اصول و مفاهیم

رمزنگاری

مطابق با سرفصل وزارت علوم، تحقیقات و فناوری برای رشته‌های کامپیوتر و فناوری اطلاعات

مولف:

دکتر محمد علی ترکمانی

شناسه : ترکمانی، محمدعلی، ۱۳۵۴ -

عنوان و نام پدیدآور: اصول و مفاهیم رمزنگاری / مولف محمدعلی ترکمانی .

مشخصات نشر : مشهد: ارسطو، ۱۳۹۴.

مشخصات ظاهری : ۲۸۴ ص.: مصور، جدول ، نمودار .؛ ۱۷×۲۴س‌م .

شابک : ۹۷۸ – ۶۰۰ – ۷۵۵۸ – ۵۱ - ۵

وضعیت فهرست نویسی : فیپای مختصر

یادداشت: این مدرک در آدرس http://opac.nlai.ir قابل دسترسی است.

شماره کتابشناسی ملی : ۳۷۶۶۴۲۸

نام کتاب : اصول و مفاهیم رمزنگاری

مولف : دکتر محمد علی ترکمانی

ناشر : ارسطو (با همکاری سامانه اطلاع رسانی چاپ و نشر ایران)

صفحه آرایی، تنظیم و طرح جلد : علی بیات

تیراژ : ۱۰۰۰ جلد

نوبت چاپ : پنجم – ۱۳۹۸

تعداد صفحات: ۲۹۰ ص

چاپ : مدیران

قیمت : ۵۸۰۰۰ تومان

تلفن های مرکز پخش : ۳۵۰۹۶۱۴۵ – ۳۵۰۹۶۱۴۶ - ۰۵۱ -۰۹۱۷۷۱۶۴۹۴۰

وب سایت: www.chaponashr.ir/Torkamani

فهرست مطالب

مقدمه:

رمزنگاری علمی اســـت که به بررســـی و مطالعه روش‌ها و الگوریتم‌های رمزنگاری می‌پردازد. رمزگذاری عبارت ا ست از یک نظام یا الگوی ریا ضی/ منطقی که بر ا ساس آن اطلاعات و مفاهیم قابل فهم برای همگان، طبق روالی برگشـت‌پذیر به اطلاعاتی نامفهوم و گنگ تبدیل می‌شـود. این اطلاعات نامفهوم و گنگ توسط کسی که روال معکوس و پارامترهای لازم را می‌داند قابل برگشت و بهره برداری است. به این روال معکوس، رمزگشایی می‌گویند. بسیاری از نیازمندیهای امنیتی به وسـیله رمزگذاری تامین می‌گردد. رمزنگاری موجب جلوگیری از بسـیاری از مشـکلات امنیتی در سیستمها و شبکه‌های رایانه ای می‌شود.

علیرغم اینکه درس رمزنگاری یکی از دروس تخصصی در رشته‌های مهندسی کامپیوتر و فناوری اطلاعات محسوب می‌شود، اما مرجع مناسبی برای آن وجود ندارد. حجم مراجع معرفی شده برای این درس بسیار زیاد ا ست و تدریس این مطالب در یک نیم سال تحصیلی دشوار ا ست. ضمنا هیچکدام از مراجع موجود به تنهایی سرفصل‌های مورد نیاز برای این درس را پوشش نمی‌دهند.

این کتاب به منظور ســـهولت کار اســـاتید و دانشـــجویان گرامی و همچنین افزایش کیفیت آموزشی درس رمزنگاری تدوین گردیده ا ست. در این کتاب سعی شده ا ست که مطالب با زبانی ســاده و به همراه مثال‌های متنوعی ارائه گردد. در انتهای هر فصـل مجموعه سـئوالات تسـتی به همراه حل آنها آورده شـده اسـت. همچنین تعدادی تشـریحی و مسـئله به همراه پاسـخ برخی از مسائل ارائه شده ا ست تا دانشجویان گرامی بهتر بتوانند خود را برای آزمون‌هایی که در پیش رو دارند آماده نمایند. امید است این اثر مورد توجه همکاران و دانشجویان گرامی قرار گیرد. از اساتید و دانشـــجویـان گـرامـی تـقـاضـــا دارم نـقـطـه نـظـرات خـود را از طـریـق ایـمـیـل m.a.torkamani@gmail.com با اینجانب در میان بگذارند تا انشـــالله در ویرایش‌های بعدی کتاب اشکالات یا کاستی‌های احتمالی آن، مورد تجدید نظر قرار گیرد.

در پایان وظیفه خود می‌دانم از زحمات آقای مهندس علی بیات به خاطر طراحی جلد و همچنین از مدیریت انتشارات ارسطو و سامانه اطلاع رسانی چاپ و نشر ایران جناب آقای حسین قنبری به خاطر مساعدت در کار چاپ تشکر و قدردانی نمایم.

محمد علی ترکمانی

بهار ۱۳۹۴

فصل اول

مفاهیم امنیت اطلاعات و رمزنگاری

۱-۱-امنیت اطلاعات چیست؟

امنیت اطلاعات عبارت است از حفاظت اطلاعات در مقابل دسترسی های غیر مجاز، استفاده، افشاء، اختلال، اصلاح، مطالعه، بازرسی، ضبط یا تخریب، همچنین علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر تغییرات غیرمجاز از محرمانگی، تمامیت و دسترس‌پذیری اطلاعات. سایر ویژگی‌های دیگر امنیت اطلاعات از قبیل اصالت، اعتبار، انکارناپذیری، قابلیت جوابگویی و قابلیت اطمینان اطلاعات نیز می تواند مشمول این حفاظت باشند.

یک سیستم درست سیستمی است که اگر ورودی خوب و درست به آن داده شود خروجی درست به ما می‌دهد. اما سیستم امن سیستمی است که اگر حمله کننده به آن ورودی بد بدهد، سیستم خراب نشود. به طور کلی طراحی امکانات بیشتر در یک سیستم از نظر امنیت اطلاعات دردسر ساز است. زیرا باید کنترل روی ورودی‌ها بیشتر باشد. در امنیت اطلاعات به دنبال ساده بودن و مینیمم بودن سیستم هستیم. در صورتی که در یک سیستم خوب همیشه به دنبال امکانات بیشتر هستیم. در کل هدف ما این است که یک سیستمی داشته باشیم که هم درست و هم امن باشد.

۲-۱-اصول امنیت اطلاعات

یک سیستم امن باید دارای ویژگی‌های زیر باشد:

- **محرمانگی:**[۱] اطلاعات باید تنها توسط افرادی که تأیید صلاحیت شده‌اند، قابل دیدن با شد. به عنوان مثال در یک سایت دانشگاه که تنها دانشجویان و اساتید و کارمندان دانشگاه حق ورود به سایت را دارند. محرمانگی به وسیله رمزنگاری تامین می‌شود.
- **صحت:**[۲] داده‌ها نباید به صورت تصادفی یا عمدی تغییر داده شوند، نابود شده و یا گم شوند. به عنوان مثال جعل اطلاعات[۳] صحت را به چالش می‌کشد.
- **دسترسی پذیری:**[۴] هرگاه کاربر به سیستم نیاز داشت سیستم وجود داشته باشد. به عبارت دیگر سیستم باید قادر باشد هنگام درخواست کاربر، سرویس یا سرویس‌های مورد نظر را ارائه دهد. به عنوان مثال قطع کردن ارتباط[۵] و یا از کار انداختن یک کامپیوتر سرویس دهنده عدم دسترسی‌پذیری را فراهم می‌کند. نمونه ای از این حملات، حمله انکار سرویس یا DOS است.[۶]

در کنار این سه اصل اساسی، نیازمندیهای امنیتی دیگری نظیر عدم انکار،[۷] تایید هویت[۸] نیز مطرح است. منظور از عدم انکار این است که فرستنده نتواند ادعا کند پیام از طرف وی ارسال نشده است.

۳-۱-اصطلاحات امنیتی

۱-۳-۱-آسیب‌پذیری[۹]

---

۱ Confidentiality
۲ Integrity
۳ Fabrication
۴ Availability
۵ Interruption
۶ Denial of Service
۷ Non-Requdiation
۸ Authentication
۹ Vulnerability

آسیب‌پذیری، یک خطا یا نقص در طراحی، پیاده‌سازی یا عملیات سیستم است. آسیب‌پذیری می‌تواند در یکی از موارد زیر باشد:

- طراحی سیستم: در این حالت پروتکل یا الگوریتم ایراد دارد. به عنوان مثال طراحی پروتکل TCP/IP درست انجام نشده و بسته‌های TCP/IP به صورت متن ساده[۱](رمز نشده) هستند. این یک ایراد طراحی است که یک آسیب‌پذیری را برای این پروتکل به وجود آورده است و باعث شده است که اگر یک نفر گوش کند، بتواند محتوای بسته‌های IP را ببیند.
- پیاده‌سازی: به عنوان مثال فرض کنید در برنامه نویسی یک پروتکل، مواردی (نظیر اصول یا استانداردهای کدنویسی امن) را رعایت نکرده‌ایم، یا اشتباهاتی داریم. علاوه بر این، در پیاده‌سازی TCP/IP با توابع C یک سری آسیب‌پذیری‌هایی دیده می‌شود که علت آن اشکالات موجود در زبان C است. برای رفع این مورد باید از نسخه‌های جدیدتر این زبان و یا زبان جاوا استفاده کرد.
- عملیات سیستم ایراد دارد: فرآیندها درست انجام نمی‌شود. به عنوان مثال یک فرم پر شده و باید به دست یک نفر برسد ولی به فرد دیگری می‌رسد که نباید آنرا ببیند.

۲-۳-۱-حمله[۲]

در علم امنیت شبکه، حمله عبارتست از بهره برداری از آسیب‌پذیری‌های یک سیستم. متخصصان رمزنگاری حمله را به این صورت تعریف می‌کنند: به هرگونه تلاش غیر مجاز برای یافتن کلید رمزنگاری یا رمزگشایی داده های رمز شده، حمله می‌گویند.

۳-۳-۱-تهدید[۳]

مجموعه‌ای از شرایط و پیشامدها که پتانسیل صدمه زدن به سیستم را دارد. فردی بدخواه که انگیزه و توانایی حمله را داشته باشد و یا یک سیستم که امکان یک حمله را فراهم می‌کند یک تهدید است.

۱Clear Text
۲Attack
۳Threat

۴-۳-۱-مفهوم AAA در امنیت اطلاعات

در دنیای امنیت اطلاعات به واژه مخفف AAA برخورد می‌کنیم که مخفف سه کلمه ذیل است:

- Authentication: تأیید هویت (احراز هویت) مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می‌شود. احراز هویت مکانیزمی است که بر اساس آن هر موجودیت(مانند یک شخص یا یک سرویس دهنده بانکی) بررسی می‌کند که آیا شریک او در یک ارتباط، همان فردی ا ست که ادعا می‌کند یا یک شخص اخلال‌گر ثالث ا ست که خود را به جای طرف واقعی جا زده است.
- Authorization: اجازه[۱] مکانیزمی است که بر اساس آن مشخص می‌شود فرد یا موجودیتی که هویت آن احراز شده، مجوز انجام چه کارها و عملیاتی را در سیستم دارد.
- Accounting: حسابداری مکانیزمی است که مشخص می‌کند فرد مورد نظر چه سهمی از منابع سیستمی و خدماتی را می‌برد. یعنی به عنوان مثال اعتبار کافی دارد یا خیر.

در میان این سه واژه، مهمترین مرحله Authentication است که تامین دو مورد دیگر را نیز بسیار ساده می‌سازد.

به عنوان مثال وقتی فردی می‌خواهد به سیستم دسترسی پیداکند، ما می‌خواهیم بدانیم آیا همان فرد مورد نظر است یا خیر، تایید هویت انجام می‌دهیم. اما اجازه، بیشتر مفهوم کنترل سطح دسترسی را می‌دهد. به عنوان مثال، در سیستم اینترنتی یک دانشگاه، کاربر هنگام ورود ابتدا تایید هویت می‌شود که مشخص شود کاربری مجاز است یا خیر. در این سیستم اساتید و دانشجویان و سایر پرسنل دانشگاه مجاز به ورود هستند. اما در خصوص اجازه دسترسی، واضح است که یک دانشجو تایید هویت شده و وارد سیستم می‌شود ولی اجازه ویرایش نمرات را ندارد.

در خصوص حسابداری نیز به این مثال توجه کنید. فرض کنید شخصی تایید هویت می‌شود و وارد یک فروشگاه الکترونیکی می‌شود. وی اجازه خرید کردن را دارد. بنابراین Authorization

---

۱Authorization

نیز با موفقیت انجام می‌شود. اما ممکن است موجودی این فرد در سایت برای خرید کردن کافی نباشد. بنابراین فرایند Accounting به وی اجازه خرید را نخواهد داد.

۵-۳-۱-عدم انکار (سندیت)[۱]

عدم انکار یعنی عمل ارسال و دریافت پیام و نیز محتوای داده و پیام توسط فرستنده و گیرنده قابل انکار نباشد (سرویسی که از انکار فرستنده و گیرنده جلوگیری می‌کند.) از این رو، وقتی پیامی ارسال گردید، فرستنده می‌تواند ثابت کند که گیرنده پیام را دریافت کرده است.

۴-۱-نفوذگر یا هکر[۲]

به کسی که به تلاش میکند به یک سیستم کامپیوتری دسترسی غیرمجاز داشته باشد، هکر گفته می‌شود.

۶-۱-برخی از حملات متداول

در این قسمت برخی از حملات متداول معرفی می‌شوند.

۱-۶-۱-افشای پیام[۳]یا سرقت اطلاعات[۴]

خواندن یک ایمیل محرمانه یا شنود یک ارتباط تلفنی نمونه‌ای از این نوع حمله است. واضح است که این حمله عدم محرمانگی را فراهم می‌کند. (محرمانگی را به چالش می‌کشد).

۱-۱-۶-۱-استراق سمع یا شنود اطلاعات[۵]

در این حمله اطلاعات مبادله شده، به روش‌های گوناگون سرقت و یا شنود می‌شوند. به برنامه‌های استراق سمع، Sniffer گویند. اینگونه نرم‌افزارها این امکان را در اختیار مهاجم قرار می‌دهند که

---

۱ Non-repudiation
۲ hacker
۳ Release of Message
۴ Interception
۵ Eavesdropping

بتواند بسته‌های شبکه را دریافت، مشاهده و سپس ارسال نماید. گونه دیگری از استراق سمع، استراق کارت‌های اعتباری و یافتن رمز کارت‌های اعتباری است.

۲-۶-۱-تحلیل ترافیک

در کانال‌های ارتباطی ناامن اطلاعات به صورت رمز شده ارسال می‌گردد تا چنانچه مهاجم پیام‌ها را شنود کند، نتواند پیام اصلی را از داخل آن استخراج نماید. اما حمله کننده می‌تواند اطلاعاتی از قبیل مبداء، مقصد و اندازه پیام‌ها را تحلیل نموده و از آنها برای یافتن برخی از پیام‌ها یا تعیین کلید رمزنگاری استفاده نماید. به عنوان مثال در یک سیستم نظامی ممکن است دشمن حجم داده‌های ارسالی را تحلیل کرده و چناچه در یک روز خاص حجم اطلاعات بیش از اندازه معمول باشد، حدس بزند که احتمالا قرار است عملیاتی انجام گردد.

۳-۶-۱-نقاب‌زنی یا بدل[۱]

حمله‌ای است که در آن حمله کننده خودش را جای فرد دیگری جا می‌زند. در واقع حمله کننده هویت فرد دیگری را سرقت می‌نماید. این حمله نوعی جعل اطلاعات است و عدم صحت را به دنبال دارد. اما چون مهاجم موفق شده خودش را به جای قربانی جا بزند، در ادامه می‌تواند اطلاعات محرمانه قربانی را خوانده (عدم محرمانگی) و یا با ارسال بسته های زیاد قابلیت دسترسی را به چالش بکشد. در ادبیات امنیت شبکه به این نوع حمله، Spoofing (حقه بازی) نیز میگویند. به عنوان مثال در IP Spoofing حمله کننده IP خودش را به عنوان IP شخص دیگری جا می‌زند و همه بسته‌های قربانی را دریافت کند. بدترین حالت آن هم این است که IP خودش را به عنوان gateway IP قرار دهد.

۴-۶-۱-حمله مرد میانی[۲]

در این حمله نفوذگر بین دو کامپیوتری که در حال تبادل اطلاعات هستند قرار می‌گیرد. در این روش مهاجم می‌تواند به نوعی اطلاعات رد و بدل شده بین دو کامپیوتر را دریافت کرده و آنرا ویرایش کند، بدون آنکه کلاینت متوجه این موضوع شود. هدف اصلی این نوع حملات

۱Masquerade

۲Man in the Middel

دسترسی به اعتبارات کلاینت‌ها و یا کاربران شبکه است. توسط این روش می‌توان اطلاعات نرم‌افزارهای مبتنی بر وب و یا مبتنی بر سیستم عامل کاربران را به دست آورد. فرض کنید دو نفر با یکدیگر در ارتباط هستند. در ادبیات امنیت شبکه به این دو نفر معمولا باب و آلیس گفته می شود. تصور کنید فردی بتواند به عنوان حمله کننده ارتباط میان این دو نفر را قطع نماید. این فرد باید بتواند ارسال پیغام‌ها را طوری انجام دهد که باب و آلیس متوجه نشوند. در واقع باید بتواند نوع ارسال پیغام‌ها را تقلید نماید. در این حالت باب و آلیس تحت حمله مرد میانی قرار گرفته‌اند.

۵-۶-۱- حمله روز تولد[۱]

حمله روز تولد نامی است که به گروهی از حملات قوی اطلاق می شود. اگر یک عملیات زمانی که با یک داده تصادفی تغذیه می‌شود، یکی از ارزش‌های k را باز گرداند، آنگاه با ارزش‌گذاری مکرر آن عملیات برای داده‌های مختلف، انتظار می‌رود که پس از $1.2k^{1/2}$ آزمایش به خروجی یکسانی دست یابیم. در واقع اگر به دنبال یافتن یک برخورد هستیم، با استفاده از تناقض (پارادوکس) روز تولد می‌توان انتظار دا شت که پس از $1.2k^{1/2}$ آزمایش مقادیر احتمالی داده، به یک تلاقی برسیم. وان اورشات[۲]و وینر[۳]نشان دادند که چنین حمله‌ای می‌تواند به کار گرفته شود. پارادکس روز تولد به شرح زیر است. فرض کنید گروهی از افراد در یک اتاق هستند. احتمال اینکه دو نفر از آنها روز تولد یکسانی داشته باشند چقدر است؟ به طور شگفت انگیزی این احتمال زیاد است. به عنوان مثال اگر ۲۳ نفر در یک اتاق باشند، آنگاه با احتمال حداقل ½، دو نفر از آنها روز تولد مشترک دارند. در کتب کلاسیک رمزنگاری اثبات این موضوع نشان داده شده است.

۶-۶-۱-حملات جهت یافتن کلمات عبور

۱Birthday
۲Van Oorschot
۳Wiener

متداول‌ترین روش‌هایی که برای یافتن کلمات عبور به کار می‌روند عبارتند از:

- **جستجوی جامع:**[۱] جستجوی جامع یک روش برای شکستن کلمات رمز و به دست آوردن آنها است. حمله جستجوی جامع حروف را به صورت ترکیبی استفاده می‌کند و با تست کردن آنها رمز عبور را پیدا می‌کند. برای مقابله با این روش باید کلمات رمزی با طول زیاد انتخاب کرد و یا کلمات رمز را هر دفعه تغییر داد. در این روش حمله کننده باید تمام رمزهای عبور (یا کلیدهای رمزنگاری) ممکن که برای رمزگذاری استفاده می‌شوند را امتحان کند تا کلمه عبور یا متن رمز نشده را به دست آورد.
- **واژه نامه:**[۲] یک روش برای به دست آوردن کلمات عبور با استفاده از لغات دیکشنری است. واژه نامه در اصل لغتنامه‌ای از کلمات معروف می‌باشد که در یک فایل ذخیره شده‌اند و به وسیله یک ابزار برای شکستن کلمات رمز، مورد استفاده قرار می‌گیرد. برای مقابله با این حمله باید از کلماتی استفاده کرد که در لغتنامه وجود ندارد.
- **روش ترکیبی برای شکستن کلمات عبور :** در این روش از ترکیب دو روش قبل استفاده می‌شود.

۸-۶-۱-حمله تکرار[۳]

به عمل دریافت داده در بین راه و ارسال مجدد آن با هدف دستیابی غیر مجاز، تکرار گویند. به عنوان مثال وقتی یک هکر به وسیله ابزارهای sniffer بسته‌های اطلاعاتی را ازروی سیم بر می‌دارد، یک حمله تکرار رخ داده است. وقتی بسته‌ها دزدیده شدند، هکر اطلاعات مهم و نام‌های کاربری و کلمات عبور را از درون آن استخراج کرده و دوباره بسته‌ها را روی خط قرار می‌دهد و یا به آنها به صورت دروغین پاسخ می‌دهد.

۱Brute force , or Exhaustive key search
۲Dictionary
۳Reply

۷-۱- رمزنگاری چیست؟

رمزنگاری[۱] علمی است که به بررسی و مطالعه روش‌ها و الگوریتم‌های رمزنگاری می‌پردازد. رمزگذاری[۲] عبارت است از یک نظام یا الگوی ریاضی/ منطقی که بر اساس آن اطلاعات و مفاهیم قابل فهم برای همگان، طبق روالی برگشت‌پذیر 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. به این روال معکوس، رمزگشایی[۳] می‌گویند. در برخی از کتاب‌ها واژه رمزنگاری را به جای رمزگذاری نیز به کار می‌برند. می‌توان فرایند رمزگذاری را به تابعی به شکل زیر تصور کرد:

$$C = f_E(P, K)$$

در این تابع P پیامی است که باید رمز شود که به آن متن ساده[۴] می‌گویند. K پارامتری است که متن ساده بر اساس آن به صورت غیر قابل پیش بینی و مبهم، درهم و بی معنی می شود. به پارامتر K، کلید رمز یا کلید رمزگذاری[۵] می‌گویند. C حاصل فرآیند رمزنگاری متن ساده P با کلید K و تابع رمزگذاری f_E است که به آن متن رمز می‌گویند. همچنین می‌توان فرایند رمزگشایی را نیز که طی آن متن رمز به متن ساده تبدیل می‌شود، به صورت زیر نمایش داد:

$$P = f_D(C, K)$$

در این رابطه f_D تابع رمزگشایی و K کلید رمزگشایی می‌باشد.

در اینجا به ذکر یک مثال از کاربرد رمزنگاری می‌پردازیم. فرض کنید در یک کانال مخابراتی نا امن، فرستنده می‌خواهد یک پیام محرمانه را برای گیرنده ارسال نماید و هدف وی حفظ محرمانگی پیام است. روش انجام کار به این ترتیب است که متن ساده یا رمز نشده توسط یک الگوریتم رمزنگاری رمز می شود و خروجی آن که متن رمز است، برای گیرنده ارسال می شود. در مقصد نیز رمزگشایی متن رمز شده، توسط یک الگوریتم رمزگشایی انجام می شود و متن ساده اولیه به دست می‌آید.

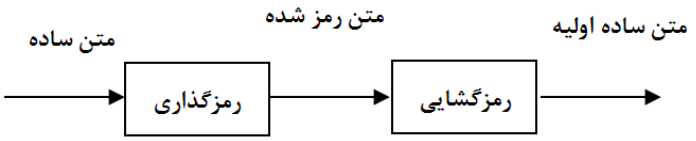
---

۱ Cryptography
۲ Encryption
۳ Decryption
۴ Plaintext/Clear Text
۵ Key

نکته: برای نوشتن متن نیاز به حروف یا سمبل‌هایی از یک الفبا داریم که یک مجموعه غیر تهی ا ست و آنرا با Σ نمایش می‌دهیم و به آن الفبای رمزنگاری می‌گوییم. به عنوان مثال الفبای رمزنگاری سزار برابر است با مجموعه حروف انگلیسی.

۱-۷-۱- سیستم‌های رمزنگاری

یک سیستم رمزنگاری[۱] سیستمی است که عملیات رمزگذاری و رمزگشایی را انجام می‌دهد (شکل ۱-۱). عملیات رمزگذاری یا رمزنگاری می‌تواند توسط سخت‌افزار یا نرم‌افزار انجام شود.



شکل۱- ۱: یک سیستم رمزنگاری

تمرین: فرم ریاضی یک سیستم رمزنگاری یا دستگاه رمزنگاری به صورت یک پنج تایی نشان داده می‌شود. در این خصوص تحقیق کنید.

سیستم‌های رمزنگاری از نظر تعداد کلید به دو دسته متقارن و نامتقارن تقسیم می شوند که در ادامه شرح داده می‌شوند.

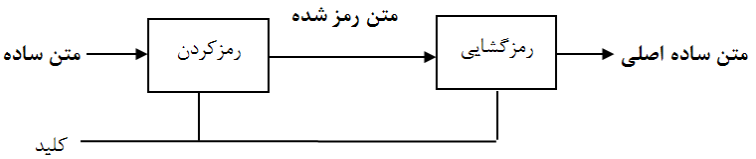
۱-۱-۷-۱-رمزنگاری متقارن[۲]

در رمزنگاری متقارن (شکل ۳-۱) کلیدهای رمزنگاری و رمزگشایی یکسان هستند. اگر P متن ساده، C متن رمز شده، K کلید مشترک[۳] یا کلید سری،[۴] E تابع رمزگذاری و D تابع رمزگشایی باشد، فرم ریاضی عملیات رمزنگاری و رمزگشایی به صورت زیر است:

$C=E(K,P)$
$P=D(K,C)$

۱Cryptosystem
۲Symmetric
۳Shared Key
۴Secret Key

همانطور که از نام کلید مشترک(کلید سری) هم پیدا است، این کلید بین فرستنده و گیرنده پیام مشترک است و باید سری بماند.



شکل۱- ۲: رمزنگاری متقارن

۲-۱-۷-۱-رمزنگاری نامتقارن[۱]

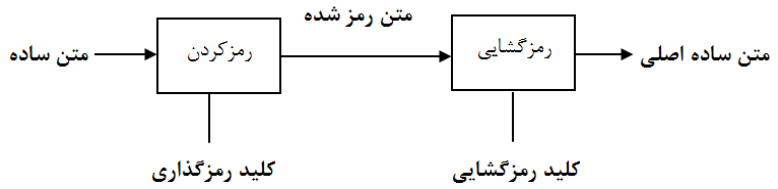
در این روش (شکل ۱-۳) کلیدهای رمزنگاری و رمزگشایی متفاوت هستند. فرم ریاضی این روش به صورت زیر است:

$$C = E(K_E, P)\ , P = D(K_D, C)$$

K_E و K_D به ترتیب کلید رمزگذاری و کلید رمزگشایی هستند. C، E،P وD نیز مشابه با روش متقارن هستند. یکی از مهم‌ترین روش‌های رمزنگاری نامتقارن، رمزنگاری با کلید عمومی[۲] است. در این روش هر فرد دارای یک کلید خصوصی[۳] و یک کلید عمومی است. کلید خصوصی را فقط مالک آن می‌داند، اما کلید عمومی را همه می‌دانند و در واقع مانند کلید مشترک در رمزنگاری متقارن، سری نیست. از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود.

در رمزنگاری متقارن، مشکل اصلی توزیع کلید است. یعنی فردی که رمزگذاری را انجام می‌دهد، چگونه کلید را به فردی که می‌خواهد رمزگشایی انجام دهد، برساند. آیا در هنگام انتقال کلید، کلید ربوده می‌شود؟ اما در روش رمزنگاری با کلید عمومی، این مشکل وجود ندارد.

۱Asymmetric
۲Public Key
۳Private Key



شکل۱-۳: رمزنگاری نامتقارن

۳-۷-۱-علم تحلیل رمز یا شکستن رمز

علم تحلیل رمز یا شکستن رمز[۱] علمی است که به مطالعه روش‌ها و اصولی می‌پردازد که بر اساس آنها می‌توان بدون در اختیار داشـــتن کلید رمز (یا اطلاعات لازم برای رمزگشـــایی)، داده‌های رمزنگاری شده را از رمز خارج کرد یا کلید رمز را به دست آورد. علم شکستن رمز شامل مباحث زیر است:

- **شکستن پیام:** یعنی از متن رمز شده به متن ساده برسیم.
- **شکستن کلید:** یعنی کلید را پیدا کنیم.
- **شکستن الگوریتم:** یعنی از یک مشکل که در الگوریتم وجود دارد استفاده کنیم.

۴-۷-۱- عملیات مورد استفاده در یک سیستم رمزگذاری

عملیات مورد استفاده در یک سیستم رمزنگاری می‌تواند یکی از موارد ذیل باشد:

- عملیات ریا ضی و منطقی، گ سترش بیت‌ها(مثلا تبدیل ۳۲ بیت به ۴۰ بیت) و تق سیم[۲] و ادغام[۳]

۱Cryptanalysis
۲split
۳Merge

- **جایگزینی:**[۱] جایگزینی یعنی اســـتفاده از یک جدول برای جایگزینی کاراکترهای متن ساده. به عنوان مثالی از جایگزینی می‌توان روش‌های رمزنگاری سزار و رمزنگاری ورنام را نام برد.
- **جایگشـــتی:**[۲] یعنی کاراکترهای متن ســـاده را جابجا کنیم. مزیت ابن روش‌ها ســـادگی ا ست و ضعف آنها این ا ست که قابل شک ستن ا ست. به عنوان نمونه‌ای از روش‌های جایگ شتی می‌توان جایگشتی ستونی را نام برد.

۶-۷-۱-اصول اساسی رمزنگاری

۱-ا ستحکام: هر الگوریتم رمزنگاری باید علیه حملات مختلف (نظیر حمله متن ساده معلوم، متن ساده انتخابی و متن رمز معلوم) م ستحکم بوده و نتیجه تلاش رمز شکن ناموفق و مایوس کننده با شد. روش‌هایی وجود دارند که در مقابل برخی از حملات مقاوم نی ستند اما می‌توانند در ترکیب با سایر روش‌ها مورد استفاده قرار بگیرند.

۲-تازگی:[۳] فرض کنید آلیس مشـــتری یک ســـیســـتم بانکی و باب کارمند بانک اســـت. آلیس برای باب یک پیام رمز شـــده بســـیار مهم مبتنی بر انتقال پول از حســـابش به حســـاب دیگری ارســـال می‌کند. فرض کنید شـــخص ثالثی این پیام را اســـتراق ســـمع کرده و به دلیل اســـتحکام بی نظیر الگوریتم رمزنگاری هرگز موفق به شکستن رمز نمی‌شود، ولی یک هفته بعد همان پیام را از طرف آلیس برای باب می‌فرســـتد و باب با رمزگشـــایی آن؛ عمل خواســـته شـــده را انجام می‌دهد، غافل از اینکه این پیام تکراری و دروغین اســـت. بنابراین رمزگشـــایی اطلاعات گرچه لازم اســـت ولی هرگز کافی نیست. باید مکانیزم‌هایی در کنار فرایند رمزنگاری اتخاذ شود تا تازگی پیام به اثبات بر سد و از حمله تکرار پی شگیری شود. در غیر این صورت امکان هرگونه اختلال و یا سوء ا ستفاده وجود دارد.

۱Substitution
۲Permutation
۳Freshness

برای اثبات تازگی پیام‌ها می‌توان برای هر پیام تاریخ و زمان صدور و مهلت اعتبار درنظر گرفت و یا هر پیام به همراه یک شناسه یکتا، رمز شده و ارسال گردد. بدین ترتیب از حمله تکرار جلوگیری خواهد شد. بنابراین در عمل ترکیبی از مهر زمان[۱] و شناسه پیام به کار می‌رود تا گیرنده بتواند تازگی پیام را اثبات کند.

۳-افزونگی[۲]: فرض کنید استاد یک درس پیامی رمز شده حاوی نمره یک دانشجو برای بانک اطلاعاتی آموزش دانشگاه ارسال می‌کند. اگر فردی در بین راه یک بیت از پیام را تغییر دهد، یک پیام معتبر به یک پیام معتبر دیگر تبدیل می‌شود و در نتیجه نمره دانشجو تغییر خواهد کرد. بنابراین پیام‌های ارسالی باید دارای افزونگی باشند و این افزونگی باید به نحوی هوشمندانه در پیام‌ها درج شود تا هر تغییر در پیام، آنرا به پیامی غیر معتبر و قابل کشف تبدیل کند.

در رمزنگاری برای رفع این مشکل از چکیده پیام[۳] استفاده می‌شود.

۸-۱- سئوالات تشریحی

۱-اصطلاحات زیر را توضیح دهید؟

الف-Confidentiality ب-Asymmetric Cryptosystem

۲- شش مورد از نیازمندی های امنیتی یک سیستم را نام برده و توضیح دهید.

۳- در هر یک از موارد زیر مشخص کنید کدامیک از سه اصل امنیت اطلاعات به چالش کشیده شده است؟

الف- جواد تمرین‌های مریم را کپی کرد.

ب- علی سیستم مهسا را از کار انداخت.

ج-فریدون مقدار موجودی حساب زهرا را از ۱۰۰ دلار به ۱۰۰۰ دلار تغییر داد.

د- داریوش امضای خودش را به جای امضای رضا گذاشت.

ه-بهرام یک دامنه با نام Yahoo.com ثبت کرد و با استفاده از آن جلوی سرویس Yahoo Buy را گرفت.

---

۱ TimeStamo

۲ Redundancy

۳ Message Digest

پاسخ:

الف) سرقت اطلاعات است و باعث عدم محرمانگی می شود .

ب) قابلیت دسترسی را دچار چالش کرده است.

ج) صحت را مخدوش کرده است.

د) چون داریوش امضای خودش را به جای امضای رضا قرار داده، پس جعل اطلاعات است و در نتیجه صحت را به چالش کشیده است و در ادامه نیز می‌تواند اطلاعات را سرقت کند و موجب عدم محرمانگی شود. ضمناً چون مهاجم امضای خودش را به جای شخص دیگری جا زده است ولی از دیدگاه سرور تأیید هویت شده است، حتی می‌تواند با ارسال بسته‌های زیاد موجب از کار افتادن سرویس‌ها شده و دسترسی پذیری را نیز به چالش بکشد. بنابراین در ادامه مهاجم می‌تواند هر سه اصل امنیت اطلاعات را دچار چالش می‌شود.

۹-۱-سئوالات چهارگزینه‌ای

۱-توانایی محافظت داده از تغییر یا خرابی با دسترسی غیر مجاز یا تصادفی چه نامیده می‌شود؟

الف. قابلیت اعتماد ب.محرمانگی ج.جامعیت و صحت اطلاعات د.احراز هویت

۲-خرابی تجهیزاتی، بلاهای طبیعی، عکس‌العمل‌های کارمندان بداندیش و حملات هکرها نمونه‌هایی از..... هستند:

الف. تهدیدها ب. آسیب‌پذیری‌ها ج. ریسک د. خرابی‌های سیستم

۳-کدام گزینه صحیح است؟

الف-Authentication مکانیزمی است که بر اساس آن مشخص می شود که فرد یا موجودیتی که هویت آن احراز شده است، مجوز چه کارها و عملیاتی را دارد.

ب-Accounting مکانیزمی است که مشخص می‌کند فرد یا موجودیتی که هویت آن احراز شده است، مجوز چه کارهایی را دارد.

ج-Authentication مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می‌شود.

د-Authorization اهمیت بیشتری از .Authentication دارد.

۴ - نام دیگر IP Spoofing چیست؟

الف- IP forgery ب- IP poisoning ج- IP Attack د-همه موارد

۵-برای جلوگیری از حمله تکرار از چه مکانیزمی استفاده می‌شود؟

الف-چکیده پیام ب- مهر زمان و شناسه پیام ج- رمزنگاری د -همه موارد

۶- Arp spoofing از حملات لایه .....است.

الف- شبکه ب- لینک ج- انتقال د- کاربرد

۷-حمله‌ای که در آن، حمله کننده اطلاعاتی از قبیل مبداء، مقصد و اندازه پیام را می‌بیند، چه نامیده می‌شود؟

الف. افشاء پیام ب. بدل ج. تحلیل ترافیک د. انکار سرویس

۸- نمونه بارز عدم رعایت اصل کرکهف کدام الگوریتم است؟

الف- RC4 ب- RSA ج- RC2 د- DES

۹- بهرام یک دامنه مشابه Yahoo com ثبت کرده و با استفاده از آن جلوی سرویس yahoo Bug را گرفت. به نظر شما کدام یک از سه اصل امنیت اطلاعات به چالش کشیده شده است؟

الف- قابلیت دسترسی ب- صحت ج- محرمانگی د- همه موارد

۱۰-داریوش امضای خودش را به جای امضای رضا قرار داده است. به نظر شما کدام یک از اصول امنیت اطلاعات به چالش کشیده شده است؟

الف- قابلیت دسترسی ب- محرمانگی ج- صحت د- همه موارد

۱۱- کدام اصل کرکهف به اصل اساسی آن مشهور است؟

الف- اول ب- دوم ج- پنجم د- چهارم

پاسخنامه

1	الف	ب	ج	د
2	الف	ب	ج	د
3	الف	ب	ج	د
4	الف	ب	ج	د
5	الف	ب	ج	د
6	الف	ب	ج	د
7	الف	ب	ج	د
8	الف	ب	ج	د
9	الف	ب	ج	د
10	الف	ب	ج	د
11	الف	ب	ج	د