رمزنگاری عملی

(امنیت تبادل اطلاعات)

دیوید وانگ

دکتر ایوب ترکیان

نیاز دانش

فهرست

عنوان **صفحه**

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

فصل پنجم: تبادل کلید ۹۰
۱.۵ تبادل کلید ۹۱
۲.۵ استانداردهای تبادل کلید ۹۵
۳.۵ خلاصه ۱۰۸
فصل ششم: رمزنگاری نامتقارن و هیبریدی ۱۱۰
۱.۶ رمزگذاری نامتقارن ۱۱۰
۲.۶ رمزگذاری نامتقارن در عمل و هیبریدی ۱۱۲
۳.۶ استانداردهای رمزگذاری نامتقارن و هیبریدی ۱۱۸
۴.۶ RSA PKCS#1 v۱/۵ ۱۲۳
۵.۶ رمزگذاری نامتقارن با RSA-OAEP ۱۲۵
۶.۶ رمزگذاری هیبریدی با ECIES ۱۲۷
۷.۶ خلاصه ۱۳۰
فصل هفتم: امضاءهای الکترونیک ۱۳۱
۱.۷ امضاء الکترونیک ۱۳۱
۲.۷ خصوصیات امنیتی و ملاحظات ۱۳۴
۳.۷ استانداردهای امضاء الکترونیک ۱۳۶
۴.۷ خلاصه ۱۴۴
فصل هشتم: راندوم بودن و اسرار ۱۴۵
۱.۸ راندوم بودن ۱۴۵
۲.۸ مولد عدد شبه‌راندومی (PRNG) ۱۴۷
۳.۸ حصول راندوم بودن در عمل ۱۵۱
۴.۸ تولید راندومی و ملاحظات امنیتی ۱۵۴
۵.۸ راندومی عمومی ۱۵۶
۶.۸ استخراج کلید با HKDF ۱۵۸
۷.۸ مدیریت کلیدها و اسرار ۱۶۲
۸.۸ پرهیز از مدیریت کلید، یا نحوه تقسیم اعتماد ۱۶۳
۹.۸ خلاصه ۱۶۶
فصل نهم: انتقال امن ۱۶۸
۱.۹ SSL/TLS ۱۶۸
۲.۹ نحوه کار TLS ۱۷۳
۳.۹ وضعیت وب رمزگذاری شده ۱۸۷
۴.۹ دیگر پروتکل‌های انتقال امن ۱۹۰
۵.۹ خلاصه ۱۹۵

فصل دهم: رمزنگاری مبدأ به مقصد ۱۹۶
۱.۱۰ ضرورت رمزنگاری مبدأ به مقصد ۱۹۶
۲.۱۰ ناپیدایی ریشه اعتماد ۱۹۸
۳.۱۰ ایمیل‌های رمزگذاری شده، PGP و عدم موفقیت وب اعتماد ۱۹۹
۴.۱۰ پیام‌دهی امن، دور شدن از PGP ۲۰۱
۵.۱۰ خلاصه ۲۱۳
فصل یازدهم: احراز هویت کاربر ۲۱۵
۱.۱۱ خلاصه مبحث احراز هویت ۲۱۵
۲.۱۱ احراز هویت کاربر ۲۱۸
۳.۱۱ احراز هویت با کمک کاربر ۲۳۶
۴.۱۱ خلاصه ۲۴۴
فصل دوازدهم: رمزنگاری در ارز دیجیتال ۲۴۶
۱.۱۲ مبانی الگوریتم‌های وفاق روم شرقی ۲۴۷
۲.۱۲ شیوه کار بیت‌کوین ۲۴۹
۳.۱۲ تور ارز دیجیتال ۲۵۸
۴.۱۲ نحوه کار لیبرا ۲۶۰
۵.۱۲ خلاصه ۲۶۶
فصل سیزدهم: رمزنگاری سخت‌افزاری ۲۶۸
۱.۱۳ مدل مهاجم رمزنگاری نوین ۲۶۸
۲.۱۳ محیط‌های غیرقابل اعتماد ۲۷۰
۳.۱۳ راهکار پیشنهادی ۲۸۲
۴.۱۳ رمزنگاری تاب‌آور به نشت ۲۸۴
۵.۱۳ خلاصه ۲۹۰
پیوست الف: رمزنگاری سطح کاراکتر ـ۲ ..... ۲۹۳

فصل ۱

مقدمه رمزنگاری

۱.۱ دنیای رمزنگاری[1]

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

یاداداشت 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 جاودیی 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 متخاصم، پایه‌ای‌ترین خدمات را بتوان ارایه 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

1 cryptography