به نام خدا

مؤسسه فرهنگی هنری
دیباگران تهران

اصول و مبانی

امضای الکترونیک و گواهی دیجیتال

مؤلفان
حمید دوست‌محمدیان
امیرحسین میرمحمد صادقی
مهناز شایق

اصول و مبانی امضای الکترونیک و گواهی دیجیتال

مؤلفان: حمید دوست‌محمدیان - امیرحسین میرمحمد صادقی - مهناز شایق
ناشر: مؤسسه فرهنگی هنری دیباگران تهران
حروفچینی و صفحه‌آرایی: مجتمع فنی تهران
طرح روی جلد: مجتمع فنی تهران
چاپ: شرکت چاپ و نشر کتاب‌های درسی
نوبت چاپ: اول
تاریخ نشر: اردیبهشت ماه ۱۳۹۲
تیراژ: ۵۰۰ نسخه
قیمت: ۱۱۵۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۲۴۰-۳
ISBN: 978-600-124-240-3

سرشناسه: دوست‌محمدیان، حمید، ۱۳۵۶-
عنوان و نام پدیدآور: اصول و مبانی امضای الکترونیک و گواهی دیجیتال/ مؤلفان حمید دوست‌محمدیان، امیرحسین میرمحمد صادقی، مهناز شایق.
مشخصات نشر: تهران: مؤسسه فرهنگی هنری دیباگران تهران، ۱۳۹۲.
مشخصات ظاهری: ۱۶۸ص.
شابک: 978-600-124-240-3
وضعیت فهرست‌نویسی: فیپا
یادداشت: کتابنامه: ص. ۱۶۷.
موضوع: امضای الکترونیکی
موضوع: رمزگذاری داده‌ها
شناسه افزوده: میرمحمد صادقی، امیرحسین، ۱۳۵۳-
شناسه افزوده: شایق، مهناز، ۱۳۶۵-
رده‌بندی کنگره: ۱۳۹۲ ۹د۷۷الف/QA۷۶
رده‌بندی دیویی: ۰۰۵/۸۲
شماره کتابشناسی ملی: ۳۰۸۴۷۱۵

نشانی دفتر مرکزی: تهران، سعادت آباد، میدان کاج، خ سرو شرقی، روبه‌روی خ علامه، پلاک ۴۹
صندوق پستی: ۱۴۳۳۵/۹۴۳ وب سایت: **dibagaran.mft.info**
نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، قبل از چهارراه لبافی‌نژاد، پلاک ۱۲۵۱
تلفن: ۱۲-۲۲۰۸۵۱۱۱ کد پستی: ۱۳۱۴۹۸۳۱۸۵
پست الکترونیکی: **bookmarket@mftmail.com** فروش اینترنتی: **www.mftshop.com**

فهرست مطالب

محتوای این کتاب با دوره‌های علمی‌کاربردی نیز همپوشانی داشته و می‌تواند مورد استفاده دانش‌پژوهان رشته‌های IT، مهندسی کامپیوتر، حقوق و تجارت و دیگر علاقه‌مندان به حوزه‌های فناوری اطلاعات و ارتباطات قرار گیرد.

مقدمه ناشر ۸

مقدمه مؤلفان ۹

فصل اول– کلیات امضای دیجیتال

مقدمه ۱۱

۱-۱ ویژگی‌های امضاهای دیجیتال ۱۲

۱-۲ امضای دیجیتال امنیت چه چیزی را تأمین می‌کند؟ ۱۳

۱-۳ روش ایجاد امضای دیجیتال ۱۳

۱-۴ روش‌های تولید امضای دیجیتال ۱۴

فصل دوم– واژه‌نامه

مقدمه ۱۷

۲-۱ خدمات مرکز صدور گواهی دیجیتال ۱۸

۲-۲ خدمات مبتنی بر زیر ساخت کلید عمومی ۱۸

فصل سوم– معرفی امضای دیجیتال

۳-۱ شناسه سند امضای دیجیتال ۲۳

۳-۲ اجزا وکاربردها ۲۳

فصل چهارم– مقررات عمومی

۴-۱ وظایف و مسئولیت‌ها ۲۷

۴-۲ التزامات ۳۱

۴-۳ تعهدات مالی ۳۲
۴-۴ تفسیر قانون و ضمانت اجرایی ۳۲
۴-۵ تعرفه‌ها ۳۳
۴-۶ مخزن وانتشار ۳۳
۴-۷ بازرسی ۳۴
۴-۸ محرمانگی ۳۶
۴-۹ حق مالکیت معنوی ۳۷

فصل پنجم– تشخیص و احراز هویت

۵-۱ ثبت نام اولیه ۳۹
۵-۲ روال تجدید کلید گواهی ۴۲
۵-۳ دریافت یک گواهی جدید پس از ابطال ۴۲
۵-۴ درخواست ابطال ۴۲

فصل ششم– خواسته‌های عملیاتی

۶-۱ درخواست گواهی ۴۳
۶-۲ صدور گواهی ۴۴
۶-۳ پذیرش گواهی ۴۴
۶-۴ ابطال و تعلیق گواهی ۴۵
۶-۵ روال بازرسی امنیتی ۴۸
۶-۶ بایگانی اطلاعات ۵۳
۶-۷ گردش کلید ۵۵
۶-۸ در خطر افشا بودن و ترمیم خرابی ۵۵
۶-۹ توقف سرویس دهی مرکز صدور گواهی ۵۷

فصل هفتم– کنترل‌های امنیت فیزیکی، رویه‌ای و فردی

۷-۱ کنترل‌های فیزیکی ۵۹
۷-۲ کنترل‌های رویه‌ای ۶۲
۷-۳ کنترل کارکنان ۶۳

فصل هشتم– کنترل‌های امنیتی فنی

۸-۱ تولید و نصب زوج کلید ۶۷
۸-۲ حفاظت از کلیدهای خصوصی ۷۰
۸-۳ وجوه دیگر مدیریت زوج کلید ۷۲
۸-۴ اطلاعات فعال ساز ۷۲
۸-۵ کنترل‌های امنیتی کامپیوتر ۷۳
۸-۶ کنترل‌های فنی طول عمر ۷۴
۸-۷ کنترل‌های امنیت شبکه ۷۵

فصل نهم– فرایند احراز هویت

۹-۱ فرایند احراز هویت ۷۷
۹-۲ سرویس‌های امنیتی ۸۰
۹-۳ رمزنگاری ۸۲
۹-۴ الگوریتم‌های متقارن ۸۶
۹-۵ الگوریتم‌های نامتقارن ۸۸
۹-۶ توابع درهم سازی ۹۶
۹-۷ امضای دیجیتال ۹۸
۹-۸ امضای دستی ۹۸
۹-۹ نحوه امضای یک پیغام دیجیتال ۹۹
۹-۱۰ اجزا اصلی الگوی جامع شناسایی امضای دیجیتال ۱۰۱
۹-۱۱ امضای الکترونیکی و محرمانگی ۱۰۲
۹-۱۲ گواهی‌نامه دیجیتال چیست؟ ۱۰۳
۹-۱۳ کلید عمومی و صاحب آن ۱۰۴
۹-۱۴ حمله امنیتی ۱۰۴
۹-۱۵ مروری بر گواهی دیجیتال ۱۰۵
۹-۱۶ امنیت امضای دیجیتال ۱۰۶
۹-۱۷ مرکز صدور گواهی ۱۰۷
۹-۱۸ دفتر ثبت نام ۱۰۹
۹-۱۹ فرایند درخواست گواهی ۱۱۰
۹-۲۰ نحوه دریافت امضا یا گواهی دیجیتال ۱۱۱

۹-۲۱ گواهیSSL ۱۱۲
۹-۲۲ جایگاه زیر ساخت کلید عمومی در ثبت سفارش ۱۱۵

فصل دهم– راهنمای ساخت کلید خصوصی و عمومی و استفاده آن

۱۰-۱ ساخت کلید اصلی ۱۱۷

فصل یازدهم– راهکار جامع زیرساخت امضای PKI

۱۱-۱ مهم‌ترین اهداف زیر ساخت امضای دیجیتال ۱۳۳
۱۱-۲ خدمات در زمینه زیر ساخت کلید عمومی ۱۳۳
۱۱-۳ پیشنهاد فنی ۱۳۴
۱۱-۴ تعیین الزامات راهکار امضای دیجیتال ۱۳۴
۱۱-۵ ارائه مؤلفه‌های نرم‌افزاری زیرساخت کلید عمومی و نصب و راه‌اندازی آن ۱۳۶
۱۱-۶ خدمات مشاوره/پیاده‌سازی پشتیبانی از PKI در یک نرم‌افزار کاربردی ۱۳۷
۱۱-۷ خدمات آزمون انطباق نرم افزار کاربردی با استانداردهای PKI ۱۳۸
۱۱-۸ راه‌اندازی مرکز صدور گواهی الکترونیکی داخلی وزارتخانه ۱۳۹
۱۱-۹ راه‌اندازی و ثبت مرکز صدور گواهی الکترونیکی میانی ۱۴۱
۱۱-۱۰ ارائه خدمات آموزشی ۱۴۵
۱۱-۱۱ مؤلفه‌های اصلی امضای دیجیتال ۱۴۶
۱۱-۱۲ نمایش جایگاه مؤلفه‌های مرکز صدور امضای دیجیتال ۱۴۶
۱۱-۱۳ مرجع صدور گواهی ۱۴۷
۱۱-۱۴ ارائه دهنده برخط وضعیت گواهی ۱۴۹
۱۱-۱۵ مرجع مهر زمانی ۱۵۰
۱۱-۱۶ مؤلفه LRA ۱۵۱
۱۱-۱۷ مؤلفه webRA ۱۵۱

فصل دوازدهم– آزمون در آزمایشگاه ارزیابی سخت افزارهای PKI

مقدمه ۱۵۳
۱۲-۱ متدولوژی آزمون ۱۵۳

فصل سیزدهم– نتیجه‌گیری

۱-۱۳ خلاصه و نتیجه‌گیری ۱۵۹

پیوست

سطوح اطمینان در سیستم‌های دولتی ۱۶۱
نظام شناسایی ۱۶۱
انواع گواهی ۱۶۳
مشخصات انواع گواهی‌های نهایی ۱۶۳
منابع ۱۶۷

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرضه کتاب‌هایی است که بتواند خواسته‌های 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 فرهنگ این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هر چند 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 پربار، معتبر و با کیفیت مناسب در اختیار علاقه‌مندان قرار دهند.

کتابی که در دست دارید با همت " **آقایان حمید دوست‌محمدیان و امیرحسین میرمحمد صادقی و سرکار خانم مهناز شایق**" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

ویراستاری: شیوا غمگسار

ویرایش و صفحه‌آرایی کامپیوتری: مهسا کوراولی

طراح جلد: مینا دیده‌بان

ناظر چاپ: علیرضا گلشادی

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 مؤلفان

در این کتاب رمزنگاری داده ها و برخی جنبه‌های آن مورد بحث قرار گرفته است. در ابتدا به معرفی رمزنگاری و انواع آن پرداخته‌ایم که در نهایت امضای دیجیتال و استفاده از پروتکل SSL را نیز شامل شده است که هر دو روش برای حفاظت از اطلاعات به کار گرفته می‌شوند.

آنچه به عنوان امضای دیجیتال در سیستم‌های اتوماسیون اداری جریان دارد عکس گرفتن از امضا و کپی کردن آن زیر نامه‌ها و اسناد است در صورتی که امضای دیجیتال در حقیقت یک مجموعه کد یا به بیان واضح‌تر ترکیبی از کلید خصوصی و کلید عمومی است که به نام یک فرد مشخص ثبت می‌شود و برای حفاظت و رمزنگاری اطلاعات مورد استفاده قرار می‌گیرد.

در اینجا لازم است از کلیه کارکنان مؤسسه فرهنگی هنری دیباگران تهران که ما را در تمام مراحل تهیه این کتاب یاری نمودند، تشکر و قدردانی گردد.

بی‌شک این اثر عاری از اشکال نیست و در پایان از کلیه اساتید و دانشجویانی که در رفع نقایص و اشتباهات این کتاب ما را یاری خواهند کرد، سپاسگزاری می‌شود.

حمید دوست‌محمدیان

امیرحسین میرمحمد صادقی

مهناز شایق

hdmohamadian@gmail.com