حسابداری، مدیریت مالی و اقتصاد
سه قلوهای سازگار

رضا قریشی
مدرس دانشگاه جامع علمی کاربردی- مرکز بازرگانی تهران

مقدمه

جامعه امروز به‌دنبال سرمایه و سرمایه گذار است. کشورهای توسعه یافته موفق شدند پس اندازهای کوچک و درآمدهای بدون مصرف آنی جامعه را از طریق ابزارهای متنوع برای سرمایه گذاری مولد به بازارهای متنوع و از جمله بازار سـرمایه سوق دهند. طبیعی اسـت که مردم شغل با آبرو و رفاه نسبی را برای حفظ هویت خویش طلب کنند. بنابراین علوم حسابداری، مدیریت مالی و اقتصاد باید کمک کنند تا مطلوبیت نسبی زندگی مردم جامعه خویش را در یک سطح قابل قبول طراحی و اجرا کنند.

حسـابداری مدیریت و حسابداری مالی بسیار به هم نزدیکند. به طوری که برخی تصور می کنند دانش حسابداری و مدیریت مالی هر دو یکی است. حسابداری وظیفه ثبت و طبقه بندی وقایع مالی به صورت یک سلسله اطلاعات را به عهده دارد و نتیجه کار آن تهیه گزارش های مالی است.

مدیریت مالی با تجزیه و تحلیل این اطلاعات در تصمیم‌گیری، برنامه‌ریزی و کنترل عملیات ازدیدگاه مالی مرتبط است. درواقع مدیریت مالی هم با اقتصاد محیط خود یعنی بازار پولی و مالی و هم با مفهوم اصلی اقتصاد یعنی کاربرد منابع کمیاب (پول) به منظوردسـتیابی به هدف های نامحدود سـروکاردارد. بنابراین، حسـابداری، مدیریت مالی و اقتصاد را می توان سه قلوهای سازگار نامید. هدف از این مقاله بیان نقش حسـابداری به عنوان گزارشگری مالی و نقش مدیریت مالی در بازار سرمایه برای ایجاد یک اقتصاد سالم و رونق خرید و فروش اوراق بهاداربه منظور تامین اعتبارات و ایجاد ابزارهای مناسب برای رشد و شکوفایی جامعه با برنامه ریزی های اقتصادی است.

انجمن حسابداران رسمی امریکا به خوبی از سودمندی و ارتباط گزارش‌های مالی (تجاری) آگاه است. از این رو در سال ۱۹۹۱ به منظور تحقیق در مورد گزارشـگری مالی، کمیته ویژه‌ای را برای افزایش ارزش اطلاعات واحدهای تجـاری و جلب اطمینان و اعتماد مردم به گزارش های مالی تشـکیل داد. اقدامات این کمیته برای جلب نظر مردم به شرح زیر بود:

افزایش سـودمندی در گزارش های مالی، جلوگیری از سـوء استفاده و شناسـایی تقلب، تقویت نظام حرفه حسابرسی و ایجاد اطمینان از استقلال و بیطرفی حسابرسان مستقل.

اهمیت گزارشگری مالی

کمیابی منابع (دارایی ها)، موجب می شـود که مردم آنها را ذخیره کنند تا به شـیوه ای موثر از آن استفاده کنند یا به افراد قابل اعتماد بسپارند تا آنها از دارایی‌هایشان به نحوه مطلوب و اثر بخش استفاده کنند. بازارهای تجارت آزاد و رقابت از جمله عواملی هستند که می‌توانند با به کاربردن موثر این منابع، موجب افزایش سطح رفاه مردم شوند. بنابراین مسئولیت حرفه حسابداری در این زمینه زیاد است. زیرا که باید عملکرد را به طور دقیق، منصفانه و به موقع

اندازه‌گیری کنند، به گونه ای که مدیران شرکت های موفق به کمک مدیران مالی خود بتوانند سـرمایه‌ها ی مردم را از طریق ارائه صورت‌های مالی برای مردم و دادن فرصت به آنها، برای مقایسـه بازده و ریسک نسبی فرصت های سرمایه گذاری شرکت ها، منابع خودرا به شکل موثرتری به کارگیرند.

ضـرورت ارائـه اطلاعات قابـل اتکا و مربـوط در تخصیص سرمایه

در یک اقتصاد سالم، تخصیص سرمایه، موجب افزایش بهره‌وری، ایجاد نوآوری و در نتیجه رونق بازاری موثر و کارا در جهت خرید وفروش اوراق بهادار و تحصیل واعطای اعتبار می‌شود. ارائه اطلاعات غیر قابل اتکا و نامربوط موجب نارسـایی در تخصیص سرمایه می‌شود و بازار اوراق بهادار را ناکارآمد می کند. بدون اطلاعات قابل اتکا و مربوط، اسـتفاده کنندگان از گزارش‌های تجاری، فرصت‌ها و خطرهای سـرمایه گذاری را به طور مناسب تشخیص نمی‌دهند. زیـرا برای تصمیم گیری آگاهانه، نیاز به اطلاعـات گوناگونی از جمله آمار و ارقامی مربوط به اقتصاد، صنایع، شـرکت‌ها و سهام است. با اتکا به اطلاعات کامـل وبی عیب و نقصی که از طرف بهترین منابع تهیه می شـود، احتمال گرفتـن بهترین تصمیم افزایش می‌یابد. اغلـب مدیریت بهترین منبع برای تهیه اطلاعات گزارشگری مالی(۴) محسوب می‌شود. اطلاعاتی که شرکت در جهت یاری کردن استفاده کنندگان به منظور تخصیص سرمایه ارائه می‌کند، شامل عناصر مختلفی اسـت که صورت های مالی یکی از این عناصر ها است.

چالش های فراروی حسـابداری مالی

شـاید بتوان بازار سـرمایه در کشورهای توسـعه یافته را در مقایسه با کشورهای دیگر کامل‌تر، روان‌تر و کاراتر به شمار آورد. دلیل این موفقیت ارائه صورت های مالی شـفاف حاوی اطلاعات قابل اتکا و مربوط اسـت. سودمندی اطلاعـات به مربوط بودن و بـه هنگام بودن آن است. بنابراین لازم است واحدهای تجاری همگام با افزایش رقابت و پیشرفت‌های سریع در فن‌آوری‌های مربوط به تجارت، رقابت خود را در ایجاد تغییرات در سیستم اطلاعاتی خود و نوع اطلاعات با معیار غیرمالی مورد نیاز همراه کنند. درشرایطی که فن آوری تجاری به سرعت شکل می گیرد، خطر عقب ماندن گزارشگری تجاری از تغییرات، بسیار محسوس است.

نیازهـای حسـابداری مالـی بـه گزارشگری مالی آینده‌نگر

به اطلاعات مالی که مربوط به آینده است، اطلاعات مالی آینده نگر گفته می‌شود. بنابراین صورت‌های مالی آینده‌نگر شامل پیش‌بینی‌ها و برنامه‌ریزی‌های مهمی از اطلاعات آینده‌نگر مالی است. صورت‌های مالی آینده نگر به‌وسیله پیش‌بینی بالقوه تجاری، نگاهی به آینده دارد. این صورت ها، می توانند پاسـخگوی مناسبی برای سوال‌های اعتباردهندگان، سـرمایه گذاران و مدیریت در ارتباط با آینده باشـند. هدف از تهیه صورت های مالی آینده نگر و صورت های مالی تاریخی تقریباً یکسـان است، ولی مراحل تهیه آن به طور کامل متفاوت است. پیش بینی مالی چیزی را بیـان می کند که مدیریت انتظار آن را درآینده دارد. صورت‌های مالی آینده نگـر کاربردها و منابع زیادی دارد. این صورت ها به شـرکت کمک می‌کنند، هدف‌های کوتاه مدت و بلند مدت خود را تنظیم کنند. در زمانی که شـرکت خواستار دریافت تسهیلات اسـت، پاسخگوی اعتباردهندگان و یا پاسخگوی سـوالاتی نظیر تحقق توسـعه شـرکت یا نرخ بازده داخلی پیش‌بینی شـده وموفقیت شرکت در آینده باشند.

در سـال ۱۹۹۴، کمیته ویژه گزارشگری مالی انجمن حسابداران رسمی آمریکا پیشـنهاد کرد که در آینده باید صـورت های مالی دارای اطلاعات زیر باشد :

نیاز به استانداردهای گزارشگری

باتوجه به این که استفاده‌کنندگان از گزارش‌های مالی، نیازهای مشترک و متضاد دارند، تدوین استانداردهای حسابداری ضروری به نظر می‌رسد. درواقع

نمودار گزارشگری مالی در آینده

باید صورت های مالی با هدف عمومی ارائه شود تا هم نیازهای عمومی استفاده کنند گان را فراهم کند و هم مدیریت مسئولیت گزارشگری خود را به شیوه ای منصفانه، شفاف و کامل انجام دهد. حرفه حسابداری به منظور پرهیز از تفسیرهای نادرست و گوناگون در تهیه صورت های مالی، مجموعه‌ای شناخته شده از استانداردها و رویه ها را پذیرفته است. با این حال نیاز به مطالعه در زمینه گزارشگری تجاری موثر و با کیفیت برای گزارشگری با کیفیت امری ضروری به نظر می‌رسد.

معیارها و اهداف سرمایه گذاری

به طور کلی سرمایه گذاری ها به وسیله سه معیار اصلی ارزیابی می‌شوند:

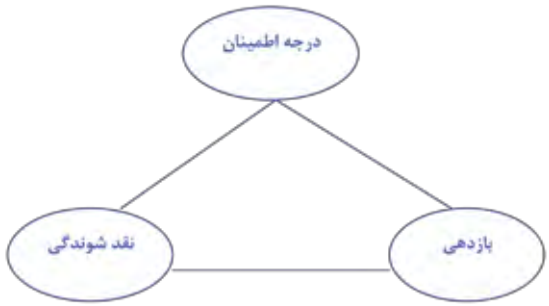
- درجه اطمینان
- نقد شوندگی
- بازدهی

سرمایه گذاران بسیار تمایل دارند که در نتیجه سرمایه گذاری خود، سود بیشتر، نرخ بالاتر و ارزش سرمایه به همراه امنیت زیاد کسب کنند. امنیت به معنی این که دسترسی آنی و سریع به مبلغ سرمایه گذاری خود داشته باشند.

درجه اطمینان – منظور از اطمینان حفظ ارزش دارایی سرمایه گذاری شده و درجه اطمینان به مفهوم میزان ریسک های مرتبط با سرمایه گذاری است. ریسک سرمایه گذاری بستگی زیادی به ثبات سیاسی، ریسک واحد پولی کشور سرمایه پذیر در سرمایه گذاری های خارجی دارد. درجه اطمینان از طریق تنوع بخشی و متوازن سازی سرمایه گذاری در انواع مختلف اوراق بهادار یا سرمایه‌گذاری در سایر محیط های اقتصادی افزایش می‌یابد.

نقد شوندگی – هرچه سرعت تبدیل سرمایه گذاری (دارایی) به وجه نقد یا اعتبار نزد بانک ها، افزایش یابد، میزان نقد شوندگی مطلوب‌تر است.

مثلث اسرارآمیز اوراق بهادار



باید صورت های مالی با هدف عمومی ارائه شود تا هم نیازهای عمومی استفاده کنند گان را فراهم کند و هم مدیریت مسئولیت گزارشگری خود را به شیوه ای منصفانه، شفاف و کامل انجام دهد

بازدهی – میزان بازدهی حاصل از سرمایه گذاری با توجه به جمع درآمدهای کسب شده ناشی از آن مشخص می شود. درآمدهای حاصل از سرمایه گذاری ممکن است به صورت منظم به سرمایه گذار پرداخت شود، یا به صورت توزیع نشده (ذخیره سود).

تضاد بین معیارهای مثلث اسرارآمیز

معیارهای اساسی یادشده را می‌توان به عنوان معیارهای مورد انتظار سرمایه گذار نام برد. این معیارها، تضادهایی به شرح زیر نیز دارند.

- تضاد بین بازده و درجه اطمینان (انواع ریسک ها) یعنی توقع داشتن بازده بیشتر با داشتن انتظار ریسک بیشتر همراه است.
- تضاد بین بازدهی و اهداف نقد شوندگی، یعنی سرمایه گذارانی که انتظارات آنها از نقد شوندگی سرمایه‌گذاری‌هایشان بیشتراست، باید توقع کمتری نسبت به بازدهی سرمایه گذاری خود داشته باشند. درواقع، انتظارات سرمایه گذاران دربازار پول و سرمایه، متفاوت است. در معاملات اوراق بهادار درهر مقطع اززمان ممکن است عوامل زیادی وجود داشته باشد. درک صحیح از عوامل و مولفه های اثر گذار بر سرمایه گذاری در بازارهای سرمایه با توجه به انگیزه ها و اهداف فردی سرمایه گذاران در انواع سرمایه گذاری‌ها، برای علوم حسابداری، مدیریت و اقتصاد به منظور برنامه ریزی بهتردر جهت افزایش ارتقای نسبی سطح زندگی مردم بیشتر از هرزمان دیگری احساس می شود.

نتیجه

برای سرمایه‌گذاری، نیاز به اطلاعات حسابداری است و بدون سرمایه‌گذاری نباید انتظار رونق اقتصادی و جذب نیروی جوان جامعه به اشتغال را داشت. درصورتی که نگاهی علمی به قوانین و مقررات و سیاست های حاکم بر بازار های جذب سرمایه داشته باشیم، لزوم یک بازنگری و طرحی نو با توجه به شناخت درست از روند گذشته، حال و آینده احساس می شود. این وظیفه، مسئولیت اندیشمندان، دانشگاهیان و هر فرد مسئولی را پیش از بیش، افزایش می دهد که با توجه به کثرت جمعیت، با تدوین قوانین مترقی و استانداردهای لازم، زمینه ارائه اطلاعات مالی سودمند و مربوط را برای گسترش بازارهای جذب سرمایه فراهم کنند. در این میان، نقش حسابداران، مدیران مالی، و اقتصاددانان به عنوان سه معمار اصلی در بهبود بازار جذب سرمایه بیشتر از دیگران خواهد بود.

منابع

Bank Verlay ,2002 , Basic Information on Investments in Securities , Bank Verlag Koeln, Germany
-Donald E. Kieso. Jerry J. Weygandt Inte
mediate Accounting
Improving Business Reporting American Institute of Certified (Public Accountants (AICPA

امضای الکترونیک و مراجع صدور گواهینامه الکترونیک

حسین ملکشاهی

مقدمه

در قرنی که در آن به سر می‌بریم، اطلاعات نقش مهمی در روابط اجتماعی، اقتصادی، تجارت و ... دارد. از این‌رو راه اندازی سیستم‌هایی ازقبیل دولت الکترونیک، تجارت الکترونیک، بانکداری الکترونیک و ... نه یک اختیار، بلکه الزام است. اما مسئله‌ای که بیش از همه خود را در فضاهای الکترونیک نمایان می‌سازد، بحث امنیت است. امنیت در فضای سایبر درواقع محافظت از اطلاعات در برابر طیف وسیعی از حمله‌ها است، به طوری‌که استمرار فعالیت را تضمین می‌کند و ریسک‌های به‌وجود آمده را به حداقل می‌رساند. امنیت اطلاعات شامل اصول پایه‌ای مانند محرمانگی(Confidentiality)، تمامیت (integrity) و دسترسی پذیری(availability) اطلاعات و همچنین اصول فرعی مانند احراز اصالت(authentication)، مسئولیت پذیری (accountability)، قابلیت اطمینان(reliability) و البته انکار نکردن (non-repudiation) است. انکار نکردن یعنی اینکه هیچ یک از طرفین ارتباط، قادر به تکذیب کل یا بخشی از ارتباط نباشند. به بیان دقیق‌تر، فرستنده یا گیرنده به ترتیب ارسال و دریافت پیام را منکر نشود. بهترین روشی که برای برقراری این اصل در فضاهای سایبر معرفی می‌شود، استفاده از امضای دیجیتال یا الکترونیک است. در دنیای واقعی نیز این اصل در نظر گرفته شده و رعایت می‌شود. هنگامی که مشتری یک بانک، چک صادره را امضا می‌کند، در واقع اصل عدم‌انکار را برقرار می‌سازد و در صورتی که مشتری ادعا کند که چک از طرف او صادر نشده، بانک می‌تواند در محاکم قضایی به امضای مشتری استناد کند. البته هنگامی که متصدی بانک با چک مواجه می‌شود، صحت امضای روی چک می‌تواند عاملی برای کنترل اصالت آن نیز باشد. یعنی امضا علاوه بر ایجاد اصل عدم‌انکار، اصلی دیگری را نیز برقرار می‌سازد که همان اصل احرازاصالت است. امضای الکترونیک نیز به طور دقیق همین حالت را دارد. اما آیا منظور از امضای الکترونیک، اسکن امضای دستی و الحاق آن به اسناد الکترونیک است؟ باید توجه داشت که منظور از امضای الکترونیک اضافه کردن اسکن یا نام یا نوشته ای خاص نیست. قبل از بررسی امضا تفاوت‌های بین اسناد فیزیکی و الکترونیکی را مرور می کنیم. تفاوت اول این است که توانایی تشخیص ایجاد تغییرات روی نسخه فیزیکی وجود دارد، اما در مورد اطلاعات الکترونیکی این امکان وجود ندارد .دوم اینکه تفاوت بین نسخه اصلی و نسخه کپی در اطلاعات فیزیکی قابل تشخیص است، اما در اطلاعات الکترونیک چنین نیست. بنابراین ساخت امضای الکترونیک راهکارهای مربوط به خود را طلب می کند. درواقع برای ساخت امضای الکترونیک از علم و الگوهای رمزنگاری استفاده می شود که در ادامه مراحل ساخت آن را مرور می کنیم.

علم رمزنگاری

رمزنگاری علمی است که در آن روش‌های پنهان نوشتن و تجزیه و تحلیل این روش‌ها مورد بررسی قرار می‌گیرد. هدف اصلی رمزنگاری این است که فرستنده و گیرنده بتوانند از طریق یک کانال ناامن ارتباط برقرار کنند، به طوری‌که دشمن(opponent) متوجه نشود که آنها چه می‌گویند. علم رمزنگاری، مطالعه روش‌هایی است که به‌وسیله آنها بتوان پیام‌ها را به صورت مخفی یعنی رمزشده انتقال داد، به طوری‌که فقط گیرنده مورد نظر بتواند پیام را رمزگشایی کند و آن‌را بخواند. این روش‌ها در دوره‌های مختلف، شکل‌های متفاوتی داشته‌اند. مثلاً گفته می‌شود که سزار روم برای این‌که یک متن را به صورت مخفی بنویسد، هر حرف را به سه حرف جلوتر از آن در ترتیب الفبایی تبدیل می‌کرد. به‌طور کلی رمزهای تولید شده به دو دسته رمز متقارن و رمز نامتقارن تقسیم می‌شوند.

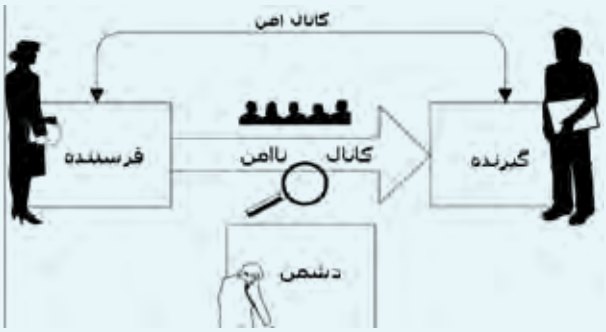
رمز متقارن

در این نوع رمزنگاری هنگامی که فرستنده بخواهد یک پیام رمز شده را به گیرنده بفرستد، از یک کلید رمزگذاری مثل e استفاده می‌کند. (منظور از کلید، یک عدد یا چندتایی مرتب و یا موارد مشابه است و طبق قانون دوم «آگوست کرکهف» کلید تنها چیزی است که در سیستم رمزنگاری به‌صورت سری نگهداری می‌شود). هنگامی که پیام رمزشده به دست گیرنده رسید، با استفاده از کلید رمزگشایی d، متن ساده مجدداً به‌دست می‌آید. در یک سیستم رمز اگر همواره کلید رمزگذاری e برابر کلید رمزگشایی d بوده یا d به سادگی از روی e قابل محاسبه باشد، آنگاه آن‌را رمز متقارن می‌نامند. رمز تغییرجا(Shift Cipher) نمونه‌ای از رمز متقارن است. در این رمز هر حرف به چند حرف جلوتر تبدیل می‌شود و تعداد جابه‌جایی همان کلید، سیستم است. اگر فرستنده و گیرنده از سیستم رمز متقارن استفاده کنند باید قبل از تبادل اطلاعات، کلید مخفی e را مبادله کنند. مبادله کلید یک مسئله اساسی است. در حالت عادی برای مبادله کلید از یک کانال امن استفاده می‌شود. به عنوان مثال هنگامی که یک شخص بخواهد با یک سازمان دولتی از طریق اینترنت و با استفاده از رمزمتقارن تبادل اطلاعات داشته باشد، ابتدا باید با رجوع به آن سازمان، کلید مورد نیاز را مبادله کند. در شکل ۱، منظره‌ای از نحوه ارتباط در رمز متقارن ارائه شده است.

رمز نامتقارن

همانطوری که گفته شد، در رمزمتقارن نیاز به یک کانال امن است و ایجاد این کانال در بسیاری از مسائل کاربردی غیرمنطقی و ناممکن است. برای مثال اگر دو شرکت در کشورهای مختلف بخواهند با استفاده از رمزمتقارن به‌صورت الکترونیک معامله کنند، مجبور می‌شوند کانالی امن پیدا کنند که کاری پرهزینه و در بسیاری از موارد غیرممکن است. برای رفع این مشکل رمز نامتقارن پیشنهاد می‌شود. اندیشه ایجاد رمز نامتقارن که یک انقلاب در علم رمزنگاری است، اولین بار در سال ۱۹۷۶ توسط «دیفی» و«هلمن» مطرح شد. در یک سیستم رمز نامتقارن کلیدهای e و d متمایز بوده و محاسبه d از روی e امکان‌پذیر نیست. در این سیستم که رمز کلیدعمومی نیز نامیده می شود، کلید رمزگذار e را می توان به‌صورت عمومی و همگانی اعلام کرد. فرستنده با استفاده از کلید e متن ساده را رمزگذاری کرده و گیرنده نیز با استفاده از کلید d آن‌را رمزگشایی می کند. در این سیستم e(کلید رمزگذار) را کلید عمومی و d(کلید رمزگشا) را کلید خصوصی می‌نامند. برای تولید کلیدهای عمومی و خصوصی و روش‌های رمزگذاری و رمزگشایی از ریاضیات و مسائل حل نشده‌ای مثل تجزیه به عوامل اول، لگاریتم گسسته، منحنی‌های بیضوی و...استفاده می‌شود. اولین رمز کلید عمومی به نام

شکل ۱- رمزنگاری متقارن با استفاده از یک کانال امن



«RSA» توسط «ریوست» و «شامیر» و «آدلمان» در سال ۱۹۷۸ معرفی شد و به شرح زیر است.

بـه طور خلاصه در الگوریتم RSA هر کاربر، اعداد اول p و q را انتخاب کرده و عدد $n=pq$ را محاسـبه می‌کند. سـپس عدد e را به گونه‌ای انتخاب می‌کند که $gcd(e,n)=1$ (یعنی بزرگترین مقسوم علیه مشترک e و n برابر یک باشد). حال عدد d را از رابطه $ed=1(\mod n)$ محاسبه می‌کند. بعد از انجام این محاسبات، اعداد (e,n) به عنوان کلید عمومی کاربر معرفی شده و عدد d به عنوان کلید خصوصی به‌صورت سـری نگهداری می‌شود. هنگامی که فرستنده بخواهد پیام xرا برای این کاربر ارسال کند، حاصل عبارت $y=x^e(\mod n)$ را محاسبه و ارسال می‌کند. y همان رمز شده پیام xدر سیستم RSA است. برای رمزگشایی نیز کاربر عبارت $y^d(\mod n)$ را محاسـبه می کند که همان پیام xاست. تنها کسـی که می تواند xرا از روی y به‌دسـت آورد، همین کاربر است. زیرا فقط او اسـت که کلید خصوصی (یعنی عدد d) را دارد. امنیت این روش توسط قضایای ریاضی اثبات می شود. سیستم RSA یکی از ده‌ها رمز نامتقارنی است که ابداع شده است. از این روش‌ها تقریباً در تمامی سیستم‌های امنیتی استفاده می‌شود. در ادامه بر اساس رمز نامتقارن، امضای الکترونیک معرفی می‌شود.

امضای الکترونیک

اندیشـه طراحی امضای الکترونیک براساس رمزنگاری نامتقارن پی‌ریزی شده است. در اینجا نیز کلید خصوصی و عمومی درگیر هستند. به این نحو که کاربر با استفاده از کلید خصوصی خود متن مورد نظر را امضا و طرف مقابل نیز با استفاده از کلید عمومی کاربر از صحت امضای او اطمینان حاصل می‌کند. در طرح امضای RSA اگر کاربر بخواهد پیـام x را امضا کند، حاصل عبارت $y=x^d(\mod n)$ را محاسـبه کرده و x,y را برای طرف مقابل می‌فرسـتد. او نیز درسـتی رابطه $x=y^e(\mod n)$ را بررسی می‌کند. اگر رابطه برقرار باشد، y را به عنوان امضا شده پیام x می‌پذیرد. در غیر این‌صورت، امضا مورد قبول واقع نمی‌شود. از طرفی تنها کسـی که می‌تواند y را تولید کند، همان کسی است که عدد d (یعنی کلید خصوصی کاربر) را دارد. از این رو این شخص نمی‌تواند امضای خود را انکار کند و در مراجع قضایی قابل پیگیری است. باید توجه داشت که تمامی محاسبات توسط رایانه و به وسیله نرم‌افزارهای مخصوص انجام می‌شود که یا به‌طور مستقل عمل می‌کنند یا بخشی از سیستم‌عامل یا برنامه‌های کاربردی دیگر هستند. با توجه به مطالب ارائه شده حال می‌توانیم تفاوت‌های زیررا بین امضاهای دستی و امضاهای الکترونیک برشماریم:

۱- امضای دستی یک شخص برای تمامی اسناد و مدارک یکسان است، اما امضای الکترونیک برای هرسند (یا پیام) فقط مخصوص آن سند است.

۲- امضای دستی به‌راحتی و با حرکت دست تولید می‌شود، در حالی که امضای الکترونیک با الگوریتم‌های پیچیده ریاضی و توسط کامپیوتر تولید می‌شود.

۳- امضای دسـتی به راحتی و با چشم تشخیص داده می‌شود، در حالی که امضای الکترونیک با محاسبات زمانبر و توسط کامپیوتر تشخیص داده می‌شود.

مراجع صدور گواهینامه

رمزنگاری و امضای الکترونیک، محرمانگی و عدم‌انکار را برقرار می‌سـازند، اما هنگام برقراری ارتباط، طرفین از کجا مطمئن می‌شوند که طرف مقابل همان کسی است که ادعا می‌کند، مراجع صدور گواهینامه (CA) مسئول انجام این کار هسـتند. یک CA، سازمان یا شرکتی است که مورد اعتماد تمامی کاربران بوده و ارتبـاط بین هویت واقعی و کلیدعمومی او را تضمیـن و برای انجام دادن این کار یک گواهینامه الکترونیک برای اشخاص صادر می‌کند. گواهینامه الکترونیک همان شناسنامه ای است که هویت واقعی را به‌صورت مجازی و به منظور کسب و کار الکترونیک تعیین می‌کند. یک گواهینامه الکترونیک معمولاً شـامل موارد زیر است:

۱- شماره نسخه (version) که عددی صحیح است.

۲- شماره سریال (Serial Number) که عددی منحصربه‌فرد برای هر گواهینامه است.

۳- شـماره شناسایی الگوریتم امضا که صادر کننده برای امضای گواهینامه استفاده می‌کند.

۴- نـام صادر کننـده گواهینامه (Issuer) که بر اسـاس اسـتاندارد بیان می‌شود.

۵- تاریـخ اعتبار (Validity date) که شـامل تاریخ شـروع و خاتمه اعتبار گواهینامه است.

۶- نام صاحب گواهینامه که بر اساس استاندارد تعیین می‌شود.

۷- کلید عمومی صاحب گواهینامه که به همراه شناسه الگوریتم رمز نامتقارن بیان می‌شود و مورد استفاده قرار می‌گیرد.

مراجـع صدور گواهینامـه خود دارای گواهینامه‌ای از سـوی مرجع صدور گواهینامه ریشـه (Root CA) هسـتند و همچنین مراجعی به‌نام مراجع ثبت نام (RA) وجود دارند، که وظیفه ثبت درخواست گواهینامه کاربر و اعلام آن به CA و اعطای گواهینامه صادره به کاربر را بر عهده دارند.

نتیجه‌گیری

در حال حاضر مرجع صدور گواهینامه ریشه در ایران وزارت بازرگانی است و تنها مرجع ثبت‌نام گواهینامه(RA) نیز سازمان بورس و اوراق بهادار است. با توجه به اینکه امضای الکترونیک ضرورتی اجتناب‌ناپذیر در تجارت الکترونیک اسـت، بانک‌ها و به‌خصوص بانک مرکزی باید برای تخصیص یک مرکز RA تعجیل کند. بانک‌های تجاری نیز باید با آموزش کارکنان و تجهیز شعب و ستاد خود این امکان را فراهم آورند تا در کوتاهترین زمان ممکن فن‌آوری مورد بحث را دریافت و به مشتریان خود ارائه دهند.

منابع

1-Cryptography Theory and Practice, Douglas Stinson, Third .Edition , CRC Press 2005
2-Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. .Van Oorschot, Scott A. Vanstone, CRC Press 1997
Cryptography and Network Security: Principles and Practice, William Stallings , Prentice Hall