امروزه در شبکه‌های بی‌سیم به راحتی می توان علامت‌های رادیویی را استراق سمع کرد و حتی این عمل در شبکه‌های سیم دار نیز ممکن است. از این رو اطلاعات و سیگنال ها باید به گونه‌ای تنظیم و ارسال شوند که در صورت استراق سمع، کماکان محفوظ بمانند و به جز گیرنده، هیچ کس دیگری امکان فهمیدن این اطلاعات را نداشته باشد. در این میان، تنها با رمزنگاری اطلاعات می‌توان محتویات را محفوظ داشت. در حال حاضر تمامی دولت‌ها به این نکته و اهمیت آن در سیستم‌های اقتصادی، سیاسی و نظامی کشور واقف هستند.

هم اکنون با توجه به رشد روزافزون شبکه اینترنت، دغدغه حفظ حریم شخصی افراد نیز به این مقوله وارد شده و تمامی افراد مایل هستند که در زمان ارسال پیام، هیچ کسی جز گیرنده امکان متوجه شدن متن پیام را نداشته باشد و در عین حال گیرنده پیام نیز باید از شخص ارسال کننده مطمئن بوده و یقین پیدا کند که کس دیگری با شناسه مشترک، پیامی ارسال نکرده است. در ابتدای امر، شرکت‌ها سعی داشتند برای این منظور سیستم‌های امنیتی و شبکه‌های ضد نفوذی را طراحی کنند، اما هر کدام تنها برای مدت کوتاهی کارآیی داشت و پس از آن راه نفوذ به سیستم، کشف و اطلاعات به سرقت برده می‌شد.

در زمینه رمز نگاری، سیستم های مختلفی وجود دارد که جایگزینی کاراکترها از جمله ساده‌ترین آنها است؛ به این معنا که به ازای هر حرف، حرف دیگری را جایگزین کنیم. این سیستم بسیار راحت رمزگشایی می‌شود و هر کسی که بتواند آن را رمز کند، به راحتی نیز از رمز خارج می کند.

اما سیستم رمز نگاری باید طوری باشد که رمزگشایی آن مشکل باشد. در این بین، دو سیستم با نام‌های DES و RSA وجود دارد که در این مقاله به آنها و به‌ویژه RSA خواهیم پرداخت.

سیستم DES

از اوائل دهه هفتاد، دولت فدرال امریکا و شرکت آی‌بی‌ام (IBM) مشترکا روشی را برای رمزنگاری داده‌ها ابداع کردند که به عنوان استانداردی برای نگهداری اسناد محرمانه دولتی مورد استفاده قرار گرفت. این استاندارد که Encryption Standard (Data DES نام گرفت، امروزه محبوبیت خود را از دست داده است.

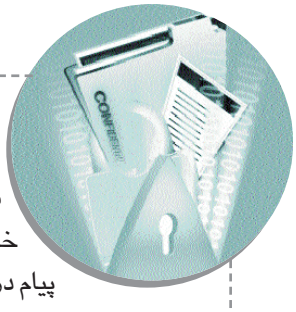
ورودی رمزنگار یک رشته ۶۴ بیتی است، بنابراین متنی که باید رمز شود در گروه‌های هشت کاراکتری دسته‌بندی می‌شود. اولین عملی که بر روی رشته ورودی ۶۴ بیتی انجام می‌شود، جابه‌جا کردن محل بیت‌های رشته ۶۴ بیتی است که این عمل طبق یک جدول جایگشتی انجام می گیرد و به آن جایگشت مقدماتی گفته می‌شود.

سپس رشته ۶۴ بیتی، از وسط تقسیم و به ۲ رشته ۳۲ بیتی چپ و راست تبدیل شده و در مرحله بعدی، قسمت چپ و راست جایش عوض می شود. پس از آن، از طریق یک جدول عملیاتی در ۱۶ مرحله، محاسبات تابعی XOR صورت می‌گیرد که در هر یک از این ۱۶ مرحله، کلمه‌ای به عنوان کلید رمز حاصل می‌شود. در

مرحله آخـر مجددا جـای چپ و راست رشته‌های ۳۲ بیتی جابه‌جا می‌شود.
در این سیستم یک رشته ۵۶ بیتی وجود دارد که به اصطلاح، رمزنگاری با قدرت ۵۶ بیت گفته می‌شود و حاوی ۱۶ کلید رمز است؛ اما برای رمزگشایی تنها به یکی از کلیدها احتیاج داریم. استفاده از هر بلوک ۸ کاراکتری برای رمز نگاری بلوک بعدی و رمز نگاری مجدد بلوک قبلی و این گونه تکرار بلوک‌ها، کار را برای رمز شکن‌های سیستم DES ساده‌تر می‌کند. نکته خاص آن است که چـون کلید رمزنگاری و رمزگشایی، هر دو یکی است، لذا باید از کلید شدیدا حفاظت شود.
این الگوی رمز نگاری به عنوان استانداردی برای اسناد حساس فدرال امریکا پذیرفته شد تا آنکه در سال ۱۹۷۷ یکی از محققان دانشگـاه استانفورد (Stanford) با هزینـه‌ای معادل ۲۰ میلیون دلار ماشینی را طراحی کرد که در عرض ۲۴ ساعت می‌توانست رمز DES را بشکند. بعد از آن ایده‌های جدیدی برای رمزنگاری مطرح شد که عملا DES را کنار زد.
به کلید این سیستم که برای رمزنگاری و رمزگشایی یکسان است، «کلید مشترک» گفته می‌شود. در این میان سیستم‌هایی نظیر Triple-DES با قدرت ۱۱۲ بیت و IDEA با قدرت ۱۲۸ بیت نیز وجود دارند.

سیستم RSA

در هـر یک از الگوهـای رمزنگاری ذکر شده، لازم است کـه فرستنده و گیرنده پیام، کلید رمز را بدانند. وقتی فرستنده پیام از کلیدی برای رمزنگاری استفاده می‌کند و گیرندگـان هم از همان کلید برای رمزگشایی بهره می برند، افشا شدن کلید رمز توسط یکی از گیرندگان پیام، امنیت را به خطر می اندازد. در الگوی جدیـد رمزنگاری، برای حل مشکل از دو کلید متفاوت استفاده می‌شود: یکی برای رمزنگاری و دیگری برای رمزگشایی که از هیچ یک نیز نمی‌توان به جـای دیگـری استفاده کرد؛ همچنین کشف کلید رمز دوم با داشتن یک کلید بسیار مشکل و غیر ممکن است.
به کلیـد و یا کلمه رمـزی که از آن برای رمزنگـاری استفـاده می‌کنیم، «کلید عمومی» و از کلیدی که برای رمز گشایی استفاده می کنیم، «کلید خصوصی» گفته می شود.
در این سیستم مبنای رمزنگاری استفاده از اعداد اول در ریاضیات است. همانطور که می‌دانید اعداد اول، به جز خودشان و یک به هیچ عدد دیگری تقسیم‌پذیر نیستنـد و بـه علاوه، تا بی‌نهایت ادامه دارند.
در این سیستم، دو عـدد اول انتخاب و آنها را در یکدیگر ضرب می کنیم و از حاصلضرب آنها در استفاده از کلید خصوصی و کلید عمومی بهره می‌بریم. نکته قابل توجهی که باعث شده این سیستم دارای امنیت بسیـار بالایی باشد، آن است کـه امکان فاکتورگیـری از عددی که حاصلضرب دو عـدد اول بـوده و سپس تجزیه آن به دو عدد اول، بسیار مشکل است.
به عنوان مثال، اعداد ۳ و ۵ را در نظر بگیرید که هر دو عدد اول هستند و حاصلضرب آنها ۱۵ است. حال می‌خواهید عدد ۱۵ را به دو عدد اول تجزیه کنید. این کار در مورد چنین عددی زیاد مشکل نیست؛ اما اگر به‌جای ۱۵ یک عدد ۲۰۰ رقمی داشتید چطور؟ با توجه به احتمالات و بی نهایت بودن تعداد اعداد اول، امکان اینکه دو کامپیوتر از دو عدد اول یکسـان بـرای رمزنگـاری استفاده کنند، بسیار پایین و حتی غیر محتمل است، پس برخلاف ادعای برخی مخالفان، احتمال حدس زدن کلید خصوصی رمز بنا به تشابهی که ممکن است بـا سیستم دیگری داشته باشد، غیـرممکـن است. (چه طور احتمال دارد دو سیستـم به طور تصادفی از دو عدد اول ۷۰ رقمی یکسان برای سیستم رمزخود بهره بگیرند؟!)
در این سیستم افراد زیادی به کلید عمومی دسترسی دارند و با استفاده از آن می توانند پیام‌های خود را برای شخص خاصی رمزنگاری کنند. شخص گیرنده، با استفاده از کلید خصوصی که صرفـا در اختیار خـودش است، متن را از حالت رمز خارج می‌کند. در این میان در صورت استراق سمع شبکه، حتی با در دست داشتن کلید عمومی، خارج کردن پیام از رمز غیر ممکن است و صرفا باید به کلید خصوصی دسترسی داشت.
در این میان تنها کافـی است کـه افراد کلید عمومی دوستان، آشنایان و همکاران را بدانند و پیام ها را برای هر یک، با کلید عمومی رمزنگاری کرده و ارسال کنند و مطمئن باشند که هیچ کسی جز گیرنده پیام (کسی که کلیـد خصوصی را در اختیار دارد) قادر به رمز گشایی آن نیست.
حال در صورت عدم دسترسی به کلید عمومی طرف مقابل و یا در صورتی که اگر قصد ارسال پیام به چندین نفر را داشتید، می توانید پیامتان را با استفاده از کلید خصوصی خودتان به رمـز درآوریـد و در مقـابل شخص و یا اشخاص گیرنـده با استفاده از کلید عمومـی، آن را از رمز خـارج کنند. در این میان گیرندگان مطمئن خواهند بود که شخص ارسال کننده شما بوده‌اید و شما نیز نمی توانید منکر ارسال چنین پیامی شوید، زیرا شخص دیگری به کلید خصوصی دسترسی نداشته است.
حتی اگر پیام مورد استراق سمع قرار گیرد، در صورت داشتن کلید عمومی قابل رمزگشایی است ولی اگر کوچک‌ترین تغییری



در آن داده شـود، دریافت کنندگـان اصلی متوجه می‌شوند زیرا که دیگر به شکل درستی بـا کلید عمومی از رمز خارج نمی‌شود و می‌تـوان فهمید که متن پیام در میان راه تغییر کرده است.

اما اعداد اول و حاصلضـرب آنها چقدر باید بزرگ باشند تا تابع یکطرفه موثری ایجاد شود؟ مفهوم رمز کردن با کلید عمومی را ویتفیلد دیفی(Whitfield Diffie) و مارتین هلمن(Martin Hellman) در سـال ۱۹۷۷ اختـراع کردنـد. پس از آن گـروه دیگری از دانشمنـدان علوم کامپیوتر، یعنی ران ریوست (Ran Rivest)، شمیر (Shmir) و لئونارد ادلمن(Leonard Adelman) با استفاده از سیستم فاکتور کردن اعداد اول تئوری دیگری را عنوان کردند که به آن، سیستم RSA (مخفف نام خانوادگی آنها) می‌گویند. آنها ادعا کردند که میلیون‌ها سال طول می کشد تا یک عدد ۱۳۰ رقمی حاصلضرب دو عدد اول، از رمز خارج شود و این بدون در نظر گرفتن مقدار نیروی محاسباتی است که برای این کار مورد استفاده قرار می گیرد. برای اثبات این امر، آنها از همه مردم دنیا خواستند تا دو فاکتور یک عدد ۱۲۹ رقمی را که در بین مردم به RSA 129 معروف است، پیدا کنند.

آنها اطمینان داشتند کـه پیـام رمز شده با استفاده از این عدد به جای کلید عمومی، برای همیشه امن خواهد بود، ولی آنها پیش‌بینی نمی‌کردند کـه تاثیرات قانون مور بتواند کامپیوترها را قدرتمندتـر سازد. در سال ۱۹۹۳، بیش از ۶۰۰ دانشمنـد و متخصص و افراد آماتور از سرتاسر جهان گرد هم آمدند و شروع به کار روی عدد ۱۲۹ رقمی کردنـد. در کمتر از یک سال، آنها توانستند آن عدد را به دو عـدد اول ۶۴ رقمی و ۶۵ رقمی تقسیم کنند. پیام رمز گشایی شده، این بـود: «واژه های سحر آمیز، نازک طبع و استخوانی اند.»

افزودن فقط چند رقم به کلید، شکستن رمز آن را بسیار مشکل‌تر می کند. به طوری که بنا به نظر ریاضی‌دانان، در حال حاضر شکستن یک کلید عمومی ۲۵۰ رقمی، غیر ممکن است.

قدرت سیستم RSA نیز مانند سیستم DES با واحد بیت محاسبه می‌شود، با این تفاوت که به دلیل محدود نبودن تعداد اعداد اول و همچنین تعداد ارقام آن و در نتیجه مقدار حاصلضرب آنها، این سیستم می‌تواند بـا هر توانایی، ارائـه و استفـاده شود. درحال حاضر، سایت‌های اینترنتی و پروتکل SSL از رمزنگاری ۱۲۸ بیتی آن استفاده می‌کنند. البته استفاده از مقادیر بالاتر نیز امکان‌پذیـر است و صرفـا زمان بیشتـری را بـرای محاسبه رمزنگاری و رمزگشایی به همراه دارد، اما شکستن رمز آن همانطور که در نمونه RSA129 نیز ذکر شد، بسیار مشکل است. همچنین لازم به ذکر است که افراد و شرکت ها و سازمان هایی که از هر گونه سیستم رمز استفاده می‌کنند، برای افزایش امنیت، رمز خود را دائم تعویض می کنند.

نحوه محاسبات در سیستم RSA

ابتدا کل پیام را بـه K بلوک تقسیم می‌کنیم. در ایـن سیستم، برخلاف سیستم DES هیچ گونـه محدودیتی در نوع بلوک‌ها وجـود نـدارد و می‌توان بلوک‌هـای یک کاراکتری یا چند کاراکتری را انتخاب کرد. سپس بر یک مبنای مشخص مانند اسکی (ASCII) و یا یونی کد (UNICODE)، بلوک‌ها را به معادل عددی آنها تبدیل می‌کنیم و نام آن را Pi می گذاریم.

به عنوان مثال، رشته M= IDESOFMARCH را در نظر بگیریـد، در جدول ۱ آن را به بلوک‌های ۲ کاراکتری و سپس معادل‌های عددی تقسیم کردیم.

سپس دو عدد اول انتخاب کرده و آنها را p و q می‌نامیم. پس از آن مقادیر n و z را طبق روابط زیر محاسبه می کنیم:

$$n = p \times q$$

$$z = (p - 1)(q - 1)$$

حال عددی مانند d را به گونه‌ای انتخاب می کنیم که نسبت به z اول باشد، یعنی هیچ عامل مشترکی که هر دو بر آن بخش پذیر باشند، نداشته باشد.

براساس d، عدد e را به گونه‌ای انتخاب می‌کنیم تا رابطه زیر برقرار باشد:

$$(e * d) \bmod z = 1$$

(عبارت mod، به معنای باقیمانده تقسیم است.)

نکته‌ای که باید رعایت شود، آن است که کدهای P_i نسبت داده شده به هر بلوک باید کوچک‌تر از n باشد.

حال طبق رابطه زیر مقادیر Pi را به Ci تبدیل می کنیم:

$$C_i = (P_i)^e \bmod n$$

رشته اصلی به بلوک‌های ۲ کاراکتری	HX	RC	MA	OF	ES	ID
تبدیل بلوک به عدد صحیح	0723	1702	1200	1405	0418	0803
بلوک های جدید عددی	P_6	P_5	P_4	P_3	P_2	P_1

جدول ۱

ادامه از صفحه ۱۳

اکنون می‌توان این مقادیر C_i را که در حقیقت مقادیر رمز شده در سیستم RSA هستند، به جای مقادیر اصلی ارسال کرد.
برای رمزگشایی نیز کافی است که مقادیر C_i را طبق رابطه زیر به حالت اولیه خود برگردانید:

$$P_i = (C_i)^d \bmod n$$

در این صورت کلید عمومی و کلید خصوصی به صورت ذیل تعریف می شود:

Public Key = (e,n)

Private Key = (d,n)

همانطور که مشاهده شد رمزنگاری و رمزگشایی با دو عدد مختلف e و d انجام می گیرد که محاسبه هر یک بدون داشتن p و q (همان دو عدد اول) غیر ممکن است و برای محاسبه آن دو عدد اول، باید از n فاکتور گیری کرد. پس می توان مطمئن بود که با داشتن کلید عمومی که اطلاعات را رمز می کند، نمی توان اطلاعات را رمز گشایی کرد و از این رو احتیاجی به مراقبت ندارد و می‌توان برای دریافت پیام‌های رمز شده، آن را در اختیار همگان قرار داد.
البته برای به توان رساندن اعداد بالا توسط کامپیوتر مدت زمان نسبتا طولانی صرف می‌شود، به همین دلیل با استفاده از فرمول‌های پیچیده‌تری به عنوان مکمل، عمل توان را با مراحل کمتر و در نتیجه سریع‌تر، انجام می‌دهند.

زمان محاسبه	تعداد ارقام
۴ ساعت	۵۰
۱۰۴ روز	۷۵
۷۴ سال	۱۰۰
۴ میلیون سال	۲۰۰
۵×۱۰^{۱۵} سال	۳۰۰
۴×۱۰^{۲۵} سال	۵۰۰

جدول ۲

قدرت سیستم RSA

در ادامه به شکستن رمز این سیستم، یعنی مدت زمان مورد نیاز برای فاکتورگیری از n می‌پردازیم. فرض کنید کامپیوتری هر عمل را در یک میکرو ثانیه انجام بدهد، جدول ۲ زمان تجزیه یک عدد را به عوامل اول بر حسب تعداد ارقام عدد مشخص کرده است.
گرچه تحقیق بر روی تجزیه اعداد به عوامل اول ادامه دارد ولی هنوز هیچ الگوریتم کارآمدی که بتواند زمان‌های جدول ۲ را کاهش دهد، پیدا نشده است و از این رو در حال حاضر قوی‌ترین، ساده‌ترین و ایمن ترین سیستم رمزنگاری به شمار می رود.

دارای ۲۵ تا ۳۵ کلمه بوده، مگر اینکه حاوی نقل قول و یا تصویر باشد. نوشته‌های طولانی علاوه بر دشواری در خواندن (در صورت استفاده از پویانمایی) نیاز به کلیک‌های بیشتری برای نمایش هر اسلاید دارند.

- هر یک از زیر مجموعه‌های مشخص شده با دایره باید حاوی یک عبارت قابل فهم باشد. جملات طولانی و توصیفی را باید به همراه نمایش اسلاید، به صورت شفاهی بیان کرد. جملات اسلاید علاوه بر القای احساس و تفکر شما در زمان ارائه، باید برای مخاطبان غایبی که بعدا فایل ارائه شما را مشاهده خواهند کرد، مناسب و به اندازه کافی گویا باشد.
- از تصاویر متناسب با موضوع استفاده کنید. یک ایده مناسب ایجاد فاصله بین نوشته‌های اسلاید توسط تصاویر است. یک تصویر خوب می‌تواند معادل هزاران کلمه برای مخاطبان مطلب داشته باشد. برای این منظور می‌توانید از تصاویر آماده موجود در PowerPoint و یا از تصاویر رایگان موجود در وب استفاده کنید؛ البته تصاویر کارتونی توجه بیشتری به خود جلب می کنند ولی باید متناسب با موضوع مورد نظر انتخاب شوند. استفاده از تصاویر و تیترهای روزنامه‌ها نیز ایده مناسبی است.
- اسلاید یکی مانده به آخر باید حاوی جمع‌بندی مطالب ارائه شده باشد. به همین دلیل باید خلاصه عقاید و نکات مهم سخنرانی را پوشش دهد. فراموش نکنید که در این اسلاید از کلمات و عبارات به کار رفته در اسلاید دوم استفاده نکرده و از جملات و عبارات جذاب دیگری بهره ببرید.
- اسلاید نهایی حاوی آدرس منابع مطالعاتی بیشتر درباره سخنرانی شما است. به علاوه این صفحه می‌تواند شامل آدرس‌های وب و یا آدرس وب‌سایت و یا وب‌لاگ شخصی شما و موارد مشابه آن باشد. آدرس پست الکترونیک و صندوق پستی خود را نیز در همین صفحه بیاورید (برخی به اشتباه آن را در صفحه اول می آورند).
- بهتر است یک نسخه چاپی از اسلایدهای خود را قبل از شروع ارائه مطلب به شنوندگان ارائه کنید. البته این کار را به مجریان برنامه محول کنید، زیرا ممکن است آنها بخواهند مطالب شما را به همراه سایر موارد دیگر در یک مجموعه به شنوندگان ارائه کنند.

در شماره‌های بعد، نکات بیشتر و مهم‌تری درباره شیوه‌های ارائه مطلب خواهید آموخت.