علم رمزنگاری و هنر تحلیل رمز

به انظمام: راهنمای کامل الگوریتم‌های ژنتیک و اصول رمزنگاری کوانتومی

تألیف و گردآوری:

ناصر آقاجان‌زاده

محمد مهدی درفشی

مجید جان نثاری

انتشارات ناقوس

NAGHOOS
PUBLICATION

سرشناسه : آقاجان‌زاده، ناصر، ۱۳۶۶-
عنوان و نام پدیدآور : علم رمزنگاری و هنر تحلیل رمز: به انظمام راهنمای کامل الگوریتم‌های ژنتیک و اصول رمزنگاری کوانتومی/ تألیف و گردآوری ناصر آقاجان‌زاده، محمدمهدی درفشی، مجید جان‌نثاری.
مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۹۱.
مشخصات ظاهری : ۲۳۱ ص.: مصور، جدول. + یک لوح فشرده.
شابک : ۹-۵۴۶-۳۷۷-۹۶۴- ۹۷۸ بها : ۹۰۰۰۰ ریال به همراه CD
وضعیت فهرست‌نویسی : فیپا
موضوع : رمزنگاری
موضوع : رمزنگاری داده‌ها
موضوع : کامپیوترها-- ایمنی اطلاعات
موضوع : الگوریتم‌های ژنتیک
شناسه افزوده : درفشی، محمدمهدی، ۱۳۶۵-
شناسه افزوده : جان‌نثاری، مجید، ۱۳۶۲-
رده بندی کنگره : ۱۳۹۱ ۷۶۸ Z ۱۰۳
رده بندی دیویی : ۶۵۲.۸
شمارهٔ کتابشناسی ملی : ۲۸۴۴۷۳۳

انتشارات ناقوس
www.naghoospress.ir
NAGHOOS PUBLICATION

نام کتاب : علم رمزنگاری و هنر تحلیل رمز
ناشر : انتشارات ناقوس
تألیف و گردآوری : ناصر آقاجان‌زاده، محمدمهدی درفشی، مجید جان‌نثاری
چاپ اول : ۱۳۹۱
تیراژ : ۱۰۰۰ جلد
لیتوگرافی : گلپا گرافیک
چاپ و صحافی : گنج شایگان
حروف‌نگار و صفحه‌آرا : مریم رضائی
قیمت به همراه CD : ۹۰۰۰۰ ریال
شابک : ۹-۵۴۶-۳۷۷-۹۶۴- ۹۷۸
ISBN : 978-964-377-546-9

چاپ اول

مراکز پخش:
۱- انتشارات ناقوس: میدان انقلاب، خیابان کارگرجنوبی، خیابان روانمهر، کوچه دولتشاهی، پلاک ۲
تلفن و فاکس : ۶۶۴۰۸۵۲۰ – ۶۶۴۰۱۷۹۸ – ۶۶۴۱۷۰۷۲ – ۶۶۴۶۶۷۹۳
۲- کتابفروشی الیاس: خیابان انقلاب، نبش فروردین تلفن: ۶۶۴۰۵۰۸۴

فهرست مطالب

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 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 ورای 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 لرزه درآورد.

در این کتاب ابتدا فارغ از هرگونه دیدگاه مهندسی مباحث اساسی علم ژنتیک و ساختار الگوریتم-های 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 به‌عنوان 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 هرکدام برروی سیستم دیگری سوار می‌شوند یعنی سیستمی برروی 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 هکرها 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 ویندوز 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 به‌عنوان 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 جزیی‌ترین 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 تیترهای 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 [illegible] 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 ۱۰۰۰روز 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 الگوریم ژنتیک این روند بهبود یابد! هدف ما در این کتاب دقیقاً ارایه‌ی 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 راهنمایی اساتید 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 توانسته 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 انیشتن 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 برروی 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 ساعت‌مچی 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 انیشتن که می‌فرمایند: مهم این است که سؤال کردن را متوقف نکنید.