

به نام خدا

۱۶۱۱۱۱۱
۹۷۶۶۶

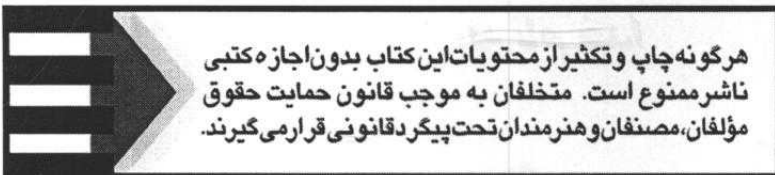


گواهی امضای دیجیتال و کاربردهای آن

مؤلف

مجید رسولیان

(متخصص فناوری اطلاعات - مراکز داده)



◀ عنوان کتاب: گواهی امضای دیجیتال و کاربردهای آن

◀ مولف: مجید رسولیان (متخصص فناوری اطلاعات-مراکز داده)

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ صفحه آرای: فرناوش عبدالهی

◀ طراح جلد: داریوش فرسای

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۳۹۷

◀ چاپ و صحافی: دانشجو

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۴۰۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۰۰-۱۲۴-۹۱۹-۸

◀ نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۰۲۲-۸۵۱۱۱-۶۶۴۱۰۰۴۶

کد پستی: ۱۳۱۴۹۸۳۱۸۵

◀ فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagaran-tehran.com

www.mftdibagaran.ir

◀ لینک ربات دیباگران : [@dibagaranetehranbot](https://t.me/dibagaranetehranbot)

◀ نشانی تلگرام: [@mftbook](https://t.me/mftbook)

اپلیکیشن دیباگران تهران را از سایت های اینترنتی دیباگران دریافت نمایید.

سرشناسه: رسولیان، مجید، ۱۳۴۷
عنوان و نام پدیدآور: گواهی امضای دیجیتال و کاربردهای آن / مولف: مجید رسولیان.
مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۷.
مشخصات ظاهری: ۲۸۸ ص: مصور.
شابک: ۹۷۸-۶۰۰-۱۲۴-۹۱۹-۸
وضعیت فهرست نویسی: فیبا
موضوع: امضای الکترونیکی
موضوع: Digital Signature
موضوع: رمزگذاری داده ها
موضوع: data encryption (computer science)
رده بندی کنگره: ۳۹۷-۷۶/۹ الف QA
رده بندی دیویی: ۰۰۵.۸۲
شماره کتابشناسی ملی: ۵۲۴۰۷۱۱

فهرست مطالب

فصل ۱.....	۱۳
تجارت الکترونیک.....	۱۳
۱-۱) تعریف تجارت الکترونیکی.....	۱۴
۱-۲) تاریخچه تجارت الکترونیکی.....	۱۵
۱-۳) عناصر تجارت الکترونیکی.....	۱۶
۱-۴) ویژگی های تجارت الکترونیکی.....	۱۷
۱-۵) مدل های تجارت الکترونیکی.....	۱۸
۱-۶) مزایای کاربرد تجارت الکترونیکی برای جامعه.....	۱۸
۱-۷) مزایای استفاده از تجارت الکترونیکی برای مصرف کنندگان.....	۱۹
فصل ۲.....	۲۱
دولت الکترونیک.....	۲۱
۲-۱) تعاریف مختلف از دولت الکترونیکی.....	۲۲
۲-۲) اهداف دولت الکترونیکی چیست ؟.....	۲۴
فصل ۳.....	۲۷
بانکداری الکترونیک.....	۲۷
۳-۱) تاریخچه.....	۲۸
۳-۲) خدمات بانکداری الکترونیک.....	۲۹
۳-۳) ویژگی ها.....	۲۹
۳-۴) شاخه های بانکداری الکترونیک.....	۳۱
۳-۵) مزایای بانکداری الکترونیک.....	۳۲
۳-۶) خلاصه مزایا.....	۳۲
فصل ۴.....	۳۵
آموزش الکترونیک.....	۳۵
۴-۱) مقدمه.....	۳۶
۴-۲) مفاهیم فراگیری الکترونیکی.....	۳۷

- ۳۷..... (۴-۳) صنعت آموزش و فراگیری الکترونیکی
- ۳۸..... (۴-۴) محتویات مطالب
- ۳۸..... (۴-۵) خدمات
- ۳۹..... (۴-۶) فرآیند ادراک و شناخت
- ۴۰..... (۴-۷) فراگیری

فصل ۵..... ۴۳

کارت هوشمند..... ۴۳

- ۴۴..... (۵-۱) کارت هوشمند چیست ؟
- ۴۴..... (۵-۲) تاریخچه کارت هوشمند
- ۴۷..... (۵-۳) برد های گوناگون کارت

بخش دوم..... ۵۱

رمزنگاری و الگوریتم های رمزنگاری..... ۵۱

فصل ۶..... ۵۲

رمزنگاری..... ۵۲

- ۵۳..... (۶-۱) رمزنگاری چیست ؟
- ۵۵..... (۶-۲) چرا رمزنگاری ؟
- ۵۶..... (۶-۳) شیوه های پایه رمزنگاری

فصل ۷..... ۵۹

الگوریتم های رمزنگاری متقارن..... ۵۹

- ۶۰..... (۷-۱) تعاریف
- ۶۲..... (۷-۲) استاندارد رمزنگاری یا DES چیست ؟
- ۶۵..... (۷-۳) استاندارد پیشرفته رمزنگاری یا AES چیست ؟

فصل ۸..... ۶۹

الگوریتم های رمزنگاری با کلید نامتقارن..... ۶۹

- ۷۰..... (۸-۱) تعریف و نحوه عملکرد

فصل ۹..... ۷۵

مدیریت کلید..... ۷۵

۹-۱) تعریف..... ۷۶

۹-۲) تولید کلید ها..... ۷۶

۹-۳) ارسال و توزیع کلید ها در شبکه های بزرگ..... ۷۸

۹-۴) تصدیق کلیدها..... ۷۸

۹-۵) طول عمر کلید ها..... ۷۹

۹-۶) مدیریت کلید توسط روش های کلید عمومی..... ۸۰

۹-۷) الگوریتم های تبادل کلید..... ۸۱

بخش سوم..... ۸۳

امضاء دیجیتال و استاندارد X.509..... ۸۳

فصل ۱۰..... ۸۵

استاندارد امضاء دیجیتال X.509..... ۸۵

۱۰-۱) تعریف..... ۸۶

۱۰-۲) گواهی نامه ها (CERTIFICATES)..... ۸۷

۱۰-۳) اخذ گواهی نامه یک کاربر..... ۹۰

۱۰-۴) ابطال گواهی نامه..... ۹۳

۱۰-۵) رویه های اعتبار سنجی..... ۹۴

۱۰-۶) نسخه سوم X.509..... ۹۷

۱۰-۷) اطلاعات کلید و خط مشی..... ۹۹

۱۰-۸) مشخصات سوژه و صادر کننده ی گواهی نامه..... ۱۰۰

۱۰-۹) محدودیت های روند گواهی کردن..... ۱۰۱

۱۰-۱۰) زیر ساخت کلید عمومی (PKI)..... ۱۰۱

۱۰-۱۱) وظایف مدیریتی PKIX..... ۱۰۴

۱۰-۱۲) پروتکل مدیریتی PKIX..... ۱۰۵

فصل ۱۱.....	۱۰۷
امضاء دیجیتال.....	۱۰۷
۱-۱۱) امضای دیجیتالی چیست؟.....	۱۰۹
۲-۱۱) طرح عمومی امضای دیجیتالی.....	۱۱۰
۳-۱۱) تاریخچه.....	۱۱۰
۴-۱۱) دلایل استفاده از امضای دیجیتالی.....	۱۱۳
۵-۱۱) اجزای تشکیل دهنده امضای دیجیتالی.....	۱۱۴
۶-۱۱) مرکز گواهی هویت (CA).....	۱۱۶
۷-۱۱) قوانین در امضاء دیجیتال.....	۱۱۷
۸-۱۱) انواع امضای دیجیتال.....	۱۱۷
۹-۱۱) معرفی مختصر مزایا و معایب چند نوع امضای دیجیتال.....	۱۲۰
۱۰-۱۱) استاندارد های امضای دیجیتال.....	۱۲۲
۱۱-۱۱) استاندارد های دیجیتال (DSS).....	۱۲۲
۱۲-۱۱) الگوریتم امضای دیجیتال ELGAMAL.....	۱۲۳
۱۳-۱۱) الگوریتم امضای (1) SCHNORR.....	۱۲۵
۱۴-۱۱) الگوریتم امضای (1) (DHA).....	۱۲۶
۱۵-۱۱) نکات منفی و نکات مثبت DSS.....	۱۲۷
۱۶-۱۱) پیاده سازی نرم افزاری و سخت افزاری DSS.....	۱۲۷
۱۷-۱۱) وضعیت سرویس امضاء دیجیتال در کشور ایران.....	۱۳۰
معرفی امضاء دیجیتال.....	۱۳۲
مفهوم رمزنگاری.....	۱۳۷
اصطلاحات رمزنگاری.....	۱۳۷
رمزنگاری کلید خصوصی (PRIVATE KEY).....	۱۳۸
معرفی امضاء دیجیتال.....	۱۴۹
تاریخچه امضای دیجیتال.....	۱۵۱
مزایای امضای دیجیتال.....	۱۵۴
اجزای زیرساخت کلید عمومی.....	۱۶۳
معماری های زیرساخت کلید عمومی.....	۱۶۸
معماری شبکه.....	۱۷۲
معماری پل (BRIDGE ARCHITECTURE).....	۱۷۵
گواهینامه ها و مراکز صدور گواهینامه ها.....	۱۷۶

۱۷۷.....	یک گواهینامه چیست ؟
۱۸۳.....	مراکز صدور گواهینامه (CA: CERTIFICATE AUTHORITY)
۱۸۴.....	انواع گواهینامه ها در اینترنت
۱۹۰.....	پروتکل های مبادله اطلاعات در اینترنت
۱۹۱.....	پروتکل SSL
۱۹۸.....	انواع SSL
۲۰۰.....	درخواست یک گواهینامه
۲۲۷.....	جایگاه امضای دیجیتالی در ثبت اسناد به شیوه الکترونیکی
۲۲۸.....	۱. کلیات
۲۳۲.....	۲. مطالعه تطبیقی جایگاه گواهینامه امضای الکترونیکی
۲۳۸.....	۳. مشکلات حقوقی - عملی ناشی از ظهور سیستم دیجیتالی امضا
۲۵۲.....	امضای دیجیتال در ایران
۲۵۹.....	توکن های هوشمند SSL
۲۶۷.....	چالشهای به کارگیری فناوری اطلاعات در ایران
۲۷۶.....	واژه نامه
۲۸۷.....	منابع

مقدمه مولف

امروزه ایجاد بستر مناسب و امن نیاز اصلی تبادل و انتقال اطلاعات است، حال آنکه تبادل اطلاعات به صورت فیزیکی رخ دهد و یا در فضای سایبر و به صورت الکترونیکی باشد. با توجه به کاربردهای وسیع گواهی الکترونیکی در اغلب حوزه‌های دانش IT، می‌توان استفاده از گواهی الکترونیک را از الزامات تجارت الکترونیک، دولت الکترونیک، خدمات الکترونیک و مکاتبات الکترونیک دانست. تذکراتی که در گواهی الکترونیک وجود دارد با سایر مباحث امنیتی مشترک است؛ متولی امر گواهی الکترونیک هر ارگانی که باشد باید به صورت علمی در کشور همه جوانب امر را مورد بررسی قرار دهد چراکه آگاهی دادن در زمینه موافقت استقفا و الزامات یکارگیری گواهی الکترونیک در کشور، نقش مرکز میانی صدور گواهی دیجیتال (CA) را ایفا می‌کند.

گواهی الکترونیکی حاوی اطلاعاتی در مورد مرکز صادر کننده گواهی، مالک گواهی، تاریخ صدور و انقضای، کلید عمومی مالک و یک شماره ریال می‌باشد که توسط یک مرکز صدور گواهی تولید و امضاء شده به گونه‌ای که هر شخص می‌تواند به صحت ارتباط بین کلید عمومی و مالک گواهی اطمینان حاصل کند. در این ارتباط مفاهیم و بخش‌های متفارس قابل تعریف می‌باشند.

با توجه به اهداف سازمان های فناوری اطلاعات در ایران در زمینه توسعه و گسترش امنیت تبادل اطلاعات در فضای سایبر، این کتاب هم‌راستا با پروژه ایجاد مرکز ملی گواهی الکترونیکی این سازمان ها تهیه و تدوین گردیده‌است.

کتاب حاضر به منظور آگاهی رسانی و ارتقای دانش در جامعه فناوری اطلاعات کشور تهیه و در اختیار علاقمندان قرار گرفته است. امید است بتوانیم با نشر مطالبی از این دست، کمکی هر چند اندک به بهبود امنیت فضای تولید و تبادل اطلاعات نماییم.