شماره ثبت: ۷۴۸۰
شماره شناسه ملی: ۱۰۸۶۰۱۶۶۳۲۶

آشنایی با مبانی رمزنگاری (۱)

گردآوری و نگارش:

محمدحسین محمدیان سرچشمه، شرکت پیشگامان کی‌پاد

mohammadian@kaipod.ir

چکیده:

در این مقاله، بخش اول مبانی رمزنگاری به طور اجمالی بیان شده است، این مباحث، شامل تعاریف و مفاهیم اساسی رمزنگاری، اصول کرکهف در سیستم‌های رمزنگاری، مفاهیم پنهان‌نگاری، رمزنگاری، کدگذاری و تفاوت آن‌ها می‌باشد.

۱. مقدمه

رمزنگاری (Cryptography)، علمی است که به بررسی و شناخت اصول و روش‌های انتقال یا ذخیرهٔ اطلاعات به صورت امن (Secure)، می‌پردازد. رمزنگاری، استفاده از روش‌های ریاضی (Mathematical Methods)، برای برقراری امنیت اطلاعات (Information Security) است. دراصل، رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است، به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی از اطلاعات رمز شده باشد و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد، نتواند به اطلاعات دسترسی پیدا کند. دانش رمزنگاری بر پایهٔ مقدمات بسیاری از قبیل تئوری اطلاعات، نظریهٔ اعداد و آمار و احتمال، بنا شده‌است و امروزه به طور خاص در حوزهٔ فناوری اطلاعات و ارتباطات (ICT) مورد بررسی و استفاده قرار می‌گیرد.

۲. مفاهیم و کلیات رمزنگاری

رمزنگاری (Cryptography) از دو کلمهٔ یونانی Kryptos به معنای پنهان، مخفی و Graphein به معنای نوشتن،نگارش، گرفته شده است. رمزنگاری عبارت است از یک نظام یا الگوی ریاضی و منطقی که بر اساس آن اطلاعات و مفاهیم آشکار و قابل فهم برای همگان، طبق روالی برگشت پذیر به اطلاعاتی نامفهوم و گنگ تبدیل می‌شود. این اطلاعات نامفهوم و گنگ توسط کسی که روال معکوس و پارامترهای لازم را می‌داند قابل برگشت و بهره برداری است. در ادامه به بیان اصول

شش‌گانهٔ کرکهف (Kerchoffs) که به ارائهٔ قوانین اساسی در رمزنگاری مدرن می‌پردازد، خواهیم پرداخت:

- سیستم رمزنگاری (Cryptosystem)، اگر نه به لحاظ تئوری، که در عمل غیرقابل شکست باشد.
- سیستم رمزنگاری باید هیچ نکتهٔ پنهان و محرمانه‌ای نداشته باشد بلکه تنها چیزی که باید سری و مخفی نگهداشته شود، کلید رمز (Cryptographic Key) است. (اصل اساسی کرکهف) طراح سیستم رمزنگاری نباید جزئیات سیستم خود را حتی از دشمنان مخفی نگهدارد.
- کلید رمز باید به‌گونه‌ای قابل انتخاب باشد که در ابتدا بتوان به‌راحتی آن را عوض کرد، به‌علاوه بتوان آن را به‌خاطر سپرد و نیازی به یادداشت کردن کلید رمز نباشد.
- متون رمزنگاری شده (Ciphertexts) باید از طریق خطوط تلگراف قابل مخابره باشند.
- دستگاه رمزنگاری یا اسناد رمزشده باید توسط یک نفر قابل حمل و نقل باشد.
- سیستم رمزنگاری باید به سهولت قابل راه‌اندازی و کاربری باشد، چنین سیستمی نباید به آموزش‌های مفصل و رعایت فهرست بزرگی از قواعد و دستورالعمل‌ها نیاز داشته باشد.

اگرچه تمام این قواعد به نحوی در دنیای رمزنگاری مورد استناد قرار گرفته‌اند؛ اما اصل دوم که تاکید می‌کند جزئیات الگوریتم‌های رمزنگاری باید آشکار و در دید عموم باشند و فقط کلیدهای رمز سری و محرمانه هستند، به اصل اساسی کرکهف شهرت یافته است. به تبعیت از همین اصل، جزئیات تمام الگوریتم‌های رمزنگاری کاملاً مشخص و در اختیار عموم قرار می‌گیرد. شاید یک تازه کار در دانش رمزنگاری را نتوان مجاب کرد که مخفی نگهداشتن جزئیات الگوریتم هیچ کمکی به نفوذناپذیری آن نمی‌کند ولی شاید استدلال‌های زیر عقلانیت نهفته در اصول کرکهف را روشن‌تر کند:

الف) هرگاه کلید رمز در اثر خیانت یا سهل انگاری و یا هر عامل دیگری لو برود، با تغییر کلید رمز جلوی ضرر گرفته می‌شود ولی افشای جزئیات یک سیستم و نفوذ در آن هیچ چیزی از سیستم باقی نمی‌گذارد و تنها راه تغییر سریع سیستم رمزنگاری است که این تغییر هرگز به راحتی و در زمان کوتاه میسر نخواهد بود.

ب) هرگاه روشی برای سال‌ها در معرض افکار پژوهشگران و متخصصان این فن باشد و به روش‌های علمی و عملی به چالش کشیده شود و هیچ تلاشی در شکستن آن به ثمر نرسد، می‌توان فقط احتمال داد که روش به‌قدر کافی محکم بوده است.

طبق اصل کرکهف، چون قرار نیست هیچ نکته‌ای در بطن الگوریتم رمزنگاری و روال معکوس آن (رمزگشایی) مخفی بماند، لذا در تمام الگوریتم‌های رمزنگاری، به پارامتری به‌نام "کلید رمز" یا (Cipher Key)، احتیاج است که با تغییر آن ماهیت گنگ و مبهم اطلاعات رمز شده به نحو غیرقابل پیش بینی تغییر می‌کند. لذا، می‌توان فرآیند رمزنگاری را تابعی دو متغیره مانند f از P و K، که دارای خروجی C می‌باشد، تصور کرد، در ادامه، به بیان این متغیرها می‌پردازیم:

- P پیامی است که باید رمزنگاری شود، P را متن آشکار یا (Plaintext) می‌گوییم.
- K پارامتری است که متن آشکار براساس مقدار آن به نحو غیرقابل پیش‌بینی و مبهم، درهم و بی معنی می‌شود. پارامتر K به "کلید رمز" شهرت دارد.
- C حاصل فرآیند رمزنگاری متن P با کلید K و تابع f، قطعه‌ای اطلاعات بی‌معنی، موسوم به "متن رمز" یا (Ciphertext) است.

به‌طور کلی عناصر مهمی که در رمزنگاری مورد استفاده قرار می‌گیرند به شرح زیر می‌باشد:

- متن آشکار (Plaintext): پیام و اطلاعات را در حالت اصلی و قبل از تبدیل شدن به حالت رمز، متن آشکار یا اختصاراً پیام می‌نامند. در این حالت، اطلاعات قابل فهم توسط انسان است.
- متن رمز (Ciphertext): به پیام و اطلاعات بعد از درآمدن به حالت رمز، گفته می‌شود. اطلاعات رمز شده توسط انسان قابل فهم نیست.

- رمزگذاری (رمز کردن) یا (Encryption): عملیاتی است که با استفاده از کلید رمز، پیام را به رمز تبدیل می‌کند.

- رمزگشایی (باز کردن رمز) یا (Decryption): عملیاتی است که با استفاده از کلید رمز، پیام رمز شده را به پیام اصلی باز می‌گرداند. از نظر ریاضی، این الگوریتم، عکس الگوریتم رمز کردن است.

- کلید رمز (Cipher Key): اطلاعاتی معمولاً عددی است که به عنوان پارامتر ورودی به الگوریتم رمز داده می‌شود و عملیات رمزگذاری و رمزگشایی با استفاده از آن انجام می‌گیرد. انواع مختلفی از کلیدهای رمز در رمزنگاری تعریف و استفاده می‌شود.

شماره ثبت: ۷۴۸۰
شماره شناسه ملی: ۱۰۸۶۰۱۶۶۳۲۶

۳. رمزنگاری (Cryptography)، پنهان‌نگاری (Steganography)، کدگذاری (Encoding)

در ادامه، به معرفی کلی اصطلاحات پنهان‌نگاری و کدگذاری و تفاوت آن‌ها با رمزنگاری می‌پردازیم. در رمزنگاری، وجود اطلاعات یا ارسال شدن پیام به هیچ وجه مخفی نمی‌باشد، بلکه ذخیره اطلاعات یا ارسال پیام مشخص است، اما تنها افراد مورد نظر می‌توانند اطلاعات اصلی را بازیابی کنند. بالعکس، در پنهان‌نگاری، اصل وجود اطلاعات یا ارسال پیام محرمانه، مخفی نگاه داشته می‌شود و غیر از طرف ارسال‌کننده و طرف دریافت‌کننده کسی از ارسال پیام آگاه نمی‌شود.

در رمزنگاری، محتویات یک متن به صورت حرف به حرف و در بعضی موارد بیت به بیت تغییر داده می‌شود و هدف تغییر محتوای متن است نه تغییر ساختار زبان‌شناختی آن. در مقابل، کدگذاری تبدیلی است که کلمه‌ای را با یک کلمه یا نماد دیگر جایگزین می‌کند و ساختار زبان‌شناختی متن را تغییر می‌دهد. به بیانی دیگر، در فرآیند کدگذاری، کلمات، نمادها و افعال موجود در ادبیات زبانی، با مقادیر مورد توافق تعویض می‌شوند، اما در رمزنگاری، دنباله‌ای از بیت‌ها یا بایت‌ها بدون توجه به محتویات زبان شناختی آن‌ها، طبق روالی معلوم و غیر سلیقه‌ای درهم و رمز می‌شود.

پنهان‌نگاری یا (Steganography)، هنر برقراری ارتباط پنهانی است و هدف آن پنهان کردن ارتباط به وسیله قرار دادن پیام در یک رسانه (Media) پوششی است به گونه‌ای که کمترین تغییر قابل کشف را در آن ایجاد نماید و نتوان موجودیت پیام پنهان در رسانه را حتی به صورت احتمالی آشکار ساخت. گاهی به جای کلمه پنهان‌نگاری از کلمه نهان‌نگاری یا الگوگذاری یا خفیه‌نگاری استفاده می‌گردد، اما عبارت درست و مصطلح آن همان پنهان‌نگاری است. تفاوت اصلی رمزنگاری و پنهان‌نگاری آن است که در رمزنگاری هدف اختفاء محتویات پیام است و نه به طور کلی وجود پیام، اما در پنهان‌نگاری هدف مخفی کردن هر گونه نشانه‌ای از وجود پیام است. در مواردی که تبادل اطلاعات رمز شده مشکل آفرین است باید وجود ارتباط پنهان گردد. به عنوان مثال، اگر شخصی به متن رمزنگاری شده‌ای دسترسی پیدا کند، به هر حال متوجه می‌شود که این متن حاوی پیام رمزی می‌باشد. اما، در پنهان‌نگاری، شخص سوم اصلاً از وجود پیام مخفی در متن اطلاعی حاصل نمی‌کند. در موارد حساس ابتدا متن را رمزنگاری کرده، آن‌گاه آن را در متن دیگری پنهان‌نگاری می‌کنند.

شماره ثبت: ۷۴۸۰
شماره شناسه ملی: ۱۰۸۶۰۱۶۶۳۲۶

منابع:

1. William Stallings, Cryptography and Network Security: Principles and Practice, 4th Edition, Prentice Hall.
2. http://en.wikipedia.org/wiki/Cryptography
3. http://en.wikipedia.org/wiki/Steganography
4. http://en.wikipedia.org/wiki/Coding_theory
۵. امنیت داده‌ها، دکتر علی ذاکرالحسینی، مهندس احسان ملکیان، انتشارات نص.