امضای دیجیتال

زینب ایزدی
z.ezadi128@gmail.com

چکیده
گسترش سطح مبادلات تجاری و لزوم سرعت‌بخشی و آسان‌سازی در معاملات بازرگانی، استفاده از ابزار الکترونیکی را در این خصوص اجتناب‌ناپذیر کرده است. هویت مجازی، شرط اوّل یک خریدار یا فروشنده الکترونیکی است؛ به‌ویژه در مواردی که عرصه کسب‌وکار گسترده‌تر می‌شود. مدیریت اسناد الکترونیکی و ارسال و دریافت اطلاعات الکترونیکی، بخش بزرگی از تبلیغات و فعالیت‌های اجرایی را در جهان امروز شامل می‌شود. یکی از فناوری‌هایی که سبب افزایش اعتماد گردیده، امضای دیجیتالی است. این تکنیکِ مبتنی بر رمزنگاری، باعث رسمیت اطلاعات الکترونیکی شده است؛ به‌طوری‌که هویت پدیدآورنده سند و جامعیت اطلاعات آن را قابل بازبینی و کنترل می‌نماید. این مقاله، سعی دارد علاوه بر معرفی امضای دیجیتال و کاربردهای آن، بر جنبه فنی امضای دیجیتالی و حداکثر اطلاعات مربوط به امضای دیجیتال و آینده فناوری اطلاعات نیز تمرکز داشته باشد.

کلیدواژگان: احراز هویت، امضای دیجیتال، دولت الکترونیک،گواهینامه دیجیتال، کلید خصوصی، کلید عمومی.

درآمد
امروزه کاغذها که حامل اصلی اطلاعات مهم بودند، کم‌کم جای خود را به دیگر راه‌های تبادل اطلاعات می‌دهند. در واقع، کاغذ، دارای معایبی از قبیل انتقال آهسته و پُرهزینه اسناد می‌باشد و بایگانی آنها نیز مشکلات فراوانی را به وجود می‌آورد. به‌تدریج، با پیشرفت فناوری اطلاعات، تبدیل تجارت سنّتی به تجارت الکترونیک، تبادل اسناد در این نوع تجارت، امری فراگیر شده است. این اسناد، اغلب حاوی اطلاعات حساسی مانند: قراردادهای حقوقی، فناوری‌های محرمانه و یا تبادلات مالی می‌باشند. برای ممانعت از دستبرد سارقان کامپیوتری که در فضای الکترونیکی همواره مترصد دست‌اندازی و خواندن مستندات می‌باشند، لازم است این اسناد به رمز درآورده شوند. اگر می‌خواهیم که اسناد ما واقعاً در امان باشند، باید آنها را به صورت دیجیتالی امضا کنیم. امضای دیجیتالی، یکی از روش‌های ایمن‌سازی اطلاعات است که کاربردی مشابه با امضای معمولی در معاملات دارد و یکی از روش‌های معتبر حفظ امنیت در شبکه می‌باشد. این روش، به‌خصوص در مسئله تجارت الکترونیک که امروزه در جهان صنعت و فناوری از طرف‌داران بسیاری برخوردار است، جایگاه ویژه‌ای دارد.

چیستی امضای دیجیتالی
امضاهای دیجیتالی، مانند «اثر انگشت الکترونیکی»، در قالب یک پیام رمزگذاری شده هستند. امضای دیجیتال، نوعی رمزنگاری نامتقارن است که خصوصیات امضای دستی را در فضای الکترونیکی فراهم می‌کند. هر موجودیت منحصربه‌فرد در فضای مجازی، دارای امضای دیجیتالی خاص خود است و تنها این موجودیت یا فرد، قادر به تولید این امضاست. در نتیجه، می‌توان مستندات، پیغام‌ها و داده‌های الکترونیکی را توسط امضای دیجیتال تأیید کرد و سندیت بخشید؛ به شکلی که مطمئن بود تولیدکننده امضا، چه کسی است و متن پیغامِ امضاشده، پس از امضا تغییر نکرده است. بدین وسیله، متن سند یا پیام امضاشده، قابل استناد و پیگیری بوده و غیرقابل انکار است. امضایِ دیجیتال برای هر مستند یا پیغام به وسیله کلید خصوصی فرد تولید می‌شود و در واقع، یک عدد با طول بلند است. کلید خصوصی فرد، به صورت امن در وسیله‌ای مانند کارت هوشمند نگهداری می‌شود.

امضاهای دیجیتالی، مانند «اثر انگشت الکترونیکی»، در قالب یک پیام رمزگذاری شده هستند. امضای دیجیتال، نوعی رمزنگاری نامتقارن است که خصوصیات امضای دستی را در فضای الکترونیکی فراهم می‌کند. هر موجودیت منحصربه‌فرد در فضای مجازی، دارای امضای دیجیتالی خاص خود است و تنها این موجودیت یا فرد، قادر به تولید این امضاست

بدین ترتیب، جعل امضای دیجیتالی، بسیار مشکل‌تر از امضای دستی است.

توسط امضای دیجیتالی، سندیت خاصی به اسناد الکترونیکی داده می‌شود. بنابراین، می‌توان به صورت قابل اعتماد و مطمئن، ارسال‌کننده پیغام یا تأییدکننده سند را شناسایی کرد. در نتیجه، اسناد الکترونیکی قابل پیگیری بوده و به کمک آن، فعالیت افراد در فضای مجازی جنبه حقوقی پیدا می‌کند و قوانین حقوقی اسناد کاغذی در مورد اسناد الکترونیکی قابل اجرا می‌شود.

از طرف دیگر، با توجه به عدم امکان جعل امضای دیجیتال، اسناد یا پیام‌های امضاشده، قابل انکار از طرف امضا کننده نیست. بدین وسیله، مراجع قضایی می‌توانند از این خصوصیت جهت استناد قانونی به سند الکترونیکی استفاده کنند؛ اما امضای دیجیتال، دارای خصوصیت دیگری نیز هست که امضای دستی، فاقد آن است. به وسیله امضای دیجیتال می‌توان مطمئن بود که محتوای سند یا پیام، بعد از امضا تغییر نکرده و افراد غیرمجاز سند الکترونیکی مربوطه را مخدوش نکرده‌اند. این بدان دلیل است که امضای دیجیتالی، به ازای هر سند یا پیام وابسته به متنِ پیام تولید می‌شود و امضای تولیدشده برای هر سند، منحصربه‌فرد می‌باشد.

بدین ترتیب، با در اختیار داشتن متن سند یا پیام در کنار امضای دیجیتالی آن، می‌توان با اعتبارسنجی امضای دیجیتال، درعین‌حال، از عدم تغییر محتوای آن نیز مطمئن شد. در نتیجه، به کمک امضای دیجیتال در کنار قابلیت شناسایی امضاکننده، امنیت خاصی نیز به اسناد الکترونیکی اضافه می‌شود که به آن، حفظ یکپارچگی سند می‌گویند؛ به این معنا که سند، قابل رؤیت و خواندن می‌باشد؛ اما نمی‌توان آن را تغییر داد یا به عبارتی، مخدوش کرد. امضای دیجیتالی، بر روش‌های رمزنگاری از طریق کلیدهای عمومی و خصوصی مبتنی است. درحال‌حاضر، در کشورهای متعدد و برای کاربردهای گوناگون، از صدور ایمیل گرفته تا نقل و انتقالات مالی و امضای اسناد تعهدآور، از امضای دیجیتال همانند ابزاری که به اطلاعات روح می‌دهد، استفاده می‌شود و کاربرد آن در شبکه‌های الکترونیکی به یک ضرورت تبدیل شده و در شرایطی که ایمیل‌های ارسال‌شده به صندوق الکترونیکی یک فرد از لحاظ امنیتی قابل تأیید نیست، امضای دیجیتالی این امکان را فراهم می‌کنند تا فرد موردنظر از لحاظ امنیتی، با اطمینان تبادلات خود را انجام دهد.

قانون فناوری اطلاعات، امضای دیجیتالی را به عنوان وسیله احراز هویت و امنیت اسناد الکترونیکی می‌داند. امضای دیجیتال، یک نشانه الکترونیکی است که اتصال بین یک نهاد و یک رکورد داده را ایجاد می‌کند و به منظور اعتبارسنجی و تأیید اعتبار استاد الکترونیکی مورد استفاده قرار می‌گیرند و به فرایند گواهینامه صدور محتویات سند اشاره دارد؛ درحالی‌که احراز هویت، به فرایند گواهی فرستنده سند اشاره دارد. می‌توان گفت که امضای دیجیتالی، یک نسخه الکترونیکی از امضای دست‌نوشته است. امضاکننده، از کلید خصوصی خود برای ایجاد امضای دیجیتالی برای یک سند استفاده می‌کند و برای رمزنگاری آن، از کلید عمومی استفاده می‌شود و این اطمینان را می‌دهد که محتوای اصلی پیام یا سندِ فرستاده‌شده، بدون تغییر است... .

به عبارت ساده‌تر، در دنیای مجازی امروز، هر مکانیزمی که بتواند سه نیاز زیر را در خصوص اسناد و مدارک دیجیتالی برآورده کند، امضای دیجیتال نامیده می‌شود:

۱. دریافت‌کننده سند یا پیام الکترونیکی بتواند هویت صاحب سند را به‌درستی تشخیص بدهد و از جعلی نبودن آن اطمینان حاصل کند؛

۲. صاحب و امضاکننده سند بعداً نتواند محتوای سند یا پیام ارسالی خود را به هر طریقی انکار کند؛

۳. یک متقلب ثالث نتواند پیام‌ها یا اسناد جعلی تولید کند و آنها را به دیگران نسبت دهد.

روش ایجاد و پیاده‌سازی امضای دیجیتال

قبل از آشنایی با شیوه عملکرد یک امضای دیجیتال، لازم است در ابتدا با برخی اصطلاحات مرتبط با این موضوع بیشتر آشنا شویم:

* کلیدها (**Keys**): از کلیدها به منظور ایجاد امضاهای دیجیتال استفاده می‌گردد. برای هر امضای دیجیتال، یک کلید عمومی و یک کلید خصوصی وجود دارد. کلید خصوصی، بخشی از کلید است که شما از آن به منظور امضای یک پیام استفاده می‌نمایید. کلید خصوصی، یک رمز عبور حفاظت‌شده است و نباید آن را در اختیار دیگران قرار داد. کلید عمومی، بخشی از کلید است که امکان استفاده از آن برای سایر افراد وجود دارد.

* حلقه کلید (**Key Ring**): شامل کلیدهای عمومی است. یک حلقه کلید، از کلیدهای عمومی افرادی که برای شما کلید مربوط به خود را ارسال نموده و یا کلیدهایی که از طریق یک سرویس‌دهنده کلید عمومی دریافت نموده‌اید، تشکیل می‌گردد. یک سرویس‌دهنده کلید عمومی، شامل کلید افرادی است که امکان ارسال کلید عمومی در اختیار آنان گذاشته شده است.

* اثر انگشت: زمانی که یک کلید تأیید می‌شود، در حقیقت، منحصربه‌فرد بودن مجموعه‌ای از حروف و اعداد که اثر انگشت یک کلید را شامل می‌شوند، تأیید می‌گردد.

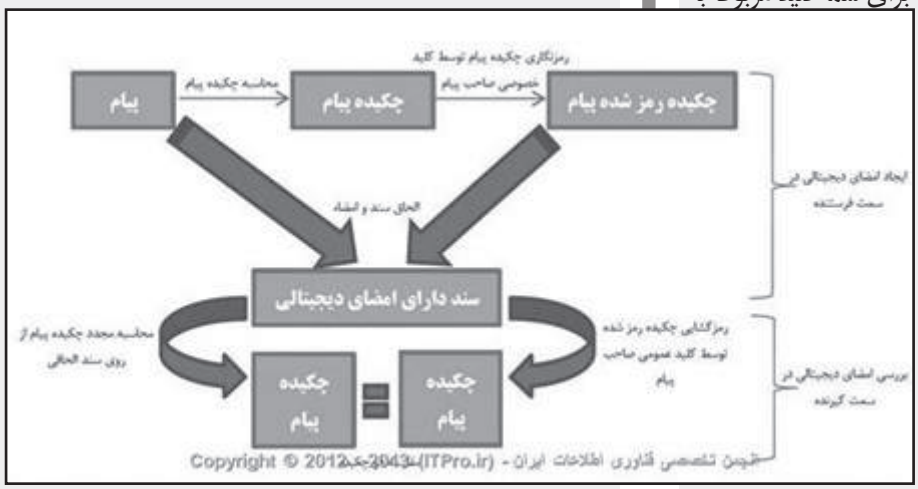
* گواهینامه‌های کلید: در زمان انتخاب یک کلید از روی یک حلقه کلید، امکان مشاهده گواهینامه کلید وجود خواهد داشت. در این باره می‌توان به اطلاعات متفاوتی نظیر: صاحب کلید، تاریخ ایجاد و اعتبار کلید دست یافت.

مهم‌ترین روش‌های پیاده‌سازی امضای دیجیتالی

۱. امضای دیجیتالی مبتنی بر چکیده پیام

در این مکانیزم، از هر سند ـ پس از ایجاد و قرار گرفتن در یک قالب استاندارد و مشخص ـ یک چکیده کوتاه چند بایتی استخراج می‌شود. این چکیده کوتاه، به طرز بسیار پیچیده‌ای از تک‌تک بیت‌ها و جایگاه آنها در متن تأثیر می‌پذیرد و به نحوی محاسبه و استخراج می‌شود که هرگونه تغییر جزیی یا کلی در متن، باعث تغییرات چشمگیر در چکیده آن خواهد شد. پس از استخراج چکیده پیام، رشته بیتی حاصل، توسط کلید خصوصی صاحب پیام رمزنگاری شده، نتیجه به‌دست‌آمده به اصلِ پیام ضمیمه می‌شود. در حقیقت، امضای دیجیتالی چیزی نیست جز یک رشته عددی که به روش پیچیده‌ای، از متن یک سند استخراج گردیده و پس از رمزنگاری با کلید خصوصی صاحب سند، به اصل سند ضمیمه و ارسال می‌شود. برای اعتبارسنجی و تأیید اصالت سند، گیرنده می‌تواند به‌راحتی چکیده ضمیمه‌شده سند را با کلید عمومی صاحب سند ـ که همه آن را می‌دانند ـ از رمز خارج کرده و همچنین، یکبار دیگر خودش رأساً چکیده سند را محاسبه نماید و این دو را با هم مقایسه کند. هرگاه این دو مقدار با هم مساوی بودند، اصالت و اعتبار سند تأیید می‌شود. در غیر این صورت، سند، جعلی است یا توسط اخلال‌گران میانی، تغییراتی در آن اعمال شده است. (نمودار شماره ۱)

نمودار شماره ۱: فرآیند امضای دیجیتال مبتنی بر چکیده پیام

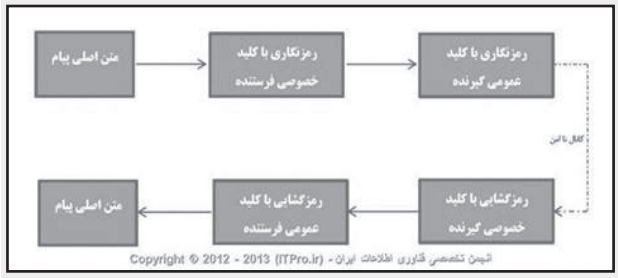


۲. امضای دیجیتالی مبتنی بر روش‌های رمزنگاری کلید عمومی

یکی از مکانیزم‌هایی که نیازهای سه‌گانه امضای دیجیتالی را برآورده می‌کند، امضا و رمزنگاری پیام به روش کلید عمومی است. روش کار به این صورت است: فرستنده ابتدا کل پیام را با کلید خصوصی خود رمز می‌کند. از آنجا که همه افراد، کلید عمومی فرستنده را می‌دانند، این مرحله از رمزنگاری، هیچ کمکی به امنیت پیام نمی‌کند؛ بلکه هرگاه افراد توانستند پیام را با کلید عمومی فرستنده از رمز خارج کنند، مطمئن خواهند شد که پیام از

طرف فرستنده صادر شده است.

سپس، فرستنده حاصل مرحله قبل را با کلید عمومی گیرنده رمز کرده، تا متن پیام محرمانه بماند. بدیهی است که فقط دارنده کلید خصوصی، یعنی گیرنده قادر به رمزگشایی خواهد بود. روال رمزگشایی و تأیید اصالت پیام، برعکس است؛ گیرنده ابتدا پیام رمزشده را با کلید خصوصی خود از رمز خارج کرده و سپس، بار دیگر آن را با کلید عمومی فرستنده رمزگشایی می‌کند. هرگاه پیام معتبری رمزگشایی شود، گذشته از حفظ محرمانگی پیام در طول مسیر، هویت فرستنده نیز تأیید می‌شود. در نمودار شماره ۲، این روال به تصویر کشیده شده است.



نمودار شماره ۲: امضا و رمزنگاری کل پیام به روش کلید عمومی

ویژگی‌های امضای دیجیتال

حال در این بخش، مزایای استفاده از امضای دیجیتال را مورد بررسی قرار خواهیم داد. یکی از دلایل به‌کارگیری امضاهای دیجیتالی که یک دلیل عادی به شمار می‌رود، ایجاد اعتبار برای امضاها در یک سامانه تبادل داده و اطلاعات است. در واقع، استفاده از امضای دیجیتال، سندیت و اعتبار ویژه‌ای به یک سند می‌بخشند. وقتی که هر فرد دارای یک کلید خصوصی در این سامانه است، با استفاده از آن می‌تواند سند را امضا کرده، به آن ارزش و اعتبار بدهد و سپس، آن را ارسال کند.

ویژگی‌های مهم امضای دیجیتال، عبارت‌اند از:

* در تولید آنها از اطلاعاتی که به طور منحصربه‌فرد در اختیار امضاکننده است، استفاده می‌شود؛

* به طور خودکار و توسط رایانه تولید می‌شوند؛

* امضای هر پیام، وابسته به کلیه بیت‌های پیام است و هرگونه دست‌کاری و تغییر در متن سند، موجب مخدوش شدن امضای پیام می‌گردد؛

* امضای هر سندی، متفاوت با امضای اسناد دیگر است؛

* باید به‌راحتی قابل بررسی و تأیید باشد تا از جعل و انکار احتمالی آن جلوگیری شود.

کاربرد امضای دیجیتال در دولت الکترونیکی

در مباحث مربوط به خدمات الکترونیکی، از جمله دولت الکترونیک، به‌جرئت می‌توان گفت بدون وجود زیرساخت‌های لازم امنیتی در فضای دیجیتال، امکان ارائه چنین خدماتی وجود ندارد؛ چراکه بدون حضور فناوری‌های لازم جهت اعتبار بخشیدن به اسناد الکترونیکی و قانونمند نمودن تراکنش‌ها و فعالیت‌های اینترنتی، نمی‌توان به فضای دیجیتالی اعتماد کرد و مسلماً افراد جامعه مایل به استفاده از آن نخواهند بود. در این زمینه، فناوری‌های خاصی مانند: امضای دیجیتال، گواهینامه دیجیتالی، مرکز صدور گواهینامه دیجیتال و مانند آن ایجاد شده است. این فناوری‌ها، نیازمندی‌های فنی لازم برای قابل اعتماد نمودن فضای دیجیتال را فراهم می‌آورند؛ اما در کنار این امکانات فنی، نیاز به قانون‌گذاری مناسب برای فضای دیجیتال احساس می‌شود. باید روال‌های قانونی برای طرح دعوی، روال پیگیری فعالیت‌های اینترنتی و امکاناتی مانند استناد و جلوگیری از جعل و غیرقابل انکار کردن فعالیت‌های اینترنتی، تدوین شود.

معایب امضای دیجیتال

با وجود تمام مزایایی که امضای دیجیتال دارد، ولی این طرح همچنان در حل برخی مشکلات ناتوان است. الگوریتم و قوانین مربوط به آن نیز نمی‌توانند تاریخ و زمان امضای یک سند را در ذیل آن درج کنند. از همین جهت، شخص دریافت‌کننده نمی‌تواند این اطمینان را حاصل کند که نامه واقعاً در چه تاریخ و زمانی به امضا رسیده است. ممکن است در محتویات سند تاریخی درج شده باشد و با تاریخی که شخص نامه را امضا کرده باشد، مطابقت نداشته باشد. البته برای حلّ این مشکل، می‌توان از یک راه حل با عنوان زمان اعتماد به مهر و امضا استفاده کرد. همان‌طورکه در ابتدای تعریف امضای دیجیتال اشاره شد، این طرح غیرقابل انکار است و ساختار امضای دیجیتال، بر همین اساس شکل گرفته است. چنان‌که می‌دانید، تکذیب در لغت، به معنای انکار هرگونه مسئولیت نسبت به یک فعالیت است. هنگامی که پیامی ارسال می‌شود و فرستنده آن را همراه امضا دریافت می‌کند، در واقع، این اطمینان در شخص دریافت‌کننده ایجاد می‌شود که نامه را چه کسی امضا کرده است و انکار امضا، کاری مشکل به نظر می‌رسد.

البته تا زمانی که کلید خصوصی به صورت مخفی باقی بماند، شخص فرستنده نمی‌تواند چنین ادعایی داشته باشد؛ ولی هنگامی که فایل امضای شخصی مورد حمله قرار بگیرد، نه تنها خود فایل امضا اعتبار لازم را از دست می‌دهد، بلکه استفاده از زمان اعتبار مهر و امضا نیز دیگر کاربردی نخواهد داشت.

یادآوری این نکته لازم است هنگامی که شما در سامانه خود از کلید عمومی بهره می‌گیرید، دیگر نمی‌توانید امضای خود را انکار کنید و در صورتی این موضوع امکان‌پذیر است که کل شبکه مورد حمله واقع شود و سامانه از اعتبار لازم ساقط شود. بنابراین، توجه به انتخاب یک راه حل درست برای پیاده‌سازی طرح امضای دیجیتال، از اهمیت ویژه‌ای برخوردار است و همان‌طورکه عنوان شد، ممکن است با یک مشکل، کل اعتبار مجموعه زیر سؤال برود. مطابق اصول فنی امضای دیجیتال، فایل امضای دیجیتال، رشته‌ای از بیت‌ها را در اجرای این طرح به کار می‌برد. در واقع، افراد در این طرح، مجموعه‌ای از بیت‌ها را که ترجمه پیام است، امضا می‌کنند.

مشکل دیگر امضای دیجیتال، این است که چون پیام توسط یک تابع مشخص به مجموعه‌ای از بیت‌ها ترجمه و پردازش می‌شود، ممکن است در طی مرحله انتقال و دریافت پیام، ترجمه پیام دچار خدشه شود و مفهوم دیگری به خود گیرد. برای حل این مشکل، از روشی با عنوان دبلیو وای اس آی دبلیو وای اس استفاده می‌شود؛ به این معنا که همان چیزی که مشاهده می‌شود، امضا می‌شود. در این روش، شخص همان اطلاعات ترجمه‌شده خود را بدون آنکه اطلاعات مخفی دیگری در آن قرار گیرد، امضا می‌کند و پس از امضا و تأیید اطلاعات از سوی شخص فرستنده درون سامانه به کار گرفته می‌شود. در واقع، این روش، ضمانت‌نامه محکمی برای امضای دیجیتال به شمار می‌رود و در سیستم‌های رایانه‌ای مدرن، قابلیت پیاده‌سازی و اجرا را خواهد داشت.

امضای دیجیتال و تأمین امنیت

امضای دیجیتال، امنیت موارد ذیل را تأمین می‌نماید:

* تصدیق هویت: تصدیق هویت، اطمینان از اینکه شخص یا طرفی که با آن در حال ارتباط هستیم، همان کسی است که ما انتظار داریم و خودش می‌گوید.

* محرمانه بودن: اطلاعات درون پیغام‌ها و یا تبادلات، محرمانه می‌شوند و تنها برای اشخاص دریافت‌کننده و ارسال‌کننده قابل فهم و خواندن می‌باشد.

قانون فناوری اطلاعات، امضای دیجیتالی را به عنوان وسیله احراز هویت و امنیت اسناد الکترونیکی می‌داند. امضای دیجیتال، یک نشانه الکترونیکی است که اتصال بین یک نهاد و یک رکورد داده را ایجاد می‌کند و به منظور اعتبارسنجی و تأیید اعتبار استاد الکترونیکی مورد استفاده قرار می‌گیرند و به فرایند گواهینامه صدور محتویات سند اشاره دارد؛ درحالی‌که احراز هویت، به فرایند گواهی فرستنده سند اشاره دارد

* امانت‌داری: اطلاعاتی که درون پیغام و یا تبادلات وجود دارد، در طول مسیر به طور اتفاقی یا عمدی، مورد دستبرد قرار نمی‌گیرند.

* غیرقابل انکار بودن: ارسال‌کننده نمی‌تواند منکر ارسال پیام یا تبادل مالی شود و دریافت‌کننده هم نمی‌تواند منکر دریافت آن شود.

حملاتِ ممکن علیه امضاهای دیجیتالی

*** حمله Key-only**

در این حمله، دشمن، تنها کلید عمومی امضاکننده را می‌داند و بنابراین، فقط توانایی بررسی صحت امضاهای پیام‌هایی را دارد که به وی داده شده‌اند.

*** حمله Known Signature**

دشمن، کلید عمومی امضاکننده را می‌داند و جفت‌های پیام/امضا را که به وسیله صاحب امضا انتخاب و تولید شده، دیده است. این

حمله، در عمل امکان‌پذیر است و بنابراین، هر روش امضایی باید در مقابل آن امن باشد.

*** حمله Chosen Message**

به دشمن اجازه داده می‌شود که از امضاکننده بخواهد که تعدادی از پیام‌های به انتخاب او را امضا کند. انتخاب این پیام‌ها ممکن است به امضاهای از قبل‌گرفته‌شده بستگی داشته باشد. این حمله در غالب حالات، ممکن است غیرعملی به نظر برسد؛ اما با پیروی از قانون احتیاط، روش امضایی که در برابر آن ایمن است، ترجیح داده می‌شود.

*** حمله Man-in-the-middle**

در این حمله، شخص از موقعیت استفاده کرده در هنگام مبادله کلید عمومی، کلید عمومی خود را جایگزین کرده، برای گیرنده می‌فرستد و بدین‌گونه، می‌تواند به پیام‌ها دسترسی داشته باشد؛ بدون اینکه فرستنده و گیرنده، مطلع باشند.

امروزه، امضا نشانه هویت یک فرد می‌باشد. کسی که یک نامه، رسید بانکی یا سندی را امضا می‌کند، در حقیقت، نشانه‌ای از خود باقی می‌گذارد که نمادِ هویت اوست. این نماد، به‌گونه‌ای می‌باشد که اگرچه همگان می‌توانند آن را بشناسند، اما کسی توان تولید آن را ندارد و منحصربه‌فرد می‌باشد. در دنیای الکترونیک و فناوری نیز موضوع تصدیق هویت، یکی از موضوعات مهم امنیتی است. ایده امضای دیجیتالی در جهان فناوری اطلاعات، همانند امضای واقعی، ابزاری مهم برای نیل به هدف تصدیق هویت و امنیت می‌باشد. روش‌ها مختلفی برای ایجاد امضای دیجیتال وجود دارد؛ اما آنچه مهم است، توجه به این نکته می‌باشد که امضای دیجیتال، موجب امنیت بیشتر در تبادل اطلاعات و از بین بردن محدودیت‌های رشد تجارت الکترونیک شده است.

گواهینامه دیجیتالی و مرکز گواهی امضای دیجیتال

گواهینامه دیجیتالی، سندی الکترونیکی است که هویت فرد را در فضای مجازی نشان می‌دهد و به‌نوعی، معادل شناسنامه یا کارت شناسایی وی است. در گواهینامه دیجیتالی که عموماً از استاندارد X.509 پیروی می‌کند، اطلاعاتی مانند: مشخصات فرد، کلید عمومی وی و امضای دیجیتالی صادرکننده این گواهینامه ثبت می‌شود. البته بنا به نوع کاربرد، داده‌های دیگری نیز در گواهینامه دیجیتالی وجود دارند. بدین وسیله و با در اختیار داشتن گواهینامه دیجیتالی یک فرد، می‌توان کلید عمومی معتبر وی را در اختیار داشت تا بتوان امضای دیجیتالی ارسالی از طرف او را اعتبارسنجی کرد.

اما برای صدور گواهینامه دیجیتالی، نیاز به مرکز صدور گواهینامه است که مانند سازمان ثبت احوال بوده و آن را به صورت مخفف CA می‌نامند. این مرکز، یک سازمان معتبر و مورد قبول همگان است که با دریافت مشخصات هویتی افراد و احراز اصالت آنها، کلید عمومی آنها را امضا می‌نماید و به عبارتی، گواهینامه دیجیتالی صادر می‌کند. مراکزCA از نیازمندی‌های اوّلیه و زیرساخت‌های لازم برای برقراری نظام امضای دیجیتال در فضای مجازی می‌باشند. این مراکز، معمولاً وابسته و تحت نظارت یک سازمان دولتی و یا جهانی هستند و اعتبار خاصی دارند.

همچنین، گواهینامه دیجیتالی آنها به صورت قابل اطمینان برای همه در دسترس است تا بتوان از آن برای بررسی صحت و اعتبار یک گواهینامه دیجیتالیِ صادرشده، استفاده کرد.

الگوریتم امضای دیجیتالی

یک طرح امضای دیجیتالی، معمولاً از سه الگوریتم تشکیل شده است:

۱. الگوریتم تولید کلید: یک الگوریتم که یک کلید خصوصی را به طور یکنواخت و به طور تصادفی، از مجموعه کلیدهای ممکن انتخاب می‌کند. خروجی‌های این الگوریتم، کلید خصوصی و کلید عمومی مطابق با آن مجموعه است.

۲. الگوریتم امضا: یک الگوریتم امضاکننده که با توجه به پیام و یک کلید خصوصی، یک امضا تولید می‌کند.

بدون حضور فناوری‌های لازم جهت اعتبار بخشیدن به اسناد الکترونیکی و قانونمند نمودن تراکنش‌ها و فعالیت‌های اینترنتی، نمی‌توان به فضای دیجیتالی اعتماد کرد و مسلماً افراد جامعه مایل به استفاده از آن نخواهند بود. در این زمینه، فناوری‌های خاصی مانند: امضای دیجیتال، گواهینامه دیجیتالی، مرکز صدور گواهینامه دیجیتال و مانند آن ایجاد شده است. این فناوری‌ها، نیازمندی‌های فنی لازم برای قابل اعتماد نمودن فضای دیجیتال را فراهم می‌آورند؛ اما در کنار این امکانات فنی، نیاز به قانون‌گذاری مناسب برای فضای دیجیتال احساس می‌شود

۳. الگوریتم صحت: یک الگوریتم تأییدیه امضا مبنی بر اینکه با توجه به پیام، کلید عمومی و امضا، ادعای پیام در مورد صحت را قبول یا رد می‌کند.

نتیجه

با توضیحاتی که درباره امضا دیجیتال ارائه شد، به نظر می‌رسد این روش می‌تواند نیاز مجموعه‌هایی را تأمین کند. نکته مهمی که بر آن تأکید شده است، انتخاب روش مناسب برای پیاده‌سازی این طرح و اجرای کامل و درست الگوریتم‌های مربوط به آن است که میزان اعتبار این طرح را تا حدود بسیاری افزایش می‌دهد. به‌طورخلاصه، برای ایجاد یک امضای دیجیتال، ابتدا امضاکننده باید از طریق کلید عمومی، امضای خود را رمزسازی نماید و سپس، آن را ضمیمه پیام داده‌ای سازد و برای مخاطب خویش ارسال نماید. مخاطب که اکنون پیام داده‌ای را به همراه امضای دیجیتال آن دریافت کرده، باید امضای رمزنگاری‌شده را که قابل فهم نیست، از داده پیام‌ها جداساخته و از طریق کلید عمومی ارسال‌کننده، پیام را برای وی ارسال کند تا خود ارسال‌کننده با کلید خصوصی‌اش، آن را رمزگشایی نماید. چنانچه نتایج یکسانی حاصل شد، یعنی همان چیزی که امضاکننده به عنوان امضای دیجیتال برای خود تعریف کرده بود هویدا گردد، معلوم می‌شود که اولاً امضای مذکور به نحو صحیحی از سوی امضاکننده ارسال شده و ثانیاً وی نمی‌تواند ادعا کند که پیام را امضا نکرده و یا اینکه پیام تغییر یافته است. بنابراین، به‌کارگیری امضای دیجیتال، شامل دو فرآیند است: مرحله اوّل، ایجاد امضا توسط ارسال‌کننده پیام توسط کلید خصوصی‌اش، و مرحله بعد نیز شامل فرآیند چک کردن امضای دیجیتال از طریق مراجعه به پیام اصلی و استفاده از کلید عمومی ارسال‌کننده می‌شود.■

منابع

1. en.wikipedia.org/wiki/EGovernment_in_Europe
2. en.wikipedia.org/wiki/Open_Government_in_Canada
3. fa.wikipedia.org
4. forum.boursekala.com
5. ictna.ir
6. mihanblockchain.com/hash-function/
7. persianv.com
8. us-cert.gov/ncas/tips/ST04-018
9. youdzone.com/signature.html