مباحثی در رمزنگاری ۲۶ شهریور ۱۳۹۱

جلسه‌ی ۱ : مقدمه

مدرس: شهرام خزائی *نگارنده: رضا بکتاش*

رمزنگاری از کلمه یونانی (Cryptography) به معنی نوشتن (graphein) پنهانی (crypto) گرفته شده است. هسته‌ی اصلی رمزنگاری ارتباط امن بین حداقل دو نفر می باشد. به این معنی که طرفین(باب و آلیس) پیام‌هایی ردوبدل می‌کنند که توسط دیگران قابل مشاهده است و هدف این است که پیام طوری نوشته شود که به جز طرفین ارتباط، کسی نتواند از محتوای آن اطلاعاتی کسب کند. باب و آلیس اولا باید بتوانند بر روی یک کلید (برای رمز کردن پیام) توافق کنند و ثانیا بتوانند یک ارتباط امن داشته باشند.

در این ارتباط از موارد زیر باید اطمینان داشته باشند:

- هیچ کس با دیدن پیام رمزی، نتواند بخش‌ای از پیام را حدس بزند.
- در صورتی که پیام تغییر کند، گیرنده پیام متوجه شود.

مورد اول محرمانه‌گی[۱] پیام و مورد دوم جامعیت[۲] پیام نامیده می‌شود.
به روش بالا «سیستم رمز با کلید مخفی»[۳] گفته می‌شود و در آن دو طرف بر سر یک کلید توافق می‌کنند و با استفاده از آن پیام‌های خود را تبدیل به رمز یا رمزگشایی می‌کنند.

رمزنگاری فقط به موارد بالا خلاصه نمی‌شود و کاربردهای زیادی دارد که از جمله آنها به چند مورد اشاره می‌کنیم:

- امضای دیجیتال[۴]: در دنیای واقعی امضای هرکس که پای مدارک مختلف نوشته می‌شود ثابت بوده و برای احراز هویت وی استفاده می‌شود. اما در دنیای دیجیتال، اگر امضا ثابت باشد، می‌توان امضای افراد را به دست آورد و از آن سوء استفاده کرد. برای همین، امضا را به صورت تابعی از پیام فرستاده شده می‌سازند تا امکان استفاده مجدد از آن نباشد.
- ارتباط با هویت مخفی[۵]: فرض کنید آلیس بخواهد از طریق اینترنت سوالی پزشکی از یک سرور بپرسد، طوری که سرور از هویت آلیس اطلاعی نداشته باشد. این ارتباط توسط چندین پروکسی انجام می‌شود که هریک پیام آلیس را رمز می‌کنند که در نهایت سرور پاسخ خود را برای آلیس می‌فرستد، بدون آن‌که بداند به چه کسی جواب می‌دهد.

---
[۱] Confidentiality
[۲] Integrity
[۳] private-key encryption scheme
[۴] digital signature
[۵] anonymous communication

- رای گیری[۶]: در یک رای‌گیری ممکن است رای‌دهنده‌ها نخواهند که رای آن‌ها برای دیگران مشخص شود و فقط در نتیجه اثر داشته باشد. می‌توان یک پروتکل طراحی کرد که آراء افراد را گرفته و فقط نتیجه را بیرون دهد و هیچ اطلاع اضافی از افراد رای‌دهنده بیرون ندهد.
- حراج مخفیانه[۷]: در برخی حراجی‌ها، کسی که بیشترین پیشنهاد را داده باشد برنده می‌شود و مبلغی که پرداخت می‌کند به اندازه‌ی دومین بیشترین پیشنهاد است. بنابراین ممکن است افراد برنده نخواهند مقدار پیشنهاد آنها مشخص باشد. در این مورد هم یک سیستم طراحی می‌شود تا افراد پیشنهادهای خود را به طور رمز شده به آن بدهند و فقط شخص برنده و مبلغ دومین بیشترین پیشنهاد محاسبه می‌شود و به صورت خروجی داده می‌شود.
- محاسبه امن برای چندین گروه[۸]: حالت کلی دو مثال قبل در این تعریف آورده شده است. در این‌جا معمولا یک محاسبه کننده‌ی قابل اطمینان طراحی می‌شود که مانند مثال رای گیری و حراج، ورودی‌های افراد مختلف را می‌گیرد و محاسبات خود را روی ورودی‌ها انجام داده و نتیجه امن را بیرون می‌دهد. حالت دیگری نیز وجود دارد که در آن محاسبه کننده‌ی قابل اطمینان نیاز نیست و افراد میتوانند در ارتباط با هم، ورودی‌های خود را به اشتراک بگذارند، بدون آنکه دیگران از آن‌ها اطلاعی کسب کنند.
- اثبات‌های دانش-صفر[۹]: فرض کنید در یک ارتباط دونفره، آلیس اطلاعاتی دارد که می‌خواهد وجود آنها را به باب ثابت کند، بدون آن‌که اطلاعات گفته شده را بروز دهد. به این نوع اثبات، اثبات دانش-صفر گفته می‌شود. رمز نگاری این امکان را فراهم می‌آورد تا چنین اثبات‌هایی را بتوان انجام داد.

در رمزنگاری سه مرحله برای هر مسئله وجود دارد:

۱- تهدیدی که متوجه پیام‌ها و اطلاعات ارسالی است، به طور واضح و صریح تعریف می‌شود. یعنی این‌که حمله‌کننده به چه اطلاعاتی می‌تواند حمله کند و هدف او از حمله چیست.

۲- ساختار سیستم رمز نوشته و پیاده‌سازی شود.

۳- اثبات شود که شکستن امنیت این سیستم رمز معادل با حل مسئله‌ای سخت است. به این ترتیب نشان داده خواهد شد که مسئله‌ی سخت به اندازه‌ای سخت است که در عمل، حل آن در زمان مطرح بودن این سیستم رمز، امکان ندارد و نتیجتاً سیستم رمز امنیت دارد.

[۶] election
[۷] anonymous auction
[۸] secure multiparty computation
[۹] zero-knowledge proofs