

علم رمزنگاری و هنر تحلیل رمز

به انضمام: راهنمای کامل الگوریتم‌های ژنتیک و اصول رمزنگاری کوانتومی

تألیف و گردآوری

ناصر آقا جان زاده

محمد مهدی درفشی

مجید جان نثاری



**NAGHOOS
PUBLICATION**

سرشناسه	: آقاچان زاده، ناصر، ۱۳۶۶-
عنوان و نام پدیدآور	: علم رمزنگاری و هنر تحلیل رمز: به انضمام راهنمای کامل الگوریتم‌های ژنتیک و اصول رمزنگاری کوانتومی/ تألیف و گردآوری ناصر آقاچان زاده، محمدمهدی درفش، مجید جان نثاری.
مشخصات نشر	: تهران: انتشارات ناقوس، ۱۳۹۱.
مشخصات ظاهری	: ۲۳۱ ص: مصور، جدول. + یک لوح فشرده.
شابک	: ۹-۵۳۶-۳۷۷-۹۶۴-۹۷۸ بها: ۹۰۰۰۰ ریال به همراه CD
وضعیت فهرست نویسی	: فیفا
موضوع	: رمزنگاری
موضوع	: رمزنگاری داده‌ها
موضوع	: کامپیوترها--ایمنی اطلاعات
موضوع	: الگوریتم‌های ژنتیک
شناسه افزوده	: درفش، محمدمهدی، ۱۳۶۵-
شناسه افزوده	: جان نثاری، مجید، ۱۳۶۲-
رده بندی کنگره	: Z ۱۰۳۱۷ع۱۳۹۱
رده بندی دیویی	: ۶۵۲۸
شماره کتابشناسی ملی	: ۲۸۴۴۷۳۳



NAGHOOS
PUBLICATION

www.naghoospress.ir

انتشارات ناقوس

چاپ اول

کتاب حقوق برای ناشر محفوظ است.
تکثیر تمامی یا قسمتی از این اثر به
صورت مکتوب یا صوتی یا چاپ مجدد،
چاپ انجمن، بی‌پایه، فتوکپی و انواع
دیگر چاپ ممنوع است و پیگرد
قانونی دارد.

نام کتاب	: علم رمزنگاری و هنر تحلیل رمز
ناشر	: انتشارات ناقوس
تألیف و گردآوری	: ناصر آقاچان زاده، محمدمهدی درفش، مجید جان نثاری
چاپ اول	: ۱۳۹۱
تیراژ	: ۱۰۰۰ جلد
لیتوگرافی	: گلپا گرافیک
چاپ و صحافی	: گنج شایگان
حروف‌نگار و صفحه‌آرا	: مریم رضانی
قیمت به همراه CD	: ۹۰۰۰۰ ریال
شابک	: ۹-۵۳۶-۳۷۷-۹۶۴-۹۷۸
ISBN	: 978-964-377-546-9

مراکز پخش:

۱- انتشارات ناقوس: میدان انقلاب، خیابان کارگر جنوبی، خیابان روانمهر، کوچه دولتشاهی، پلاک ۲

تلفن و فاکس: ۶۶۴۰۸۵۲۰ - ۶۶۴۰۱۷۹۸ - ۶۶۴۱۷۰۷۲ - ۶۶۴۶۶۷۹۳

۲- کتابفروشی الیاس: خیابان انقلاب، نبش فروردین تلفن: ۶۶۴۰۵۰۸۴

فهرست مطالب

۲۵	۱-۲۲-۳- انتخاب	۱۱	سخنی با خوانندگان
۲۵	۱-۴-۱- الگوریتم ژنتیک	۱۳	مقدمه
۲۷	۱-۴-۱- کلیات الگوریتم ژنتیک	۱۷	فصل اول: آشنایی با الگوریتم‌های ژنتیک
۲۸	۱-۲-۴-۱- مقایسه الگوریتم ژنتیک و دیگر شیوه‌های مرسوم بهینه‌سازی	۱۷	۱-۱- تاریخچه علم ژنتیک
۲۸	۱-۲-۴-۱- الگوریتم ژنتیک و سیستم مهندسی	۱۹	۲-۱- هوش مصنوعی AI
۲۹		۱۹	۳-۱- علم ژنتیک
۳۱	فصل دوم: تشریح الگوریتم ژنتیک	۲۰	۱-۳-۱- صفت
۳۱	۱-۲- مقدمه	۲۰	۲-۳-۱- صفات متقابل
۳۱	۲-۲- مفهوم الگوریتم ژنتیک	۲۰	۳-۳-۱- صفات بارز و نهفته
۳۲	۳-۲- ساختار الگوریتم ژنتیک	۲۱	۴-۳-۱- ژن
۳۲	۱-۳-۲- افراد یا کروموزوم‌ها	۲۱	۵-۳-۱- DNA
۳۲	۲-۳-۲- جمعیت	۲۱	۶-۳-۱- لوکوس
۳۳	۲-۳-۲- نمایش و کدگذاری کروموزوم‌ها	۲۱	۷-۳-۱- آلل
۳۳	۱-۳-۲- سیستم کدگذاری دودویی	۲۱	۸-۳-۱- جهش
۳۳	۲-۳-۲- سیستم کدگذاری مبنای هشت	۲۲	۹-۳-۱- فنوتیپ
۳۴	و شناخته	۲۲	۱۰-۳-۱- ژنوتیپ
۳۴	۱-۳-۲- سیستم کدگذاری جایگشتی	۲۲	۱۱-۳-۱- موتان
۳۴	- مسئله فروشنده دوره گرد	۲۲	۱۲-۳-۱- ژنوم
۳۵	۴-۳-۲- سیستم کدگذاری مقدار	۲۲	۱۳-۳-۱- خالص (هموزیگوت)
۳۶	۴-۳-۲- سیستم کدگذاری درختی	۲۲	۱۴-۳-۱- ناخالص (هتروزیگوت)
۳۶	۵-۳-۲- سیستم کدگذاری ارجاع	۲۲	۱۵-۳-۱- هیبرید (دورگه)
۳۸	۴-۲- تفاوت همانندسازی و نسخه‌برداری	۲۳	۱۶-۳-۱- کروموزوم
۳۸	۵-۲- کدگذاری و قیود مسئله	۲۴	۱۷-۳-۱- تکامل
۳۹	۶-۲- جمعیت	۲۴	۱۸-۳-۱- نو ترکیبی
۳۹	۱-۶-۲- جمعیت در حال تعادل	۲۴	۱۹-۳-۱- جهش
۴۱	۲-۶-۲- تشکیل جمعیت اولیه	۲۵	۲۰-۳-۱- تولید مثل
۴۲	۷-۲- تابع هدف	۲۵	۲۱-۳-۱- مهاجرت
۴۲	۸-۲- برازندگی	۲۵	۲۲-۳-۱- نوسان ژنتیکی

۵۷	۱۲-۲- ترنسلوکاسیون	۴۳	۹-۲- انتخاب
۵۸	۱۳-۲- واژگونی	۴۳	۱-۹-۲- تکنیک‌های انتخاب
۵۸	۱۴-۲- ترنسپوزون‌ها و عناصر دخیلی	۴۳	۲-۹-۲- چرخ گردان
۵۸	۱۵-۲- ساختار جهش	۴۴	۳-۹-۲- انتخاب مسابقه‌ای
۵۹	۱۶-۲- ترمیم، تعمیر	۴۵	۱۰-۲- تقاطع
۵۹	۱۷-۲- سیستم SoS	۴۵	۱-۱۰-۲- ژن‌های وابسته
۶۰	۱۸-۲- حذف	۴۵	۲-۱۰-۲- کراسینگ اور چیست؟
۶۰	۱۹-۲- تعویض یا جابه‌جایی	۴۶	۳-۱۰-۲- مکانیسم کراسینگ اور
۶۰	۲۰-۲- الگوریتم نخبه‌گرا	۴۶	۴-۱۰-۲- نظریه کلاسیک
۶۱	۲۱-۲- قیدهای ترمیمی، جریمه‌ای، حذفی	۴۷	۵-۱۰-۲- نظریه نوترین
۶۱	۲۲-۲- دستور خاتمه الگوریتم	۴۷	۶-۱۰-۲- تئوری انتخاب روست
۶۲	۲۳-۲- الگوریتم ژنتیک در یک نگاه	۴۸	۷-۱۰-۲- کراسینگ اور بین ژن
۶۵	فصل سوم: آشنایی با رمزنگاری	۴۹	۸-۱۰-۲- تقاطع یک نقطه‌ای
۶۵	۱-۳- تاریخچه رمزنگاری	۵۰	۹-۱۰-۲- تقاطع چند نقطه‌ای
۶۶	۲-۳- تفاوت رمزنگاری و کدگذاری	۵۰	۱۰-۱۰-۲- تقاطع یکنواخت
۶۶	۳-۳- ماشین‌های رمزنگاری	۵۰	۱۱-۱۰-۲- تقاطع به روش تکثیر میلی
۶۸	۴-۳- رمزنگاری چیست؟	۵۱	۱۲-۱۰-۲- تقاطع براساس جهت‌گیری
۶۸	۵-۳- تعریف کلید	۵۱	۱۱-۲- جهش
۶۹	۶-۳- چرا رمزنگاری؟	۵۲	۱-۱۱-۲- موتاسیون
۷۰	۷-۳- شیوه‌های پایه رمزنگاری	۵۲	۲-۱۱-۲- جهش زایی
۷۰	۱-۷-۳- رمزنگاری جابه‌جایی (Transposition)	۵۲	۳-۱۱-۲- موتاسیون‌های خود به خودی
۷۰	۲-۷-۳- رمزهای جانشینی (substitution cipher)	۵۲	۴-۱۱-۲- موتاسیون‌های نقطه‌ای
۷۱	۳-۷-۳- رمزهای جانشینی (substitution cipher)	۵۲	۵-۱۱-۲- جهش خاموش یا بی اثر
۷۲	۸-۳- دو اصل اساسی در رمزنگاری	۵۳	۶-۱۱-۲- موتاسیون خنثی
۷۲	۱-۸-۳- افزونگی (Redundancy)	۵۴	۷-۱۱-۲- موتاسیون نشتی
۷۲	۲-۸-۳- تازگی پیام‌ها	۵۴	۸-۱۱-۲- موتاسیون‌های بی‌معنی
۷۳	۹-۲- مفهوم کلیدهای رمزنگاری	۵۴	۹-۱۱-۲- موتاسیون حذفی
۷۳	۱-۹-۳- کلیدهای محرمانه	۵۵	۱۰-۱۱-۲- موتاسیون افزایشی
۷۳	۲-۹-۳- کلیدهای عمومی و خصوصی	۵۵	۱۱-۱۱-۲- موتاسیون تغییر چهارچوب
۷۳	۳-۹-۳- کلیدهای اصلی و کلیدهای مشتق‌شده (Master keys and derived keys)	۵۵	۱۲-۱۱-۲- جهش شرطی
۷۴	۴-۹-۳- کلیدهای رمزکننده کلید (Key-encrypting keys)	۵۵	۱۳-۱۱-۲- موتاسیون کشنده
۷۵	۵-۹-۳- کلیدهای رمزکننده کلید (Key-encrypting keys)	۵۶	۱۴-۱۱-۲- جهش ترانزسیون
۷۷	فصل چهارم: الگوریتم‌های رمزنگار	۵۶	۱۵-۱۱-۲- موتاسیون الحاقی
		۵۷	۱۶-۱۱-۲- جهش مستقیم
		۵۷	۱۷-۱۱-۲- جهش‌های معکوس
		۵۷	۱۸-۱۱-۲- جهش با وسعت زیاد
		۵۷	۱۹-۱۱-۲- جهش تغییردهنده چهارچوب

۹۳	۴-۲-۷-۱ - فیدبک خروجی
۹۳	۸-۴-DES :TDES سه گانه
۹۵	۹-۴-سیستم امن
۹۵	۱۰-۴-یک طرح ساده از رمزنگاری یک طرفه
۹۵	۱-۱۰-۴-رمزنگاری کلمه عبور
۹۶	۱۱-۴-رمزنگاری باپتیستا
۹۷	۱-۱۱-۴-کیاس و کیاس چرخشی
۹۸	۲-۱۱-۴-الگوریتم کلاسیک باپتیستا
۹۸	۳-۱۱-۴-رمزگذاری و رمزگشایی در الگوریتم باپتیستا.
۹۹	۴-۱۱-۴-خصوصیات الگوریتم باپتیستا
۹۹	۱-۴-۱۱-۴-مقاومت کم در برابر حملات
۹۹	۲-۴-۱۱-۴-استحکام الگوریتم
۱۰۰	۱۲-۴-تحلیل فراوانی حروف
۱۰۱	۱۳-۴-استاندارد پیشرفته رمزنگاری
۱۰۲	۱-۱۳-۴-طرز کار AES
۱۰۳	۱۴-۴-دیگر الگوریتم‌های کلید خصوصی
۱۰۴	۱-۱۴-۴-IDEA
۱۰۴	۲-۱۴-۴-PC5
۱۰۴	۳-۱۴-۴-Skipjack
۱۰۴	۴-۱۴-۴-Blowfish
۱۰۴	۵-۱۴-۴-CAST
۱۰۴	۶-۱۴-۴-GOST
۱۰۴	۱۵-۴-رمزهای دنباله ای
۱۰۵	۱-۱۵-۴-ساختار مولدهای بیت شبه تصادفی و رمزهای دنباله ای
۱۰۵	۱-۱۱-۱۵-۴-مولدهای منفرشتی خطی (LCG)
۱۰۵	۲-۱۱-۱۵-۴-ثبات های انتقال پسخور(FSR)
۱۰۶	۳-۱۱-۱۵-۴-ثبات های انتقال پسخور غیرخطی(NLFSR)
۱۰۶	۴-۱۱-۱۵-۴-ثبات های انتقال پسخور خطی(LFSR)
۱۰۷	۲-۱۵-۴-کاربردهای رمزهای دنباله ای، مزایا و معایب
۷۷	۱-۴-مقدمه
۷۸	۲-۴-رمزنگاری
۷۸	۳-۴-کاربرد رمزنگاری
۷۹	۴-۴-اصطلاحات رمزنگاری
۷۹	۱-۴-۴-رمزنگاری
۷۹	۲-۴-۴-محرم نامه سازی
۷۹	۳-۴-۴-تمامیت
۸۰	۴-۴-۴-مجوز شخصی
۸۰	۵-۴-۴-امنیت مطلق
۸۰	۶-۴-۴-متن ساده
۸۰	۷-۴-۴-متن رمزی
۸۰	۸-۴-۴-الگوریتم
۸۰	۹-۴-۴-کلید
۸۰	۱۰-۴-۴-رمزنگاری
۸۰	۱۱-۴-۴-رمزگشایی
۸۰	۱۲-۴-۴-رمز شناسی
۸۰	۱۳-۴-۴-رمزشناس
۸۱	۱۴-۴-۴-کشف رمز
۸۱	۱۵-۴-۴-کشف کننده رمز
۸۱	۵-۴-حملات رمزنگاری
۸۱	۱-۵-۴-نقطه ضعف های الگوریتم
۸۱	۲-۵-۴-حملات نفوذ به سیستم
۸۱	۳-۵-۴-نقاط ضعف سیستم جانبی
۸۲	۴-۵-۴-OTP
۸۴	۶-۴-رمزنگاری کوانتومی
۸۴	۱-۶-۴-اصول رمزنگاری کوانتومی
۸۵	۲-۶-۴-اصل عدم قطعیت هایزنبرگ
۸۵	۳-۶-۴-توزیع کلید کوانتومی
۸۷	۴-۶-۴-امنیت
۸۹	۵-۶-۴-نظریه اطلاعات
۹۰	۷-۴-رمز گذاری متقارن
۹۱	۱-۷-۴-رمز انسدادی
۹۱	۲-۷-۴-رمزهای جریانی
۹۲	۳-۷-۴-DES
۹۲	۱-۳-۷-۴-کتاب کد الکترونیکی
۹۳	۲-۳-۷-۴-سلسله بلوک رمز
۹۳	۳-۳-۷-۴-فید بک رمز

فصل پنجم: امضای دیجیتال ۱۲۵

۱۲۵	۱-۵- مقدمه
۱۲۵	۲-۵- امضای دیجیتال چیست؟
۱۲۶	۱-۲-۵- تابع خردکننده امن
۱۲۷	۳-۵- مدیریت کلید
۱۲۷	۴-۵- تولید کلید
۱۲۸	۵-۵- توزیع کلید
۱۲۸	۶-۵- تصدیق کلید
۱۲۹	۷-۵- حفاظت کلید
۱۲۹	۸-۵- ابطال کلید
۱۳۰	۹-۵- اعتماد
۱۳۰	۱-۹-۵- مدل سلسله مراتبی
۱۳۱	۱-۱-۹-۵- ایجاد یک CA
۱۳۲	۲-۱-۹-۵- ابطال گواهینامه‌ها
۱۳۲	۲-۹-۵- مدل وب

فصل ششم: هنر رمزشکنی ۱۳۳

۱۳۳	۱-۶- مقدمه
۱۳۵	۲-۶- تاریخچه هنر تحلیل رمز
۱۳۶	۳-۶- حمله به رمز
۱۳۶	۱-۳-۶- اصل کرکف
۱۳۶	۲-۳-۶- Ciphertext only
۱۳۶	۳-۳-۶- Know Plaintext
۱۳۷	۴-۳-۶- Chose plaintext
۱۳۷	۵-۳-۶- Adaptive Chosen Plaintext
۱۳۷	۶-۳-۶- Related Key Attack
۱۳۸	۴-۶- آزمون‌های شکستن یک الگوریتم
۱۳۸	۵-۶- منابع حمله به سیستم رمز
۱۳۸	۱-۵-۶- زمان
۱۳۸	۲-۵-۶- حافظه
۱۳۸	۳-۵-۶- داده
۱۳۹	۶-۶- حملات بر روی سیستم‌های رمزی
۱۳۹	۱-۶-۶- حملات Man in the Middle
۱۳۹	۲-۶-۶- امنیت رمزهای عبور
۱۴۰	۳-۶-۶- حملات مبتنی بر لغتنامه (Dictionary)
۱۴۱	۴-۶-۶- حملات جامع Brute-Force

۱۰۸	۱۶-۴- رمز قطعه‌ای
۱۰۹	۱-۱۶-۴- کاربردهای گوناگون رمزهای قطعه‌ای
۱۱۰	۲-۱۶-۴- طراحی الگوریتم رمز قطعه‌ای
۱۱۱	۳-۱۶-۴- طراحی امنیت و اجرای مؤثر الگوریتم رمز قطعه‌ای
۱۱۱	۱۷-۴- انواع حملات قابل اجرا بر روی الگوریتم
۱۱۱	۱-۱۷-۴- آزمون جامع فضای کلید
۱۱۱	۲-۱۷-۴- حمله مکملیت
۱۱۲	۳-۱۷-۴- حمله‌های عمومی بر علیه رمزنگاری
۱۱۲	۱-۳-۱۷-۴- حمله نقطه متن رمز شده
۱۱۳	۲-۳-۱۷-۴- حمل متن روشن معلوم
۱۱۳	۳-۳-۱۷-۴- حمله متن روشن منتخب
۱۱۳	۴-۳-۱۷-۴- حمله تطبیقی روشن منتخب
۱۱۳	۴-۱۷-۴- ملزومات طرح مؤثر و کارای تیم-افزایی الگوریتم رمز
۱۱۴	۱۸-۴- رمزنگاری نامتقارن و یا کلید عمومی
۱۱۵	۱-۱۸-۴- رمزنگاری کلید عمومی چیست؟
۱۱۵	۲-۱۸-۴- تبادل کلید با روش Diffie-hellman
۱۱۶	۱-۲-۱۸-۴- نحوه عملکرد Diffie-hellman
۱۱۶	۲-۱۸-۴- الگوریتم جستجوی کوانتومی
۱۱۸	۳-۱۸-۴- RSA
۱۱۸	۱-۴-۱۸-۴- تولید کلیدهای RSA
۱۱۸	۲-۴-۱۸-۴- طرح RSA
۱۲۱	۳-۴-۱۸-۴- رمزگشایی
۱۲۲	۱۹-۴- رمزهای پیوندی یا ترکیبی (Hybrid)
۱۲۲	۲۰-۴- رمز جریانی RC4
۱۲۳	۲۱-۴- الگوریتم‌های دیگر کلید عمومی
۱۲۳	۱-۲۱-۴- Elgamal
۱۲۴	۲-۲۱-۴- DSA
۱۲۴	۳-۲۱-۴- رمزنگاری منحنی بیضوی

- ۱۶۵ MD5 -۳-۳-۷-۷ الگوریتم
- ۱۶۶ -۴-۳-۷-۷ اضافه کردن بیت‌های نرم‌کننده
- ۱۶۶ -۵-۳-۷-۷ افزایش طول
- ۱۶۶ MD -۶-۳-۷-۷ تعیین بافر برای
- ۱۶۷ -۷-۳-۷-۷ پردازش پیام در بلاک‌های
- ۱۶۷ کلمه‌ای
- ۱۶۸ MD5 -۸-۳-۷-۷ شبه کد پیاده‌سازی الگوریتم
- ۱۶۹ -۹-۳-۷-۷ خروجی
- ۱۷۰ md5 -۱۰-۳-۷-۷ تصادم در
- ۱۷۱ -۱۱-۳-۷-۷ تأثیر بیت‌های متن اصلی
- ۱۷۱ -۱۲-۳-۷-۷ MD5 OR MD4
- ۱۷۱ Message Digest 6 -۴-۷-۷
- ۱۷۲ SHA-1 -۵-۷-۷ الگوریتم
- ۱۷۴ SHA-1 -۱-۵-۷-۷ شبه کد الگوریتم
- ۱۷۵ SHA-1 -۲-۵-۷-۷ شکست
- ۱۷۶ -۸-۷-۷ نتیجه‌گیری
- ۱۷۹ پیوست اول: محاسبات کوانتومی
- ۱۷۹ الف -۱- محاسبات کوانتومی
- ۱۸۰ الف -۲- کیوبیت
- ۱۸۰ الف -۳- تاریخچه کامپیوتر کوانتومی
- الف -۴- تفاوت یک کامپیوتر کوانتومی و کامپیوتر کلاسیک
- ۱۸۱ الف -۵- برقراری ارتباط در کامپیوترهای کوانتومی
- ۱۸۲ الف -۶- محاسبات کوانتومی
- ۱۸۳ الف -۷- درهم تافتگی
- ۱۸۵ الف -۸- کیوبیت‌ها
- ۱۸۶ الف -۹- فوتون‌ها
- ۱۸۶ الف -۱۰- الکترون‌ها
- ۱۸۶ الف -۱۱- اتم‌ها و یون‌ها
- ۱۸۷ الف -۱۲- دام‌های یونی
- ۱۸۷ الف -۱۳- نقاط کوانتومی
- ۱۸۷ الف -۱۴- ناخالصی‌های نیمه رسانا
- ۱۸۷ الف -۱۵- مدارهای ابررسانا
- ۱۸۸ الف -۱۶- دام‌های نوری
- ۱۴۱ -۵-۶-۶ جدول مراجعه هش (HLT)
- ۱۴۲ -۷-۶ ماتریس احتمال پسورد
- ۱۴۶ -۸-۶ حملات Brute-forcing به صورت آفلاین
- ۱۴۴ -۹-۶ استفاده مجدد از جریان کلید
- ۱۴۵ -۱-۹-۶ جدول‌های لغت‌نامه‌ای رمزگشایی بر
- ۱۴۶ مبنای بردار اولیه (IV)
- ۱۴۶ -۲-۹-۶ حمله فلرر، هانتین و شمیر (FMS)
- ۱۴۶ -۱۰-۶ فروپاشی سیستم‌های رمز
- ۱۴۷ -۱۱-۶ تحلیل خطی رمز
- ۱۵۰ -۱-۱۱-۶ پیچیدگی عملی تحلیل خطی
- ۱۵۱ -۱۲-۶ تحلیل تفاضلی سیستم‌های رمز متقارن
- ۱۵۱ -۱۳-۶ حملات توانی تفاضلی
- ۱۵۳ -۱۴-۶ تحلیل زمانی
- ۱۵۵ فصل هفتم: رمزنگاری یک‌طرفه
- ۱۵۵ -۱-۷ توابع رمزنگار (یک‌طرفه) هش
- ۱۵۶ -۱-۱-۷ کاربردهای رمزنگار یک‌طرفه
- ۱۵۷ -۲-۱-۷ فضای حالت در رمزنگاری یک‌طرفه
- ۱۵۷ -۲-۷ هش چیست؟
- ۱۵۷ -۱-۲-۷ هشینگ و کلمات عبور
- ۱۵۸ -۳-۷ رمزنگاری یک‌طرفه و دوطرفه
- ۱۵۸ -۴-۷ Collision (تصادم) در Hash
- ۱۵۹ -۵-۷ چند تابع هش‌نگار
- ۱۵۹ -۶-۷ Hash Table
- ۱۶۰ MD -۷-۷
- ۱۶۱ Message Digest 2 -۱-۷-۷
- ۱۶۲ MD2 -۱-۱-۷-۷ هش‌های
- ۱۶۲ -۲-۱-۷-۷ ارزیابی امنیت
- ۱۶۲ Message Digest 4 -۲-۷-۷
- ۱۶۴ -۱-۲-۷-۷ ارزیابی امنیت
- ۱۶۴ Message Digest 5 -۳-۷-۷
- ۱۶۴ -۱-۳-۷-۷ الگوریتم MD5 و نقاط ضعف
- آن
- ۱۶۴ -۲-۳-۷-۷ پیچیدگی عملیات نگاشت

پیوست سوم: رمزنگاری به وسیله اتوماتای سلولی
۲۰۷

- ج - ۱ - رمزنگاری بر اساس اتوماتای سلولی ۲۰۷
ج - ۱ - ۱ - اتوماتای سلولی ۲۰۷
ج - ۲ - اتوماتاهای سلولی چیست؟ ۲۰۸
ج - ۱ - ۲ - یک تعریف علمی از اتوماتای سلولی ۲۰۸
ج - ۲ - ۲ - یک تعریف محاسباتی از اتوماتای سلولی ۲۰۹
ج - ۲ - شبکه ۲۰۹
ج - ۴ - همسایگی ۲۰۹
ج - ۵ - مرز حلقه‌ای ۲۱۰
ج - ۶ - مرزهای متحرک ۲۱۰
ج - ۷ - قوانین اتوماتای سلولی ۲۱۰
ج - ۸ - رشته رمزی ۲۱۱
ج - ۹ - رشته کلیدی ۲۱۲
ج - ۱۰ - کلید رمزی مشترک ۲۱۲
ج - ۱۱ - تابع درجه‌ای ۲۱۲
ج - ۱۲ - روش ولفرام ۲۱۳
ج - ۱۳ - روش مبتنی بر انتقال ۲۱۳
ج - ۱۴ - برای رمزگشایی پیام ۲۱۴
ج - ۱۵ - اتوماتای سلولی مرتبه دوم ۲۱۴
ج - ۱۶ - اتوماتای سلولی بلوکی ۲۱۵
ج - ۱۷ - رمزگذاری ۲۱۵
ج - ۱۸ - رمزگشایی ۲۱۵

پیوست چهارم: NTRU Encrypt ۲۱۷

- د - ۱ - NTRU Encrypt ۲۱۷
د - ۲ - ساخت کلید عمومی ۲۱۸
د - ۳ - رمزگذاری ۲۱۹
د - ۴ - رمزگشایی ۲۲۰

ضمیمه اول: توضیحات مربوط به محتویات CD همراه با کتاب ۲۲۳

CUDA Files and Programs ۲۲۹

مراجع لاتین ۲۳۱

الف - ۱۷ - واهمدوسی ۱۸۸

الف - ۱۸ - قدرت و توانایی محاسبه کوانتومی ۱۸۹

الف - ۱۹ - نحوه عملکرد یک کامپیوتر کوانتومی ۱۸۹

الف - ۲۰ - نوشتن در کامپیوتر کوانتومی ۱۹۰

الف - ۲۱ - خواندن از کامپیوتر کوانتومی ۱۹۰

الف - ۲۲ - توان یک کامپیوتر کوانتومی ۱۹۱

الف - ۲۳ - کامپیوتر کوانتومی و عملیات ۱۹۱

الف - ۲۴ - الگوریتم‌های کوانتومی ۱۹۱

الف - ۲۵ - الگوریتم شور Shor's Algorithm ۱۹۲

الف - ۲۶ - الگوریتم گرور Graver's ۱۹۲

الف - ۲۷ - نرم‌افزارهای کوانتومی ۱۹۳

پیوست دوم: برگشت از رمزنگاری یکطرفه به ۱۹۵

به وسیله جستجوی هیوریستیک ۱۹۵

ب - ۱ - معرفی ۱۹۵

ب - ۱ - ۱ - مقدمه ۱۹۵

ب - ۲ - MDS ۱۹۶

ب - ۳ - تشریح مدل پیشنهادی ۱۹۸

ب - ۱ - ۲ - تشکیل جمعیت اولیه ۱۹۸

ب - ۱ - ۳ - زیر جمعیت نخبه ۱۹۸

ب - ۲ - ۱ - ۳ - زیر جمعیت تولید شده ۱۹۸

توسط عملگرها ۱۹۸

ب - ۳ - ۱ - ۳ - زیر جمعیت مربوط به تابع ۱۹۸

تولید نسل ۱۹۹

ب - ۲ - ۲ - تولید نسل جدید ۱۹۹

ب - ۳ - ۲ - تابع جهش ۲۰۱

ب - ۴ - ۲ - تابع تقاطع ۲۰۲

ب - ۵ - ۲ - نحوه پایان یافتن الگوریتم ۲۰۴

ب - ۱ - ۵ - ۲ - یافتن جواب نهایی در نسل ۲۰۴

جدید ۲۰۴

ب - ۲ - ۵ - ۲ - انتظار برای آرامش ۲۰۴

ب - ۳ - ۵ - ۲ - جستجوی ثانویه ۲۰۵

ب - ۴ - نتیجه‌گیری ۲۰۵

سخنی با خوانندگان

قبل از هر چیز خداوند منان را شاکر و سپاسگذاریم که توفیق نگارش این مقدمه‌ای بر الفبای علم رمزنگاری را به ما عطا فرمودند.

در هزاره سوم و عصر اطلاعات و یا دروازه‌های ورود به عصر مجازی زندگی گره خورده‌ای با رایانه‌ها و دنیای دیجیتال را تجربه می‌کنیم که بخش بزرگی از برقراری امنیت آن بر پایه الگوریتم‌های رمزنگاری بنا نهاده شده است.

میان رمزنگارها و رمزشکن‌ها مسابقه‌ای بزرگ در گرفته است که برای بازندگان آن هزینه سنگین شکست الگوریتم‌ها و یا هزینه و زمان از دست رفته، تعیین شده است. در این مسابقه دائماً سازمان‌ها و گروه‌های فعال در این حوزه الگوریتم‌های رنگین‌تر از قبل برای حفاظت از داده‌ی خود طراحی می‌کنند و در نقطه مقابل عده‌ای در تلاش برای دستیابی به واری این الگوریتم‌ها هستند.

در چنین فضایی لازم است تا محققان حوزه فن‌آوری اطلاعات آشنایی ویژه‌ای با بحث رمزنگاری داشته باشند. همان‌طور که اشارهای هم شد مطالب این کتاب در زمینه آشنایی خوانندگان با الگوریتم‌های رمزنگاری، تحت عنوان "علم رمزنگاری" و گردآوری مجموعه‌ای از روش‌های رمزشکنی تحت عنوان "هنر تحلیل رمز" تلاش خواهد نمود و در واقع هدف اصلی این نوشتار قراردادن واژه هنر تحلیل رمز در برابر علم رمزنگاری برای یادآوری این نکته به سازمان‌ها و نهادهاست که رمزنگاری فقط باید یک مرحله و یکی از ابزارهای تأمین امنیت اطلاعات سازمان باشد و نه تمام اتکای آن! به همین منظور کتاب را حتی با بخش‌هایی کاملاً به دور از رمزنگاری (ژنتیک) شروع کردیم که یادآور باشیم هنر رمزشکنی از هر ابزار و خلاقیتی برای جستجو در فضای بی‌نهایت پاسخ استفاده خواهد نمود. تحلیل‌گر رمز یک هنرمند است و برای هنرمند چهارچوبی از قوانین علمی وجود ندارد. هر لحظه هنر و خلاقیت به وی اجازه می‌دهد قوانین علمی دنیای رمزنگاری را به لورده برآورد.

در این کتاب ابتدا فارغ از هرگونه دیدگاه مهندسی مباحث اساسی علم ژنتیک و ساختار الگوریتم‌های ژنتیک را به طور ساده ولی در عین حال جامع و کامل شرح داده شده است و در ادامه منطق الگوریتم‌های ژنتیک و نحوه عملکرد و طراحی آن‌ها را با چند مثال ساده آورده‌ایم تا خواننده جدا از دیدگاه این کتاب (کاربردهای رمزنگاری) بتواند از این مطالب برای سایر کاربردهای الگوریتم ژنتیک در صنعت و حوزه آکادمیک از آن بهره‌مند شود.

در فصل‌های سوم تا هفتم سعی شده است علاوه بر نگاهی به تاریخچه رمزنگاری، الگوریتم‌های جدید رمزنگاری مورد بحث قرار بگیرند. بخش قابل توجهی از انگیزه این کتاب جمع‌آوری یکجای الگوریتم‌ها و روش‌های مختلف رمزنگاری برای استفاده ساده‌تر و منظم‌تر آن‌ها برای محققین بوده است. جدا از این سعی بر این بوده، که نگاهی به روش‌های مرسوم تحلیل رمزنگاری (تحلیل خطی و تفاضلی) داشته باشیم. همچنین به عنوان پیوست مطالب خوبی راجع به محاسبات کوانتومی و رمزنگاری کوانتومی ارائه شده است و نیز یک CD حاوی مطالب و برنامه‌های ارزشمندی برای مطالعه بیشتر خوانندگان و محققین گرامی همراه این کتاب ارائه شده است که در سه بخش مقالات و سخنرانی‌ها.

برنامه‌های کامپیوتری و همچنین سخت‌افزار تماماً هر کدام بر روی سیستم دیگری سوار می‌شوند یعنی سیستمی بر روی سیستمی است و این موضوع باعث می‌شود که اگر نقطه ضعفی یافت شد در سایر جوانب سیستم اثر گذار باشد. (مخصوصاً از کلمه‌ی سیستم استفاده می‌کنم تا بتوانم بیان کنم که منظورم فقط سخت‌افزار کامپیوتر یا برنامه‌های کامپیوتری نیست زیرا وقتی از نفوذ و ضد نفوذ صحبت می‌کنیم در واقع به هرجایی که اطلاعات ارزشمندی در هر قالبی موجود باشد و عده‌ای برای دستیابی به آن اطلاعات حاضر باشد دست به هرکاری بزنند مربوط می‌شود).

با نگاهی نه چندان فنی به سایت‌هایی که آسیب‌پذیرهای برنامه را گزارش می‌کنند متوجه می‌شویم که روزانه نواقص زیادی انتشار می‌یابند و هرکس یا بهتر است بگوییم کراکرها با کمک این نواقص، سیستم‌ها و سایت‌های کامپیوتری را موردنظر قرار می‌دهند و به اطلاعات آن‌ها آسیب می‌زنند. اما این روند تا کی ادامه خواهد داشت؟ اگر از مطالعه‌کنندگان این قبیل سایت‌ها بوده باشید حتماً متوجه شده‌اید که آسیب‌پذیرهای سیستم‌عامل ریندوز از زمانی که ویندوز هفت به بازار ارائه شده است به شدت کاهش یافته، البته این ظاهر امر است و بسیاری از آسیب‌پذیرهای مهم به صورت زیرزمینی و با قیمت‌های بالایی معامله می‌شوند. اما آنچه که به ظاهر معلوم است آسیب‌پذیری‌های این سیستم‌عامل به مرور زمان کاهش یافته است و شاید این قضیه را بتوان برای سایر برنامه‌ها نیز تعمیم داد. یعنی به مرور زمان با آمدن نسخه‌های جدید از برنامه‌های مختلف، آسیب‌پذیری‌های قبلی آنان رفع شده و راه‌های یافتن آسیب‌پذیری جدید کاهش یافته است و مسلماً روش‌های یافتن آسیب‌پذیری‌ها نیز به مراتب پیچیده شده است زیرا ساختمان کدنویسی و برنامه‌سازی نسبت به گذشته پیچیده‌تر و البته نه ایمن‌تر شده است. سابقاً اکثر برنامه‌ها با زبان‌هایی به عنوان مثال C و C++ داخل ویرایشگرهای نه چندان مناسبی نوشته می‌شدند ولی امروزه برنامه‌های بسیاری در داخل IDEهای قدرتمندی نوشته می‌شوند. بنابراین می‌توان مطمئن بود که یک برنامه‌ی تحت NET، بسیاری از ایرادهای امنیتی گذشته را ندارد و خود چهارچوب Net Framework در زمینه‌ی تأمین امنیت برنامه‌های نوشته شده تحت آن، سدی محکم است و البته نه محکم‌تر!!

افزایش پیچیدگی سیستم‌های کامپیوتری اجتناب‌ناپذیر است و این صنعت نیز به مانند دیگر صنایع به مرور زمان پیچیده‌تر شده است و در جزئی‌ترین بخش‌ها نیز نیاز به متخصص خود دارد. اگر به رمزنگاری به دید یک تفریح ماجراجویانه که دست‌مایه‌ی داستان‌های علمی تخیلی یا فیلم‌های گوناگونی در زمینه‌ی امنیت اطلاعات شده است نگاه کنیم می‌بینیم که تئورهای جنجال برانگیز زیادی در این زمینه انتشار یافته است ولی رمزنگاری و تحلیل رمز نیز به مانند دیگر علوم کامپیوتر نیازمند تحقیق و مطالعه‌ی بسیار است زیرا جزو حیطه‌هایی است که تغییر در آن زیاد است و چیزی که ما امروز آن را نسبتاً امن می‌خوانیم ممکن است فردا تبدیل به یک آسیب‌پذیری امنیتی شود و اصطلاح ناامن بیشتر برازنده‌ی آن گردد!!

اطلاعات در این دوره دارای ارزش زمانی خاصی است و ما مجبوریم برای اینکه به این اطلاعات دست پیدا کنیم یا ارزش آن را بپردازیم یا به روش‌هایی متوسل شویم که با استفاده از آن روش‌ها دست به کار شویم، که اطلاعات ارزشمند است به آن‌ها برسیم. مثالی در این مورد می‌تواند این چنین

باشد که فردی هر ۲۴ ساعت رمز حساب بانکی خود را تغییر می‌دهد، پس در این مثال اگر ما قصد Crack کردن رمز حساب بانک شخص را طبق آزمون و خطا و به کمک سلسله رموز اتفاقی داشته باشیم باید حتماً این کار را زیر ۲۴ ساعت انجام دهیم، زیرا پس از ۲۴ ساعت ممکن است رمزی را که در دوره‌ی قبلی آزموده‌ایم و غلط بوده است می‌تواند در این دوره دقیقاً رمز موردنظر باشد. پس اطلاعات دارای ارزش زمانی است و اگر من مطمئن باشم که یک نفوذگر برای پیدا کردن رمز حساب بانکی من به یک دوره‌ی ۳۰ ساله زمان نیاز دارد، هرگز آن را تغییر نخواهم داد.

هدف به کارگیری روش‌های مدرن در شکستن الگوریتم‌های رمزنگاری کاهش این زمان رخنه است. عملیات کرکی که ۵ سال پیش ۱۰۰۰ روز زمان نیاز داشت، امروزه باید با سرعت بیشتری انجام شود زیرا سخت‌افزار و الگوریتم‌ها بهبود پیدا کرده‌اند و شاید بتوانیم این ۱۰۰۰ روز را به ۱۰ روز کاهش دهیم ولی حتی این ۱۰ روز هم از حوصله‌ی ما خارج است، شاید به کمک روش‌های جدیدی در زمینه‌ی Crack کردن مانند استفاده از جست‌وجوهای اکتشافی کلونی مورچگان و الگوریتم ژنتیک این روند بهبود یابد! هدف ما در این کتاب دقیقاً ارائه‌ی روش‌های جدید و ابتکاری و مقایسه‌ی آن‌ها با روش‌های رایج گذشته است.

بسیار لازم می‌دانم از همه‌ی عزیزانی که دانش خود را بی‌منت در اختیار ما قرار دادند تشکر و قدردانی بسیار کنیم. و اگر کمک و راهنمایی‌های بزرگوار و افرادی که در این زمینه مطالعه کرده‌اند در اختیار ما نبود مسلماً این مسیر بسیار سخت‌تر و طاقت‌فرساتر می‌گذشت. امیدوارم که با انتشار این کتاب ذره‌ای به پیشرفت این حوزه خدمت کرده باشیم و بتوانسته باشیم راه را برای افرادی که بعد در این زمینه می‌پردازند هموارتر کرده باشیم.

گرچه تحقیقات در این قبیل زمینه‌ها ادامه خواهد داشت و مسلماً در آینده روش‌هایی ابداع خواهد گشت که پردازشی را که من در مدت ۱ ساعت انجام می‌دهم دیگران در مدت ۱ ثانیه، عده‌ای دیگر در مدت ۰/۱ ثانیه، عده‌ای دیگر در مدت ۰/۰۱ ثانیه انجام دهند و این روند پیشرفت ادامه خواهد داشت تا جایی که ما قادر به تصور کردن آن نیستیم. همان‌طور که زمانی نیوتن تئوری حرکت ماهواره را بیان کرد و مردم به او خندیدند هرگز تصور نمی‌کردند که قوانین او ما را به فضا ببرد و فرمول‌های او دید ما را به جهان تغییر دهد.

واقعاً نمی‌شود عظمتی مانند نیوتن را در $F = mg$ یا انیشتین را در $E = mc^2$ خلاصه کرد. باید بسیار خواند، بسیار بسیار گوش کرد و بسیار بسیار فکر کرد تا شاید بتوانیم به نزدیکی مرز دانش برسیم و پا بر روی آن بگذاریم و با جرأتی وصف‌ناشدنی از آن عبور کنیم و وارد دنیای ترسناک ناشناخته‌ها شویم. شاید نهایت علم الکترونیک، ساخت ابرکامپیوتری به اندازه‌ی یک ساعت‌چی باشد و شاید وقتی بشر از این دیوار بلند بالا رفت منظره‌ی زیبایی از دشت طراحی را ببیند که نهایتش باز، ناپیدا باشد. نوع بشر باید صبور باشد و همان‌طور که سفر به ماه و تسخیر مریخ را دیده روی به فراسوی تخیل کنونی می‌رود و انشاالله آیندگان از ما به نیکی یاد کنند.

و به قول آقای انیشتین که می‌فرمایند: مهم این است که سؤال کردن را متوقف نکنید.