

رمزنگاری عملی (امنیت تبادل اطلاعات)

دیوید وانگ

دکتر ایوب ترکیان

نیاز دانش

سرشناسه	: وانگ، دیوید	Wong, David
عنوان و نام پدیدآور	: رمزنگاری عملی (امنیت تبادل اطلاعات)/دیوید وانگ؛ ترجمه ایوب ترکیان.	
مشخصات نشر	: تهران: نیاز دانش، ۱۴۰۰.	
مشخصات ظاهری	: ۳۲۰ص: مصور(رنگی).	
شابک	: 978-622-7790-00-9	
وضعیت فهرست نویسی	: فیپا	
یادداشت	: عنوان اصلی: Real-World Cryptography.	
موضوع	: رمزنگاری	Cryptography
موضوع	: رمزگذاری داده‌ها	Data encryption (Computer science)
موضوع	: تشخیص هویت	Identification
شناسه افزوده	: ترکیان، ایوب، ۱۳۳۷-، مترجم	
رده بندی کنگره	: Z۱۰۳	
رده بندی دیویی	: ۶۵۲/۸	
شماره کتابشناسی ملی	: ۸۴۱۱۰۶۸	
اطلاعات رکورد کتابشناسی	: فیپا	



نام کتاب : رمزنگاری عملی (امنیت تبادل اطلاعات)

مؤلف : دیوید وانگ

مترجم : دکتر ایوب ترکیان

مدیر اجرایی - ناظر بر چاپ : حمیدرضا محمد شیرازی - محمد شمس

ناشر : نیاز دانش

صفحه‌آرا : واحد تولید انتشارات نیاز دانش

نوبت چاپ : اول - ۱۴۰۰

شمارگان : ۱۰۰ نسخه

قیمت : ۸۶۰۰۰۰ ریال

ISBN: 978-622-7790-00-9

شابک : ۹۷۸-۶۲۲-۷۷۹۰-۰۰-۹

هرگونه چاپ و تکثیر (اعم از زیراکس، بازنویسی، ضبط کامپیوتری و تهیه‌ی CD) از محتویات این اثر بدون اجازه کتبی ناشر ممنوع است، متخلفان به موجب بند ۵ از ماده ۲ قانون حمایت از مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گیرند.

کلیه حقوق این اثر برای ناشر محفوظ است.

آدرس انتشارات: تهران، میدان انقلاب، خیابان ۱۲ فروردین، تقاطع وحید نظری، پلاک ۲۵۵، طبقه ۱، واحد ۲

۰۲۱-۶۶۴۷۸۱۰۶-۶۶۴۷۸۱۰۸-۰۹۱۲۷۰۷۳۹۳۵

www.Niaze-Danesh.com

مشاوره جهت نشر: ۰۹۱۲-۲۱۰۶۷۰۹

فهرست

صفحه	عنوان
۱	فصل اول: مقدمه رمزنگاری.....
۱	۱.۱ دنیای رمزنگاری
۱۶	۲.۱ رمزنگاری دنیای واقعی
۱۹	۳.۱ هشدار
۲۰	۴.۱ خلاصه
۲۱	فصل دوم: توابع هش.....
۲۱	۱.۲ تابع هش
۲۴	۲.۲ خصوصیات امنیتی تابع هش
۲۷	۳.۲ ملاحظات امنیتی توابع هش
۲۸	۴.۲ توابع هش در عمل
۳۰	۵.۲ توابع هش استاندارد شده
۴۱	۶.۲ هش کردن رمزعبورها
۴۳	۷.۲ خلاصه
۴۴	فصل سوم: کدهای احراز هویت پیام
۴۴	۱.۳ کد احراز هویت پیام
۴۷	۲.۳ خصوصیات امنیتی کد احراز هویت پیام
۵۰	۳.۳ MAC در دنیای واقعی
۵۱	۴.۳ کدهای احراز هویت پیام در عمل
۵۳	۵.۳ SHA-2 و حملات بسط طول
۵۶	۶.۳ خلاصه
۵۷	فصل چهارم: کدهای احراز هویت شده
۵۷	۱.۴ رمز
۶۰	۲.۴ رمزگذاری متقارن در دنیای واقعی
۶۱	۳.۴ الگوریتم رمزگذاری AES-CBC-HMAC
۷۱	۴.۴ رمزگذاری احراز هویت شده با داده‌های ذی ربط (AEAD)
۸۲	۵.۴ کلیدپوشی و مقاومت سوءاستفاده نانس
۸۵	۶.۴ نگاشت رمزگذاری احراز هویت شده
۸۶	۷.۴ دیگر انواع رمزگذاری متقارن
۸۹	۸.۴ خلاصه

۹۰	فصل پنجم: تبادل کلید
۹۱	۱.۵ تبادل کلید
۹۵	۲.۵ استانداردهای تبادل کلید
۱۰۸	۳.۵ خلاصه
۱۱۰	فصل ششم: رمزنگاری نامتقارن و هیبریدی
۱۱۰	۱.۶ رمزگذاری نامتقارن
۱۱۲	۲.۶ رمزگذاری نامتقارن در عمل و هیبریدی
۱۱۸	۳.۶ استانداردهای رمزگذاری نامتقارن و هیبریدی
۱۲۳	۴.۶ RSA PKCS#1 v1.5
۱۲۵	۵.۶ رمزگذاری نامتقارن با RSA-OAEP
۱۲۷	۶.۶ رمزگذاری هیبریدی با ECIES
۱۳۰	۷.۶ خلاصه
۱۳۱	فصل هفتم: امضاءهای الکترونیک
۱۳۱	۱.۷ امضاء الکترونیک
۱۳۴	۲.۷ خصوصیات امنیتی و ملاحظات
۱۳۶	۳.۷ استانداردهای امضاء الکترونیک
۱۴۴	۴.۷ خلاصه
۱۴۵	فصل هشتم: راندوم بودن و اسرار
۱۴۵	۱.۸ راندوم بودن
۱۴۷	۲.۸ مولد عدد شبه‌راندومی (PRNG)
۱۵۱	۳.۸ حصول راندوم بودن در عمل
۱۵۴	۴.۸ تولید راندومی و ملاحظات امنیتی
۱۵۶	۵.۸ راندومی عمومی
۱۵۸	۶.۸ استخراج کلید با HKDF
۱۶۲	۷.۸ مدیریت کلیدها و اسرار
۱۶۳	۸.۸ پرهیز از مدیریت کلید، یا نحوه تقسیم اعتماد
۱۶۶	۹.۸ خلاصه
۱۶۸	فصل نهم: انتقال امن
۱۶۸	۱.۹ SSL/TLS
۱۷۳	۲.۹ نحوه کار TLS
۱۸۷	۳.۹ وضعیت وب رمزگذاری شده
۱۹۰	۴.۹ دیگر پروتکل‌های انتقال امن
۱۹۵	۵.۹ خلاصه

۱۹۶	فصل دهم: رمزنگاری مبدأ به مقصد
۱۹۶	۱.۱۰ ضرورت رمزنگاری مبدأ به مقصد
۱۹۸	۲.۱۰ ناپیدایی ریشه اعتماد
۱۹۹	۳.۱۰ ایمیل‌های رمزگذاری شده، PGP و عدم موفقیت وب اعتماد
۲۰۱	۴.۱۰ پیام‌دهی امن، دور شدن از PGP
۲۱۳	۵.۱۰ خلاصه
۲۱۵	فصل یازدهم: احراز هویت کاربر
۲۱۵	۱.۱۱ خلاصه مبحث احراز هویت
۲۱۸	۲.۱۱ احراز هویت کاربر
۲۳۶	۳.۱۱ احراز هویت با کمک کاربر
۲۴۴	۴.۱۱ خلاصه
۲۴۶	فصل دوازدهم: رمزنگاری در ارز دیجیتال
۲۴۷	۱.۱۲ مبانی الگوریتم‌های وفاق روم شرقی
۲۴۹	۲.۱۲ شیوه کار بیت‌کوین
۲۵۸	۳.۱۲ تور ارز دیجیتال
۲۶۰	۴.۱۲ نحوه کار لیبرا
۲۶۶	۵.۱۲ خلاصه
۲۶۸	فصل سیزدهم: رمزنگاری سخت‌افزاری
۲۶۸	۱.۱۳ مدل مهاجم رمزنگاری نوین
۲۷۰	۲.۱۳ محیط‌های غیرقابل اعتماد
۲۸۲	۳.۱۳ راهکار پیشنهادی
۲۸۴	۴.۱۳ رمزنگاری تاب‌آور به نشت
۲۹۰	۵.۱۳ خلاصه
۲۹۳	پیوست الف: رمزنگاری سطح کاراکتر -۲

فصل ۱

مقدمه رمزنگاری

۱.۱ دنیای رمزنگاری^۱

سفر ما از اینجا با مقدمه رمزنگاری، دانش پروتکل‌های حفاظتی که دشمنان می‌توانند به صورت فعال سعی در خرابکاری آن داشته باشند، شروع می‌شود.

یادداشت پروتکل هر سناریویی است که در آن، چندین شرکت‌کننده (شامل افراد بالقوه بد نیت)، سعی در دست یافتن به چیزی دارند. فضای زیر را تصور کنید: مدنظر است که اسلحه جاودیدی خویش را برای چند ساعت برای استراحت کردن ترک کنید. یک پروتکل برای انجام این کار به صورت زیر است:

- اسلحه را زیر زمین خاک کنید.
- زیر درخت استراحت کنید.
- اسلحه را از زیر زمین بازیابی نمایید.

در زمان‌های قدیم، در موقعی که شاهان و ژنرال‌ها مشغول خیانت به یکدیگر و برنامه‌ریزی برای کودتا بودند، بزرگترین مسئله آنها یافتن روشی برای به اشتراک گذاشتن اطلاعات محرمانه با افرادی بودند که به آنها اعتماد داشتند. از این مسایل، ایده رمزنگاری متولد شد. ولی امروزه، رمزنگاری همه جا وجود داشته، تا در فضای دنیای پر از آشوب و متخصص، پایه‌ای‌ترین خدمات را بتوان ارائه داد.

داستان این کتاب درباره روش رمزنگاری در جهان نوین است. سفری به دنیای محاسباتی شروع شده، تا پروتکل‌های فعلی پوشش داده شده، نشان داده شود از چه بخش‌هایی تشکیل شده، و چگونه همه آنها به یکدیگر وصل می‌شوند. تقریباً فرمول‌های ترسناک ریاضی وجود نخواهد داشت. هدف این