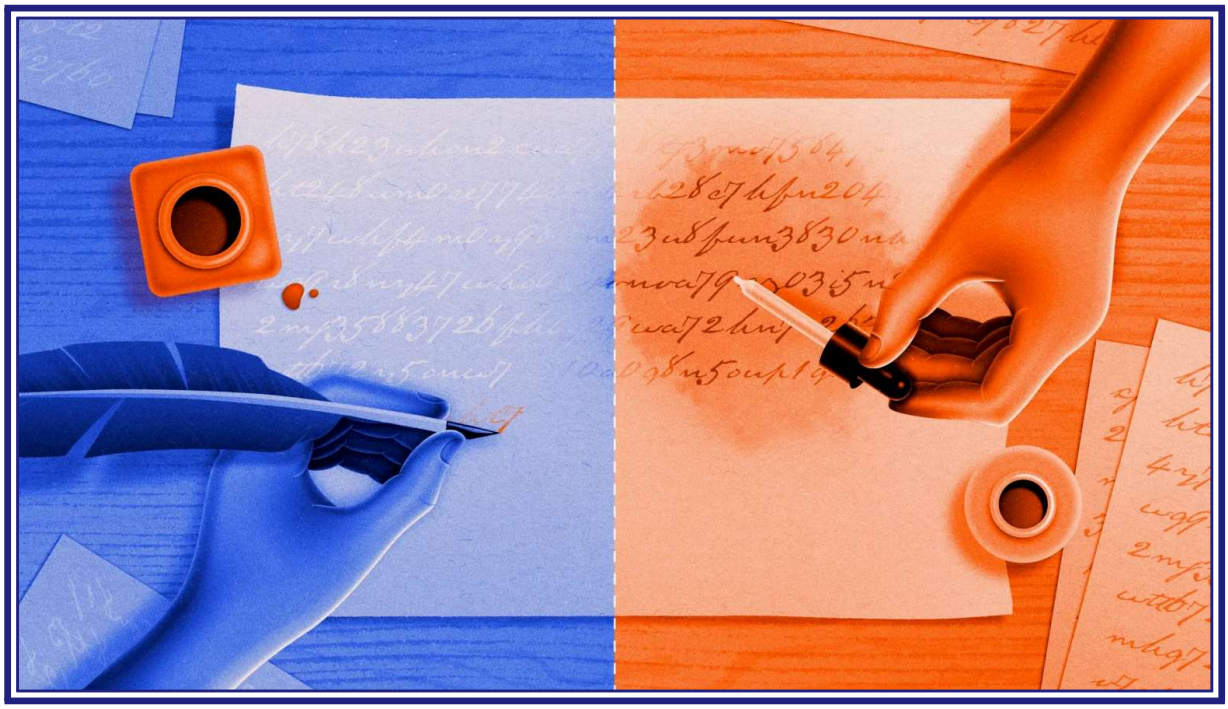
چگونه رمزنگاری کلید عمومی واقعا کار می‌کند، با استفاده از ریاضیات ساده *

جان پاولوس

مترجم: فاطمه آقایی **



سیستم امنیتی که زیربنای اینترنت را تشکیل می‌دهد، از یک واقعیت عجیب استفاده می‌کند: می‌توانید بخشی از رمزگذاری خود را منتشر کنید تا اطلاعات خود را بسیار ایمن‌تر کنید.

به‌مدت هزاران سال، اگر می‌خواستید یک پیام مخفی ارسال کنید، اساساً یک راه برای انجام آن وجود داشت. شما با استفاده از یک قانون خاص که فقط شما و مخاطب موردنظر شما می‌دانستید، پیام را رمزگذاری می‌کردید. این قانون مانند کلید یک قفل عمل می‌کرد. اگر کلید را داشتید، می‌توانستید پیام را رمزگشایی کنید؛ در غیر این‌صورت، باید قفل را باز می‌کردید. برخی از قفل‌ها آن‌قدر موثر هستند که حتی با زمان و منابع نامحدود نیز قابل باز کردن نیستند. اما حتی آن طرح‌ها از همان نقطه ضعف بنیادینی رنج می‌برند که همه سیستم‌های رمزنگاری مشابه را آزار می‌دهد: چگونه آن کلید را به دست افراد آشنا برسانید، در حالی‌که آن را از دسترس افراد مغرض و ناآشنا دور نگه دارید؟

راه حل غیرشهودی، که به‌عنوان رمزنگاری کلید عمومی شناخته می‌شود، نه براساس حفظ امنیت یک کلید، بلکه براساس در دسترس قراردادن گسترده آن استوار است. ترفند این است که از یک کلید دوم نیز استفاده کنید که هرگز آن را با کسی به اشتراک نگذارید، حتی با شخصی که با او ارتباط برقرار می‌کنید. تنها با استفاده از این ترکیب دو کلید - یکی عمومی و دیگری خصوصی - است که کسی می‌تواند هم پیام را رمزگذاری و هم رمزگشایی کند.

برای درک نحوه عملکرد این روش، راحت‌تر است که به‌جای کلیدهایی که در یک قفل قرار می‌گیرند، به آن‌ها به عنوان دو ماده مکمل در یک جوهر نامرئی فکر کنیم. ماده اول باعث محو شدن پیام‌ها و ماده دوم باعث ظاهر شدن آن‌ها می‌شود. اگر جاسوسی به نام بوریس بخواهد پیام مخفی خود را برای همتای خود ناتاشا ارسال کند، پیامی می‌نویسد و سپس از ماده اول برای نامرئی کردن آن روی صفحه استفاده می‌کند. (این کار برای او آسان است: ناتاشا فرمول آسان و شناخته شده‌ای برای جوهر ناپدید شونده منتشر کرده است.) وقتی ناتاشا کاغذ را از طریق پست دریافت می‌کند، ماده دوم را اعمال می‌کند که باعث می‌شود پیام بوریس ظاهر شود.

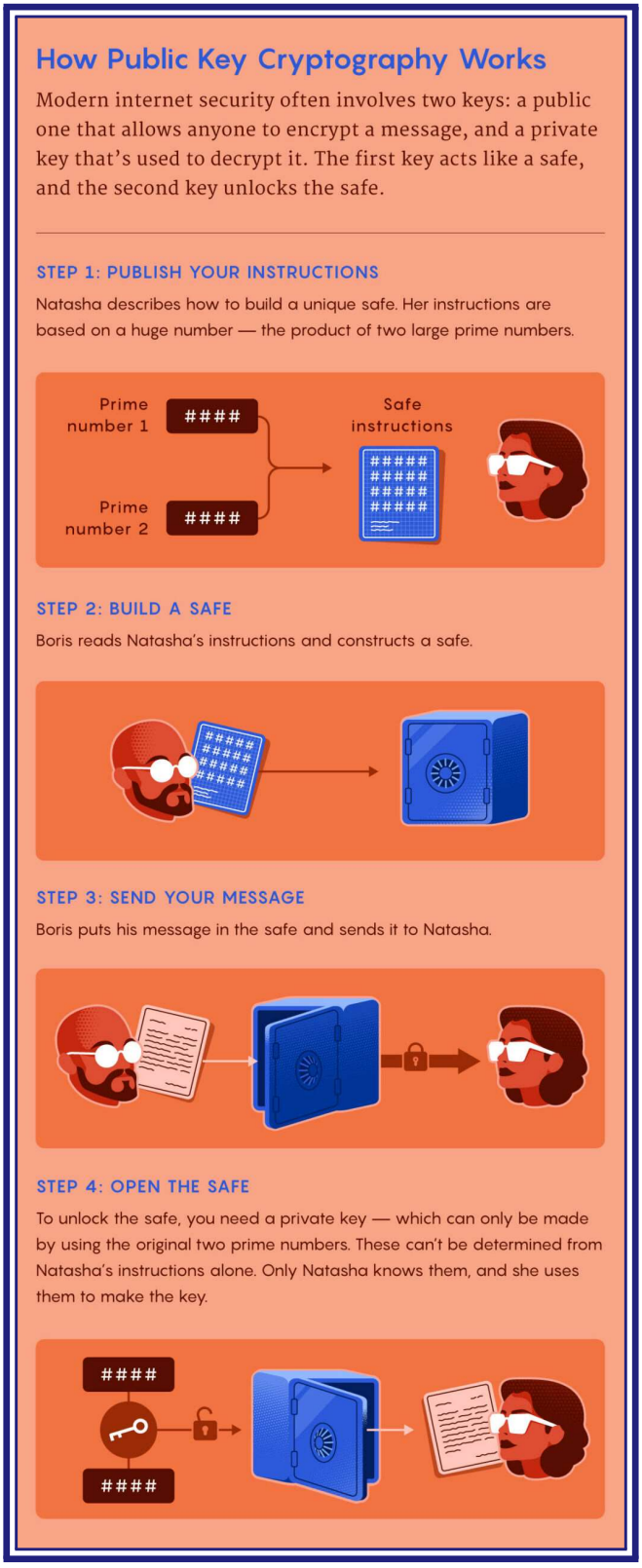
در این طرح، هر کسی می‌تواند پیام‌ها را نامرئی کند، اما فقط ناتاشا

می‌تواند آنها را دوباره قابل‌مشاهده کند و از آنجایی که او هرگز فرمول ماده دوم را با کسی به اشتراک نمی‌گذارد - حتی با بوریس - می‌تواند مطمئن باشد که پیام در طول مسیر رمزگشایی نشده است. وقتی بوریس می‌خواهد پیام‌های مخفی دریافت کند، به‌سادگی همان روش را اتخاذ می‌کند: او یک دستورالعمل آسان برای ناپدید کردن پیام‌ها (که ناتاشا یا هرکس دیگری می‌تواند استفاده کند) منتشر می‌کند، در حالی‌که دیگری را فقط برای خودش نگه می‌دارد که باعث می‌شود آنها دوباره ظاهر شوند.

در رمزنگاری کلید عمومی، کلیدهای «عمومی» و «خصوصی» درست مانند مواد اول و دوم در این جوهر نامرئی ویژه عمل می‌کنند: یکی پیام‌ها را رمزگذاری می‌کند و دیگری آنها را رمزگشایی می‌کند. اما به جای استفاده از مواد شیمیایی، رمزنگاری کلید عمومی از معماهای ریاضی به نام «توابع درب پشتی» استفاده می‌کند. این توابع در یک جهت به راحتی قابل محاسبه هستند اما محاسبه و معکوس آنها بسیار دشوار است. این توابع حاوی اطلاعاتی هستند که اگر دانسته شوند، محاسبه توابع را در هر دو جهت بسیار آسان می‌کنند.

یک تابع درب پشتی رایج شامل ضرب دو عدد اول بزرگ است، کاری که به راحتی قابل انجام است. اما معکوس کردن آن - یعنی شروع با حاصل‌ضرب و یافتن هر عامل اول - از نظر محاسباتی غیر عملی است. برای ساختن یک کلید عمومی، با دو عدد اول بزرگ شروع کنید. اینها درب های پشتی شما هستند. دو عدد را در هم ضرب کنید، سپس برخی عملیات ریاضی اضافی را انجام دهید. این کلید عمومی اکنون می‌تواند پیام‌هارا رمزگذاری کند. برای رمزگشایی آنها، به کلید خصوصی مربوطه نیاز دارید که حاوی عوامل اول - درب های پشتی ضروری است. با آن اعداد، رمزگشایی پیام آسان است. آن دو عامل اول را مخفی نگه دارید تا پیام مخفی بماند.

رمزنگاری کلید عمومی برای اولین بار بین سال های ۱۹۷۰ و ۱۹۷۴ توسط ریاضی‌دانان بریتانیایی که برای ستاد ارتباطات دولتی انگلیس کار می‌کردند، کشف شد، همان آژانس دولتی که کد انیگمای نازی را در طول جنگ جهانی دوم شکست. کار آنها (که تا سال ۱۹۹۷ طبقه بندی شده باقی ماند) با آژانس امنیت ملی ایالات متحده به اشتراک گذاشته شد، اما به‌دلیل ظرفیت محاسباتی محدود و گران قیمت، هیچ یک از دولت‌ها این سیستم را پیاده سازی نکردند.



در سال ۱۹۷۶، محققان آمریکایی ویتفیلد دیفی[۱] و مارتین هلمن[۲] اولین طرح رمزنگاری کلید عمومی شناخته شده عمومی را کشف کردند که تحت تأثیر رمزنگار رالف مرکل[۳] بود. تنها یک سال بعد، الگوریتم RSA که به نام مخترعان آن ران ریوست[۴]، آدی شامیر[۵] و لئونارد ادلمان[۶] نامگذاری شده است، راه عملی برای استفاده از رمزنگاری کلید عمومی را ایجاد کرد. این الگوریتم هنوز هم کاربرد گسترده ای دارد و یکی از زیربناهای اساسی اینترنت مدرن است و امکان انجام همه چیز از خرید تا ایمیل مبتنی بر وب را فراهم می‌کند.

این سیستم دوکلیدی همچنین «امضاهای دیجیتال» را ممکن می‌سازد، این‌که یک پیام توسط دارنده یک کلید خصوصی ایجاد شده است، اثبات ریاضی دارد. این کار به این‌دلیل است که کلیدهای خصوصی نه تنها برای رمزگذاری پیام‌ها بلکه می‌توانند برای رمزگشایی آنها نیز استفاده شوند. البته، این برای مخفی نگه داشتن پیام‌ها بی‌فایده است: اگر از کلید خصوصی خود برای رمزگذاری یک پیام استفاده کنید، هر کسی می‌تواند از کلید عمومی مربوطه برای رمزگشایی آن استفاده کند. اما این ثابت می‌کند که شما و فقط شما، پیام را ایجاد کرده‌اید، زیرا به‌عنوان دارنده کلید خصوصی، فقط شما می‌توانستید پیام را رمزگذاری کنید. ارزهای دیجیتال مانند بیت کوین بدون این ایده نمی‌توانستند وجود داشته باشند.

اگر دو کلید رمزنگاری به‌جای یک کلید بسیار موثر باشد، چرا کشف آن هزاران سال طول کشید؟ به گفته راسل ایمپگلیازو[۷]، دانشمند کامپیوتر و نظریه پرداز رمزنگاری در دانشگاه کالیفرنیا، سن دیگو، مفهوم تابع درب پشتی قبل از اختراع رایانه‌ها به اندازه کافی مفید نبود. او می گوید: «این موضوعی مربوط به فناوری است».

«در قرن نوزدهم فردی در یک جنگ واقعی، رمزنگاری برای انتقال اطلاعات نظامی در میدان جنگ را تصور می‌کرد. بنابراین اگر اولین قدم شما، انتخاب دو عدد اول ۱۰۰ رقمی برای ضرب کردن با هم باشد، جنگ قبل از انجام این کار تمام خواهد شد». اگر دشواری را به چیزی که یک انسان بتواند به سرعت انجام دهد کاهش دهید، امنیت چندانی نخواهد داشت.

اما در حالی که رایانه‌ها به امکان‌پذیر شدن رمزنگاری کلید عمومی کمک کردند، همچنین شکاف‌هایی در زره آن ایجاد کرده‌اند. در سال ۱۹۹۴، ریاضیدان پیتر شور[۸] راهی را برای رایانه‌های کوانتومی کشف کرد تا به‌طور کارآمد توابع تله‌ای را که زیربنای اکثر سیستم‌های رمزنگاری کلید عمومی فعلی از جمله تجزیه به عوامل اول هستند، را معکوس کنند. این الگوریتم، در صورت پیاده‌سازی، مانند یک «جوهر ظاهر کننده» همه‌منظوره عمل می‌کند و قادر است هر پیام نامرئی را دوباره ظاهر کند. خداحافظ، امنیت اینترنت!

خوشبختانه، کامپیوترهای کوانتومی خودشان «هنوز در فاز ENIAC هستند»، ایمپگلیازو با اشاره به ماشین اتاقی که در سال ۱۹۴۵ برای ارتش ایالات متحده ساخته شد، می گوید:« تا زمانی که کامپیوترهای کوانتومی به اندازه کافی پیچیده شوند تا تهدید واقعی برای رمزنگاری کلید عمومی ایجاد کنند، توابع درب پشتی اصلی آن می‌توانند با نسخه های «کوانتومی ایمن» به‌نام مشکلات شبکه جایگزین شوند. البته، این «جوهر» محاسباتی جدید ممکن است در آینده نیز مستعد حمله شود. اما این نکته جالب رمزنگاری کلید عمومی است: تا زمانی که بتوانیم توابع جدیدی برای استفاده پیدا کنیم، می‌توانیم به‌سادگی چرخ را دوباره اختراع کنیم. یا در این مورد، کلید را.

*John Pavlus, How Public Key Cryptography Really Works, Using Only Simple Math, Quantamagazine, November 15, 2024.

**دانشگاه یزد

[1] Whitfield Diffie [2] Martin Hellman [3] Ralph Merkle [4] Ron Rivest [5] Adi Shamir [6] Leonard Adleman [7] Russell Impagliazzo [8] Peter Shor