ویژه نامه

مرکزملی شماره گذاری کالاوخدمات ایران
وابسته به مؤسسه مطالعات وپژوهشهای بازرگانی

رمزینه(بارکد)، ورود و جمع آوری خودکار اطلاعات فنی/بازرگانی
رمزینه(بارکد) زبان مشترک زنجیرهٔ تجارت
با استفاده از رمزینه، ورود به عرصه‌های تجارت الکترونیکی هموار می‌گردد

تجارت الکترونیکی

- افزایش بهره‌وری در تجارت
- صرفه‌جویی در زمان
- کاهش هزینه‌های معاملات
- گسترش زمینه افزایش رقابت
- استفاده از روش «رأس موعد» (JIT) در انبارداری
- بهبود فرایند پرداخت
- افزایش کارآیی تجاری

MEMBER OF
EAN INTERNATIONAL

انتشارات مؤسسه پیرامون EDI و تجارت الکترونیکی

- ازمبادله الکترونیکی اطلاعات تاتجارت الکترونیکی (EDI)
- تکنولوژی اطلاعات وتسهیل تجارت ملی (جلداول)
- فن آوری اطلاعات وتسهیل تجارت ملی (جلددوم)
- رهنمودهایی در شیوه های تسهیل تجاری
- توصیه ها و رهنمودهایی برای کارایی تجاری

مرکزملی شماره گذاری کالاوخدمات ایران :

تهران۱۴۱۵۹ ـ بلوارکشاورز ـ خیابان شهیدعبدالله زاده ـ نبش کوچه افشار ـ شماره ۱۹ ـ طبقه دوم

تلفن : ۶۵۴۷۴۴ ـ۶۵۰۹۶۴ نمابر : ۶۵۳۴۲۵ صندوق پستی : ۵۹۶۵ ـ ۱۴۱۵۵

E-mail:

eaniran@irtp.com

iranafact@irtp.com

ویژگی‌های تجارت الکترونیکی بر مبنای اینترنت

اشاره:

تجارت الکترونیکی به صورت مبادلهٔ الکترونیکی داده‌ها (EDI) در دو دههٔ گذشته در بخش‌های خرده‌فروشی و فروش لوازم یدکی، به صورت تراکنش‌های نرم‌افزار به نرم‌افزار به‌طور معمول مورد استفاده قرار گرفته است.

در صنایع دفاع و صنایع سنگین نیز، مدیریت چرخه تجارت الکترونیکی به صورت مفهوم بسیار پیچیده‌ای بوده که هدفش جمع‌آوری اطلاعات در تمام قسمت‌های زنجیره از طراحی تا تعمیر و نگهداری و تغییر آن بوده است.

پیشرفت‌های جنجال‌برانگیزی که در تجارت الکترونیکی به چشم می‌خورد ناشی از اینترنت و وب جهانی World Wide Web می‌باشد. این پیشرفت‌ها سبب میشوند تا تجارت الکترونیکی بیش از پیش قابل دسترس باشد و انواع مختلف تجارت الکترونیکی با حداقل هزینه و حداکثر کارآیی گسترش یابند.

اینترنت نه‌تنها تجارت الکترونیکی به‌صورت نرم‌افزار به نرم‌افزار را همانند مبادلهٔ الکترونیکی داده‌ها (EDI) انجام می‌دهد، بلکه موارد «شخص‌به‌شخص» و «شخص به نرم‌افزار» تجارت الکترونیکی را نیز دربرمی‌گیرد.

تجارت الکترونیکی اینترنتی فرصت‌های تجاری بسیار متنوعی را از تلفیق شبکه‌ها، تراکنش‌ها، چندرسانه‌ها و داده‌پردازی ایجاد می‌کند.

تجارت الکترونیکی برمبنای اینترنت مجموعه‌ای از انواع راه‌های مهم تجاری را شامل می‌شود. این تجارت شامل تجارت الکترونیکی کالاهای فیزیکی و تجارت الکترونیکی نامحسوس مانند تجارت اطلاعات می‌باشد و تمام مراحل تجاری از قبیل بازار لحظه‌ای (On-line)، سفارش، پرداخت و پشتیبانی تحویل کالاها را دربرمی‌گیرد و خدمات الکترونیکی مثل پشتیبانی از فروش و توصیه‌های حقوقی را شامل می‌شود.

این نوع تجارت، مشارکت بین سازمان‌ها از قبیل مشارکت در طراحی و مهندسی لحظه‌ای (On-line) با گروه‌های مشاوره‌ای تجارت مجازی را دربرمی‌گیرد و لذا نمی‌توان آن را به صورت منحصربه‌فرد تعریف کرد.

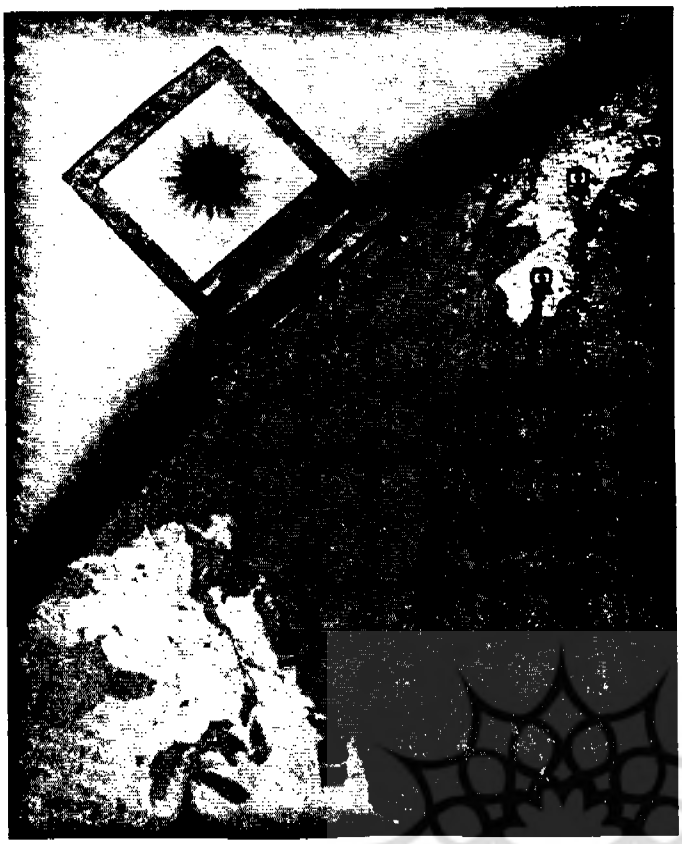
در این مقاله به بررسی توسعهٔ روزافزون تجارت الکترونیکی برمبنای اینترنت و پیش‌بینی‌های موجود درخصوص روند توسعهٔ این نوع تجارت در آینده می‌پردازیم.

پیش‌بینی می‌شود تا پایان سال جاری میلادی ۳۷۵ میلیون نفر در سراسر جهان، مشترک اینترنت شوند که این رقم نسبت به یکصدمیلیون نفر مشترک اینترنت در آغاز سال جاری میلادی، رشد چشمگیری را نشان می‌دهد. انتظار می‌رود شمار مشترکان اینترنت تا سال ۲۰۰۳ میلادی به ۶۰۰ میلیون نفر برسد.

روند روبه‌افزایش شمار مشترکان اینترنت در سه سال آینده، نشان می‌دهد که تجارت الکترونیکی برمبنای اینترنت در اوایل قرن بیست‌ویکم، از رشد روزافزونی برخوردار خواهد شد. این در حالی است که اشکال مختلف تجارت الکترونیکی تا چند سال پیش به نسبت محدودی در بین مردم جهان انتشار یافته و مورد استقبال قرار گرفته بود.

تا چند سال پیش حدود پنجاه هزار شرکت در سراسر اروپا و ۴۴۰۰ شرکت در آمریکا از مبادله الکترونیکی داده‌ها (EDI) استفاده می‌کردند که بستگی به نحوهٔ عملکرد آنها داشت. این رقم کمتر از یک درصد کل شرکت‌ها در اروپا و آمریکا بود. در واقع، مبادلهٔ الکترونیکی داده‌ها (EDI) برای شرکت‌هایی که در بخش صنعتی، قوی بودند و کنترل کیفی بالایی را اعمال می‌نمودند، بنابه نیازهای مدیریتی، مورد استفاده قرار می‌گرفت.

اما پیش‌بینی‌های پژوهشی سال ۱۹۹۷، این نتیجه را نشان داد که تجارت الکترونیکی "B-to-B"[1] تا سال ۲۰۰۲ به ۳۲۷ میلیارد دلار در سال



می‌رسد، یعنی ارزش کالاها و خدماتی که از طریق اینترنت مبادله می‌شوند، بالغ بر ۳۲۷ میلیارد دلار است. این رقم شامل ارزش سخت‌افزار، نرم‌افزار و خدماتی که جهت اجرای تجارت الکترونیکی موردنیاز است، نمی‌شود. در حالی که ارزش این خدمات نیز حدود چند میلیارد دلار تخمین زده شده است. در همین حال رقم مذکور اشکال مختلف تجارت الکترونیکی مثل مشارکت در طراحی و مهندسی یا معاملات الکترونیکی در بازارهای مالی را نیز دربرنمی‌گیرد.

پیش‌بینی تجارت ۳۲۷ میلیارد دلاری سال ۲۰۰۲ که در سال ۱۹۹۷ انجام شد، در واقع حدود یک درصد ارزش اقتصاد جهانی (۳۰ تریلیون دلار) در سال ۲۰۰۲ را دربرمی‌گیرد.

پیش‌بینی‌های انجام شده در سال ۱۹۹۸ نشان می‌داد که تجارت "B-to-B" در آمریکا تا سال ۲۰۰۳ به ۱۰۳ تریلیون دلار خواهد رسید که این رقم نیز حدود ۴ درصد اقتصاد جهانی می‌باشد.

تحقیقات دیگری که انجام شده است، نشان می‌دهد که این ارقام تا سال ۲۰۱۰ میلادی به حدود ۳۰ درصد ارزش اقتصاد جهانی خواهد رسید. زمانی که چنین نرخ رشد بالایی متوقف شد، واضح است که تجارت الکترونیکی غالب خواهد شد.

مؤسسهٔ دیتامونیتور[2] در سال

1– *Business to Business*

2- *Data Monitor*

۱۹۹۷ پیش‌بینی کرد که ظرف پنج سال (یعنی تا سال ۲۰۰۲) ۶۳۰ هزار شرکت آمریکایی و ۲۴۵ هزار شرکت اروپایی به‌طور کامل درگیر تجارت "B-to-B" خواهند شد.

در همین حال بر اساس نظرخواهی که مؤسسه ایتو۹۹ انجام داد، پیش‌بینی کردند که ۴۷ درصد شرکت‌های اروپایی از برخی اشکال تجارت الکترونیکی در سال ۱۹۹۹ استفاده می‌کردند. در همین سال فروش On-line شرکت آی‌بی‌ام (IBM) به یک میلیارد دلار رسید که این رقم غیر از درآمد ماهیانه‌اش که ۳/۳ میلیارد دلار بود، می‌باشد.

براساس نظرخواهی مؤسسهٔ «گرینکر»[1] در سال ۱۹۹۸ فقط ۸ درصد از شرکت‌های مصاحبه شده به منظور انجام خدمات تعمیر و نگهداری از اینترنت استفاده می‌کردند، اما ۸۵ درصد شرکت‌ها تصمیم گرفتند که سفارشات لحظه‌ای (On-line) و تعمیر و نگهداری و عملیات[2] خود را در حد قابل‌ملاحظه‌ای افزایش دهند. پیش‌بینی می‌شود که از هر چهار شرکت، یک شرکت در آینده از اینترنت برای سفارش و عملیات "MRO" از اینترنت استفاده کند.

این مطالعه نشان داد که مانع اصلی برای ۴۹ درصد از شرکت‌هایی که از سفارش لحظه‌ای استفاده نمی‌کردند، دسترسی نداشتن آنها به اینترنت بوده است.

نتیجه این مطالعات، با اطلاعات به‌دست آمده از «گزارش تجارت جهانی» در سال ۱۹۹۸ متفاوت بود. در آن گزارش انتظار می‌رفت که دسترسی به اینترنت در زمینهٔ تجاری از ۱۰ درصد در سال ۱۹۹۷ به ۹۰ درصد در سال ۲۰۰۱ افزایش یابد.

گزارش مؤسسهٔ آی.دی.سی نیز پیش‌بینی کرده بود که تجارت الکترونیکی برمبنای "B-to-B" در سال ۲۰۰۲ در فرانسه ۴۳ درصد، بر اساس MRO، ۳۰ درصد، بر مبنای کالاهای اولیه شامل مواد خام، سفارشات خرید توسط توزیع‌کننده‌ها ۲۵ درصد و سفارشات شخصی به ۲ درصد می‌رسد.

بررسی مؤسسهٔ «فورستر» در خصوص تجارت الکترونیکی برمبنای "B-to-B" نشان می‌دهد که از شروع این نوع تجارت در سال ۱۹۹۷ تا سال ۲۰۰۰ رشد آرامی مشاهده می‌شود و ارزش این مبادلات به حدود ۹۰ میلیارد دلار رسید. اما تا سال ۲۰۰۲ این رقم به حدود ۳۶۰ میلیارد دلار و در سال ۲۰۰۳ به یک تریلیون و ۳۰۰ میلیارد دلار بالغ خواهد شد.

مؤسسهٔ «پرایس» ارزش مبادلات الکترونیکی برمبنای "B-to-B" را در سال ۲۰۰۲ به میزان ۴۲۰ میلیارد دلار تخمین زده است.

پژوهش‌های شرکت‌های مختلف نشان می‌دهد که آنها در مورد توسعهٔ تجارت الکترونیکی در آینده، پیش‌بینی‌های متفاوتی دارند و هنوز در خصوص آینده آن اختلافات زیادی وجود دارد. با این حال انتظار می‌رود که تعداد اتصالات فردی به اینترنت به‌طور نهایی رشد کند و از طرف دیگر رشد فوق‌العاده تعداد رایانه‌های میزبان اینترنت در چند سال آینده ادامه دارد.

با این وجود تجارت الکترونیکی برمبنای "B-to-B" اگرچه به سرعت رشد کرده، اما به نظر نمی‌رسد به سطح رشد بسیار زیادی در چند سال آینده برسد.

اکثر پژوهش‌ها در سال ۱۹۹۷ پیش‌بینی کردند که "B-to-C"[3] در حدود ۱۰ تا ۲۰ درصد از کل تجارت الکترونیکی را دربرمی‌گیرد. بنابراین "B-to-B" قسمت اعظم تجارت الکترونیکی را شامل می‌شود.

وضعیت بازارها در نقاط مختلف جهان در خصوص به‌کارگیری تجارت الکترونیکی کاملاً با هم تفاوت دارد.

در اکثر نقاط، آمریکا رتبهٔ اول را در تجارت الکترونیکی دارد. تخمین زده شده که بازار اروپا حدود یک تا سه سال آینده بعد از آمریکا به سمت تجارت الکترونیکی برمبنای "B-to-B" پیش می‌رود. اگر چه رشد بالاتری را نسبت به آمریکا در سال ۱۹۹۸ به جاگذارد.

در همین حال اروپا در برخی خدمات تجارت الکترونیکی مانند پرداخت‌های الکترونیکی و استفاده از کارت‌های هوشمند، توسعهٔ بیشتری پیدا کرده است.

با این وجود، پیش‌بینی می‌شود که در چند سال آتی رشد تجارت الکترونیکی در بازار آسیا - اقیانوسیه از رشد آن در بازار اروپا پیشی بگیرد.

▣

1- *Grainqer*
2- *Maintenance, Repair and Operation (MRO)*
3- *Business to Consumer*

سیستم‌های پرداخت الکترونیکی در شبکه اینترنت

اشاره:

تجارت الکترونیکی بر روی اینترنت عبارت از انجام پرداخت‌های الکترونیکی بر روی یک شبکه عمومی برای سفارش کالا یا خدمت به طریق الکترونیکی و گرفتن تعهد برای تحویل کالاهای فیزیکی است.

برای یک شرکت جهت ورود به تجارت بر روی اینترنت دو دلیل عمده وجود دارد که ابتدا توانایی برای دستیابی به مشتریان جدید و ایجاد رابطه با همهٔ آنها و دوم کاهش هزینه‌های توزیع اطلاعات و خدمات‌رسانی به مشتریان است.

بر روی اینترنت هر دادوستدی یک حضور جهانی دارد. حتی شرکت‌های کوچک و متوسط نیز اکنون می‌توانند به آسانی به همه مشتری‌ها در سراسر دنیا دسترسی پیدا کنند.

از سوی دیگر اینترنت به‌طور شگرفی هزینه‌های توزیع اطلاعات را کاهش می‌دهد. در دنیایی که مشتری‌های متفاوت اطلاعات بیشتری را دربارهٔ محصولات و خدماتی که می‌خرند، تقاضا می‌کنند، توانایی برای تحویل آن اطلاعات (و انجام آن به‌طور ارزان) قسمت مهمی از فرآیند فروش را تشکیل می‌دهد.

اما اینترنت امنیت را فراهم نمی‌کند. بنابراین نگرانی زیادی در ارتباط با ارسال داده‌های مالی، از قبیل شماره کارت‌های اعتباری و شماره حساب‌ها بر روی اینترنت وجود دارد. به این علت همان‌طور که فعالیت‌های تجاری بر روی اینترنت رشد پیدا می‌کند، امنیت نیز مورد توجه بیشتری قرار می‌گیرد.

در این مقاله به بررسی سیستم‌های پرداخت الکترونیکی متداول در جهان و جنبه‌های امنیتی هر کدام می‌پردازیم.

نگرانی در خصوص امنیت تجارت بر روی اینترنت از چند جنبه حایز اهمیت است. اول آنکه اینترنت یک شبکهٔ عمومی است. بدون امنیت خوب، کلاهبرداری از طریق رایانه قابل ردیابی نمی‌باشد. از سوی دیگر تجارت اطلاعات مشکل است، زیرا نسخه‌برداری، توزیع و اصلاح اطلاعات از این طریق آسان است و در نهایت آنکه رایانه‌ها داده‌ها را جمع‌آوری می‌کنند.

تمرکز اصلی در تجارت الکترونیکی بر روی اینترنت، در طراحی سیستم‌های پرداخت الکترونیکی برای آن است. به‌طور کلی سیستم‌های پرداخت الکترونیکی که امروزه بر روی اینترنت متداول هستند یا برای استفاده بر روی آن پیشنهاد شده‌اند، عبارتند از: سیستم‌های مبتنی بر کارت اعتباری، چک‌های الکترونیکی، سیستم‌های پرداخت پول الکترونیکی، سیستم‌های ریزپرداخت و X-Cash.

انتظار می‌رود که تا پایان سال ۲۰۰۰، سیستم‌های مبتنی بر کارت اعتباری ۱۷ درصد، چک‌های الکترونیکی ۱۳ درصد و سیستم‌های پرداخت پول الکترونیکی ۴۱ درصد از تراکنش‌های لحظه‌ای (On-line) را

تشکیل دهد.

نیازهای امنیتی تراکنش‌های تجاری در شبکه اینترنت

یک راه‌حل امنیتی برای پردازش تراکنش‌های تجاری در شبکه اینترنت باید نیازهای امنیتی از جمله محرمانگی، تصدیق اصالت، صحت داده‌ها، عدم انکار و به‌کارگیری انتخابی خدمات را برآورده کند.

محرمانگی: به مفهوم آن است که اطلاعات برای هر کس به جز فرستنده و دریافت‌کننده غیرقابل دسترس باشند.

تصدیق اصالت: به مفهوم آن است که هر دو طرف تجاری باید بتوانند آسوده‌خاطر باشند که آنها با طرفی ارتباط برقرار می‌کنند که قصد دارند دادوستد انجام دهند.

صحت داده‌ها: به معنای آن است که داده‌های فرستاده شده به عنوان قسمتی از تراکنش نباید در طی ارسال تغییر داده شوند.

عدم انکار: به مفهوم آن است که هیچ طرفی نباید بتواند شرکت کردنش در یک تراکنش را پس از ارتکاب جرم، تکذیب کند.

به‌کارگیری انتخابی خدمات: به این مفهوم است که ممکن است لازم باشد تا قسمتی از تراکنش از نظر مخفی نگاه داشته شود، در حالی که باقیمانده همان تراکنش این چنین نباشد.

محرمانگی معمولاً از طریق رمزگذاری فراهم می‌شود. تصدیق اصالت، صحت داده‌ها و عدم انکار هم معمولاً از طریق امضاهای رقمی و گواهینامه‌های کلید عمومی فراهم می‌شوند. در واقع چهار نیازمندی اولیه برای ارتباطات تجاری، نسبتاً استاندارد هستند. هر چند پنجمین مورد نیز جنبهٔ مهمی است. سناریوی زیر را در نظر بگیرید:

یک مشتری می‌خواهد کالایی را از یک بازرگان مفروض بخرد. در روال معمول، مشتری کارت اعتباری‌اش را به دست بازرگان می‌دهد که او نیز شمارهٔ آن را به مؤسسهٔ مالی می‌فرستد تا پردازش شود. با فرض اجازه برای برداشتن از حساب، بازرگان با فروش موافقت می‌کند. این مدل به‌طور غیرضروری به بازرگان اجازه دستیابی به شماره کارت اعتباری مشتری را می‌دهد. اکنون حالت دیگری را درنظر بگیرید که مشتری می‌خواهد کالایی را از یک بازرگان مفروض بخرد. مشتری می‌تواند اطلاعات کارت اعتباری‌اش را بسته‌بندی کند و آنها را در یک پاکت مهر و موم کند، به‌طوری که تنها توسط بانک قابل رؤیت باشد. پاکت همراه با سفارش خرید به بازرگان فرستاده می‌شود. بازرگان هم پاکت را به بانکی که اجازه برای خرید را فراهم می‌کند، می‌فرستد. به محض دریافت اجازه، بازرگان به فروش خاتمه می‌دهد.

روش‌های رمزنگاری مورد استفاده در سیستم‌های پرداخت الکترونیکی

سیستم‌های پرداخت، به‌منظور تعیین هویت و قصد طرف‌های وارد شده در یک معاملهٔ مبتنی بر پرداخت، به یک تعداد از مکانیزم‌های متفاوت تکیه می‌کنند. متداول‌ترین روش به‌کارگیری امضای انسان برای یک سند است که به عنوان مبنای قانونی برای آن معامله عمل خواهد کرد. هویت امضاکننده می‌تواند با مقایسه با یک امضای نمونه ذخیره شده، تأیید شود.

اجزای اصلی این مکانیزم‌ها می‌توانند در شبکه‌های رایانه‌ای با استفاده از روش‌های رمزنگاری تکرار شوند. به علاوه، رمزنگاری برای محافظت در برابر انواع وسیعی از حملات بر روی ارتباطات بین دو طرف نیز مفید است. ما در این بخش روش‌های رمزنگاری ضروری برای فهم این که چگونه سیستم‌های پرداخت الکترونیکی کار می‌کنند را معرفی خواهیم کرد.

رمزنگاری و رمزگشایی[1]

یک پیام در شکل قابل خواندن توسط انسان در اصطلاحات رمزنگاری متن واضح نامیده می‌شود. پردازش پنهان کردن یک پیام به‌طوری که مفادش مخفی نگه داشته شود، رمزگذاری نامیده می‌شود و پیام نتیجه، متن رمز شده نامیده می‌شود. پردازش عکس (رمزگشایی)، پیام رمز شده را به عنوان ورودی می‌گیرد و متن واضح ابتدایی را برمی‌گرداند.

رمزگذاری متقارن[2]

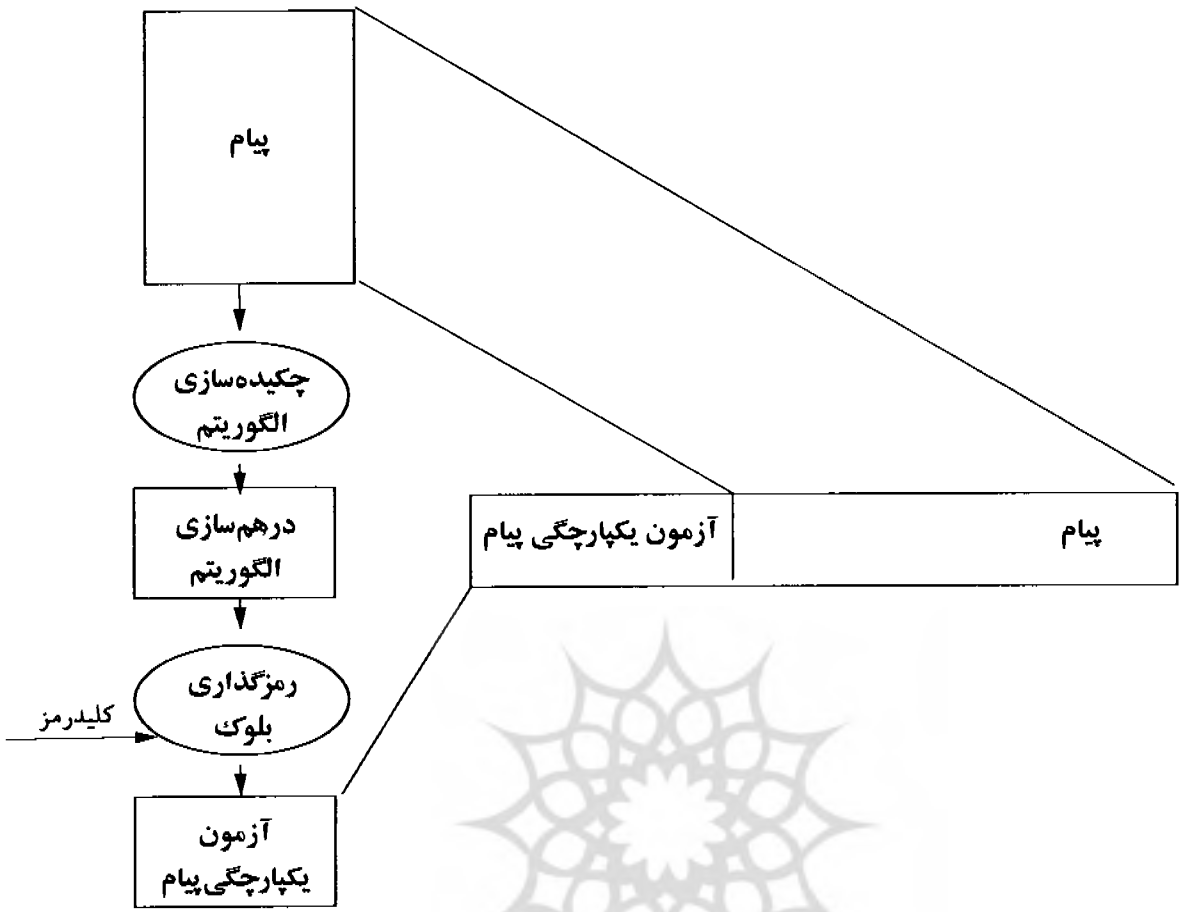
همان‌طور که از نامش پیداست، رمزگذاری متقارن مستلزم این است که هر دو طرف یک ارتباط باید ابتدا یک نسخه از یک کلید سری واحد را به‌دست آورند. مورد استفاده‌ترین الگوریتم در این دسته (DES)[3] است.

چکیده‌سازی[4] یا درهم‌سازی[5] پیام

هنگامی که الگوریتم‌های متقارن برای یک پیام به‌کار برده شوند، آنها دو خدمت اصلی را فراهم می‌کنند. نخست آنکه، محتویات پیام از استراق‌سمع کنندگان مخفی نگه داشته می‌شود و دوم اینکه، صحت پیام بیمه می‌شود.

در خیلی از حالات، یک کنترل بر روی صحت پیام، تمام آن چیزی است که خواسته می‌شود و زمان صرف شده، در فراهم نمودن محرمانگی تلف می‌شود. در

1– *Encryption and Decryption*
2– *plain text or clear text*
3– *Data Encryption Standard*
4– *Digesting*
5– *Hashing*



بسیاری از کاربردهای تجاری، استفاده‌کنندگان نگران استراق‌سمع کردن حمله‌کنندگان بر روی پیام نیستند، اما در صورتی نگران می‌شوند که محتویات پیامشان در راه تغییر داده شود.

یک راه برای فراهم نمودن صحت بدون محرمانگی، استفاده از طرحی است که به عنوان یک چکیده از پیام شناخته می‌شود. این شامل به‌کار بردن یک الگوریتم درهم‌سازی یا چکیده‌سازی بر روی یک پیام (طولانی) است تا یک چکیدهٔ کوتاه از پیام تولید شود. کلید سری هم می‌تواند برای این درهم‌سازی به‌کار برده شود و نتیجه به همراه پیام از طریق شبکه فرستاده شود. نمودار بالا نشان می‌دهد که چگونه الگوریتم درهم‌سازی ابتدا برای تمام پیام به‌کار برده می‌شود. درهم‌سازی سپس رمز می‌شود تا آزمون یکپارچگی پیام (MIC) تولید شود که قبل از ارسال پیام به آن افزوده می‌شود. از آنجا که رمزگذاری تنها برای یک مقدار خیلی کوچک به‌کار برده می‌شود و چکیده‌سازی پیام خیلی سریع‌تر از رمزگذاری آن است، این پردازش می‌تواند به‌طور قابل ملاحظه‌ای سریع‌تر از رمز نمودن تمام پیام باشد.

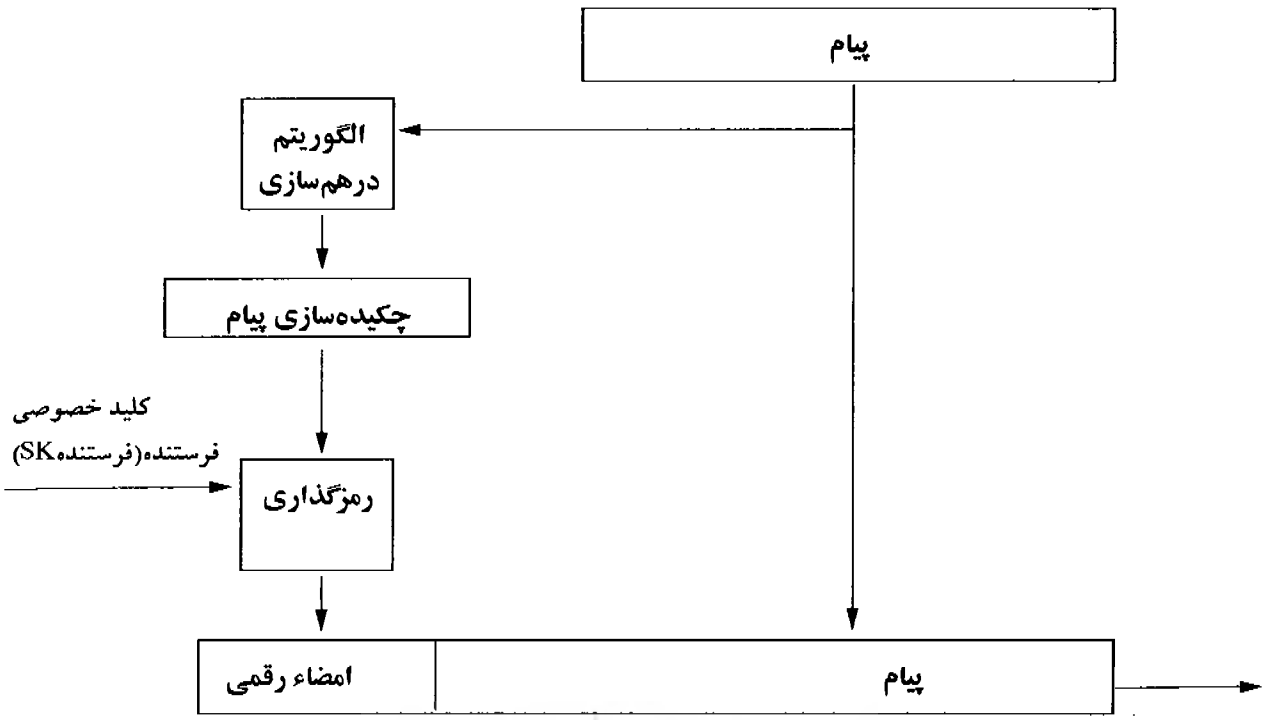
هنگامی که پیام می‌رسد، دریافت‌کننده با استفاده از همان الگوریتم، یک درهم‌سازی از پیام محاسبه می‌کند. اگر این درهم‌سازی با MIC خارج شده از رمز که همراه با پیام آمده مطابقت کرد، آنگاه پیام تحریف نشده است. دو تابع درهم‌سازی معروف که در پروتکل‌های پرداخت استفاده می‌شوند، MD5 و SHA هستند.

رمزگذاری به شیوهٔ کلید عمومی یا رمزگذاری نامتقارن[1]

بزرگترین مسأله در استفاده از سیستم‌های رمز متقارن این است که قبل از این که هر ارتباطی بتواند مشاهده شود، هر دو طرف باید به طریقی یک کلید اشتراکی را به دست آورند. این امر در یک شبکه باز خیلی سخت‌تر است، به دلیل اینکه طرف‌هایی که قبلاً هیچ‌گونه ارتباطی با هم نداشته‌اند، ممکن است بخواهند تا به یک ارتباط ناخواسته وارد شوند. یک مثال خوب در این مورد آن است که یک متقاضی بخواهد تا کالاهایی را از طریق شبکه از بازرگانی که کاملاً ناشناخته است، بخرد.

رمزنگاری به شیوهٔ کلید عمومی، اولین بار در سال ۱۹۷۶ توسط مارتین هالمن و ویتفیلد دیفی به منظور حل مسأله مدیریت کلید مذکور پیشنهاد شد. در رمزنگاری به شیوهٔ کلید عمومی، هر شخص یک جفت کلید که کلید سری و کلید عمومی نامیده می‌شود را به‌دست می‌آورد. کلید عمومی منتشر می‌شود و در بسیاری از جاها توزیع می‌شود، در

1- *Asymmetric Encryption*



حالی که کلید سری هرگز ارسال یا به اشتراک گذاشته نمی‌شود. بنابراین هنگامی که علی می‌خواهد تا یک پیام رمز شده را به بابک بفرستد، او ابتدا کلید عمومی بابک (PKB) را در یک کشوی عمومی جستجو می‌کند یا آن را از طریق دیگری به‌دست می‌آورد و برای رمز نمودن پیام از آن استفاده می‌کند و آن را به بابک می‌فرستد. بابک هم کلید سری‌اش (SKB) را استفاده می‌کند تا پیام را از رمز خارج نماید. هر کسی که به کلید عمومی بابک دسترسی داشته باشد، می‌تواند یک پیام رمز شده به او بفرستد. اما هیچ کس دیگری به غیر از بابک نمی‌تواند آن را از رمز خارج کند. یکی از الگوریتم‌های استاندارد برای پیاده‌سازی رمزنگاری به شیوهٔ کلید عمومی، الگوریتم RSA است.

امضاهای رقمی[1] و پنهان‌سازی[2]

سیستم‌های کلید عمومی می‌توانند برای دو هدف استفاده شوند: رمز کردن یک پیام با کلید عمومی دریافت‌کننده برای رسیدن به محرمانگی یا رمز کردن یک پیام با کلید سری فرستنده برای رسیدن به تصدیق اصالت پیام. هر دوی اینها الگوریتم کلید عمومی را برای تمام پیام به‌کار می‌برند. الگوریتم‌های کلید عمومی مورد استفاده امروز با تأکید بر محاسبه[3] هستند، و با پیام‌های بزرگ ممکن است بیش از حد گران یا برای بعضی کاربردها، بیش از حد کند باشند، اما راه‌حل‌های دیگری نیز وجود دارد.

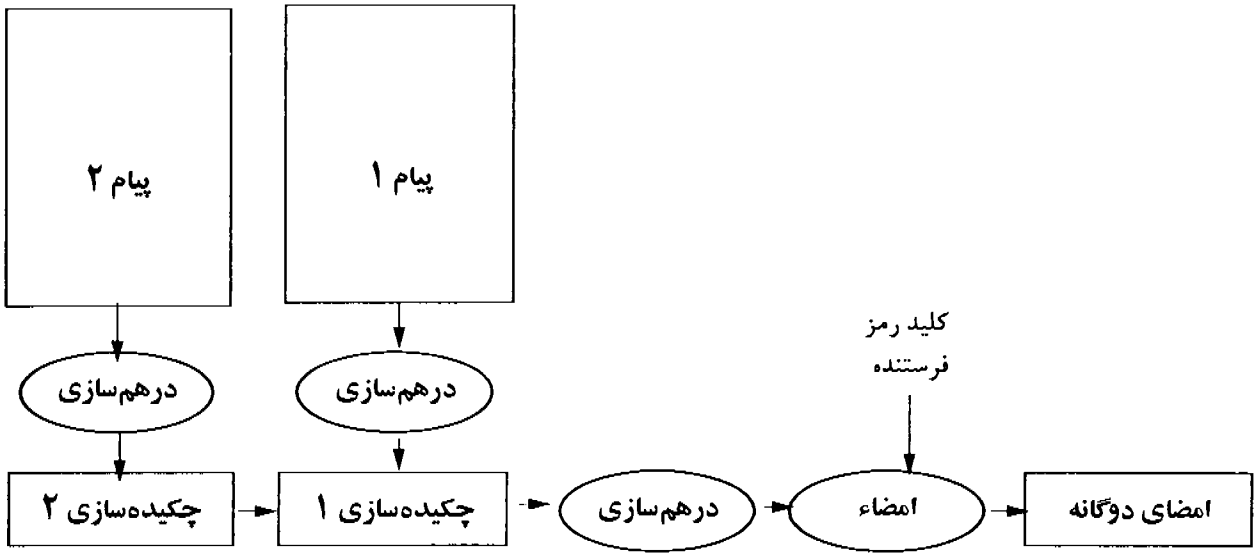
اگر تصدیق اصالت پیام موردنظر باشد، یک راه ساده برای رسیدن به آن استفاده از یک الگوریتم از قبیل MD5 یا SHA است. ابتدا یک چکیده از پیام محاسبه می‌کنیم، سپس کلید سری فرستنده را برای آن به‌کار می‌بریم. کمیت نتیجه می‌تواند به عنوان یک امضای رقمی درنظر گرفته شود و قبل از این که پیام ارسال شود به آن افزوده شود. تصویر زیر این پردازش را نشان می‌دهد. در مقصد، دریافت‌کننده الگوریتم درهم‌سازی یکسانی را برای تولید یک چکیده از پیام استفاده می‌کند و با استفاده از کلید عمومی فرستنده بررسی می‌کند که چکیده محاسبه شده با امضای از رمز خارج شده مطابقت دارد یا نه. در حالت تطابق، او می‌تواند مطمئن شود که پیام از فرستنده موردنظر صادر شده و در طی ارسال تغییر داده نشده است.

اگر محرمانگی پیام موردنظر فرستنده باشد، سپس پیام می‌تواند پنهان‌سازی شود. برای رسیدن به این منظور، فرستنده می‌تواند یک کلید به صورت تصادفی بسازد. سپس این کلید را همراه با یک الگوریتم رمزگذاری متقارن (سریع) استفاده کند تا پیام را رمز نماید. این کار پیام را از استراق سمع‌کنندگان محافظت خواهد نمود. به منظور انتقال این کلید به دریافت‌کننده، با کلید عمومی دریافت‌کننده رمز می‌شود و در پیام ارسالی گنجانده می‌شود. هنگامی که پیام رسید، دریافت‌کننده کلید سری‌اش را استفاده می‌کند تا کلید رمزگذاری محتوی را باز کند، به‌طوری که به او اجازه دستیابی به پیام در متن واضح را بدهد.

امضاهای دوگانه[4]

امضاهای رقمی به منظور مرتبط ساختن یک هویت با محتوی یک پیام

1– *Digital Signature*
2– *Enveloping*
3– *Computing*
4– *Dual Signature*



بخصوص استفاده می‌شوند. به منظور تأیید پیام، دریافت‌کننده باید بتواند به محتوی پیام دسترسی پیدا کند. در پروتکل‌هایی که سه طرف را دربردارند، از قبیل یک تراکنش کارت اعتباری، یک روش رمزنگاری که گاهی اوقات به کار برده می‌شود، امضای دوگانه است. این روش یک ارتباط بین یک پیام و یک هویت فراهم می‌کند، بدون اینکه نیاز به دیدن محتویات پیام باشد. همان‌طور که نامش اشاره دارد، در کاربردهایی استفاده می‌شود که دو پیام وابسته به هم فرستاده می‌شوند. هر زمان که یک پرداخت انجام می‌شود، بین جزییات مالی موردنیاز برای انجام تراکنش و جزییات آنچه خریداری شده است، می‌تواند فرق گذاشته شود. اینها می‌توانند به دو پیام مجزا از هم تفکیک شوند.

نمودار بالا نشان می‌دهد که چگونه یک امضای دوگانه ساخته می‌شود. نخست آنکه دو پیام وابسته به هم به طور مجزا توسط بعضی از الگوریتم‌های چکیده‌سازی پیام، درهم‌سازی می‌شوند. سپس دو چکیده به هم الحاق می‌شوند و یک چکیده جدید محاسبه می‌شود که با کلید خصوصی فرستنده امضا می‌شود.

اگر علی دو پیام داشته باشد و بخواهد تا پیام اول را به بابک و پیام دوم را به رضا بفرستد، و به هر دوی بابک و رضا اطمینان دهد که یک پیام مرتبط دومی نیز وجود دارد، او می‌تواند پیام ۱، چکیدهٔ ۲ و امضای دوگانه را به بابک و همچنین پیام ۲، چکیده ۱ و امضای دوگانه را به رضا بفرستد. هنگامی که بابک این داده‌ها را دریافت می‌کند، او می‌تواند الگوریتم درهم‌سازی را برای پیام ۱ به‌کار برد، آن را به چکیدهٔ ۲ الحاق کند، نتیجه را درهم‌سازی کند و بررسی نماید که این با امضای دوگانه مطابقت می‌کند یا نه.

بنابراین، هر چند او تنها می‌تواند محتویات پیام ۱ را ببیند، علاوه بر آن می‌تواند مطمئن شود که یک پیام ۲ نیز موجود است که به چکیده ۲ درهم‌سازی می‌شود و امضای دوگانه این دو سند را به هم پیوند می‌دهد. رضا نیز در موقعیت مشابهی است که تنها می‌تواند پیام ۲ را ببیند، اما می‌تواند بررسی کند که امضای دوگانه پیام ۲ را به پیام ۱ پیوند می‌دهد یا نه.

امضاهای چشم‌بسته[1]

استفاده از امضاهای چشم‌بسته، روشی است که به یک شخص اجازه می‌دهد تا یک پیام را بدون اینکه قادر به دیدن محتویاتش باشد، امضا کند. این روش برای پیاده‌سازی پروتکل‌های پول دیجیتال و رأی‌گیری استفاده شده است. امضاهای چشم‌بسته اولین بار توسط دیوید چوام پیشنهاد شده‌اند.

پردازش ناخوانا کردن یک پیام می‌تواند به‌صورت گذاشتن آن در یک پاکت همراه با یک تکه کاغذ کاربن تصور شود. هیچ کس نمی‌تواند پیام قرار داده شده، در پاکت را بخواند. امضای چشم‌بسته با امضا کردن روی پاکت ساخته می‌شود. امضا از طریق کاغذ کاربن به پیام منتقل می‌شود. هنگامی که پیام از پاکت بیرون آورده شود، امضا شده خواهد بود و امضاکننده هم نخواهد دانست که چه چیزی را امضا کرده است. در مراحل زیر، علی پروتکل امضای چشم‌بسته را استفاده می‌کند تا کاربر دیگر، بابک را وادار به امضای پیام کند، بدون اینکه وی از محتویات آن پیام اطلاع پیدا کند.

۱ علی پیام را می‌گیرد و آن را در یک عدد تصادفی (عامل ناخوانایی)[2] ضرب می‌کند. این عمل پیام را ناخوانا می‌کند، به‌طوری که محتویاتش نمی‌توانند خوانده شوند.

۲ - علی، پیام ناخوانا شده را به بابک می‌فرستد.

۳- بابک هم سند ناخوانا را به صورت رقمی امضا می‌کند و آن را به علی برمی‌گرداند.

۴ - علی، پیام امضا شده توسط بابک را بر عامل ناخوانایی تقسیم می‌کند و پیام ابتدایی را به‌دست می‌آورد.

برای این منظور توابع امضا و ضرب باید جابجاپذیر باشند.

■

1– *Blind Signatures*

2– *Blinding Factor*