رمزگذاری و رمزگشایی: ارتباط با ایمنی کامل

نویسنده: ژان ـ لویی نیکولا [۱]

مترجم: ارسلان شادمان

ویراستاران: فرج‌الله محمودی، شهناز عباسپور

در جهان امروز که مخابرات جایگاهی کلیدی دارد، رمزنگاری ترفند عمده‌ای است. این موضوع که به دانش پیچیده‌ای تبدیل شده است، نمی‌تواند از ریاضی‌دانانی در سطح بسیار عالی بی‌نیاز باشد.

در مارس ۲۰۰۰، عنوان درشتی به مضمون زیر، صفحهٔ اول روزنامه‌ها را پر کرد: «اعلام خطر در مورد ایمنی کارت‌های بانکی». چه چیزی رخ داده بود؟ در فرانسه، رازداری کارت‌های مورد بحث، از ۱۹۸۵، به کمک یک روش کدگذاری انجام می‌شد که در آن یک عدد بزرگ N با ۹۷ رقم دخالت می‌کرد. این عددِ «N» می‌بایست حاصلضرب دو عدد اول بزرگ باشد، یعنی حاصلضرب دو عدد مانند ۷ و ۱۹ که جز بر ۱ و خود، بر هیچ عدد دیگری بخشپذیر نیستند. راز یک کارت بانکی دقیقاً از این دو عدد تشکیل می‌شود؛

[۱] Nicolas, Jean-Louis: *Cryptage et décryptage: communiquer en toute sécurité*, in: L'explosion des mathématiques, SMF et SMAI, Paris, 2002, p. 15-18

پرداخت با کارت اعتباری، خرید ازطریق اینترنت: روش‌های رمزنگاری که ریاضیات برازنده‌ای را به‌کار می‌گیرند، برای ایمنی این‌گونه عملیات مورد نیازند (عکس از: تصاویر گتی)[۱]

در دهۀ ۱۹۸۰، محاسبۀ آن‌ها با شروع از «N» عملاً غیرممکن بود. اما با افزایش توان رایانه‌ها و با بهبود روش‌های ریاضی، در سال‌های آخر قرن، اندازۀ اعدادی که می‌توان عامل‌های اول آن‌ها را در زمانی معقول محاسبه کرد. از صد رقم هم گذشت (رکورد فعلی ۱۵۸ رقم، مربوط به ژانویه ۲۰۰۲ است). یک ترفندْ بازِ متخصص در دانش اطلاعات توانست دو عدد اولی را که حاصلضرب آن‌ها N است تشخیص دهد و از آن‌ها برای ساختن کارت‌های جدید استفاده کرد. از این رو، برای آن که ایمنی کارت‌های پلاستیک کوچک ما، تضمین شود سازمان مسؤول ادارۀ این کارت‌های بانکی، بی‌درنگ اعداد جدید Nی ساخت که آشکارا خیلی بزرگترند.

رمزنگاری جدید در میعادگاه ریاضیات و دانش اطلاعات

این حادثه روشنگر آن است که امروزه دانش رمزورزی، یعنی کدگذاریِ پیامها، که برای اشخاص فضول غیرقابل خواندن شوند، از چه اهمیت قابل توجهی برخوردار است. رمزگذاری و رمزگشاییِ پیام‌هایِ محرمانه، فعالیتی با دیرینۀ چند قرن و یا حتی چند هزاره است. این فعالیت دیگر منحصر به محدودۀ دیپلماتیک و نظامی نیست و دنیای مخابرات

[۱] Getty Images

مَدَنی را کاملاً فراگرفته است: از آن جمله فرایندهای تشخیص اصالت، نقل و انتقالات بانکی، تجارت الکترونیک، حفاظت منزلگاه‌ها و پرونده‌های کامپیوتری و غیره.

رمزنگاری در طول دهه‌های اخیر شاهد پیشرفت‌هایی بوده است. در اثنای این پیشرفت‌ها، رمزنگاری به دانشی پیچیده تبدیل شده است که ترقیات آن محصول کار متخصصین با آموزش‌های سطح بالایی در ریاضیات و دانش اطلاعات است. این جنبهٔ تخصصی از جنگ جهانی دوم آشکار شده است. امروز می‌دانیم که شکستن رمز و خواندن پیامدهایی که آلمانی‌ها با ماشین های انیگمای[۱] خود کدگذاری کرده بودند، چه نقش تعیین کننده‌ای در سرنوشت این جنگ برای متفقین داشت. وانگهی ریاضیدان برجستهٔ بریتانیایی، آلن تورینگ[۲] که یکی از پدران علوم کامپیوتر نظری نیز هست، سهمی اساسی در این رمزگشایی ایفا نمود.

در سال‌های ۱۹۷۰، رمزنگاری شاهد تحول کوچکی شد: اختراع رمزنگاری با «کلید عمومی[۳]» به‌وسیلهٔ روش RSA[۴]. موضوع این ماجرا چیست؟ تا آن زمان، طرف‌های خواهان تبادل پیام می‌بایست یک کلید محرمانه در اختیار داشته باشند، اما خطر لو رفتن این کلید خیلی زیاد بود. قرارداد RSA که نام آن از نام سه مخترع آن (رونالد ریوست[۵]، آدی شامیر[۶] و لئونارد آدلمن[۷]) گرفته شده است، این مشکل را برطرف کرد. در این روش از دو کلید استفاده می‌شود: یک کلید، رمزگذاری عمومی است که همه می‌توانند آن را بشناسند ـ و یک کلید، رمزگشاست که محرمانه باقی خواهد ماند. این روش، متکی بر این اساس است که می‌توان اعدا اول بزرگی (با صد رقم، هزار رقم و یا بیشتر) ساخت، ولی یافتن عوامل اول p و q از روی یک عدد بزرگِ $N = p \times q$ بسیار مشکل است، همان‌گونه که در مورد کارت‌های بانکی هم به این روش اشاره کردیم. اجمالاً، شناخت عددِ N به منزلهٔ شناخت کلید عمومی رمزنگاری است، در حالی که شناخت p و q در حکم شناخت کلید محرمانهٔ رمزگشاست.

البته، اگر کسی می‌توانست روشی برای تجزیهٔ سریع اعداد بزرگ به عوامل اول

---

۱ Enigma

۲ Alan Turing

۳ Clé publique

۴ Rivest-Shamir-Adleman

۵ Ronald Rivest

۶ Adi Shamir

۷ Leonard Adleman

آن بیابد، آنگاه پروتکل RSA از دور خارج می‌شد. اما این امکان هم وجود دارد که ریاضیدانان ثابت کنند چنین روشی وجود ندارد، در این صورت ایمنی پروتکل RSA تقویت هم می‌شود. در این موارد با موضوع‌هایی قطعی برای پژوهش سروکار داریم.

روش‌هایی که، مانند پروتکل RSA، نظریهٔ اعداد را در سطح پیشرفته‌ای دخالت می‌دهند، مطلب مهمی به ما می‌آموزند: پژوهش‌هایی با نهایت خلوص و بدون منافع مادی در ریاضیات (و به‌ویژه راجع به اعداد اول) انجام شده‌اند که سالها و گاهی دهها سال بعد، به گونه‌ای غیرقابل پیش‌بینی، برای این یا آن کاربرد، جنبهٔ حیاتی یافته‌اند. گ.ه.هاردی[۱] (۱۹۴۷–۱۸۷۷) بریتانیایی، نظریه‌پرداز بزرگ در نظریهٔ اعداد و صلح‌طلبی پرحرارت، در کتاب خود تحت عنوان « دفاعیّهٔ از یک ریاضیدان» هدف کار خود را در زمینهٔ ریاضی کاملاً محض، یعنی حساب، که ظاهراً «سودمند» تلقی نمی‌شد، قرار داد. شاید کارهایش در زمان خود او «بی‌فایده» می‌نمود، اما امروز دیگر چنین نیست.

خم‌های بیضوی: هندسهٔ جبری در خدمت مأموران مخفی

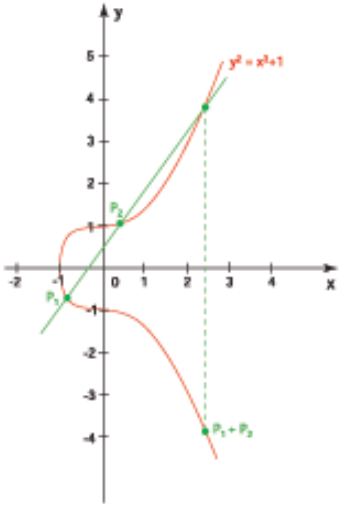
آنچه گفتیم منحصربه نظریهٔ اعداد نیست. حوزه‌های دیگری در ریاضیات که پیش از این می‌پنداشتند، هیچگونه کاربردی ندارند، در دانش رمزگذاری سهیم‌اند. در سال‌های اخیر روش‌های امیدبخشی در رمزنگاری ظاهر شده‌اند که بر اصولی نزدیک به اصول پروتکل RSA متکی هستند. یکی از این روش‌ها همان است که به نام روش لگاریتم گسسته[۲] نامیده می‌شود. این روش هم به نوبهٔ خود موجب شد به فکر روش‌های دیگری باشند که بر ویژگی‌های خم‌های بیضوی بنا می‌شوند. این خم‌ها به شکل بیضی نیستند بلکه خم‌هایی هستند که مطالعهٔ آن‌ها در قرن ۱۹، در جهت حل مسألهٔ پیچیدهٔ محاسبهٔ محیط بیضی آغاز شد. این خم‌ها که مختصات (x, y) یک نقطهٔ آن‌ها در معادلهٔ $y^2 = x^3 + ax + b$ صدق می‌کنند، ویژگی‌های جالبی دارند ـ که بررسی آن‌ها جزء هندسهٔ جبری است، که خود حوزهٔ وسیعی در ریاضیات فعلی است. مثلاً به کمک یک ساختمان هندسی مناسب، می‌توان به شکلی عمل جمع را بین نقاط خم بیضوی تعریف کرد. به‌طور کلی‌تر، خم‌های بیضوی که اشیائی هندسی هستند، دارای ویژگی‌های حسابی هستند که می‌تواند مورد استفاده در رمزنگاری قرار گیرد. به همین گونه است که یک روش

---

[۱] G. H. Hardy

[۲] logarithme discret

رمزنگاری موسوم به لگاریتم گسسته روی خم‌های بیضوی، تأسیس و گسترده شده است.



نمودار خم بیضوی به معادلهٔ $y^۲ = x^۳ + ۱$، خم‌های بیضوی ویژگی جالبی دارند: می‌توان دو نقطهٔ روی خم را طبق روشی که شکل نشان می‌دهد «با هم جمع کرد». عمل جمعی که به این طریق تعریف می‌شود از قواعد متداول حساب پیروی می‌کند (مثلاً $(P_۱ + (P_۲ + P_۳) = (P_۱ + P_۲) + P_۳$). برخی از روش‌های نوین رمزنگاری با توسل به خم‌های بیضوی و ویژگی‌های جبری آن انجام می‌پذیرند.

اخیراً، جهت دیگری نیز به ظهور پیوسته است. در کنگرهٔ بین‌المللی ریاضیدانان ۱۹۹۸ در برلین، پیتر شور[۱] از آزمایشگاه $AT\&T$ ، موفق به دریافت جایزهٔ نوانلینا[۲] به خاطر کارهایش روی رمزنگاری کوانتیک[۳] گردید. معنای این اصطلاح چیست؟ چند سال پیش، ریاضیدانان و فیزیکدانان به فکر افتادند که شاید بشود یک روز رایانه‌ای کوانتیک ساخت، یعنی رایانه‌ای که کارش بر مبنای قوانین عجیب و غریب فیزیک کوانتومی باشد، قوانینی که بر دنیای بی‌نهایت کوچک حاکم‌اند. متوجه شده‌اند که اگر این ساخت تحقّق یابد، آنگاه چنین رایانه‌ای قادر خواهد بود اعداد بزرگ را هم تجزیه کند و بدین ترتیب کارآیی روش RSA را از بین می‌برد. اخیراً تحقیقاتی دربارهٔ تحقّق عملی

---

[۱] Peter Shor

[۲] Nevanlinna

[۳] cryptogrphie quantique

این گونه رایانه‌های کوانتیک در مجلهٔ بریتانیایی نیچر[۱] منتشر شده است (آخرین مرجع ذیل). از سوی دیگر، محققین به پروتکل‌هایی برای رمزنگاری کوانتیک پرداخته‌اند، یعنی روش‌هایی مبتنی بر اشیائی (از قبیل فوتون‌ها، اتم‌ها و غیره) که از قوانین کوانتیک پیروی می‌کنند. این پروتکل‌های کوانتیک به شرط تحقق، ضامن ایمنی بدون چون‌وچرا خواهند بود. همهٔ این مسائل در دست بررسی است و امکان دارد ظرف چند سال آینده به شکل عملی درآید...

ژان‌لویی نیکولا
انیستیتو ژیراردزارگ، ریاضیات
دانشگاه کلود ـ برنار (لیون۱)

چند مرجع

- D. Kahn, *La guerre des codes secrets* (Interéditions, 1980).
- J. Stern, *La science du secret* (Odile Jacob, 1998).
- S. Singh, Histoire des codes secrets (J.-C. Lattès, 1999).
- J.-P. Delahaye, *Merveilleux nombers premiers* (Belin/pour la Science, 2000).
- D. Stinson, *Cryptographie, théorie et pratique* (Vuibert, 2001).
- L. M. K. Vandersypen et al., "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance", *Nature, vol. 414*, pp. 883-887 (20 décembre 2001)

Jean-Louis Nicolas
Institut Girard Desargues, Mathématiques,
Université Claude-Bernard (Lyon 1)

---

[۱] Nature