

به نام خدا

۱۵۵۵۹۴۰
۹۹۹/۴



مبانی و ابانش امن

مؤلفان

مهندس ماحد شکری

(کارشناس ارشد امنیت اطلاعات و مدرس دانشگاه)

مهندس فرهاد زمانی

(کارشناس ارشد شبکه های کامپیوتری و مدرس دانشگاه)

هر گونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی
ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق
مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

مبانی رایانش امن

مولفان : مهندس ماحد شکری

مهندس فرهاد زمانی

ناشر: مؤسس فرهنگی هنری دیباگران تهران

صفحه آرای: فرنوس عبدلهی

طرح روی جلد: داریوش رسایی

چاپ: دانشجو

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۶

تیراژ: ۱۰۰ جلد

قیمت: ۲۶۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۷۵۷-۶

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.mftshop.com

نشانی تلگرام: @mftbook

پست الکترونیکی: bookmarket@mftmail.com

سرشناسه: شکری، ماحد، ۱۳۷۱-

عنوان و نام پدید آور: مبانی رایانش امن

مولفان: ماحد شکری، فرهاد زمانی

مشخصات نشر: تهران - دیباگران تهران - ۱۳۹۶

مشخصات ظاهری: ۲۰۸ ص. مصور.

شابک: ۹۷۸-۶۰۰-۱۲۴-۷۵۷-۶

وضعیت فهرست نویسی: فیا

موضوع: کامپیوترها- ایمنی اطلاعات

موضوع: computer security

موضوع: شبکه های کامپیوتری - تدابیر ایمنی

موضوع: computer networks-security measures

موضوع: داده های پردازش توزیع شده

موضوع: electronic data processing-distributed processing

شناسه افزوده: زمانی، ماحد، ۱۳۷۱-

رده بندی کنگره: ۱۳۹۶: ۸ ش ۷۶/۹۱

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۴۹۷۳۸۸۵

نشانی اینستاگرام: Dibagaran_publishing

فهرست مطالب

فصل اول : مقدمه‌ای بر رایانش امن ۱۱

۱۲	۱,۱ مقدمه
۱۵	۱,۲ اهداف امنیتی
۱۷	۱,۳ حملات
۲۱	۱,۴ حملات فعال در مقابل حملات غیرفعال
۲۲	۱,۵ سرویس‌ها و مکانیزم‌ها
۲۷	۱,۶ رابطه بین سرویس‌ها و مکانیزم‌ها
۲۸	۱,۷ بدافزارها
۲۹	۱,۸ چرخه حیات بدافزار
۳۱	۱,۹ ویروس‌ها
۳۸	۱,۱۰ کرم‌ها
۴۱	۱,۱۱ اسب‌های تروا یا تروجان
۴۴	۱,۱۲ جاسوس افزار

۴۷..... ۱,۱۳ تبلیغ افزار

۴۸..... ۱,۱۴ باج افزار

۵۱..... ۱,۱۵ بد افزار درپستی

۵۱..... BOTNET ۱,۱۶

۵۲..... ROOTKIT ۱,۱۷

۵۳..... ۱,۱۸ اسپیم

۵۴..... ۱,۱۹ بمب منطقی

۵۵..... فصل دوم : رمزنگاری

۵۶..... ۲,۱ مقدمه

۵۷..... ۲,۲ رمزنگاری کلید متقارن

۶۱..... ۲,۳ اصول شش گانه کرشهف

۶۲..... ۲,۴ تحلیل رمز

۶۶..... ۲,۵ گروه بندی رمزهای سنتی

- ۲,۶ رمزهای دنباله‌ای و بلوکی ۸۲
- ۲,۷ رمزهای بدون کلید ۸۵
- ۲,۸ اجزای رمز بلوکی مدرن ۸۶
- ۲,۹ رمزهای حاصل ۹۰
- ۲,۱۰ استاندارد رمزگذاری داده (DES) ۹۳
- ۲,۱۱ استاندارد رمزگذاری پیشرفته (AES) ۱۰۷
- ۲,۱۲ الگوریتم رمزنگاری IDEA ۱۱۴
- ۲,۱۳ الگوریتم رمزنگاری BLOWFISH ۱۱۵
- ۲,۱۴ الگوریتم رمز ۱۴ بیتی CAST-۱۲۸ ۱۱۶
- ۲,۱۵ الگوریتم رمزنگاری RC۵ ۱۱۶
- ۲,۱۶ استفاده از رمزهای بلوکی مدرن ۱۱۷
- ۲,۱۷ رمزنگاری کلید نامتقارن ۱۲۶
- ۲,۱۸ نیاز به هر دو نوع از رمزنگاری (متقارن و نامتقارن) ۱۲۸
- ۲,۱۹ سیستم رمز RSA ۱۲۹
- ۲,۲۰ سیستم رمز رأین ۱۳۴
- ۲,۲۱ سیستم رمز الجمال ۱۳۶
- ۲,۲۲ رمزنگاری کوانتومی ۱۳۷

۱۴۶	۳,۱ مقدمه
۱۴۷	۳,۲ سیر تاریخی پنهان نگاری اطلاعات
۱۵۱	۳,۳ روش های پنهان نگاری اطلاعات
۱۵۲	۳,۴ عملیات پنهان نگاری در بهرورت طرح وار
۱۵۳	۳,۵ مقایسه پنهان نگاری و رمز نگاری
۱۵۷	۳,۶ کشف پنهان نگاری یا پنهان نگاری
۱۵۸	۳,۷ حملات پنهان نگاری
۱۵۹	۳,۸ کاربردهای پنهان نگاری
۱۶۱	۳,۹ علائم حق تکثیر
۱۶۲	۳,۱۰ واترمارکینگ
۱۶۵	۳,۱۱ پنهان نگاری اطلاعات در رسانه های مختلف
۱۶۷	۳,۱۲ روش های ساده و کاربردی جهت پنهان نگاری اطلاعات

۴,۱ مقدمه ۱۹۰

۴,۲ مقایسه رمزنگاری و کدینگ ۱۹۱

۴,۳ صحیح و تشخیص خطا ۱۹۱

۴,۴ انواع خطا ۱۹۲

۴,۵ افزونگی ۱۹۴

۴,۶ کدینگ ۱۹۴

۴,۷ رابطه شانون ۱۹۵

۴,۸ انواع کدینگ ۱۹۶

۴,۹ روش‌های تشخیص و تصحیح خطا ۱۹۷

۴,۱۰ فاصله همینگ ۱۹۹

۴,۱۱ روش همینگ ۲۰۱

۴,۱۲ روش بررسی افزونگی چرخشی (CRC) ۲۰۴

مراجع ۲۰۸

خط مشی کیفیت انتشارات مؤسسه فرهنگی دیباگران تهران در عرصه کتاب الکترونیک 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.

گسترده‌گی علم 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 راه برای 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 پژوهش‌ها، 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 پربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "مهمانان ماندگار" - فرهاد زمانی " و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از ید 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

بدون شک امنیت اطلاعات و رایانش امن یکی از مباحث بسیار مهم در علوم کامپیوتر و فناوری اطلاعات است، به‌طوری‌که هر روزه شاهد تحولات بسیار زیادی در این زمینه هستیم.

کتاب پیش رو از چهار فصل تشکیل شده است. در فصل اول که مقدمه‌ای بر رایانش امن است، به مفاهیم و تعاریف موردنیاز در زمینه امنیت اطلاعات پرداخته‌ایم، در فصول دوم تا چهارم نیز به‌طور کلی مفاهیم رمزنگاری، پنهان‌نگاری و کدینگ اطلاعات را ارائه داده‌ایم.

درواقع کتاب از این سرفصل‌ها این است که خواننده بتواند مبانی رایانش امن را به‌صورت کلی شناخته و همچنین تفاوت بین مفهوم رمزنگاری، پنهان‌نگاری و کدینگ را به خوبی درک نماید، چراکه متأسفانه برخی از افراد این مفاهیم ذکر شده قائل نیستند و آن‌ها را به‌جای یکدیگر به‌کار می‌گیرند.

محتوای کتاب به نحوی تدوین شده است که هم برای دانشجویان رشته‌های علوم کامپیوتر و هم به‌عنوان منبعی عمومی جهت آشنایی با مفاهیم رایانش امن و امنیت اطلاعات برای علاقه‌مندان به این علم قابل‌استفاده خواهد بود.

کتاب حاضر خالی از اشکال نیست، لذا از خوانندگان محترم خواهشمندم با ارائه نظرات و پیشنهادات سازنده خود، ما را در جهت اصلاح و ارتقای سطح علمی کتاب در ویرایش‌های بعدی یاری نمایند.

فرهاد زمانی

مادح شکری

zamani.f.67@gmail.com

madeh.shokri@gmail.com