به نام خدا

مؤسسه فرهنگی هنری
دیباگران تهران

رمزنگاری

مولف :

دکتر بهروز فروزان

مترجمین :

مهندس مادح شکری

کارشناس ارشد امنیت اطلاعات و مدرس دانشگاه

مهندس ابوالفضل یوسفی راد

کارشناس ارشد امنیت اطلاعات ،دبیر آموزش و پرورش و مدرس دانشگاه

عنوان کتاب اصلی :Cryptography and Network security

عنوان کتاب : رمزنگاری

مؤلف: دکتر بهروز فروزان

مترجمین :مادح شکری –ابوالفضل یوسفی راد

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه‌آرایی: خانم مژگان شیرین

طرح روی جلد: مجتبی حجازی

چاپ: صدف

نوبت چاپ: دوم

تاریخ نشر: ۱۳۹۸

تیراژ: ۵۰جلد

قیمت: ۱۴۰۰۰۰۰ ریال

شابک: ۳-۵۱۸-۱۲۴-۶۰۰-۹۷۸

ISBN: ۹۷۸-۶۰۰-۱۲۴-۵۱۸-۳

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، روبروی پاساژ مهستان، پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

کد پستی: ۱۳۱۴۹۸۳۱۸۵

فروشگاههای اینترنتی:

www.mftbook.ir

www.dibagarantehran.com

نشانی تلگرام:@mftbook

نشانی اینستاگرام : Dibagaran_publishing

سرشناسه :فروزان ،بهروز،۱۳۲۳-

عنوان و نام پدید آور :رمزنگاری /مولف :بهروز فروزان:مترجمان :مادح شکری، ابوالفضل یوسفی راد

مشخصات نشر: تهران- دیباگران تهران -۱۳۹۵

مشخصات ظاهری:۴۹۵ ص

شابک :۳-۵۱۸-۱۲۴-۶۰۰-۹۷۸

وضعیت فهرستنویسی : فیپا

یادداشت : کتاب حاضر ترجمه گزیده ای از Cryptography and network security است.

موضوع: شبکه های کامپیوتری – تدابیر ایمنی

موضوع : Computer networks-security measures

موضوع : رمزنگاری

موضوع:Cryptography

شناسه افزوده : شکری ،مادح،۱۳۷۱-مترجم

شناسه افزوده : یوسفی راد ، ابوالفضل،۱۳۶۵-مترجم

رده بندی کنگره: ۸۰۱۱۳۹۵ ر ۴ ف / ۵۹/ TK ۵۱۰۵

رده بندی دیویی : ۰۰۵/۸

شماره کتابشناسی ملی : ۴۵۰۵۹۷۹

فهرست مطالب

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی است که بتواند خواسته های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گستردگی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت " **اقایان مهندس مادح شکری و مهندس ابوالفضل یوسفی راد از کارشناسان ارشد امنیت اطلاعات و مدرس دانشگاه** " و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
Publishing@mftmail.com

مقدمه مترجمان

کتاب حاضر ماحصل تلاش ها و تحقیقات پروفسور بهروز فروزان، استاد ممتاز دانشکده DeAnza کالیفرنیا است، که یکی از منابع اصلی در زمینه امنیت اطلاعات می باشد. عنوان اصلی کتاب "رمزنگاری و امنیت شبکه" است، اما تصمیم گرفتیم فقط مباحث مربوط به رمزنگاری اطلاعات را به عنوان یک کتاب جداگانه ترجمه کرده و جهت مطالعه در دسترس علاقمندان به این علم قرار دهیم.

کتاب از سه بخش که شامل ۱۰ فصل می باشد، تشکیل شده است. بخش اول شامل معرفی و مقدمه ای بر امنیت اطلاعات، بخش دوم شامل ریاضیات و رمزهای کلید متقارن سنتی و مدرن و بخش سوم شامل ریاضیات و رمزهای کلید نامتقارن می باشد.

کتاب پیشرو می تواند یک منبع دانشگاهی یا یک منبع تخصصی برای مخاطبین حرفه ای در زمینه امنیت اطلاعات باشد. در واقع این کتاب می تواند به عنوان منبع درسی برای دانشجویان رشته های مرتبط همچون، مهندسی فناوری اطلاعات، مهندسی نرم افزار، علوم کامپیوتر و مهندسی برق در سطح کارشناسی و کارشناسی ارشد مورد استفاده قرار گیرد.

به یقین کتاب حاضر خالی از اشکال و خطا نیست. پس از خوانندگانی که ما را از این اشکالات و خطاها از طریق ناشر و یا پست های الکترونیک زیر مطلع می نمایند، نهایت تشکر و قدردانی را داریم.

مادح شکری
madeh.shokri@gmail.com

ابوالفضل یوسفی راد
usefirad@gmail.com