امنیت شبکه

دکتر سید نوراله واله
استاد دانشگاه آزاد اسلامی
واحد تهران شرق

۱۳۹۴

بسم الله الرحمن الرحیم

سرشناسه	: واله، سید نواله، ۱۳۲۹ -
عنوان و نام پدید آور	: امنیت شبکه / سید نور اله واله.
مشخصات نشر	: تهران: سید نوراله واله، ۱۳۹٤.
مشخصات ظاهری	:۹٤ ص.: مصور ، جدول ، نمودار.
شابک	:978-600-04-4219-4
وضعیت فهرست نویسی	: فیپا
عنوان اصلی	: Network Security
موضوع	: شبکه های کامپیوتری- - تدابیر ایمنی
موضوع	: کامپیوترها- -ایمنی اطلاعات
موضوع	: رمزگذاری داده ها
رده بندی کنگره	: ۱۳۹٤ ۸ الف۲و/TK۵۱۰۵/۵۹
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ٤۱۱۱٤٦۲

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	:	۱۳۹٤
شابک	:	۹۷۸-٦۰۰-۰٤-٤۲۱۹-

شابک: ۹۷۸-۶۰۰-۰۴-۴۲۱۹-۴

ISBN: 978-600-04-4219-4

تلفن: ۰۹۱۲٤٤۳۰۸٤۰ - ۸۸۲۵٤۳۰۰

مقدمه

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 کوانتمی بتواند درمحیط 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 مشتق 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 الگوریتم ها 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 دارند 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. اصلی‌ترین الگوریتم کلید عمومی RSA است که قدرت خود را از آنجایی به دست آورده که تجزیه اعداد بزرگ به عامل اول، بسیار بسیار دشوار است .

اسناد قانونی، تجاری و نظایر آن ها، نیازمند امضا هستند. بر این اساس روش‌های متنوعی برای امضای دیجیتالی ابداع شده که در آن هم از الگوریتم‌های رمزنگاری با کلید متقارن و هم از روش‌های کلید عمومی، بهره گرفته شده است.

امروزه وب جولانگاه اخلالگران و ترودیهایی است که به کارهای 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

۱۳۹۴

فهرست مطالب

عنوان — صفحه