

رمزگذاری و رمزگشایی داده های کامپیوتری

www.ketab.ir

نویسندگان: مهدی نجف زاده، خلیل کولیوند

سرشناسه: نجف زاده، مهدی ۱۳۵۰
عنوان و نام نویسندگان: رمز گذاری و رمز گشایی داده های کامپیوتری/ نجف زاده، مهدی ۱۳۵۰ - کولیوند، خلیل ۱۳۶۰
ویراستار: عمادی سرخی، سیدمحمد رضا، ۱۳۶۳
وضعیت ویراست: اول
مشخصات نشر: تهران: نیروی پدافند ارتش جمهوری اسلامی ایران ۱۳۹۹
مشخصات ظاهری: ۱۷۶ صفحه، مصور، جدول، رنگی
شابک: ۹۷۸-۶۰۰-۸۹۸۰-۸۱-۰۰
قیمت: ۳۵۰۰۰۰ ریال
وضعیت فهرست نویسی: فیبا
عنوان اصلی:

رمز گذاری و رمز گشایی داده های کامپیوتری

موضوع: شبکه های کامپیوتری - - تدابیر ایمنی
موضوع: رمز گذاری داده ها - - رمز نگاری
موضوع: کامپیوترها - - ایمنی اطلاعات
شناسه افزوده: کولیوند، خلیل ۱۳۶۰
شناسه افزوده: عمادی سرخی، سیدمحمد رضا، ۱۳۶۳
شناسه افزوده: تهران: ارتش. نیروی پدافند هوایی آجا
رده بندی کنگره: TK ۵۱۰۵ / ۵۹
رده بنده دیویی: ۰۰۵/ ۸۲
شماره کتابشناسی ملی: ۸۴۰۳۱۱۴



www.ketab.ir

عنوان: رمز گذاری و رمز گشایی داده های کامپیوتری

نویسندگان: مهدی نجف زاده، خلیل کولیوند

ویراستار: سید محمد رضا عمادی سرخی

طراح جلد و صفحه آرا: علی قموشی

ناظر نشر: سید محمد رضا عمادی سرخی

مدیر برنامه ریزی: جواد سلطانیان

ناشر: قرارگاه پدافند هوایی خاتم الانبیاء (ص) آجا

چاپ و صحافی: مرکز مطالعات راهبردی ن پ ه آجا

شابک: ۹۷۸-۶۰۰-۸۹۸۰-۸۱-۰۰

شمارگان: ۱۰۰۰ نسخه

چاپ اول: ۱۴۰۰

قیمت: ۳۵۰۰۰۰ ریال

نشانی: تهران، بزرگراه بسیج، بلوار هجرت، ستاد نیروی پدافند هوایی آجا

تلفن: ۰۲۱)۳۳۲۴۰۴۶۸ (۰۲۱) دورنگار: ۰۲۱)۳۳۲۴۰۴۶۹

* کلیه حقوق این اثر به انتشارات نیروی پدافند هوایی آجا تعلق دارد *

امروزه در دنیای دیجیتال حفاظت از اطلاعات رکن اساسی و مهمی در تبادلات پیام‌ها و مبادلات تجاری ایفا می‌نماید. برای تأمین نیازهای امنیتی تراکنش امن، از رمزنگاری استفاده می‌شود. با توجه به اهمیت این موضوع و گذار از مرحله سنتی به مرحله دیجیتال آشنایی با روش‌های رمزگذاری ضروری به نظر می‌رسد. در این مطالب ضمن بررسی الگوریتم‌های رمزنگاری کلید عمومی (نامتقارن) و کلید خصوصی (متقارن)، جنبه‌های گوناگون کلید عمومی مورد بررسی قرار می‌گیرد و ویژگی‌های هر کدام بیان می‌گردد.

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و برای قرن‌ها به‌منظور محافظت از پیام‌هایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل می‌شده، استفاده شده است تا پیام‌های آن‌ها محرمانه بماند.

هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیام داریم و در ضمن باید از عدم تغییر محتوای پیام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند.

اغلب این مسئله باید تضمین شود که یک پیام فقط می‌تواند توسط کسانی خوانده شود که پیام برای آن‌ها ارسال شده است و دیگران این اجازه را ندارند. روشی که تأمین‌کننده این مسئله باشد "رمزنگاری" نام دارد. رمزنگاری هنر نوشتن به‌صورت رمز است بطوریکه هیچ‌کس به‌غیر از دریافت‌کننده موردنظر نتواند محتوای پیام را بخواند.

مهدی نجف زاده ۱۳۹۹