

۱۳۹۴

امنیت شبکه

www.ketab.ir

دکتر سید نوراله واله
استاد دانشگاه آزاد اسلامی
واحد تهران شرق
۱۳۹۴

بسم الله الرحمن الرحيم

سرشناسه	: والد، سید نواله، ۱۳۲۹ -
عنوان و نام پدید آور	: امنیت شبکه / سید نور اله واله.
مشخصات نشر	: تهران: سید نوراله واله، ۱۳۹۴.
مشخصات ظاهری	: ۹۴ ص.: مصور، جدول، نمودار.
شابک	: 978-600-04-4219-4
وضعیت فهرست نویسی	: فیبا
عنوان اصلی	: Network Security
موضوع	: شبکه های کامپیوتری - - تدابیر ایمنی
موضوع	: کامپیوترها - ایمنی اطلاعات
موضوع	: رمزگذاری داده ها
رده بندی کنگره	: ۱۳۹۴ ۸ الف و ۵۹/۵۱۰۵ TK
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۴۱۱۱۴۶۲

نام کتاب	: امنیت شبکه
تالیف	: دکتر سید نوراله واله
ناشر	: ناشر مولف دکتر سید نوراله واله
نوبت چاپ	: اول
چاپ	: مهدی
تیراژ	: ۵۰۰ نسخه
قیمت	: ۵۰،۰۰۰ ریال
تاریخ انتشار	: ۱۳۹۴
شابک	: ۹۷۸-۶۰۰-۰۴-۴۲۱۹-۴

*کلیه حقوق برای مؤلف محفوظ است.

شابک: ۹۷۸-۶۰۰-۰۴-۴۲۱۹-۴

ISBN: 978-600-04-4219-4

تلفن: ۸۸۲۵۴۳۰۰ - ۰۹۱۲۴۴۳۰۸۴۰

رمزنگاری، ابزاری است مؤثر برای محرمانه نگاه داشتن اطلاعات و اطمینان از صحت و هویت آنها است. سیستم‌های رمزنگاری جدید براساس قانون کرکهف، بنا شده‌اند؛ یعنی الگوریتم بکار رفته در آنها آشکار و عمومی و فقط کلید رمز، سری است. بسیاری از الگوریتم‌های رمزنگاری، از تبدیلات پیچیده ریاضی شامل عملیات جانشینی و جایگشتی برای تبدیل متن به رمز، بهره گرفته‌اند، ولیکن هرگاه رمزنگاری کوانتومی بتواند در محیط عمل وارد شود، روش One - Time - Pad یک سیستم رمزنگاری واقعاً غیر شکست، ارائه خواهد شد.

الگوریتم‌های رمزنگاری را می‌توان به دو دسته تقسیم بندی کرد: الگوریتم‌های با کلید متقارن و الگوریتم‌های با کلید عمومی. الگوریتم‌های با کلید متقارن، بیت‌های متن را در چندین مرحله و براساس پارامترهای مشترک شده از کلید اصلی ترکیب و مخلوط می‌کنند تا در نتیجه متن رمز شده، به دست آید. در حال حاضر الگوریتم AES (Rijndael) و Triple DES مشهورترین الگوریتم‌ها با کلید متقارن هستند. از این الگوریتم‌ها می‌توان در حالت‌های Electronic Code Book و Cipher Block Chaining Mode و Counter Mode و Stream Cipher Mode و نظایر آن بهره گرفت. الگوریتم رمزنگاری با کلید عمومی این ویژگی را دارد که کلیدهای رمزنگاری و رمزگشایی متفاوت از یکدیگر هستند و نمی‌توانند با داشتن کلید رمزنگاری، کلید رمزگشایی را استخراج کرد، این ویژگی اجازه می‌دهد تا بتوان کلیدهای عمومی را منتشر کرد. اما برای رمزگشایی الگوریتم کلید عمومی RSA است که قدرت خود را از آنجایی به دست آورده که تجزیه اعداد بزرگ با عامل اول، بسیار بسیار دشوار است.

امروزه وب جولانگاه اخلاص‌گران و ترودیهای است که به کارهای مختلف خود مشغولند، امنیت شبکه دربر گیرنده عناوین و موارد بسیار گسترده است. همچنین امنیت را می‌توان در ارتباط با افرادی تعبیر کرد که تلاش میکنند به سرویس‌های راه دور در شبکه راه پیدا کنند بنابراین به تکنیک‌هایی جهت احراز هویت مبتنی بر رمزنگاری نیاز می‌باشد. در مجموع، مهمترین عامل امنیت شبکه، الگوریتم‌های رمزنگاری در آن شبکه می‌باشد. امید است این مجموعه مؤثر و مفید واقع گردد.

دکتر سید نوراله واله

استاد دانشگاه آزاد اسلامی واحد تهران شرق

۷	فصل اول
۷	رمزنگاری
۹	رمزهای جانشینی (Substitution Cipher)
۱۱	رمزنگاری جایگشتی (Transposition)
۱۲	رمز one time – pad (به هم ریزی محتوی پیام)
۱۸	دو اصل اساسی در رمزنگاری
۲۰	الگوریتم‌های رمزنگاری با کلید متقارن (Symmetric-Key)
۲۱	رمزنگاری DES (Data Encryption Standard)
۲۴	استاندارد پیشرفته رمزنگاری AES
۲۸	الگوریتم‌های کلید عمومی (Public Key)
۳۰	RSA
۳۱	الگوریتم‌های کلید عمومی دیگر
۳۲	امضاهای دیجیتالی
۳۲	امضاهای دیجیتال با کلید متقارن
۳۴	امضاهای با کلید عمومی
۳۶	خلاصه‌ی پیامها (Message Digests)
۳۹	حمله روز تولد
۴۱	فصل دوم
۴۱	امنیت ارتباطات
۴۱	IPSec
۴۵	دیوار آتش
۵۰	شبکه خصوصی VPN

امنیت شبکه‌های بی سیم.....	۵۷
امنیت وب.....	۶۲
نامگذاری مطمئن.....	۶۲
SSL، لایه سوکتهای امن.....	۶۴
امنیت کدهای محرک.....	۶۷
فصل سوم	۷۱
پروتکل‌های احراز هویت.....	۷۱
احراز هویت براساس کلید مشترک و سری.....	۷۲
ایجاد کلید مشترک.....	۷۴
احراز هویت توسط مرکز توزیع کلید (IDC).....	۷۵
پروتکل احراز هویت نیدهام - شرور.....	۷۸
پروتکل احراز هویت « آتوی - ریس ».....	۸۲
روش احراز « هویت قورباغه دهان گشاد » (Wide Mouthed Frog).....	۸۴
احراز هویت با KERBEROS.....	۸۵
احراز هویت با استفاده از کلید عمومی.....	۹۰
فهرست مراجع.....	۹۳