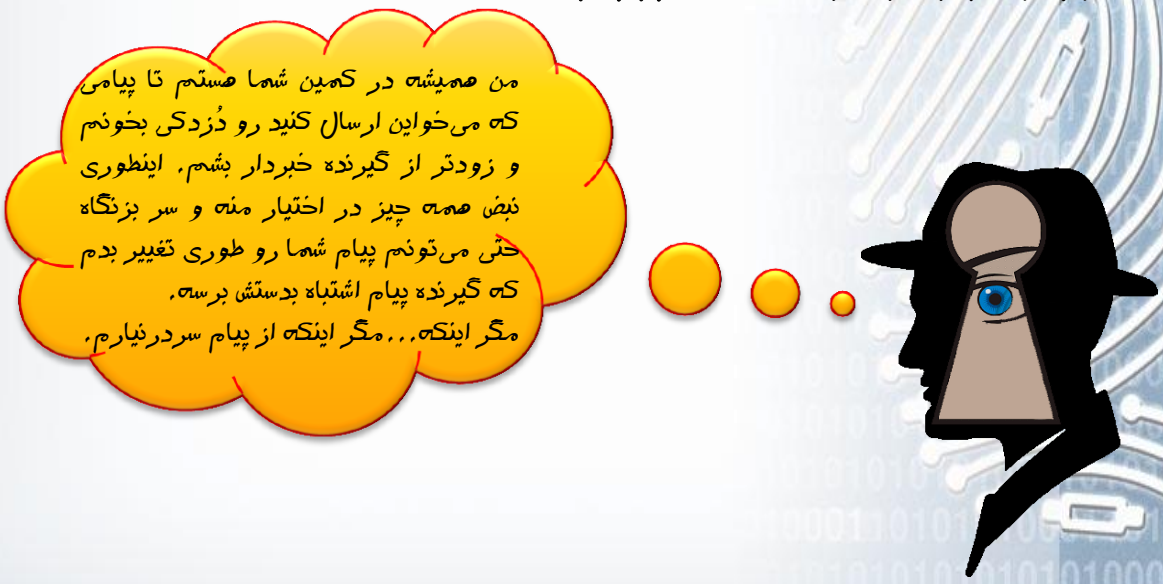
رمزنگاری... چیست و چرا؟

تاریخ باستان نشان می‌دهد که همواره انسان در کنار خود، تعدادی دوست و تعدادی دشمن داشته است. دوستان او انسان‌هایی بودند که منافع مشترکی با او داشتند و دشمنانش کسانی بودند که تلاش می‌کردند این منافع را از دست او برُبایند.

با پیشرفت جوامع بشری، شیوه‌ی هجوم دشمنان به ذخایر یک ملّت نیز پیشرفته شد. دشمن فهمید که فقط با زور بازو نمی‌تواند در جنگ پیروز شود و سعی کرد با جاسوسی، اخبار مهمی که به ذخایر ارزشمند اشاره دارد را به دست آورد و همه را غافلگیر کند.

به همین خاطر، **پیام‌های مهم** بین دوستان می‌بایست طوری رد و بدل می‌شد که دشمن از مفهوم پیام سر در نیاورد. در اینجا بود که **هنر رمزنگاری** به‌وجود آمد.

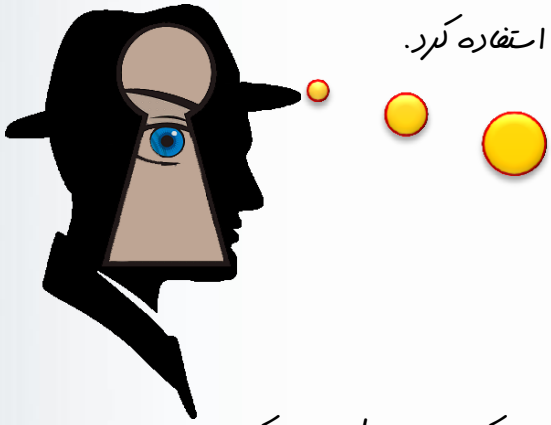


هر گردی گردو نیست!

هر پیام نامفهوم رمز نیست. آیا می‌توانید این پیام را بخوانید؟

明天來在8個街道

این جمله با کلمات چینی نوشته شده و به معنی «فردا ۸ صبح بیا خیابان هشتم» است. ما رسم الخط چینی را نمی‌فهمیم ولی چون عده‌ی زیادی از انسان‌ها به طور معمول از آن استفاده می‌کنند (چینی‌ها)، نمی‌توان برای پنهان سازی پیام استفاده کرد.



بنابراین الفبای پیام مهم نیست. بلکه مهم این است که پیام را طوری که همه می‌توانند بخوانند ارسال نکنیم و طوری حروف پیام را عوض کنیم که در نگاه اول کاملاً بی معنی به نظر آید:

«نابایخ متشه»

عجله نکنید! حروف بالا درست تایپ شده ولی هرکسی نمی‌تواند آن را بفهمد. من به شما می‌گویم آن را چگونه بخوانید: هر کلمه را از سَر به تَه بخوان. حالا فهمیدی؟

یک پیام معمولاً به صورت یک متن، یک تصویر و یا یک صدای ضبط شده ارسال می‌شود. در دوران قدیم، روش‌های پنهان کردن پیام پایه‌و اساس علمی نداشت و امروز ما این روش‌ها را می‌توانیم به شکل یک معمای جالب در یک جمع دوستی نیز مطرح کنیم:

«آلیس گفتین کیف پول کجاست؟»

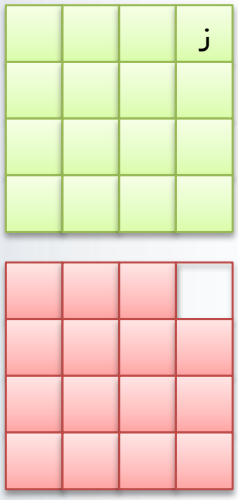
سلام بابا. دیروز رفتیم با دوستام فوتبال زدیم و خیلی کیف کردیم. دو تیم ۵ نفره شدیم که یه تیم شد لیورپول و اون یکی تیم شد منچستر. اول بازی چنان زیر توپ زدم که هیچ کسی تاحالا ندیده بود. فکر نکنم پله و مارادونا هم بتونن. توپ رو شوت کردم آنقدر تا توچال رفت بالا و اومد پایین. اینجوری روی همه رو کم کردم.

این نامه چه ربطی به کیف پول داره؟ بذار بیشتر به متن نگا کنم. ما خرابکارها کوتاه نمی‌یایم. بیشتر از اینکه شما سعی می‌کنید پیامتون رو نامفهوم جلوه بدین ما تلاش می‌کنیم تا پیام شما رو بفهمیم. پس به جای اینکه فکر کنین رمزتون خیلی قویه، بهتره به دنبال برطرف کردن هر نقطه ضعفی باشین. آهان! حالا یه چیزایی داره دستگیرم می‌شه. کلمات آخر هر جمله... آره... کیف پول زیر...

با حساس‌تر شدن اطلاعات در بین بشر، روش‌های رمزنگاری اطلاعات پیچیده‌تر شد. تا اینکه امروزه می‌بینیم روش‌های رمزنگاری کاربردی مبتنی بر هندسه و یا ریاضیات پیشرفته است. با ظهور رایانه در عصر نوین نیز، الفبای رمزنگاری دوحرفی شد: ۰ و ۱. که این ۰ یا ۱ ارزش کوچکترین واحد حافظه یعنی «بیت» را در رایانه مشخص می‌کند. بنابراین پیام‌های محرمانه در ارتباطات الکترونیکی به صورت رشته‌ی طولانی از ۰ یا ۱ ارسال می‌شود.

می‌خواهیم شما را با یک روش رمز کلاسیک و نه کاربردی آشنا کنیم تا به زبان ساده‌تری مفهوم رمزنگاری را درک کنید.

مربع رمز



فرض کنید که می‌خواهید جمله‌ی زیر را به دوست خود ارسال کنید.

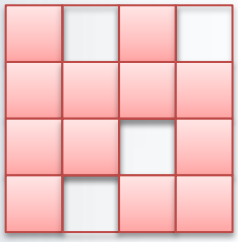
"زنگ بعدی یا آبخوری"

این جمله ۱۶ حرف دارد. می‌خواهیم حروف این جمله را طوری در خانه‌های مربع رمز (مربع سبز) ۴×۴ بنویسیم که کسی محتوای آن را نفهمد.

مربع دیگری (مربع قرمز) را تهیه کنید که ابعاد آن با ابعاد اوّلی برابر باشد. یکی از خانه‌های گوشه را سوراخ کنید. با روی هم قرار دادن این دو مربع می‌توانید حرف اول جمله را روی شبکه‌ی بالا بنویسید. به این شبکه‌ی سوراخ شده، «شابلون» می‌گوییم.

شابلون را ۹۰ درجه در جهت حرکت عقربه‌های ساعت بچرخانید ولی مربع رمز را در جای خود ثابت نگهدارید. در این صورت حرف دوم را در محل سوراخ روی مربع رمز بنویسید. با ادامه‌ی این

روند فقط ۴ حرف اول جمله، در چهار گوشه‌ی مربع رمز قرار می‌گیرند. فایده ندارد و باید خانه‌های دیگری را روی شابلون سوراخ کنیم. چون هر سوراخ ۴ حرف را روی مربع رمز قرار می‌دهد، پس کافی است که ۴ خانه از شابلون را سوراخ کنیم. امّا جای ۳ سوراخ دیگر کجا باید باشد؟



البته سوراخ دوم نمی‌تواند در ۳ گوشه‌ی دیگر شابلون باشد. زیرا سوراخ اول هر ۴ گوشه را پُر می‌کند. پس باید خانه‌هایی را سوراخ کرد که با چرخیدن‌ها، روی هم قرار نگیرند. مثلاً این یک شابلون کامل است.

حالا که شابلون کامل شد، حروف جمله را با دستور زیر بنویسید (**الگوریتم رمز**) :

- مربع رمز را تکان ندهید و در جای خود ثابت نگه دارید.
- شابلون را روی مربع رمز قرار دهید. از ردیف بالا شروع کنید و از راست به چپ اگر خانه‌ای سوراخ است یک حرف از جمله را روی مربع رمز بنویسید و سپس به ردیف بعدی بروید.
- شابلون را ۹۰ درجه در جهت عقربه‌های ساعت بچرخانید و دوباره مرحله‌ی قبل را اجرا کنید تا هر ۱۶ حرف روی مربع رمز قرار بگیرند.

	ن		ز
		گ	
	ب		

۱

	ن		ز
د			ع
	ی	گ	
	ب		ب

۲

	ن	ی	ز
د	ا		ع
	ی	گ	
ب	ب	ا	ب

۳

خ	ن	ی	ز
د	ا	و	ع
ی	ی	گ	ر
ب	ب	ا	ب

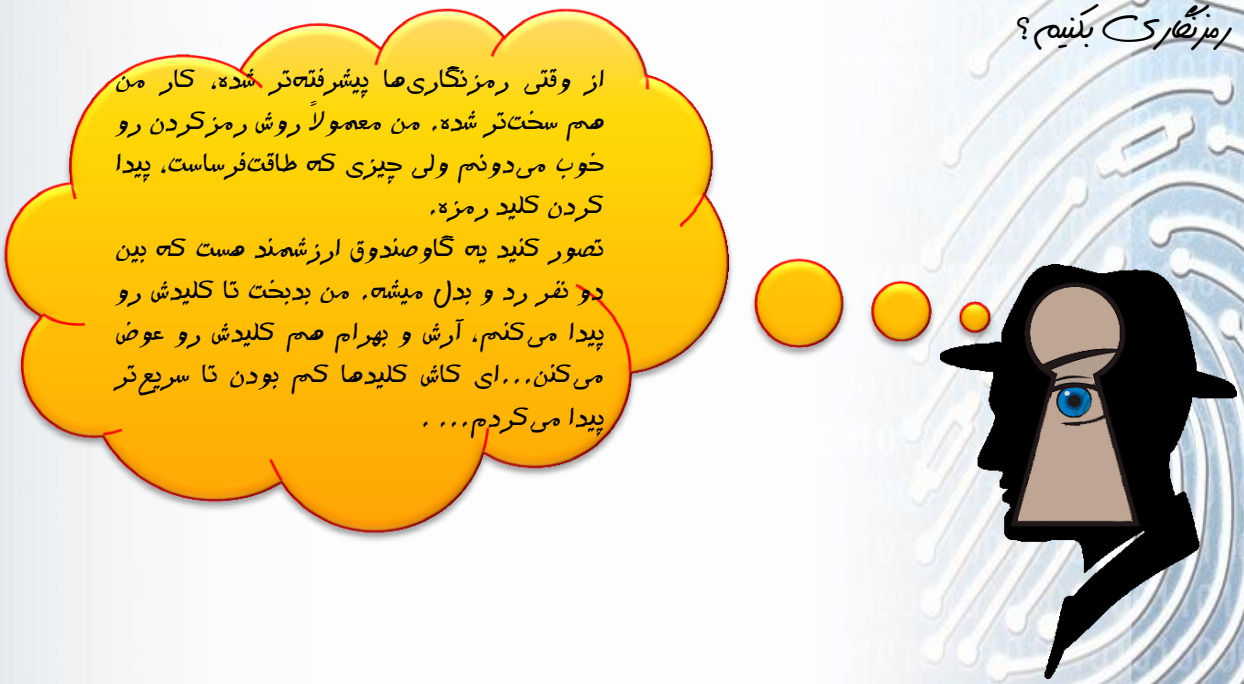
۴

کلید رمز

الگوریتم‌های نوینِ رمز، هرچند هم پیچیده و پیشرفته باشند، همگی در یک چیز مشترکند: **کلید رمز**. در روش «مربع رمز» شابلون همان کلید رمز است. جالب است بدانید با روش‌های ساده‌ی شمارش ثابت می‌شود ۶۴ شابلون متفاوت می‌توان ساخت و یک مربع رمز ۸×۸ تقریباً یک میلیارد شابلون خواهد داشت. بنابراین حتی اگر خرابکار روش رمز مربعی را بلد باشد، باید یک میلیارد «کلید» را برای یافتن پیام بررسی کند.

امروزه رمزنگاری در ارتباطات اینترنتی، سازمان‌های اطلاعاتی و ارگان‌های نظامی کاربرد دارد. امّا بدون در نظرگرفتن حساسیت استفاده از آن، ساده شده‌ی پیکربندی رمزنگاری به شکل زیر است:

آرش با پای خود متن رمز را به بهرام نمی‌دهد. زیرا در غیر این صورت پیام اصلاً احتیاجی به رمزکردن ندارد. پس آرش پیام را رمز می‌کند تا در راه ارسال بیشتر مطمئن باشد کسی از متن پیام سر در نمی‌آورد. در واقع اگر فرض بشود معبر ارسال پیام امن است دیگر برای چه منظوری رمزنگاری بکنیم؟



در نمودار قبل معبر ارسال پیام می‌تواند خطوط تلفن، شبکه‌ی خطوط موبایل و یا شبکه‌ی اینترنت باشد. امّا همانطور که می‌بینید **رمزکردن** یک پیام همانند قفل کردن است و **رمزگشایی** آن مانند بازکردن قفل می‌باشد. پس خرابکار همیشه به دنبال یافتن کلید است. هرچه یافتن کلید سخت‌تر باشد، رمز مورد نظر قوی‌تر است.

فرستنده و گیرنده باید کلید یک‌تی داشته باشند تا پیام‌های رمزشده را بتوانند با همان کلید رمزگشایی کنند. ولی با یک بار رد و بدل کردن کلید، آرش و بهرام بارها می‌توانند پیام‌های محرمانه‌ای رد و بدل کنند. از این رو می‌توان فرض کرد آرش و بهرام در یک ملاقات محرمانه، هرچند هزینه سنگینی برایشان داشته باشد، کلید را رد و بدل می‌کنند.

بیا بگیر، اینم کلید. آسه برو آسه بیا، به هیچ کسی نگو منو اینجا ملاقات کردی، راستی یادت باشه چند ماه بعد یه ملاقات دیگه داشته باشیم تا یه کلید دیگه رد و بدل کنیم، اینجوری مطمئن می‌شیم آقای خرابکار هرچی هم تلاش کرده باشه همه نقش بر آب می‌شه، من دوباره برمی‌گردم به کشور خودم و از اونجا پیام رمز رو روی سایت می‌گذارم، تو فقط می‌تونی رمزگشایی کنی، چون تو فقط کلید رو داری، نگران نباش.

پس مجبر ارسال کلید همیشه امن فرض می‌شود. زیرا فقط یک بار کافی است کلید رد و بدل شود و می‌تواند با یک امنیت کامل این کار انجام شود، هرچند هزینه‌ی زیادی در بر داشته باشد.

خیال نکنید با مخفی کردن الگوریتم رمز، خیالتان راحت خواهد شد، من هم روش‌های پیشرفته‌ای برای رمزگشایی دارم، ولی قوی‌ترین رمزها، آنهایی هستند که با اینحال که الگوریتم رمز را می‌دانم، کلیدش را هرچه سعی می‌کنم پیدا نمی‌کنم.