

الگوریتم‌های امضای دیجیتالی در شبکه‌های کامپیوتری

www.ketab.ir

تألیف: دکتر سید نوراله واله
عضو هیات علمی دانشگاه آزاد اسلامی
واحد تهران شرق

۱۳۹۲

سرشناسه : والہ، سیدنورالہ، ۱۳۲۹ -
عنوان و نام پدیدآور : الگوریتم‌های امضای دیجیتال در شبکه‌های کامپیوتری / تألیف سیدنورالہ والہ.

Algorithms of Digital Signature in Computer Networks

مشخصات نشر : تهران : سید نورالہ والہ، ۱۳۹۲.

مشخصات ظاہری : ۱۲۵ ص. : نمودار.

شابک : 978-964-04-9464-6

وضعیت فهرست نویسی : فیما

موضوع : امضای الکترونیکی

موضوع : کنترل دستیابی

موضوع : کامپیوترها - ایفنی اطلاعات

موضوع : بارگانی الکترونیکی

رده بندی کنگره : ۱۳۹۲ QA۷۶/۹ : ۵۹۲/۹

رده بندی دیویی : ۰۰۵/۸

شماره کتابشناسی ملی : ۲۱۳۸۱۷۹

نام کتاب : الگوریتم‌های امضای دیجیتال در شبکه‌های کامپیوتری

تألیف : دکتر سید نورالہ والہ

ناشر : دکتر سید نورالہ والہ

نوبت چاپ : اول

تیراژ : ۱۰۰۰ جلد

تاریخ انتشار : ۱۳۹۲

چاپ : مهدی

قیمت : ۴۵۰۰۰ ریال

شابک : ۹۷۸-۹۶۴-۰۴-۹۴۶۴-۶

*کلیه حقوق برای مولف محفوظ است

شابک : ۹۷۸-۹۶۴-۰۴-۹۴۶۴-۶

ISBN: 978 - 964 - 04 - 9464 - 6

تلفن : ۸۸۲۵۴۳۰۰ - ۹۱۲۴۴۳۰۸۴

مقدمه

در دنیای امروزه، فن آوری اطلاعات با تکنولوژی ارتباطات از طریق مجموعه‌ای از ماهواره‌ها و شبکه‌های کامپیوتری صورت می‌گیرد بطوریکه در این مجموعه، ویژگی‌های الگوریتم‌های دیجیتالی در عملکرد انتقال اطلاعات مؤثر می‌باشند.

استاندارد ویژگی‌های یک الگوریتم امضای دیجیتالی DSA می‌تواند در تولید یک امضای دیجیتالی و همچنین در آشکار کردن اطلاعات غیرمجاز برای دیتا و سپس تصدیق کردن هویت امضاءکننده آن مورد استفاده قرار گیرد.

از نقطه نظر امنیت اطلاعات، امضای دیجیتالی به معنای نتیجه کارکرد اطلاعاتی خاص با استفاده از تکنیک‌های خاص می‌باشد. هر چند امضای دیجیتالی به معنای هر شکلی از امضای کامپیوتری بوده ولیکن در این مجموعه امضای دیجیتالی بر واژه امنیت اطلاعات استوار می‌باشد.

با امضای دیجیتالی، اطلاعات انتقالی امضاءکننده بصورت سندی معتبر و قانونی تبدیل می‌گردد که در نهایت به تأیید و تصویب ارسال‌کننده آن خواهد رسید. در این راستا مهمترین عامل در امنیت اطلاعات کامپیوتری بر پایه الگوریتم‌های دیجیتالی و رمزنگاری می‌باشد.

در این مجموعه ابتدا در مورد شبکه‌های اینترنتی و سپس در خصوص کسب و کار الکترونیکی و مدل‌های کسب درآمد از طریق شبکه‌های کامپیوتری و سپس در مورد امنیت شبکه‌های الکترونیکی و در نهایت در مورد الگوریتم‌های دیجیتالی در شبکه‌های کامپیوتری بررسی شده است. امید است این مجموعه بتواند مؤثر واقع گردد.

دکتر سید نوراله واله

عضو هیات علمی دانشگاه آزاد اسلامی

واحد تهران شرق

۱۳۹۲

فهرست مطالب

صفحه

عنوان

فصل اول : شبکه های اینترنتی

۱-۱- شکاف دیجیتال.....	۱
۱-۲- زیرساخت های نرم افزاری.....	۱
۱-۳- ساختار شبکه اینترنت.....	۳
۱-۴- معماری شبکه اینترنت.....	۴
۱-۵- ساختارهای مهم لایه های اول، دوم در شبکه های باسیم.....	۵
۱-۶- ساختارهای مهم لایه های اول و دوم در شبکه های بی سیم.....	۷
۱-۷- پرتکل های لایه های سوم و چهارم شبکه.....	۹
- مسیریابی و کنترل اطلاعات.....	۱۰
- پرتکل های لایه انتقال اطلاعات.....	۱۱
- پرتکل های مهم در لایه کاربرد.....	۱۲

فصل دوم : کسب و کار الکترونیکی

۲-۱- کسب و کار الکترونیکی.....	۱۶
۲-۲- زیر بخش های کسب و کار الکترونیکی.....	۱۷
- مدیریت ارتباط با مشتریان.....	۱۸
- برنامه ریزی کلان منابع.....	۱۸
- مدیریت دانش.....	۱۹
- مدیریت روندها.....	۱۹
- سیستم مدیریت اسناد.....	۱۹
- مدیریت منابع انسانی.....	۱۹
- سیستم مدیریت محتوا.....	۲۰
- مدیریت زنجیره تامین.....	۲۰
- سیستم تراکنش های مالی بر خط.....	۲۰
- بازیابی برخط.....	۲۱
۲-۳- مدل های کلی ارتباطات در کسب و کار الکترونیکی.....	۲۱
- دولت- بنگاه.....	۲۲
- دولت- مصرف کننده.....	۲۲
- بنگاه- بنگاه.....	۲۲
- بنگاه- مصرف کننده.....	۲۲
- مصرف کننده- مصرف کننده.....	۲۳
۲-۴- مراحل ایجاد و توسعه کسب و کار الکترونیکی.....	۲۳
مرحله اول : شناسائی و تعریف اهداف.....	۲۳
مرحله دوم : بررسی کسب و کار.....	۲۴
مرحله سوم : بررسی سایر کسب و کارهای مرتبط.....	۲۴
مرحله چهارم : بررسی مشتریان.....	۲۴

مرحله پنجم : بررسی رقبا.....	۲۵
مرحله ششم : طراحی استراتژی بازاریابی.....	۲۵
مرحله هفتم : برنامه ریزی پیاده سازی و عملیاتی شدن.....	۲۵
مرحله هشتم : برنامه ریزی مالی.....	۲۶
مرحله نهم : طراحی دقیق طرح کسب و کار الکترونیکی.....	۲۶
مرحله دهم : بازبینی و توسعه.....	۲۶

فصل سوم : مدل های کسب درآمد در شبکه های کامپیوتری

۳- مدل کسب درآمد اینترنتی.....	۲۷
۳-۱- مدل بازرگانی مرتبط.....	۲۸
- تبادل.....	۲۸
- پرداخت براساس کلیک.....	۲۸
- اشتراک درآمد (پرداخت براساس خرید).....	۲۹
۳-۲- مدل انجمنی.....	۳۰
- کد منبع باز.....	۳۰
- محتوای باز.....	۳۱
- اطلاع رسانی عمومی (عمداری داوطلبانه).....	۳۱
- خدمات شبکه های اجتماعی.....	۳۱
۳-۳- مدل اشتراکی.....	۳۲
- خدمات محتوا.....	۳۲
- خدمات شبکه های فرد به فرد.....	۳۳
- خدمات اطمینانی.....	۳۳
- سرویس دهندگان اینترنت.....	۳۳
۳-۴- مدل کاربردی.....	۳۴
- اندازه گیری مصرف.....	۳۴
- اندازه گیری میزان بهره وری از اشتراک.....	۳۴
۳-۵- مدل تبلیغاتی.....	۳۵
- پرتال عمومی.....	۳۶
- پرتال شخصی.....	۳۷
- پرتال تخصصی.....	۳۷
- تبلیغات دسته بندی شده.....	۳۸
- تبلیغات براساس درخواست جستجو.....	۳۸
- تبلیغات مفهومی.....	۳۹
- ثبت نامی.....	۳۹
- تخفیفی.....	۴۰
۳-۶- مدل واسطه های.....	۴۰
- واسطه حراجی.....	۴۱

عنوان

صفحه

۴۱	- حراجی معکوس (سیستم تجمع درخواست)
۴۲	- بازار تبادل
۴۲	- تجمع خریدار
۴۳	- عامل جستجو
۴۳	- بازار مجازی
۴۴	- تکمیل خرید / فروش
۴۴	- پخش
۴۵	- واسط انعامی
۴۵	- واسط مالی
۴۶	۳-۷ - مدل واسط اطلاعاتی
۴۷	- شبکه های تبلیغاتی
۴۷	- سرویس های سبش مخاطب
۴۷	- بازاریابی انگیزشی
۴۸	- واسط اطلاعاتی کلان
۴۸	۳-۸ - مدل فروش اینترنتی
۴۸	- فروشنده مجازی
۴۹	- فروشنده کاتالوگی
۴۹	- کلیک اندمورتار
۴۹	- فروشنده دیجیتالی
۵۰	۳-۹ - مدل تولیدی
۵۰	- خرید
۵۰	- اجاره
۵۱	- اجازه استفاده
۵۱	- محتوای تجمع شده نام تجاری
	فصل چهارم : امنیت در شبکه های الکترونیکی
۵۲	۴ - امنیت شبکه های پرداخت الکترونیکی
۵۲	۴-۱ - حملات متداول به شبکه های پرداخت الکترونیکی
۵۳	- حملات متداول به سیستم های رایانه ای
۵۵	- خدمات احراز امنیت
۵۵	۴-۲ - اجراء نهادن ترفندهای امنیتی
۵۷	- توابع درهم ریز
۵۷	- ترفند کنترل دسترسی
۵۸	- ترفند تبادل اعتبار
۵۸	- ترفند درج ترافیک
۵۸	- ترفند تازه سازی پیام
۵۸	۴-۳ - مدیریت کلید (رمز نگاری)

پر تکل های تبادل کلید.....	۵۹
توزیع کلید عمومی.....	۵۹
سیستم های امنیت پرداخت الکترونیکی.....	۴-۴-۶۰
امنیت صورت حساب پرداخت.....	۶۱
امنیت پول دیجیتال.....	۶۱
امنیت چک الکترونیکی.....	۶۲
تर्फدهای امنیتی در سیستم پرداخت الکترونیکی.....	۴-۵-۶۲
ناشناس بودن کاربرد و موقعیت.....	۶۳
محرمانه بودن صورتحساب.....	۶۴
ناشناس بودن هزینه کننده.....	۶۴
زیرساختهای امنیتی.....	۴-۶-۶۶
امنیت اتصالات ارتباطی.....	۶۷
امنیت رایانه ها.....	۶۷
امنیت پایانه ها.....	۶۸
امنیت کارتها.....	۶۹

فصل پنجم: الگوریتم های دیجیتالی در شبکه های کامپیوتری

رمز نگاری.....	۵-۱-۷۴
رمز نگاری متقارن (کلید خصوصی).....	۷۶
رمز نگاری نامتقارن (کلید عمومی).....	۷۹
امضای دیجیتالی.....	۵-۲-۸۱
گواهینامه های کلید عمومی.....	۸۵
الگوریتم های امضای دیجیتالی DSA.....	۵-۳-۸۸
الگوریتم نامتقارن برگشت پذیر.....	۸۸
الگوریتم هاشینگ.....	۸۸
استاندارد برای الگوریتم امضای دیجیتالی DSS.....	۵-۴-۹۲
ویژگیهای استاندارد امضای دیجیتالی.....	۵-۵-۹۶
پارامترهای الگوریتم امضای دیجیتالی.....	۹۸
تولید امضاء.....	۹۹
نظم دادن امضاء.....	۹۹
شاخص های تولید امضای دیجیتالی.....	۱۰۰
امضای الکترونیکی.....	۵-۶-۱۱۷
انواع امضای الکترونیکی.....	۱۱۷
پول الکترونیکی.....	۵-۷-۱۲۰
ویژگیهای پول الکترونیکی.....	۱۲۲