نام کتاب	لینک خرید چاپی	لینک خرید الکترونیکی	لینک فایل نمونه
مبانی رایانه و برنامه‌نویسی به زبان C++	http://daneshnegar.com/book_380238.html	http://ktbr.ir/b30588	http://ketabesabz.com/dl/52319
آشنایی با مبانی امنیت شبکه (امنیت اطلاعات)	http://daneshnegar.com/book_371137.html	http://ktbr.ir/b30327	
اصول طراحی پایگاه داده‌ها	http://daneshnegar.com/book_371655.html	http://ktbr.ir/b29943	http://ketabesabz.com/dl/52155
آموزش گام‌به‌گام برنامه‌نویسی پایتون	http://daneshnegar.com/book_392582.html	http://ktbr.ir/b29984	http://ketabesabz.com/dl/52181
آزمایشگاه کامپیوتر C++ (حل مسائل مرجع کامل)	http://daneshnegar.com/book_392262.html	http://ktbr.ir/b29982	http://ketabesabz.com/dl/53546
آموزش گام‌به‌گام C # با LINQ	http://daneshnegar.com/book_369388.html	http://ktbr.ir/b28451	
ساختمان داده‌ها با C++	http://daneshnegar.com/book_379094.html	http://ktbr.ir/b29676	http://ketabesabz.com/dl/52156
طراحی سیستم‌های شی‌گرا با زبان C#	http://daneshnegar.com/book_374658.html	http://ktbr.ir/b29621	http://ketabesabz.com/dl/52126
مدیریت استراتژیک فناوری اطلاعات	http://daneshnegar.com/book_374659.html	http://ktbr.ir/b29779	http://ketabesabz.com/dl/52125
گرافیک رایانه‌ای با زبان برنامه‌نویسی C#	http://daneshnegar.com/book_376021.html	http://ktbr.ir/b29674	http://ketabesabz.com/dl/51049
درس و کنکور پایگاه داده پیشرفته	http://daneshnegar.com/book_392578.html	http://ktbr.ir/b29644	http://ketabesabz.com/dl/52102
فیزیک الکتریسیته	http://daneshnegar.com/book_379161.html	http://ktbr.ir/b29680	
تجارت الکترونیکی	http://daneshnegar.com/book_379188.html	http://ktbr.ir/b29619	http://ketabesabz.com/dl/51013
راهنمای کاربردی کاربری OPNET برای شبکه‌های شبیه‌سازی کامپیوتر	http://daneshnegar.com/book_392583.html	http://ktbr.ir/b28504	
درس و کنکور سیستم عامل پیشرفته	http://daneshnegar.com/book_392580.html	http://ktbr.ir/b28505	http://ketabesabz.com/dl/52180
شبکه‌های کامپیوتری با رویکرد کاربردی، آزمایشگاه شبیه‌سازی شبکه	http://daneshnegar.com/book_392254.html	http://ktbr.ir/b28528	
آزمایشگاه پایگاه داده SQL Server با 2012	http://daneshnegar.com/book_377301.html	http://ktbr.ir/b28503	http://ketabesabz.com/dl/53447
کاربرد رایانه در مدیریت و حسابداری	http://daneshnegar.com/book_375892.html	http://ktbr.ir/b28450	http://ketabesabz.com/dl/53446
آموزش گام‌به‌گام برنامه‌نویسی بانک	http://daneshnegar.com/book_368929.html	http://ktbr.ir/b28449	http://ketabesabz.com/dl/53488

اطلاعاتی با ویژوال بیسیک‌نت			
آموزش گام‌به‌گام برنامه‌نویسی به زبان C++	http://daneshnegar.com/book_380238.html	http://ktbr.ir/b28452	
دانلود کتاب آموزش گام‌به‌گام برنامه‌نویسی بانک اطلاعاتی با #C	http://daneshnegar.com/book_368486.html	http://ktbr.ir/b28448	http://ketabesabz.com/dl/51047
حل مسائل پاسکال		http://ktbr.ir/b28398	
حل مسائل C++	http://daneshnegar.com/book_392262.html	http://ktbr.ir/b28401	http://ketabesabz.com/dl/51048
دانلود کتاب حل مسائل #C	http://daneshnegar.com/book_374657.html	http://ktbr.ir/b28399	http://ketabesabz.com/dl/51011
دانلود کتاب حل مسائل C		http://ktbr.ir/b28397	

آشنایی با

مبانی امنیت شبکه

(امنیت اطلاعات)

تالیف :
مهندس رمضان عباس نژاد ورزی
مهندس آتنا فرجی

برخی از عناوین مهم

مقدمه‌ای بر امنیت
رمزگذاری‌های کلاسیک
رمزگذاری‌های پیشرفته متقارن و نامتقارن
امنیت شبکه و محیط کاری
بد افزار
فایروال
امنیت در تجارت الکترونیک
سرویس‌ها و برنامه‌های کاربردی امنیت اطلاعات
هرزتماس و هرزنامه

آشنایی با
مبانی امنیت شبکه(امنیت اطلاعات)

تالیف:

مهندس رمضان عباس‌نژادورزی
مهندس آتنا فرجی

فن‌آوری نوین

سرشناسه	: عباس‌نژادورزی، رمضان، ۱۳٤۸-
عنوان و نام پدیدآور	: آشنایی با مبانی امنیت شبکه(امنیت اطلاعات) / تالیف رمضان عباس‌نژادورزی، آتنا فرجی
مشخصات نشر	: بابل:فن‌آوری نوین، ۱۳۸۹
مشخصات ظاهری	: ۱۹۲ ص. مصور ، جدول.
شابک	: ۶۰۰۰۰ ریال:۹۷۸٦۰۰۹۱٤۱۳۸۸
وضعیت فهرست نویسی	: فیپا
یاداشت	: کتابنامه
موضوع	: شبکه‌های کامپیوتری -- اقدامات تامینی
موضوع	: کامپیوترها—ایمنی اطلاعات
شناسه افزوده	: فرجی، آتنا، ۱۳٦۱-
رده بندی کنگره	: ۱۳۸۹ ٥ آ۲ع/TK٥۱۰٥/٥۹
رده بندی دیویی	: ۰۰٥/۸
شماره کتابشناسی ملی	: ۲۱۸۴۶۶۸

فن‌آوری نوین

بابل، کدپستی ٤۷۱٦۷-۷۳٤٤۸ تلفن: ۲۲۵٦٦۸۷-۰۱۱۱

www.fanavarienovin.net

آشنایی با مبانی امنیت شبکه (امنیت اطلاعات)

تألیف: مهندس رمضان عباس‌نژادورزی – مهندس آتنا فرجی

نوبت چاپ: چاپ اول

سال چاپ: زمستان ۱۳۸۹

شمارگان: ۱۰۰۰ جلد

قیمت: ٦۰۰۰ تومان

نام چاپخانه و صحافی: فرنگاررنگ

شابک: ۸- ۸- ۹۱٤۱۳ - ٦۰۰ - ۹۷۸

نشانی ناشر: بابل، چهارراه نواب، کاظم‌بیگی، جنب حسینیه منصور کاظم‌بیگی، طبقه همکف

طراح جلد: کانون آگهی و تبلیغات آبان (احمد فرجی)

تهران، خ اردیبهشت، نبش وحید نظری، پلاک ۱٤۲ تلفکس: ٦٦٤۰۰۲۲۰-٦٦٤۰۰۱٤٤

فهرست مطالب

فصل پنجم: بد افزار

فصل ششم: فایروال

فصل هفتم: امنیت در تجارت الکترونیک

فصل هشتم: سرویس‌ها و برنامه‌های کاربردی امنیت اطلاعات

مقدمه

امروزه اینترنت و یکی از مهم‌ترین مدل‌های ارتباطی در آن، یعنی شبکه جهانی وب (World Wide Web)، تغییرات اساسی در زندگی و روابط بین انسان‌ها ایجاد کرده است. به طوری که در عصر اطلاعات، فعالیت‌هایی از قبیل اطلاع رسانی، کسب و کار و تجارت، مدیریت و غیره به صورت مجازی انجام می‌شوند. فضای مجازی، در معرض چالش‌ها، آسیب‌ها و تهدیدهای مختلفی از قبیل تخریب اطلاعات، جاسوسی، خراب‌کاری، نقض حریم خصوصی، حملات انکار سرویس و دسترسی غیرمجاز می‌باشد. از طرف دیگر، کلیه کاربردهای فناوری اطلاعات مانند دولت الکترونیک، کسب‌وکار الکترونیک، تجارت الکترونیک، بانکداری الکترونیک، سلامت الکترونیک و دیگر کاربردها نیاز به زیرساخت اینترنت و شبکه‌های کامپیوتری دارند.

بی‌شک هیچ یک از این کاربردها بدون وجود امنیت نمی‌توانند مورد استفاده قرار گیرند. ایجاد امنیت در شبکه‌های کامپیوتری و اینترنت به امر خطیری تبدیل شده است، به طوری که در رشته‌های فناوری اطلاعات (IT) و فناوری اطلاعات و ارتباطات (ICT) درسی به نام **آشنایی با مبانی امنیت شبکه** تدوین شده است.

کتاب حاضر براساس سال‌ها تجربه در زمینه تالیف کتب دانشگاهی و تدریس طراحی گردید. این کتاب براساس سر فصل جدید وزارت علوم، تحقیقات و فناوری اطلاعات برای درس‌های آشنایی با مبانی امنیت شبکه، امنیت اطلاعات و امنیت شبکه در رشته‌های IT و ICT تدوین شده است.

در پایان امیدواریم این اثر نیز مورد توجه اساتید و دانشجویان عزیز قرار گیرد.

از تمامی عزیزانی که در جمع‌آوری این اثر ما را یاری نمودند، صمیمانه تشکر می‌کنیم.

بابل، زمستان۱۳۸۹

مولفین

فصل ۱ مقدمه‌ای بر امنیت

اکثر افراد قبل از ارسال نامه، آن را در پاکت قرار می‌دهند. اگر بپرسیم چرا این کار را می‌کنید، برخی پاسخ‌های زیر را می‌شنویم:

"واقعاً نمی‌دانم"، "از روی عادت"، "زیرا، بقیه این کار را می‌کنند".

آیا این پاسخ‌ها واقعاً صحیح هستند؟ یا دلایل دیگری وجود دارد. افراد در اصل برای جلوگیری از خواندن نامه‌ها توسط دیگران آن را درون پاکت قرار می‌دهند. حتی، اگر محتوی نامه شامل اطلاعات مهم یا شخصی نباشد، بسیاری از افراد برای این که مطمئن شوند، مکاتبات شخصی آن‌ها خصوصی می‌ماند آن را در پاکت قرار می‌دهند و مهر می‌کنند تا از دید افراد دیگر مخفی بماند و به دست گیرنده برسد. چون، اگر نامه را در یک پاکت باز قرار دهند و آن را ارسال نمایند، در بین راه افراد به راحتی می‌توانند محتوی آن را بخوانند و تغییر دهند، به طوری که راهی برای تشخیص خواندن و تعویض آن وجود ندارد.

امروزه، اکثر افراد از پست‌الکترونیک[1] به جای ارسال نامه‌ها از طریق اداره پست استفاده می‌کنند. پست‌الکترونیک ابزاری سریع برای انتقال نامه است. اما، در آن پاکتی برای محافظت از محتوی نامه (اطلاعاتی که از طریق پست الکترونیک ارسال می‌شود)، وجود ندارد. در واقع، ارسال نامه از طریق پست‌الکترونیک شبیه به پست نمودن نامه بدون پاکت است. بنابراین، اگر فردی بخواهد پیام شخصی یا اطلاعات محرمانه را از طریق پست‌الکترونیک ارسال کند، باید راهی جهت محافظت از نامه خود (جلوگیری از خواندن و تغییر توسط افراد دیگر) پیدا کند.

رایج‌ترین راه‌حل، استفاده از پنهان‌سازی است. زیرا، این روش پیام را رمز می‌کند. در این حالت، اگر پیام رمزشده (کدشده) به دست فرد دیگری (به جزگیرنده) برسد، آن فرد با خواندن پیام چیزی از اطلاعات آن نمی‌فهمد. با چگونگی رمزکردن[2] اطلاعات در فصل‌های دوم و سوم آشنا خواهید شد.

---

[1].Email [2].Cryptography

۱- ۱. اهمیت امنیت اطلاعات

قبل از این که به اهمیت امنیت اطلاعات بپردازیم، مقوله امنیت را در گذشته مورد بحث قرار می‌دهیم. همان‌طور که می‌دانید، امنیت در زمان‌های ماقبل تاریخ نیز جایگاه ویژه‌ای داشته است. در آن زمان انسان‌ها از جان خود در مقابل حیوانات وحشی محافظت می‌کردند. ابتدا، انسان‌ها برای خودشان خانه‌هایی ساختند تا از گزند حیوانات وحشی در امان بمانند. سپس، برای درب‌های خانه قفل‌ها تعبیه کردند یا نگهبان استخدام نمودند تا از اموال خانه (سرمایه) محافظت نمایند. با توجه به میزان اهمیت چیزی که از آن محافظت می‌شود، امنیت می‌تواند لایه‌ها و سطوح مختلف داشته باشد. به عنوان مثال، یک طلا فروشی را در نظر بگیرید. طلا فروش برای برقراری امنیت سه لایه (سطح) امنیتی را ایجاد می‌کند که عبارت‌اند از:

۱.درب مغازه طلا فروشی را می‌بندد.

۲.طلاها را در گاوصندوق ضد سرقت قرار می‌دهد.

۳.طلا فروشی را به سیستم ضد سرقت مجهز می‌نماید.

حال، یک نانوایی را در نظر بگیرید. نانوا، پس از خاتمه کار نانوایی، فقط درب نانوایی را می‌بندد (یعنی نیازی به گاوصندوق و سیستم ضد سرقت ندارد). بنابراین، همان‌طور، که بیان گردید، سطوح امنیتی که برای طلا فروشی ایجاد می‌کنیم، خیلی قوی‌تر و پیچیده‌تر از یک نانوایی است. زیرا، ارزش یک کیلوگرم طلا به مراتب بیشتر از چند کیسه آرد می‌باشد. پس ، امنیت برای چیزهایی مطرح می‌شود که مهم هستند و ارزش زیادی دارند. یعنی، برقراری امنیت برای سرمایه‌هایی از قبیل پول، طلا، عکس‌ها و فیلم‌های خانوادگی، رازهای زندگی، رمز کارت‌های حساب بانکی و غیره مهم هستند.

اکنون این سوال مطرح می‌شود، آیا اطلاعات در فضای کامپیوتر (مجازی) سرمایه هستند یا خیر؟ آیا این اطلاعات نیاز به محافظت دارند یا نه؟

برای این که به این سوال پاسخ دهیم، به مثال‌های زیر می‌پردازیم:

۱. فرض کنید کارمند شهرداری یکی از شهرهای بزرگ هستید. در سیستم رایانه‌ای شهرداری اطلاعاتی از قبیل طرح‌های نوسازی شهر، اتوبان‌هایی که قرار است در شهر ایجاد شوند و مکان آن‌ها، مکان فضاهای سبز، پارک‌ها و غیره ذخیره شده است. آیا این اطلاعات نیاز به محافظت دارند. در نگاه اول ممکن است فکر کنید، این اطلاعات ارزش چندانی ندارند و نیاز به محافظت ندارند. اما، اگر این اطلاعات به دست افراد خاصی برسند، می‌توانند درآمدهای چند میلیاردی از آن کسب کنند. زیرا، این افراد زمین‌های اطراف این مکان‌ها را به قیمت خیلی پایین می‌خرند و پس از مدت کوتاهی این زمین‌ها را با چندین برابر قیمتی که خریداری کردند، می‌فروشند.

۲. فرض کنید در شرکتی کار می‌کنید که در مناقصات میلیاردی شرکت می‌کند و اطلاعات پیشنهادی قیمتش را در کامپیوتر شرکت ذخیره می‌کند. از طرف دیگر، فرض کنید، فقط چند شرکت در این مناقصات شرکت می‌کنند. اگر یک شرکت بتواند اطلاعات پیشنهاد قیمت شرکت-های دیگر را به دست آورد، به راحتی می‌تواند در مناقصه برنده شود.

۳. شرکتی را در نظر بگیرید که مواد اولیه کارخانجات کشور را خریداری می‌کند. این شرکت مواد اولیه مورد نیاز را در فایل‌های اکسل و **Word** ذخیره می‌کند و برروی کامپیوتر شرکت نگهداری می‌نماید. آیا این اطلاعات نیاز به محافظت دارند؟ برای پاسخ به این سوال، سوال دیگری مطرح می‌شود. اگر این اطلاعات در اختیار دشمنان کشورمان قرار بگیرند، چه مشکلی را ایجاد می‌کند؟ چون این مواد از کشور خارجی خریداری می‌گردد و چنانچه مشخص باشد، مواد اولیه از کدام کشور خریداری می‌شود، دشمنان با تنگ کردن حلقه‌ی تحریم، موجب جلوگیری از فروش آن مواد به ایران می‌شوند.

٤. فرض کنید، کارتی دارید که از طریق آن از عابر بانک‌ها پول برداشت می‌کنید. آیا کارت و کلمه عبور آن را در اختیار غریبه قرار می‌دهید؟

۵. فرض کنید، از طریق اینترنت خرید و فروش الکترونیکی انجام می‌دهید. اگر بدانید که فضای اینترنت امن نیست و ممکن است سرمایه‌تان سرقت شود، آیا در این فضا خرید و فروش انجام خواهید داد؟

از طرف دیگر، شاید در خبرها شنیده باشید که بی‌توجهی و سهل‌انگاری در برقراری امنیت اطلاعات، خسارت‌های زیادی را به افراد حقیقی و حقوقی وارد کرده است. چند نمونه از این خبرها در زیر آمده‌اند:

۱. یک هکر هزینه‌ای برابر با دوازده هزار دلار را روی دست آژانس فدورال مدیریت آژانس آمریکا گذاشت.

۲. گروهی از هکرها ادعا می‌کنند که توانسته‌اند به صندوق پست الکترونیکی خانم سارا پلین (معاون نامزد جمهوری خواهان در انتخاب ریاست جمهوری ایالات متحده) دست یابند.

۳. حساب بانکی رئیس جمهور فرانسه (نیکولاساركوزی) هک شد.

٤. یک هکر که به حساب‌های بانک شهروندان تهرانی نفوذ می‌کرد، به دام افتاد.

۵. به فاصله کوتاهی پس از عبور تانک‌های ارتش روسیه از مرزهای گرجستان، وب سایت دولتی گرجستان آماج حمله قرار گرفت.

٦. بنابر تخمین شرکت سمانتیک امروزه ۱/۲ درصد از پیام‌های پست‌الکترونیک حاوی بدافزارهای مخرب هستند.

۷. به تازگی هرزنامه جدیدی در فضای اینترنت منتشر شده است که وانمود می‌کند، از سوی جان پیستول، معاون مدیر FBI صادر شده است.

۸. یک کامپیوتر دست دوم که اطلاعات کارت اعتباری تعدادی از مشتریان بانک انگلیسی برروی آن ذخیره شده بود، در جریان یک بی‌احتیاطی فروخته شد.

۹. تعداد کل بدافزارهای تولید شده در سال ۲۰۰۷ برابر کل بدافزارهای تولید شده در ۱۵ سال قبل آن بوده است.

۱۰. بنابر اعلام شرکت سمانتیک ۷۸ درصد از حجم کل ایمیل‌های جهان از اسپم تشکیل شده است.

۱۱. آیا موساد پشت نرم‌افزارهای اسرائیلی پنهان شده است؟

پیدا کردن برخی اطلاعات شخصی و پاسخ به سوالات امنیتی می‌تواند از طریق جستجو در اینترنت به راحتی صورت گیرد. یکی از هکرها به همین صورت موفق گردید، به پست الکترونیکی خانم سارا پلین دسترسی پیدا کند.

علاوه براین خبرها، هر روز هزاران خبر دیگر را در زمینه سرقت اطلاعات در اینترنت می‌بینید. از طرف دیگر، امروزه با توسعه رایانه‌ها و گسترش شبکه‌های کامپیوتری مانند اینترنت، امنیت شبکه‌های کامپیوتری و اطلاعات به امری بسیار مهم و حیاتی تبدیل گردیده است.

۲ – ۱. مقایسه امنیت اطلاعات در گذشته و حال

امنیت اطلاعات یکی از دغدغه‌های بسیار مهم بشر بوده است. به طوری که در گذشته اطلاعات مهم را در قفسه‌های قفل‌دار نگهداری می‌کردند. این قفسه‌ها را در مکان‌های امن قرار می‌دادند و از نگهبان جهت محافظت از این مکان استفاده می‌کردند. در حالی که امروزه، این اطلاعات در کامپیوترها نگهداری می‌شوند. برای برقراری ارتباط از شبکه‌های کامپیوتری استفاده می‌شود و از روش‌های متعددی از قبیل رمزگذاری، امضای دیجیتال و غیره برای برقراری امنیت اطلاعات استفاده می‌شود. با این روش‌های برقراری امنیت در ادامه بیشتر آشنا خواهیم شد.

به زبان ساده می‌توان گفت در گذشته امنیت با حضور فیزیکی و نظارت تامین می‌گردید. ولی، امروزه از ابزارهای خودکار و مکانیزم‌های هوشمند برای برقراری امنیت و حفاظت از داده استفاده می‌کنند.

فصل ۲ رمزگذاری‌های کلاسیک

در فصل اول، انواع حملات را دیدید. یکی از حملات، حمله غیر فعال استراق سمع می‌باشد. برای جلوگیری از این حمله، از رمزنگاری استفاده می‌شود. دو مدل رمزنگاری وجود دارد:

۱. مدل رمزنگاری متقارن (Symmetric Cipher Model).

۲. مدل رمزنگاری نامتقارن (Asymmetric Cipher Model).

۱ –۲. مدل رمزگذاری متقارن

در این نوع رمزنگاری یک کلید بین فرستنده و گیرنده اطلاعات مشترک است. فرستنده متن ساده[۲] (اصلی) را با الگوریتم رمزگذاری[۲] و کلید سرّی[۳] به متن رمز شده[٤] تبدیل می‌کند و گیرنده متن رمز شده را گرفته و با الگوریتم رمز گشایی[٥] و همان کلید آن را به متن ساده و قابل فهم تبدیل می‌کند (شکل ۱–۲).

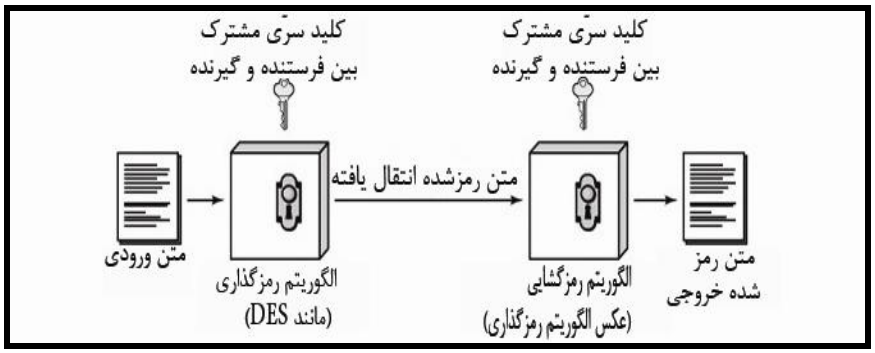
مدل رمزنگاری متقارن از پنج عنصر تشکیل شده است که عبارت‌اند از:

☒ **متن ساده (اصلی)**: پیام قابل فهم یا داده‌ای که ورودی الگوریتم رمزگذاری است.

☒ **الگوریتم رمزگذاری**: الگوریتم رمزگذاری که جانشینی‌ها و جابه‌جایی‌های گوناگون را روی متن ساده انجام می‌دهد تا آن را به متن رمز شده (غیر قابل فهم) تبدیل کند.

---

[1].PlianText [2].Encryption Algorithm [3]. Secret Key [4].CipherText [5].Decryption Algorithm



شکل ۱ – ۲ مدل ساده شده رمزگذاری مرسوم.

☒ **کلید سرّی:** کلیدی که یکی از ورودی‌های الگوریتم رمزگذاری و رمزگشایی است. چون این کلید بین فرستنده و گیرنده پیام مشترک است، باید سرّی بماند. کلید سرّی به متن و الگوریتم وابسته نیست. یعنی، جابه‌جایی و جانشینی دقیق توسط الگوریتم وابسته به کلید اجرا می‌شوند.

☒ **متن رمزشده:** پیامی غیر قابل فهم که خروجی الگوریتم رمزگذاری می‌باشد. غیر قابل فهم بودن این متن، به طول کلید سرّی و قدرت الگوریتم رمزگذاری وابسته است.

☒ **الگوریتم رمزگشایی:** در حقیقت این الگوریتم معکوس الگوریتم رمزگذاری است. این الگوریتم متن رمز شده و کلید سرّی را به عنوان ورودی دریافت می‌کند و خروجی آن متن ساده (متن اصلی قابل فهم) می‌باشد.

برای ایمن سازی رمزگذاری دو نیازمندی وجود دارد:

۱. الگوریتم رمزگذاری قوی: یعنی، الگوریتم باید به گونه‌ای باشد که معارض[3] نتواند متن رمزشده را رمزگشایی کند یا کلید را کشف کند.

۲. فرستنده و گیرنده باید کپی کلید سرّی را از یک روش امن به دست آورده و کلید را جای امنی نگهداری کنند.

اگر فردی بتواند کلید را کشف کرده و الگوریتم را بداند، تمام مکاتبات فرستنده و گیرنده که از این کلید استفاده گردد، قابل فهم (خواندن) می‌شود.

---

[1].opponent

فرض می‌کنیم دانش الگوریتم رمزگذاری/ رمزگشایی مشخص باشد، با این حال رمزگشایی پیام رمزشده، عملی نیست. یعنی، نیازی نیست الگوریتم را مخفی کنیم، فقط باید کلید مخفی باشد. این ویژگی رمزگذاری متقارن آن را جهت استفاده به صورت گسترده عملی می‌نماید. این واقعیت که نیازی نیست الگوریتم مخفی بماند، به این معنی است که سازندگان می‌توانند الگوریتم‌های رمزگذاری و رمزگشایی داده را برروی یک تراشه ارزان قیمت قرار دهند.

در هنگام استفاده از رمزگذاری متقارن مسئله اصلی امنیت، پنهان نگه داشتن کلید است. شکل ۲ – ۲ جزئیات رمزگذاری متقارن را نشان می‌دهد. پیام به صورت دنباله‌ای از کاراکترها ($X = [x_1,x_2,\ldots x_n]$) می‌باشد. N، تعداد حروف الفبای متناهی است (الفبای لاتین از ۲۶ حرف تشکیل شده است).

امروزه از الفبای باینری $\{0 , 1\}$ استفاده می‌گردد. کلید به شکل $k = \{k_1, k_2,\ldots,k_j\}$ تولید می‌شود. بعد از تولید کلید، باید توسط کانالی امن به مقصد تحویل داده شود. کلید می‌تواند توسط شخص ثالث تولید شده و به منبع (مبداء) و مقصد تحویل داده شود.

الگوریتم رمزگذاری، پیام X و کلید رمزگذاری K را به عنوان ورودی دریافت کرده، متن رمز $y = [y_1,y_2,\ldots,y_n]$ را تولید می‌کند. یعنی:

$$Y = E (K , X)$$

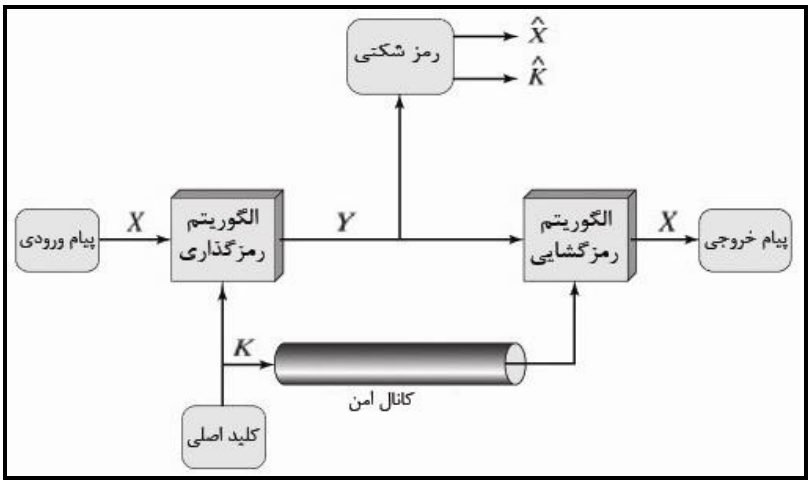
این فرمول نشان می‌دهد الگوریتم رمزگذاری E (به عنوان یک تابع) با استفاده از کلید K و متن ساده X، متن رمز شده Y را تولید می‌کند.

همان‌طور که بیان کردیم کلید K بین گیرنده و فرستنده مشترک است. بنابراین، گیرنده با فرمول مقابل می‌تواند متن رمز شده Y را به متن ساده X برگرداند:

$$X = D (K , Y)$$

در این فرمول D، معکوس تابع E است.

مهاجم (معارض)، که Y را در اختیار دارد، ولی K یا X را ندارد، سعی می‌کند X یا K یا هر دو را به دست آورد. فرض شده است که معارض الگوریتم رمزگذاری (E) و رمزگشایی (D) را می‌داند، اگر معارض بخواهد این پیام را رمزگشایی کند، آنگاه روی این پیام متمرکز می‌شود که بتواند پیام را رمزگشایی نماید. در این حالت تلاش می‌کند کلید K را به دست آورد که پیام X را تولید می‌کند (شکل ۲–۲).



شکل ۲ – ۲ مدل سیستم رمزقراردادی.

۲–۲. رمز نویسی

سیستم‌های رمزنویسی[4] از سه بعد زیر با یکدیگر مقایسه می‌شوند:

۱. نوع عملیات استفاده شده برای تبدیل متن ساده به متن رمز، تمام الگوریتم‌های رمزگذاری براساس دو اصل کلی (جانشینی و جابجایی) بنا شده‌اند. **جانشینی**[2] یعنی، هر عنصر در متن، یک بیت، بایت، حرف، مجموعه‌ای از بیت‌ها یا حروف) با عنصر دیگر جایگزین می‌شود. **انتقال**[3] یعنی، جای (مکان) عناصر در متن جابه‌جا می‌شود. در این جابه‌جایی و جانشینی نباید هیچ اطلاعاتی گم شود. یعنی، همه عملیات برگشت پذیر باشند. اکثر سیستم‌هایی که به صورت سیستم‌های محصول[4] در آمده‌اند، مراحل چندگانه جابه‌جایی و جانشینی را انجام می‌دهند (مانند الگوریتم DES).

۲. تعداد کلیدهای استفاده شده، اگر گیرنده و فرستنده از یک کلید مشترک استفاده کنند، سیستم به صورت متقارن (تک کلید یا کلید سرّی) تعریف می‌شود (نام دیگر این الگوریتم قراردادی است). ولی، چنانچه گیرنده و فرستنده از کلیدهای متفاوتی استفاده نمایند، سیستم به صورت نامتقارن (دو کلید یا الگوریتم کلیدی عمومی) تعریف می‌شود.

۳. روشی که در آن متن پردازش می‌شود، رمز کننده ممکن است بلوکی[5] یا دنباله‌ای[2] باشد. در رمزکننده بلوکی، یک بلوک از عناصر به عنوان ورودی دریافت می‌شود، و بلوکی از عناصر رمز شده

---

[1] .Cryptography [2]. Substitution [3]. Transposition [4].Product Systems

تولید می‌شود. ولی، رمز کننده دنباله‌ای، عناصر ورودی را به صورت متوالی (پشت سرهم) پردازش کرده و یک عنصر خروجی رمز شده را در یک لحظه تولید می‌کند.

۳ -۲. رمز شکنی خطی

اساساً، هدف حمله به سیستم رمزگذاری کشف کلید استفاده شده است. یعنی، حمله‌کننده می‌خواهد به جای کشف متن ساده از متن رمز، کلید را به دست آورد. دو روش کلی حمله به الگوریتم مرسوم رمزگذاری وجود دارد که عبارت‌اند از:

۱. رمزشکنی خطی[۳] **۲.** حمله جستجوی جامع[٤]

---

[5].Block [2].Stream [3].Cyptanalysis [4].Brute – Force Attack

فصل ۳ رمزگذاری‌های پیشرفته متقارن و نامتقارن

۱ – ۳. رمزگذاری‌های پیشرفته

در فصل دوم، با برخی از رمزگذاری‌های کلاسیک آشنا شدیم. همان‌طور که در این رمزگذاری‌ها دیدید، رمزگشایی بدون داشتن کلید با تلاش امکان‌پذیر بوده است. در این فصل می‌خواهیم برخی از رمزگذاری‌های پیشرفته را بیاموزیم که رمزگشایی بدون کلید مشکل است. برخی از این رمزگذاری‌ها عبارت‌اند از:

۱. رمزگذاری بلوکی
۲. رمزگذاری DES
۳. رمزگذاری AES
۴. رمزگذاری RC4
۵. رمزگذاری RC5
۶. رمزگذاری نامتقارن (کلید عمومی)

۲–۳. رمزگذاری بلوکی

رمزگذاری بلوکی[6] یک بلوک از متن را گرفته با روش‌های جایگشتی، جانشینی و کلید آن را رمزکرده، یک بلوک رمزشده را برمی‌گرداند. در ادامه برخی از این نوع رمزگذاری‌ها را می‌بینید.

۱ – ۲ –۳ . اصول رمزهای بلوکی

این روش ترکیبی از روش‌های ساده جانشینی و جایگشت است که ترکیب آن‌ها الگوریتم پیچیده و امنی را ایجاد می‌کند. اغلب الگوریتم‌های بلوکی متقارن از ساختار رمز بلوکی فیستل[2] استفاده می‌کنند.

این فصل را با مقایسه رمزکننده دنباله‌ای[3] و رمزکننده‌های بلوکی آغاز می‌کنیم. سپس، راجع به هدف ساختار رمزکننده بلوکی فیستل بحث می‌کنیم. در پایان به برخی مفاهیم و رمزگذاری‌های پیشرفته می‌پردازیم.

۲ – ۲ –۳ . رمزکننده دنباله‌ای و بلوکی

دو نوع رمزگذاری وجود دارد که عبارت‌اند از:

---

[6].Block cipher [2].Feistel Cipher [3].Stream Ciphers [4].Vernam Cipher

☒**رمزکننده دنباله‌ای**، نوعی از رمزگذاری است که دنباله داده دیجیتال را به صورت یک بیتی یا یک بایتی در یک مرحله رمزگذاری می‌کند. یک نمونه از رمزکننده دنباله‌ای کلاسیک رمز ویجنرو رمز ورنام[٤] است.

☒ **رمزکننده بلوکی**، بلوک‌های متنی را به بلوک‌های رمز شده با طول یکسان تبدیل می‌کند. در کل، در این نوع رمزکننده اندازه بلوک ٦٤ بیتی یا ۱۲۸ بیتی است. رمزکننده‌های بلوکی کاربرد بیشتری نسبت به رمزکننده‌های دنباله‌ای دارند. بنابراین، روی این رمزکننده‌ها تمرکز می‌شود.

۳ – ۲ – ۳ . هدف ساختار رمزکننده فیستل

رمزکننده بلوکی، بلوک n بیتی متن را به بلوک رمزشده n بیتی تبدیل می‌کند. اکنون ۲^n بلوک متنی مختلف برای برگرداندن متن اصلی وجود دارد. این نوع تبدیل‌ها، برگشت‌پذیر[۷] یا غیر یکتا[۲] نامیده می‌شوند. به عنوان مثال، تبدیل‌های برگشت‌پذیر و برگشت‌ناپذیر را به صورت زیر مشاهده می‌کنید.

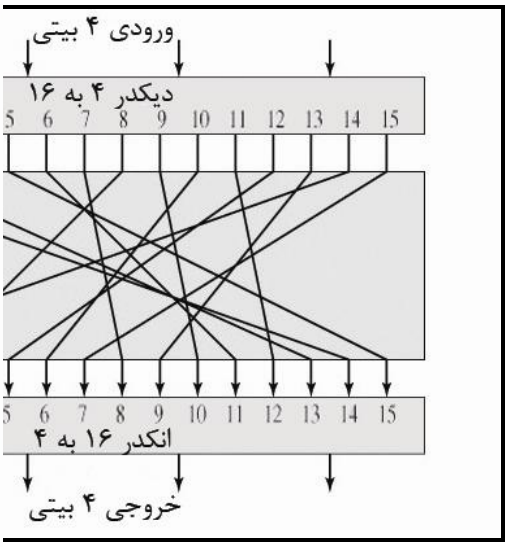
نگاشت برگشت‌ناپذیر	
متن رمزشده	متن اصلی
11	00
10	01
01	10
01	11

نگاشت برگشت‌پذیر	
متن رمزشده	متن اصلی
11	00
10	01
00	10
01	11

در نگاشت برگشت ناپذیر، متن رمزشده "01" توسط یک یا دو بلوک متنی بوجود آمده است. بنابراین، اگر به نگاشت‌های برگشت‌پذیر محدود شویم تعداد تبدیل‌های مختلف $!۲^n$ می‌شود. شکل ۱– ۳ منطق رمز جاینشینی برای n = 4 را نشان می‌دهد. ورودی ٤ بیتی یکی از ١٦ حالت ممکن ورودی را تولید می‌کند، که توسط رمز جانشینی به یکی از ١٦ حالت ممکن خروجی یکتا نگاشت می‌شود، که هر کدام با ٤ بیت رمزشده نشان داده می‌شود.

---

[7].Reversible [2].Nonsignular



شکل ۱ – ۳ جانشینی بلوکی n بیت جامع.

متن رمزشده	متن اصلی
1110	0000
0100	0001
1101	0010
0001	0011
0010	0100
1111	0101
1011	0110
1000	0111
0011	1000
1010	1001
0110	1010
1100	1011
0101	1100
1001	1101
0000	1110
0111	1111
1110	0000
0011	0001
0100	0010
1000	0011
0001	0100
1100	0101
1010	0110
1111	0111
0111	1000
1101	1001
1001	1010
0110	1011
1100	1100
0010	1101
0000	1110
0101	1111

شکل ۲ – ۳ جدول رمزگذاری و رمزگشایی

این کلی‌ترین شکل رمزگذاری بلوکی است و می‌توان آن را برای هر نگاشت برگشت‌پذیر برای متن اصلی و متن رمزشده تعریف کرد. فیستل از این روش به عنوان رمز بلوکی مطلوب استفاده می‌کند، زیرا حداکثر تعداد نگاشت‌های رمزگذاری ممکن را از بلوک متنی می‌پذیرد. نگاشت‌های رمزگذاری و رمزگشایی با جدول‌بندی قابل تعریف هستند، که در شکل ۲ – ۳ نشان داده شده است. اما یک مشکل اصلی برای رمز بلوکی وجود دارد. اگر اندازه کوچکی از بلوک مانند $n = 4$ بکار رود، سیستم مانند یک سیستم رمز جانشینی کلاسیک عمل می‌کند.

همان‌طور که دیدیم، این گونه سیستم‌ها با تحلیل آماری متن آسیب‌پذیرند. این ضعف در استفاده از رمز جانشینی همیشگی نیست، اما به نسبت بلوک‌های کوچک حاصل می‌شود. اگر n به اندازه کافی بزرگ باشد و جانشینی برگشت‌پذیر مطلق بین متن اصلی و متن رمزشده مجازی باشد، ویژگی‌های آماری متن اصلی به کلی پوشیده می‌شود که این نوع رمز جانشینی برگشت‌پذیر مطلق برای بلوک با اندازه بزرگ از نظر کارایی و اجرا کاربردی نیست.

در این نوع تبدیل، نگاشت خودش کلید را ترکیب

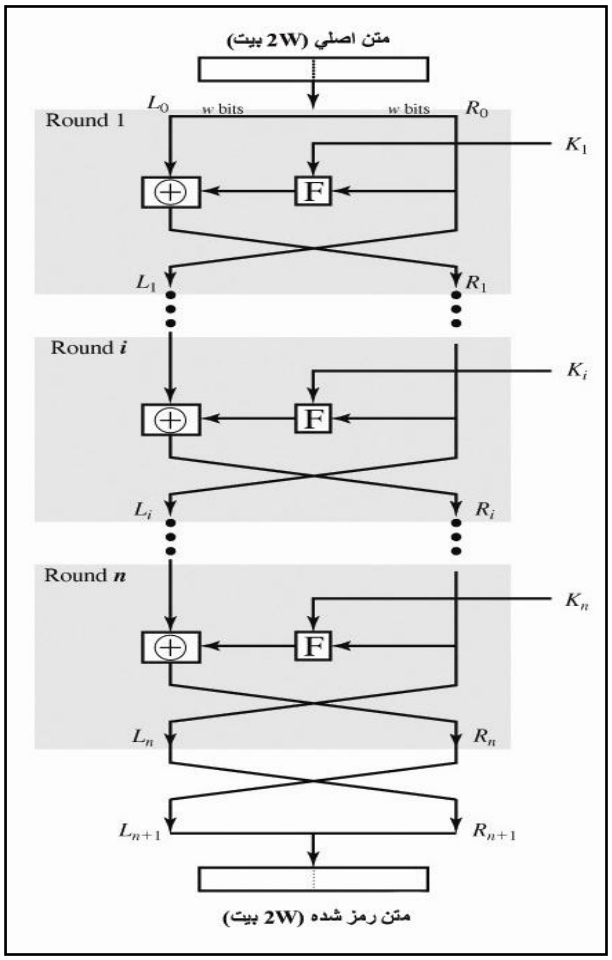
می‌کند. با برگشت به شکل ۲ – ۳ که نگاشت **برای رمزجانشینی**. برگشت‌پذیر را تعریف می‌کند، می‌بینیم که نگاشت می‌تواند توسط ورود در ستون دوم تعریف شود. که مقدار متن رمزشده را برای هر بلوک متنی نشان می‌دهد. این اساساً کلیدی است که نگاشت بخصوصی از میان نگاشت‌های موجود را تعیین می‌کند. در این حالت، طول کلید مورد نیاز بیت ٦٤ = ١٦سطر × ٤ بیت می‌باشد.

در کل، برای رمز بلوکی ایده‌آل n بیتی، طول کلید تعریف شده در این روش $n \times 2^n$ بیت است. برای بلوک ٦٤ بیتی که طول مناسبی برای خنثی کردن حملات آماری است، طول کلید مورد نیاز $2^{70} = 2^{64} \times 64 \sim 10^{21}$ بیت است.

با ملاحظه این مشکلات، فیستل مولفه‌های لازم برای تولید رمزبلوکی نزدیک به سیستم رمزبلوکی مطلوب برای nهای بزرگ را نشان می‌دهد.

۳–۳. رمز فیستل

فیستل در رابطه با رمز بلوکی، پیشنهادی را مطرح نمود که می‌توان رمز بلوکی مناسبی را با بکارگیری رمز تولیدشده تقریب زد، اجرای دو یا چند رمز ساده بطور متوالی است. در این روش، نتیجه نهایی قوی‌تراز رمزهای ترکیبی است.



در این روش طول کلید K بیت بوده و طول بلوک n بیت است که 2^k تبدیل ممکن را بیشتر از $2^n!$ تبدیل موجود با رمز بلوکی مناسب مجاز می‌کند. در سیستم رمز فیستل جانشینی‌ها و جایگشت‌ها به نوبت انجام می‌شود.

۱–۳–۳. ساختار رمز فیستل

در شکل ۳ – ۳ ساختار پیشنهادی فیستل را می‌بینید.

ورودی‌های الگوریتم رمزگذاری، بلوک متن اصلی با طول 2w بیت و

کلید k بیتی است. متن اصلی به دو نیمه L_0 و R_0 تقسیم می‌شوند.
این دو نیمه از یک فرآیند n مرحله‌ای عبور کرده و سپس، جهت تولید بلوک متن رمزشده باهم ترکیب می‌شوند که در شکل ۳-۳ این مراحل را مشاهده می‌کنید. **شکل ۳ – ۳ شبکه فیستل کلاسیک**.

ورودی هر مرحله (iام)، L_{i-1}، R_{i-1} و زیر کلیدها است. این ورودی‌ها از مرحله قبلی و کلید اصلی k مشتق شده‌اند.
در واقع، زیر کلیدهای k_i با کلید اصلی k و همچنین با خودشان متفاوت هستند. تمامی مراحل ساختار مشابه دارند. جانشینی روی نیمه چپ داده انجام می‌شود. این عمل با بکارگیری تابعی گردکننده[۸] به نام F روی نیمه راست داده انجام می‌شود و سپس، خروجی تابع F با نیمه چپ داده OR انحصاری (XOR) می‌شود. تابع گردکننده F همان ساختار را برای هر مرحله دارد. اما با زیر کلید k_i هر مرحله مقداردهی می‌شود. به دنبال این جانشینی، جایگشت اجرا می‌شود که از تعویض دو نیمه داده تشکیل شده است. این ساختار روش شانون[۲] را بری شبکه جانشینی – جایگشتی[۳] نشان می‌دهد

[8] .Round Function [2] .Shannon [3].Substition – Permutation Network (SPN)

فصل ۴ امنیت شبکه و محیط کاری

قبل از این که به امنیت شبکه و محیط کاری بپردازیم، ابتدا تهدیداتی که برای شبکه وجـود دارنـد، را بررسی می‌کنیم. دو نوع تهدید موجود در شبکه عبارت‌اند از:

۱. دسترسی افراد غیر مجاز در شبکه.
۲. تخریب داده‌ها در شبکه.

بنابراین، در این فصل ابتدا به روش‌های دسترسی غیر مجاز در شبکه و دلایـل تخریـب اطلاعـات می‌پردازیم. سپس، لیست‌های کنترل امنیتی که سازمان‌ها و اشخاص باید چک کنند تا از دسترسی افراد غیر مجاز به شبکه و تخریب داده‌ها جلوگیری نمایند را می‌بینید.

۱ – ۴. دسترسی افراد غیر مجاز در شبکه

امروزه یکی از رایج‌ترین و مهم‌ترین تهدیداتی که در شبکه‌های کامپیوتری وجـود دارد، دسترسـی افراد غیرمجاز است. دسترسی افراد غیر مجاز در یکی از بخش‌های زیر رخ می‌دهد:

۱. اتصالات فیزیکی شبکه
۲. سرورها و زیرساخت‌های مرکزی و اصلی
۳. کامپیوترهای رومیزی

۱ – ۱ – ۴ . اتصالات فیزیکی شبکه

امروزه کامپیوترها در شبکه به روش‌های مختلفی با یکدیگر متصل می‌گردند. برخی از این روش‌ها عبارت‌اند از:

۱. شبکه‌های کابلی
۲. شبکه‌های فیبر نوری
۳. شبکه‌های بی‌سیم

۱. شبکه‌های کابلی

اکثر شبکه‌های محلی از کابل‌های مسی مانند کابل‌های شبکه معمولی و کابل‌های تلفن برای اتصال رایانه‌ها به شبکه‌ها استفاده می‌کنند. از آنجائی که در کابل‌های مسی امکان شنود و استراق سمع وجـود

دارد، لذا، به کارگیری آن‌ها در محیط‌های ناامن جهت تبادل و انتقال اطلاعات محرمانه، خطرناک می‌باشد.

۲. شبکه‌های فیبرنوری

شبکه‌هایی که از فیبرنوری[۹] تشکیل شده‌اند، بندرت جهت اتصال کامپیوترها در شبکه‌ها استفاده می‌شوند. زیرا، هزینه راه‌اندازی و نگهداری آن‌ها بسیار بالا است. اما، شبکه‌هایی که از فیبرنوری برای اتصال کامپیوترها استفاده می‌کنند، نسبت به روش‌های دیگر شنودپذیری و استراق سمع کمتری دارند.

۳. شبکه‌های بی‌سیم

استفاده از شبکه‌های بی‌سیم[۲] به مراتب خطرناک‌تر از شبکه‌های کابلی و فیبرنوری است. زیرا، از آنجائی که دسترسی به شبکه، خارج از ساختمان و در محل دیگر امکان‌پذیر است، امکان شنود در این شبکه‌ها را به مراتب بیشتر از شبکه‌های دیگر افزایش می‌دهد.

روش‌های ایجاد ارتباط ایمن در شبکه

روش‌های متعددی برای ایجاد ارتباط ایمن در شبکه وجود دارند. دو روش ایجاد ارتباط ایمن را در زیر می‌بینید:

۱. استفاده از شبکه‌های محلی مجازی[۳]

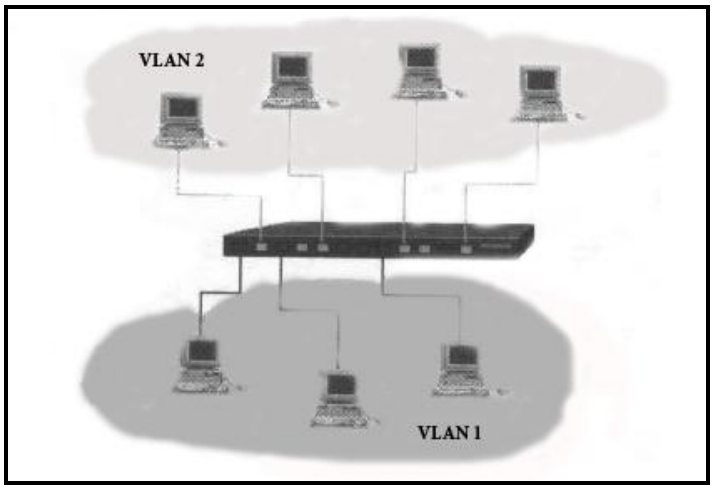
۲. استفاده از شبکه‌های خصوصی مجازی[٤]

۱. استفاده از شبکه‌های محلی مجازی

اگر بدون تغییر ساختار فیزیکی شبکه با تنظیم روی سوئیچ‌های شبکه، بتوانیم شبکه‌ای مستقل ایجاد کنیم، به صورتی که کامپیوترهای دیگر موجود در شبکه نتوانند به این شبکه دسترسی داشته باشند، تشکیل شبکه VLAN را داده‌ایم. در شکل ۱ – ٤ نمونه‌ای از شبکه VLAN را می‌بینید. در این شکل کامپیوترهای عضو VLAN1 نمی‌توانند به کامپیوترهای عضو VLAN2 دسترسی داشته باشند.

---

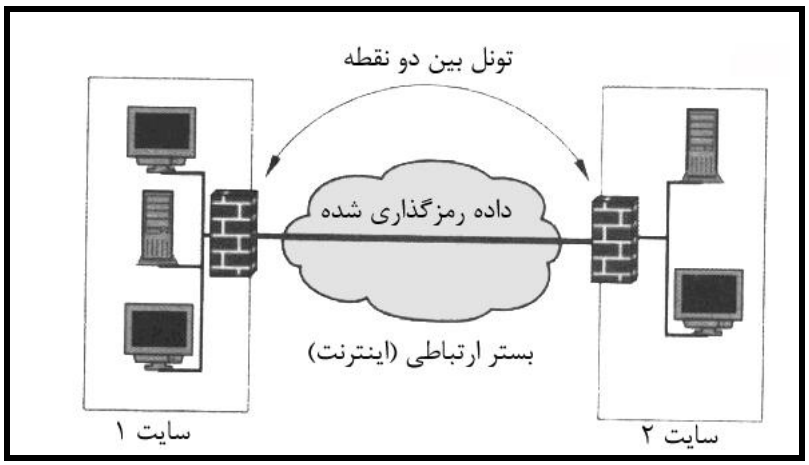
[9] .Fiber Optic [2].Wireless [3] .Virtual LAN [4].Virtual Private Network



شکل ۱ – ۴ محیط شبکه محلی مجازی (VLAN).

۲. شبکه خصوصی مجازی

همان‌طور که می‌دانید، گاهی اوقات نیاز است که اطلاعات از طریق فضای ناامن مانند اینترنت تبادل شوند. برای جلوگیری سرقت اطلاعات بین کامپیوترهای مبداء و مقصد، یک شبکه VPN ایجاد می‌نماییم. این عمل، به **تونل زدن** معروف است. در شکل ۲ – ٤ نمونه‌ای از تونل زدن را می‌بینید. در این شکل اطلاعات در محیط اینترنت بین دو کامپیوتر با رمزگذاری و تونل زدن انتقال می‌یابند.



شکل ۲ – ۴ تونل مجازی.

۲ – ۱ – ۴. سرور و زیر ساخت مرکزی و اصلی

سرورها معمولاً در اتاق‌های ظاهراً خوبی محافظت شده، در زیر زمین یا طبقه همکف قرار داده می‌شوند و در مقایسه با اتاق‌ها در یک طبقه بالاتر، خطر دزدی و ورود سیلاب را به عنوان نکته‌ای مهم باید در نظر داشت.

به خصوص، تخصیص مناسب اتاق‌ها و طرح‌هایی که دستیابی عموم را به طبقات آسان می‌سازد، باعث می‌شوند که پیدا کردن اتاق سرور حتی برای غریبه‌ها آسان شود و اگر تعداد افراد غیر عضو یا غریبه (مانند مشتریان تامین کنندگان) به این طبقه دسترسی داشته باشند، حضور آن‌ها در جلوی اتاق‌های سرور باعث جلب توجه نمی‌شود. در کمپانی‌های کوچک، اتاق‌های سرور غالباً به عنوان محل‌های انبار نیز استفاده می‌شوند که این امر بدین معنی می‌باشد که افرادی که نباید وارد اتاق‌های سرور بشوند، می‌توانند به آن‌ها دستیابی پیدا کنند. در بیشتر موارد، تفکیک اتاق یا محل انبار مستلزم هزینه و تلاش زیادی نمی‌باشد. همچنین، پرینترهای مرکزی و اصلی (مانند پرینترهای لیزری رنگی، پرینترهای با سرعت بالا) نباید برای پایین نگهداشتن تعداد افراد که به آن‌ها دسترسی دارند، در اتاق سرور قرار داده شوند و بلکه بهتر است که دو یا سه اتاق جداگانه داشته باشیم که اولی می‌تواند محل قرار دادن وسایل مرکزی و اصلی باشد که توسط تعداد زیادی از کارکنان (لیزر رنگی، پلاتر یا رسام) مورد استفاده قرار می‌گیرد. در اتاق دوم نیز وسایلی قرار داده می‌شوند که ضروری و مهم نمی‌باشند که در بعضی از شرکت‌ها می‌تواند شامل سرورهای وب باشد. در اتاق سوم نیز ایمن‌ترین وسایل و تجهیزات یعنی فایل سرور[۱۰] و سرور مجوز و تایید اعتبار (مانند کربروس[۲]، Active Directory) قرار داده می‌شوند. با مفهوم سرویس کربروس در ادامه آشنا خواهید شد.

در سازمان‌های کوچک، پشتیبان‌ها نیز مستقیماً در فایل سرور انجام می‌شوند و به منظور حفاظت قویاً توصیه می‌شود که آن‌ها را در محل دیگری نگهداری و ذخیره کنید و ضروری است که این محل نیز باید بسیار مطمئن و ایمن باشد. حفاظت از نسخه‌های پشتیبان در برابر تخریب توسط آتش، سیل، زلزله و موارد مشابه غالباً زیاد مهم نمی‌باشد، زیرا احتمال اینکه نسخه‌های پشتیبان و همچنین داده‌های اصلی در یک زمان از بین بروند نسبتاً کم می‌باشد.

به هر حال این خطر که افراد غیر مجاز بتوانند به نسخه‌های پشتیبان دسترسی پیدا کنند، بسیار زیاد می‌باشد. بهترین سیستم‌های کنترل دستیابی و تایید مجوز در شبکه داخلی اگر تمام داده‌ها در روی نوارها قابل دسترسی باشند، بی‌فایده هستند. زیرا برای مثال، شخصی می‌تواند آن‌ها را به سادگی در یک کیف دستی یا روی صندلی عقب اتومبیل خود جا بگذارد.

---

[10].File Server [2]. Kerberos [3].Workstation

فصل ۵ بدافزارها

کلمه ویروس به عنوان یک عبارت عمومی برای انواع مختلف حمله‌های رایانه‌ای با کد مخرب استفاده می‌شود. به عنوان مثال، ویروس‌های رایانه‌ای، تروجان‌ها، کرم‌ها و سایر بدافزارهایی که در این فصل می‌بینید، همگی نوعی ویروس محسوب می‌شوند.

اغلب کاربران حداقل یک بار با یکی از انواع ویروس‌ها دچار آلودگی شده‌اند. ویروس می‌تواند از طریق نصب یک نرم‌افزار آلوده، یک دستگاه آلوده (مانند فلش)، باز کردن پست‌الکترونیکی آلوده، وارد شدن به وب سایتی که آلوده است، به رایانه‌تان منتقل شود.

به طور کلی ویروس‌ها نرم‌افزارهای مخربی هستند که می‌توانند رایانه‌تان را آلوده کرده، منابع آن را به نفع خودشان استفاده کرده، داده‌های رایانه‌تان را سرقت یا خراب کنند. در این فصل با مفاهیم بدافزار[11] (برنامه‌های مخرب[2]) و انواع آن‌ها آشنا می‌شویم.

بدافزار، نرم‌افزاری مخرب است. برخی از بدافزارها که نیت تخریب دارند در زیر آمده‌اند:

۱. ویروس‌ها (Virus)

۲. کرم‌ها (Warms)

۳. تروجان‌ها (Trojans)

۱ – ۵. ویروس

ویروس، قطعه کدی (برنامه نرم‌افزاری) است که خود را در برنامه‌های بزرگ‌تر کپی کرده، آن‌ها را تغییر می‌دهد. برنامه‌هایی که ویروس خودش را در آن‌ها کپی می‌کند، میزبان **نام دارند. بنابراین، ویروس‌ها مستقل نیستند. یعنی، زمانی که برنامه‌های میزبان اجرا می‌شوند، ویروس‌ها نیز اجرا می‌گردند و شروع به تکثیر خود و آلوده نمودن برنامه‌های دیگر می‌نمایند. ویروس دو جزء مهم دارد: ۱.** مکانیزم انتشار، **مکانیزمی است که ویروس را تکثیر می‌کند و برنامه‌ها و رایانه‌های مختلف را آلوده می‌نماید. ۲.** مکانیزم اجرا، **مکانیزمی است که موجب می‌شود ویروس اجرا شده، عمل تخریب خودش را شروع کند. به عنوان مثال، ویروس میکلانژ در تاریخ تولد میکلانژ فعال گردید و عمل تخریبی‌اش را شروع نمود.**

---

[11] **.Malware** [2] **.Malicious Software**

۲ – ۵. کرم

کرم، برنامه‌ای است که به صورت مستقل اجرا می‌گردد (برای اجرا نیاز به میزبان ندارد). برخلاف ویروس‌ها که خودشان را در فایل‌های دیگر کپی می‌کردند، کرم‌ها استقلال خود را حفظ نموده، برنامه‌های دیگر را تغییر نمی‌دهند. کرم‌ها برای بقای خودشان، منابع میزبان از قبیل پهنای باند شبکه، منابع محلی را مصرف می‌کنند و منجربه حملات انکار سرویس می‌شوند. برخی از کرم‌ها، بدون مداخله کاربر اجرا شده، خودشان را تکثیر می‌کنند. در حالی که برخی دیگر از کرم‌ها، نیاز دارند کاربر آن‌ها را مستقیماً اجرا نموده تا بتوانند خودشان را تکثیر کنند. کرم‌ها علاوه بر تکثیر خود می‌توانند خرابکاری را نیز در سیستم انجام دهند.

۳ – ۵. تروجان

یک اسب تروا[۱۲] (تروجان)، قطعه برنامه‌ای است که در ظاهر کار مفید انجام می‌دهد، ولی دارای کد مخفی است که عمل تخریب را انجام می‌دهد.

اسب تروا، خودش را منتشر نمی‌کند، بلکه معمولاً برای کپی کردن خودش، از یک ویروس یا کرم استفاده می‌کند. هدف اصلی یک اسب تروا، تخریب کار کاربر یا عملیات معمولی سیستم است. به عنوان مثال، اسب تروا ممکن است یک درب پشتی[۲] را در سیستم باز کند تا هکر از طریق آن بتواند سرقت اطلاعات را انجام داده یا پیکربندی سیستم را تغییر دهد (تروجان‌هایی که به هکرها اجازه دسترسی از راه دور را می‌دهند، تروجان‌های دسترسی راه دور[۳] **نام دارند).**

۴-۵. نرم افزار Bonus

نرم افزار Bonus، نرم‌افزاری است که علاوه بر نرم‌افزار اصلی شامل بسته‌های دیگر نرم‌افزاری است. وجود بسته‌های دیگر در یک نرم‌افزار تجاری رایج است. به عنوان مثال، فرض کنید یک مرورگر[۴] نصب می‌کنید، این برنامه ممکن است شامل بسته‌هایی نظیر نرم‌افزارهای چند رسانه‌ای یا Adobe Acrobat باشد. بنابراین، گاهی اوقات نیاز است برای نصب یک نرم‌افزار، بسته‌های دیگری را نصب نمایید. درهنگام نصب برنامه اصلی، نصب نرم‌افزارهای جانبی (نرم‌افزارهای اضافی علاوه بر نرم‌افزار اصلی) به اطلاع کاربر می‌رسد. چون عملکرد نرم‌افزارهای Bonus معمولاً متفاوت از نرم‌افزار اصلی است، اگر کاربر چاره‌ای داشته باشد، مسلماً نباید آن‌ها را نصب کند.

---

۱۲. در اسطوره‌های قدیمی، اسب تروا، اسب توخالی ساخته شده از چوب است که توسط سردار سپاه یونان در جنگ امپراتوری تروا ساخته شد. سربازان یونان در این اسب مخفی شدند و از طریق آن وارد شهر شدند. در شب هنگام، از داخل اسب بیرون آمدند و دروازه شهر را برای سربازان یونان باز کردند و به این ترتیب در جنگ پیروز شدند.

2.Back door 3.Remote Access Trojans 4.Browser

۵-۵. انواع عملیات نرم‌افزار مخرب (بد افزار)

محدودیتی در چگونگی فعالیت بدافزارها روی کامپیوترتان وجود ندارد، اما، این برنامه‌ها در برخی از فعالیت‌ها مشترک هستند. این فعالیت‌ها در زیر آمده‌اند:

۱. رونویسی یا حذف داده‌ها

بعضی از بدافزارها، واقعاً مخرب هستند، این گونه بدافزارها با نصب نرم‌افزارها روی کامپیوترتان سریع می‌توانند فایل‌های ذخیره شده در دیسک سخت را پاک یا با اطلاعات غلط رونویسی کنند. به طوری که اطلاعات رونویسی یا حذف شده قابل بازیابی نباشند.

۲. نصب یک برنامه تروا

امروزه، این عملکرد بدافزارها خیلی رایج شده است. اگر روی رایانه‌تان برنامه‌ای نصب شده است که سیستم عامل استفاده زیادی از آن می‌کند، بدافزار می‌تواند به جای این برنامه، برنامه خود را جایگزین کند تا تاثیر مخربش را بگذارد.

علاوه براین، بدافزارها می‌توانند برنامه‌های دیگر را در سیستم‌تان نصب کنند تا در زمان از پیش تعیین شده نظیر زمان روشن شدن رایانه یا تاریخ خاص فعال و اجرا گردند.

۳. نرم‌افزارهای سربار

نرم‌افزارهای سربار[۱۳]، نرم‌افزارهایی هستند که بدافزارها برروی رایانه‌تان نصب می‌کنند و هنگامی که رایانه‌تان روشن می‌شود یا برنامه خاصی را اجرا می‌کنید، اجرا می‌شوند.

۴. ثبت کلیدهای تایپ شده

گاهی بدافزارها، نرم‌افزارهایی برروی رایانه‌تان نصب می‌کنند که تمام کلیدهای تایپ شده را در فایلی ذخیره می‌کنند. این نرم‌افزارها، ثبت‌کننده کلید[۲] **نام دارند. فایلی که کلیدهای ثبت شده در آن ذخیره شده است، می‌تواند از طریق درب پشتی مورد استفاده قرار گیرد یا از طریق پست‌الکترونیکی یا وب به نویسنده نرم‌افزار فرستاده شود. پس اگر در هنگامی که در وب شماره کارت اعتباری یا کلید عبور خود را تایپ می‌کنید و صفحه وب ایمن نباشد (اطلاعات در هنگام انتقال رمزگذاری نشود)، این برنامه هر چه را تایپ می‌کنید، دقیقاً ثبت می‌کند. بنابراین، در هنگام تایپ شماره کارت اعتباری و کلمه عبور در صفحات وب دقت لازم را داشته باشید یا اگر صفحه وب علاوه بر صفحه کلید کامپیوترتان، صفحه کلید مخصوص به**

---

[13].Payload Software [2].Keyloggers

خود را طراحی نموده است که مکان کلیدها به طور تصادفی انتخاب می‌شوند، حتماً از این صفحه کلید استفاده کنید.

فصل ۶ فایروال

فایروال (دیواره آتش)[۱۴] ، موانعی بین شبکه یا رایانه شخصی قابل اعتماد و اینترنت غیر قابل اعتماد است. به عبارت دیگر، فایروال، ابزاری است که کنترل دستیابی به سیستم محلی یا سیستم‌های شبکه را بنابر سیاست امنیتی تعریف می‌کند.

از لحاظ فنی، یک گره شبکه شامل نرم‌افزار و سخت افزاری است که شبکه خصوصی را از شبکه عمومی ایزوله می‌کند. در اینترنت، داده‌ها و درخواست‌های فرستاده شده از یک رایانه به دیگری به قسمت‌هایی به نام بسته[۲] شکسته می‌شوند. هر بسته شامل آدرس اینترنتی رایانه فرستنده داده‌ها، آدرس اینترنتی رایانه گیرنده داده و حاوی اطلاعات دیگری است که بسته‌ها را از یکدیگر متمایز می‌کند. فایروال، همه بسته‌هایی که از آن عبور می‌کنند را بررسی می‌کند و سپس یکی از اعمال اجازه عبور یا اجازه عبورندادن را با توجه به سیاست امنیتی تعریف شده می‌دهد. فایروال‌ها برای محافظت از موارد زیر طراحی شده‌اند:

۱. ورود از راه دور، وقتی فردی از راه دور به رایانه‌تان متصل می‌گردد و کنترل آن را به دست می‌گیرد، می‌تواند اطلاعات رایانه‌تان را خوانده یا تخریب نماید.

۲. درب‌های پشتی برنامه کاربردی، بعضی از برنامه‌ها می‌توانند امکان دسترسی از راه دور را فراهم کنند. در برخی از برنامه‌ها خطاهایی وجود دارد که یک درب پشتی (دسترسی مخفی) را فراهم می‌کنند.

۳. همه بسته‌های ارسال شده از یک آدرس معینی متوقف شوند، گاهی اوقات شرکت‌ها از این روش برای مسدود کردن درخواست‌های رسیده از شرکت‌های رقیب استفاده می‌کنند.

۴. ویروس‌ها، مفهوم ویروس‌ها را قبلاً دیدید. برخی از فایروال‌ها از ورود ویروس‌ها به شبکه جلوگیری می‌کنند.

۵. هرزنامه‌ها، همان طور که بیان گردید، پست‌های الکترونیکی ناخواسته، هرزنامه هستند. هرزنامه‌ها می‌توانند خطرناک باشند، زیرا، حاوی پیوند به سایت‌های خطرناک هستند.

---

[14].Firewall [2].Packet

۶. هر بسته‌ای که از بیرون می‌آید و آدرس رایانه درونی را دارد متوقف نماید، بعضی اوقات نفوذگر رایانه خود را به جای رایانه درون سازمان جا می‌زند. بنابراین، با این روش شرکت‌ها می‌توانند درخواست‌های این چنینی را مسدود کنند.

فایروال ممکن است دستگاهی سخت‌افزاری یا نرم‌افزاری نصب شده برروی رایانه باشد. در هر حالت، فایروال در محل اتصال دو شبکه قرار می‌گیرد. یعنی، فایروال معمولاً بین شبکه محلی و عمومی (اینترنت) قرار می‌گیرد.

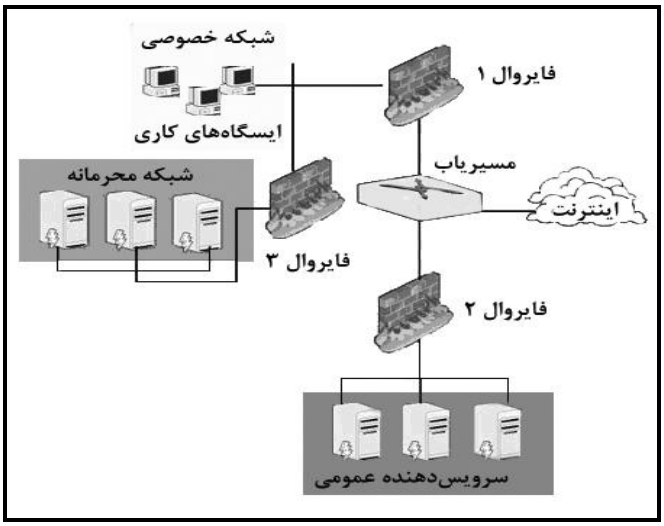
در شکل ۱ – ٦ فایروال و محل قرار گرفتن آن را مشاهده می‌کنید. برای آشنایی بهتر با مفهوم فایروال، چهار ناحیه[۱۵] شکل ۱ – ٦ را در زیر می‌بینید:

۱. شبکه خصوصی[۲] (LAN) ، ناحیه‌ای است که فقط کارکنان و مدیران سازمان در آن قرار دارند. بنابراین، باید حفاظتی ایجاد گردد تا به جز کارکنان و مدیران سازمان افراد دیگر نتوانند از طریق اینترنت وارد این شبکه شوند و به منابع و داده‌های آن دستیابی داشته باشند.

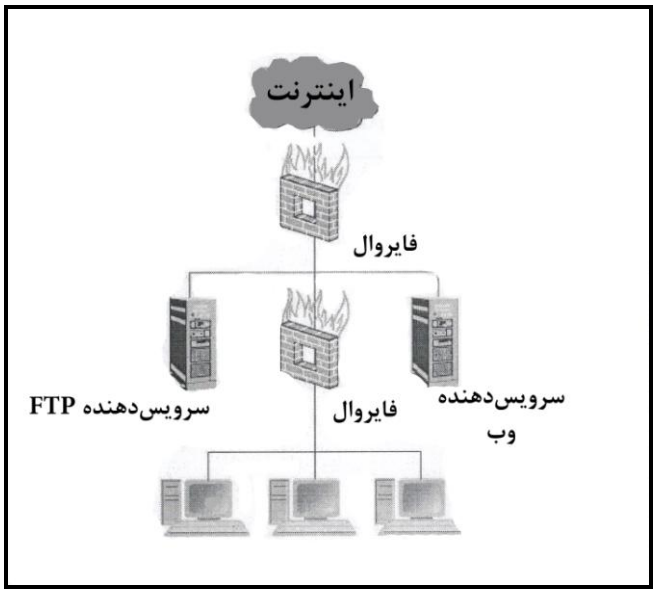
۲. ناحیه بی‌طرف[۳] (DMZ) ، ناحیه‌ای از شبکه است که بین شبکه داخلی سازمان و شبکه خارجی (اینترنت) قرار دارد و این دو شبکه را از لحاظ فیزیکی جدا (ایزوله) می‌سازد. این ایزوله‌سازی با قوانین اعمال شده از طرف فایروال کنترل می‌گردد. به عنوان مثال، فرض کنید، سازمانی می‌خواهد وب سایت خود را اداره نماید. در پیکربندی DMZ، سازمان سرویس‌دهنده وب‌اش را در شبکه‌ای قرار می‌هد تا عموم بتوانند به آن دستیابی داشته باشند و بقیه سرویس‌دهنده‌ها را در شبکه خصوصی قرار می‌دهد. سپس، فایروالی را پیکربندی می‌کند تا درخواست‌های رسیده از بیرون (عموم) را به سرویس‌دهنده مورد نظر هدایت نماید. در اکثر اوقات فایروال دومی، در دروازه ورود شبکه داخلی قرار می‌گیرد تا از ورود درخواست‌های نفوذگران به شبکه داخلی با تضمین بیشتری جلوگیری شود. در شکل ۲ – ٦ نمونه‌ای از ناحیه بی‌طرف (DMZ) را می‌بینید.

---

[15].Zone [2].Private Network [3].Demilitarized Zone



شکل ۱ – ۶ ناحیه‌های مختلف فایروال.



شکل ۲ – ۶ نمونه‌ای از ناحیه بی‌طرف.

فصل ۷ امنیت در تجارت الکترونیک

پرداخت‌های الکترونیکی مانند پرداخت‌های سنتی، مشکلاتی از قبیل احتمال کپی نمودن اسناد مالی دیجیتالی، احتمال ایجاد امضای دیجیتال جعلی یا الحاق اطلاعات هویتی شخص پرداخت‌کننده به تراکنش مالی را دارد. یک تاجر باید موارد بیان شده را در نظر بگیرد. سیستم انتخابی باید بالاترین سطح امنیتی را داشته باشد و در عین حال، نیازهای مشتریان را برآورده نماید. البته، ایجاد این امکانات وظیفه تاجر نیست، بلکه نهادهای سیاست‌گذار و مجری هر کشور باید بسترهای آن را فراهم کنند تا استفاده‌کنندگان در شرایط امن و قابل اعتماد بتوانند یکی از روش‌های پرداخت را انتخاب کنند.

از طرف دیگر، تراکنش‌های الکترونیکی و سایت‌ها ریسک‌های بازرگانی ایجاد می‌نمایند. مجرمان در هر نقطه دنیا خیلی بیشتر از گذشته اطلاعات کارت اعتباری، کلمه عبور حساب بانکی و دیگر اطلاعات شخصی را می‌دزدند. دامنه تهدیدات از حملات ترکیبی فرا مدرن تا ضریب‌های جازدن فروفناوری تغییر می‌کنند. به همین دلیل، یک استراژی امنیت تجارت الکترونیکی (شامل چندین لایه امنیتی) لازم است. این استراتژی امنیت تجارت الکترونیکی را به عنوان فرآیند جلوگیری و تشخیص استفاده غیر مجاز از نام تجاری، هویت، سایت، نام الکترونیکی، اطلاعات یا اموال با ارزش سازمان و تلاش برای کلاهبرداری از سازمان، مشتریان یا کارمندان آن سازمان می‌بینند. از اقدامات جلوگیری، برای جلوگیری از ورود کاربران غیر مجاز (نفوذ گران یا مهاجمان)، به هر بخشی از تجارت الکترونیک استفاده می‌شود. از اقدامات تشخیص جهت تشخیص، این که آیا نفوذ گران تلاش کردند وارد سیستم شوند یا این که موفق بودند، و این که چه کاری ممکن است انجام داده باشند، استفاده می‌شوند.

بخش مهم بهبود تجربه خریدار، اطمینان حاصل کردن از این است که خرید ایمن و بی‌خطر باشد. معمولاً هدف نهایی امنیت تجارت الکترونیک **تضمین اطلاعات**[۱۶] است. تضمین اطلاعات، محافظت سیستم‌های اطلاعاتی از دسترسی غیر مجاز یا تغییر اطلاعات در ذخیره، پردازش، انتقال، محافظت از انکار سرویس به کاربران مجاز، و اقدامات لازم برای تشخیص، مستند کردن و مقابله با تهدیدات می‌باشد.

در این فصل مطالبی درباره استراتژی‌های امنیتی تجارت الکترونیک، اقدامات جلوگیری و تشخیص و نیاز به رویکرد امنیتی دفاع کامل را می‌آموزید. به عنوان مثال، فایروال[۲] (دیوارهای آتش)

---

1. (IA = Information Assurance)
2. Firewall
3. Human Firewalls

محافظ شبکه‌های بازرگانی نمی‌تواند از تمام حملات جلوگیری کند، اگر شرکت فایروال‌های انسانی[۳] نداشته باشد (فایروال‌های انسانی، دسترسی کارمندان به اسناد حیاتی بازرگانی را محدود می‌کنند و سیاست‌های سخت‌گیر امنیتی را اجرا نمایند) نمی‌تواند امنیت را به طور کامل اجرا نماید. شرکت‌ها، علاوه بر چندین لایه دفاعی به چندین لایه بازیابی نیز نیاز دارند.

بنابراین در این فصل به مفاهیم امنیت و روش‌های ایجاد آن در تجارت الکترونیک می‌پردازیم.

۱ – ۷. لایه سوکت‌امن (SSL)

تکنولوژی SSL[۱۷] اساس وب گسترده جهانی[۲] امن را تشکیل می‌دهد. لایه سوکت امن، پروتکلی است که از گواهی‌های استاندارد جهت احراز هویت و رمزنگاری داده استفاده می‌کند تا اطمینان از محرمانگی داده را ایجاد کند. امروزه، یکی از پروتکل‌های اصلی در حال استفاده برای ایمن‌سازی تجارت الکترونیک SSL می‌باشد که به عنوان امنیت لایه انتقال (TLS)[۳] نیز شناخته می‌شود.

SSL، توسط شرکت نت‌اسکیپ تولید گردید تا از گواهی استاندارد جهت احزار هویت و رمزگذاری داده برای اطمینان از محرمانگی داده استفاده گردد. SSL، استاندارد اصلی مورد استفاده پرداخت‌های کارت اعتباری است. یعنی، SSL رمزگذاری شماره‌های کارت اعتباری و دیگر انتقال‌های بین سرویس‌دهنده وب و مرورگر وب را امکان‌پذیر می‌نماید. در مورد تراکنش‌های کارت اعتباری، جهت خرید در وب، باید کارهای دیگری علاوه بر دادن شماره کارت به فروشنده انجام گردد. برخی از این کارها عبارت‌اند از:

۱. اعتبار شماره باید بررسی گردد.

۲. بانک مشتری باید به مشتری اجازه دهد تا فرآیند خرید انجام شود.

SSL، به جز انتقال شماره کارت، هیچ یک از اعمال بیان شده را مدیریت نمی‌کند.

مهمترین اجزای پروتکل SSL، جلسه SSL و اتصال SSL هستند که به صورت زیر تعریف می‌شوند:

☒ **اتصال**، انتقالی است (در مدل لایه‌بندی OSI) که یک سرویس مناسب را فراهم می‌کند. در SSL اتصالات نقطه به نقطه و گذرا هستند هر اتصال تنها به یک جلسه متصل می‌شود.

☒ **جلسه**، جلسه SSL ارتباطی بین یک کلاینت و یک سرور است. جلسات با پروتکل دست دادن[۴] تولید می‌شوند، جلسات پارامترهای امنیت رمزگذاری را تعریف می‌کنند که بین اتصالات به صورت مشترک استفاده می‌شود. جهت ایجاد هر جلسه به پارامترهایی نیاز است که به صورت زیر می‌بینید:

☒ **شناسه جلسه**[۵]، رشته دلخواه یکتایی که توسط سرور برای تعیین جلسه قابل استفاده انتخاب می‌شود.

☒ گواهی گره[۶]، گواهی x509.V3 مربوط به طرف اتصال که می‌تواند تهی باشد.

---

[17].Secure Socket Layer [2]. WWW (World Wide Web) [3]. Transport Layer Secure
[4].Hand Shaking [5].Session Identifier [6].Peer Certificate

☒ **روش فشرده‌سازی**، الگوریتمی که برای فشرده‌سازی قبل از رمزگذاری استفاده می‌شود.

☒ **مشخصات رمز**، شامل الگوریتم رمزگذاری از قبیل AES و الگوریتم درهم‌سازی از قبیل SHA-1 است.

☒ **کلید اصلی**، کلید ٦٤ بیتی که بین دو طرف (کلاینت سرور) مشترک است.

☒ **پرچم ادامه**[18]، پرچمی که نشاندهنده این است که جلسه می‌تواند بین دو اتصال جدید استفاده شود یا خیر.

پارامترهای مورد نیاز در یک اتصال را به صورت زیر می‌بینید:

☒اعداد تصادفی انتخاب شده در دو طرف اتصال.

☒کلید استفاده شده برای محاسبه MAC در سرور

☒کلید مشابه در طرف کارفرما

☒کلید متقارن رمزگذاری داده توسط سرور

☒کلید مشابه‌ی در طرف کارفرما

☒بردار اولیه برای رمز در حالت CBC

شماره سریال، هر طرف یک شماره سریال دارد که حداکثر ۱ – 2^{64} است.

۲–۷. تراکنش الکترونیکی امن

تراکنش الکترونیکی امن (SET)[2] ، یک رمزگذاری از دو مشخصات امن است که برای تامین امنیت تراکنش‌های کارت اعتباری در اینترنت طراحی گردید. نسخه اولیه SET، ناشی از فراخوانی استاندارد امنیتی توسط شرکت‌های ویزا کارت و مستر کارت در فوریه ۱۹۹٦ می‌باشد. شرکت‌های متعددی از قبیل IBM، مایکروسافت، نت‌اسکیپ، RSA و غیره در ایجاد مشخصات اولیه SET نقش داشته‌اند و تست‌های متعددی روی آن انجام دادند تا در سال ۱۹۹۸ اولین محصول سازگار با SET ارائه گردید.

برخلاف اشتباه بعضی‌ها، SET، یک سیستم پرداخت نیست، بلکه یک سری از پروتکل‌های استاندارد و فرمت‌های امنیتی است تا کاربران را قادر سازد، زیرساخت‌های پرداخت کارت اعتباری موجود را روی شبکه‌های نظیر اینترنت استفاده کنند. در اصل SET سه سرویس زیر را فراهم می‌نماید:

☒ **محرمانگی اطلاعات**، چون کانال امنی بین شرکت‌کنندگان در تراکنش فراهم می‌کند، بنابراین، محرمانگی برقرار می‌شود. یعنی، اطلاعات پرداخت و حساب صاحب کارت، در هنگام انتقال در شبکه دارای امنیت است. زیرا، مانع از این می‌گردد که بازرگانان، شماره کارت اعتباری صاحب کارت

---

[18].Is presumable [2].Secure Electronic Transaction

را ببینند. این اطلاعات فقط در اختیار صادرکننده کارت می‌باشد. SET، برای تامین محرمانگی از رمزگذاری DES استفاده می‌نماید.

☒ **تمامیت داده‌ها (جامعیت)**، اطلاعات پرداخت از قبیل اطلاعات سفارش، داده‌های شخصی، و دستورالعمل‌های پرداخت از صاحبان کارت به فروشندگان فرستاده می‌شود. SET، از طریق امضای دیجیتال RSA و با کدهای درهم سازی SHA-1 تمامیت پیام را در هنگام انتقال تامین می‌کند. یعنی، تضمین می‌کند اطلاعات در هنگام انتقال تغییر نمی‌یابند.

☒ **احزار هویت**، سرویس احراز هویت SET دو نوع احزار هویت را انجام می‌دهد که عبارت‌اند از:

۱. **احراز هویت بازرگان (فروشنده)**، صاحب کارت را قادر می‌سازد تا اثبات نماید که فروشنده یا موسسه مالی‌ای که اجازه می‌دهد کارت‌های اعتباری پرداخت را بپذیرد.

۲. **احزار هویت صاحب کارت**، فروشنده را قادر می‌سازد تا بررسی نماید آیا صاحب کارت، کاربر قانونی شماره حساب کارت اعتباری است یا خیر.

SET، برای تامین هر دو نوع احزار هویت از گواهی نامه‌های دیجیتال X.509V3 با امضای دیجیتال RSA بهره می‌گیرد.

تجارت الکترونیک امن (SET) رمزگذاری باز بوده و امنیتی را برای دو طرف ارتباط تعیین می‌کند که برای محافظت از تراکنش‌های کارت اعتباری در اینترنت طراحی شده است. SETV1 از یک تماس برای استاندارد امنیتی توسط کارت اعتباری و ویزا در فوریه سال ۱۹۹۶ پدید آمده است. حوزه وسیعی از شرکت‌ها از قبیل IBM، مایکروسافت، نت‌اسکیپ، RSN با این تکنولوژی سروکار دارند.

در آغاز سال ۱۹۹۶ آزمایشات متعددی انجام شد تا در سال ۱۹۹۸ اولین موج محصولات ترکیبی SET بوجود آمدند.

فصل ۸ سرویس‌ها و برنامه‌های کاربردی امنیت اطلاعات

امنیت شبکه و اطلاعات توسط سرویس‌ها و برنامه‌های کاربردی تامین می‌شود. هر یک از بخش‌های شبکه برای تامین امنیت از سرویس‌ها و برنامه‌های کاربردی مخصوص به خود استفاده می‌کنند. بنابراین، در این فصل، برخی از سرویس‌ها و برنامه‌های کاربردی امنیت شبکه را می‌آموزیم. این سرویس‌ها و برنامه‌های کاربردی عبارت‌اند از:

۱. سرویس‌های امنیت پست‌الکترونیک
۲. امنیت معماری IP
۳. سرویس‌های کنترل دسترسی داده
٤. سیستم زیست‌سنجی
٥. احراز هویت
٦. مدیریت شبکه آسان (SNMP)

۱-۸. سرویس‌های امنیت پست‌الکترونیک

امروزه سازمان‌ها برای ارسال داده‌ها و نامه‌ها از پست‌الکترونیک استفاده می‌کنند تا در زمان و هزینه صرفه‌جویی نمایند. بنابراین، باید امنیت داده‌های ارسالی و محرمانه ماندن محتویات آن‌ها مورد توجه ویژه‌ای قرار گیرد. اکثر کاربران سرویس احرازهویت را جهت محرمانه ماندن پیام‌هایشان به کار می‌برند. دو ابزار مهم برای ایمن نگه داشتن پست‌الکترونیک وجود دارد:

۱. سرویس PGP[۱۹] ۲. سرویس S/MIME[۲]

[19].Pretty Good Privacy [2]. Secure/ Multipurpose Internet Mile Extension

۱-۱ – ۸. سرویس PGP

سرویس PGP، توسط آقای فیل زیمرمان ارائه گردید. این سرویس قابلیت اعتماد و سـرویس احراز هویت که در برنامه‌های پست‌الکترونیک و ذخیره فایل استفاده می‌شود را فـراهم مـی‌کنـد. اهداف سرویس PGP عبارت‌اند از:

- **برای ایجاد بلوک‌ها از بهترین الگوریتم‌های رمزگذاری استفاده شود.**
- **الگوریتم‌های مورد استفاده در قالب یک برنامه کاربردی مجتمع شـوند و بـا مجموعـه‌ای دستورات ساده بتوان از آن‌ها استفاده کرد.**
- **در قالب یک بسته نرم‌افزاری به همراه مستندات که کد برنامه را نیز شـامل مـی‌شـود بـه سادگی از طریق اینترنت، تابلوی اعلانات و شبکه تجـاری از قبیـل AOL[۲۰] قابـل دسترسـی باشد.**
- **با هر نسخه‌ای سازگاری داشته و کم هزینه باشد.**

سرویس PGP، خیلی سریع گسترش یافت و مورد استفاده قرار گرفته است. زیرا، این سرویس به طور رایگان قابل دسترس بوده و روی سیستم عامل‌های مختلفـی از قبیـل ویننـدوز، یـونیکس، مکینتاش و بسیاری دیگر قابل اجرا است.

جدول ۱ – ۸ نمادهای سرویس PGP.

نماد	توضیح
K_s	کلید جلسه استفاده شده در الگوریتم‌های متقارن.
PR_a	کلید خصوصی کاربر A.
PU_a	کلید عمومی کاربر A.
EP	رمزگذاری کلید عمومی (نامتقارن).
DP	رمزگشایی کلید عمومی (نامتقارن).
EC	رمزگذاری متقارن.
DC	رمزگشایی متقارن.
H	تابع درهم‌ساز.
||	الحاق (بهم چسباندن[۲]).
Z	فشرده‌سازی با استفاده از الگوریتم ZIP.
R64	تبدیل قالب radix64 به ASCI.

[20] America on Line

[2] Concatenation

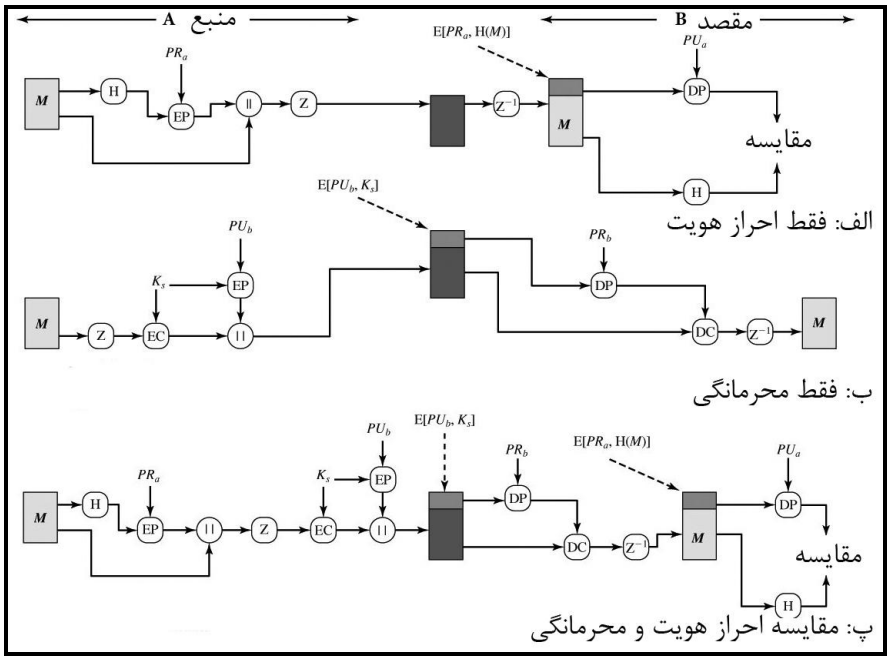
در این سرویس، از الگوریتم‌های رمزگذاری کلید عمومی متقارن قوی و معروفی از قبیل DES، RSA، IDEA، CAST-128 و SHA-1 استفاده شده است و در حوزه وسیعی از برنامه‌ها قابل استفاده است، به خصوص سازمان‌هایی که از یک استاندارد برای رمزگذاری فایل‌ها و پیام-های محرمانه به افراد استفاده می‌کنند. این سرویس، توسط دولت بخصوصی طراحی و کنترل نمی‌شود. جهت توصیف عملکرد سرویس PGP ابتدا باید نمادهای آن را بشناسیم. این نمادها در جدول ۱ – ۸ آمده‌اند.

PGP، سرویس‌های متعددی ارائه می‌کند که آن‌ها را در جدول ۲ – ۸ می‌بینید.

جدول ۲ – ۸ سرویس‌های اصلی **PGP**

تابع	الگوریتم	توضیح
امضای دیجیتال (**Digital Signature**)	**DSS/ SHA** یا **RSA/SHA**	کد درهم‌ساز خلاصه پیام با استفاده از الگوریتم **SHA-1** ایجاد می‌شود. خلاصه پیام با استفاده از **DSS** یا **RSA** با کلید خصوصی فرستنده رمزگشایی شده و خلاصه پیام به همراه پیام ارسال می‌شود.
رمزگذاری پیام (Message Encryption)	**CAST** یا **IDEA** یا **DES** سه گانه یا **RSA**	پیام توسط **CAST-128**، **IDEA** یا **3DES** با کلید جلسه تولید شده توسط فرستنده رمزگذاری می‌شود. کلید جلسه با استفاده از **RSA** با کلید عمومی گیرنده به همراه پیام رمزگذاری می‌شود.
فشرده‌سازی (**Compression**)	**ZIP**	ممکن است پیام جهت ذخیره‌سازی یا انتقال با الگوریتم **ZIP** فشرده-سازی شود.
سازگاری با پست-الکترونیک (**Email Compatibility**)	تبدیل **Radix64**	جهت فراهم کردن شفافیت در برنامه‌های پست الکترونیکی، پیام رمزگذاری شده باید توسط تبدیل **Radix64** به رشته اسکی تبدیل شود.
تقسیم و ترکیب (**Segmentation**)		جهت غلبه بر محدودیت‌های حداکثر اندازه پیام، **PGP** پیام را تکه‌تکه کرده و سپس، در مقصد مجتمع می‌کند.

در شکل ۱– ۸ فرآیند ایجاد احرازهویت و محرمانگی را در سرویس PGP می‌بینید.



شکل ۱ – ۸ ایجاد احراز هویت و محرمانگی در سرویس PGP .

روند ایجاد این سرویس به صورت زیر است:

۱. فرستنده پیام را تولید می‌کند.

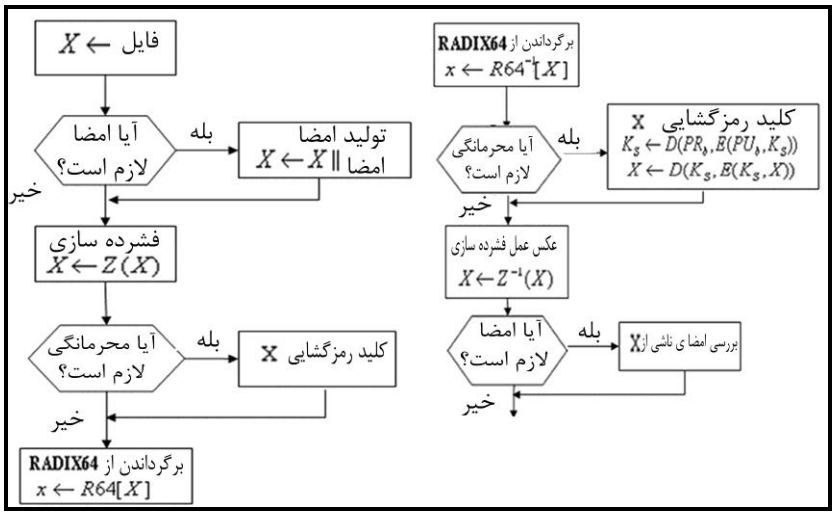
۲. تابع SHA-1 برای ایجاد خلاصه پیام 160 بیتی استفاده می‌شود.

۳. کد درهم توسط RSA و با استفاده از کلید خصوصی فرستنده رمزگذاری شده و نتیجه به پیام اضافه می‌شود.

٤. گیرنده با استفاده از RSA و کلید عمومی فرستنده خلاصه پیام را رمزگشایی و بازیابی می‌کند.

۵. گیرنده، خلاصه پیام جدیدی از پیام ایجاد کرده و آن را با خلاصه پیام رمزگشایی شده مقایسه می‌کند. اگر باهم برابر بودند، پیام به عنوان پیام معتبر پذیرفته می‌شود.

به هنگام ارسال و دریافت پیام در سرویس PGP چهار سرویس PGP که قبلاً دیدید با هم ارتباط برقرار می‌کنند. این ارتباط را در شکل ۲ – ۸ می‌بینید.



شکل ۲ – ۸ فرآیند ارتباط چهار سرویس اصلی PGP با یکدیگر.

هنگام انتقال اگر لازم باشد، امضا با استفاده از خلاصه پیام متن غیرفشرده تولید می‌شود. آن-گاه، پیام به همراه امضا فشرده می‌شود. سپس، اگر قابلیت اعتماد نیاز باشد، بلوک (متن فشرده شده یا امضای فشرده شده به همراه پیام) رمزگذاری شده و با کلید رمزگذاری متقارن رمزگذاری شده کلید عمومی به پیام اضافه می‌شود. در پایان، کل بلوک به قالب Radix 64 تبدیل می‌شود.

هنگام دریافت پیام، بلوک دریافتی ابتدا از فرمت Radix64 به فرمت باینری تبدیل می‌شود. آن‌گاه، بلوک حاصل از حالت فشرده خارج می‌شود. اگر پیام امضا شده بود. گیرنده، خلاصه پیام انتقالی را بازیابی کرده و آن را با خلاصه پیام محاسبه شده خود مقایسه می‌کند. در صورت تطابق، پیام تصدیق می‌شود.

۲–۱ – ۸. سرویس توسعه پست الکترونیکی چند منظوره (S/MIME)

سرویس S/MIME، برای افزایش امنیت به استاندارد قالب پست‌الکترونیکی طراحی گردید که براساس تکنولوژی امنیت داده RSA عمل می‌کند. گرچه، هم PGP و هم S/MIME براساس استاندارد IETF هستند، اما S/MIME، به عنوان استاندارد صنعتی برای استفاده تجاری و سازمانی به کار می‌رود، درحالی که PGP، برای امنیت پست‌الکترونیکی شخصی کاربران استفاده می‌شود. S/MIME از دو استاندارد RFC822 و MIME استفاده می‌کند. شرح این دو استاندارد را در زیر می‌بینید:

استاندارد RFC822

RFC822، قالبی برای پیام‌های متنی که از طریق پست‌الکترونیک ارسال می‌شوند، تعریف می‌کند. در این استاندارد، قالب پیام و محتوی آن به صورت بسته است. یک بسته شامل اطلاعات مورد نیاز برای ارسال و دریافت است. محتویات شامل اطلاعاتی است که باید به گیرنده تحویل داده شود.

RFC822، فقط برای امنیت محتویات به کار می‌رود. پس، استاندارد محتویات شامل مجموعه‌ای از فیلدهای سرآیند است که توسط سیستم پست جهت ایجاد بسته استفاده می‌شوند و این استاندارد جهت آسان نمودن فهم پیام توسط برنامه‌ها استفاده می‌شود. سرآیند شامل تعدادی کلمات کلیدی است که با کاراکتر ";" از هم جدا می‌شوند. کلیدهای اصلی از سرآیند شامل From، TO، Subject و Date می‌باشند.

مثال: پیام زیر با استفاده از استاندارد RFC822 ایجاد می‌شود:

Date :Tue, 16/04/2010 Time : 14 : 20 : 17 pm
From : "fanavarie novin" <fanavarie novin@yahoo.com>
Subject : RFC822
TO : "Ramazan Abbasnezhad" < abbasnezhad@yahoo.com>
Hello. This is a Sample of RFC822 Standard That is Sent For you.

استاندارد MIME

این استاندارد برای رفع محدودیت‌های RFC822 تحت پروتکل انتقالSMTP[۲۱] طراحی گردید. برخی از محدودیت‌های SMTP/822 را در زیر می‌بینید:

۱. SMTP قادر به عبور فایل‌های اجرایی یا اطلاعات دودویی نمی‌باشد. برای رفع این مشکل باید از راهکارهای Unencode / Undecode استفاده نمود.

۲. SMTP، داده‌های متنی که شامل کاراکترهای زبان ملی هستند را عبور نمی‌دهد. چون، این کاراکترها به صورت کدهای ۸ بیتی با ارزش ۱۲۸ دسیمال یا بالاتر نشان داده می‌شوند. ولی، SMTP تا ۷ بیت اسکی محدود شده است.

۳. سرورهای SMTP ممکن است پیام‌های بزرگتر از یک طول معین را قبول نکنند.

۴. SMTP پیاده‌سازی یکسانی را براساس استاندارد RFC821 از قبیل حذف، اضافه، شکستن، حذف فاصله و Tab را بین خطوط و کاراکترها انجام نمی‌دهد.

---

[21] **.Simple Mile Transfer Protocol**

استاندارد MIME برای رفع این مشکلات طراحی شد. این استاندارد از مولفه‌های زیر تشکیل شده است:

- **پنج فیلد جدید در سرآیند پیام تعریف می‌شوند. این فیلدها، اطلاعاتی در مورد بدنه پیام ایجاد می‌کنند.**
- **تعدادی قالب‌بندی محتوی تعریف می‌شوند که از طریق آن‌ها پست‌الکترونیک چند رسانه‌ای استاندارد می‌شود (ارسال صدا، فیلم، تصویر).**
- **کدگذاری‌های محتوی تعریف می‌شوند تا تبدیل هر قالب‌بندی محتوی، به شکلی که از حذف توسط سیستم پست محافظت شوند، ممکن شود.**

پنج فیلد سرآیند در MIME به صورت زیر تعریف می‌شوند:

- **نسخه MIME[۲۲]، مقدار آن حتماً باید 0 و 1 باشد. این فیلد نشان دهنده این است که پیام با RFC2045 و RFC2046 مطابقت دارد.**
- **نوع محتوی[۲]، محتوی داده‌های جزئی در مورد نوع محتوی پست الکترونیک است، به‌طوری که قابل شناسایی باشد.**
- **کدگذاری روی محتوی[۳]، نوع کدگذاری که بدنه پیام را نشان می‌دهد، به طوری که پیام قابل انتقال باشد.**
- **شناسه محتوی[۴]، جهت شناسایی عناصر MIME به صورت یکتا در مواقعی که چند قطعه هم زمان در یک پیام درج شده باشند، تعریف می‌شود.**
- **توصیف محتوی[۵]، نوع محتوی پیام را توصیف می‌کند. این فیلد وقتی که پیام قابل خواندن نیست (مانند پیام صوتی)، قابل استفاده است.**

جدول ۳ – ۸ محتوی استفاده شده در MIME را نشان می‌دهد.

یک مثال از محتوی چند قسمتی (Multipart) را در زیر می‌بینید:

```
From : Nathaniel Boreenstein  <nsb@bellcore.com>
To : Ned Freed <ned@innosoft.com>
Subject : Sample Message
 MIME – Version 10
Content –type : multipart / mixed ; boundary =" Simple boundary"
This is The preamble. It is to be ignored, Though it is a handy place for mail
Composers      to include an explanatory note to non-MIME Conformant readers.
Simple boundary
This is implicitly typed plain ASCII text.
It does NOT end with a linebreak.
Simple boundary
```

---

[22].MIME-version [2].Content-type [3].Content-Transfer-Encoding
[4].Content-ID [5].Content-Description

Content-type : text / plain: Charest = us-ascii
This is explicitly typed plain ASCII text.
It Does end with linebreak.
Simple boundary
This is the epilogue. It is also to be ignored.

جدول ۳ – ۸ محتوی استفاده شده در MIME.

نوع	زیرنوع	توصیف
Text	**Plain**	**متن قالب‌بندی نشده، که ممکن است اسکی یا ISO8859 باشد.**
	Enriched	**انعطاف‌پذیری بیشتری برای قالب‌بندی فراهم می‌شود.**
Multipart	**Mixed**	**قسمت‌های متفاوت مستقل هستند، اما با هم عبورداده می‌شوند. این قسمت‌ها باید با همان ترتیب اولیه به گیرنده تحویل داده شوند.**
	Parallel	**تنها تفاوت آن با mixed این است که ترتیبی در دریافت بخش‌های پیام رعایت نمی‌شود.**
	Alternative	**قسمت‌های مختلف نسخه‌های دیگر از همان اطلاعات هستند و طوری مرتب شده‌اند که مثل همان حالت اولیه بوده و باید به بهترین نسخه به گیرنده نشان داده شوند.**
	Digest	**همانند mixed است. اما، نوع / زیر نوع پیش فرض هر بخش از پیام RFC822 است.**
Message	**RFC822**	**بدنه آن به صورت پیامی است که در بسته‌ای قرار داده شده است که با RFC822 مطابقت دارد.**
	Partial	**جهت صدور اجازه قطعه شدن پست‌های بزرگ به صورتی‌که برای گیرنده شفاف باشد.**
	External body	**از اشاره‌گری به یک شیء که در محل دیگری قرار دارد، تشکیل شده است.**
Image	**jpeg**	**تصویر با قالب‌بندی JPEG و کدگذاری JFIF است.**
	gif	**تصویری با قالب‌بندی GIF است.**
Video	**Mpeg**	**قالب MPEG است.**
Audio	**Basic**	**کانال ۸ بیتی ISDN که با قانون M با نرخ نمونه‌برداری 8KHZ رمزگذاری شده است.**
Application	**Postscript**	**Adobe PostScript**
	Octet-Stream	**داده‌های دودویی عمومی شامل بایت‌های ۸ بیتی است.**

پیوست پرسش‌های چهار گزینه‌ای

۱. فرآیندی که به بازدیدکنندگان وب سایت اطمینان می‌دهد که سایت متقلب نیست، چه نامیده می‌شود؟

الف: اثبات ب: تایید ج: تایید اعتبار و صحت اسناد د: امنیت

۲. فرآیندی که از طریق آن موسسه‌ای مطمئن می‌شود، موسسه دیگر همان کسی است که ادعا می‌کند، چه نامیده می‌شود.

الف: اثبات ب: رسیدگی ج: احراز هویت و صحت اسناد د: مجوز دادن

۳. فرآیندی که تعیین می‌کند آیا کاربر حق اجرا یا خواندن داده خاصی را دارد، چه نامیده می‌شود؟

الف: اثبات ب: رسیدگی ج: احراز هویت و صحت اسناد د: مجوز دادن

۴. فرآیند گردآوری اطلاعات درباره دستیابی به منابع خاص، استفاده از مزایای به خصوص، یا اجرای دیگر فعالیت‌های امنیتی، چه نامیده می‌شود؟

الف: اثبات ب: رسیدگی ج: احراز اعتبار و صحت اسناد د: امنیت

۵. ایده‌ای که اطلاعات محرمانه و حساس نباید برای افراد، نهادها، یا فرآیندهای نرم‌افزار کامپیوتر فاش شوند، چه نامیده می‌شوند؟

الف: قابلیت اعتماد ب: رسیدگی ج: احراز اعتبار و صحت‌اسناد د: امنیت

۶. توانایی محافظت داده از تغییر یا خرابی با دسترسی غیر مجاز یا تصادفی، چه نامیده می‌شود؟

الف: قابلیت اعتماد ب: رسیدگی ج: احراز اعتبار و صحت اسناد د: جامعیت

۷. حمله‌ای که توسط یک هکر جریانی از بسته‌های داده‌ای را به کامپیوتر هدف جهت اضافه کردن بار منابعش ارسال می‌کند، چه نامیده می‌شود؟

الف: ویروس ب: مهندسی اجتماعی

ج: برنامه مخرب اسب تروا د: حمله انکار سرویس

۸. مهاجمی ویروسی را نوشته که خودش را به صدها حساب کاربری پست‌الکترونیکی براساس دفترچه آدرس کامپیوتر آلوده شده می‌فرستد. در هنگام ظهر براساس زمان تعیین شده، هر کامپیوتر آلوده توسط ویروس در خواست جستجویی را به یاهو می‌فرستد، در این صورت بار یاهو اضافه شده، سرورها خاموش می‌گردند، این حمله چه نوعی است؟

الف: حمله غیر فنی ب: حمله اجتماعی

ج: برنامه مخرب اسب تروا د: حمله انکار سرویس توزیع شده

۹. نوجوانی برنامه‌ای را به عکس خاص پیوست می‌کند و به هزاران آدرس پست‌الکترونیک ارسال می‌کند. این برنامه سبب می‌گردد، هر کامپیوتری که عکس در آن باز شده باشد، هر شب ساعت ۷ برنامه مخرب خاصی را اجرا کند. این مثالی از یک ..... است؟

الف: ویروس ب: مهندسی اجتماعی ج: حمله غیرفنی د: حمله انکار سرویس

۱۰. علی نرم‌افزار رایگانی را جهت ویرایش تصویر دانلود می‌نماید. این نرم‌افزار به خوبی کار می‌کند. اما، علاوه برکارش، مسیر هر وب سایتی که علی مراجعه کرده است را ذخیره کرده، در هر هفته یک بار به سرویس دهنده مرکزی خاصی ارسال می‌کند. این عمل چه نامیده می‌شود؟

الف: ویروس ب: کرم ج: برنامه اسب تروا د: مهندسی اجتماعی

۱۱. تفاوت اصلی بین کرم و ویروس چیست؟

الف: ویروس از نرم‌افزار خاصی برای ارسال بسته‌های داده به کامپیوترهای هدف استفاده می‌کند. درصورتی که یک کرم دستیابی غیر قانونی به کامپیوترها را دارد و از این کامپیوترهای میزبان برای ارسال داده استفاده می‌کند.

ب: ویروس خطایی در یک نرم‌افزار است که می‌تواند مستقیماً توسط یک هکر برای دستیابی به کامپیوتر استفاده شود. در حالی که کرم خطایی در یک نرم‌افزار است که دستیابی به اطلاعات و قابلیت‌هایی که می‌توانند به عنوان یک جای پا برای ورود غیر قانونی به کامپیوتر دیگر استفاده شود.

ج: ویروس به صورت محلی انتشار می‌یابد. در حالی که کرم بین سیستم‌ها انتشار می‌یابد.

د: ویروس معمولاً زمانی که برنامه کاربردی شامل ویروس اجرا یا باز گردد، فعال می‌شود. در حالی که کرم برنامه‌ای است که به ظاهر سودمند است، اما شامل عوامل مخفی می‌باشد که ریسک امنیتی را ارائه می‌نماید.

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

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

۱۳. فرآیند شناسایی طرفین مجاز و مشروع در یک تراکنش یا معامله خرید و فروش چه نامیده می‌شود؟

الف: ارزیابی ب: اثبات ج: احراز هویت و صحت اسناد د: نظارت

۱۴. در رمزنگاری، پیام اصلی که توسط انسان قابل خواندن می‌باشد، چه نامیده می‌شود؟

الف: کلید ب: متن رمز شده ج: پیام عادی یا دستکاری نشده د: الگوریتم رمزگذاری

منابع

۱. **عباس‌نژادورزی، رمضان، عباس‌نژادورزی، یوسف، "** تجارت الکترونیکی**" (چاپ اول)، فناوری نوین، ۱۳۸۹.**

۲. **علاءالدین، حمیده، "**امنیت در یادگیری الکترونیکی**" (چاپ اول)، دانشگاه علوم کشاورزی و منابع طبیعی گرگان، ۱۳۸۸.**

۳. **بختیاری، شهرام، قاضی مغربی، سعید، "**اصول امنیت سیستم‌ها و شبکه‌های رایانه‌ای**"، موسسه انتشارات علمی، (چاپ اول)، ۱۳۸۵.**

۴. **صفایی کوچکسرایی، فاطمه، اکبری، احمد، "**تبعات هرزتماس‌هاو ضرورت استفاده از مکانیزم‌های ضد هرزتماس در سیستم‌های صوتی اینترنت**"، اولین کنفرانس دانشجویی فناوری اطلاعات ایران دانشگاه کردستان، ۱۳۸۹.**

5. **William Stallings,**"Cryptography and Network Security Principles and Practices"**, Fourth Edition, Prentice Hall, 2005.**

6. **Vense Hassler,** "Security Fundamentals For E-Commerce "**,Atrech House".**

7. **Efraim Turban, Divid king, judy mckay / peter marshall, jae lee, Dennis Viehland,**"Electronic commerce a Managerial Perspective 2008, Prentice Hall"**.**

8. **William Stallings ,**"Cryptography and network Security principles and practices"**, Fifth Edition, prantice Hall, 2008.**

9. **Chris McNab**" Network Security Assessment"**, O'Reilly, 2004.**

10. **Fred Piper and Sean Murphy .**"Cryptography: A Very Short Introduction"**, Oxford University Press.2002.**

11. **JoAnn Ward,**"Caesar Ciphers: An Introduction to Cryptography"**, Purdue University GK-12, 2006-07.**

12. **Matt Bishop,** "Computer Security: Art and Science"**, Addison Wesley, 2002.**

13. **WWW. Purde.edu/df/gk12/downloads/Cryptography.pdf**

14. **WWW.Math.Cudenver.edu**

15. **WWW.CS.berkeley.edu**

16. **WWW.CS.Trinconn.edu**