شبکه در اخبار

تهیه و تنظیم: سعید وحید

رمزبندیِ پیامها

پیامها و پرونده‌هایی که روی شبکهٔ اینترنت فرستاده می‌شود برای رسیدن به مقصد نهایی باید از چندین ایستگاهِ بینابینی عبور کنند. تمام ایستگاههای شبکه سطحِ امنیتی یکسانی ندارند: برخی از آنها کاملاً حفاظت‌شده هستند و نفوذ به آنها به‌سادگی امکان‌پذیر نیست، ولی تعدادی دیگر ممکن است چنین نباشند، یعنی افرادِ باهمارت که دارای سوءنیت یا مقاصد خرابکارانه باشند می‌توانند با کمی تلاش به چنین سیستمهایی نفوذ کنند و به‌اطلاعات موجود در آنها، از جمله پیامها و پرونده‌هایی که روی شبکه رد و بدل می‌شود، دسترسی یابند.

برای رفع این مشکل، روشهای مختلفی ابداع شده است که یکی از آنها استفاده از یک کامپیوترِ واسط بین کامپیوتر اصلی و شبکهٔ اینترنت است. این کامپیوترها که به دیوار آتش (firewall) موسوم‌اند حفاظت از کامپیوتر اصلی در مقابل نفوذ افراد غیرمجاز را به‌عهده می‌گیرند و در واقع چنین نفوذی را غیرممکن می‌سازند. به‌کارگیری دیوار آتش هزینهٔ زیادی به همراه دارد از این رو تمام ایستگاههای شبکه از آن استفاده نمی‌کنند. پس تا زمانی که تمام ایستگاههای شبکه به چنین سیستمی مجهز شوند باید به دنبال راه دیگری بود. روشی که از دیرباز برای حفاظت پیامها و نامه‌ها به‌کار می‌رفته رمزبندی (encryption) است. در این روش، پیام با استفاده از رمزی که نویسنده و همچنین گیرندهٔ پیام به آن دسترسی دارند تهیه می‌شود تا از دسترسی سایرین به محتوای آن جلوگیری شود. مشابه این روش در شبکهٔ اینترنت نیز ابداع شده است. استفاده از رمزبندی کامپیوتری، صرف‌نظر از کاربردهایی که در مکاتبات جدی ممکن است داشته باشد، سبب آشنایی جامعهٔ علمیِ کشور با شگردها و الگوریتمهای به‌کاررفته در این سیستم خواهد شد که خود بسیار مهم است.

سیستم رمزبندی رایج در اینترنت 'PGP' خوانده می‌شود که مخففِ کلماتِ pretty good privacy است. این سیستم در سال ۱۹۹۱ توسط فیلیپ زیمِرمَن ابداع شد. با استفاده از PGP می‌توان پیامها را به‌گونه‌ای رمزبندی کرد که فقط کسانی که نویسندهٔ پیام مد نظر دارد بتوانند آن را بخوانند. علاوه بر این، PGP امکان می‌دهد تا نویسنده، پیام خود را امضا کند. با استفاده از این امضای الکترونیک، گیرنده می‌تواند مطمئن باشد پیامی را که دریافت کرده واقعاً از جانب نویسنده است و کسی در بین راه آن را دستکاری نکرده است. روش رمزبندیِ PGP محبوبیت فراوانی یافته است که دلایل آن را می‌توان چنین برشمرد:

- بهترین الگوریتمهای رمزبندی (RSA، IDEA، و MD5) در آن به‌کار رفته است.
- این الگوریتمها در نرم‌افزاری گنجانده شده‌اند که روی اکثر سیستم‌عامل‌ها اجرا می‌شود و استفاده از آن نیز آسان است.
- این نرم‌افزار، مستنداتِ همراه آن و حتی متن برنامه (source code) به‌رایگان در اختیار همگان قرار دارد.

در نرم‌افزار PGP برای رمزبندیِ اطلاعات از کلیدهایی استفاده می‌شود که با استفاده از یک مولدِ اعدادِ تصادفی (random number generator) درست می‌شوند. این مولد از جنبهٔ رمزبندیِ داده‌ها بسیار قدرتمند است. هسته(seed)های مورد نیاز برای تولید اعدادِ تصادفی روی پرونده‌ای ذخیره می‌شود. هنگام تولید این پرونده از اعدادِکاملاً تصادفی، مانند فاصلهٔ زمانی بین فشردن کلیدها توسط کاربر، استفاده می‌شود. هر بار که این مولد اجرا می‌شود پروندهٔ حاوی هسته‌ها را با استفاده از منابعِ کاملاًتصادفی، مانند ساعت اجرا، بهنگام کرده هسته‌های جدیدی وارد آن می‌سازد.

الگوریتمهای به‌کارگرفته‌شده در PGP برای رمزبندی اطلاعاتْ ترکیبی از RSA و IDEAاست، به این ترتیب که برای رمزبندی کلیدها از الگوریتمِ RSA، و برای رمزبندیِ متنِ اصلی از الگوریتمِ IDEA ـبه خاطر سرعتِ زیادِ آن‌ـ استفاده می‌شود. اندازهٔ بلوک‌های متن معمولی (plaintext) و متنِ رمزبندی‌شده (ciphertext) در الگوریتمِ IDEA ۶۴ بیت است و در آن از کلیدهای ۱۲۸بیتی استفاده می‌شود. این الگوریتم بر اساس مفاهیمی در نظریهٔ گروهها بنا شده است. الگوریتم IDEA در سال ۱۹۹۰ در دانشگاه ETH زوریخ در سوئیس ارائه شد و از آن زمان تلاشهای زیادی برای شکستن رمزِ متنهای رمزبندی‌شده با IDEA در محافل دانشگاهی و نظامی در سراسر دنیا انجام گرفته که همه ناموفق بوده‌اند و این امر سبب شده تا اعتماد نسبت به این روش بیشتر شود. قبل از آن برای امتحانِ الگوریتمی موسوم به DES، یکی از پژوهشگران توانسته بود مداری را طراحی و آزمایش کند که می‌توانست در هر ثانیه ۵۰ میلیون کلید را حدس بزند. به گفتهٔ او ساخت این مدار با هزینهٔ ۱۰ دلار امکان‌پذیر بود و می‌شد با صرف یک‌میلیون دلار کامپیوتری ساخت که ۵۷,۰۰۰ عدد از این مدارها را در خود جای دهد. این کامپیوتر حداکثر در مدت ۷ ساعت (به‌طور متوسط ۳٫۵ ساعت) می‌توانست رمزهای DES را بگشاید. الگوریتم IDEA قوی‌تر از DES است و تا کنون روشی مشابهِ روش فوق برای شکستن رمزهای آن ارائه نشده است.

نرم‌افزار PGP قبل از رمزبندی متن، آن را فشرده (compress) می‌سازد، زیرا فشرده‌سازی بعد از رمزبندیْ عملی نیست. مزیت فشرده‌سازی در این است که مدت زمان ارسال اطلاعات روی خطوط ارتباطیْ کوتاهتر می‌شود و اطلاعاتِ فشرده جای کمتری را روی دیسک اشغال می‌کنند. مهمتر از همه اینکه فشرده‌سازیْ ضریب اطمینان رمزبندی را بیشتر می‌کند. بسیاری از روشهایی که برای شکستن رمز به‌کار می‌روند از افزونگی(redundancy)های موجود در متنِ اصلی برای کشف رمز استفاده می‌کنند؛ ولی وقتی که اطلاعاتْ فشرده شوند چنین افزونگیهایی در آنها وجود نخواهد داشت. روش فشرده‌سازی

که در PGP استفاده می‌شود 'ZIP' نام دارد و همان روشی است که در نسخهٔ ۲/۰ برنامه PKZIP نیز به‌کار رفته است. علت انتخاب ZIP این بوده است که جزئیات و متن کاملِ برنامه به‌رایگان در اختیار همگان قرار دارد و علاوه بر این از سرعت اجرا و ضریب فشرده‌سازی خوبی برخوردار است.

برای تولید امضای الکترونیک، PGP خلاصه‌ای از پیام (message digest) را رمزبندی کرده در انتهای متن قرار می‌دهد. خلاصهٔ پیام، یک بلوک ۱۲۸ بیتیِ فشرده‌شده و «تلخیص‌شده» از آن پیام است و شبیه مجموع مقابله‌ای (checksum) عمل می‌کند. (برای مثال، رقم سمت راست در ISBNِ کتابها مجموع مقابله‌ای است و برای کنترل درستیِ بقیه ارقام از آن استفاده می‌شود.) خلاصهٔ پیام را می‌توان به‌عنوان اثر انگشتِ پیام نیز در نظر گرفت، یعنی هر پیامْ اثر انگشتِ منحصر به فردِ خود را دارد و چنانچه متن پیام قبل از رسیدن به دست گیرندهٔ اصلی دستکاری شود، چون تطابق بین متن و امضا (اثر انگشت) از بین می‌رود گیرنده می‌تواند متوجه ایجاد تغییر شود. امضا فقط حاوی خلاصهٔ پیام نیست چرا که الگوریتمهای تولیدِ خلاصهٔ پیام در دسترس همگان قرار دارد، و بنابراین سارق اطلاعات به‌راحتی می‌تواند در متن پیام تغییر دهد و با تولید خلاصهٔ پیام جدید، آن را دوباره برای گیرندهٔ اصلی ارسال کند. برای امضای متن، باید کلمهٔ رمزِ امضاکننده نیز ارائه شود؛ بنابراین امکان ایجاد تغییر و قرار دادنِ امضای جدید منتفی می‌شود. در PGP از یک تابعِ درهم‌سازیِ یک‌سویه (one way hash function) برای تولید خلاصهٔ پیام استفاده می‌شود. بنابراین، از دیدگاه محاسباتی محال است کسی بتواند پیام اصلی را با پیام دیگری عوض کند که امضای هر دو یکسان باشد. الگوریتمی که در PGP برای تولید خلاصهٔ پیام به‌کار می‌رود 'MD5' نام دارد.

روش استفاده از PGP به این شکل است که هر استفاده‌کننده دو کلید دارد: کلید شخصی (secret key) و کلید همگانی (public key). کلید شخصی از دسترس دیگران دور نگه داشته می‌شود ولی کلید همگانی در اختیار کسانی که با نویسندهٔ پیام مکاتبه دارند گذاشته می‌شود. برای مثال، اگر دوستانتان بخواهند برای شما نامه‌ای بفرستند، قبل از ارسالْ آن را با کلیدِ همگانیِ شما رمزبندی می‌کنند و فقط کلید شخصی شماست که می‌تواند رمز آن پیام را بگشاید. اگر بخواهید پیامی را امضا کنید این کار را با استفاده از کلید شخصیِ خود انجام می‌دهید و دوستانتان می‌توانند با کمک کلید همگانیِ شما اطمینان پیدا کنند که نویسندهٔ واقعیِ آن پیامْ شما بوده‌اید.

نرم‌افزارِ PGP برای کاربردهای غیرتجاریْ رایگان است و روی اکثر سیستم‌عامل‌ها، مانند یونیکس، VAX، DOS، و غیره، می‌توان آن را اجرا کرد. اگرچه این نرم‌افزار یک راهنمای ۷۵صفحه‌ای دارد ولی استفاده از آن ساده است. نسخهٔ مخصوص سیستم‌عاملِ DOSِ نرم‌افزارِ PGP در کامپیوترِ «زاگرس» مرکز تحقیقات موجود است و با روش انتقال پرونده (ftp) از نشانی zagros.ipm.ac.ir می‌توان آن را دریافت کرد. این نرم‌افزار در کشو(directory)ی /pub/msdos/PGP و در پروندهٔ pgp262i.zip قرار دارد.

نخستین کاری که پس از نصب برنامه و مطالعهٔ پروندهٔ راهنما باید انجام دهید، تولید کلید شخصی و همگانی با استفاده از دستورِ pgp -kg است. اجرای این دستورات سبب می‌شود تا دو کلید و دو جاکلیدی (key-ring) درست شود. جاکلیدیِ همگانی‌ای که به این ترتیب ایجاد می‌شود محلی است که کلید همگانیِ دوستان و همکارانِ خود را در آن قرار خواهید داد. پس از آن باید نسخه‌ای از کلید همگانی خود را تهیه و برای دوستان و همکارانتان ارسال کنید. این کار را می‌توان با استفاده از دستور pgp -kxa انجام داد. برای مثال کلید همگانیِ نویسنده در انتهای مقاله آمده است.

وقتی دیگران کلید همگانی شما را دریافت می‌کنند باید آن را با دستورِ -ka به جاکلیدی خود اضافه کنند. پس از آنکه کلید همگانیِ شخصی را به جاکلیدیِ خود اضافه کردید می‌توانید برای او پیام رمزبندی‌شده بفرستید و همچنین امضای الکترونیکِ او در زیر نامه‌ها را تأیید کنید. فرض کنید کلید همگانیِ شخصی به نام «علی» را با دستور فوق به جاکلیدی خود اضافه کرده‌اید و اکنون می‌خواهید نامه‌ای را با استفاده از PGP رمزبندی کرده برای او بفرستید. اگر این نامه در پرونده‌ای به نامِ letter.doc باشد با اجرای دستور زیر می‌توان به‌هدف فوق رسید:

```
pgp -ea letter.doc
```

پرونده‌ای را که در نتیجهٔ اجرای این دستور ایجاد می‌شود می‌توان با پست الکترونیک برای علی فرستاد و او نیز می‌تواند آن را با استفاده از کلید شخصیِ خود رمزگشایی کرده بخواند.

اطلاعات بیشتر در مورد PGP از جمله نسخه‌های مخصوصِ سیستم‌عامل‌های گوناگون و متن برنامه را می‌توان از نشانیِ http://www.ifi.uio.no\u0161taalesc/PGP/home.html به‌دست آورد.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2i
mQBtAzAM9u0AAAEDAMh+P9Y0aVbjaKPYBEW 0nXM47wQ0eQTZsns4TyFVp2LTmcTr
qz0edGs7LEgyRb3DNnzJz4MZo539fLrXVnzG5km+ LZjgp8nE3GxFC7wQ6XQLuXMN
Uqx8jkmJf1c6qhfQfQAFEbQbU2FlZWQgVmFoaWQ gPHZhaGlkQGdwZy5jb20+
=00DV
-----END PGP PUBLIC KEY BLOCK-----
```