رمزنگاری اطلاعات

گسترش و رشد بی سابقه اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد ، سازمانها و موسسات شده است . امنیت اطلاعات یکی از مسائل مشترک شخصیت های حقوقی و حقیقی است . کاربران اینترنت در زمان استفاده از شبکه، اطلاعات حساس و مهمی را بدفعات ارسال و یا دریافت می دارند. اطمینان از عدم دستیابی افراد غیر مجاز به اطلاعات حساس از مهمترین چالش های امنیتی در رابطه با توزیع اطلاعات در اینترنت است . اطلاعات حساس که ما تمایلی به مشاهده آنان توسط دیگران نداریم ، موارد متعددی را شامل می شود. برخی از اینگونه اطلاعات بشرح زیر می باشند :

اطلاعات کارت اعتباری

شماره های عضویت در انحمن ها

اطلاعات خصوصی

جزئیات اطلاعات شخصی

اطلاعات حساس در یک سازمان

اطلاعات مربوط به حساب های بانکی

تاکنون برای امنیت اطلاعات بر روی کامپیوتر و یا اینترنت از روش های متعددی استفاده شده است . ساده ترین روش حفاظت از اطلاعات نگهداری اطلاعات حساس بر روی محیط های ذخیره سازی قابل انتقال نظیر فلاپی دیسک ها است . متداولترین روش حفاظت اطلاعات ، رمز نمودن آنها است . دستیابی به اطلاعات رمز شده برای افراد غیر مجاز امکان پذیر نبوده و صرفا" افرادیکه دارای کلید رمز می باشند ، قادر به باز نمودن رمز و استفاده از اطلاعات می باشند .

رمز نمودن اطلاعات کامپیوتر مبتنی بر علوم رمز نگاری است .استفاده از علم رمز نگاری دارای یک سابقه طولانی و تاریخی است . قبل از عصر اطلاعات ، بیشترین کاربران رمزنگاری اطلاعات ، دولت ها و مخصوصا" در موارد نظامی بوده است . سابقه رمز نمودن اطلاعات به دوران امپراطوری روم بر می گردد. امروزه اغلب روش ها و مدل های رمزنگاری اطلاعات در رابطه با کامپیوتر بخدمت گرفته می شود. کشف و تشخیص اطلاعاتی که بصورت معمولی در کامپیوتر ذخیره و فاقد هر گونه روش علمی رمزنگاری باشند ، براحتی و بدون نیاز به تخصصی خاص انجام خواهد یافت .

اکثر سیستم های رمزنگاری اطلاعات در کامپیوتر به دو گروه عمده زیر تقسیم می گردند:

- رمزنگاری کلید – متقارن
- رمزنگاری کلید – عمومی

رمز نگاری کلید – متقارن

در روش فوق ، هر کامپیوتر دارای یک کلید رمز (کد) بوده که از آن برای رمزنگاری یک بسته اطلاعاتی قبل از ارسال اطلاعات بر روی شبکه و یا کامپیوتر دیگر ، استفاده می نماید .دراین روش لازم است در ابتدا مشخص گردد که کدامیک از کامپیوترها قصد مبادله اطلاعاتی با یکدیگر را دارند ، پس از مشخص شدن هر یک از کامپیوترها، در ادامه کلید رمز بر روی هر یک از سیستم ها می بایست نصب گردد. اطلاعات ارسالی توسط کامپیوترهای فرستنده با استفاده از کلید رمز ، رمز نگاری شده وسپس اطلاعات رمز شده ارسال خواهند شد. پس از دریافت اطلاعات رمز شده توسط کامپیوترهای گیرنده ، با استفاده از کلید رمز اقدام به بازگشائی رمز و برگرداندن اطلاعات بصورت اولیه و قابل استفاده خواهد شد . مثلا" فرض کنید پیامی را برای یکی از دوستان خود رمز و سپس ارسال می نمائید . شما برای رمز نگاری اطلاعات از روشی استفاده نموده اید که بر اساس آن هر یک از حروف موجود در متن پیام را به دو حرف بعد از خود تبدیل کرده اید. مثلا" حروف A موجود در متن پیام به حروف C و حروف B به حروف D تبدیل می گردند. پس از ارسال پیام رمز شده برای دوست خود ، می بایست با استفاده از یک روش ایمن و مطمئن کلید رمز را نیز برای وی مشخص کرد. در صورتیکه گیرنده پیام دارای کلید رمز مناسب نباشد ، قادر به رمز گشائی و استفاده از اطلاعات نخواهد بود. در چنین حالتی می بایست به دوست خود متذکر گردید که کلید رمز ، " شیفت دادن هر حرف بسمت جلو و به اندازه دو واحد است . " گیرنده پیام با انجام عملیات معکوس قادر به شکستن رمز و استفاده از اطلاعات خواهد بود .

رمزنگاری کلید – عمومی

در روش فوق از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می شود. کلید خصوصی صرفا" متعلق به کامپیوتر فرستنده بوده و کلید عمومی توسط کامپیوتر فرستنده در اختیار هر یک از کامپیوترهائی که قصد برقراری ارتباط با یکدیگر را دارند ، گذاشته می شود. برای رمزگشائی یک پیام رمز شده ، کامپیوتر می بایست از کلید عمومی که توسط فرستنده ارائه شده، بهمراه کلید خصوص ی خود استفاده نماید. یکی از متداولترین برنامه های رمزنگاری در این رابطه (PGP)Pretty Good Privacy است . با استفاده از PGP می توان هر چیز دلخواه را رمز نمود .

بمنظور پیاده سازی رمزنگاری کلید – عمومی در مقیاس بالا نظیر یک سرویس دهنده وب ، لازم است از رویکردهای دیگری در این خصوص استفاده گردد. " امضای دیجیتال " یکی از رویکردهای موجود در این زمینه است یک امضای دیجیتالی صرفا" شامل اطلاعات محدودی بوده که اعلام می نماید ، سرویس دهنده وب با استفاده و بکارگیری یک سرویس مستقل با نام " امضای مجاز " ، امین اطلاعات است . "امضای مجاز "

بعنوان یک میانجی بین دو کامپیوتر ایفای وظیف می نماید. هویت و مجاز بودن هر یک از کامپیوترها برای برقراری ارتباط توسط سرویس دهنده انجام و برای هر یک کلید عمومی مربوطه را فراهم خواهد کرد .

یکی از متداولترین نمونه های پیاده سازی شده از رمزنگاری کلید -عمومی ، روش SSL)Secure Sokets Layer)است . روش فوق در ابتدا توسط "نت اسکیپ " پیاده سازی گردید SSL .یک پروتکل امنیتی اینترنت بوده که توسط مرورگرها و سرویس دهندگان وب بمنظور ارسال اطلاعات حساس ، استفاده می گردد . SSLاخیرا" بعنوان بخشی از پروتکل (TLS)Transport Layer Security در نظر گرفته شده است.

در مرورگر می توان زمان استفاده از یک پروتکل ایمن نظیز TLS را با استفاده از روش های متعدد اعلام کرد. استفاده از پروتکل "https" درعوض پروتکل "http" یکی از روش های موجود است . در چنین مواردی در بخش وضعیت پنجره مرورگر یک "Padlock" نشان داده خواهد شد .

رمزنگاری کلید – عمومی ، مدت زمان زیادی را صرف انجام محاسبات می نماید. بنابراین در اکثر سیستمها از ترکیب کلید عمومی و متقارن استفاده می گردد .زمانیکه دو کامپیوتر یک ارتباط ایمن را بایکدیگر برقرار می نمایند ، یکی از کامپیوترها یک کلید متقارن را ایجاد و آن را برای کامپیوتر دیگر با استفاده از رمزنگاری کلید – عمومی ، ارسال خواهد کرد. در ادامه دو کامپیوتر قادر به برقرار ارتباط بکمک رمزنگاری کلید متقارن می باشند. پس از اتمام ارتباط ، هر یک از کامپیوترها کلید متقارن استفاده شده را دور انداخته و در صورت نیاز به برقراری یک ارتباط مجدد ، می بایست مجددا" فرآیند فوق تکرار گردد (ایجاد یک کلید متقارن ، (....

مقدار Hash

رمزنگاری مبتنی بر کلید عمومی بر پایه یک مقدار hash ، استوار است . مقدار فوق ، بر اساس یک مقدار ورودی که دراختیار الگوریتم hashing گذاشته می گردد ، ایجاد می گردد. در حقیقت مقدار hash ، فرم خلاصه شده ای از مقدار اولیه ای خود است . بدون آگاهی از الگوریتم استفاده شده تشخیص عدد ورودی اولیه بعید بنظر می رسد . مثال زیر نمونه ای در این زمینه را نشان می دهد:

عدد ورودی الگوریتم Hash مقدار

10,667 Input # x 143 1,525,381

تسخیص اینکه عدد ۱,۵۲۵,۳۸۱ (مقدار (hash از ضرب دو عدد 10.667 و ۱۴۳ بدست آمده است ، کار بسیار مشکلی است . در صورتیکه بدانیم که یکی از اعداد ۱۴۳ است ، تشخیص عدد دوم کار بسیار ساده ای خواهد بود. (عدد ۱۰,۶۶۷) .رمز نگاری مبتنی بر کلید عمومی بمراتب پیچیده تر از مثال فوق می باشند. مثال

فوق صرفا "ایده اولیه در این خصوص را نشان می دهد .

کلیدهای عمومی عموما" از الگوریتم های پیچیده و مقادیر Hash بسیار بزرگ برای رمزنگاری استفاده می نمایند. در چنین مواردی اغلب از اعداد ۴۰ و یا حتی ۱۲۸ بیتی استفاده می شود. یک عدد ۱۲۸ بیتی دارای 2 128حالت متفاوت است.

آیا شما معتبر هستید ؟

همانگونه که در ابتدای بخش فوق اشاره گردید ، رمزنگاری فرآیندی است که بر اساس آن اطلاعات ارسالی از یک کامپیوتر برای کامپیوتر دیگر ، در ابتدا رمز و سپس ارسال خواهند شد. کامپیوتر دوم (گیرنده) ، پس از دریافت اطلاعات می بایست ،اقدام به رمزگشائی آنان نماید .یکی دیگر از فرآیندهای موجود بمنظور تشخیص ارسال اطلاعات توسط یک منبع ایمن و مطمئن ، استفاده از روش معروف " اعتبار سنجی " است . در صورتیکه اطلاعات "معتبر " باشند ، شما نسبت به هویت ایجاد کننده اطلاعات آگاهی داشته و این اطمینان را بدست خواهید آورد که اطلاعات از زمان ایجاد تا زمان دریافت توسط شما تغییر پیدا نکرده اند. با ترکیب فرآیندهای رمزنگاری و اعتبار سنجی می توان یک محیط ایمن را ایجاد کرد .

بمنظور بررسی اعتبار یک شخص و یا اطلاعات موجود بر روی یک کامپیوتر از روش های متعددی استفاده می شود :

- رمز عبور . استفاده از نام و رمز عبور برای کاربران ، متداولترین روش "اعتبار سنجی " است . کاربران نام و رمز عبور خود را در زمان مورد نظر وارد و در ادامه اطلاعات وارد شده فوق ، بررسی می گردند. در صورتیکه نام و یا رمز عبور نادرست باشند ، امکان دستیابی به منابع تعریف شده بر روی سیستم به کاربر داده نخواهد شد .

- کارت های عبور . این نوع کارت ها دارای مدل های متفاوتی می باشند. کارت های دارای لایه مغناطیسی (مشابه کارت های اعتباری) و کارت های هوشمند (دارای یک تراشه کامپیوتر است) نمونه هائی از کارت های عبور می باشند .

- امضای دیجیتالی . امضای دیجیتالی، روشی بمنظور اطمینان از معتبر بودن یک سند الکترونیکی (نظیر: نامه الکترونیکی ، فایل های متنی و ...) است . استاندارد امضای دیجیتالی (**DSS**) ، بر اساس نوع خاصی از رمزنگاری کلید عمومی و استفاده از الگوریتم امضای دیجیتالی (DSA) ایجاد می گردد.الگوریتم فوق شامل یک کلید عمومی (شناخته شده توسط صاحب اولیه سند الکترونیکی – امضاء کننده) و یک کلید عمومی است . کلید عمومی دارای چهار بخش است . در صورتیکه هر چیزی پس از درج امضای دیجیتالی به یک سند الکترونیکی ، تغییر یابد ، مقادیر مورد نظری که بر اساس آنها امضای دیجیتالی با آن مقایسه خواهد شد ، نیز تغییر خواهند کرد .

سیستم های متعددی برای "اعتبار سنجی " تاکنون طراحی و عرضه شده است . اکثر سیستم های فوق از زیست سنجی برای تعیین اعتبار استفاده می نمایند. در علم زیست سنجی از اطلاعات زیست شناسی برای تشخیص هویت افراد استفاده می گردد. برخی از روش های اعتبار سنجی مبتنی بر زیست شناسی کاربران ، بشرح زیر می باشند :

پیمایش اثر انگشت) انگشت نگاری(

پیمایش شبکیه چشم

پیمایش صورت

مشخصه صدا

یکی دیگر از مسائل مرتبط با انتقال اطلاعات ، صحت ارسال اطلاعات از زمان ارسال و یا رمزنگاری است . می بایست این اطمینان بوجود آید که اطلاعات دریافت شده ، همان اطلاعات ارسالی اولیه بوده و در زمان انتقال با مشکل و خرابی مواجه نشده اند .در این راستا از روش های متعددی استفاده می گردد :

. Checksum ●یکی از قدیمی ترین روش های استفاده شده برای اطمینان از صحت ارسال اطلاعات است . Checksum، به دو صورت متفاوت محاسبه می گردد . فرض کنید Checksum یک بسته اطلاعاتی دارای طولی به اندازه یک بایت باشد ، یک بایت شامل هشت بیت و هر بیت یکی از دو حالت ممکن) صفر و یا یک) را می تواند داشته باشد. در چنین حالتی ۲۵۶ وضعیت متفاوت می تواند وجود داشته باشد. با توجه به اینکه در اولین وضعیت ، تمام هشت بیت مقدار صفر را دارا خواهند بود ، می تواند حداکثر ۲۵۵ حالت متفاوت را ارائه نمود .

▪در صورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی ، ۲۵۵ و یا کمتر باشد ، مقدار Checksum شامل اطلاعات واقعی و مورد نظر خواهد بود .

▪در صورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی ، بیش از ۲۵۵ باشد ، Checksumمعادل باقیمانده مجموع اعداد بوده مشروط بر اینکه آن را بر ۲۵۶ تقسیم نمائیم .

مثال زیر ، عملکرد CheckSum را نشان می دهد .

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Total	Checksum
212	232	54	135	244	15	179	80	1,151	127

1,151 / 256 = 4.496 (round to 4)
4 x 256 = 1,024
1,151 - 1,024 = 127

. Cyclic Redundancy Check)CRC) ●روش CRC در مفهوم مشابه روش Checksum است .

روش فوق از تقسیم چمد جمله ای برای مشخص کردن مقدار CRC استفاده می کند. طول CRC معمولا" ۱۶ و

یا ۳۲ بیت است . صحت عملکرد روش فوق بسیار بالا است . در صورتیکه صرفا" یک بیت نادرست باشد ، CRCبا مقدار مورد نظر مطابقت نخواهد کرد .

روش های Checksum و CRC امکانات مناسبی برای پیشگیری از بروز خطای تصادفی درارسال اطلاعات می باشند، روش های فوق در رابطه با حفاظت اطلاعات و ایمن سازی اطلاعات در مقابل عملیات غیر مجاز بمنظور دستیابی و استفاده از اطلاعات ، امکانات محدودتری را ارائه می نمایند. رمزنگاری متقارن و کلید عمومی ، امکانات بمراتب مناسب تری در این زمینه می باشند .

بمنظور ارسال و دریافت اطلاعات بر روی اینترنت و سایر شبکه های اختصاصی ، از روش های متعدد ایمنی استفاده می گردد .ارسال اطلاعات از طریق شبکه نسبت به سایر امکانات موجود نظیر : تلفن ، پست ایمن تر می باشد . برای تحقق امرفوق می بایست از روش های متعدد رمزنگاری و پروتکل های ایمنی بمنظور ارسال و دریافت اطلاعات در شبکه های کامپیوتری خصوصا" اینترنت استفاده کرد.