محمود داورزني، تينا اسدي، مبينا صفري
دبيرستان فرزانگان حضرت زينب (س) دوره دوم، شهرری

سهم هر کدام از این راز

چکیده

تقسیم یک عدد به‌عنوان یک رمز بین چند نفر، «تسهیم راز» نامیده می‌شود. هدف از یک طرح تسهیم راز آستانه‌ای این است که برای کشف رمز، حداقل K نفر نیاز باشند و اگر کمتر از این تعداد حضور داشته باشند، از کنار هم قرار دادن سهم‌های خود، هیچ‌گونه اطلاعاتی دربارهٔ رمز به‌دست نیاورند. در این مقاله، طرح‌های تسهیم رازی را بررسی می‌کنیم که کشف رمز نیازمند حداقل ۲، ۳، ...، t نفر است و این کار را به کمک چندجمله‌ای‌ها درجهٔ ۱، ۲ و t−۱ انجام می‌دهیم. در پایان به کمک یک رابطه، تسهیم راز آستانه‌ای را برای هر عدد دلخواه K تعمیم می‌دهیم. نمودار توابعی که شامل این چندجمله‌ای‌هاست، شامل خط راست، سهمی و تابع درجهٔ سوم می‌شود که با مطالب درسی پایه‌های نهم تا دوازدهم تطبیق دارد و می‌تواند به‌عنوان کاربرد این نمودارها بیان شود.

کلید واژه‌ها: تسهیم راز، توابع چندجمله‌ای، طرح آستانه‌ای، درون‌یابی لاگرانژ

مقدمه

تسهیم راز که «تقسیم راز» نیز نامیده می‌شود، روشی برای توزیع یک رمز بین چند نفر است، به‌طوری که تعداد اعضای مشخصی با کنار هم قرار دادن سهم‌های خود، بتوانند رمز را کشف کنند و اگر از تعداد مشخصی، افراد کمتری سهم‌های خود را کنار یکدیگر قرار دهند، رمز قابل شناسایی نباشد و البته هیچ اطلاعاتی نیز دربارهٔ رمز نتواند کسب کنند. مثال زیر برای روشن شدن مطلب بسیار مفید است. فرض کنید رمز یک گاوصندوق، عددی پنج‌رقمی، مانند ۷۳۰۹۴ است. اگر هر رقم را به همراه شمارهٔ جایگاه آن (یکان، دهگان و ...) به یک نفر بدهیم، واضح است که با حضور پنج نفر، رمز گاوصندوق قابل شناسایی است. حال اگر چهار نفر حضور داشته باشند و سهم‌های خود را به شکل ۷۳□۹۴ کنار یکدیگر قرار دهند، اگرچه رمز شناسایی نشده است، ولی با امتحان کردن ۱۰ رقم (۰، ۱، ۲، ...، ۹) می‌توان رمز را کشف کرد. در این مثال با حضور پنج نفر، رمز معلوم است و با حضور تعداد کمتری از اعضا هم رمز قابل شناسایی است. اما هر قدر افراد بیشتری حضور داشته باشند، زمان کمتری برای کشف رمز نیاز خواهد بود.

تسهیم راز چیزی فراتر از مثال بالاست. به عنوان نمونه، در یک طرح تسهیم راز که با حضور پنج نفر، رمز قابل شناسایی است، با حضور تعداد کمتری از پنج نفر، هیچ اطلاعاتی دربارهٔ رمز نمی‌توان کسب کرد و در حقیقت مانند آن است که هیچ کدام از اعضا، سهم خود را به مشارکت قرار نداده است. ایدهٔ چنین طرح‌های تسهیم راز در سال ۱۹۷۹ توسط **ادی شمیر**[1] و **جورج بلاکلی**[2] به‌طور مستقل بنیان گذاشته شد و تا به امروز این ایده گسترش یافته است.

طرح‌هاي تسهيم راز آستانه‌اي

در یک طرح تسهیم راز، رمزی بین n نفر توزیع می‌شود. با حضور حداقل t نفر از اعضا، رمز قابل شناسایی است و اگر تعداد افراد حاضر کمتر از t نفر باشد، هیچ اطلاعی دربارهٔ رمز کسب نخواهند کرد. به چنین طرح‌هایی، طرح‌های تسهیم راز آستانه‌ای (t,n) گفته می‌شود. در این مقاله، طرح‌های تسهیم راز آستانه‌ای (۲,n)، (۳,n) و (t,n) را که در آن‌ها $t \geq 4$ است، بررسی می‌کنیم. در یک طرح آستانه‌ای، به هر یک از افراد، یک زوج مرتب یا نقطه اختصاص می‌یابد که در آن مؤلفهٔ اول، همان شمارهٔ فرد و مؤلفهٔ دوم، عدد مختص آن فرد است.

۱. طرح آستانه‌ای (۲,n)

در یک طرح آستانه‌ای (۲,n)، یک رمز بین n نفر تقسیم می‌شود، به‌طوری که هیچ کس به تنهایی نتواند آن رمز را به‌دست آورد و اگر دو نفر یا بیشتر، سهم‌های خود را با هم به اشتراک بگذارند، می‌توانند رمز را پیدا کنند. فرض کنیم: n=۳ و به نفرات اول تا سوم نقاط زیر را به‌عنوان سهم آن‌ها اختصاص می‌دهیم:

(۳,۹۳۴), (۲,۹۶۴), (۱,۹۹۴)

اکنون اگر هر نفر سهم خود را که یک نقطه است، با سهم فرد دیگری کنار یکدیگر قرار دهند، می‌توانند معادلهٔ خط گذرنده از آن نقاط را بنویسند. به‌عنوان نمونه، خطی که از سهم نفر اول و دوم می‌گذرد، عبارت است از:

$$y-۹۹۴=\frac{۹۹۴-۹۶۴}{۱-۲}(x-۱)\Rightarrow y=-۳۰x+۱۰۲۴$$

به همین شکل، معادلهٔ خط‌هایی که از سهم نفر دوم و سوم و همچنین سهم نفر اول و سوم می‌گذرد، عبارت‌اند از:

$$y-۹۹۴=\frac{۹۹۴-۹۳۴}{۱-۳}(x-۱)\Rightarrow y=-۳۰x+۱۰۲۴$$

$$y-۹۶۴=\frac{۹۶۴-۹۳۴}{۲-۳}(x-۲)\Rightarrow y=-۳۰x+۱۰۲۴$$

بنابراین هر دو نفر که با یکدیگر مشارکت کنند، به معادلهٔ خط $y=-۳۰x+۱۰۲۴$ خواهند رسید. اکنون اگر رمز را مقدار ثابت معادلهٔ خط، یعنی ۱۰۲۴ در نظر بگیریم و تمام اعضا نیز از قبل بدانند که رمز تقسیم شده، مقدار ثابت معادلهٔ خط است، طبق بحث انجام شده، هر دو نفری قادر به دستیابی به این عدد خواهند بود.

از دید هندسی، این روش تقسیم رمز بسیار واضح است. فرض کنید عرض از مبدأ یک خط را به‌عنوان رمز انتخاب کرده‌ایم و به هر نفر، یک نقطهٔ از این خط را داده‌ایم. روشن است که برای دستیابی به معادلهٔ خط، دو نقطهٔ آن نیاز است و اگر تنها یک نقطه از این خط را داشته باشیم، با توجه به اینکه بی‌نهایت خط از این نقطه می‌گذرد، هیچ اطلاعی نسبت به خط مورد بحث نخواهیم داشت. در حقیقت، وجود یا نبود یک نقطه به تنهایی هیچ تأثیری در کشف رمز ندارد.

۲. طرح آستانه‌ای (۳,n)

در یک طرح آستانه‌ای (۳,n)، یک رمز بین n نفر تقسیم می‌شود، به‌طوری که برای کشف رمز، مشارکت حداقل سه نفر ضروری است. در این طرح، رمز مورد نظر را مقدار ثابت سهمی، یعنی عدد c در معادلهٔ $y=ax^۲+bx+c$ انتخاب می‌کنیم و به هر فرد نقطه‌ای از این سهمی را به‌عنوان سهم اختصاص می‌دهیم. به‌عنوان نمونه، اگر رمز عدد ۱۵ باشد، سهمی $y=۲x^۲-۳x+۱۵$ را که ضرایب x و $x^۲$ آن به‌طور تصادفی انتخاب شده‌اند، انتخاب می‌کنیم و به هر فرد نقطه‌ای از این سهمی را به‌عنوان سهم آن فرد اختصاص می‌دهیم، به‌طوری که مؤلفهٔ اول نقطه‌های تخصیص داده شده، شمارهٔ فرد مورد نظر است. به‌عنوان نمونه، اگر داشته باشیم: n=۴، سهم این چهار نفر عبارت‌اند از:

(۱,۱۴), (۲,۱۷), (۳,۲۴), (۴,۳۵)

اکنون فرض کنید سه نفر اول سهم خود را به مشارکت می‌گذارند. برای این کار هر نقطه را در معادلهٔ $y=ax^۲+bx+c$ قرار می‌دهیم و با کنار یکدیگر قرار دادن معادله‌های حاصل شده، دستگاه زیر به‌وجود می‌آید:

$$\begin{cases}a+b+c=۱۴\\ ۴a+۲b+c=۱۷\\ ۹a+۳b+c=۲۴\end{cases}$$

برای حل این دستگاه، مقدار c را از معادلهٔ اول به‌دست می‌آوریم:

$$a+b+c=۱۴\Rightarrow c=۱۴-a-b$$

و این مقدار را به جای c در معادله‌های دوم و سوم دستگاه بالا قرار داده و دستگاه حاصل را حل می‌کنیم:

$$\begin{cases}۴a+۲b+c=۱۷\\ ۹a+۳b+c=۲۴\end{cases}\Rightarrow\begin{cases}۴a+۲b+(۱۴-a-b)=۱۷\\ ۹a+۳b+(۱۴-a-b)=۲۴\end{cases}\Rightarrow$$

$$\begin{cases}۳a+b=۳\\ ۸a+۲b=۱۰\end{cases}\Rightarrow a=۲,b=-۳$$

پس مقدار c نیز به شکل زیر به‌دست می‌آید:

$$c=۱۴-a-b\Rightarrow c=۱۴-۲+۳=۱۵$$

بنابراین معادلهٔ سهمی می‌شود: $y=۲x^۲-۳x+۱۵$ و در نتیجه عدد رمز ۱۵ است (c=۱۵).

هر سه نفر دیگر از این چهار نفر نیز می‌توانند سهم‌های خود را به اشتراک بگذارند و مقدار رمز را کشف کنند. نکته‌ای که باید به آن دقت داشت این است که در معادلهٔ $y=ax^۲+bx+c$، سه مجهول a، b و c وجود دارد و باید حداقل سه نقطه از سهمی مشخص باشد تا بتوان در یک دستگاه سه معادله و سه مجهول، a، b و c را پیدا کرد. با توجه به اینکه در یک طرح آستانه‌ای (۳,n)، حضور حداقل سه نفر ضروری است، بنابراین تعداد گروه‌های با کمترین عضو که می‌توانند رمز را کشف کنند، عبارت است از:

$$\binom{n}{۳}=\frac{n!}{۳!\times(n-۳)!}=\frac{n(n-۱)(n-۲)}{۶}$$

۳. فرمول درون‌یابی لاگرانژ

نقاط زیر را در صفحه در نظر بگیرید:

$$(x_۱, y_۱), (x_۲, y_۲), (x_۳, y_۳)$$

چندجمله‌ای $P(x)$ که از این نقطه‌ها عبور می‌کند، عبارت است از:

$$P(x) = \frac{(x-x_۲)(x-x_۳)}{(x_۱-x_۲)(x_۱-x_۳)} y_۱ + \frac{(x-x_۱)(x-x_۳)}{(x_۲-x_۱)(x_۲-x_۳)} y_۲ + \frac{(x-x_۱)(x-x_۲)}{(x_۳-x_۱)(x_۳-x_۲)} y_۳$$

این رابطه به «فرمول درون‌یابی لاگرانژ» معروف است.

برای مثال، چندجمله‌ای که از نقطه‌های (۱،۱۴)، (۲،۱۷) و (۳،۲۴) می‌گذرد، عبارت است از:

$$\begin{aligned} P(x) &= \frac{(x-۲)(x-۳)}{(۱-۲)(۱-۳)} \times ۱۴ + \frac{(x-۱)(x-۳)}{(۲-۱)(۲-۳)} \times ۱۷ + \frac{(x-۱)(x-۲)}{(۳-۱)(۳-۲)} \times ۲۴ \\ &= ۷(x^۲ - ۵x + ۶) - ۱۷(x^۲ - ۴x + ۳) + ۱۲(x^۲ - ۳x + ۲) \\ &= ۷x^۲ - ۳۵x + ۴۲ - ۱۷x^۲ + ۶۸x - ۵۱ + ۱۲x^۲ - ۳۶x + ۲۴ \\ &= ۲x^۲ - ۳x + ۱۵ \end{aligned}$$

بنابراین با وجود سه نقطه، چندجمله‌ای که از این نقطه‌ها می‌گذرد، از درجهٔ دوم است.

در حالت کلی، اگر t نقطه به شکل زیر داشته باشیم:

$$(x_۱, y_۱), (x_۲, y_۲), (x_۳, y_۳), \ldots, (x_t, y_t)$$

طبق فرمول درون‌یابی لاگرانژ، چندجمله‌ای از درجهٔ $t-۱$ که از این نقطه‌ها عبور می‌کند، عبارت‌است از:

$$P(x) = \frac{(x-x_۲)(x-x_۳)\ldots(x-x_t)}{(x_۱-x_۲)(x_۱-x_۳)\ldots(x_۱-x_t)} y_۱ + \frac{(x-x_۱)(x-x_۳)\ldots(x-x_t)}{(x_۲-x_۱)(x_۲-x_۳)\ldots(x_۲-x_t)} y_۲ + \ldots + \frac{(x-x_۱)(x-x_۳)\ldots(x-x_{t-۱})}{(x_t-x_۱)(x_t-x_۲)\ldots(x_t-x_{t-۱})} y$$

۴. طرح آستانه‌ای (t,n)

در یک طرح تسهیم راز آستانه‌ای (t,n)، باید یک رمز را بین n نفر توزیع کرد، به‌طوری که با حضور حداقل t نفر، رمز قابل دستیابی باشد. برای این کار، رمز را مقدار $a_۰$ در چندجمله‌ای زیر انتخاب می‌کنیم:

$$P(x) = a_{t-۱}x^{t-۱} + a_{t-۲}x^{t-۲} + \ldots + a_۱x + a_۰$$

و سهم فرد با شمارهٔ i، نقطهٔ $(i, P(i))$ است. اکنون اگر t نفر از n نفر، سهم‌های خود را به مشارکت بگذارند، طبق فرمول درون‌یابی لاگرانژ که در بند ۳ همین مقاله آمده است، چندجمله‌ای $P(x)$ از درجهٔ $t-۱$ نوشته شده و از آن مقدار ثابت چندجمله‌ای، یعنی $a_۰$، مشخص می‌شود.

با توجه به اینکه در یک طرح آستانه‌ای (t,n)، حضور حداقل t نفر ضروری است، بنابراین تعداد گروه‌های با کمترین عضو که می‌توانند رمز را کشف کنند، عبارت است از:

$$\binom{n}{t} = \frac{n!}{t! \times (n-t)!}$$

نتیجه‌گیری

هر خط به معادلهٔ $y = ax + b$، به‌عنوان یک چندجمله‌ای درجهٔ یک، با دو نقطه، هر سهمی به معادلهٔ $y = ax^۲ + bx + c$ به‌عنوان یک چندجمله‌ای درجهٔ دو، با سه نقطه و به همین ترتیب، هر چندجمله‌ای از درجهٔ t، با $(t-۱)$ نقطه از آن قابل دستیابی است. این ویژگی ساده، پایه و اساس یکی از بخش‌های مهم رمز با عنوان تسهیم راز است. در این مقاله، طرح‌های آستانه‌ای تسهیم راز به شکل (t,n) به‌طور کامل بررسی شدند. در حالت‌های ابتدایی این طرح که $t=۱$ و $t=۲$ است، خط و سهمی به ترتیب اساس کار هستند و این مطالب نیز تا پایهٔ دهم به‌طور کامل در کتاب‌های درسی آموزش داده شده‌اند. هر دانش‌آموز می‌تواند با مطالعهٔ طرح‌های تسهیم راز بیان شده، به اهمیت مطالب درسی در سطح عالی پی ببرد.

پی‌نوشت‌ها

1. Adi Shamir
2. George Blakley

منابع

۱. اسماعیلی، مرتضی (۱۳۸۷). مقدمه‌ای بر رمزنگاری. مرکز نشر دانشگاه صنعتی اصفهان.

2. Douglas R. Stinson (2005). Cryptography: Theory and Practice. Chapman and Hall/CRC; 3rd edition.