پنجمین کنفرانس بین المللی انجمن رمز ایران در تهران برگزار شد

پیامی برای خوانده نشدن

نخستین بار ژولیوس سزار، امپراتور روم باستان برای آن‌که بتواند بدون اطلاع دشمن با ارتشش در سراسر قلمروش در ارتباط باشد، نوعی رمز را به کار گرفت. رمز سزار به این شکل بود که برای فرستادن یک پیام، جای هر حرف را با سومین حرف پس از آن در الفبا عوض می‌کرد؛ مثلا به جای حرف A حرف D و به جای حرف X حرف A را قرار می‌داد؛ بنابراین برای از کد خارج‌کردن پیام، گیرنده آن باید ساختار رمز را می‌دانست و جای هر حرف را با سومین حرف پس از آن در الفبا عوض می‌کرد. با گذشت زمان، علم رمزنگاری هم پیشرفت‌های بسیاری داشت. با پدید آمدن رایانه‌ها و افزایش قدرت محاسباتی آنها، دانش رمزنگاری وارد حوزه گسترده‌تری شد و هنوز هم درخشان‌ترین مغزهای این سرزمین وقت عمده‌ای را در این شاخه مهم دانش سپری می‌کنند.

بنفشه رحمانی

عکس: corbis

رمزنگاری، علم کدها و رمزهاست. وقتی با امنیت اطلاعات سر و کار داریم باید هویت فرستنده و گیرنده پیغام را اثبات کنیم و از تغییرنکردن محتوای پیغام مطمئن شویم. در این میان باید تضمین شود یک پیغام فقط توسط کسانی که پیام برای آنها ارسال شده، قابل خواندن است. در رمزنگاری، به پیام و اطلاعات در حالت اصلی و قبل از تبدیل شدن به رمز، متن آشکار یا به اختصار پیام می گویند. در این حالت، اطلاعات برای انسان قابل فهم است. همین اطلاعات وقتی به حالت رمز درآیند به آن متن رمز گفته می شود. رمزگذاری یا رمز کردن، عملیات تبدیل پیام به رمز با استفاده از کلید رمز است و رمزگشایی عکس این عمل را انجام می دهد؛ یعنی در رمزگشایی با استفاده از کلید رمز، پیام رمز شده به پیام اصلی باز می گردد.

پنجمین کنفرانس انجمن رمز ایران، برای اولین بار در گستره بین المللی با هدف گردهمایی متخصصان و علاقه مندان حوزه امنیت اطلاعات و ارتباطات و رمز در زمینه های علمی و کاربردی ۱۶ و ۱۷ مهرماه در دانشگاه صنعتی مالک اشتر برگزار شد. هدف از برگزاری این کنفرانس، شناسایی خبرگان و متخصصان حوزه امنیت اطلاعات و رمز، تعامل و ارتباط با صنعت در حوزه های مرتبط، امکان معرفی جدیدترین دستاوردهای علمی و کاربردی در زمینه امنیت و رمز و فراهم کردن بستری برای ارائه دستاوردهای مرتبط بود. سخنرانی های علمی، ارائه مقاله های مرتبط، میزگردهای تخصصی، کارگاه‌های آموزشی، مسابقه و نمایشگاه، بخش های اصلی این کنفرانس ۲ روزه بودند. از این همایش ـ که با حضور وزیر ارتباطات و فناوری اطلاعات و جانشین وزیر دفاع برگزار شد ـ وزارت ICT، وزارت دفاع، وزارت امورخارجه، بانک مرکزی جمهوری اسلامی ایران، مرکز پژوهش های مجلس، موسسه آموزشی و تحقیقاتی صنایع دفاع، دانشگاه صنعتی شریف و دانشگاه صنعتی امیرکبیر حمایت می کردند. دکتر مرتضی براری، دبیر پنجمین کنفرانس انجمن رمز ایران یکی از هدف های برگزاری این کنفرانس را شناسایی موسسات فعال این حوزه و معرفی قابلیت های آنها معرفی کرد: ارائه نیازمندی های دستگاه های اجرایی در حوزه امنیت و هم اندیشی و ارتقای علمی و کاربردی مباحث امنیت و رمز از هدف های مهمی است که در این همایش دنبال شد.

به گفته دکتر براری، از میان ۲۳۰ مقاله ای که به دبیرخانه همایش ارسال شده است، ۵۵ مقاله به کنفرانس راه یافته و ارائه شدند. همه این مقالات در حوزه رمز و امنیت بودند. در این همایش، رقابتی میان مقاله های ارائه شده وجود نداشت و هیچ مقاله ای به عنوان مقاله برتر انتخاب نشد.

کارگاه‌های رمزی

در کنار همایش ۲ روزه انجمن رمز، ۱۱ عنوان کارگاه آموزشی مرتبط هم برگزار شد که زمان برپایی آنها پیش از آغاز کنفرانس بود. این کارگاه‌ها روزهای ۱۳، ۱۴ و ۱۵ مهر در دانشگاه صنعتی مالک اشتر برپا شدند و مدت هر کدام ۴ تا ۶ ساعت بود.

کارگاه سیستم های تشخیص و ممانعت از نفوذ از تئوری تا عمل، امنیت نرم افزار، نحوه پیاده سازی موثر الگوریتم های رمز و کاربرد الگوریتم های هوشمند در رمزنگاری، امنیت وب، امنیت در ابر رایانه ها و مسائل حقوقی امنیت در فضای سایبر، برخی کارگاه هایی است که در این ۳ روز برپا شده اند.

الگوریتم‌های رمزنگاری

یکی از مهم ترین مباحث در مقوله رمزنگاری و امنیت، الگوریتم های مورد استفاده در این حوزه است. طراحان سیستم هایی که در آنها از رمزنگاری استفاده می شود، باید از نقاط قوت و ضعف الگوریتم های موجود مطلع باشند و الگوریتم مناسب را تعیین کنند. اگرچه رمزنگاری نسبت به گذشته پیشرفت های بسیاری داشته، ولی کشف رمز نیز پابه‌پای رمزنگاری پیش آمده است و الگوریتم های کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند. به همین دلیل، تعداد الگوریتم هایی که در سیستم های رایانه‌ای عملی و سیستم های برپایه کارت هوشمند استفاده می شوند، بسیار کم است.

اصطلاح الگوریتم رمزنگاری یک مفهوم جامع است و لازم نیست هر الگوریتم از این دسته به شکل مستقیم برای رمزگذاری اطلاعات استفاده شود، بلکه وجود کاربرد مربوط به رمزنگاری مورد نظر است.

در گذشته، سازمان ها و شرکت هایی که نیاز به رمزنگاری داشتند، الگوریتم رمزنگاری منحصر به فردی طراحی می کردند. با گذشت زمان مشخص شد گاهی ضعف های امنیتی بزرگی در این الگوریتم ها وجود دارد که موجب سهولت شکسته شدن رمز می شود. به همین دلیل امروزه رمزنگاری مبتنی بر پنهان نگاه داشتن الگوریتم رمزنگاری، منسوخ شده و در روش های جدید رمزنگاری، فرض بر این است که اطلاعات کامل الگوریتم رمزنگاری منتشر شده و آنچه پنهان نگاه داشته می شود، فقط کلید رمز است؛ بنابراین تمام امنیت حاصل شده از الگوریتم ها و پروتکل های رمزنگاری استاندارد، متکی به امنیت و پنهان ماندن کلید رمز است و جزئیات کامل این الگوریتم ها و پروتکل ها برای همه منتشر می شود.

کلید می تواند متقارن یا نامتقارن باشد. در سیستم های کلید متقارن، از یک کلید برای رمزنگاری و رمزگشایی استفاده می شود، ولی در سیستم های کلید نامتقارن از کلیدهای مختلف برای رمزنگاری و رمزگشایی بهره می برند.

بعضی از کلیدهای متقارن ـ امروزه ـ در عرض چند ساعت توسط رایانه های معمولی شکسته می شوند، بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شوند، در حالی که سیستم های کلید نامتقارن امنیت بیشتری برای حفظ اطلاعات دارند. در بعضی از این سیستم ها فرستنده پیام، متن را با کلید عمومی گیرنده کد کرده و گیرنده آن را با کلید اختصاصی خود رمزنگاری می کند.

به عبارتی، تنها با کلید اختصاصی گیرنده می توان متن کدشده را به متن اولیه صحیح تبدیل کرد؛ یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است، ولی نمی تواند از متن کد شده به متن اصلی دست یابد. به این ترتیب پیام کد شده برای هر گیرنده‌ای بجز گیرنده مورد نظر فرستنده بی معنی خواهد بود.

زمانی برای رقابت

یکی از بخش های پنجمین کنفرانس بین المللی انجمن رمز ایران که هنوز هم به پایان نرسیده، مسابقه است. این مسابقه ها در ۲ نوع شنود و نفوذ اجرا شده که به دلیل پیچیدگی های زیاد و سختی مسابقه ها، رقابت همچنان بین شرکت کنندگان وجود دارد و برنده ها هنوز اعلام نشده اند، هدف از مسابقه شنود، شنود ترافیک رمز شده بین ۲ سیستم با کمک سوئیچ است. به این ترتیب که یک نود ارتباطی روی سوئیچ قرار می گیرد و داوطلبان باید دریافت و تحلیل ترافیک را طی ۳ مرحله انجام دهند: ۱ـ شنود ترافیک سوئیچ با قرار دادن سوئیچ در حالت قابل شنود ۲ـ جمع آوری و تحلیل ترافیک شبکه ۳ـ رمزگشایی ترافیک جمع آوری شده و به دست آوردن بسته های رمز شده.

در روش‌های جدید رمزنگاری، فرض بر این است که اطلاعات کامل الگوریتم رمزنگاری منتشر شده وآنچه‌پنهان نگاه داشته می‌شود فقط کلید رمز است

داوری با تایید ۲ داور فنی انجام می شود و در صورتی که نتایج مشابه حاصل شود، افرادی که در کوتاه ترین زمان عملیات خود را انجام داده باشند، جوایز بالاتری دریافت می کنند.

مسابقه دوم، مسابقه نفوذ به سرورها در ۳ مرحله آسان، متوسط و سخت است. در مرحله آسان و متوسط نفوذ به سرور از طریق یافتن یک نقطه ضعف امنیتی با به دست آوردن یک خط فرمان با دسترسی root انجام می شود. در مرحله سخت، نفوذ به سرور مورد نظر از طریق یافتن یک ضعف امنیتی در نرم افزار اجرا شده روی آن و حذف و اضافه داده ها در نرم افزار صورت می گیرد. در تمام مراحل این مسابقه، تامین ابزارهای نفوذ به عهده خود فرد است و استفاده از هر ابزاری باید با کنترل و تایید مسوول فنی مسابقه باشد. در این مسابقه، در صورت گذاشتن رد پا توسط نفوذگر در هریک از مراحل، جوایز نصف می شود. علاوه بر این، در صورت رسیدن به نتایج مشابه، افرادی که در کوتاه ترین زمان عملیات خود را انجام داده باشند، جوایز بالاتری دریافت می کنند.

بسته‌بندی مواد غذایی سلامت جامعه را تهدید می‌کند

براساس مطالعات انجام شده توسط محققان، افزایش کاربرد نوعی ترکیب شیمیایی موسوم به بیسفنول که معمولا در بسته بندی های پلاستیکی موادغذایی و نوشیدنی ها مورد استفاده قرار می گیرد، نقش بسیار مهمی در افزایش آمار مبتلایان به بیماری های قلبی ـ عروقی، دیابت نوع دوم و همچنین ایجاد اختلال در آنزیم های کبدی دارد. این ماده با تولید جهانی بیش از ۲ میلیون تن در سال ۲۰۰۳ و افزایش تقاضای ۶ تا ۱۰ درصد در سال به عنوان یکی از مواد شیمیایی که در حجم بسیار زیادی در سراسر دنیا تولید می شود، شناخته شده است که از آن در بسته بندی و پوشش پلاستیکی بسیاری از محصولات مصرفی استفاده می شود. بر این اساس قرار گرفتن در معرض این ماده شیمیایی از طریق مواد غذایی، آب آشامیدنی، مواد پرکننده دندانپزشکی، تنفس پوستی و همچنین استنشاق گرد و غبار خانگی می تواند نشان دهنده وجود مقادیر قابل توجهی بیسفنول در بیش از ۹۰ درصد کشورها در سطح دنیا باشد. وجود شواهدی مبنی بر پیامدهای نامطلوب ناشی از افزایش سطح این ماده در میان جمعیت های حیوانات نشان دهنده این است که باید برای جلوگیری از گسترش این پیامدها در جوامع انسانی تدابیری اتخاذ شود.

اگر چه این نخستین بار است که مطالعاتی در این زمینه انجام می شود، اما محققان امیدوارند با استفاده از نتایج به دست آمده از آن بتوانند سطح طبیعی مقدار این ماده در محیط را شناسایی کنند. آنها دریافته اند مقدار متوسط غلظت این ماده با توجه به در نظر گرفتن شرایط سنی و جنسیت افراد نقش موثری در ابتلا به بیماری های قلبی ـ عروقی و دیابت دارد و سبب افزایش ۳۹ درصدی این گروه از بیماری ها شده است. علاوه بر این افزایش غلظت این ماده منجر به افزایش اختلال در آنزیم های کبدی ایجاد و تغییرات غیرطبیعی در غلظت ۳ آنزیم کبدی خواهد شد. اگرچه اثرات نامطلوب و قابل توجه این ماده در کاهش سلامت انسان ها مورد تایید قرار گرفته و لزوم اتخاذ تدابیری مناسب برای کاهش غلظت این ماده در محصولات مصرفی را آشکار کرده است، اما همچنان لازم است در این زمینه مطالعات بیشتری انجام شود. از آنجا که تولید جهانی بیسفنول در حال حاضر به حدود ۴ میلیارد کیلوگرم در سال رسیده است، به نظر می رسد جلوگیری از کاربرد مستقیم آن در ظروف محتوی مواد غذایی و نوشیدنی در مقایسه با دستیابی به راهکارهایی برای حل بحران ناشی از گسترش آلودگی های این ماده شیمیایی به علت دفن فرآورده های حاوی این ماده در محل جمع آوری زباله یا انباشته شدن آن در اکوسیستم های آبزی به مراتب بسیار آسان تر باشد؛ اگرچه بسیاری از کشورها آلودگی های ناشی از تجمع مواد حاوی ماده شیمیایی بیسفنول را یکی از بزرگ ترین و پرمخاطره ترین آلودگی های زیست محیطی اعلام کرده اند. با توجه به این که تایید نتایج به دست آمده از این تحقیقات مدت زمان زیادی به طول خواهد انجامید و انتخاب جایگزین مناسب برای این ماده در ساخت بسته بندی های پلاستیکی مواد غذایی و نوشیدنی ها مستلزم انجام تحقیقات بسیار زیادی است تا بتوان با انتخاب ماده‌ای مناسب و بی ضرر پیامدهای ناشی از این ماده در سلامت عمومی را به حداقل رساند، بنابراین به نظر می رسد مداخله سازمان های دولتی مسوول تامین بهداشت عمومی و سلامت جامعه می تواند نقش موثری در بهبود وضعیت سلامت افراد جامعه و کاهش مشکلات ناشی از آن در سلامت افراد داشته باشد.

مترجم: فرانک فراهانی جم
منبع: Science daily

نخستین همایش تخصصی
نقش آموزش الکترونیک در توسعه آموزشهای میراث فرهنگی، صنایع دستی و گردشگری
روزهای برگزاری: ۱۳ و ۱۴ آذرماه ۱۳۸۷، مکان: سالن همایشهای سازمان میراث فرهنگی، صنایع دستی و گردشگری
آدرس دبیرخانه: تهران، خیابان لارستان، نبش کوچه افتخاری نیا، پلاک ۳۴، تلفکس: ۰۲۱ ۸۸ ۸۹ ۵۲ ۷۷
مهلت ارسال مقالات تا ۱۳۸۷/۸/۳۰
پست الکترونیک: elearning@chtl.ir
آدرس اینترنتی: chtl.mirasariaco.ir

آگهی دعوت به همکاری

یک کارخانه تولیدی واقع در زنجان جهت جذب یک نفر مهندس صنایع مجرب و دارای شرایط ذیل را به همکاری دعوت می‌نماید.
الف) دارای مدرک کارشناسی مهندسی صنایع (ترجیحاً در گرایش‌های تولید یا تجزیه تحلیل سیستمها) یا مدیریت صنعتی و مسلط به نرم افزار Microsoft Offic
ب) تسلط کامل به مراحل استقرار کامل سیستمهای کیفیت ISO 9000 ، ISO 22000 ، IMS
ج) تسلط به نرم‌افزارهای تخصصی مهندسی صنایع ، از جمله نرم‌افزار های کنترل پروژه و اقتصاد مهندسی
د) آشنایی با تکنیکها و الگوهای نوین علوم مدیریت از جمله مدلهای تعالی سازمانی
پ) محل خدمت زنجان
متقاضیان می‌توانند مدراک خود را به مدت ۵ روز از تاریخ چاپ آگهی به صندوق پستی ۷۶۱۹-۱۵۸۷۶ ارسال نمایند.

آگهی مناقصه عمومی دو مرحله‌ای
شمارهٔ ر/۸۷/۵۴۸
وزارت نیرو
شرکت برق منطقه‌ای خراسان
شرکت برق منطقه‌ای خراسان در نظر دارد تهیه و تأمین ۴۰ دستگاه ترمینال PLC و تجهیزات جانبی مربوطه را از طریق برگزاری مناقصه عمومی دو مرحله‌ای خریداری نماید. لذا از کلیه شرکتهای واجد شرایط در رشته مخابرات و دیسپاچینگ که دارای گواهینامه تایید صلاحیت از سازمان معاونت برنامه‌ریزی و نظارت راهبردی ریاست جمهوری می‌باشند دعوت بعمل می‌آید تا در صورت تمایل نسبت به خرید اسناد مناقصه با ارائه معرفینامه کتبی و رسید بانکی واریز وجه بشرح ذیل اقدام نمایند.
۱- تاریخ فروش اسناد مناقصه : از تاریخ ۸۷/۷/۳۰ لغایت ۸۷/۸/۶ در ساعات اداری
۲- قیمت فروش یک سری اسناد مناقصه : مبلغ ۸۰۰٫۰۰۰ ریال می‌باشد که باید به حساب جاری شماره ۴۹۵۵۸۷ بانک سپه شعبه رضاشهر مشهد (۱۵۶۷-۸۶۴) به نام شرکت توس اشتات واریز گردد.
۳- نشانی محل های فروش اسناد مناقصه :
۱-۳- مشهد بلوار وکیل‌آباد - بین هفتم تیر و وکیل آباد ۱۷ ، ساختمان شماره ۵/۶ ، شرکت مهندسین مشاور توس اشتات ، واحد مناقصات و قراردادها ، تلفن: ۸۶۶۳۱۵۳ دورنگار: ۸۶۳۶۱۳۹
۲-۳- تهران - میدان ونک ، خیابان بیستم گاندی ، ساختمان شماره ۱۸ ، واحد شماره ۵ ، شرکت توس اشتات
۴- آخرین مهلت تسلیم و ارائه پیشنهادات : ساعت ۹ صبح روز یکشنبه مورخ ۸۷/۸/۲۱ و گشایش پیشنهادها نیز ساعت ۱۰ صبح همانروز می‌باشد.
۵- محل تسلیم و ارائه پیشنهادها : مشهد - خیابان امام رضا(ع) ، اداره مرکزی شرکت برق منطقه‌ای خراسان ، امور تدارکات و قراردادها
۶- مبلغ تضمین شرکت در مناقصه : ۱۹۵٫۰۰۰٫۰۰۰ ریال می‌باشد.
آدرس الکترونیکی : E-Mail: bazargani@KREC.ir Web site : WWW.KREC.ir
روابط عمومی شرکت برق منطقه‌ای خراسان

اصلاح سند مناقصه شماره ۱-۲۰۸-۳-۸۷
شرکت آب و فاضلاب استان اصفهان
شرکت آب و فاضلاب استان اصفهان در نظر دارد بهره برداری و خدمات امور مشترکین تعدادی از شهرهای استان به شرح ذیل را به پیمانکاران واجد شرایط واگذار نماید .

نام شهر	دیزیچه وطالخونچه	مبارکه	زیباشهر و کرکوند	سمیرم (۱)	سمیرم (۲)	نطنز
مبلغ تضمین (ریال)	۴۰٫۳۰۰٫۰۰۰	۳۲٫۱۷۶٫۰۰۰	۲۳٫۶۱۹٫۰۰۰	۱۷٫۹۶۰٫۰۰۰	۲۷٫۴۶۰٫۰۰۰	۱۹٫۴۰۰٫۰۰۰

نام شهر	گز	شاهین شهر و میمه	نجف آباد(۱)	نجف آباد (۲)	ورزنه	دهاقان
مبلغ تضمین (ریال)	۱۶٫۶۶۰٫۰۰۰	۶۸٫۵۲۷٫۰۰۰	۳۵٫۲۹۰٫۰۰۰	۴۳٫۲۴۰٫۰۰۰	۱۱٫۴۳۶٫۰۰۰	۱۳٫۵۱۷٫۰۰۰

مهلت تحویل پیشنهادها به دبیرخانه کارفرما : ۸۷/۸/۲
گشایش پیشنهادها : ساعت ۸ صبح یکشنبه ۸۷/۸/۵
تلفن تماس : (۰۳۱۱)۶۶۸۰۰۳۰
محل دریافت اسناد مناقصه : پایگاه اینترنتی www.abfa-esfahan.com
شرکت آب و فاضلاب استان اصفهان

سودوکو ۳۷۳

برای حل جدول اعداد باید در هر مربع کوچکتر ۳ در ۳ هیچ عدد تکراری وجود نداشته باشد. همچنین هیچ عددی در یک سطر یا ستون مربع بزرگ ۹ در ۹ تکرار نشده باشد. **پاسخ جدول را در صفحه ۱۴ شماره بعد ملاحظه کنید.**

۱								
		۸	۷	۱				
		۳			۸	۹	۷	
		۴					۳	
	۲			۶			۱	
	۹					۵		
	۵	۹	۶			۳		
				۸	۴	۲		۵
								۶
								۱
							۳	
							۵	
							۶	۳
		۹	۸	۷				
		۵			۳	۸	۷	
		۸					۴	
	۱			۹			۳	
	۹					۷		
	۸	۷	۵			۴		
				۳	۶	۲		
۴								

								۳
		۱	۲	۵				
		۷			۶	۱	۸	
		۳					۵	
	۷			۲			۶	
	۶					۴		
	۱	۲	۸			۷		
				۱	۳	۵		
۹	۳							
	۷							
	۸							
۱								
۲								
۸		۷	۲	۵				
		۳			۱	۲	۷	
		۶					۸	
	۷			۱			۶	
	۳					۹		
	۱	۹	۸			۷		
				۶	۷	۴		
								۲