به بهانهٔ دههٔ ریاضیات

ریاضیات و رمز نگاری

نویسنده: عبدالحسین مصحفی*

تبدیل یک واژه یا یک پیام را به یک نشانه یا به مجموعه‌ای از نشانه‌ها، به گونه‌ای که مگر کسانی معین، دیگران به مفهوم آن پی نبرند، *به رمز درآوردن*، *رمزنویسی* و یا *رمزنگاری* می‌نامند. عمل عکس، یعنی عمل پی‌بردن به مفهوم پیام رمزی را، *از رمزدرآوردن*، *رمزخوانی*، و یا *رمزگشایی* می‌گویند.

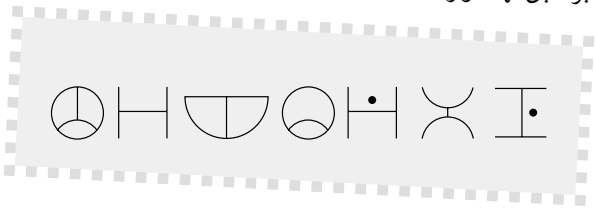
گونه‌ای ساده و همگانی از به‌کار بردن رمز، ایما و اشاره‌هایی است که دو نفر در یک جمع با هم ردّ و بدل می‌کنند. دو دانش‌آموز که در یک آزمون دیکته، بنا بر قرارداد قبلی، با مالاندن چشم، با خاراندن گونه، ... و با اشاره‌هایی از این گونه به یکدیگر می‌فهمانند که باید ز، ض یا ظ را به‌کار برد گونه‌ای پیام‌های رمزی را به کار می‌برند. کسی که در یک نوشتار یا در یک گفتار، جمله‌ای را بیان می‌کند و یا شعری را می‌خواند و کسانی از آن به دستوری معین پی می‌برند، یک پیام رمز را به کار برده است. حرف‌های مقطّع که در آغاز بعضی از سوره‌های قرآن بیان شده‌اند، رمزهایی هستند که مفسّران قرآن در پی گشایش آن‌ها بوده‌اند. در انجمن‌های سرّی فیثاغورسی‌ها، و در بیش‌تر انجمن‌های سرّی، هر عضو یک نام رمزی داشته که با آن شناسایی می‌شده است. امروزه هم در به‌کار بردن پست الکترونیکی، هرکس یک رمز شناسایی باید داشته باشد که تنها با ارایهٔ آن می‌تواند نامه‌هایش را بفرستد یا نامه‌های رسیده را ببیند و بخواند. در گذشته، کسانی که با شبه‌علم‌های پنج‌گانهٔ *کیمیا*، *لیمیا*، *هیمیا*، *سیمیا* و *ریمیا* سروکار داشته‌اند، داده‌ها و دستورهای کار را با نشانه‌هایی رمزی می‌نوشته‌اند. بیش از همه درجنگ‌ها و از گذشته‌های بسیار دور تا به امروز، پیام‌های رمزی و گشایش آن‌ها، کاربرد مهم داشته‌اند و دارند.

رمزنگاری ساده است و هرکس به سادگی می‌تواند با شیوه‌ای ابتکاری آن را انجام دهد. در برابر، رمزگشایی به ویژه اگر رمزنگاری با مهارت انجام گرفته باشد، کاری دشوار است. امروزه به کمک ریاضیات است که می‌توانند به شیوهٔ مطمئن رمزنگاری کنند و در رمزگشایی توانایی لازم را به دست آورند. در

این نوشتار، نمونه هایی از رمزنگاری ها نموده می شوند و به ویژگی های آن ها اشاره می شود.

نمونهٔ ۱. از کتاب اسرار قاسمی، بخش ریمیا

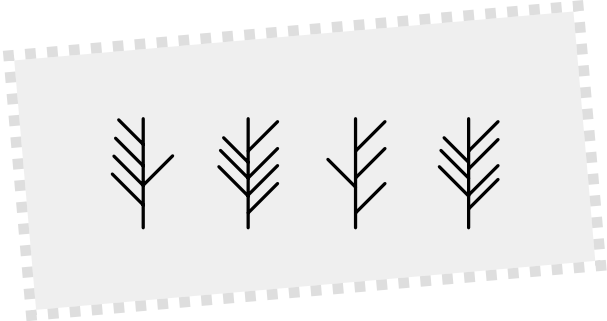
لعب الطیر این چنان است که مرغ بریان در طبق آواز کند و عملش چنان است که قدری در گلوی وی نهد و در تنور آویزد و بر طبق نهد آواز کند.



در این شیوهٔ رمزنویسی، الفبای فارسی به الفبایی با نشانه های من در آوردی تبدیل شده است. با یک کلمهٔ به این زبان، نمی توان به رمز پی برد. مگر آنکه کلمه ها و جمله های دیگری از آن را با هم بررسی کرد.

نمونهٔ ۲. از کتاب خزائن العلوم

بدان که کتب مشهوره که قدما در علوم خمسهٔ محتجبه نوشته اند بسیار است، ...، و قلم های رمزی که در این تألیفات به کار رفته نیز بسیار است و از جملهٔ آنها *الفبای درختی* است و مثلاً محمد را چنین نویسند:



در نمونهٔ ۱ و در نمونه هایی از همان گونه، نشانه های رمزی بدون قاعده گزیده می شوند. اما در نمونهٔ۲، نشانه ها بر پایهٔ قاعده ای معین به دست می آیند. ۲۸ حرف الفبای زبان عربی به ۸ جملهٔ « **ابجد، هوز، حطی، کلمن، سعفص، قرشت، ثخذ، ضظغ** » دسته بندی می شوند. این کلمه ها به ترتیب از ۱ تا ۸ شماره گذاری می شوند و حرف های هریک از جمله ها نیز یک شمارهٔ ترتیب دارند. به این ترتیب، به هر حرف دو شماره نظیر می شود؛ شمارهٔ جملهٔ شامل آن حرف و شمارهٔ آن حرف در این جمله. خطی قائم و کوتاه به عنوان ساقهٔ درخت رسم می شود و در سمت راست آن، شاخه هایی به شمارهٔ جمله و در سمت چپ آن شاخه هایی به شمارهٔ حرف به ساقه افزوده می شوند. حرف م در مرتبهٔ ۳ از جملهٔ کلمن (=جملهٔ چهارم) جای دارد. پس با چهار شاخه در سمت راست و سه شاخه در سمت چپ نموده می شود. به عبارت دیگر، حرف م با عدد دورقمی ۴۳، و نام محمد هم به صورت «۴۳، ۳۱، ۴۳، ۱۴» به رمز در می آید.

نمونهٔ ۳. رمزنگار سزاری

ژول سزار امپراطور روم قدیم را نخستین فرمانروایی می شناسند که پیام های خود را به رمز در می آورد. شیوهٔ رمزنگاری او به این ترتیب بود که به جای هر حرف از الفبا، حرف مرتبهٔ سوم پس از آن را به کار می برد و در شمارش حرف ها، پس از آخرین حرف به حرف یکم و به حرف های پس از آن برمی گشت. با این شیوه، جملهٔ «ریاضیات را به کار ببرید» به جملهٔ رمزی زیر تبدیل می شود:

سپتعپت چستثب متست شسپز

شیوهٔ رمزنگاری سزاری در طول تاریخ با تحول هایی به کار رفته و امروزه هم با تحول هایی جدید به کار می رود.

نمونهٔ۴. رمزنگاری با حساب هم نهشتی

در حساب هم نهشتی، عددی به عنوان *پیمانه* گزیده می شود و هر دو عدد را که در تقسیم بر عدد پیمانه، باقی مانده های برابر داشته باشند، هم نهشت به آن پیمانه می نامند. اگر ۷ را پیمانه بگیریم دو عدد ۴۵ و ۱۲۹ هم نهشت می شوند و می نویسیم:

$$129 \equiv 45 \pmod{7}$$ (پیمانهٔ ۷)

در رمزنگاری با حساب هم نهشتی، تعداد حرف های الفبا را پیمانه می گیرند؛ این پیمانه، برای الفبای فارسی ۳۲، برای حرف های الفبای عربی ۲۸ و برای الفبای انگلیسی ۲۶ می شود. حرف های الفبا نیز به ترتیب شماره گذاری می شوند. در زبان

فارسی برای الف شمارهٔ ۱ ، برای ب شمارهٔ۲ ، ... ، و سرانجام برای ی شماره ۳۲ را خواهیم داشت . اکنون اگر مضرب دلخواهی از ۳۲ را به شمارهٔ یک حرف بیفزاییم عددی که به دست می آید با شمارهٔ آن حرف هم نهشت است . برای نمونه ، شمارهٔ حرف س برابر با ۱۵ است . عدد دلخواهی مثلاً ۱۷ را در ۳۲ ضرب می کنیم که می شود ۵۴۴ و این را با ۱۵ جمع می کنیم می شود ۵۵۹ . اگر این عدد بر ۳۲ تقسیم شود ، باقی ماندهٔ تقسیم ۱۵ می شود . بنابراین دو عدد ۵۵۹ و ۱۵ به پیمانهٔ ۳۲ هم نهشت اند .

برای به رمز درآوردن یک جمله یا یک عبارت ، هر حرف آن را به شماره اش تبدیل می کنند و به جای این شماره ، عددی دلخواه اما هم نهشت با آن را رمز آن حرف انتخاب می کنند . هر عدد را هم که در آن جمله یا عبارت باشد به همان پیمانهٔ ۳۲ به رمز در می آورند . جمله یا عبارت به دنباله ای از عددها تبدیل می شود .

مثال . نمایندهٔ یک بازرگان می خواهد پیام «طلا رو به بالاست» را برای بازرگانی به رمز فاکس کند . او حرف های این جمله را به ترتیب زیر به رمز در می آورد :

$$ط = 19 \to 19 + 32 \times 29 = 947$$
$$ل = 27 \to 27 + 32 \times 83 = 2683$$
$$ا = 1 \to 1 + 32 \times 56 = 1793$$
$$ا = 1 \to 1 + 32 \times 56 = 1793$$
$$س = 15 \to 15 + 32 \times 17 = 559$$
$$ت = 4 \to 4 + 32 \times 45 = 1444$$

و پیام رمزی زیر را روی فاکس بازرگانی مخابره می کند :

947 – 2683 – 1793 – 748 – 606 – 706 – 2143 – 2242 – 417 – 475 – 2017 – 559 – 1444.

بازرگان پس از دیدن این پیام ، هر کدام از عددها را بر ۳۲ تقسیم می کند و مطابق با باقی ماندهٔ تقسیم ، حرف نظیر آن از الفبا را به دست می آورد و از این راه به اصل پیام پی می برد .

نمونهٔ ۵. دسته بندی حرف های الفبا

همانند شیوهٔ الفبای درختی ، حرف های الفبای زبان به چندین دسته تقسیم می شوند به گونه ای که تعداد دسته ها و تعداد حرف های هر دسته ، عددهایی یک رقمی باشند . دسته ها شماره گذاری و حرف های هر دسته نیز شماره گذاری می شوند . با این فرآیند ، به هرحرف دو شمارهٔ یک رقمی تعلق می گیرد و هر حرف با عددی دو رقمی نموده می شود . برای مثال ، حرف های الفبای فارسی را به گونهٔ زیر به ۶ دسته تقسیم می کنیم :

۱) ا ب پ ت ث
۲) ج چ ح خ
۳) د ذ ر ز ژ
۴) س ش ص ض ط ظ
۵) ع غ ف ق ک گ
۶) ل م ن و ه ی

و خواهیم داشت :

ا=۱۱ ، ب= ۱۲ ، پ= ۱۳ ، ... ، ز= ۳۴ ، ... ، غ= ۵۲ ، ... ، ی= ۶۶ وجملهٔ «کامیاب باشید» به شکل زیر در می آید :

۵۵ , ۱۱ , ۶۲ , ۶۶ , ۱۱ , ۱۲ , ۱۲ , ۱۱ , ۴۲ , ۶۶ , ۳۱

در ارتباط با رایانه ، رمزهایی به کار می روند که به همین شیوهٔ دسته بندی ، از حرف های الفبا ، رقم های عدد نویسی و تعدادی از نشانه ها فراهم آمده اند و در جای خود به چگونگی نمایش آن ها اشاره خواهد شد .

کلید رمز

مسألهٔ مهم در به رمز درآوردن یک پیام ، به ویژه که امروزه پیام ها با امواج رادیویی و با ابزارهای الکترونیکی پخش می شوند ، به کار بردن شگردهایی است که غیر خودی ها با دست یافتن به پیام نتوانند آن را از رمز درآورند و به مفهوم آن پی ببرند . برای این کار ، برای هر پیام رمزی ، رمز ویژه ای را نیز به کار می برند که گیرندهٔ پیام تنها با آگاهی با آن می تواند به شگرد به کار رفته درعمل رمزنگاری پی ببرد . این رمز ویژه را *کلیدرمز* می نامند .

از جمله شگردهایی که در به کارگیری ابجد ، هوز ، ... به کار می برده اند عوض کردن و تغییر دادن ترتیب حرف ها بوده است و هر ترتیب جدید را با نامی می نموده اند که کلید رمز به شمار می آمده است . از جملهٔ این ترتیب ها ، *ابجد کبیر* ، *ابجدصغیر* ،

ابجد شرقی، *ابجد مغربی*، *ابجد وسیط*، *ابجد جامع*، *ابجد معکوس*، *ابجد جَفْری*، ... بوده است. برای نمونه، در رمزگذاری با ترتیب ابجد معکوس، جملهٔ «کلیدرمز» به جملهٔ «صفقذ طعت» تبدیل می شود.

شگردی که در رمزگذاری به شیوهٔ سزاری عموماً به کار می رود این است که تبدیل حرف ها به حرف های دیگر، نه با فاصله های برابر بلکه با فاصله های مختلف انجام می گیرد. برای نمونه، حرف یکم پیام به حرف یکم پس از آن، حرف دوم پیام به حرف سوم پس از آن، حرف سوم به حرف هشتم پس از آن، حرف چهارم به حرف دوم پس از آن، و برای حرف های بعدی این فرآیند تکرار می شود و عدد ۱۳۸۲ کلید رمز می شود. برای نمونه، جملهٔ «آماده باش اعلام کنید» با این کلید رمز به جملهٔ «بهخریث خصبقت پنم ثبذ» تبدیل می شود.

در این شیوهٔ رمزگذاری، کلید رمز هرچه طولانی تر باشد عمل رمزنگاری از اطمینان بیش تر برخوردار است و رمزگشایی آن برای حریفان دشوارتر خواهد بود.

امروزه شیوه های تبدیل حرف به عدد، معمول ترین شیوهٔ رمزنگاری است و افزون بر حرف های الفبا، عددها و علامت ها را نیز در برمی گیرد. شگردی که در این شیوه ها به کار می رود، تبدیل عددهای اصلی نظیر به پیام به عددهای دیگر است و این کار به کمک ریاضیات انجام می گیرد. یک فرمول ریاضی را کلید رمز می گیرند و عدد را با این فرمول به عددی جدید تبدیل می کنند و پس از آن هم یک رقم کنترل سمت راست عدد می نویسند. برای نمونه، اگر فرمول

$$y = 2a + 5b + 7c$$

کلید رمز و با یک شیوهٔ دسته بندی، حرف ع به عدد سه رقمی ۱۰۹ تبدیل شده باشد، رقم ۱ را به جای a، رقم ۰ را به جای b و رقم ۹ را به جای c می گذارند که عدد ۶۵ به دست می آید. مجموع رقم های این عدد ۱۱ و عددی فرد است. پس یک رقم دلخواه فرد مثلاً ۷ را هم سمت راست ۶۵ می نویسند و رمز حرف ع می شود ۶۵۷. حرف ها و علامت های دیگر پیام هم به همین ترتیب به عدد تبدیل می شوند.

یک روش ریاضی دیگر به کار بردن *ماتریس ها* است. ماتریس ها جدول هایی عددی هستند که در ریاضیات تعریف می شوند و در همهٔ زمینه ها کاربرد دارند. یک ماتریس دلخواه مثلاً ماتریس سه در سهٔ

$$\begin{bmatrix} 1 & 3 & 2 \\ 1 & 2 & 4 \\ 1 & 2 & 3 \end{bmatrix}$$

به عنوان کلید رمز پذیرفته می شود. برای آن که پیام «قرارداد را بپذیرید» به رمز درآید، شماره های حرف ها در ترتیب الفبا سه به سه دسته بندی می شوند:

[24 12 1] , [12 10 1] , [10 12 1] , [2 3 11] , [32 12 32] , [10 32 10]

و این ماتریس ها به ترتیب در ماتریس کلید رمز ضرب می شوند. بنابر قاعدهٔ ضرب ماتریس ها، حاصل ضرب ها به ترتیب برابرند با:

[62,52,51] , [44,36,35] , [48,38,37] , [33,52,41] , [132,184,152] , [128,116,106].

و پیام رمز می شود:

۶۲, ۵۲, ۵۱, ۴۴, ۳۶, ۳۵, ۴۸, ۳۸, ۳۷, ۳۳, ۵۲
۴۱, ۱۳۲, ۱۸۴, ۱۵۲, ۱۲۸, ۱۱۶, ۱۰۶.

رساندن کلید رمز به گیرندهٔ اصلی پیام

کسی که باید پیام رمز را دریافت و به آن عمل کند لازم است که کلید رمز آن را هم بداند. مسئولان رمزنویسی و رمزخوانی در سازمان ها، معمولاً جدول هایی را در دسترس دارند و کافی است بدانند جدول با کدام شماره را به کار ببرند. رساندن همین شماره، کلید رمز به شمار می آید. در موردهایی، کلید رمز را به گونه ای در پیام رمزی جای می دهند و یا با آن همراه می کنند. اما این عمل هم خالی از خطر نیست. حریفان که در پی دست یابی به پیام های رمزی و خواندن آن ها هستند از متخصصانی یاری می گیرند که هم هوشمند و هم در زمینهٔ کار خود کارکشته اند و مهم تر این که یا ریاضی دان اند و یا از ریاضی دانان کمک می گیرند. پیش تر، ریاضی دانان برای رمزگشایی پیام هایی که بر پایهٔ جابه جایی های گوناگون حرف ها به رمز درآمده بودند با

به کارگیری ویژگی ها و قانون های آمار و احتمال، روش هایی ارایه داده بودند که بدون در دست داشتن کلید رمز هم می شد پیام را رمزگشایی کرد. برای رمزنگاری هم ریاضی دانان روش هایی را به دست داده بودند که بدون آگاهی بر کلید رمز نمی شد رمزگشایی کرد. اما مسأله ای که مطرح بود این بود که اگر حریفان، هم به پیام رمزی و هم به کلید رمز دست یابند چه شگردی باید به کار برده شده باشد تا آنان توانایی رمزگشایی را نداشته باشند؟ در سال ۱۹۷۷، دو تن از ریاضی دانان *انستیتوتکنولوژی ماساچوست* راه حلی را برای این مسأله به دست دادند. آنان برای رمزنگاری، فرآیندی عددی و بر پایهٔ تجزیهٔ عددهای بزرگ را به دست دادند که رمزگشایی آن عملاً بسیار دشوار و وقت گیر است. این شیوهٔ رمزنگاری به نام RSA (= حرف های اول نام های دو ریاضی دان) شناخته می شود و امروزه در بیش تر کشورها به کار می رود.

یک عدد طبیعی را اول می نامند هرگاه مگر بر یک و بر خودش، بر عدد دیگر بخش پذیر نباشد. دو عدد اول را هرچند هم بزرگ باشند با کمک رایانه ها به سادگی می توان درهم ضرب کرد. اما تجزیهٔ یک عدد بزرگ، یعنی معلوم کردن این که حاصل ضرب کدام عددهای اول است، کار دشوار و در موردهایی برای ریاضی دانان، یک زورآزمایی و مبارز طلبی بوده است و می باشد.

در شیوهٔ رمزنگاری RSA، رمزنگار، دو عدد اول بزرگ را برمی گزیند و حاصل ضرب آن ها را کلید رمز می گیرد، با به کار بردن دو هم نهشتی که پیمانهٔ یکی از آن ها در ارتباط با دو عدد اول انتخابی به دست می آید و پیمانهٔ دیگری همان کلید رمز است، شماره های حرف های متن پیام را به عددهایی جدید تبدیل می کند و با آن ها پیام را به رمز درمی آورد. متن این پیام رمزی همراه با کلید رمز را برای گیرندهٔ پیام می فرستد. حال اگر حریف به این پیام رمزی و به کلید رمز دست یابد تنها آن گاه می تواند رمز گشایی کند که عدد کلید رمز را به ضرب عامل های اول تجزیه کند و این کار به سادگی عملی نیست. یک بار که بنا بود ریاضی دان ها عددی صدرقمی را تجزیه کنند، با روش برنامه نویسی موازی و تقسیم کار بین ۴۰۰ کامپیوتر غول آسا در آمریکا و اروپا و استرالیا و ۸۰۰۰ ساعت محاسبه های این کامپیوترها، ۲۶ روز طول کشید تا توانستند دریابند که آن عدد حاصل ضرب دو عدد اول ۶۰رقمی و ۴۱ رقمی است.

امروزه نه تنها در زمینه های علمی بلکه در امور اقتصادی، اداری، امنیتی، اطلاعاتی و ضد اطلاعاتی و در کشورداری و در جنگ ها و ستیزها، گره هایی پیش می آید که گشایش آن ها موکول به همکاری ریاضی دانان و به کارگیری ریاضیات است.

در پایان نوشتار، یکی از پیام های رمزی جنگ هشت سالهٔ تحمیلی ارایه می شود:

اغع یوشغ نتیچم

که به رمز درآمدهٔ

پیش به سوی کربلا

بوده است. خوانندهٔ نوشتار می تواند معلوم کند که این رمزنگاری به چه روشی انجام گرفته است.

زیرنویس

* آقای عبدالحسین مصحفی، مؤسس و سردبیر مجلهٔ یکان بودند که از سال ۱۳۴۲ تا سال ۱۳۵۵، منتشر شد. **یکان**، خدمت بزرگی به ریاضی مدرسه ای در ایران کرد و نامی آشنا، برای تمام ریاضی دوستان ایران است.

منابع

۱ـ **اسرار قاسمی**، ملاحسین کاشفی.
۲ـ **خزائن العلوم**، ملا احمد نراقی.
۳ـ دربارهٔ رمزنویسی، **اطلاعات هفتگی**، دی ۱۳۶۱.
۴ـ رمزنویسی، عبدالحسین مصحفی، **دانشمند** ۳۰۵.
۵ـ علم حساب و اسرار دولت ها، ترجمهٔ عبدالحسین مصحفی، **دانشمند** ۳۰۶.
۶ـ الفبای دو نشانه ای، عبدالحسین مصحفی، **دانشمند** ۳۴۷.
۷ـ **آشنایی با رمزگشایی**، دکتر محمودیان و درودیان.