آب یا «پت»؟! رمزنگاری با روش جابه‌جایی

محمود داورزنی

دنیای امروز سرشار از اطلاعاتی است که به‌طور مداوم بین انسان‌ها و رایانه‌ها دست به دست می‌شوند. بعضی از این اطلاعات باید به رمز بیان شوند تا هر کسی نتواند به آن‌ها دسترسی پیدا کند و فقط افراد یا دستگاه‌های خاص بتوانند آن‌ها را رمزگشایی کنند. مثلاً امواج رادیویی و تلویزیونی همه‌جا قرار دارند، ولی فقط دستگاه‌های خاصی می‌توانند این اطلاعات را به نحو شایسته‌ای کدگشایی کنند و در اختیار ما قرار دهند. یا اطلاعات ارسالی از یک ماهواره که باید به زمین مخابره شود، به‌گونه‌ای است که لزوماً باید کُد و رمز شده باشد تا هر کسی نتواند از آن استفاده کند. در این شماره و چند شمارهٔ آیندهٔ مجله، شما را تا حدودی با رمز کردن پیام و رمزگشایی آن را آشنا می‌کنیم.

یکی از ساده‌ترین روش‌های به رمز درآوردن پیام استفاده از رمز «جابه‌جایی»[1] است. در این روش یک عدد مانند m=۲ را در نظر می‌گیریم و هر حرف کلمه از متن اولیه را با ۲ حرف بعد از آن جابه‌جا می‌کنیم. مثلاً کلمهٔ «آب» به کلمهٔ «پت» رمز می‌شود.

حروف الفبای فارسی

آ	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	
ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	

اکنون در کلمهٔ رمز شده و با داشتن m=۲، می‌توانید هر حرف را به دو حرف قبل از آن تبدیل کنید تا متن اولیه مشخص شود.

مثال: با عدد رمز m=۲، متن «باید برویم» را رمز می‌کنیم.

حروف اولیه	ب	ا	ی	د	ب	ر	و	ی	م
حروف رمز شده	ت	پ	ب	ر	ت	ژ	ی	ب	و

پس متن رمز شده عبارت است از: «تپبرتژیبو». می‌بینید که برای حروف انتهای جدول الفبای فارسی، به ابتدای جدول برمی‌گردیم. حال فرض کنید متن رمز شدهٔ شما به‌دست فرد غریبه یا دشمن برسد. او چه‌طور می‌تواند رمز شما را بشکند و متن اولیه را تشخیص دهد؟ اگر او بداند که شما از رمز جابه‌جایی استفاده کرده‌اید، می‌تواند با امتحان کردن حالت‌های m=۳۲ و ... و m=۲ و m=۱ روی چند حرف اولیه و مشاهدهٔ این که کدام متن با معنی می‌شود، عدد رمز را پیدا کند و کل متن رمز شده را به راحتی به متن اولیه تبدیل کند. بنابراین شکستن این رمز خیلی سخت نیست و البته با داشتن یک رایانه، این کار بسیار راحت است.
متن زیر به کمک رمز جابه‌جایی به‌دست آمده است. متن اولیه را پیدا کنید. پاسخ آن را می‌توانید در صفحهٔ ۳۸ مجله ببینید.

سخعص ظنژلشضص وژلش‌ضیع، زسنقششض نض زص گسنل، سخعص زص زصنل، زسنقششض ضس نض زص گسنژل.
وزضژس س ا نضصت لن‌شن زسخججص زص عسضژل عججصصن دژل. لن وژلذص شصق دیص نض عککخصن ژدژصل، ضوضن ژلشصل، اضصل ضزنسو خلنعززژل طضاصل، ضرض صضلعضژ طضال، وزضژ ضو ازض خلنعززژلعن ضیع.

پی‌نوشت :
1. Shift