافی برای آنهایی که علاقمند به توسیع و تعمیق اطلاعات خود هستند، دربر دارد.

در کل، خیلی خوشحال هستم که نویسندگان در ایجاد مقدمه‌ای با ارزش در موضوع رمزنگاری کاربردی توفیق یافته‌اند. امیدوارم که در ایجاد سیستم‌های امن‌تر بر مبنای رمزنگاری، راهنمایی برای شاغلان بوده و زمینه‌ای برای پژوهش‌های آتی در جهت کشف دنیای جذاب رمزنگاری و کاربردهای آن باشد.

بارت پرِنیل

لیوون

اگوست ۲۰۰۹

پیش‌گفتار نویسندگان

رمزنگاری به درون هر چیزی راه یافته است؛ از برنامه‌های وب و ایمیل تا گوشی‌های موبایل، کارت‌های بانکی، خودروها و حتی ایمپلنت‌های پزشکی. در آینده‌ی نزدیک کاربردهای هیجان‌انگیز جدید رمزنگاری را مانند برچسب‌های شناسایی فرکانس رادیویی (RFID)[1] برای پادجعل‌ها، یا ارتباطات خودرو به خودرو (که هم‌اکنون روی هر دوی این کاربردها کار می‌کنیم)، خواهیم دید. این وضعیت به‌طور کامل با گذشته متفاوت است که در آن رمزنگاری به طور سنتی در کابردهای معین ارتباطات دولتی و سیستم‌های بانکی پیدا می‌شد. به عنوان نتیجه‌ای از فراگیری الگوریتم‌های رمز، افراد زیادی باید از نحوه کارکرد و کاربرد عملی آنها آشنایی داشته باشند. این کتاب با تمهید یک مقدمه‌ی قابل درک در رمزنگاری جدید، این موضوع را پی می‌گیرد که برای دانشجویان و شاغلان در صنعت مناسب است.

کتاب حاضر خواننده را به‌طور کامل با نحوه کارکرد طرح‌های رمزنگاری آشنا می‌کند. مفاهیم ریاضی لازم را به نحوی معرفی می‌کنیم که برای هر خواننده‌ای با کم‌ترین زمینه قبلی در حسابان دبیرستانی قابل درک باشد. بنابراین، این کتاب به‌طور کامل مناسب کلاس‌های دوره لیسانس یا اوایل فوق‌لیسانس و کتاب مرجعی برای مهندسان و دانشوران کامپیوتر است که علاقه‌مند شناخت کامل از رمزنگاری جدید هستند.

این کتاب دارای جنبه‌های متعددی است که آن را منبع یکتایی برای شاغلان و دانشجویان قرار داده است. با معرفی اکثر الگوریتم‌هایی که در کاربردهای دنیای واقعی جدید مورد استفاده قرار می‌گیرند، روی جنبه‌های کاربردی تمرکز کرده‌ایم. برای هر طرح رمز، تخمین‌های فعلی ایمنی و توصیه‌هایی در مورد طول کلید ارائه شده است و نیز در مورد هر الگوریتم روی موضوع مهم پیاده‌سازی نرم‌افزاری و سخت‌افزاری بحث شده است؛ علاوه بر الگوریتم‌های رمز، بحث‌هایی مانند پروتکل‌های رمزنگاری مهم، روش‌های عمل، سرویس‌های ایمنی و روش‌های استقرار کلید معرفی شده‌اند. بیش‌تر بحث‌های کاملاً به روز، مانند رمزهای سبک‌وزن که برای کاربردهای محدود (از قبیل برچسب‌های RFID یا کارت‌های هوشمند) بهینه شده‌اند یا روش‌های عمل جدید نیز در این کتاب جای دارند.

بخش بحث، در انتهای هر فصل، با منابع اضافی، موضوعات فراوانی را برای مطالعه بیش‌تر فراهم می‌کند. این بخش‌ها منابع بسیار خوبی برای پروژهٔ درسی هستند. به ویژه، موقوع استفاده از آن

[1] radio frequency identifications tags

به عنوان یک کتاب درسی، سایت www.crypto-textbook.com به‌طور کامل توصیه می‌شود که خوانندگان خیلی از ایده‌های پروژه‌های درسی، لینک‌های به نرم‌افزارهای منبع باز، بردارهای آزمون، و خیلی از اطلاعات را در مورد رمزنگاری فعلی پیدا خواهند کرد. لینک درس‌های ویدیوئی موجود است.

چگونه از کتاب استفاده کنیم

موضوعات این کتاب در طول چندین سال تکامل یافته و در کلاس آزمون پس داده‌اند. این کتاب را هم برای دانشجویان سال اول فوق‌لیسانس و هم برای دانشجویان پیشرفته لیسانس و هم به عنوان یک درس محض برای دانشجویان رشته IT تدریس کرده‌ایم. می‌توان بیش‌تر محتوای کتاب را در دو نیمسال، با هفته‌ای ۹۰ دقیقه تدریس و ۴۵ دقیقه تمرین، با استاندارد ECTS تدریس نمود. در شیوه آمریکایی سه ترمی یا در شیوه اروپایی یک ترمی، باید برخی از موضوعات حذف شوند. در این‌جا چند انتخاب معقول برای یک درس یک ترمی داده می‌شوند:

برنامه آموزشی ۱ ـ تمرکز روی کاربردهای رمزنگاری: به عنوان مثال در علوم کامپیوتر یا مهندسی الکترونیک. این درس رمزنگاری یک افزوده خوبی برای درس‌های شبکه‌های کامپیوتر یا درس‌های پیشرفته‌تر در مورد امنیت است: فصل ۱؛ بخش‌های ۱.۲ ـ ۲.۲؛ فصل ۴؛ بخش ۱.۵؛ فصل ۶؛ بخش‌های ۱.۷ ـ ۳.۷؛ بخش‌های ۱.۸ ـ ۴.۸؛ بخش‌های ۱.۱۰ ـ ۲.۱۰؛ فصل ۱۱، فصل ۱۲ و فصل ۱۳.

برنامه آموزشی ۲ ـ تمرکز روی الگوریتم‌های رمزنگاری و پیش‌نیازهای ریاضی آنها: برای مثال به عنوان یک درس رمزنگاری کاربردی در علوم کامپیوتر، مهندسی الکترونیک در برنامه ریاضی دوره لیسانس. این درس رمزنگاری می‌تواند به مثابه آمادگی برای یک درس تکمیلی نظری‌تر در رمزنگاری باشد: فصل ۱؛ فصل ۲؛ فصل ۳؛ فصل ۴؛ فصل ۶؛ فصل ۷؛ بخش‌های ۱.۸ ـ ۴.۸؛ فصل ۹؛ فصل ۱۰؛ و بخش‌های ۱.۱۱ ـ ۲.۱۱.

به عنوان مهندسان تعلیم دیده، به مدت بیش از ۱۵ سال در رمزنگاری کاربردی و ایمنی کار کرده‌ایم و امیدواریم که خوانندگان نیز مانند ما شیفته این حوزه جذاب باشند.

کریستف پار

جان پلت‌سُل

بوخوم

سپتامبر ۲۰۰۹