رمزنگاری با پایتون

مولف:

شانون و. بِری

مترجم:

ایوب ترکیان

نیاز دانش

فهرست

عنوان **صفحه**

پیشگفتار

در چند سال گذشته، کشورهای مختلف قوانینی وضع کرده تا مطمئن شوند هر ارتباط، ایمیل، پیام متنی، یا چت ویدئویی، در صورت نیاز، قابل خواندن توسط پلیس یا نیروهای امنیتی باشد. شرکت‌های فناور ملزم به تأمین درگاه‌های مخفی یا کلید رمز مورد نیاز به دولت بوده، تا آنها بتوانند امنیت کشور را تأمین کنند.

نزاع بین قانون‌گذاران و پلاتفرم‌های پیام‌رسان رمزنگاری شده، به عرصه‌های جدیدی وارد شده است. دنیایی را تصور کنید که در آن، دولت از هر فرصت برای اسکن کردن هر پیام الکترونیکی توسط نرم‌افزار اسکن مورد تأیید خویش استفاده می‌کند. حریم خصوصی و امنیت همه کاربران، در صورت شکسته شدن سیستم‌های رمزنگاری توسط پلیس و دیگر سازمان‌های قانونی آسیب می‌بینند. طرفداران رمزگذاری مبدأ به مقصد، نظیر میکروسافت، فیسبوک، و گوگل، ممکن است در حفظ اولویت امنیت کاربران به عنوان یک اولویت، موفق نشوند.

در مواقعی مثل موارد جنایی، قابل خوانش شدن داده‌های رمزگذاری شده مفید است. آیا می‌توان به مجرمین اجازه داد، برنامه‌های خویش را به صورت سرّی پیاده‌سازی کنند؟ مرز حریم خصوصی از کجا شروع می‌شود؟ در واقعیت، مسایل فنی و حقوقی وجود داشته، که اجازه می‌دهد دولت‌ها این کار را انجام بدهند؛ این امر البته به شدت مورد مخالفت شرکت‌ها و طرفداران حریم خصوصی است. نزاعی در مورد اینکه چه چیزی می تواند یا باید رمزگذاری شده، و چه کسانی باید کلید باز کردن قفل رمزگذاری فرد دیگری را داشته باشند، در جریان است.

صرف نظر از مخالفت یا موافقت در مورد میزان قدرت دولت نسبت به ارتباطات رمزگذاری شده در یک کشور، شناخت رمزگذاری، نحوه اعمال آن در صورت نیاز، و شیوه اطمینان از موثق و محرمانه بودن داده‌های دریافتی، ضروری است. در این کتاب، مبانی استفاده از رمزنگاری برای امن کردن پیام‌ها، فایل‌ها، یا ترافیک اینترنت با استفاده از برنامه‌های قابل فهم پایتون ایجاد شده با نسخه پایتون ۳ مورد بررسی قرار خواهد گرفت.

محتوای کتاب

تمرکز این کتاب بر روی انتخاب محیط مناسب پایتون برای رفع نیازهای رمزنگاری است. اصول شناخت الگوریتم‌ها فراهم شده، و مبانی پایتون مورد کاوش قرار خواهد گرفت.

پس از طرح مطالب اولیه برای شروع، مروری در مورد رمزنگاری، معنای محرمانگی، و تاریخچه رمزنگاری و تغییرات ایجاد شده در زندگی انسان‌ها در اثر استفاده از آن، صورت خواهد گرفت.

برای شناخت کامل بعضی از مفاهیم رمزنگاری، یک مقدار ریاضی لازم است. شناختی از اعداد صحیح، تئوری گروه، و مولدهای عدد شبه‌راندومی، در تدوین راهکارهای رمزنگاری کمک حال است. اینها مبانی شناخت جریان‌های مختلف و رمزهای بلوکی را تشکیل داده، و برخی از نمادها و نقاط ضعف رمزنگاری آنها را برجسته می‌کند.

هر بحث رمزنگارانه با تصاویر بهتر قابل فهم بوده و بنابراین، یک فصل به نحوه کار رمزنگاری تصویر و امور پنهان‌نگاری[1] تخصیص داده می‌شود. بعضی از موضوعات مورد نیاز که در هنگام کار با تصاویر باید نسبت به آنها آگاه بود، نیز مطرح خواهد شد.

انسجام پیام به همان اندازه محرمانگی پیام اهمیت دارد. اطلاع از اینکه چه کسی برای شما پیام ارسال کرده، ارتباط مستقیمی با قابل اعتماد بودن پیام دارد. نحوه تولید کدهای احراز هویت پیام، برای اطمینان از انسجام در حین انتقال، نیز مطرح خواهد شد.

قدرت رمزنگاری در انتهای کتاب نشان داده شده که در آن، شِماهای PKI مطرح شده و شیوه پیاده‌سازی رمزنگاری منحنی بیضوی در یک اپ، ترسیم می‌گردد. اپ ساخته شده، داده‌ها را در فرمت به شدت امن روی یک کانال ناامن تبادل خواهد کرد. بدین‌طریق، اطمینان ایجاد شده که بتوان روی شِمای رمزگذاری مبدأ به مقصد کنترل داشته، تا بتوان بدون نیاز به کلیدهای ایجاد شده، رمزگشایی را انجام داد.

پیش‌زمینه

در این کتاب فرض می‌شود که رمزنگاری زمینه جدیدی برای شماست. اگر چه مقدمه اجمالی در مورد نحوه برپایش و استفاده از پایتون فراهم شده، در صورتی که با زبان برنامه‌سازی دیگری تجربه داشته باشید، استفاده بیشتر و بهتری از موضوعات خواهید کرد.

ابزار مورد نیاز

مفاهیم مطرح شده در این کتاب را می‌توان روی ویندوز، لینوکس، کروم‌بوک، یا iOS اجرا کرد. انتخاب ادیتور احتمالاً به سیستم عامل نهشته بستگی داشته، اگر چه اکثر دستورالعمل‌های پایتون ارایه شده در اینجا، در اکثر ادیتورهای آنلاین و پوسته‌های استفاده‌کننده از مفسر پایتون ۳ یا بالاتر، قابل استفاده است.

نحوه استفاده

موضوعات این کتاب به مرور پیشرفته شده و بنابراین، پیشنهاد می‌شود از ابتدا شروع کرده و به تدریج مهارت‌های خویش را افزایش بدهید. از این کتاب به عنوان مرجع نیز می‌توان در موقعیت‌های زیر استفاده کرد:

---

1 steganography

- در حین تلاش برای امن کردن داده‌ها، به مشکل بر می‌خورید.
- باید با استفاده از رمزنگاری کاری صورت داده، که هرگز قبلاً انجام نداده‌اید.
- یک مقدار وقت پیدا کرده‌اید و تمایل دارید پایتون و رمزنگاری یاد بگیرید.

سعی شده که هر فصل روی یک موضوع گسترده تمرکز داشته باشد. اگر بعضی از مطالب در ابتدا مشکل بود، مأیوس نشوید. با پیاده‌سازی نمونه کدها و ساخت جواب نهایی، شناخت مفاهیم به تدریج ساده‌تر خواهند شد.

وب‌سایت کتاب

تقریباً هر مطلب مطرح شده در کتاب، مثال‌هایی را همراه خود دارد. این مثال‌های مفید گنجانده شده در کتاب را می‌توانید (و باید) دانلود کنید. صحه‌گذاری شده که هر فایل در محیطی که از پایتون ۳٫۰ و بالاتر استفاده می‌کند، قابل اجرا باشد.

فایل‌ها در github.com/braycrypto/cryptography و نیز در سایت خود کتاب قابل دست‌یابی است: www.wiley.com/go/cryptographywithpython