# با «آتش» رمز کنید!

## رمزنگاری با استفاده از کلمهٔ رمز

محمود داورزنی

**دنیای امروز سرشار از اطلاعاتی است که به‌طور مداوم بین انسان‌ها و رایانه‌ها دست‌به‌دست می‌شوند. بعضی از این اطلاعات باید رمز شوند تا هر کسی نتواند به آن‌ها دسترسی پیدا کند و فقط افراد یا دستگاه‌های خاصی بتوانند آن‌ها را رمزگشایی کنند. مثلاً امواج رادیویی و تلویزیونی همه‌جا هستند، 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، به گونه‌ای است که لزوماً باید کد و رمز شده باشد تا هر کسی نتواند از آن استفاده کند. در شمارهٔ قبلی با روش جابه‌جایی برای رمزنگاری آشنا شدید. در این شماره با رمزنگاری با استفاده از کلمهٔ رمز آشنا می‌شوید.**

استفاده از یک کلمهٔ رمز (به‌جای عدد رمز) روش دیگر رمز کردن است. در این روش یک کلمهٔ رمز مانند «آتش» را در نظر می‌گیرند. اکنون با توجه به اینکه «آ»، «ت» و «ش» حروف اول، چهارم و شانزدهم حروف فارسی هستند، کافی است حروف متن اولیه را به بخش‌های سه‌تایی تقسیم کنیم و سپس حروف اول را به یک حرف بعدی، حرف دوم را به چهار حرف بعدی و حرف سوم را به شانزده حرف بعدی تبدیل کنیم تا به این روش کل متن رمز شود.

**مثال:** با کلمه رمز آتش، متن «فردا ساعت دو» را رمز می‌کنیم.

| حروف اولیه | ف | ر | د | ا | س | ا | ع | ت | د | و |
|---|---|---|---|---|---|---|---|---|---|---|
| حروف رمزشده | ق | ش | گ | ب | ط | ص | غ | ح | گ | ه |

| کلمه رمز | ا | ت | ش |
|---|---|---|---|
| شماره حرف | ۱ | ۴ | ۱۶ |

بنابراین متن رمز شده عبارت است از: «قشگب طصغع گه».

در اینجا یک سؤال جالب این است که اگر متن رمز شده در اختیار فرد سوم یا یک دشمن قرار گیرد، چه‌طور می‌تواند متن اولیه را تشخیص دهد؟

مطمئناً با داشتن کلمهٔ رمز این کار بسیار راحت است، ولی بدون داشتن این کلمه کار رمزگشایی کمی سخت است. البته به کمک وسایل محاسباتی مانند رایانه این کار نیز آسان می‌شود که در این مختصر از روش رمزگشایی آن صرف‌نظر می‌کنیم.

در رمز جابه‌جایی به m و در روش دوم به کلمهٔ رمز، «کلید خصوصی» می‌گوییم که با داشتن آن‌ها کار رمزگشایی بسیار آسان خواهد بود. به‌نظر شما آیا روشی وجود دارد که کار رمزگشایی آن روزها یا سال‌ها به طول انجامد؟

جواب مثبت است و این رمزها در بانک‌ها و سازمان‌های نظامی و مخابراتی استفادهٔ زیادی دارند. برای مطالعهٔ بیشتر در این مورد، می‌توانید از منابعی که در زیر معرفی شده، استفاده کنید.

**مسئله:** جملهٔ زیر را با استفاده از یک کلمه، رمز کرده‌ایم:

ظپ ساسل فک چعاهض هلبق ثاکق قت فعحگه وح ختض هکقث صگ ظت بظ بص غع اغق ثظق گو تهث گلثمص صق عطب.

اگر کلمهٔ رمز از یک کلمهٔ سه حرفی و از متن زیر انتخاب شده باشد، این کلمه را بیابید و سپس متن اولیه را به کمک آن رمزگشایی کنید.

«چون عقل کامل گردد، سخن اندک باشد» حضرت علی(ع)

می‌توانید متن اصلی رمز شده را در صفحهٔ ۳۸ ببینید.

**منابع**

۱. بوخمان، جوهانز؛ **مقدمه‌ای بر رمزنگاری**، ترجمه دکتر مرتضی اسماعیلی، انتشارات دانشگاه اصفهان، چاپ دوم، سال ۱۳۸۷.

**2.** Stinson. Douglas. R, **Cryptography Theory and Practice**, CRC Press, 2008