

رمزنگاری کاربردی در دات نت و خزانۀ کلید آژور

راهنمای عملی رمزگذاری در دات نت و دات نت هسته

استیفن هونتز

مترجمین:

حسین نجفی خسروشاهی

دانشجوی دکترای مهندسی کامپیوتر

امیرپاک مهر

دانشجوی دکترای مهندسی کامپیوتر

رمزنگاری کاربردی در دات نت و خزانه کلید آژور

راهنمای عملی رمزگذاری در دات نت و دات نت هسته

مؤلف: استیفن هونتز		ترجمه: حسین نجفی خسروشاهی، امیرپاک مهر
طرح جلد و صفحه آرایی: مریم فتاحی		مدیر هنری: شیرین مرتضوی
ناشر: جهاد دانشگاهی واحد چهارمحال و بختیاری		تیراژ: ۵۰۰ نسخه
شابک: ۹۷۸-۶۲۲-۷۲۰۵-۴۲-۸	چاپ: اول / پاییز ۱۴۰۰	۱۱۰/۰۰۰ تومان

سرشناسه: هونتز، استیفن. Haunts, Stephen
عنوان و نام پدیدآور: رمزنگاری کاربردی در دات نت و خزانه کلید آژور؛ راهنمای عملی رمزگذاری در دات نت و دات نت هسته / مؤلف استیفن هونتز؛ ترجمه حسین نجفی خسروشاهی، امیرپاک مهر.
ملاحظات نشر: جهاد دانشگاهی، واحد چهارمحال و بختیاری، انتشارات، ۱۴۰۰.

مشخصات ظاهری: ۳۱۲ ص، مصور.

شابک: ۹۷۸-۶۲۲-۷۲۰۵-۴۲-۸؛ ریل ۱/۱۰۰/۰۰۰

وضعیت فهرست نویسی: فیا

یادداشت: عنوان اصلی: Applied cryptography in .net and Azure key vault: a practical guide to encryption

۲۰۱۹. in .net and .net core

عنوان دیگر: راهنمای عملی رمزگذاری در دات نت و دات نت هسته.

موضوع: نرم افزار مایکروسافت

موضوع: Microsoft software

موضوع: شبکه های کامپیوتری

موضوع: Computer networks

موضوع: کامپیوترها -- ایمنی اطلاعات

موضوع: Computer security

موضوع: مایکروسافت دات نت فریم ورک

موضوع: Microsoft .NET Framework

شناسه افزوده: نجفی خسروشاهی، حسین، ۱۳۶۲-، مترجم

شناسه افزوده: پاک مهر، امیر، ۱۳۶۸-، مترجم

شناسه افزوده: جهاد دانشگاهی، واحد استان چهارمحال و بختیاری، انتشارات

رده بندی کنگره: QA۷۶/۵۸۵

رده بندی دیویی: ۱۶۵/۰۰۴

شماره کتابشناسی ملی: ۸۵۱۹۷۳۷



استان چهارمحال و بختیاری

انتشارات جهاد دانشگاهی واحد چهارمحال و بختیاری
شهرکرد- میرآباد شرقی، نبش میدان جهاد دانشگاهی
ساختمان ستاد جهاد دانشگاهی استان، طبقه دوم
۰۳۸۳۲۲۲۰۳۲۳-۰۳۸۳۲۲۲۰۰۷۰

www.jchb.ir

www.l6book.ir

همه حقوق محفوظ و متعلق به انتشارات جهاد دانشگاهی است.

فهرست

۲۰.....	فصل ۱: نقض داده‌ها چیست؟.....
۲۲.....	انواع داده‌ها در یک نقض و پیامدهای آن‌ها.....
۲۲.....	تأثیر بر یک شرکت.....
۲۳.....	ضرر مالی.....
۲۳.....	دادخواهی.....
۲۳.....	تأثیرات قانون.....
۲۴.....	از دست دادن اعتبار.....
۲۵.....	چرا حفاظت از شبکه به تنهایی کافی نیست؟.....
۲۶.....	چگونه توسعه دهندگان می‌توانند کمک کنند؟.....
۲۷.....	چه انتظاری از این کتاب می‌توانید داشته باشید؟.....
۲۷.....	آنچه شما خواهید آموخت.....
۳۰.....	دانت استاندارد و دانت هسته.....
۳۰.....	نمونه کدها در این کتاب.....
۳۳.....	فصل ۲: تاریخچه مختصر رمزنگاری.....
۳۵.....	زمان‌های قدیم.....
۳۶.....	افزایش پیچیدگی رمز.....
۳۹.....	رمزهای انیگما و مکانیکی.....
۴۲.....	رمزنگاری مدرن.....
۴۲.....	رمزنگاری متقارن.....
۴۴.....	کلید رمزنگاری عمومی و خصوصی.....
۴۵.....	چرا رمزنگاری مهم است؟.....
۴۶.....	نمونه‌هایی از رمزنگاری مدرن.....

۴۸.....	چهار رکن رمزنگاری مدرن.....
۴۸.....	محرم‌انگی.....
۴۸.....	یکپارچگی.....
۴۸.....	احراز هویت.....
۴۹.....	عدم انکار.....
۴۹.....	خلاصه.....
۵۱.....	فصل ۳: اهمیت اعداد تصادفی.....
۵۳.....	تولید اعداد تصادفی قطعی.....
۵۵.....	تولید اعداد تصادفی ایمن.....
۵۸.....	خلاصه.....
۵۹.....	فصل ۴: درهم‌سازی و کدهای تأیید اعتبار درهم‌سازی شده.....
۶۰.....	درهم‌سازی و یکپارچگی.....
۶۲.....	MD5.....
۶۶.....	خانواده الگوریتم درهم‌سازی ایمن.....
۷۱.....	تأیید اعتبار درهم‌سازی.....
۷۹.....	خلاصه.....
۸۱.....	فصل ۵: ذخیره ایمن رمزهای عبور.....
۸۳.....	ذخیره‌گذاری‌ها در حالت واضح.....
۸۴.....	رمزگذاری‌گذاری‌ها.....
۸۵.....	استفاده از درهم‌سازی برای ذخیره‌گذاری‌ها.....
۹۱.....	استفاده از توابع مشتق کلید مبتنی بر گذرواژه.....
۹۸.....	خلاصه.....
۱۰۱.....	فصل ۶: رمزگذاری متقارن.....
۱۰۳.....	رمزگذاری متقارن.....
۱۰۳.....	مزیت: بسیار امن.....

- ۱۰۳..... مزیت: سریع
- ۱۰۴..... عیب: اشتراک کلیدها سخت است
- ۱۰۴..... عیب: خطرناک است اگر تحت کنترل قرار بگیرد
- ۱۰۵..... تاریخچه DES و DES سه‌گانه
- ۱۰۸..... DES و DES سه‌گانه چگونه کار می‌کنند؟
- ۱۱۰..... تاریخچه AES
- ۱۱۱..... AES چگونه کار می‌کند
- ۱۱۲..... AES چقدر در برابر حملات جستجوی فراگیر امن است؟
- ۱۱۴..... مشترکات API در چارچوب دانت
- ۱۱۸..... AcsManaged و AcsCryptoServiceProvider
- ۱۱۸..... انجام رمزگذاری متقارن با دانت
- ۱۳۱..... خلاصه
- ۱۳۳..... فصل ۷: رمزگذاری نامتقارن
- ۱۳۵..... مزیت: بسیار امن
- ۱۳۵..... مزیت: سریع
- ۱۳۵..... عیب: اشتراک کلیدها سخت است
- ۱۳۶..... عیب: خطرناک است اگر تحت کنترل قرار بگیرد
- ۱۳۶..... رمزگذاری نامتقارن چیست؟
- ۱۳۷..... تاریخچه RSA
- ۱۳۸..... RSA چگونه کار می‌کند؟
- ۱۳۸..... مشتق کلید
- ۱۴۱..... رمزگذاری و رمزگشایی
- ۱۴۲..... RSA در دانت
- ۱۴۲..... کلیدهای مقیم در حافظه
- ۱۴۳..... کلیدهای مبتنی بر XML

۱۴۴.....	ارائه دهنده خدمات رمزنگاری.....
۱۴۷.....	رمزگذاری و رمزگشایی.....
۱۵۴.....	خلاصه.....
۱۵۵.....	فصل ۸: امضاهای دیجیتال.....
۱۵۸.....	نگاه سطح بالا به امضاهای دیجیتال.....
۱۶۲.....	امضاهای دیجیتال در داتانت.....
۱۶۹.....	خلاصه.....
۱۷۱.....	فصل ۹: رمزگذاری ترکیبی.....
۱۷۴.....	ترکیب متقارن و نامتقارن.....
۱۸۹.....	اضافه کردن آزمایش‌های یکپارچگی.....
۱۹۶.....	مقایسه آرایه‌های بایت به‌طور امن.....
۱۹۸.....	گسترش با امضاهای دیجیتال.....
۲۰۶.....	خلاصه.....
۲۰۹.....	فصل ۱۰: ذخیره‌سازی کلید و مخزن کلید آژور.....
۲۱۰.....	کاوش در گزینه‌های مدیریت کلید.....
۲۱۳.....	معرفی مخزن کلید آژور.....
۲۱۳.....	حالت سخت‌افزاری مخزن کلید آژور.....
۲۱۴.....	حالت نرم‌افزاری مخزن کلید آژور.....
۲۱۴.....	کلیدها در برابر امنیت.....
۲۱۵.....	مثالی از هزینه‌های مخزن کلید آژور.....
۲۱۷.....	راه‌اندازی مخزن کلید آژور.....
۲۱۸.....	ایجاد مخزن کلید.....
۲۱۹.....	ثبت برنامه خود با دایرکتوری فعال آژور.....
۲۲۲.....	برنامه خود را برای استفاده از کلیدها و محرمانه مجاز کنید.....
۲۲۴.....	ایجاد دستی کلیدها و محرمانه.....

۲۲۷.....	برنامه "Hello World" مخزن کلید آژور.....
۲۴۰.....	خلاصه.....
۲۴۱.....	فصل ۱۱: الگوهای استفاده مخزن کلید آژور.....
۲۴۳.....	محیط‌های چندگانه.....
۲۴۷.....	پیکربندی به عنوان محرمانه.....
۲۵۰.....	بیچش کلید محلی.....
۲۵۸.....	کاوش بیشتر بیچش کلید.....
۲۶۰.....	چرخش کلید و نسخه‌سازی.....
۲۶۱.....	محافظت از گذرواژه.....
۲۷۰.....	تغییر تکرار در طول زمان.....
۲۷۲.....	امضای دیجیتال.....
۲۷۵.....	به روزرسانی مثال رمزگذاری ترکیبی.....
۲۸۸.....	خلاصه.....
۲۸۹.....	فصل ۱۲: خلاصه نهایی.....
۲۹۰.....	خلاصه رمزنگاری.....
۲۹۲.....	اعداد تصادفی.....
۲۹۳.....	درهم‌سازی و احراز هویت.....
۲۹۵.....	ذخیره گذرواژه‌ها.....
۲۹۶.....	رمزگذاری متقارن.....
۲۹۸.....	رمزگذاری نامتقارن.....
۲۹۹.....	امضاها و دیجیتال.....
۳۰۰.....	رمزگذاری ترکیبی.....
۳۰۳.....	مخزن کلید آژور.....
۳۰۷.....	محیط را فراموش نکنید.....
۳۰۸.....	مراحل بعدی.....
۳۰۹.....	واژه‌نامه انگلیسی به فارسی.....

سخن نویسنده استیفن هونتز

دوست دارم این کتاب را به همسرم، آماندا و دو فرزندم، امی و دانیل اختصاص دهم. حمایت آنها باعث می شود تکمیل پروژه های بزرگ مانند این وقتی که خودم در یک اتاق بنشینم و بنویسم، بسیار ساده تر باشد.

درباره نویسنده (استیفن هونتز)

استیفن هونتز در ۲۵ سال گذشته یک توسعه دهنده نرم افزار بوده و در بسیاری از صنایع مانند بازی های ویدئویی، خدمات مالی، بیمه و مراقبت های بهداشتی مشغول به کار بوده است. یکی از اصلی ترین تخصص های وی امنیت و رمزنگاری است و وی در بسیاری از شرکت ها از جمله وام دهندگان مالی، شرکت های مدیریت مطالبات بیمه و بانک های جهانی طیف وسیعی از روش ها را در بسیاری از سیستم ها اجرا کرده است. استیفن مرتباً در کنفرانس ها و گروه های کاربری در مورد برنامه نویسی ایمن در دانت صحبت کرده است و او همچنین یک دوره رمزنگاری با سطح بالا برای Pluralsight تألیف کرده است.