مبانی رمزنگاری

امنیت داده‌ها چیزی نیست که فقط نگرانی شرکت‌های بزرگ باشد. به همه فایل‌هایی فکر کنید که دوست ندارید چشم نامحرم به آنها بیفتد. بسیاری از مردم ترجیح می‌دهند نامه‌های شخصی و پروژه‌های حساس‌شان در اینترنت محرمانه بماند، و تنها راه حفاظت عملی از آنها از طریق **رمزنگاری** (encryption) تحقق می‌یابد.

رمزنگاری چیست؟

نرم‌افزارهای رمزنگاری داده‌ها از الگوریتم‌های پیشرفته برای رمزی‌کردن محتویات یک فایل به گونه‌ای بهره می‌گیرند که هیچ کسی _ به جز کسانی که **کلید** درست را برای رمزگشایی دارند _ نتواند آنها را بخواند. الگوریتم‌های رمزنگاری یا الگوریتم‌های ریاضی هستند یا قواعد دیگری را روی فایل‌ها به کار می‌بندند، که به طور سیستمی محتویات آن فایل‌ها را تغییر می‌دهد. وقتی کودکان در کلاس درس می‌خواهند یک پیام رمزی را به هم بدهند، ممکن است از روش جایگزینی الفبایی بهره بگیرند، مثلاً به جای «الف» از «ب» ، و به جای «ب» از «پ» ، و مانند آن استفاده کنند. جابه‌جاکردن حروف، الگوریتم این نوع رمزنگاری است، و اگر کسی نداند که چند حرف جابه‌جا شده است یا چگونه حروف جابه‌جا شده‌اند نخواهد توانست که رمزگشایی کند. **رمزنگاری داده‌ها** ـ از هر نوع که باشد ـ به عمل پردازش یک پیام به وسیله الگوریتمی گفته می‌شود که آن پیام را درهم می‌ریزد، و نتیجه باید از طریق الگوریتم معکوس، پیام اولیه را بازگردانی کند.

کلیدها و الگوریتم‌ها

فناوری رمزنگاری مدرن به داده‌هایی مشهور به **کلید** (key) اتکا دارد. در روزگار باستان، یک نوار کاغذی را روی یک لوله بلند می‌پیچاندند و پیام خود را روی آن می‌نوشتند. پس از نوشتن پیام، نوار کاغذی را باز می‌کردند و به مقصد ارسال می‌کردند. نوار کاغذی در خارج از لوله، حاوی یک رشته حروفی تصادفی بود. گیرنده فقط وقتی می‌توانست پیام را بخواند که لوله‌ای دقیقاً به قطر لوله استفاده‌شده برای نوشتن پیام می‌داشت.

رمزنگاران امروز از **مقادیر کلیدی** به عنوان معادل لوله‌های رمزنگاری باستان بهره می‌گیرند. آنها از این کلیدها برای رمزنگاری و رمزگشایی بهره می‌گیرند.

لوله‌ای را تصور کنید که طول آن از زمین تا ماه باشد و قطر آن در نقاط بسیار زیادی از این طول تغییر کند، از اندازه تنه یک درخت تا قطر یک مداد. حالا می‌توانید دریابید که پیداکردن کلیدهای امروزی چقدر دشوار است.

پرسش: رمزنگاری (encrypt) یک فایل یا پیام یعنی چه؟

پاسخ: وقتی یک فایل را رمزنگاری می‌کنید، محتویات اصلی آن را به کُدی ترجمه می‌کنید که آن فایل را محرمانه نگه می‌دارد. نرم‌افزارهای رمزنگاری داده‌ها از الگوریتم‌های پیشرفته برای رمزنگاری محتویات یک فایل به گونه‌ای بهره می‌گیرند که توسط کسی که کلید درست را برای رمزگشایی ندارد قابل خواندن نباشد.

پرسش: رمزگشایی (decrypt) یک فایل یا پیام یعنی چه؟

پاسخ: رمزگشایی عکس رمزنگاری است. رمزگشایی داده‌ها یعنی برگرداندن یک فایل رمزی‌شده از طریق الگوریتم عکس به حالت اولیه فایل.

پرسش: <u>گواهینامه</u> (certificate) چیست؟

پاسخ: در رمزنگاری **کلید عمومی** (public key)، دو کلید متفاوت برای رمزنگاری و رمزگشایی اطلاعات به کار می‌رود. **کلید خصوصی** (private key) کلیدی است که فقط در اختیار صاحب آن است، در حالی که **کلید عمومی** مکمل آن را می‌توان در اختیار کامپیوترهای دیگر شبکه، کاربران دیگر، و سرویس‌های گوناگون قرار داد.

این دو کلید متفاوت هستند، اما در عمل مکمل یکدیگر هستند. به عنوان مثال، **کلید عمومی** یک کاربر می‌تواند در داخل یک **گواهینامه** در یک پوشه انتشار یابد به گونه‌ای که برای افراد دیگر یک سازمان قابل دستیابی باشد. فرستندهٔ پیام می‌تواند **گواهینامهٔ** آن کاربر را بازیابی کند، **کلید عمومی** را از گواهینامه بگیرد، و سپس پیام را با استفاده از **کلید عمومی** گیرنده رمزنگاری کند. اطلاعاتی که با **کلید عمومی** رمزنگاری می‌شود فقط با استفاده از **کلید خصوصی** متناظر با آن رمزگشایی می‌شود، که در اختیار صاحب آن گیرندهٔ پیام است.

یک **گواهینامهٔ کلید عمومی**، که معمولاً فقط **گواهینامه** نامیده می‌شود، حکمی است که به طور دیجیتال امضا شده است، و مقدار یک **کلید عمومی** را به هویت یک شخص، وسیله، یا سرویس پیوند می‌زند که صاحب و دارندهٔ **کلید خصوصی** متناظر با آن است. **گواهینامه‌ها** معمولاً حاوی اطلاعات زیر هستند:

- مقدار کلید عمومی صاحب گواهینامه
- اطلاعات معرفی صاحب گواهینامه، مانند نام و نشانی ایمیل.
- دورهٔ اعتبار گواهینامه (مدت زمانی که گواهینامه معتبر است).
- اطلاعات معرف صادرکننده.
- امضای دیجیتال صادرکننده.□