یک رمز و چند نفر!

نُهمی‌ها حتماً بخوانند!

تقسیم یک رمز بین چند نفر

محمود داورزنی

همان‌طور که در شماره‌های قبلی اشاره شد، دنیای امروز سرشار از اطلاعاتی است که به‌طور مداوم بین انسان‌ها و رایانه‌ها، دست‌به‌دست می‌شوند. بعضی از این اطلاعات باید رمز داشته باشند تا هر کسی نتواند به آن‌ها دست پیدا کند و فقط افراد یا دستگاه‌های خاص بتوانند آن‌ها را رمزگشایی کنند. مثلاً امواج رادیویی و تلویزیونی همه‌جا هستند، ولی فقط دستگاه‌های خاصی می‌توانند این اطلاعات را به نحو شایسته‌ای کدگشایی کنند و در اختیار ما قرار دهند و یا اطلاعات ارسالی از یک ماهواره که باید به زمین مخابره شود، به‌گونه‌ای است که لزوماً باید کد و رمز داشته باشد تا هرکسی نتواند از آن استفاده کند. در این شماره با روش تقسیم یک رمز بین چند نفر آشنا می‌شویم.

در این مطلب به اختصار نشان می‌دهیم که چه‌طور می‌توان یک پیام را بین چند نفر تقسیم کرد، به‌گونه‌ای که فقط با حضور آن چند نفر پیام حاصل شود و در غیر این صورت «هیچ» اطلاعاتی از آن پیام فاش نشود و به این ترتیب، امنیت رمز بیشتر شود.

فرض کنید شما رمز یک کیف را که به‌صورت یک عدد پنج رقمی است، در اختیار دارید و می‌خواهید هر رقم آن را در اختیار یک جمع ۲۰ نفره بگذارید. مثلاً اگر رمز به‌صورت

۰	۶	۷	۵	۲

باشد، عدد ۲ را در اختیار هفت نفر، عدد ۵ را در اختیار شش نفر و به همین ترتیب هر رقم را در اختیار تعدادی از اعضای آن گروه قرار دهید. اکنون برای دسترسی به این رمز، باید پنج نفر که هر کدام از یکی از گروه‌ها هستند، حضور داشته باشند و اگر کمتر از پنج نفر باشند، نمی‌توان رمز را شناسایی کرد، البته اطلاعات زیادی از آن رمز را می‌توان به‌دست آورد. مثلاً اگر چهار نفر از چهار گروه اول (که ترتیب قرار گرفتن اعداد رمز را نیز می‌دانند) بتوانند اعداد خود را کنار هم قرار دهند، رمز به‌طور ناقص به شکل

۲	۵	۷	۶	

به‌دست می‌آید و بدون حضور نفر پنجم از گروه پنجم، می‌توانند ارقام ۰ تا ۹ را به جای رقم آخر قرار دهند و با امتحان کردن حالت‌های مختلف، رمز به سادگی و به‌طور دقیق مشخص می‌شود. سؤالی که در اینجا مطرح می‌شود این است که: آیا می‌توان رمز را طوری تقسیم کرد که بدون حضور نفر پنجم، این رمز قابل شناسایی نباشد؟ یعنی حضور نداشتن نفر پنجم مانند حضور نداشتن تمام افراد باشد؟

یک راه حل این مشکل، استفاده از معادلات خط یا سهمی یا شکل‌های دیگر در صفحه است. هر خط راست در صفحه دارای معادله‌ای به‌صورت $y=ax+b$ است که در آن a و b اعداد حقیقی هستند؛ مانند خط $y = ۲x + ۳$. نوشتن معادلهٔ این خط یا ترسیم آن در صفحهٔ مختصات، نیازمند معلوم بودن حداقل دو نقطهٔ متمایز از خط است زیرا از یک نقطه، خط‌های بسیاری می‌گذرد. فرض کنید مقدار ثابت این خط یعنی عدد ۳، رمز مورد نظر ما باشد و ما به هر نفر از افرادی که قرار است رمز را بگشایند، مختصات یک نقطهٔ متفاوت از این خط را بدهیم. پس لازم است، حداقل دو نفر از آن‌ها نقاط خود را کنار هم قرار دهند تا بتوانند معادلهٔ خط را بنویسند. یک راه نوشتن معادلهٔ خط با داشتن دو نقطهٔ $(x_۱ , y_۱)$ و $(x_۲ , y_۲)$ از آن، استفاده از رابطهٔ زیر است:

$$y - y_۱ = \frac{y_۲ - y_۱}{x_۲ - x_۱}(x - x_۱)$$

یا این که آن نقاط را در معادلهٔ خط قرار دهیم و یک دستگاه دو معادله-دو مجهولی برحسب a و b به دست آوریم. برای مثال، به چهار نفر، چهار نقطه از این خط را به‌صورت زیر داده‌ایم.

نفراول	نفر دوم	نفر سوم	نفر چهارم
(۱,۵)	(۰,۳)	(-۱,۱)	(۲,۷)

اگرچــه هر نفر یــک نقطه از خط را در اختیار قــرار دارد ولی نمی‌تواند معادله خط را تشخیص دهد (در واقع نمی‌تواند رمز را بدون حضور فرد دوم تشخیص دهد). اگر نفر اول و دوم نقاط خود را کنار یکدیگر قرار دهند، داریم:

$$(1,5),(0,3) \Rightarrow y-5=\frac{3-5}{0-1}(x-1)$$
$$\Rightarrow y-5=2x-2 \Rightarrow y=2x+3$$

و اگر نفر دوم و چهارم نقاط خود را به اشتراک گذارند، داریم:

$$(0,3),(2,7) \Rightarrow y-1=\frac{7-1}{2+1}(x+1)$$
$$\Rightarrow y-1=2x+2 \Rightarrow y=2x+3$$

هر خط به‌صورت $y=ax+b$ یک چندجمله‌ای درجهٔ اول اســت کــه بــرای تعیین آن به داشــتن حداقل دو نقطه نیاز اســت. به‌طور مشــابه، هر منحنــی به‌صورت $y=ax^2+bx+c$ که یک چندجمله‌ای درجهٔ دوم و شــکل آن یک سهمی است، به حداقل ســه نقطه نیاز دارد تا به‌طور کامل مشخص شود و به همیــن ترتیب برای منحنی‌های با درجهٔ بزرگ‌تر، تعداد نقاط مورد نیاز بیشتر می‌شود. مطالعهٔ بیشتر دربارهٔ آن‌ها را به عهدهٔ خود شما دانش‌آموزان عزیز قرار می‌دهیم.

با توجه به صحبت‌های بــالا، اگر بخواهیم امنیت رمزی را بالا ببریم و آن را بین افراد بیشــتری تقســیم کنیم، می‌توانیم از چندجمله‌ایِ با درجهٔ بالاتر اســتفاده کنیم. مثلاً اگر بخواهیم حضور دقیقاً ســه نفر برای رمزگشــایی عدد رمز ۱- ضروری باشد، از یک ســهمی کمک می‌گیریم. فرض کنید (۲- و ۱)، (۱- و ۲) و (۲و ۳) ســه نقطه از آن باشــند که به سه نفر داده شده است. در این صورت چندجمله‌ای درجهٔ دومی که از این سه نقطه می‌گذرد را می‌توانیم طبق فرمول زیر به‌دست آوریم:

$$y=y_1\frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)}+y_2\frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)}$$
$$+y_3\frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)}$$

یا با جای‌گذاری نقاط در معادلهٔ ســهمی، و حل دســتگاه سه معادله-ســه مجهولــی، ضرایب معادله را بیابیم. مــا این کار را کردیم و معادلهٔ زیر به دست آمد:

$$y=x^2-2x-1$$

اکنــون می‌توانیم مقدار این چندجمله‌ای را در $x=0$ که برابر با $y=-1$ است، به‌عنوان عدد رمز به‌دست آوریم.

مســئله ۱ اگر عدد رمــز برابر با ۲۵۷۶۰ باشــد که در ابتدای مطلب به آن اشاره کردیم، و بخواهیم آن را بین چهار نفر توزیع کنیم که با حضور حداقل ســه نفر بتوان این عدد را شناســایی کرد، مراحل انجام این کار را بنویســید و سهم هرکدام از چهار نفر را مشخص کنید.

مســئلــهٔ ۲ اگر بخواهیم عدد رمــز ۷ را بین چهار نفر توزیع کنیم که فقط با حضور هر چهار نفر این عدد کشــف شــود، آیا می‌توانید روند ساده‌ای را برای رمز کردن این عدد پیدا کنید؟

منابع

۱. بوخمان، جوهانزا، مقدمه‌ای بر رمزنگاری، ترجمه دکتر مرتضی اســماعیلی، انتشارات دانشگاه صنعتی اصفهان، چاپ دوم، سال ۱۳۸۷.

2. Stinson, Douglas. R, *Cryptography Theory and Practice*, CRC Press, 2008.