برقراری امنیت در قراردادهای الکترونیکی*

بتول آهنی – عضو هیأت علمی

چکیده

یکی از راههای انعقاد قرارداد، تبادل الکترونیکی داده‌هاست. مسائل حقوقی متعددی در این نوع قرارداد که قرارداد الکترونیکی نامیده می‌شود، مطرح شده که نیازمند نقد و بررسی است؛ اما آیا استفاده از فن‌آوری اینترنت در انعقاد قرارداد به اندازه بهره‌گیری از شیوه‌های سنتی ایمن و قابل اعتماد است؟

علت اساسی این پرسش آن است که مقدمه فنی و ضروری طرح مسائل حقوقی و فقهی راجع به قراردادها مثل اعتبار اسناد الکترونیکی بعنوان دلیل در دعاوی، انتساب اعلام اراده، مسائل راجع به اشتباه و... حصول اطمینان از صحت اعلام اراده و تمامیت پیام از خطر جعل و تحریف است.

از دیدگاه متخصصان اعلام هویتهای غیر واقعی، جعل محتوای پیام و انکار آن از مهمترین خطراتی است که متوجه قراردادهای الکترونیکی است. لذا، ضرورت دارد با اتخاذ تدابیری مناسب شناسایی طرف قرارداد، حفظ پیام از احتمال جعل و تحریف، سری نگه‌داشتن تبادلات و ممانعت از انکار و رد پیام ممکن گردد.

---

* کار ارزیابی این مقاله در تاریخ ۸۲/۳/۲۴ آغاز شد و در تاریخ ۸۲/۴/۲ به پایان رسید.

واژگان کلیدی

قرارداد الکترونیکی، امنیت، رمزگذاری، شناسایی

هدف نهایی از بحث تجارت الکترونیکی در کشورهای مختلف و بررسی جنبه‌های حقوقی آن، جایگزین ساختن این شکل از تجارت و قرارداد با اشکال سنتی آن است. اما تأمین این هدف و ترغیب تجار به پذیرش شیوه نوین، تنها با ذکر مطلوبیتها و امتیازات اقتصادی و اجتماعی آن ممکن نیست؛ تجاری که سالها به شیوه‌های سنتی تجارت خو کرده‌اند و مطلوبیتهای خاص آن را می‌شناسند، تنها هنگامی از شیوه جدید استقبال می‌کنند که قراردادهای الکترونیکی بتوانند قابلیتهای تجارت و قراردادهای سنتی را دارا باشند.

مهمترین قابلیت و مزیت قرارداد سنتی در قیاس با قرارداد الکترونیکی جنبه‌های امنیتی آن است. برقراری امنیت و محرمانه نگه داشتن اطلاعات در اشکال سنتی یعنی معاملات حضوری و مکاتبه‌ای بسادگی صورت می‌گیرد؛ اما در تجارت الکترونیکی که انعقاد قرارداد از طریق شبکه پیچیده‌ای از رایانه‌ها انجام می‌شود و میلیونها نفر به آن دسترسی دارند، قضیه به همان سادگی نخواهد بود. لذا، بعد از تعریف تجارت الکترونیکی و ذکر اهمیت آن ـ که در شماره پیشین آمد ـ و قبل از نقد و بررسی جنبه‌های حقوقی قراردادهای الکترونیکی به شناسایی خطراتی که متوجه تجارت الکترونیکی است، تعیین اهداف امنیتی و بررسی راه‌کارهای فنی حصول این اهداف می‌پردازیم.

الف) تهدیدها

تهدیدها اوضاع و حوادثی هستند که امنیت تبادلات الکترونیکی را از میان می‌برند. آنها از منابع مختلفی ناشی می‌شوند؛ گاه رخنه‌گرها با فریب کاربران، آنها را وادار به افشای اطلاعات محرمانه خود می‌کنند و گاه مستقیماً با از میان بردن اطلاعات با ارزش، جعل هویت، سرقت خدمات و غیره مشکل آفرین می‌شوند.

مهمترین انعکاس این تهدیدها در تجارت الکترونیکی دغدغه عدم اطمینان از هویت طرف مقابل است. از آنجا که تبادلات الکترونیکی حضوری نیستند، این احتمال وجود دارد

که ارسال کننده پیام، هویتی غیر از هویت مورد ادعا داشته باشد. حتی با اطمینان از هویت طرف مقابل، یقینی به مصون ماندن محتوای پیام از تعرض وجود ندارد. میلیونها کاربر به شبکه‌ای که پیام از طریق آن منتقل می‌شود، دسترسی دارند. لذا، می‌توان احتمال داد که تمام یا بخشی از پیام دریافت شده چیزی غیر از داده‌های ارسالی باشد. مسأله سری نگه‌داشتن روابط تجاری و نیز ممانعت از انکار بعدی پیام، از دیگر معضلات تجارت الکترونیکی است. بر خلاف قراردادهای سنتی که بسادگی می‌توانند محرمانه باشند، قراردادهای الکترونیکی ـ فی نفسه ـ از این امتیاز برخوردار نیستند. علاوه بر این، تضمینی وجود ندارد که ارسال کننده پیام بعداً منکر آن نگردد.

موارد مذکور بیانگر تمامی مشکلات امنیتی تجارت الکترونیکی نیستند. بیانیه شماره ۵۰۹ و ۸۰۰ اتحادیه بین‌الملل ارتباطات دور[1] تهدیدهای اطلاعاتی را به قرار ذیل بر می‌شمارد:

۱. ممانعت از شناسایی طرفین قرارداد توسط شخص ثالث؛

۲. اعلام هویت جعلی؛

۳. دوباره اجرا کردن تمام یا قسمتی از پیام قبلی بعد از ثبت آن؛

۴. قطع کردن اطلاعات از طریق مشاهده نامشروع یا مخفی مبادلات بوسیله ثالث یا کاربر غیر مجاز (یعنی بگونه غیر مجاز همان تغییراتی را در داده‌ها می‌دهد که اصولاً تنها در اختیار سوپروایزر است)؛

۵. دستکاری در محتوای پیام ارسال شده، از طریق جانشین کردن، الحاق، حذف و سازماندهی‌دوباره پیام کاربر توسط شخص ثالث غیر مجاز؛

۶. انکار تمام یا قسمتی از اطلاعات مبادله شده توسط کاربر؛

۷. محروم کردن کاربر مجاز از دسترسی به منابعی که بطور معمول در دسترس وی بودند، از طریق ایجاد وقفه در برقراری ارتباط یا تحمیل تأخیر بر زمان عملکرد[2]؛

1- ITU – T (International Telecommunication Union Telecommunication standardization sector)

2- Denial – of – service Attacks

۸. رهگزینی نابجای پیام از یک کاربر به دیگری[1] (یا انتقال اشتباه داده از ایستگاهی خاص در شبکه، به یک ایستگاه راه دور در شبکه‌ای دیگر)؛

ب) اهداف

به منظور مقابله با تهدیدهای موجود و با انگیزه ایجاد زمینه‌های حقوقی لازم برای پذیرش قراردادهای الکترونیکی، تأمین برخی اهداف امنیتی ضروری است؛ این اهداف عبارتند از:

۱. محرمانه بودن[2]؛ محرمانه بودن پیام به این معناست که ثالث غیر مجاز به پیام ارسال شده دسترسی نداشته باشد تا علاوه بر سری نگه‌داشتن پیام، امکان دستکاری در پیام نیز منتفی گردد.

۲. شناسایی[3] ؛ شناسایی اطمینان یافتن از هویت مورد ادعای ارسال دارنده پیام است و غالباً با بررسی ارتباطی که از قبل بین اشخاص و برخی ممیزات آنها مانند پس ورد[4] یا کلید کریپتوگرافی[5]، وجود داشته است، حاصل می‌گردد. شناسایی، دسترسی به منابع شبکه را نیز کنترل می‌کند[6]؛ به این معنا که تنها اشخاص مجاز و شناسایی شده قادر به دسترسی به منابع خواهند بود.

۳. تأیید اصالت[7] ؛ تأیید اصالت احراز ارسال پیام از همان منبع مورد ادعاست که مقدمه عدم قابلیت انکار و رد پیام است و ارتباط نزدیکی با مفهوم شناسایی دارد.

---

1 - Misroutting
2 -Confidentiality
3 - Identification
4 - Password
5 - Key Cryptography
6- Control access
7 - Authentication

۴. عدم رد[1] ؛ ضروری است که میان داده پیام و مرجع آن، رابطه غیر قابل انکاری برقرار شود تا ارسال کننده پیام پس از ارسال داده و دریافت دارنده پس از دریافت، قادر به رد و انکار آن نباشند.

۵. تمامیت[2]؛ داده پیام باید از وصف تمامیت برخوردار گردد و این در صورتی است که تبادل داده‌ها مطابق انتظارات کاربران باشد؛ یعنی پیام بعد از ایجاد و قبل از دریافت دچار تغییرات غیر مجاز یا مجاز ولی نابجا یا اشتباه نگردد و در نتیجه کاربران اطمینان یابند که پیام دریافت شده دقیقاً همان چیزی است که ارسال گردیده است.

ج) فن آوری‌ها و استراتژی‌های کنونی در خدمت تأمین اهداف امنیتی

پس از تعیین اهداف امنیتی باید به بررسی این موضوع پرداخت که امکانات و فن‌آوری‌های موجود چگونه می‌توانند هر یک از اهداف مذکور را تأمین نمایند.

ج.۱) محرمانه بودن پیام

محرمانه بودن پیام این امر را تضمین می‌کند که اطلاعات تنها بین کسانی که مجاز به دریافت آن بوده‌اند، جریان داشته است. با فن‌آوریهای موجود، محرمانه نمودن یا سری کردن پیام از طریق سیستم رمز نگاری ممکن می‌گردد(Guinier, 1999, P.60). رمزنگاری فرآیندی ریاضی است که پیام اصلی را به متنی غیر قابل خواندن تبدیل می‌کند. سیستم رمزنگاری بر دو نوع است:

الف) سیستم رمزنگاری سایمتریک[3] : در این سیستم، یک کلید مشترک در اختیار ارسال کننده و دریافت کننده پیام قرار دارد. ارسال کننده با استفاده از این کلید، پیام را به شکل رمز درآورده ارسال می‌کند، تا دریافت دارنده در مقصد با استفاده از همان کلید، رمز را

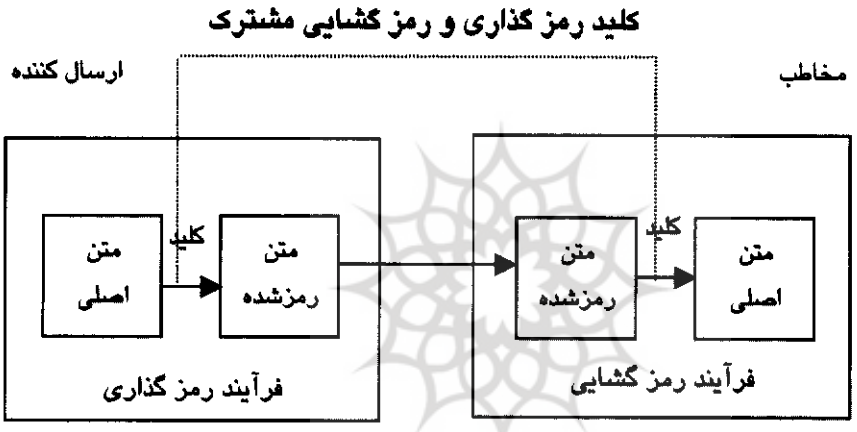
1- Nonrepudiation

2 - Inteyrity

3 - Symmetric Cryptography

بگشاید. در واقع، کلیدی که ارسال کننده برای مخفی کردن پیام از آن استفاده می‌کند، همان کلیدی است که دریافت کننده مجاز از آن بهره می‌برد (شکل ۱).

در این سیستم، تبادل کلید میان طرفین قبل از انجام معامله صورت می‌گیرد. مشکل اصلی این نوع رمزنگاری نیز همین است. هنگامی که امکان دیدار حضوری برای تبادل کلید وجود ندارد، انتقال کلید از طریق رایانه‌ای صورت می‌گیرد که چندان ایمن نخواهد بود.



شکل ۱ – سیستم رمزنگاری سایمتریک

ب)رمزنگاری اسایمتریک یا کلید عمومی[1]: به منظور حل مشکل تبادل کلید در سیستم سایمتریک، روش‌دیگری در سال ۱۹۷۶ ابداع گردید (Diffie,w and Hellman, M.E, 1976, P. 644.) در این سیستم، طرفین بجای در اختیار داشتن یک کلید مشترک هر کدام یک جفت کلید دارند. این جفت کلیدها که کلید عمومی[2] و کلید خصوصی[3] نامیده می‌شوند، با یکدیگر قرینه و جفت هستند. کلید عمومی سری نیست و می‌تواند در اختیار همه مردم از جمله طرف معامله قرار گیرد ، اما

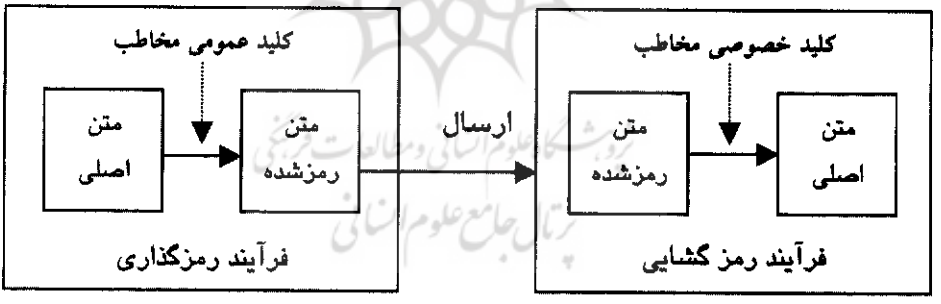
1- Asymmetric Cryprography
2- Public Key
3- Private Key

کلید خصوصی کاملاً محرمانه و تنها در اختیار مالک آن می‌باشد. از آنجا که کلید خصوصی از کلید عمومی قابل استنباط نیست، می‌توان از یک کلید برای رمز نگاری و از کلید دیگر برای رمز گشایی استفاده کرد.

برای مثال دو کاربر «الف» و «ب» هر کدام یک جفت کلید دارند؛ طرفین با تبادل اطلاعات یا توسط شخص ثالث، کلید عمومی یکدیگر را در اختیار می‌گیرند، حال اگر «الف» بخواهد پیامی را به گونه سری و محرمانه برای «ب« ارسال دارد، با استفاده از کلید عمومی«ب» آن را به صورت رمز در آورده، پیام رمز شده را به مقصد «ب» ارسال می‌کند. از آنجا که «ب» تنها شخصی است که کلید قرینه کلید عمومی خود را داراست، می‌توان - و البته تنها او می‌تواند – رمز را بازگشایی کرده، پیام را بخواند.

حال «ب» نیز می‌تواند پاسخ خود را با استفاده از کلید عمومی «الف» رمزگذاری و ارسال نماید تا «الف» آن را با کلید خصوصی خود بگشاید (شکل ۲).

شکل ۲ – سیستم رمزنگاری کلید عمومی



ب – مخاطب	الف – ارسال کننده
اطلاعات مخاطب	**اطلاعات ارسال کننده**
کلید عمومی مخاطب	کلید عمومی ارسال کننده
کلید خصوصی مخاطب	کلید خصوصی ارسال کننده
کلید عمومی ارسال کننده	کلید عمومی مخاطب

ج. ۲) شناسایی متعاملین و کنترل دسترسی

شناسایی، جریان بررسی هویت اشخاص با اتکا بر جنبه‌های شناسایی منحصر بفرد آنهاست. روشهای متعددی به این منظور طراحی گردیده است که پایه آنها گاه، استفاده از اطلاعات کاربر می‌باشد مانند «پس‌ورد»، و گاه چیزهایی است که وی در اختیار دارد مانند کارتهای شناسایی.

شیوه بکارگیری اطلاعات دارای شکل ساده‌ای است؛ هر کاربر با یک «پس‌ورد» شناخته می‌شود، اما از آنجا که اشخاص بطور معمول، پس‌ورد خود را در یک فایل مرکزی ذخیره می‌کنند یا رمزی را انتخاب می‌نمایند که مانند شماره شناسنامه، شماره تلفن، آدرس و تاریخ تولد به نوعی با هویت آنها مرتبط است، امکان کشف آن نیز وجود دارد.

شیوه دیگر استفاده از کارتهای شناسایی است. این کارتها بطور مغناطیسی در بردارنده برخی اطلاعات مانند نام کاربر، شماره شناسایی و نظایر آن می‌باشند. شخص با قرار دادن کارت شناسایی در دستگاه کارت‌خوان، شماره خود را وارد می‌نماید؛ در صورت انطباق شماره مذکور با شماره ذخیره شده در کارت، وی مجاز خواهد بود که به منابع دسترسی داشته باشد، اما استفاده غیر مجاز و ارائه شماره اشتباه منجر به توقیف کارت خواهد شد.

کارت شناسایی امکان دسترسی غیر مجاز را به نحو قابل توجهی کاهش می‌دهد، اما مشکلی که باقی می‌ماند، همان محدودیتهای ذاتی پدیده‌های فیزیکی مانند گم شدن، خرابی یا سرقت است. روش دیگر، شناسایی با اعمال یا خصوصیات فیزیکی کاربر مانند اثر انگشت، صدا، تصویر و مانند آن است[1]. جهت استفاده از این شیوه لازم است که خصوصیات شخص از پیش ذخیره گردد. هنگامی که کاربری ادعای داشتن هویتی خاص را کند، خصوصیات وی با ویژگیهای ذخیره شده سنجیده می‌شود. اشکال این روش آن است که امکان دستکاری و تقلب در داده‌های فیزیکی نیز وجود دارد. علاوه بر این با بالا رفتن دقت شناسایی، گاه هویت کاربر مجاز نیز رد می‌شود (Scherman, S.A, R.Skibom, and R.S Murray, P.61-72).

1 - Biometricks

در حال حاضر، امضای دیجیتال یعنی رمز کردن پیام با کلید خصوصی و رمز گشایی آن با کلید عمومی که در اختیار دریافت دارنده پیام است، مطمئن‌ترین شیوه شناسایی است؛ زیرا کاربر را با علایمی که بین دو طرف قرارداد مشترک است، مرتبط می‌نماید.

کاربرد عمده شناسایی در کنترل دسترسی است؛ کنترل دسترسی به معنای اطمینان از دسترسی اشخاص مجاز به منابع است. دسترسی‌های غیر مجاز خطر سوء استفاده، افشاء، تغییر یا از میان بردن اطلاعات را بهمراه دارند. بنابراین لازم است که سیستم امنیتی دسترسی به تمامی موضوعات داخل سیستم مثل فایلها، و دایرکتوری‌ها را کنترل کند. شیوه چنین است که شرح حالی از کاربران مجاز مشتمل بر نام یا نام مستعار، پس‌ورد، گروه عضویت و محدودیتها و امتیازات هر یک از آنها در استفاده از منابع مختلف ضبط می‌گردد تا معین شود که کدام کاربر امکان دسترسی به کدامین منابع و تا چه حدودی را داراست.

ج ۳۰) تأیید اصالت

هدف از تأیید اصالت ، احراز انتساب پیام به مرجع صادر کننده آن است. شیوه عملی در تأیید اصالت نیز استفاده از سیستمهای رمزنگاری است.

هنگامی که طرفین از سیستم رمز نگاری سایمتریک استفاده می‌کنند، از آنجا که ایشان تنها کسانی هستند که از کلید سری اطلاع دارند، تبادل پیام نشان دهنده اصالت آن نیز خواهد بود؛ زیرا کس دیگری غیر از آنها امکان دسترسی به این کلید را نداشته است.

استفاده از سیستم کلید عمومی نیز این هدف را بر آورده می‌کند؛ هنگامی که ارسال کننده پیام با کلید عمومی مخاطب پیام را رمز کرده ارسال می‌دارد تا مخاطب در مقصد آن را با کلید خصوصی خود بگشاید و پاسخ دهد، به دلیل ارتباطی که بین این دو کلید وجود دارد، دریافت پاسخ ارسال کننده را متقاعد می‌سازد که پیام را از دارنده کلید خصوصی متقابل دریافت کرده است و این امر به معنای تأیید اصالت پیام خواهد بود.

دو شیوه مذکور از حیث اثبات اصالت پیام، اختلافی ندارند، اما بر خلاف رمزنگاری «سایمتریک» که تأیید اصالت و شناسایی را بطور همزمان ممکن می‌کند، استفاده از کلید عمومی تنها مبین اصالت آن است؛ زیرا در سیستم سایمتریک دارندگان کلید مشترک از

پیش یکدیگر را می‌شناسند. بنابراین استفاده از کلید مذکور مترادف با شناسایی و تأیید اصالت خواهد بود. اما در سیستم کلید عمومی، به علت عدم آشنایی قبلی اشخاص نفس دریافت پیام رمز شده و پاسخگویی به آن تنها حاکی از وصول پیام از دارنده کلید متقابل، یعنی مرجع آن است که صرفاً مؤید اصالت خواهد بود. برای آنکه در استفاده از سیستم «اسایمتریک» امر شناسایی نیز ممکن گردد، دخالت شخص ثالث ضروری است. این شخص دفتری مانند دفتر تلفن دارد که در آن اسامی مالکان در برابر کلید عمومی آنان قید شده است و بسادگی می‌تواند معرف هویت دارندگان کلید باشد.

ج.۴) عدم رد

شخصی که مبادرت به تبادل داده و در نتیجه انعقاد قراردادی الکترونیکی می‌کند، نباید امکان انکار و رد کلی یا جزئی آن را داشته باشد. یعنی با اتخاذ تدابیر مناسب باید مانع از آن گردید که شخص بتواند منکر پیام ارسالی خود گردد یا وصول پیامی را که در واقع دریافت نموده است، تکذیب کند. انکار تبادل داده چیزی غیر از اقاله یا فسخ یک قرارداد است. در موارد اخیر شخص منکر پیام مبادله شده نبوده، بلکه بر مبنای قانونی مبادرت به بی‌اثر کردن آن می‌کند. حال آنکه در انکار و رد، منکر اصل تبادل داده می‌شود.

توصیه نامه شماره ۸۱۳ اتحادیه بین‌المللی ارتباطات راه دور بهترین شیوه تأمین عدم رد و جلوگیری از انکار بعدی پیام را ایجاد دلیل برای احراز ارسال و دریافت پیام و ثبت و نگهداری دلایل ایجاد شده می‌داند.

ممانعت از رد و انکار در دو شکل انجام می‌شود: شکل یا سرویس اول که سرویس مبدأ می‌باشد و با منع ارسال دارنده از انکار پیام ارسالی، از دریافت دارنده پیام حمایت می‌کند. در سرویس دوم یا سرویس مقصد، با اثبات این امر که مخاطب، پیام را دریافت نموده است از ارسال دارنده پیام حمایت می‌شود.

شیوه فنی اطمینان از عدم رد استفاده از امضاء الکترونیکی، مداخله ثالث بعنوان شاهد و مهر زمانی[1] است: در رمز نگاری کلید عمومی، از آنجا که هر کاربر مالک انحصاری کلید

1- Time - Stamping

خصوصی خود می‌باشد، قادر به انکار ارسال پیامی که با کلید خصوصی او بصورت رمز در آمده است و در حقیقت دارای امضای الکترونیکی وی می‌باشد، نخواهد بود. مداخله شخص ثالث نیز به این معناست که شخص ثالث قابل اعتماد[1]، از معامله آگاه بوده، به جمع‌آوری دلایل بپردازد تا پس از بروز اختلاف قادر به ارائه دلایل گردد.

در روش مهر زمانی از رابطه‌ای که بین هر پیام و تاریخ ارسال یا دریافت آن وجود دارد، استفاده می‌شود؛ هدف از بکارگیری این روش آن است که اشخاص نتوانند منکر ارسال یا دریافت پیام در یک دوره زمانی یا تاریخ معین گردند. در این روش، زمان تعیین شده توسط شخص ثالث موثق، ملاک عمل است. به این ترتیب که ارسال کننده، پیام خود را با کلیدی که میان او و شخص ثالث از قبل مشترک بوده است، رمزنگاری و سپس ارسال می‌نماید. شخص ثالث نیز پیام را با استفاده از همان کلید گشوده، با کلید مشترک میان خود و مخاطب، رمزنگاری کرده، ارسال می‌دارد. در حقیقت شخص ثالث مأمور تسلیم و دریافت پیام تلقی می‌شود. لذا قادر است دلایل مربوط به زمان ارسال و دریافت پیام را نیز جمع‌آوری کند.

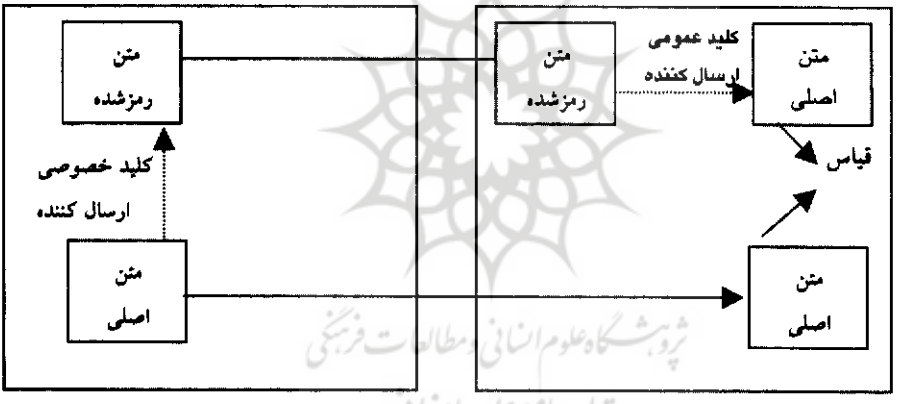
ج.۵) تمامیت داده

لازمه حفظ تمامیت داده، یعنی مصون ماندن آن از جعل و تحریف آن است که احتمال تغییرات غیر مجاز در جریان انتقال پیام از ارسال کننده به دریافت دارنده منتفی شود. در روابط سنتی، شیوه تأمین این هدف چنین است که ارسال کننده پیام خود را در پاکتی قرار داده، آن را مهر می‌نماید. به این ترتیب هر گونه دستکاری در محتوای پیام مستلزم شکستن مهر و در نتیجه کشف ماجراست. استفاده از این شیوه در تجارت الکترونیکی ممکن نیست، اما هدف مذکور به گونه‌ای دیگر قابل حصول است. یک سری «بایت» که همانند اثر انگشت منحصر بفرد بوده و به پیام ملحق می‌گردد، نقش مهر را ایفا می‌کند. شیوه‌های مختلفی به این منظور ابداع گردیده است که به شرح مهمترین آنها می‌پردازیم:

1- Thrasted third party

۱- ***حفظ تمامیت داده از طریق رمزنگاری کلید عمومی:*** چنانکه گفتیم، در این سیستم هرکس دارای یک جفت کلیداست. در اینجا ارسال‌کننده، از کلیدخصوصی خود کـه نقـش مهر را ایفامی‌کنداستفاده‌کرده، پیام را بصورت رمز درمی‌آورد؛ سپس، پیام‌رمزشده را همـراه متن‌اصلی پیام‌ارسال می‌دارد. در مقصد، مخاطب با استفاده از کلید عمومی ارسال کننده،رمز گشایی کرده به مقایسه دو متنی که در اختیار اوست می‌پردازد. همسانی دو متن نشان‌دهنده تمامیت پیام، و اختلاف آنها بیانگر نقض تمامیت است. در این روش بررسی تمـامیت پیام توسط هر شخص که کلید عمومی ارسال‌کننده را دارا باشد، ممکن‌می‌شود (شکل ۳).

شکل ۳



۲- ***حفظ تمامیت داده از طریق رمز نگاری سایمتریک :*** در اینجا، اصل پیام بـه همـراه پیامی که از طریق کلید مشترک رمز نگاری شده است، ارسال می‌گردد. در مقصد، مخـاطب با استفاده از همان کلید رمز را گشوده، به قیاس دو متن می‌پردازد؛ در این سیستم، بررسـی تمامیت داده تنها توسط شخصی که دارای کلید مشترک است، ممکن خواهد بود.

۳- ***حفظ تمامیت داده با استفاده از سیستم هش فانکشن[1] :*** این سیستم بر مبنای تبدیـل یک سلسله علایم مانند نوشته با هر طولی که باشد به یک زنجیره از علایم ـ با طول ثـابت

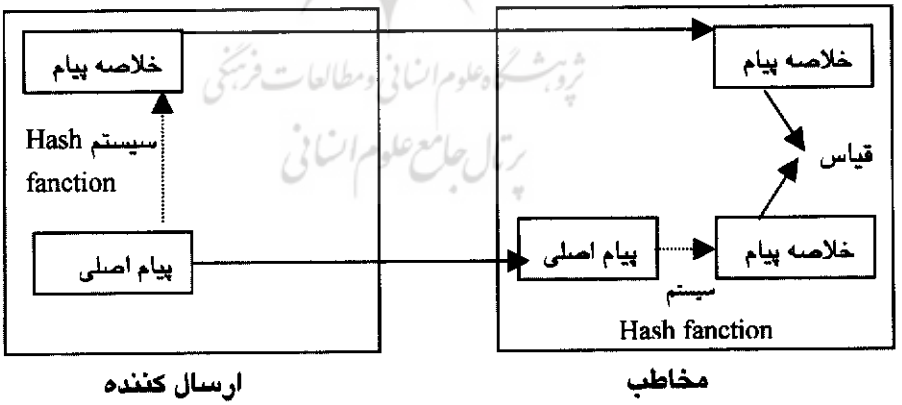
1-Hash Function

که معمولاً کوتاهتر از طول پیام اصلی است ـ استوار است. به حاصل این فرآیند، «خلاصه پیام[1]» گفته می‌شود.

این سیستم دارای چند خصوصیت است که ایمنی حاصل از بکارگیری آن را افزایش می‌دهد. اول آنکه احتمال ایجاد دو خلاصه پیام یکسان از دو متن مختلف، بسیار اندک است؛ بطوری که اختلاف جزئی در متن، موجب اختلاف کلی دو «خلاصه پیام» می‌شود. دوم آنکه عملکرد این سیستم یکطرفه می‌باشد؛ یعنی پیام اصلی قابلیت تبدیل به «خلاصه پیام» را دارد، اما با در اختیار داشتن «خلاصه پیام» نمی‌توان به متن اصلی دست یافت.

روش بکارگیری سیستم آن است که ارسال کننده، اصل پیام را با «خلاصه پیام» که از طریق یک فرآیند ریاضی و با یک الگوی تعریف شده حاصل گردیده است، ارسال می‌کند؛ چنانچه الگوی تعریف شده ارسال کننده برای مخاطب شناخته شده باشد، او می‌تواند پیام اصلی را با استفاده از همان الگو به صورت «خلاصه پیام» در آورد و دو «خلاصه پیام» را با یکدیگر مقایسه نماید. با همسانی این دو، تمامیت پیام محرز می‌شود (شکل ۴).

شکل ۴ – سیستم Hash Function



1- message digest or cryptographic check sum, finger print contradiction comprestion, hash value

قابل ذکر است که سیستم هش فانکشن قابلیت ترکیب با سیستم رمزنگاری کلید عمومی و سایمتریک را نیز داراست. از آنجا که رمز نگاری یک متن طولانی با استفاده از روش کلید عمومی بسیار کند و وقت گیر است، ارسال کننده می‌تواند پیام اصلی را با بکارگیری این سیستم، به متنی کوتاه تبدیل کند و سپس آن را با کلید خصوصی خود بصورت رمز درآورده، همراه با پیام اصلی ارسال دارد. در مقصد، مخاطب با استفاده از کلید عمومی ارسال دارنده، رمز پیام را می‌گشاید؛ سپس متن اصلی را نیز تبدیل به «خلاصه پیام» کرده، دو «خلاصه پیام» را با یکدیگر مقایسه می‌کند.(Schneier, B., 1996, P. 32) این الگو در سیستم سایمتریک نیز قابل اعمال است.

از مباحث طرح شده این نتیجه به دست می‌آید که خطرات تهدید کننده تجارت الکترونیکی بسیار جدی است. تا هنگامی که خطرات مذکور به نحو اطمینان بخشی مرتفع نشود تجارت سنتی مزیتهای خود را نسبت به تجارت الکترونیکی حفظ خواهد کرد. مع هذا بررسی امکاناتی که فن‌آوری‌ها و استراتژی‌های کنونی در اختیار ما می‌گذارد، نشان می‌دهد که تجارت الکترونیکی هم اکنون نیز قادر است تضمینات امنیتی تجارت سنتی را تأمین نماید؛ حتی بنظر می‌رسد که احتمال جعل و تزویر در قراردادهای سنتی بمراتب بیشتر از قراردادهای الکترونیکی باشد. پس همانطور که احتمال تقلب در اسناد کاغذی مانع انعقاد و اجرای قراردادهای سنتی نگردیده است، می‌توان امیدوار بود که تجارت الکترونیکی نیز با این محظور مواجه نگردد.

منابع و مآخذ :

- Diffie, W. and Hellman, M.E, ***New Directions in Cryptography***, 1976
- Guinier, D. ***Argument Pour la Reconnaissance Juridique de la signature electronigue***: Expertises, 1999
- Scherman, S. A, Skibom, R., Murry, R.S, ***Secure Network access using Multiple applications,*** 1994
- Schneier, B., ***Applied cryptography***, 2nd edition, 1996