

به نام خدا



مؤسسه فرهنگی هنری
دیبانگران تهران

رمزنگاری

مؤلف :

دکتر بهروز فروزان

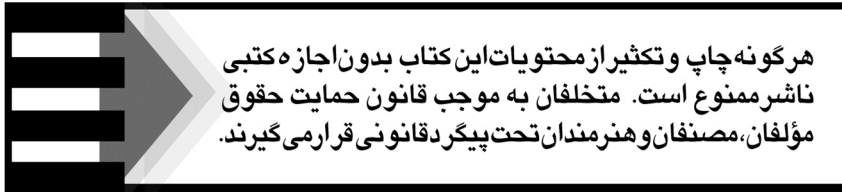
مترجمین :

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



هرگونه 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 می‌گیرند.

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: ۵۰ جلد

قیمت: ۱۴۰۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۵۱۸-۳

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

سرشناسه: فروزان، بهروز، ۱۳۲۳-

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

مشخصات نشر: تهران- دیباگران تهران- ۱۳۹۵

مشخصات ظاهری: ۴۹۵ ص

شابک: ۹۷۸-۶۰۰-۱۲۴-۵۱۸-۳

وضعیت فهرست نویسی: فیبا

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: ۸۰۱ ۱۳۹۵ ر ۴ / ۵۹ / ۵۱۰۵ TK

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۴۵۰۵۹۷۹

نشانی اینستاگرام: Dibagaran_publishing

فهرست مطالب

۱۵ مقدمه مترجمان
۱۷ بخش اول
۱۷ مقدمه
۱۷ فصل اول
۱۷ مقدمه ای بر امنیت اطلاعات
۱۷ اهداف فصل
۱۹ ۱.۱ اهداف امنیتی
۱۹ محرمانگی
۲۰ جامعیت
۲۰ در دسترس پذیری
۲۰ ۱.۲ حملات
۲۱ حملات علیه محرمانگی
۲۲ حملات علیه جامعیت
۲۴ حملات علیه در دسترس پذیری
۲۴ حملات فعال درمقابل حملات غیرفعال
۲۶ ۱.۳ سرویس ها و مکانیزم ها
۲۶ سرویس های امنیتی
۲۸ مکانیزم های امنیتی
۳۱ رابطه بین سرویس ها و مکانیزم ها
۳۱ ۱.۴ تکنیک ها
۳۲ رمزنگاری
۳۳ پنهان نگاری

۳۷	۱.۵ منابع پیشنهادی
۳۷	کتاب ها
۳۷	وبسایت ها
۳۷	۱.۶ عبارات کلیدی
۳۹	۱.۷ خلاصه
۴۱	بخش دوم
۴۱	رمزنگاری کلید متقارن
۴۱	فصل دوم
۴۱	ریاضیات رمزنگاری
۴۱	(حساب پیمانه ای، هم ارزی و ماتریس)
۴۲	۲.۱ حساب اعداد صحیح
۴۲	مجموعه اعداد صحیح
۴۲	عملیات دودویی
۴۳	تقسیم اعداد صحیح
۴۶	تقسیم پذیری
۵۴	معادلات خطی دیوفانتین
۵۷	۲.۲ حساب پیمانه ای
۵۷	عملگر پیمانه ای
۵۹	مجموعه باقیمانده ها: Z_n
۵۹	هم ارزی
۶۲	عملیات در Z_n
۶۷	معکوس
۷۳	جداول جمع و ضرب
۷۴	مجموعه های مختلف برای جمع و ضرب

۷۵ دو مجموعه دیگر
۷۶ ۲.۳ ماتریس
۷۶ تعاریف
۷۷ عملیات و روابط
۸۰ دترمینان
۸۳ ۲.۴ هم ارزی خطی
۸۳ معادلات خطی تک - متغیره
۸۵ مجموعه معادلات خطی
۸۷ ۲.۵ منابع پیشنهادی
۸۷ کتاب ها
۸۷ وبسایت ها
۸۷ ۲.۶ عبارات کلیدی
۸۸ ۲.۷ خلاصه
۹۲ فصل سوم
۹۲ رمزهای کلید متقارن سنتی
۹۲ اهداف فصل
۹۳ ۳.۱ مقدمه
۹۶ اصل کیرشهف
۹۶ تحلیل رمز
۱۰۱ گروه بندی رمزهای سنتی
۱۰۱ ۳.۲ رمزهای جانشینی
۱۰۲ رمزهای جانشینی تک الفبایی
۱۱۳ رمزهای جانشینی تک الفبایی
۱۳۳ ۳.۳ رمزهای جابجایی

۱۳۳.....	رمزهای جابجایی بدون کلید.....
۱۳۵.....	رمزهای جابجایی کلید دار.....
۱۳۶.....	ترکیب دو روش.....
۱۴۴.....	۳.۴ رمزهای دنباله ای و بلوکی.....
۱۴۴.....	رمزهای دنباله ای.....
۱۴۶.....	رمزهای بلوکی.....
۱۴۷.....	ترکیب.....
۱۴۷.....	۳.۵ منابع پیشنهادی.....
۱۴۸.....	کتاب ها.....
۱۴۸.....	وبسایت ها.....
۱۴۸.....	۳.۶ عبارات کلیدی.....
۱۵۰.....	۳.۷ خلاصه.....
۱۵۲.....	فصل چهارم.....
۱۵۲.....	ریاضیات رمزنگاری (ساختارهای جبری).....
۱۵۳.....	۴.۱ ساختارهای جبری.....
۱۵۳.....	گروه ها.....
۱۶۴.....	حلقه.....
۱۶۶.....	میدان.....
۱۶۹.....	خلاصه.....
۱۶۹.....	۴.۲ میدان های $GF(2^n)$
۱۷۱.....	چند جمله ای ها.....
۱۸۲.....	استفاده از مولد.....
۱۸۵.....	۴.۳ منابع پیشنهادی.....
۱۸۵.....	کتاب ها.....

۱۸۵	وبسایت ها
۱۸۶	۴.۴ عبارات کلیدی
۱۸۷	۴.۵ خلاصه
۱۹۰	فصل پنجم
۱۹۰	مقدمه ای بر رمزهای کلید متقارن مدرن
۱۹۱	۵.۱ رمزهای بلوکی مدرن
۱۹۳	جانشینی یا جابجایی
۲۰۰	اجزای رمز بلوکی مدرن
۲۰۵	S-Boxes
۲۱۲	رمزهای حاصل
۲۱۶	دو کلاس از رمزهای حاصل
۲۲۲	حملات روی رمزهای بلوکی
۲۳۰	۵.۲ رمزهای دنباله ای مدرن
۲۳۱	رمزهای دنباله ای همزمان
۲۳۹	رمزهای دنباله ای غیر همزمان
۲۳۹	۵.۳ منابع پیشنهادی
۲۳۹	کتاب ها
۲۴۰	وبسایت ها
۲۴۰	۵.۴ عبارات کلیدی
۲۴۲	۵.۵ خلاصه
۲۴۵	فصل ششم
۲۴۵	استاندارد رمزگذاری داده (DES)
۲۴۶	۶.۱ مقدمه
۲۴۶	تاریخچه

۲۴۷مرور اجمالی
۲۴۷۶.۲ ساختار DES
۲۴۸جایگشت های اولیه و نهایی
۲۵۱راندها
۲۵۸رمز و معکوس رمز
۲۶۵مثال ها
۲۶۷۶.۳ تحلیل DES
۲۶۸خصوصیات
۲۶۹معیارهای طراحی
۲۷۱نقاط ضعف DES
۲۷۸۶.۴ DES چندگانه
۲۸۰DES دوگانه
۲۸۲DES سه گانه
۲۸۴۶.۵ امنیت DES
۲۸۴حمله جستجوی فراگیر
۲۸۴تحلیل رمز تفاضلی
۲۸۵تحلیل رمز خطی
۲۸۵۶.۶ منابع پیشنهادی
۲۸۵کتاب ها
۲۸۵وبسایت ها
۲۸۶۶.۷ عبارات کلیدی
۲۸۷۶.۸ خلاصه
۲۸۹فصل هفتم
۲۸۹استاندارد رمزگذاری پیشرفته (AES)

۲۹۰	۷.۱ مقدمه
۲۹۰	تاریخچه
۲۹۱	معیارها
۲۹۱	راندها
۲۹۳	واحدهای داده
۲۹۶	ساختار هر راند
۲۹۷	۷.۲ تبدیلات
۲۹۸	جانشینی
۳۰۴	جایگشت
۳۰۷	مخلوط کردن
۳۱۱	اضافه کردن کلید
۳۱۲	۷.۳ توسعه کلید
۳۱۳	توسعه کلید در AES-128
۳۱۹	توسعه کلید در AES-192 و AES-256
۳۲۰	تحلیل توسعه کلید
۳۲۰	۷.۴ رمزها
۳۲۱	طراحی اصلی
۳۲۲	طراحی ثانویه
۳۲۵	۷.۵ مثال ها
۳۲۸	۷.۶ تحلیل AES
۳۲۸	امنیت
۳۲۹	پیاده سازی
۳۳۰	سادگی و هزینه
۳۳۰	۷.۷ منابع پیشنهادی

۳۳۰.....	کتاب ها.....
۳۳۰.....	وبسایت ها.....
۳۳۱.....	۷.۸ عبارات کلیدی.....
۳۳۱.....	۷.۹ خلاصه.....
۳۳۵.....	فصل هشتم.....
۳۳۵.....	رمزگذاری با استفاده از رمزهای کلید متقارن مدرن.....
۳۳۶.....	۸.۱ استفاده از رمزهای بلوکی مدرن.....
۳۳۶.....	حالت کتابچه الکترونیکی (ECB).....
۳۴۰.....	حالت زنجیره بلوک های رمز (CBC).....
۳۴۴.....	حالت بازخورد رمز (CFB).....
۳۴۸.....	حالت بازخورد خروجی (OFB).....
۳۵۱.....	حالت شمارنده (CTR).....
۳۵۴.....	۸.۲ استفاده از رمزهای دنباله ای.....
۳۵۴.....	RC4.....
۳۵۹.....	A5/1.....
۳۶۴.....	۸.۳ مسائل دیگر.....
۳۶۴.....	مدیریت کلید.....
۳۶۴.....	تولید کلید.....
۳۶۵.....	۸.۴ منابع پیشنهادی.....
۳۶۵.....	کتاب ها.....
۳۶۵.....	وبسایت ها.....
۳۶۶.....	۸.۵ عبارات کلیدی.....
۳۶۶.....	۸.۶ خلاصه.....
۳۶۹.....	بخش سوم.....

۳۶۹.....	رمزنگاری کلید نامتقارن.....
۳۶۹.....	فصل نهم.....
۳۶۹.....	ریاضیات رمزنگاری (اعداد اول و معادلات هم ارزی مرتبط).....
۳۷۰.....	۹.۱ اعداد اول.....
۳۷۰.....	تعریف.....
۳۷۲.....	کاردینالیتی (مرتب‌ه) اعداد اول.....
۳۷۳.....	بررسی اول بودن.....
۳۷۵.....	تابع فی اولر.....
۳۷۷.....	قضیه کوچک فرما.....
۳۸۰.....	قضیه اولر.....
۳۸۲.....	تولید اعداد اول.....
۳۸۴.....	۹.۲ آزمون اول بودن.....
۳۸۴.....	الگوریتم های قطعی.....
۳۸۷.....	الگوریتم های احتمالی.....
۳۹۶.....	آزمون اول بودن پیشنهادی.....
۳۹۷.....	۹.۳ فاکتورگیری.....
۳۹۸.....	قضیه بنیادی حساب.....
۳۹۹.....	روش های فاکتورگیری.....
۴۰۱.....	روش فرما.....
۴۰۲.....	روش $p - 1$ پولارد.....
۴۰۳.....	روش rho پولارد.....
۴۰۷.....	روش های کارآمدتر.....
۴۰۸.....	۹.۴ قضیه باقیمانده چینی.....
۴۱۱.....	کاربردها.....

۴۱۲	۹.۵ هم ارزی درجه دوم
۴۱۲	هم ارزی درجه دوم با پیمانۀ عدد اول
۴۱۵	هم ارزی درجه دوم با پیمانۀ عدد مرکب
۴۱۶	۹.۶ بتوان رسانی و لگاریتم
۴۱۶	بتوان رسانی
۴۱۹	لگاریتم
۴۲۷	۹.۷ منابع پیشنهادی
۴۲۷	کتاب ها
۴۲۸	وبسایت ها
۴۲۸	۹.۸ عبارات کلیدی
۴۳۰	۹.۹ خلاصه
۴۳۲	فصل دهم
۴۳۲	رمزنگاری کلید نامتقارن
۴۳۲	۱۰.۱ مقدمه
۴۳۴	کلیدها
۴۳۴	ایده کلی
۴۳۶	نیاز به هر دو
۴۳۷	تابع یک طرفه درجه دار
۴۳۹	سیستم رمز کوله پشتی
۴۴۴	۱۰.۲ سیستم رمز RSA
۴۴۴	مقدمه
۴۴۵	رویه
۴۴۸	تعدادی مثال آموزشی
۴۵۰	حملات روی RSA

۴۶۰	پیشنهادات
۴۶۰	پدینگ بهینه رمزنگاری نامتقارن (OAEP)
۴۶۴	کاربردها
۴۶۴	۱۰.۳ سیستم رمز رایین
۴۶۵	رویه
۴۶۸	امنیت سیستم رایین
۴۶۸	۱۰.۴ سیستم رمز الجمال
۴۶۸	سیستم رمز الجمال
۴۶۹	رویه
۴۷۰	اثبات
۴۷۱	تجزیه و تحلیل
۴۷۲	امنیت الجمال
۴۷۴	کاربرد
۴۷۴	۱۰.۵ سیستم رمز منحنی بیضوی
۴۷۵	منحنی بیضوی روی اعداد حقیقی
۴۷۹	منحنی بیضوی روی $GF(p)$
۴۸۱	منحنی بیضوی روی $GF(2^n)$
۴۸۳	شبیه سازی سیستم رمزنگاری الجمال با منحنی بیضوی
۴۸۷	۱۰.۶ منابع پیشنهادی
۴۸۷	کتاب ها
۴۸۷	وبسایت ها
۴۸۸	۱۰.۷ عبارات کلیدی
۴۸۹	۱۰.۸ خلاصه
۴۹۳	منابع

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی است که بتواند خواسته‌هایی 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 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 پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت " آقایان 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 حاصل 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.

ابوالفضل یوسفی راد
usefirad@gmail.com

مادح شکری
madeh.shokri@gmail.com