

سرشناسه	: موجبی، محمود، ۱۳۵۹ -
عنوان و نام پدیدآور	: الگوریتم‌های رمزنگاری متقارن و نامتقارن : معرفی الگوریتم‌های رمزنگاری و مروری بر حملات پایه مخابرات - الکترونیک کامپیوتر/ تالیف محمود موجبی، امین جعفری ؛ [برای] شرکت مخابراتی و الکترونیکی موج نصر گستر.
مشخصات نشر	: تهران: آرنا، ۱۳۹۲.
مشخصات ظاهری	: ۳۰۰ص.
شابک	: ۹۷۸-۶۰۰-۷۰۳۶-۱۹-۹
وضعیت فهرست نویسی	: فیبا
عنوان دیگر	: معرفی الگوریتم‌های رمزنگاری و مروری بر حملات پایه مخابرات - الکترونیک کامپیوتر
موضوع	: الگوریتم‌های کامپیوتری
موضوع	: رمزنگاری
شناسه افزوده	: جعفری، امین، ۱۳۵۴ -
شناسه افزوده	: شرکت مخابراتی و الکترونیکی موج نصر گستر
رده بندی کنگره	: ۰۰۵/۱۳۰۳۸ : ۱۳۹۲۷/۹/۷۰۳۶-۱۹ م
رده بندی دیویی	: ۰۰۵/۱۳۰۳۸
شماره کتابشناسی ملی	: ۲۱۶۲۳۷۷



عنوان	: الگوریتم‌های رمزنگاری متقارن و نامتقارن
مؤلف	: مهندس محمود موجبی - مهندس امین جعفری
ناشر	: آرنا
ناظر چاپ	: مرتضی هانی
صفحه آرایي	: فرشته زند
طراح جلد	: سید مرتضی مختاری آل هاشم
نوبت چاپ	: اول ۱۳۹۲
شمارگان	: ۱۰۰۰ نسخه
شابک	: 978-600-7026-19-9
قیمت	: ۱۲۰۰۰ تومان

فهرست مطالب

عنوان	صفحه
فصل اول: مقدمه‌ای بر رمزنگاری	۱۱
۱-۱. مقدمه	۱۲
۲-۱. رمزنگاری چیست؟	۱۳
۱-۲-۱. رمزنگاری - پنهان کاری، کدگذاری	۱۳
۲-۲-۱. تاریخچه رمزنگاری	۱۴
۳-۲-۱. مراحل تکامل رمزنگاری	۱۵
۴-۲-۱. اصول ششگانه کرکف	۱۸
۳-۱. تعاریف و اصطلاحات رمزنگاری	۱۹
۱-۳-۱. مفاهیم اولیه	۱۹
۲-۳-۱. اهداف رمزنگاری	۲۰
۳-۳-۱. پروتکل رمزنگاری	۲۱
۴-۳-۱. الگوریتم رمزنگاری	۲۲
۵-۳-۱. پایه علم رمزنگاری	۲۳
۶-۳-۱. کاربردهای علم رمزنگاری	۲۴
۷-۳-۱. انواع مختلف رمزنگاری	۲۵
فصل دوم: مقدمه‌ای بر رمزنگاری کلاسیک	۲۷
۱-۲. مقدمه	۲۸
۲-۲. سیستم رمز شیف	۳۰
۳-۲. سیستم رمز جانشینی	۳۷
۴-۲. سیستم رمز آفین	۳۹
۵-۲. سیستم رمز ویگنر	۴۵
۶-۲. سیستم رمز هیل	۴۸
۷-۲. سیستم رمز جایگشتی	۵۶

۵۹	۸-۲. رمز جریانی
۶۷	فصل سوم: الگوریتم‌های رمزنگاری متقارن
۶۸	۱-۳. معرفی رمزنگاری متقارن
۶۹	۲-۳. سیستم رمز بلوکی
۷۴	۱-۲-۳. شبکه‌های جانشینی - جایگشتی
۸۱	۲-۲-۳. سیستم رمز DES
۹۹	۳-۲-۳. سیستم رمز 3DES
۹۹	۴-۲-۳. سیستم رمز AES
۱۱۲	۵-۲-۳. سیستم رمز RC5
۱۲۰	۳-۳. سیستم رمز جریانی
۱۲۲	۱-۳-۳. شیفت رجیستر با بازخورد خطی (LFSR)
۱۲۶	۲-۳-۳. پیچیدگی خطی، مشخصات پیچیدگی خطی، اصول گالامپ
۱۳۱	۳-۳-۳. طرح‌های مبتنی بر LFSR
۱۳۳	۴-۳-۳. سیستم رمز A5/1
۱۳۶	۵-۳-۳. سیستم رمز A5/2
۱۳۹	فصل چهارم: الگوریتم‌های رمز نامتقارن
۱۴۰	۱-۴. معرفی سیستم رمز نامتقارن
۱۴۲	۲-۴. مزایا و معایب رمزنگاری کلید عمومی در مقایسه با رمزنگاری کلید خصوصی
۱۴۳	۳-۴. پیش‌زمینه‌های ریاضی الگوریتم‌های رمزنگاری نامتقارن
۱۴۳	۱-۳-۴. آزمون اول بودن اعداد
۱۵۰	۲-۳-۴. لگاریتم گسسته
۱۵۷	۴-۴. الگوریتم رمزنگاری نامتقارن
۱۵۷	۱-۴-۴. الگوریتم رمزنگاری RSA
۱۶۰	۲-۴-۴. الگوریتم تبادل کلید دیفی-هلمن
۱۶۳	۵-۴. مدیریت کلید
۱۶۴	۱-۵-۴. تولید کلیدها
۱۶۵	۲-۵-۴. ارسال و توزیع کلیدها در شبکه‌های بزرگ

۱۶۶	۳-۵-۴. تصدیق کلیدها.....
۱۶۷	۴-۵-۴. طول عمر کلیدها.....
۱۶۸	۵-۵-۴. مدیریت کلید توسط روش های کلید عمومی.....
۱۷۱	فصل پنجم: تحلیل رمز و اصول رمز شکنی.....
۱۷۲	۱-۵. حمله و رمز شکنی.....
۱۷۴	۲-۵. جدول احتمالات اتفاق ۲۶ حرف در زبان انگلیسی.....
۱۷۶	۳-۵. تحلیل سیستم رمز آفین.....
۱۷۸	۴-۵. تحلیل سیستم رمز جاسینی.....
۱۸۲	۵-۵. تحلیل سیستم رمز ویکتر.....
۱۸۸	۶-۵. تحلیل سیستم رمز هیل.....
۱۸۹	۷-۵. تحلیل رمز جریانی شیفتر رجیستر با بازخورد خطی.....
۱۹۱	۸-۵. سایر حملات.....
۱۹۳	منابع.....

سخن مدیر عامل

«سپس، به کاتبان و نویسندگان بنگر و بهترین آن ها را بر کارهای خود بگمار...
کاتبان و نویسندگانی برگزین که قدر خود را بشناسند، چون کسی که به قدر خود شناخت ندارد، دیگران را هم نمی شناسد.»

«برگرفته از نامه ۵۳ نهج البلاغه به مالک اشتر»
حمد و سپاس و ثنای خداوند یکتا را که فرصتی بخشید تا با تقدیم کتابی با ارزش بتوانیم نسبت به کشور عزیز و اسلامی ایران ادای وظیفه بنماییم و بتوانیم از طریق نشر علوم و فنون بر غنای فرهنگی و علمی این مرز و بوم بیفزاییم.
کتاب حاضر بر پایه اصول طراحی و ارائه الگوریتمهای رمز نگاری و بر اساس جدید ترین دستاوردها برای استفاده اهل علم و دانش تدوین شده است.
بدیهی است چنانچه در این کتاب اشکالی مشاهده فرمودید و یا مطالب دیگری که می توانست بر غنای علمی این کتاب بیفزاید ما را مطلع نموده تا در چاپهای بعدی اعمال گردد.

شایان ذکر است از زحمات شادروان مهندس احمد رضا رئیسی، مهندس علی صادقوند، مهندس حسن بهجتی راد، مهندس حمیدرضا حسینی، مهندس حبیب پارسا و سایر عزیزان که ما را در تالیف این کتاب یاری رساندند کمال تقدیر و تشکر را دارم.
در پایان لازم به ذکر است که این شرکت جهت پیشرفت علمی و فنی و همچنین خود کفایی در زمینه تولید علم و فناوری کشور عزیزمان ایران بعد از استعانت از حضرت حق تبارک و تعالی، دست کمک و یاری و همکاری تمامی اساتید و فرهیختگان را به گرمی و صمیمی می فشارد.

مدیر عامل شرکت مخابراتی و الکترونیکی موج نصر گستر

مسعود ترکمن