نخ‌نما

گاه‌نامه‌ی جمع علمی - ترویجی رستا
شماره‌ی شش
سال دوم
تیر ۱۴۰۰

مکبدغ
مردی سگی را گاز گرفت
سفر در زمان

عکس از سید محمدسینا رضوی

شماره‌ی شش
سال دوم
تیر ۱۴۰۰
۳۰ صفحه

گاه‌نامه‌ی جمع علمی - ترویجی رستا، نیم‌خط

صاحب امتیاز: جمع علمی - ترویجی رستا
سردبیر: آیلا تیموری
مدیر مسئول: سینا ریسمانچیان

باحضور


سید سروش رضوی


سید محمدسینا رضوی


سیده فاطمه احمدزاده


آیلا تیموری


حنا جمالی


نونا رجبی


امیرمسعود جعفرپیشه


پارمیدا جوادیان


هلیا طارمی


هانیه هاشمی


ساجده رفیعی


زهرا سادات بحرینی


عرفان فرهادی


سید علیرضا هاشمی


فرناز کریمی


شکیبا جوانمردی


رضا ابوالقاسمی

هیئت تحریریه: سید محمدسینا رضوی، سیده فاطمه احمدزاده، شکیبا جوانمردی، آیلا تیموری

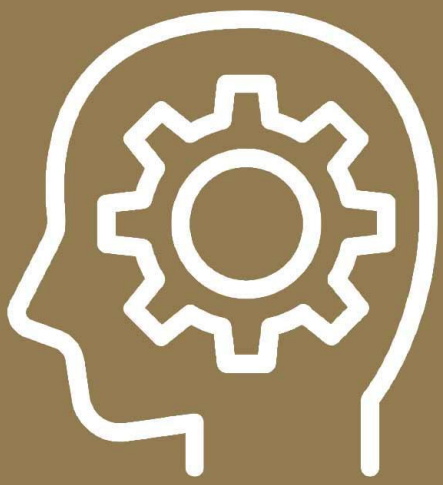
نویسندگان: سید سروش رضوی، عرفان فرهادی، سید علیرضا هاشمی، حنا جمالی، امیرمسعود جعفرپیشه، فرناز کریمی، رضا ابوالقاسمی

ویراستاران: نونا رجبی، ساجده رفیعی، هلیا طارمی، پارمیدا جوادیان

صفحه آرایان: هانیه هاشمی، زهرا سادات بحرینی، بهار بهادران، سید محمدسینا رضوی

با تشکر از: مهربان رضوانی، مریم امام‌جمعه‌زاده، نرگس کاظم‌پور

فهرست



به نام آن که جان را فکرت آموخت چراغ دل به نور جان برافروخت

شیخ محمود شبستری

سرمقاله

آیلا تیموری

سلام

امیدواریم تو این روزای گرم و شبای بی‌برق تابستون، درخشش چشماتون خیره‌کننده باشه که دل ما با برق نگاه شما روشنه!

همون‌طور که شما دوستان رستا می‌دونید، این جمع همیشه سعی داشته به کمک عینک خاصی که در اختیارش بوده با دید متفاوتی به زیبایی‌هایی که اطرافش وجود داره نگاه کنه و این نگاه رو با مخاطبان کنجکاو و خلّاقش به اشتراک بذاره! یکی از لنزهای گوناگون رستا، گاه‌نامه‌ی نیم‌خطه که تلاش می‌کنه گوشه‌ای از افق رنگارنگ دانش و فرهنگ و شناخت رو برای خوانندگانش نمایان کنه...

تو این شماره مثل همیشه با این عینک، به تماشای نمایشی از فیزیک و علوم کامپیوتر خواهیم نشست، سری به دنیای رمزنگاری و اطلاعات خواهیم زد و با هم‌دیگه با چالش‌های سفر در زمان روبرو خواهیم شد! یه معرفی کتاب ویژه هم برای نوکنکوری‌ها آوردیم. هم‌چنین اگه کنجکاوید ادامه‌ی داستان مرموز «من و مریم» و ماجرای مهسا با تخیل عجیبش رو بدونید، خبر خوشی براتون داریم.

اگه دوست دارید که با هم‌دیگه سفر کوتاهی به دنیای کلمات داشته باشیم، همین الآن لنز عینک‌هاتون رو عوض کنید و ورق بزنید...

امیدواریم از این شماره لذت ببرید :)

نوشته‌ها

نفسی
بیا
و
بنشین
سخنی
بگوی
و
بشنو

کتاب «هرکسی می‌تواند آشپزی کند»

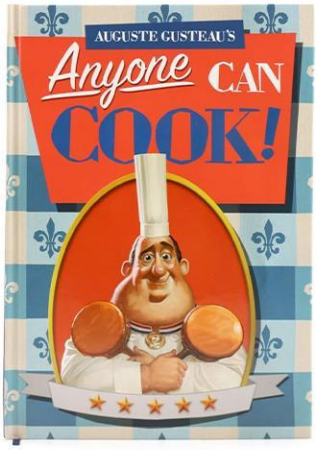
راهنمای زندگی پس از کنکور

سید سروش رضوی

«چیزی که درسته اینه: هرکسی می‌تونه آشپزی کنه، ولی فقط اون‌هایی که شجاعن می‌تونن فوق‌العاده باشن.»

انیمیشن «Ratatouille» با معرفی سرآشپز معروف، *آگوستو گوستو* شروع می‌شه. سرآشپزی که نه تنها به خاطر رستوران معروفش، که توسط کتاب آموزش آشپزیش به شهرت رسیده؛ کتاب «همه می‌توانند آشپزی کنند». ادامه‌ی داستان این انیمیشن بر اساس همین اعتقاد سرآشپز گوستو که هرکسی می‌تونه یه آشپز بزرگ بشه، پیش می‌ره. موشی که می‌خواد سرآشپز بزرگی بشه اما طبیعتاً کسی انتظارش رو نداره که بتونه و پسر خود سرآشپز گوستو که همه انتظار دارن مثل پدرش سرآشپز بزرگی باشه اما برای اون کار مناسب نیست.

چند سال پیش که می‌خواستم برای یک کلاس پر از دانشجوهای ترم یک دانشگاه درباره‌ی ۵-۴ سال پیش‌روشون صحبت کنم، متوجه شباهت عجیب کنکور و داستان انیمیشن موش سرآشپز شدم. توی اون کلاس، حدود ۴۰ جفت چشم به من خیره شده بودن که به تازگی یه عدد -رتبه‌ی کنکور- رو از سایت سنجش دیده بودن و قرار بود بفهمن در سال‌های آینده‌ی زندگیشون -زندگی پس از کنکور- چی به سرشون می‌آد. در اون لحظات کشف کردم که کتاب معروف سرآشپز گوستوی داستان موش سرآشپز، نه تنها برای آموزش آشپزی به درد یک موش می‌خوره، که راهنمای زندگی بعد از کنکور هم هست.



اگر دقیق‌تر نگاه کنیم، زندگی بی‌شباهت به شغل آشپزی نیست. انتخاب‌ها، علایق، آدم‌ها، تلاش‌ها و... چیزهایی هستن که طعم زندگی هرکسی رو مشخص می‌کنن. کنکور یکی از مهم‌ترین اتفاقاتیه که می‌تونه طعم زندگی بعد از خودش رو خوب یا بد کنه. اگه شما هم جزو آدم‌هایی هستین که بیشتر از یک ماه از روز کنکورتون می‌گذره، احتمالاً بعضی روزها -توی اون روزهای ایده‌آل بعد از کنکور که وعده‌ش رو بهتون داده بودن- به این فکر می‌کنید که از روزی که نتایج کنکور می‌آد، قراره زندگی‌تون چه طعمی باشه. اما سرآشپز گوستو معتقده یه آشپز خوب لازمه خلاق باشه و این‌قدر شجاعت داشته باشه که توی غذا پختن، چیزهایی رو انتخاب کنه که از قبل مطمئن نیست قراره طعم غذا رو خوب کنن. چشم‌هایی که به این متن دوخته شدن، حدود سه ماه بعد از دیدن دفترچه سوالات کنکور قراره به صفحه‌ی مانیتور و عددی خیره بشن که رتبه‌ی کنکور رو نشون می‌ده و در اون لحظه صاحب اون چشم‌ها حس می‌کنه که طعم زندگیش قراره خوب بشه یا بد. اما این هم فقط یه ادویه‌ست؛ یه ادویه که توسط سرآشپز یه زندگی انتخاب شده. آشپزی که اگه شجاعت انتخاب‌های بد و درست کردنشون رو نداشته باشه، هیچ‌وقت نمی‌تونه غذاهای خوش‌مزه درست کنه.

شاید
بتونیم با این مقدمه‌ی طولانی، دوران
بعد از کنکور رو دوران یادگرفتن آشپزی بدونیم. وقتی
که کنکور-به‌عنوان یک ادویه- طعم زندگیمون رو خوب یا بد
کرده، بدونیم که این فقط اولین انتخاب ما به‌عنوان سرآشپز
زندگیمون بوده. اما در واقع آشپزی از اون‌جایی شروع می‌شه که سعی
می‌کنیم غذایی با طعم خاص خودمون درست کنیم. اگه می‌خوایم طبق
دستورالعمل سرآشپز گوستو برای آشپزی عمل کنیم، باید به این فکر کنیم که از این
به بعد چه ادویه‌هایی می‌تونه طعم زندگیمون رو خوب و خاص خودمون کنه. اما
مهم‌ترین نکته‌ی کتاب سرآشپز گوستو اینه که مهم نیست چقدر ادویه‌هایی که توی
آشپزخونه‌تون دارین فوق‌العاده و باکیفیتن یا ساده و معمولی؛ کسی که آشپزی بلد نیست
می‌تونه همه‌ی اون‌ها رو توی غذای اشتباهی استفاده کنه. کتاب «همه می‌توانند آشپزی کنند»
نه فقط راهنمای زندگی پس از کنکور برای افرادی با رتبه‌های معمولی و نه‌چندان خوب، که
برای آدم‌هایی با رتبه‌های خوب و بسیار خوب هم هست. افرادی که شاید یه ادویه‌ی خوب توی
غذای زندگیشون داشته باشن اما در صورتی که آشپزی رو یاد نگیرن، قراره به‌زودی غذاهای خیلی
معمولی بپزن.
در قسمتی از فیلم، پدر رمی(موش سرآشپز) اون رو به دیدن مغازه‌ی فروش تله و مرگ‌موش
می‌بره تا بهش نشون بده، انتخاب‌هاش در زندگی قراره به مرگش منتهی شه. پدر رمی بهش
می‌گه تو طبیعتت -موش بودنت- رو نمی‌تونی عوض کنی. اما شاید جوابی که رمی به پدرش
می‌ده، شروع سرآشپز شدنشه؛ یه سرآشپز واقعی، اون‌طوری که آگوستو گوستو بهش باور
داشته. سرآشپزی که مهم نیست کیه و چه امکاناتی داره؛ همیشه می‌خواد و می‌تونه
غذای خوب بپزه.
«طبیعت، تغییر کردنه پدر. همون قسمتی که می‌تونیم روش تاثیر بذاریم و
تغییر وقتی شروع می‌شه که تصمیم بگیریم.»

"Change is nature, Dad. The part that we can influence. And it starts when we decide."

من و مریم

عرفان فرهادی

همان‌طور که می‌دانید مهسا و آیدا دو دوست قدیمی هستند که با هم المپیاد ریاضی می‌خوانند. مهسا در روز تولدش می‌فهمد که به نظر همه شبیه مریم میرزاخانی است. شیوع کرونا باعث می‌شود در دل تنهایی قرنطینه، این شباهت ظاهری تبدیل به یک خیال‌پردازی بزرگ در ذهن مهسا شود؛ این اصرار و نیاز به تأیید با یک ملاقات حضوری که با ابتلای خانواده‌ی آیدا به کرونا همراه می‌شود دوستی این دو نفر را دچار چالشی جدی می‌کند. مهسا خود نیز حال مساعدی ندارد؛ تست کرونا می‌دهد غرق در کابوس‌هایی‌ست که در آن‌ها خود را به جای مریم میرزاخانی می‌بیند.

«در دنیا چه چیزی از بلاک‌شدن توسط صمیمی‌ترین دوستت بدتر است؟»

این پرسشی بود که مهسا از خودش در بستر بیماری می‌پرسید. آفتاب به قدری بالا آمده بود که از پنجره‌ی باز اتاق بگذرد و روی صورتش بیفتد اما او توانِ برخاستن و بستن پنجره یا کشیدن پرده را نداشت. شاید هم اصلاً میلی به این کار نداشت. از دو روز پیش که تست داده بود تا همین لحظه، کمتر از یک‌ساعت ایستاده یا نشسته بود. در اتاق را بسته بود و تنها ارتباطش با دنیای خارج از زیر یا کنار در بود. مهسا واقعا تلاش می‌کرد اتفاقات را مرور کند؛ بالاخره دوران نقاهت بیماری معمولاً زمان تسویه‌حساب‌های شخصی با خود است اما تب و سردرد در بیداری و کابوس‌ها در خواب، هر رشته‌ی فکری را پاره می‌کردند و ضمناً که مهسا تنها بود! انگار ذهنش از اتفاقات روزهای گذشته خالیِ خالی بود. خبری از مریم هم نبود تا با او جروبحث کند. حداقل هنوز.

+ مهسا وقت داروئه!

- بذارش همون پشت در، می‌آم برمی‌دارم.

+ این دارو گیاهیه که خالت گفته رو درست کردم. جوشیدنیه باید تا ته‌نشین نشده سریع بخوری.

- مامان گفتم بذارش دم در می‌آم برمی‌دارم دیگه!

به سختی سر جایش نشست و دنبال ماسک و عینکش گشت. صدای باز و بسته شدن در آمد. مهسا سرش را به طرف دیوار برد و بلند و با پرخاش گفت:

- مامان مگه نگفتم بذار دم درا! من ماسک نزدم وامی‌گیری ازم! حواست نیست؟

پاسخی نشنید. سرش را برگرداند. مریم با لباس سفید پرستاری و لیوانی در دست لبخندزنان رو به او ایستاده بود. مهسا متعجب فریاد زد:

- چی می‌خوای از جونم؟!

+ علیک‌سلام مهسا خانوم.

- سلام. چی می‌خوای از جونم؟!

+ مگه جونی برات مونده با این همه حرصی که می‌خوری؟! من اومدم حالت رو خوب کنم بابا!

- از وقتی سروکله‌ی تو پیدا شده همه‌چیز به هم ریخته؛ دوستم بلاکم کرده، نمی‌دونم اصلاً کجاست، چی کار می‌کنه، خودم هم که این‌جور! به این روز افتادم.

در همین حین، مامان، باز مهسا را صدا زد.

+ مهسا این سرد شد. بیا برش دار دیگه!

مهسا فریاد زد:

- به درک! به درک! به درک! ولم کنین!

+ باشه خب حالا...

مریم با طعنه به مهسا نگاه کرد و گفت:

+ این هم من بودم. مگه نه؟!

مهسا با سرافکندگی جواب داد.

- ولی من نمی‌خوام این‌طوری باشم.

+ می‌خوای! اگه نه که من این‌جا نبودم!

- تو هم نمی‌خوام دور و برم باشی!

+ واقعا نمی‌خوای؟! پس چرا این چند روز هر کاری می‌کردی که برگردم؟!

مهسا سکوت کرده بود.

+ من دیگه هستم مهسا جون! این یه چیز اثبات‌شده است!

مهسا صورتش را در دست‌هایش گرفته بود.

+ پاشو بیا این استامینوفن رو بخور اقلاً جون بگیری. چرا انقدر آخه خودت رو اذیت می‌کنی؟ مگه تقصیر تو بوده؟!

- آره بوده! یعنی نه... نمی‌دونم... ولی بود. تقصیر من بود! اگه بلایی سرشون بیاد چی؟! وای...

+ باشه حالا آروم باش! فعلا بپا بلایی سر خودت نیاری.

مریم دست مهسا را گرفت و به سختی او را بلند کرد. از روی میز قرصی از بسته جدا کرد و با لیوان آب به مهسا داد. نگاه مهسا از پنجره به ساختمان روبه‌رویی بود. پرده‌های اتاق آیدا کشیده بود و چیزی پیدا نبود. مریم به آرامی با آرنج به پهلوی او زد و به لیوان اشاره کرد.

+ بابا بخور دیگه این‌قدر که ناز نداره!

- نمی‌خوام! اصلاً ولش کن! بذار از کرونا همین‌طوری بمیرم.

لیوان را روی میز گذاشت و دوباره روی تخت و زیر چند لایه پتو خزید. زیر دست‌وپا و پتوها دنبال گوشی گشت تا دوباره به آیدا زنگ بزند. مریم به طرف او دوید تا گوشی را از او بگیرد.

+ لازم نکرده. فایده‌ای هم نداره جواب نمی‌ده که!

زنگ تلفن خانه بلند شد و سر هر دو نفر به طرف در چرخید. صدای پای صدرا را شنیدند که به طرف تلفن می‌دوید.

+ بله؟! بله هستش.

صدای پا به سمت در اتاق آمد. صدرا تلفن بی‌سیم را از زیر در رد کرد.

+ اگه سر من هم مثل مامان داد نمی‌کشی تلفن باهات کار داره.
مریم خم شد و تلفن بی‌سیم را برداشت و دکمه‌ی اسپیکر را فشار داد بی‌خبر از آن‌که آن‌چه پرستار خانه‌ی بهداشت محله در ۴۰ ثانیه‌ی بعد به زبان می‌آورد مهسا را به نقطه‌ای بی‌بازگشت می‌رساند.
+ خانم میرزایی؟
- بله بفرمایید؟!
+ شما پریروز این‌جا تست کرونا دادید دیگه؟ درسته؟!
- بله. پریروز. یه‌شنبه بود فکر کنم.
+ علائمی داشتید از اون روز؟ آب‌ریزش بینی؟ سرفه؟ تب‌ولرز؟
- سرفه نه. فقط تب و سردرد...
+ خب گوش کن خانمم. شما تستت منفی شده. احتمالاً زیر پنکه‌ای چیزی خوابیده بودی چاییدی. حالا باز هم سعی کن که...
مهسا دیگر نمی‌شنید. مریم گوشی را قطع کرد. چشم در چشم مهسا زل زده بود.
+ پس که من مقصرم؟ پس که ما مقصریم؟ بله؟! که یه کاری کردیم همه‌شون کرونا بگیرن؟!
کمی طول کشید تا بهت مهسا هم به خشم تبدیل شود. در همین فاصله‌ی کوتاه که صدرا و مامان از تلفن اصلی خانه متوجه شوند و در اتاق را باز کنند تا مهسا را در آغوش بگیرند، او پاسخ سوالش را یافت.
«بدتر از بلاک‌شدن توسط صمیمی‌ترین دوستت، بلاک‌شدن به «ناحق» توسط بهترین دوستت است.»
مهسا در آغوش خانواده به مریم نگاه می‌کرد که با اجازه‌ی او پنجره‌ی اتاق را می‌بست، پرده را می‌کشید و شماره‌ای را برای همیشه از روی گوشی‌اش پاک می‌کرد.

****

+ به‌نام‌خدای بخشنده‌ی مهربان. امتحان انشای پایان‌ترم. صدرا میرزایی کلاس هفتم ب. «ما و کرونا». کشور ما از اوایل اسفندماه سال گذشته درگیر بیماری کرونا شده است. کرونا یک بیماری ویروسی است که...»
فصل امتحانات در خانه‌ی میرزایی‌ها شروع شده است. مادر خانه مشغول سروکله‌زدن با برگه‌های امتحانی اسکن‌شده‌ای است که در واتسپ برایش ارسال کرده‌اند و نابلدی در زوم‌کردن روی عکس‌ها، خواندن آن‌ها را برایش عذاب‌آور کرده است. مهسای خواب‌آلود، در اتاقش، با تمام سرعت مشغول فشار دادن دکمه‌های کنترل و f به صورت همزمان روی لپ‌تاپ است تا پاسخ‌های امتحان دین‌وزندگی را در سایت امتحانات مدرسه وارد کند و صدرا هم از انشایی که نوشته ویس می‌گیرد تا در گروه کلاسشان بفرستد.
+ در خانواده‌ی ما خوش‌بختانه کسی به این بیماری مبتلا نشده است و با این‌که خواهرم، مهسا، علائم بیماری را داشت اما تست او مثبت نشد.
شاخک‌های مهسا حتی همین حین امتحان هم به شنیدن اسمش حساس بود.
+ سال گذشته در کتاب علوم تجربی درباره‌ی بهداشت روان مطالبی را مطالعه کردیم. بیماری کرونا نیز به جز بهداشت جسمی بر روی بهداشت روانی ما تأثیر می‌گذارد. به نظر من خواهرم با این که درگیر بیماری جسمی کرونا نشده بود اما حتماً به کرونای روانی مبتلا شده است که مدام در اتاقش با خودش صحبت می‌کند و به جای شب‌ها، روزها تا سر ظهر می‌خوابد.
مهسا با عصبانیت از اتاق بیرون زد.
- مامان! ببین صدرا چی می‌گه!
+ عههههه! مگه نگفتم دارم به معلمم ویس می‌دم حرف نزنین!
- خب آخه این چه انشاییه نوشتی؟
+ مگه دروغ می‌گم؟ خب با خودش حرف می‌زنه!
- روانی خودتیا!
مهسا به سمت صدرا جهید و گوش او را گرفت.
+ آخ آخ آخ. ول کن.
- نمی‌کنم.
صدرا هم دست دراز کرد تا در تلافی موهای مهسا را بکشد؛ به قدری بلند شده بودند که در دست بیایند. داد مهسا هم بلند شد.
+ ول کن تا ول کنم. ول کن تا ول کنم!
دعواهای خواهر و برادری همیشه شیرینی خود را دارند؛ البته نه برای والدین. مامان بچه‌ها را جدا کرد.
+ بسه دیگه. مگه الان جفتتون امتحان ندارین. برین سر امتحانتون.
- تا پاک نکنه نمی‌رم!
+ پاکش کن صدرا. خواهرت یه کم فقط اضطراب امتحانش رو داره. همین.
با وساطت مامان مهسا به اتاق برگشت. در مدت زمانی که صدرا انشایش را بازنویسی و دوباره ضبط می‌کرد مهسا سوالات را با سرعت پاسخ داد و شروع به لباس پوشیدن کرد.
+ بیماری کرونا نیز به جز بهداشت جسمی بر روی بهداشت روانی ما تأثیر می‌گذارد. یکی از دوستان خواهرم با این‌که درگیر بیماری جسمی کرونا نشده است اما مدام در اتاقش با خودش صحبت می‌کند و به جای شب‌ها روزها تا سر ظهر می‌خوابد. من در اخبار تلویزیون دیدم که آمار دعواهای خانوادگی در دوران کرونا افزایش یافته است.
تلفن مهسا زنگ خورد. او ماسک پارچه‌ای صورتی رنگش را به صورت زد و به تلفن گفت:
- الان می‌آم پایین.
کوله‌اش را برداشت و از اتاق بیرون زد. مادرش با تعجب و صدای آهسته‌ای پرسید:
+ کجا؟
- گفتم بهت که دیروز! آقای احمدی گفت امروز بیاین پیشم مرحله دوی سال‌های قبل رو امتحان بدین.
صدرا همچنان در حال ضبط بود.
+ در نهایت به نظر من این بیماری لعنتی کرونا به‌جز مرگ‌ومیر باعث مشکلات روحی زیادی در جامعه شده است که دانشمندان باید برای آن‌ها نیز واکسنی تهیه کنند. پایان.
پیش از آن‌که صدرا ویس را ارسال کند یا مامان فرصت کند به طور دقیق‌تری از مهسا بپرسد «آخه کجا؟!» مهسا فریاد کشید:
- امضا، صدرا خله! امضا، صدرا خله!
و از در خانه بیرون جست. در آسانسور با مریم به شیطنتی که کرده بودند خندیدند و با حالی خوش سوار سمند سفیدرنگی شدند که انتظارش را می‌کشید.
اگر توقف کوتاهی که در مسیر داشتند را محاسبه کنیم، ۲۵ دقیقه بعد یعنی ساعت یازده و سه دقیقه، مهسا جلوی در دانشگاهی بود که فکر می‌کرد قرار است چند سال آینده از زندگی آینده‌اش را آن‌جا بگذراند.

از آن‌جا که ایستاده بود میدان آزادی پیدا بود. سرش را بلند کرد و به آجرهای نارنجی‌رنگی که همیشه تنها از کنارشان رد شده بود نگاه کرد. کمی آن‌طرف‌تر چهره‌ی جوانی روی دیوار بلند ساختمان بزرگی نقاشی شده بود و زیر آن نوشته بود «شهید مجید شریف واقفی».

مریم دست مهسا را گرفت و به سمت ورودی برد. از تونل باریک و کم‌عرض آبی‌رنگی رد شدند که در ثانیه‌ای، دوشی از مواد ضدعفونی روی آن‌ها پاشید. در حال عبور بود که ناگهان مردی از اتاقک نگهبانی زیر سردر خارج شد و با لهجه‌ی بامزه‌ی گیلکی گفت:

+ دانشگاه تعطیله خانوم‌جان! برگه‌ی تردد دارین یا کارت؟!

مهسا مدت کوتاهی با تعجب به مرد نگاه کرد و بعد آب‌دهانش را قورت داد و به مریم نگاه کرد. مریم دست در جیب مانتویش کرد و دستش را به طرف مرد دراز کرد. مرد کارت را از دست مهسا گرفت. مرد نگهبان لحظه‌ای با خودش فکر کرد نامی که بر این کارت پرس‌شده‌ی قدیمی می‌بیند چقدر آشناست. نگاهی به چهره‌ی مهسا کرد. مریم به سرعت عینکش را، که زیر آفتاب خردادماه مشکی و دودی شده بود، از صورت برداشت و مهسا هم کمی ماسک را پایین داد و لبخندی تصنعی زد. مرد بار دیگر به کارت نگاه کرد. با کمی مکث گفت:

+ خانوم میرزاخانی بفرمایید داخل. فقط این کارت‌های انجمن فارغ‌التحصیلان قدیمی رفته. اگه تشریف ببرید ساختمون جدید آموزش دانشگاه براتون عوضش می‌کنند. مستقیم برید اون جلو یه بریدگی هست اون‌جاست.

مریم تشکر کرد و عینک دودی را دوباره به چشم زد. مهسا کارت را پس گرفت و در زیپ نیم‌باز کوله‌اش انداخت. به سرعت مسیر مستقیم را پیش گرفتند و راه افتادند. هنوز با اضطراب و واهمه چند قدم دور نشده بودند که دیگر نتوانستند جلوی خنده‌یشان را بگیرند.

****

+ فقط این کارت‌های انجمن فارغ‌التحصیلان قدیمی شده.

مریم ادای مرد نگهبان را درمی‌آورد.

- دیگه هر چی نداشت این قرنطینه حداقل استادی فتوشاپ رو برای ما داشت.

مریم خندید.

- اصلا اگه مرحله دو قبول نشدم می‌رم تو یکی از همین تایپ‌وتکثیری‌ها کار می‌کنم. چه‌طوره؟

مریم چیزی نگفت.

- بعدش هم کم‌کم می‌زنم تو خط جعل سند و این‌ها. چه‌طوره؟ مدرک زبان، پاسپورت، حتی پول!

+ چرت نگو انقدر مهسا.

- جدی می‌گم! مثل این زنه هست تو مانی‌هایست! نایروبی!

+ دوباره دیشب نشستی پای این؟

- مگه مامانمی انقدر سخت می‌گیری بهم؟ بی‌خیال مریم خانوم من که دیگه دارم باهات راه میام! ندیدی مرده فرقمون رو نفهمید؟ بخند خوشگله. او بلا چاو، بلا چاو، بلا چاو چاو چاو...

مریم لبخندی زد.

- الان هم که دیگه اومدیم شریف! تهش همین‌جاست دیگه!

+ واقعا که نیومدی! دزدکی اومدی.

- حالا می‌آم دیگه بالاخره. من که خودم رو می‌شناسم.

+ با این وضع سریال و یوتیوب و فتوشاپ و ساعت ۴ صبح خوابیدن... شما سر همین امتحان امروز خوابت نبره؛ قبول شدن پیش‌کش‌ات!

- بابا گیر نده دیگه. می‌گم حساس شدی می‌گی نه. گوش صدرا رو هم الکی پیچوندی. گناه داشت بچه.

+ خیلی پررو تشریف داره! حقش بود!

- حالا بالاخره بود یا نبود.. هر چی اصلاً. بگو ببینم این دانشکده‌ی فخیمه‌ی ریاضی کجا تشریف دارند؟

مریم با انگشت ساختمانی دو سه طبقه را نشان داد. مهسا راه افتاد و از میان چمن‌های نسبتا بلند عبور کرد و به دو در شیشه‌ای رسید. پرسید:

- سمت چپ یا راست؟

پاسخی نشنید. مریم کنارش نبود. برگشت و پشت سرش را نگاه کرد. مریم روبروی مجسمه‌ای سنگی ایستاده بود. زیر مجسمه نوشته بود «یادبود کشته‌شدگان حادثه‌ی سقوط اتوبوس دانشجویان ریاضی - اسفند ۷۶». مهسا مریم را صدا زد.

- چیزی شده؟!

مریم سر برگرداند.

+ نه چیزی نیست. سمت راست.

عکس از سید محمدسینا رضوی

سید علیرضا هاشمی

مَکبِدغ ۳

کشور افتاده در دد لاک را نجات دهید!

مکبدغ چیست؟

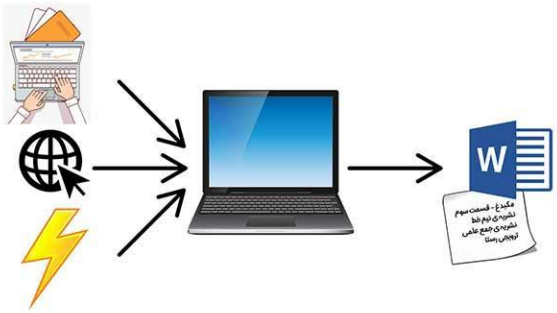
اگر حال ندارید تا شماره‌ی اول بروید و ببینید مکبدغ چیست، همین‌جا می‌گویم که این کلمه، سرآیندِ «مفاهیم کامپیوتری برای دنیای غیرکامپیوتری» است. در سری متن‌های مکبدغ به دنبال این هستیم که کمی، از دریچه‌ی کلمات کامپیوتری به دنیای اطرافمان نگاه کنیم.

آنچه گذشت

در قسمت دوم از مکبدغ، در مورد «تابع» که یک مفهوم کامپیوتری است، حرف زدیم و گفتیم تابع، چیزی‌ست که یک سری ورودی می‌گیرد، یک سری پردازش رویشان انجام می‌دهد و یک خروجی تحویلمان می‌دهد. هم‌چنین در شماره‌ی قبل ادعای بزرگی کردیم و گفتیم انگار می‌شود به هر پدیده‌ای به چشم تابع نگاه کرد. یک سری مثال هم زدیم از درخت و مغز و کامپیوتر که همه‌شان یک‌جورهایی تابع‌اند!

ادعای بزرگ

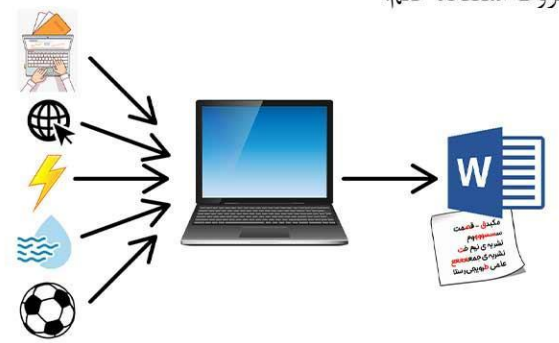
در این شماره می‌خواهیم در مورد آن ادعای بزرگ حرف بزنیم و برایش دلیل و مدرک بیاوریم. اول‌ازهمه، گفتیم که هر تابع، یک سری ورودی می‌گیرد؛ مثلاً همین لپ‌تاپی که دارم با آن این متن را تایپ می‌کنم، برق، اینترنت و فشار انگشتان من را ورودی می‌گیرد، cpu و ram و سایر اجزای داخلی‌اش یک سری کار را این ورودی‌ها انجام می‌دهند و در نهایت پس از طی شدن عملیات‌های مختلف، متن من تایپ و ذخیره می‌شود.



آیا به نظرتان لپ‌تاپ من فقط همین سه مورد (برق، اینترنت و فشار انگشتان) را ورودی می‌گیرد؟ چه می‌دانم، مثلاً آیا رطوبت اتاق تأثیری در متن من ندارد؟ به نظرتان اگه رطوبت اتاق خیلی‌خیلی زیاد باشد، مثلاً من رفته باشم در سونای بخار و این متن را تایپ کنم، آیا بازهم متن من تایپ می‌شود؟

جواب سؤال بالا مشخص است؛ احتمالاً در سونای بخار، این‌قدری هوا بد هست که قطعات داخل لپ‌تاپ من بسوزند و من دیگر نتوانم این متن را تایپ کنم. پس می‌بینیم که اگر رطوبت هوا تغییر پیدا کند، خروجی کار (متن من) هم عوض می‌شود.

خب تا حالا ۴ تا ورودی برای تابع لپ‌تاپ من پیدا شده. به نظرتان ورودی‌های دیگری وجود ندارند؟ تا حالا به «توپ فوتبال بچه‌ی همسایه» فکر کرده‌اید؟ آیا آن هم یک ورودی برای تابع لپ‌تاپ من محسوب می‌شود؟ اگر درحالی‌که من این متن را تایپ می‌کنم، بچه‌ی همسایه توپ فوتبالش را شوت کند و بزند پنجره‌ی اتاق من را بشکاند و توپ بیفتد روی صفحه‌کلید لپ‌تاپم، آیا بازهم همان متنی که الان داشتم تایپ می‌کردم، تایپ می‌شود؟ با افتادن توپ روی صفحه‌کلید لپ‌تاپم، احتمالاً یک سری حروف درهم‌برهم و اضافی تایپ می‌شوند که البته می‌توانم پاکشان کنم، ولی بازهم روی متن من تأثیر داشتند. اصلاً این هم ممکن است که وقتی توپ فوتبال بچه‌ی همسایه افتاد روی صفحه‌کلید لپ‌تاپم، بزند و تعدادی از دکمه‌های صفحه‌کلید را خراب کند و دیگر نتوانم در متنم از بعضی حروف استفاده کنم.



جالب است‌ها! انگار همین لپ‌تاپی که به چشم تابع به آن نگاه می‌کردیم و متن من را خروجی داده، ورودی‌های زیادی داشته که اصلاً حواسمان به آن‌ها نبوده.

بگذارید یک مثال دیگر هم بزنم: فرض کنید رفته‌اید سر جلسه‌ی کنکور. شما در آن لحظه یک تابع هستید؛ تابعی که پارامترهای میزان درس خوانده‌شده، میزان استرس و خیلی چیزهای دیگر را ورودی می‌گیرد و در پایان، رتبه‌ی کنکور شما را خروجی می‌دهد.
همان‌طور که در مثال لپ‌تاپ هم دیدیم، تابع شما سر جلسه‌ی کنکور ورودی‌های زیادی داشته که اصلاً به آن‌ها فکر هم نکرده‌اید؛ مثلاً پارامتر «نشستی سقف اتاق»! از کجا معلوم که دقیقاً سقف بالای سر شما زمان کنکور نشتی نداشته باشد و آب از آن نچکد و نریزد روی پاسخ‌نامه‌تان و خرابش نکند؟ یک عامل دیگر هم هست به نام «مراقبین حرّاف»! از کجا معلوم سر جلسه‌ی کنکور دو تا مراقب که انگار شونصد سال است همدیگر را ندیده‌اند، کنار دست شما نیفتند و در مورد خاطرات کودکی‌شان تا عروسی فلانی، باهم حرف نزنند؟ می‌بینید؟ بازهم یک سری ورودی هست که کمتر به آن‌ها توجه کرده بودیم.

برگردیم سر ادعای بزرگمان. من هنوز هم می‌گویم به همه چیز می‌شود به چشم تابع نگاه کرد، ولی این دفعه این قید را هم می‌آورم که لزوماً همه‌ی ورودی‌های این تابع را نمی‌فهمم و نمی‌توانم کنترلشان کنم؛ مثلاً شما نمی‌توانید سر جلسه‌ی کنکور کاری کنید که سقف بالای سرتان یکهو نشتی نکند و آب نریزد روی برگه‌ی پاسخ‌نامه‌تان، یا مثلاً نمی‌توانید کاری کنید که توپ بچه‌ی همسایه یک‌دفعه پنجره‌ی اتاقتان را نشکاند و صاف نخورد وسط لپ‌تاپتان!

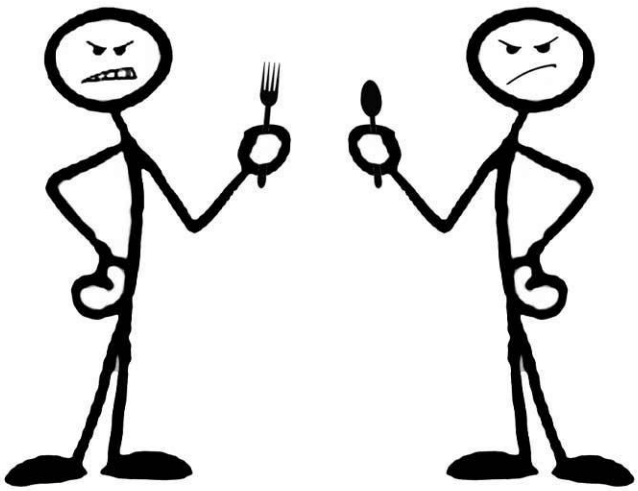
توکل

احتمالاً واژه‌ی «توکل» به گوشتان خورده. به نظرم آمد این‌جا بهتر از هرجای دیگری می‌شود در مورد توکل صحبت کرد. وقتی شما تابعی دارید که یک سری از ورودی‌هایش دست شماست و می‌توانید کنترلشان کنید و از آن طرف یک سری ورودی دارد که تحت کنترل شما نیست، برای عملکرد درست تابعتان چاره‌ای جز «توکل‌کردن» ندارید! توکل یعنی همان ورودی‌هایی از تابع را که دست خودتان است، درست فراهم کنید و بقیه‌ی ورودی‌ها را بسپارید به خدا که اگر صلاح دید، برایتان فراهمش کند تا تابعتان درست کار کند.

هیچ موقع فکر می‌کردید «تابع» و «توکل» به هم ربط داشته باشند؟

دِدلاک

بعد از مفهوم تابع، به سراغ مفهوم دیگری در دنیای کامپیوتر به نام ددلاک «DeadLock» می‌رویم که ترجمه‌شده‌اش می‌شود «قفل مرگ»! بگذارید این مفهوم را با یک مثال توضیح دهم:
علی و محمد دوتا دوست هستند که می‌خواهند باهم ناهار بخورند. هرکدام از آن‌ها غذای خودش را دارد، ولی متأسفانه برای خوردن غذاها روی‌هم ۱ قاشق و ۱ چنگال بیشتر ندارند. فرض کنید هر یک از این دو نفر وقتی می‌خواهد غذای خودش را بخورد، باید هم قاشق و هم چنگال داشته باشد (یعنی کارش با یک قاشق خالی یا یک چنگال خالی راه نمی‌افتد). اگر در همان لحظه که آن‌ها شروع به غذا خوردن می‌کنند، علی قاشق را و محمد چنگال را بردارد، قبول دارید که هیچ‌کدامشان نمی‌توانند غذایشان را بخورند؟ چون هرکدامشان فقط یکی از ابزارهای لازم برای خوردن غذا را دارد و نمی‌تواند با همان ابزار غذایش را بخورد.



در مثال بالا، علی و محمد در «ددلاک» یا همان «قفل مرگ» گیر افتاده‌اند؛ می‌گویم قفل مرگ، چراکه علی و محمد در این وضعیت **قفل** شدند و اگر هیچ‌کدامشان هیچ اقدامی انجام ندهد (مثلاً از خودگذشتگی نکند و قاشق یا چنگالش را به نفر مقابل ندهد)، جفتشان از گرسنگی **خواهند مرد**! این مثال از مسئله‌ی معروف «غذا خوردن فیلسوفان» گرفته شده بود که می‌توانید از این‌جا بیشتر درموردش بخوانید.

قحطی در کامپیوتر

به نظرتان ددلاک کجای کامپیوتر اتفاق می‌افتد؟ نظری ندارید؟ طبیعی است. من هم خودم ترم ۵ دانشگاه با مفهوم ددلاک آشنا شدم، در درسی به نام سیستم‌های عامل. احتمالاً می‌دانید که همین لپ‌تاپ، کامپیوتر یا موبایلی که دارید از آن استفاده می‌کنید، رویش یک سیستم‌عامل نصب است. معمولاً سیستم عامل لپ‌تاپ‌ها و کامپیوترها ویندوز است و سیستم عامل گوشی‌ها اندروید. اگر خیلی پول‌دار باشید و ماشاءالله هزار ماشاءالله بزنم به تخته وضعتان خوب باشد، سیستم‌عامل لپ‌تاپتان مک و سیستم‌عامل موبایلتان ios است.

از دید سیستم‌عامل، ما یک سری «پردازه» و یک سری «منبع» داریم. کارهای مختلفی که در کامپیوتر یا موبایل انجام می‌شود، هرکدامش یک پردازه است؛ مثلاً همین‌الان اگر شما یک تب جدید در مرورگرتان باز کنید، پردازه‌ی جدیدی ایجاد کرده‌اید، یا مثلاً من که دارم این متن را تایپ می‌کنم، از ویرایشگری استفاده می‌کنم که آن هم یک پردازه است. اگه دوست داشتید، می‌توانید فهرستی از پردازه‌های در حال اجرا روی سیستم‌عامل ویندوز را با کمک این نوشته، مشاهده کنید.

از آن طرف، کامپیوتر یک سری منبع هم دارد؛ مثلاً CPU یک منبع است که محاسبات کامپیوتر را انجام می‌دهد یا RAM یک منبع برای ذخیره‌سازی اطلاعات است. ظرفیت CPU یا RAM محدود است و این‌طور نیست که CPU بتواند بی‌شمار عملیات محاسبه کند و یا مثلاً RAM بتواند بی‌نهایت اطلاعات در خودش ذخیره کند.

هر پردازه برای درست انجام شدن به یک سری منبع نیاز دارد؛ همان‌طور که علی و محمد برای غذا خوردن به قاشق و چنگال احتیاج داشتند. اگر جایی این پردازه‌ها نتوانند منابع موردنیاز خودشان را تأمین کنند و سر تأمین منابع باهم به مشکل بخورند، در ددلاک می‌افتند! شاید تا حالا برایتان پیش آمده باشد که وقتی شونصدتا برنامه‌ی مختلف را روی کامپیوتر خودتان اجرا می‌کنید، یک‌دفعه کامپیوترتان قفل کند. در این حالت کامپیوترتان در ددلاک افتاده و پردازه‌ها دربه‌در دنبال منبع می‌گردند تا کارشان را به سرانجام برسانند، ولی چون یک عالم پردازه دارید، منبع به پردازه‌ها نمی‌رسد و قحطیِ منبع رخ می‌دهد! تهش هم احتمالاً مجبور شده‌اید برای نجات از ددلاک، کامپیوتر را restart کنید.

کوچه تنگه؟

علاوه بر غذا خوردن علی و محمد و قفل‌کردن کامپیوترتان وقتی شونصدتا برنامه را باهم باز می‌کنید، مثال‌های دیگری از ددلاک مانند «رانندگان در کوچه‌ی تنگ» یا «کشور در حال پسرفت» هم وجود دارد. به نظرتان چه‌جوری یک کشور به آن بزرگی می‌تواند در ددلاک افتاده باشد؟ یا مثلاً ارتباط کوچه‌ی تنگ با ددلاک چه می‌تواند باشد؟

برای یافتن پاسخ این پرسش‌ها تا شماره‌ی بعدی مکبدغ منتظر باشید. ان‌شاءالله من نویسنده هم توی ددلاک نیفتم و بتوانم متن بعدی را بنویسم. :)

کلماتی از کمانچه

سیدمحمدسینا رضوی

برای گوش کردن به این موسیقی
تصویر سمت راست رو اسکن کن
یا **اینجا** کلیک کن!

قطعه‌ی **«محبوب من، مگذار من دل‌سرد شوم!»** ساخته‌ی *کالین* جیکوبسن و با اجرای *کیهان کلهر*(کمانچه) و بروکلین *رایدر*(ویولن)، آخرین قطعه از آلبوم «شهر خاموش» کیهان کلهر است. سازنده‌ی این قطعه، آن را با الهام از منظومه‌ی «لیلی و مجنون» نظامی گنجوی تنظیم کرده است. این قطعه، گویی شرح سیر رهرویی بی‌تاب، از ناتوانی و افتادگی تا برخاستن و به آرامش رسیدن است.

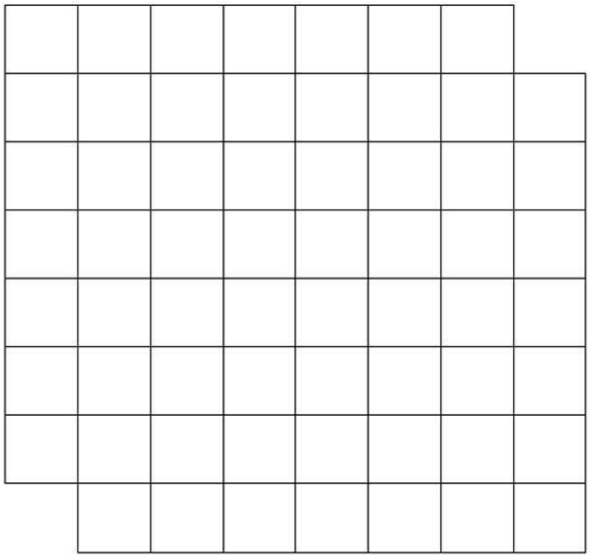
از [۰۰:۰۰]: رهرو گویی دل‌سرد است و دل‌سوخته و از به یادآوردن گذشته‌ی خود، خجل. با صدای ضعیفی می‌نالد و خود را بر زمینی بیابانی، نه در آرزوی آب، که در آرزوی سرابی می‌کشاند. در لحظاتی شجاعت‌های شکست‌خورده‌ی خود را در گذشته می‌ستاید اما دوباره فرو می‌افتد. پاهایش نای برخاستن را ندارند.
در اواسط قطعه، گویی می‌پذیرد که هرچند این سیل رنج، برگ‌هایش را با خود خواهد برد اما ریشه‌هایش را آبیاری خواهد کرد. تسلیم می‌شود و سوزن تیز رنج را این‌بار مشتاقانه به رگ‌هایش راه می‌دهد.
از [۰۵:۳۶]: درست در میانه‌ی راه، این سوزن به ناگاه خونی تازه را در رگ‌هایش جاری می‌کند؛ خونی از جنس امید. انگار دستی او را به برخاستن و حرکت فرا می‌خواند. به پا می‌خیزد و هر آن، صدای گام‌هایش بلندتر می‌شود؛ چنان‌که گویی هرگز زخمی نبوده است.
از [۰۷:۴۸]: ناگهان یادِ غم‌های گذشته، باز از سرعت گام‌های رهرو می‌کاهد. اما این‌بار، او در مسیر است؛ راه، پیش روی اوست و مقصد، روشن.
از [۰۸:۳۰]: نمی‌ایستد، غم را به کناری می‌نهد و همچنان به نواختن خود ادامه می‌دهد. این‌بار، با چشمانی بازتر، از بی‌پروایی قدم‌هایش می‌کاهد و سرانجام آرامشی را که در آرزوی آن بود، می‌یابد.
از [۰۹:۳۷]: در پایان، رهرو در آغوش آرامش ابدی خویش آرام می‌گیرد. نه‌با اندوه‌و اکراه، بلکه غرق‌در رضایت‌ویک‌رنگی.

نمایشی از موج صدای این قطعه

معما

حنا جمالی

چند سال پیش تو یه نمایشگاه دانش‌آموزی غرفه‌ای رو دیدیم که اگر تو یه بازی موفق می‌شدیم، برنده ۱ میلیون تومن می‌شدیم. بازی اینطوری بود: یه جدول ۸×۸ داشتیم که دو گوشه‌ی مقابلش حذف شده بود و باید با ۳۱ تا مستطیل دوتایی به‌هم‌چسبیده این جدول رو پر می‌کردیم. یه چیزی شبیه شکل زیر:



قبل از اینکه جواب رو بخونید بذارید بهتون بگم که اون بچه‌ها ریسکی رو قبول نکردن. مطمئن بودن که کسی نمی‌تونه اینکار رو بکنه! حالا سعی کنید خودتون بگید چرا.

صفحه ۸×۸ ما رو یاد صفحه‌ی شطرنج می‌ندازه. پس این صفحه رو شطرنجی رنگ می‌کنیم. دقت کنید که دو تا خونه‌ای که حذف شدن هم‌رنگن! و هر مستطیل ۲×۱ای که توی جدول قرار می‌دیم دو خونه مجاور که یکی سفیده و یکی سیاه رو می‌پوشونه. دو گوشه‌ای که از این جدول حذف شده‌ن هم‌رنگن. یعنی ابتدای بازی ما ۳۲ خونه سفید و ۳۰ خونه سیاه، یا ۳۰ خونه سفید و ۳۲ خونه سیاه داریم. به ازای هر مستطیلی که قرار داده می‌شه اختلاف خونه‌های سفید و سیاه باقی‌مونده ثابت می‌مونن. پس با این اوصاف چون در نهایت می‌خوایم که این اختلاف صفر باشه، هیچ‌وقت نمی‌تونیم جدول رو پر کنیم.

حالا بیاید رو یه سوال دیگه هم فکر کنیم تا بعد بریم سراغ یه ایده‌ی پرکاربرد تو حل معماها.
روی تخته اعداد ۱ تا ۲۵ نوشته شدن. هربار سه تا از اعداد رو تخته مثل a و b و c رو پاک می‌کنیم و به جاش عدد $a^3+b^3+c^3$ رو می‌نویسیم. ثابت کنید موقعی که فقط یه عدد روی تخته مونده اون عدد نمی‌تونه 2013^3 باشه. (راهنمایی: باقی‌مانده‌ی n و n^3 بر عدد سه با هم برابرن)

شباهت سوال اعداد با سوال جدول چیه؟ شاید فکر کنید هیچی. ولی در واقع تو حل جفتشون از یه روش استفاده می‌کنیم. یکی از روش‌های حل سوال اعداد اینه که بیایم باقی‌مانده‌ی مجموع اعداد روی تخته بر ۳ رو در نظر بگیریم. ابتدای کار داریم که ۱۳×۲۵ (مجموع اعداد روی تخته) که باقیمانده‌ش بر ۳ برابر ۱ هست. از طرفی باقیمانده‌ی هر عددی به توان سه بر سه با باقی‌مانده خود اون عدد بر ۳ برابره. پس با هر عملیاتی که انجام می‌شه باقی‌مانده‌ی مجموع اعدادی که روی تخته هست بر ۳ تغییری نمی‌کنه. و چون باقی‌مانده‌ی 2013^3 به ۳ برابر صفر هست هیچ‌وقت نمی‌تونیم اون رو داشته باشیم.

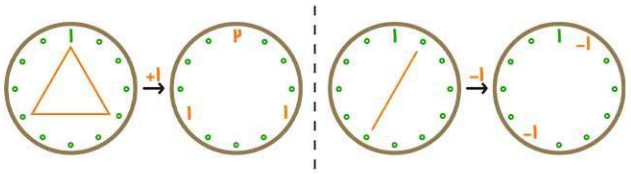
هر چیزی که که ثابت می‌مونه یک **ناوردا**ست. ایده‌ی حل جفت این سوال‌ها ناوردایی بود. یعنی ما یک ویژگی رو در نظر می‌گیریم که با هر عملیاتمون تغییری نکنه و بعد بررسی می‌کنیم که آیا در حالت ابتدایی و حالتی که می‌خوایم بهش برسیم یکسان هست یا نه. این ویژگی تو سوال اول اختلاف تعداد خونه‌های سفید و سیاهِ پوشانده نشده بود که تو حالت ابتدایی ۲ بود و ما می‌خواستیم به حالتی برسیم که این تعداد صفر باشه. تو سوال دوم هم ناوردای ما باقیمانده‌ی مجموع اعداد روی تخته بر سه بود. ناوردا هرچیزی می‌تونه باشه. از اختلاف و مجموع و ضرب اعداد مساله گرفته تا برآیند بردارها و صحیح یا گویا بودن مختصات...

حـالا سـعی کنیـد نـاوردای سـوال زیـر رو پیـدا کنیـد و حلش کنید.
منتظر جواب‌هاتون در @Rastaiha_info هستیم.

یـه صفحـه‌ی دایـره‌ای شـکل داریـم کـه ۱۲ تـا عـدد مثـل اعداد ساعت دورش نوشـتیم. از سـاعت ۱ تـا ۱۱ اعـداد صفـرن و عـدد نوشـته شـده روی سـاعت ۱۲ برابـر یکـه. در هر مرحلـه می‌تونیم یـک سـری از اعـداد روی دایـره رو انتخـاب کنیـم و از هرکـدوم یکـی کـم و یـا بـه هرکـدوم یکـی اضافـه کنیـم به طوری که:

- دو تـا عـددِ رو بـه روی هـم باشـن (مثـلا اعـداد نوشته شده تو ساعت ۶ و ۱۲).
- سـه تـا عـدد روی سـه راس یـک مثلـث متسـاوی‌الاضلاع باشن (مثلا عددای ساعتای ۱و ۵ و۹).
- چهار تا عدد روی رئوس یه مربع باشن (۲ و ۵ و ۸ و ۱۱).
- شـش تـا عـدد کـه روی رئـوس یـه شـش ضلعـی منتظمـن (اعداد نوشته روی ساعتای زوج).

آیـا می‌تونیـم بـه حالتـی برسـیم کـه همـه‌ی ۱۲ تـا عـدد با هم برابر باشن؟



مردی سگی را گاز گرفت...!

امیرمسعود جعفرپیشه

به گزارش واحد خبری نیم‌خط، «در شب گذشته، سگی، مردی را گاز گرفت». بله، درست متوجه شدید؛ سگی، مردی را گاز گرفت. نکند انتظار داشتید که واقعاً مردی، سگی را گاز گرفته باشد؟ مگر تاکنون چند مرد را دیده‌اید که سگی را گاز گرفته باشند؟ (البته شاید سگی که مردی را گاز گرفته باشد هم ندیده باشید!)

همان‌طور که دیدیم، دو گزاره‌ی در ظاهر مشابه، می‌توانند اطلاعات متفاوتی به ما بدهند. اما به‌راستی اطلاعات چه معنایی می‌تواند داشته باشد؟ آیا می‌توانیم تعریفی ریاضی برای اطلاعات داشته باشیم؟ و آیا اصلاً می‌توان مقدار اطلاعات موجود در یک پیام را سنجید؟ برای این کار خوب است سعی کنیم اطلاعات سه گزاره‌ی زیر را با هم مقایسه کنیم:

- فردا خورشید از مشرق طلوع می‌کند.
- فردا زلزله‌ای ۸ ریشتری در تهران رخ می‌دهد.
- فردا مدرسه‌ها به‌علت آلودگی هوا تعطیل می‌شوند.

به نظر شما کدام یک از سه گزاره‌ی فوق، اطلاعات بیشتری به ما منتقل می‌کند؟ انتظار دارید که کدام یک از این گزاره‌ها تیترِ یک روزنامه‌ها شود؟ چرا هیچ روزنامه‌ای تیترِ یک خبری خودش را به «طلوع خورشید از مشرق» اختصاص نمی‌دهد؟

همان‌طور که احتمالاً حدس زده‌اید، گزاره‌ی «فردا زلزله‌ای ۸ ریشتری در تهران رخ می‌دهد.»، بیشترین اطلاعات را به ما منتقل می‌کند ولی گزاره‌ی «فردا خورشید از مشرق طلوع می‌کند.» تقریبا هیچ اطلاعات جدیدی به ما اضافه نمی‌کند. اما چه چیزی بین این سه گزاره تفاوت ایجاد می‌کند؟

در زندگی روزمره وقتی می‌خواهیم اطلاعاتی در مورد یک فرد به دست آوریم، اصطلاحا *آمار* آن فرد را می‌گیریم! شاید خوب باشد در این جا نیز آمار گزاره‌های مطرح‌شده را بگیریم و سعی کنیم بر اساس مشاهدات روزمره‌ی خودمان، در مورد میزان اطلاعات هریک از گزاره‌ها نظر دهیم. طلوع خورشید از مشرق، یک حقیقت علمی است که همواره رخ می‌دهد. تعطیلی مدرسه‌ها (در دوران پیش از کرونا البته!)، هم پدیده‌ای است که گاه و بی‌گاه رخ می‌دهد. اما وقوع زلزله‌ای ۸ ریشتری، اتفاقی نادر است که انتظار نداریم هر روز یا حتی هر سال رخ دهد.

مطابق نظریه‌ی *شانون* و در یک مدل ریاضی، میزان اطلاعات یک برآمد[1] آزمایش تصادفی، متناسب با احتمال وقوع آن برآمد است و هرچه احتمال وقوع آن برآمد کمتر باشد، اطلاعات بیشتری دارد. به بیان دقیق‌تر، میزان اطلاعاتی که از وقوع برآمد x که احتمال وقوع آن P(x) است، به دست می‌آید، برابر است با[2]:

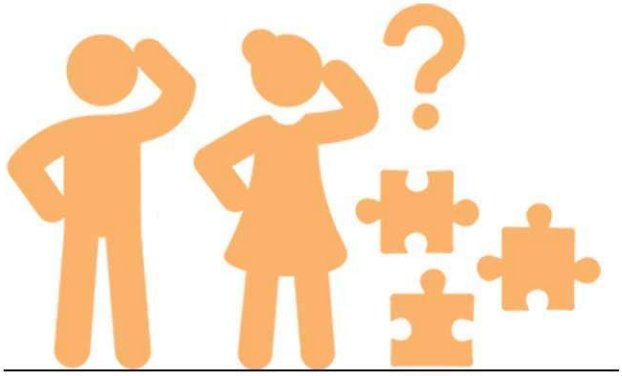
$$I(x) = -\log_2 P(x)$$

در این حالت واحد اطلاعات را بیت می‌گویند. (البته این بیت، با آن بیتی که معمولاً در اندازه‌گیری ظرفیت حافظه‌ها می‌شناسیم، لزوما برابر نیست.)

رابطه‌ی بالا چهار خاصیت مهم دارد. (سعی کنید با توجه به تعریف تابع اطلاعات، به چرایی هرکدام از آن ها فکر کنید و یا مثال مناسبی بزنید.)

- اطلاعات هر برآمد، کمیتی غیرمنفی است.
- اگر $P(A) \geq P(B)$ باشد، آن‌گاه $I(A) \geq I(B)$ است.
- اگر $P(A) = 1$، آن‌گاه $I(A) = 0$.
- اگر A و B دو برآمد کاملا مستقل باشند، آن‌گاه اطلاعات توام آن دو برآمد، برابر جمع اطلاعات دو برآمد است. (برای بررسی چرایی، به خواصی که تابع لگاریتم دارد، توجه کنید.)

نکته‌ی جالب در مورد اطلاعات، معادل بودن آن با ابهام است. به بیان بهتر، وقتی که اطلاعاتی در مورد یک برآمد تصادفی به دست می‌آوریم، عملاً ابهام ما در مورد آن برآمد از بین می‌رود یا کم می‌شود.



۱) در یک آزمایش تصادفی، به هر عضو از فضای نمونه یک برآمد گفته می‌شود. به عنوان مثال در پرتاب سکه، فضای نمونه آزمایش {رو، پشت} است و برآمدهای این آزمایش رو یا پشت است.

۲) برای محاسبه عبارت $\log_2 P(x)$ که به صورت لگاریتم $P(x)$ در پایه (یا مبنای) ۲ خوانده می‌شود، لازم عددی را پیدا کنیم که اگر ۲ را به توان آن عدد برسانیم، برابر $P(x)$ شود. به عنوان مثال، $\log_2 \frac{1}{4} = -2$، زیرا $(2)^{-2} = \frac{1}{4}$. بنابراین برای محاسبه اطلاعات داریم:

$$I(x) = -\log_2 P(x) \leftrightarrow 2^{-I(x)} = P(x) \leftrightarrow 2^{I(x)} = \frac{1}{P(x)}$$

مثلا هنگامی که یک سکه را پرتاب می‌کنیم، احتمال آن که رو یا پشت بیاید، برابر با $\frac{1}{2}$ است. بنابراین قبل از پرتاب سکه، در مورد آن‌که رو می‌آید یا پشت ابهام داریم ولی وقتی که رو آمد، به میزان $\log_2 \frac{1}{\frac{1}{2}} = 1$ بیت اطلاعات به دست می‌آوریم و ابهام ما به‌طور کامل برطرف می‌شود.

برای آن‌که با معادل بودن مفهوم ابهام و اطلاعات بیشتر آشنا شویم، فرض کنید که امیر یک طرفدار جدی فوتبال و والیبال است. در ابتدای تابستان، او می‌داند که ۱۶ تیم به مرحله یک‌هشتم نهایی یورو ۲۰۲۰ صعود کردند و ۴ تیم نیز به مرحله نیمه نهایی لیگ والیبال ملت‌ها صعود کرده‌اند. اما برای انجام یک ماموریت کاری، امیر به یک مسافرت دو هفته‌ای می‌رود که در آن هیچ‌گونه دسترسی به اخبار ندارد. بنابراین امیر که علاقه‌مند است قهرمان مسابقه‌ها را بداند، در مورد قهرمان این مسابقه‌ها دچار ابهام می‌شود. اما پس از دو هفته و بازگشت به خانه، قهرمان این دو رویداد را می‌فهمد و ابهامش برطرف می‌شود. به نظر شما با فهمیدن قهرمان کدام‌یک از این دو رویداد، امیر اطلاعات بیشتری به دست می‌آورد؟ میزان این اطلاعات چقدر است؟ برای سادگی می‌توانید احتمال قهرمانی تمام تیم‌ها در هر یک از مسابقه‌ها را یکسان فرض کنید!

در واقعیت ممکن است برآمدهای مختلف یک آزمایش تصادفی، احتمال‌های برابر نداشته باشند. به‌عنوان مثال، بهتر نیست که احتمال قهرمانی آلمان را بیشتر از احتمال قهرمانی ولز بدانیم؟ (شاید به همین دلیل است که اگر ولز قهرمان یورو شود، شگفت‌زده خواهیم شد!). یا در یک منطقه‌ی نسبتاً خشک از نظر آب‌وهوایی، انتظار داریم که پیش‌بینی هوای روز بعد، بیشتر آفتابی باشد تا بارانی. مثلا با توجه به وضعیت جوی یک منطقه، انتظار داریم که ایستگاه هواشناسی آن منطقه، ۸۰ درصد اوقات وضعیت هوا را آفتابی اعلام کند و ۲۰ درصد اوقات بارانی (با فرض آن‌که تنها همین دو پیش بینی را می‌توانند انجام دهد). حال اگر این ایستگاه هواشناسی اعلام کند که فردا هوا بارانی است، به میزان ۲.۳۲۲ بیت اطلاعات به ما می‌دهد و اگر اعلام کند که فردا هوا آفتابی است، به میزان ۰.۳۲۲ بیت به ما اطلاعات داده شده است.

اما این ایستگاه هواشناسی هر روز چه میزان اطلاعات به ما می‌دهد؟ برای پاسخ به این سوال باید میانگین اطلاعاتی را که این ایستگاه در هر روز به ما می‌دهد، محاسبه کنیم. مطابق تعریف، آنتروپی، متوسط اطلاعاتی است که می‌توان از برآمدهای مختلف یک آزمایش تصادفی انتظار داشت؛ اما از آن‌جایی که احتمال برآمدهای مختلف یک آزمایش تصادفی لزوما برابر نیستند، برای محاسبه‌ی آنتروپی از میانگین وزن‌دار استفاده می‌کنیم. به‌عنوان مثال برای محاسبه‌ی آنتروپی مربوط به این ایستگاه هواشناسی، لازم است تا میانگین وزن‌دار اطلاعات ایستگاه هواشناسی در روزهای مختلف -که وزن‌ها همان احتمال بارانی یا آفتابی بودن هوا است- را محاسبه کنیم:

$$\frac{P(\text{بارانی}) \times -\log_2(P(\text{بارانی})) + P(\text{آفتابی}) \times -\log_2(P(\text{آفتابی}))}{P(\text{بارانی}) + P(\text{آفتابی})} = \frac{۰.۲ \times ۲.۳۲۲ + ۰.۸ \times ۰.۳۲۲}{۱} = ۰.۷۲۲$$

بنابراین آنتروپی این ایستگاه هواشناسی برابر با ۰.۷۲۲ بیت است و به این معنا است که این ایستگاه هواشناسی هر روز به‌طور متوسط، مقدار ۰.۷۲۲ بیت به ما اطلاعات می‌دهد. اما فرض کنید که ما در تاسیس این ایستگاه‌های هواشناسی محدودیت داشته باشیم؛ به نظر شما بهتر است این ایستگاه‌ها را در چه مناطقی تأسیس کنیم تا بیشترین میزان متوسط اطلاعات را به‌دست آوریم؟ (لازم است مناطقی را از نظر آب‌وهوایی بیابید که در آن‌ها، این ایستگاه‌ها بیشترین میزان متوسطِ اطلاعات (آنتروپی) را دارند.)

همان‌طور که دیدیم، واژه‌ی ساده‌ای مانند اطلاعات، می‌تواند دارای یک تعریف ریاضی و دقیق باشد که از قضا با شهود ما هم تا حد خوبی سازگار است. البته شاید جالب باشد بدانید که تعریف ارائه‌شده، تنها تعریف موجود برای اطلاعات نیست و تعریف‌های دیگری هم برای اطلاعات و میزان آن، ارائه شده است. بنابراین شاید از این به بعد، هنگام جمع‌آوری اطلاعات -که یکی از بخش‌های مهم انجام یک پژوهش است- اولین سوالی که می‌پرسیم آن باشد که به راستی در این‌جا چه تعریفی از اطلاعات مد نظر است؟

ضمنا فراموش نکنید که پاسخ‌های خود به سوالات متن را با رستا اینفو (@Rastaiha_info) به اشتراک بگذارید.

فرناز کریمی

سوار بر مرکب عقربه‌های ساعت

سفر در زمان افسانه است یا واقعیت؟ اگر بین سفر به آینده و گذشته فقط یک حق انتخاب داشتید، کدام را تجربه می‌کردید؟

شاید رویای سفر در زمان به قدمت تخیل و بلندپروازی‌های بشر باشد. هر انسانی حداقل یک بار در زندگی خود به این موضوع فکر کرده است که صد سال، پانصد سال یا هزار سال قبل از من، دنیا چه شکلی بوده و حال و هوای فلان دوره‌ی تاریخی چقدر با امروز تفاوت داشته است. و حتی شاید بارها خودمان را در دوره‌ی تاریخی مورد علاقه‌مان تصور کرده باشیم. مثلاً خیال کرده‌ایم که در دربار یکی از پادشاهان باستان حضور داریم و یا در بین مردم آن زمان قدم می‌زنیم و زندگی روزمره‌شان را تماشا می‌کنیم. از طرف دیگر، شاید پیش آمده که دویست سال یا حتی دو هزار سال بعد را در ذهنمان ترسیم کرده باشیم و دلمان خواسته بدانیم که آیا واقعا جهان آن زمان، شبیه تصورات ذهنی ما هست یا نه؟ گاهی دلمان می‌خواهد به آینده برویم تا ببینیم زندگی‌مان چه تغییری خواهد کرد؟ ببینیم چند سال بعد فرزندان ما و یا نوه‌هایمان کجا هستند و چه کار می‌کنند؟

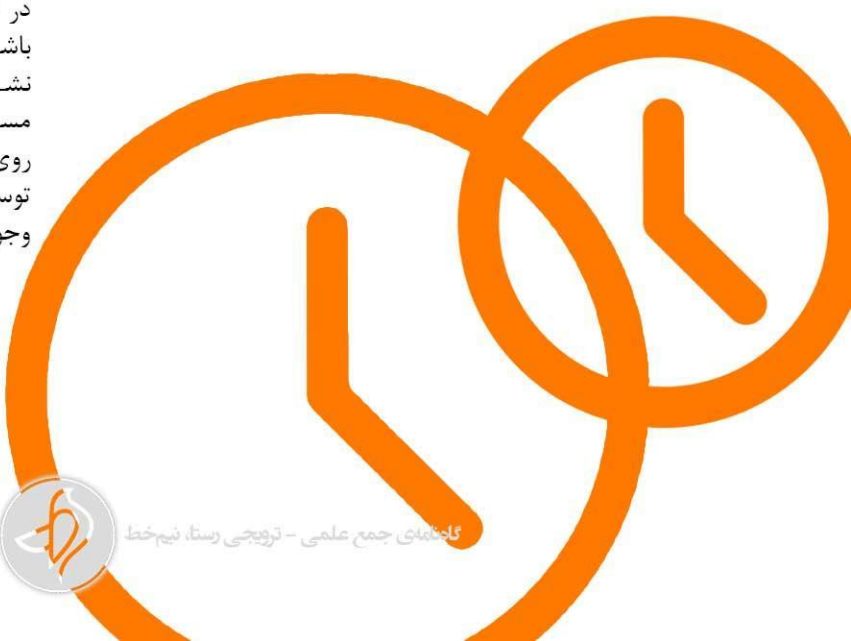
اولین و شاید حتی آخرین راه‌حل برای تجسم عینی این‌گونه رویاها، سفر در زمان باشد. آیا این سفر از نظر علمی و یا منطقی امکان‌پذیر است؟ در واقع تا همین چند سال پیش، سفر در زمان به لحاظ علمی ناممکن به نظر می‌رسید و فقط در داستان‌ها و کتاب‌های تخیلی به آن پرداخته می‌شد. برای مثال دانشمند مشهوری مثل نیوتن معتقد بود که زمان در تمامی گستره‌ی جهان به شکل ثابت و یکسان در حال گذر است و هیچ‌چیز نمی‌تواند روی این جریان ثابت ازلی و ابدی تاثیری بگذارد. اما آیا واقعا باید رسیدن به این رویا را فراموش کرد، یا می‌توان به تحقق آن امیدی داشت؟ در این یادداشت سعی می‌کنیم تا اندازه‌ای به دنبال جواب این سوال‌ها باشیم.

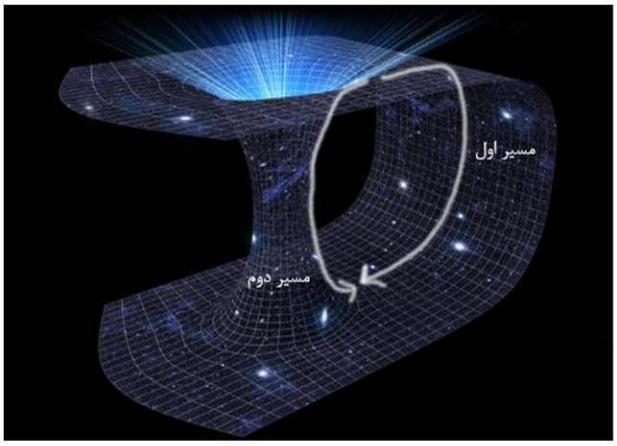
راه‌های سفر در زمان

از حدود اوایل قرن بیستم و با ارائه‌ی نظریه‌ی نسبیت خاص و سپس نسبیت عام انیشتین، همه‌چیز به ناگهان عوض شد. از دیدگاه آلبرت انیشتین سفر در زمان از نظر تئوری امکان‌پذیر است. او گفته بود که اگر جسمی بتواند با سرعتی بیشتر از سرعت نور حرکت کند، در واقع توانسته است در زمان سفر کند. نظریه‌ی نسبیت نشان داد که جریان زمان برخلاف تصور نیوتن، در همه نقاط جهان ثابت و یکسان نیست، بلکه این جریان در بعضی قسمت‌های کیهان تندتر و در قسمت‌های دیگر، مثلاً در نزدیکی کهکشان‌ها و ستاره‌های پرجرم،کندتر و حتی متوقف می‌شود. این جریان حتی می‌تواند در نقاطی حالت گردابی یا حلقه‌ای پیدا کند.

یکی از راه‌های پیش‌بینی‌شده برای سفر در زمان «کرم‌چاله» است. کرم‌چاله‌ها تا کنون به صورت تجربی مشاهده نشده‌اند اما وجود آن‌ها به طور نظری پیش‌بینی شده و گفته شده که می‌توانند بین دو نقطه از فضا و زمان پیوند ایجاد کنند. وارد شدن به یک کرم‌چاله می‌تواند آغاز یک سفر هیجان‌انگیز در زمان باشد اما نکته این‌جاست که به دلیل جاذبه‌ی شدید درون کرم‌چاله، عملاً جسم ورودی به سرعت متلاشی می‌شود و پیش از آغاز سفر، از بین می‌رود. همینطور خود کرم‌چاله هم بسیار ناپایدار است و بلافاصله بعد از به وجود آمدن از بین می‌رود. در حقیقت کوچک‌ترین ذراتی همچون فوتون نیز در صورت عبور، می‌توانند کرم‌چاله را به شدت ناپایدار کنند. اما شاید روزی با کشف روش‌های پیشرفته، هم بتوان پایداری یک کرم‌چاله را بیش‌تر کرد و هم بتوان در برابر جاذبه‌ی بسیار زیاد درون آن مقاومت کرد تا این راه‌حل برای سفر در زمان عملی شود.

به‌منظور درک بهتر مفهوم کرم‌چاله، صفحه‌ای کاغذی را در نظر بگیرید که دو نقطه از آن علامت‌گذاری شده باشند. هریک از این نقاط، دو محل متفاوت از فضا-زمان را نشان می‌دهند. در ابتدا به نظر می‌رسد کوتاه‌ترین مسیر برای اتصال دو نقطه از این کاغذ، مسیر طی شده روی کاغذ باشد. اما با تا کردن کاغذ و سوراخ کردن آن توسط یک میله می‌توان دید که مسیری کوتاه‌تر نیز وجود دارد که الزاماً روی کاغذ قرار ندارد.





در شکل بالا دو مسیر ممکن به‌منظور طی کردن مسیر بین دو نقطه نشان داده شده‌اند. حال فرض کنید این صفحه همان صفحه‌ی فضا-زمان باشد. از این رو ممکن است یکی از این نقاط روی زمین و نقطه دوم در کهکشان دیگری قرار داشته باشد. در نتیجه شما می‌توانید با وارد شدن به دروازه‌ی روی زمین، فضا-زمان را میانبر زده و به کهکشانی دیگر و یا به زمانی دیگر سفر کنید.

تناقضات

یکی از بزرگ‌ترین مسائلی که امکان سفر در زمان را به طور جدی به چالش می‌کشد «پارادوکس پدربزرگ» است. طبق این تناقض اگر شما بر فرض موفق شدید به گذشته سفر کنید و در آن‌جا پدربزرگ خود را ببینید و به طور مثال او را از بین ببرید، عملا موجودیت شما زیر سوال می‌رود. و یا مثلا اگر مانع ازدواج پدر و مادر خود شوید، در این صورت باز هم شما نمی‌توانید متولد شده باشید تا روزی در زمان سفر کنید! به نظر شما آیا شما اصلا می‌توانید مانع ازدواج پدر و مادر خود شوید؟ برای مثال فرض کنید اگر کسی به گذشته می‌رفت و به طریقی از ازدواج پدر و مادر «آدولف هیتلر» رهبر خون‌خوار نازی‌ها جلوگیری می‌کرد، با این کار جان میلیون‌ها انسان نجات داده می‌شد! راستی اگر شما می‌توانستید به گذشته سفر کنید، چه کارهایی انجام می‌دادید؟!

یک تناقض دیگر که شاید قبل از این تناقض به ذهن برسد آن است که اصلا شما چگونه می‌توانید به زمانی بروید و در آن حضور داشته باشید که در آن زمان متولد نشده بودید؟ همه‌ی این‌ها سوالاتی است که باید برای حل مسئله‌ی امکان‌پذیربودن سفر در زمان، به آن‌ها پاسخ داده شود.

به عنوان یک تناقض دیگر، مثلاً تصور کنید که شما دوچرخه خود را در کنار یک مغازه پارک می‌کنید اما فراموشتان می‌شود که آن را به جایی قفل کنید. خرید خود را انجام می‌دهید و وقتی برمی‌گردید، می‌بینید که دوچرخه شما به سرقت رفته است. آن‌گاه ماشین زمان خود را روشن می‌کنید که به چند دقیقه قبل برگردید تا این‌بار دوچرخه خود را قفل کنید و از دزدیده‌شدن آن جلوگیری کنید. اما با برگشتن به آن زمان، احتمال دارد که شما دوباره تبدیل به همان آدم فراموش‌کار چند دقیقه قبل شوید و مجدداً از یاد ببرید دوچرخه را قفل کنید. پس دوچرخه باز هم دزدیده می‌شود و دوباره فکر استفاده از ماشین زمان به ذهن شما خطور می‌کند. در این صورت شما در یک تله‌ی زمانی گیر می‌افتید و این خود یکی از مشکلاتی است که درباره امکان‌پذیربودن سفر در زمان وجود دارد.

یک سوال دیگر که توسط «استفن هاوکینگ» فیزیک‌دان برجسته قرن اخیر مطرح شد و ما را در مورد ممکن‌بودن سفر در زمان دچار تردید می‌کند این است که اگر سفر در زمان عملی است پس چرا تا به حال کسی از زمان آینده به زمان حال سفر نکرده و خودش را به عنوان مسافر زمان به ما معرفی نکرده است؟ چرا تا کنون با چنین شخصی مواجه نشده‌ایم؟ شاید این‌جا یک سوال دیگر به وجود بیاید که اگر شخصی از آینده به زمان ما بیاید، اصلا می‌تواند به ما بگوید؟ از کجا معلوم؟ شاید تا به حال کسی از آینده به زمان حال آمده باشد اما قوانین فیزیک این اجازه را به او نمی‌دهند که به ما چیزی در این باره بگوید.

پاسخ به تناقضات

طبق تحقیقات جدید توسط «ژرمن توبر»، پاسخی به تناقض اول یعنی همان «پارادوکس پدربزرگ» داده شده است که باید دید چقدر با واقعیت هم‌خوانی دارد. او می‌گوید:

«از دیدگاه دینامیک کلاسیک اگر شما از وضعیت یک سیستم در زمان مشخصی اطلاع داشته باشید، به تاریخچه سیستم دست پیدا می‌کنید. با این حال نظریه نسبیت عام اینشتین حلقه‌های زمانی یا سفر در زمان، جایی که رویداد می‌تواند در گذشته و آینده رخ دهد را پیش‌بینی می‌کند.»

محاسبات این فیزیک‌دان نشان می‌دهد فضا-زمان می‌تواند خود را به گونه‌ای سازگار کند تا از پارادوکس جلوگیری کند. به عنوان مثال تصور کنید فردی به گذشته سفر می‌کند تا از شیوع یک بیماری جلوگیری کند. در صورتی که این ماموریت با موفقیت انجام شود دیگر بیماری‌ای برای شکست دادن در گذشته وجود ندارد و این تناقض است. پژوهش این فیزیک‌دان که در ژورنال Classical and Quantum Gravity به چاپ رسیده، به این موضوع اشاره می‌کند که اگر شما سعی کردید به طریقی از شیوع این بیماری جلوگیری کنید، آنگاه آن بیماری از روش‌های متفاوت دیگری شیوع پیدا می‌کند و همین امر می‌تواند از پارادوکس جلوگیری کند و مسافر زمان هرکاری که انجام دهد، نمی‌تواند جلوی این بیماری را بگیرد. در مثال پدربزرگ، شما هر کاری بکنید نمی‌توانید باعث از بین رفتن پدربزرگ خود شوید و یا نگذارید پدر و مادرتان با هم ازدواج کنند. چرا که هرقدر تلاش کنید، قوانین فیزیک به گونه‌ای عمل می‌کنند که شما نتوانید نهایتاً هیچ‌کدام از آن‌ها را انجام دهید. این نظر «ژورمن توبر»است.

در شماره‌ی بعدی نیم‌خط قصد داریم تا اندکی بیشتر به مقوله سفر در زمان بپردازیم و همین‌طور رمان‌ها و فیلم‌هایی که در این زمینه موجود هستند را بررسی کنیم تا با دیدگاه‌های مختلفی که در آن‌ها مطرح شده‌اند، آشنا شویم.

داستان رمزنگاری

رضا ابوالقاسمی

سلام بچه‌ها! :)
در قسمت‌های قبل تاریخچه‌ای از رمزنگاری‌های سنتی را دیدیم. هم‌چنین با مثال‌هایی از رمزگذاری‌های جانشینی (جایگزینی هر عنصر با یک عنصر دیگر) و جای‌گشتی (جابه‌جایی عنصرهای رمزشده) آشنا شدیم. در آخر هم دنبال روشی بودیم تا بتونیم تشخیص بدیم یک رمزنگاری چه‌قدر خوب و کاربردی‌ست.
در این قسمت قصد داریم باهم یک نمونه‌ی دیگر رمزنگاری را ببینیم و روش شکستن آن را بررسی کنیم.

داستان رمزنگاری (قسمت سوم)

اولاً بیایید باهم فرضی کنیم. ما فرض می‌کنیم شخص مهاجم [محترم] که می‌خواهد رمزمان را بشکند، الگوریتم (روش) رمزنگاری ما را می‌داند. در حقیقت ما دنبال رمزنگاری‌ای هستیم که به‌قدری قوی باشد که مهاجم با دانستن الگوریتم هم نتواند پیام رمزشده را تشخیص دهد و یا کلید رمز را استخراج کند.
اما مهاجم چه اطلاعات دیگری ممکن است داشته باشد که به او کمک کند؟
در بعضی حالات، مهاجم با داشتن تنها الگوریتم رمزنگاری، قادر است معکوس آن را ایجاد کند و رمز را بی‌اثر کند. اما در بعضی از حملات، مهاجم به اطلاعات بیشتری نیاز دارد. مثلاً گاهی نیاز است که چند نمونه متن رمزشده داشته باشد، در برخی موارد لازم است چند جفت پیام ساده و رمزشده‌ی آن‌ها را داشته باشد، در بعضی دیگر نیاز دارد که خود بتواند متن ساده‌ی دلخواه را وارد کند و متن رمزشده‌ی آن‌ها را دریافت کند.
حالا بیایید باهم یک رمزنگاری را بررسی کنیم.

رمزنگاری Vigenere

رمزنگاری ویژنیر در حقیقت نوع قوی‌شده‌ای از رمزنگاری سزار است، که در شماره‌ی سوم نیم‌خط با رمز سزار آشنا شدیم.
بیایید با یک مثال روش کار این رمزنگاری را بررسی کنیم.
فرض کنیم می‌خواهیم متن "Attack in the morning" را رمز کنیم.
در این روش ابتدا باید یک کلید انتخاب کنیم. مثلاً TFRXSE

حال جریان کلید را به این شکل تعریف می‌کنیم:

TFRXSETFRXSETFRXSETFRXSE...

حال با استفاده از جدول زیر متن رمزشده را ایجاد می‌کنیم. به این شکل که برای هر حرف متن، ستون معادل و برای هر حرف جریان کلید، سطر معادل را انتخاب می‌کنیم و حرفی که در آن خانه‌ی جدول وجود دارد را به‌عنوان حرف رمزشده انتخاب می‌کنیم.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

مثلاً برای حرف اول سطر A و ستون T را انتخاب می‌کنیم که حرف رمز معادل T است. برای حرف دوم سطر T و ستون F را انتخاب می‌کنیم که حرف رمز معادل Y است.
با ادامه‌ی این فرایند متن رمزشده به این شکل خواهد بود:

TYKXUOBSKEWQHWEFFK

حال بیایید با هم یک متن رمزشده در این روش را رمزگشایی کنیم.

تلاش برای شکستن Vigenere

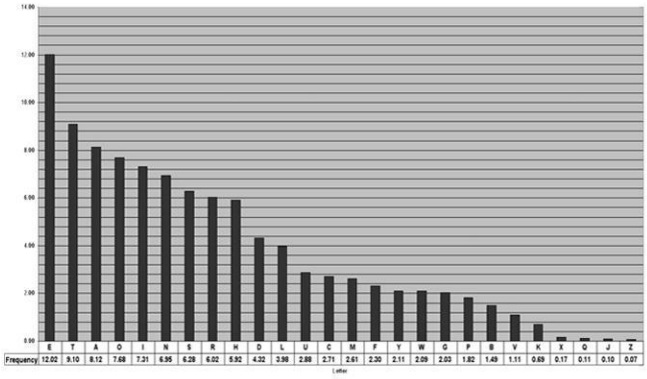
فرض کنید ما تنها یک پیام رمزشده داریم و سعی داریم کلید رمز را با استفاده از آن تشخیص دهیم.

متن رمز شده:

YWJHRYPKOTWLCVKPWLSXYBKYVTCTABSOG
UWFVGSRXQYOTXJKLGWMVSTHMJIRHWSWNY
MXZHKBCHKJENPVMKGUVFZXFHZBYBVMITHE
DAOZBSAKJHSLYDBYPSVWJZTJHRXAABSOVVPJ
ZISTXAOJTQKOWAJZYHKJCTSBPMRFMTXXVON
LKHGDZKHEUZUAXHBOVGKWXJHSNOKXSBOH

خب به نظرتان چه‌طور می‌شود این رمز را شکاند؟

در قسمت‌های قبل گفتیم که یکی از روش‌های مورد استفاده در شکستن رمزهای از نوع جانشینی، استفاده از فراوانی حروف در متن‌های زبان است. در عکس زیر میزان فرکانس تکرار حروف در متن‌های انگلیسی است.



در حقیقت با استفاده از میزان تکرر حروف در پیام رمزشده، حدس می‌زنیم که هر حرف رمزشده معادل با کدام حرف واقعی است.

اما در رمزنگاری ویژینیر نمی‌توان به‌راحتی از این تکنیک استفاده کرد، چراکه باتوجه به کلید، نگاشت حروف از نظم موردنظر ما برخوردار نیست و نیاز به تحلیل‌های بیشتری دارد.

بیاید سعی کنیم تا طول کلید را حدس بزنیم. فرض کنید حدس خوبی زدیم و طول کلید k شد. حال می‌توانیم از یک حرف شروع کنیم و با گام‌های kتایی جلو برویم و با استفاده از تحلیل فرکانسی، حروف و کلید را حدس بزنیم.

نکته‌ای که باید به آن دقت کنیم، ترکیب‌های حروف است که در متن‌ها تکرار می‌شود. در حقیقت این ترکیب‌ها احتمالاً پس از رمز شدن نیز به یک شکل خواهند بود و قابل‌پیش‌بینی هستند.

پس بیایید ۳تایی‌های تکراری در متن رمزشده را پیدا کنیم.

فاصله‌ها	تعداد تکرار	۳ تایی
۱۲۱	۲	JHR
۱۰۰	۲	ABS
۱۰۰	۲	BSO
۸۰	۲	HKJ
۸۵	۲	JHS

به نظر می‌آید ترکیب‌های تکراری با ضریب ۵ یا ۱۰ با هم فاصله دارند. پس احتمالاً طول کلید ۱۰ یا ۵ است.

فرض کنید طول کلید ۵ باشد. پس باید حروف در جایگاه $5k + r$ را تحلیل فرکانسی کنیم.

برای $r = 1$ داریم:

حرف	Z	B	W	M	L	A	P	C	O	K	X	V	Q	J	E	I	N
تکرار	۶	۵	۴	۴	۳	۳	۲	۲	۲	۲	۲	۱	۱	۱	۱	۱	۱

همان‌طور که در جدول بالا مشاهده می‌کنید، S و Y و J حروف پرتکرار هستند. از طرفی جایگاه این حروف (در الفبای انگلیسی) به ترتیب برابر با ۱۹ و ۲۵ و ۱۰ است.

حال به لیست پرتکرارهای زبان انگلیسی توجه کنید. در این لیست حرف‌های E و T و A و O و I و N و S و R و H پرتکرارها هستند. جایگاه آن‌ها به ترتیب برابر با ۵ و ۲۰ و ۱ و ۱۵ و ۹ و ۱۴ و ۱۹ و ۱۸ و ۸ است.

اما از بین این حروف متداول، آن‌هایی مطلوب هستند که اختلاف جایگاهشان مثل اختلاف جایگاه حروف S و Y و J است. پس باید یک عدد و به‌علاوه‌ی ۹ و به‌علاوه‌ی ۱۵ آن در پرتکرار باشد. تنها عددی که این خاصیت را دارد ۵ است؛ یعنی حرف J معادل با E، حرف S معادل با N و حرف Y معادل با T است. پس حرف اول کلید برابر است با F.

حرف	S	Y	J	X	H	W	P	T	F	K	M	D	Z	R	Q	N	U
تکرار	۶	۵	۵	۳	۳	۲	۲	۲	۲	۲	۲	۲	۱	۱	۱	۱	۱

همان‌طور که در جدول بالا مشاهده می‌کنید، Z و B حروف پرتکرار هستند. از طرفی جایگاه این حروف (در الفبای انگلیسی) به ترتیب برابر با ۲۶ و ۲ است. پس با همان استدلال قسمت قبل به دنبال دو حرف متداول با تکرر بالا و با فاصله‌ی ۲ می‌گردیم. حروف R و T این خاصیت را دارند. پس حرف دوم کلید برابر با I می‌شود.

تمرین

با ادامه دادن این روند می‌شه به کلید و متن اصلی رسید. شما سعی کنید این دو را پیدا کنید و برای رستا اینفو (@rastaiha) ارسال کنید. (برای راهنمایی باید بهتان بگویم که کلید کلمه‌ای با معنی است.)

حالا که با یک مسئله‌ی کمی واقعی کلنجار رفتیم، احتمالاً بیشتر متوجه میزان قدرت یک رمزنگاری سنتی شدیم. اگر رمزنگاری‌ای که دیدیم کلید بزرگ‌تری داشت، کارمان خیلی سخت می‌شد. البته این متن رمزشده خیلی کوتاه بود و تحلیل فرکانسی روی متن‌های بلندتر، بهتر و دقیق‌تر کار می‌کند.
در قسمت بعدی به رمزنگاری‌های قوی‌تر و مدرن‌تری خواهیم پرداخت.

لینک نظرسنجی

با پرکردن این نظرسنجی ما را در بهبود نیم‌خط یاری کنید.

عکس از مریم اصلاح‌جمع‌زاده

گردباد وادی حیرت ز منزل غافل است
راه کوی لیلی از مجنون سرگردان مپرس

صائب تبریزی