چالش ها در پیاده سازی امضای دیجیتال در فضای سایبری براساس فناوری اطلاعات رمزنگاری شده

آیدا نوبخت نمین

دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات گرایش کسب و کار الکترونیک، دانشگاه آزاد اسلامی واحد تهران مرکزی (نویسنده مسئول)

گلناز رسولی

دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات گرایش کسب و کار الکترونیک، دانشگاه آزاد اسلامی واحد تهران مرکزی

مریم فرشادی وفا

دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات گرایش کسب و کار الکترونیک، دانشگاه آزاد اسلامی واحد تهران مرکزی

محمدرضا خسروی

دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات گرایش کسب و کار الکترونیک، دانشگاه آزاد اسلامی واحد تهران مرکزی

چکیده:

امضای دیجیتال یک طرح بررسی شناسایی پیغام یک فرستنده به کمک عملیات ریاضی است که همانند امضای دستی میتواند به عنوان یک ابزار قوی برای شناسایی افراد و سازمانها مورد استفاده قرار گیرد. فرستنده ی پیغام، امضای دیجیتال را که به کمک تابع درهم سازی و تابع رمزنگاری از متن پیغام به دست میآید، به پیام خود ضمیمه میکند. بر خلاف امضای دستی، امضای دیجیتال با پیامهای مختلف تغییر میکند. امضای دیجیتال تضمین میکند که محتوای پیغام مورد تأیید فرستنده است و توسط شخص دیگری تغییر نکرده است.

در مقاله حاضر به بررسی موضوع چالش ها در پیاده سازی امضای دیجیتال در فضای سایبری براساس فناوری اطلاعات رمزنگاری شده پرداخته شده است. درحال حاضر با گسترش استفاده از امضای الکترونیکی، میتوان از امضای دیجیتال، به عنوان جایگزین امضای دستی استفاده کرد. امضای دیجیتال نوعی امضای الکترونیکی است که شامل یک رشته کدهای ریاضی مختص شخص معین است. با این حال هنوز ضعف های امنیتی وجود دارد که استفاده از امضای دیجیتال را تحت شعاع قرار میدهد .در بسیاری از رهنمون ها و دستورالعمل های امضای الکترونیکی، الزاماتی برای امضای الکترونیکی پیشرفته که همان امضای دیجیتال است، بیان شده است. در این مقاله سعی شده است با بررسی و بهبود این الزامات گامی در جهت بهبود امنیت امضای دیجیتال برداشته شود.

واژگان کلیدی: امضای دیجیتال، فضای سایبری، فناوری اطلاعات، رمزنگاری، تحول دیجیتال

بیان مسئله:

امضای دیجیتال، نوعی رمزنگاری نامتقارن است. هنگامی که پیغامی از کانالی ناامن ارسال می‌شود، یک امضای دیجیتال که به شکل صحیح پیاده‌سازی شده باشد، می‌تواند برای شخص گیرنده پیام، دلیلی باشد تا ادعای شخص فرستنده را باور کند یا به عبارت بهتر، شخص گیرنده از طریق امضای دیجیتال می‌تواند این اطمینان را حاصل کند که همان شخص فرستنده، نامه را امضا کرده‌است و نامه جعلی نیست. امضاهای دیجیتال در بسیاری از جنبه‌ها مشابه امضاهای سنتی دستی هستند؛ جعل‌کردن امضاهای دیجیتال به شکل صحیح بسیار مشکلتر از یک امضای دستی است. طرح فایل امضای دیجیتال بر مبنای رمزنگاری نامتقارن هستند و می‌بایست به شکل صحیح صورت گیرد تا مؤثر واقع شود. همچنین امضاهای دیجیتال می‌توانند امضاهایی غیرقابل انکار را ایجاد کنند به این معنی که شخص امضاکننده نمی‌تواند تا زمانی که کلید شخصی فرد به صورت مخفی باقی‌مانده‌است، ادعا کند که من این نامه که امضای من را به همراه دارد، را امضا نکرده‌ام؛ ولی در زمانی که کلید شخصی فرد در شبکه افشا گردد، شخص می‌تواند امضای دیجیتال خود را انکار کند هرچند که با اضافه کردن مهر زمانی، امضا معتبر مانده و این مشکل حل می‌گردد. این پیام‌های امضا شده می‌توانند هرچیزی که قابل نمایش به رشته بیتی است، باشد، مانندپست الکترونیک، قراردادها یا پیام‌هایی که از طریق قواعد رمزنگاری‌های دیگر ارسال شده باشند . درواقع امضای دیجیتال مکانیزمی است که به یک پیام در فضای تبادل اطلاعات اعتبار می بخشد(مرادی،۱۴۰۱).امضای دیجیتال امنیت تصدیق هویت، محرمانه بودن، امانتداری و غیرقابل انکار بودن را تأمین می‌کند و از اطلاعات محرمانه در مقابل هرگونه تغییر غیرمجاز محافظت می نماید؛ بنابراین این امضای دیجیتال از دستکاری و خدشه دار کردن اطلاعات جلوگیری می‌کند. این امضای دیجیتال برای هر شخصی منحصر به فرد می باشد. بزرگترین تفاوت امضاهای دستی با امضاهای دیجیتال در آن است که امضاهای دستی ثابت اند و شکل آنها نباید تغییر کند در حالی که امضاهای دیجیتالی ماهیتاً وابسته به پیام اند و به ازای هر پیام تغییر می‌کنند.درواقع امضای دیجیتال یک فرایند رمزنگاری نامتقارن می‌باشد که نوعی مکانیزه امنیتی است که به دو کلید خصوصی و عمومی وابسته است که از این کلیدها برای رمزگذاری پیام در زمان انتقال پیغام و رمزگشایی هنگام دریافت پیام استفاده می نمایند امضای دیجیتال با به کارگیری یک الگوریتم ریاضی، که از دید کاربر پنهان است، موارد زیر را در مورد یک پیام تضمین می کند : تمامیت (دستکاری نشدن) پیام: گیرنده یک پیام باید اطمینان داشته باشد که پیام بدون هیچ تغییری، توسط فرستنده ارسال شده است.احراز هویت دیجیتال: هر فرد همان کسی است که ادعا می کند. هر پیام واقعاً توسط کسی ارسال شده است که ادعا می شود فرستنده پیام است.انکارناپذیری: کسی که پیامی را ارسال کرده یا صحت پیامی را تایید کرده است، در آینده نتواند ارسال کردن یا تایید کردن پیام را انکار کند. امضاهای دیجیتال اغلب برای به انجام رساندن امضاهای الکترونیکی به کار می‌روند. در تعدادی از کشورها، مانند آمریکا و کشورهای اتحادیه اروپا، امضاهای الکترونیکی قوانین مخصوص به خود را دارند. هرچند، قوانین درباره امضاهای الکترونیکی همواره روشن نمی‌سازند که آیا امضاهای دیجیتال به درستی به کار گرفته شده‌اند یا اهمیت آن‌ها به چه میزان است. در حالت کلی قوانین به شکل واضح در اختیار کاربران قرار نمی‌گیرد و گاهی آنان را به گمراهی می‌کشاند .از طریق امضای دیجیتال، دسترسی افراد به حساب هایشان کنترل می شود؛ افراد می توانند اسناد الکترونیکی را امضای دیجیتالی کنند؛ برداشت از حساب و انتقال پول با تایید صاحبان حساب خواهد بود؛ و بسیاری کاربردهای دیگر. در همه این ها، هم کاربر و هم موجودیتی که به کاربر خدمات ارائه می دهد نسبت به امن بودن فعالیت خود اطمینان می یابند. بنابراین، نه دسترسی های غیرمجاز، امنیت کاربر را تهدید می کند و نه کاربر می تواند عملیاتی را که انجام داده است، انکار نماید . با داشتن امضای دیجیتال در صورتی که خواسته شود در فضای اینترنت، مبادله الکترونیکی با هویت مجازی داشته باشد، می‌تواند خود را به گونه ای معرفی کند که طرف مقابل به اعتماد کند و گیرنده می تواند از ماهیت فرستنده و اینکه اطلاعات حین انتقال تغییر پیدا نکرده مطمئن باشد . به عبارت دیگر می توان گفت به کارگیری گواهی الکترونیکی امضای دیجیتال در سامانه ها، امضای دیجیتال اسناد و تراکنش های الکترونیکی مزایای زیر را به همراه دارد : احراز هویت دیجیتال: اطمینان از این که پیام دریافتی واقعا از منبع مورد انتظار باشد، یعنی اصالت فرستنده و پیام برای گیرنده احراز شود . محرمانگی: گیرنده می تواند مطمئن باشد که افراد غیر مجاز نمی توانند به محتوای داده دست پیدا کنند . تمامیت: اطمینان از این که در متن ارسالی هیچ گونه تغییری رخ نداده است . انکارناپذیری : فرستنده نمی تواند امضای دیجیتال خود را انکار نماید یکی از دلایل به‌کارگیری امضاهای دیجیتالی که یک دلیل عادی به‌شمار 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 و به آن ارزش و اعتبار داده و سپس آن را ارسال کند. اهمیت ایجاد اطمینان قطعی و محکم برای شخص دریافت‌کننده پیام درباره صحت ادعای فرستنده در برخی از انواع انتقال اطلاعات مانند داده‌های مالی به خوبی خود را نشان می‌دهد و اهمیت وجود امضای دیجیتال درست را بیش از پیش به نمایش می‌گذارد. به عنوان مثال شعبه‌ای از یک بانک قصد دارد دستوری را به دفتر مرکزی بانک به منظور درخواست ایجاد تعادل در حساب‌های خود را ارسال کند. اگر شخص دریافت‌کننده در دفتر مرکزی متقاعد نشود که این پیام، یک پیام صادقانه است و از سوی یک منبع مجاز ارسال شده‌است طبق درخواست عمل نکرده و در نتیجه مشکلاتی را به وجود می‌آورد.(نریسو[1]،۲۰۲۳) در موارد بسیار زیادی، فرستنده و گیرنده پیام نیاز دارند این اطمینان را به دست بیاورند که پیام در مدت ارسال بدون تغییر باقی‌مانده‌است. هرچند رمزنگاری محتوای پیام را مخفی می‌کند ولی ممکن است امضا در یک سامانه از اعتبار ساقط شود و محتویات یک پیام دست‌خوش تغییرات گردد؛ ولی استفاده از امضای دیجیتال به عنوان روشی از رمز نگاری می‌تواند ضامن درستی و بی نقصی یک پیام در طی عملیات انتقال اطلاعات باشد زیرا همان‌طور که در ساختار اجرایی شدن الگوریتم مشاهده کردید از تابع درهم‌سازی بهره گرفته شده‌است و همین نکته ضمانت بهتری را برای درستی و صحت یک پیام ایجاد می‌نماید .رمزنگاری با استفاده از کلید عمومی روشی است برای ایجاد یک ارتباط پنهان میان دو شخص بدون اینکه نیازی به تعویض کلیدهای خصوصی باشد. همچنین با استفاده از این روش می‌توان امضاهای دیجیتال را ایجاد کرد.

ادبیات موضوع:

امضای دیجیتال یک طرح بررسی شناسایی پیغام یک فرستنده به کمک عملیات ریاضی است که همانند امضای دستی میتواند به عنوان یک ابزار قوی برای شناسایی افراد و سازمانها مورد استفاده قرار گیرد. فرستنده ی پیغام، امضای دیجیتال را که به کمک تابع درهم سازی و تابع رمزنگاری از متن پیغام به دست میآید، به پیام خود ضمیمه میکند. بر خلاف امضای دستی، امضای دیجیتال با پیامهای مختلف تغییر میکند. امضای دیجیتال تضمین میکند که محتوای پیغام مورد تأیید فرستنده است و توسط شخص دیگری تغییر نکرده است(دریس[2]،۲۰۲۳)

خواص و مزایای امضای دیجیتال

از جمله ویژگیها و مزایایی که میتوان در مورد امضای دیجیتال مطرح کرد به شرح زیر است:

در تولید آنها از اطلاعاتی که به طور منحصربه فرد 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.

به راحتی قابل بررسی و تأیید میباشد که باعث میشود از جعل و انکار احتمالی آن جلوگیری شود

امضای دیجیتال احراز هویت منبع پیام را تضمین میکند

امضای دیجیتال از محتوای داده ها در طول جریان داده محافظت میکند.

از سرقت اطلاعات و تغییر دادن آن توسط اشخاص دیگر جلوگیری میکند. همچنین تضمین میکند اطلاعات ارسال شده توسط گیرنده به درستی دریافت شده است

[1] Neriso
[2] Deris

صرفه جویی در مصرف کاغذ، پست، هزینه های مطبوعاتی و سرعت را فراهم میکند(جیسون[3]،۲۰۲۳)

نحوی ایجاد و تأیید امضای دیجیتال

به طور خلاصه فرآیند امضا را میتوان در دو بخش قرار داد؛ بخش اول ایجاد امضای دیجیتال و ارسال پیام به همراه امضاء است که توسط فرستنده‌ی پیام انجام میشود. بخش دوم بازبینی پیام و امضاء برای تأیید آن است که توسط گیرندهی پیام انجام میشود. در بخش اول فرد امضاکننده به کمک تابع درهم سازی، چکیده ی پیام خود را محاسبه میکند که برای هر پیام، مقدار به دست آمده از تابع درهم سازی مقدار یکتایی است. در مرحله‌ی بعد فرستنده می بایست چکیده ی به دست آمده از پیام را به شکل رمز شده در آورد. از الگوریتم رمزنگاری نامتقارن برای ایجاد رمز از پیام استفاده میشود الگوریتم رمزنگاری نامتقارن دارای سه بخش برای تولید کلید، ایجاد رمز و رمزگشایی است. امضاء کننده به کمک الگوریتم تولید کلید، دو کلید عمومی و خصوصی را به دست می آورد.کلید خصوصی کاملا محرمانه است و نزد فرستنده نگهداری میشود و کلید عمومی باید در دسترس افرادی که امضا را دریافت میکنند، قرار گیرد چکیده با استفاده از کلید خصوصی و یک الگوریتم رمزنگاری نامتقارن به یک عبارت رمزی تبدیل میشود. رمز به دست آمده در این مرحله همان امضای دیجیتال است که به همراه پیام و کلید عمومی به گیرنده ی پیام ارسال میشود در بخش دوم از فرآیند امضا فردی که امضا را دریافت کرده است ابتدا مقدار درهم سازی پیام دریافتی را به کمک تابع درهم سازی که فرستنده استفاده کرده است، به دست میآورد. در مرحلهی بعد، امضای دیجیتال که یک عبارت رمزی است را به کمک کلید عمومی و الگوریتم رمزگشایی به چکیده ی پیام تبدیل میکند. چکید های که از رمزگشایی به دست میآید با چکیده ی تابع درهم سازی مقایسه میشود و درصورتیکه این دو مقدار برابر باشند، امضا و پیام صحیح و مورد تأیید است .درصورتی که پیام یا امضا توسط فرد دیگری تغییر کرده باشد، مقدار چکیده ی به دست آمده یکسان نخواهد بود زیرا مقدار درهم سازی برای هر پیام منحصربه فرد است(دیوید[4]،۲۰۲۳)

تهدیدات و خطرات

شش تهدید که امضای دیجیتال را بیشتر تهدید میکند به شرح زیر است:(راستین،۱۴۰۱)

- سرقت توکن و کلمه عبور

در حالت خوشبینانه، فرض بر این است که مالک میتواند با خیال راحت کارت رمزنگاری و کلید امضای خود را به صورت مخفی نگه دارد؛ اما در دنیای واقعی اینطور نیست. مالک مسئولیت قانونی در مورداستفاده مخرب توسط شخص ثالث دارد. برای دسترسی به کارت ارائه یک PIN لازم است واز طرفی چون تعداد شماره های PIN و کلمات عبور به سرعت در حال رشد است، نمیتوان انتظار داشت که مالک یک سند مکتوب در مورد PIN های خود به خاطر داشته باشد. حتی اگر این مورد هم نباشد، مهاجم میتواند کارت مالک را دقیقاً یکبار استفاده کند، به عنوان مثال زمانی که مالک دور از دفترش است و برخی دستگاه ها، سوابق تلاش برای فعالسازی دستگاه ایجاد امضا را در حافظه غیر فرار خود ذخیره کرده اند بنابرین در این تهدید همانطور که بیان شده است با فرض دانستن PIN به هر روشی، سرقت توکن و کلمه عبور باهم رخ می دهد.

- اعداد تصادفی ضعیف

بسیاری از الگوریتم های امضا از پارامترهای تصادفی برای ایجاد امضا استفاده میکنند. مشکل این است که درصورتیکه اعداد تصادفی ضعیف باشد ممکن است کلید امضای مخفی فاش بشود. هیچ مکانیزمی که نشان دهد که randomness ضعیف یا خوب است، وجود ندارد. در بسیاری از طرحهای امضا، ایجاد یک امضا، شامل انتخاب یک پارامتر تصادفی است. طرح های رمزنگاری بیان می کند که این پارامترهای

[3] Jayson
[4] David

تصادفی به طور یکنواخت (احتمال یکسان) از فضای داده شده و همچنین به صورت تصادفی انتخاب میشوند. مشاهده شده است که اگر این الزامات یعنی انتخاب عدد تصادفی انجام نشود ممکن است منجر به فروپاشی کامل ویژگیهای امنیتی شود. از سوی دیگر هیچ روش قابل اعتمادی که بتواند ثابت کند که خروجی مولد عدد تصادفی یکنواختی را برآورده میکند، وجود ندارد. آنچه که میتوان انجام داد این است حذف ژنراتورهای ضعیف که خروجی آنها به طور آشکارا خواص آماری که همان توزیع با احتمال یکنواخت است را نقض میکند از این لحاظ وجود اعدادتصادفی ضعیف تهدید محسوب می شود که مهاجم می تواند با دانستن الگوریتم تولید کلید و همچنین ضعیف بودن اعداد تصادفی با تولید کلیدهای خصوصی متعدد در نهایت به کلید خصوصی که با کلید عمومی هدف حمله مطابقت دارد، دسترسی پیدا کند

- تبانی ارائه دهنده گواهی

ارائه دهنده خدمات صدور گواهینامه نه تنها مسائل گواهی با کیفیت، بلکه مجاز است کلید امضای مخفی (داده ایجاد امضا) را برای مشتریان خود ایجاد میکند. در این موارد نگهداری یک کپی از کلیدهای مخفی و یا داده ای که میتواند برای بازسازی کلیدها استفاده شود، ممنوع است. با این حال، اجرای این مورد تنها برای اعمال قانون کیفری است. هیچ مکانیزمی فنی که تضمین کند ارائه دهنده خدمات کلیدها را نگهداری نمیکند، وجود ندارد و ممکن است کلیدها را با یک روش کاملا غیرحرفه ای ذخیره کند بدیهی است که منظور از تبانی ارائه دهنده، تبانی وی با مهاجم که قصد سوء استفاده از هویت فرد خاصی را دارد، می باشد.

- حمله ی Kleptography

به غیر از randomness ضعیف که باعث فاش شدن کلید امضای مخفی میشود، کد kleptography هم ممکن است در دستگاه درج شده باشد. حمله kleptography حمله ایست که با استفاده از رمزنگاری نامتقارن یک در پشتی یا رخنه رمزنگاری را پیاد هسازی میکند .به عنوان مثال، یک حمله میتواند به صورت ماهرانه نحوی تولید جفت کلید عمومی و خصوصی توسط سیستم رمزنگاری را تغییر دهد به طوری که کلید خصوصی را میتوان از کلید عمومی با استفاده از کلید خصوصی مهاجم به دست آورد

- استانداردها و الزامات فنی مبهم

تمایل به ارزیابی کیفیت محصولات مورد استفاده برای اهداف رمزنگاری بر اساس انجام استانداردهای فنی وجود دارد. استانداردهای فنی بسیاری عوامل خطر را تحت کنترل حفظ میکنند به ویژه هنگامی که طراحان تخصص محدودی دارند. هر استاندارد باید روی مجموعه ای از مسائل که محصول را عمل پذیر و قابل مقایسه میکند، تمرکز کند. استفاده از استانداردهای فنی لزوماً موجب تضمین امنیت نیست، به طوری که اتفاق افتاده که درهمان روز انتشار استاندارد امنیتی، استاندارد شامل نقص امنیتی جدی بوده است یکی از مواردی که موجب می شود این مورد تهدید محسوب گردد به عنوان مثال استاندارد معیار مشترک که برای ارزیابی محصولات رمزنگاری استفاده می شود است. این استاندارد درتوانایی کاربرد روش های ارزیابی طیف وسیعی از ویژگی های امنیتی در گستره ی محصولات فناوری اطلاعات انعطاف پذیر است، بنابرین اگر از این انعطاف پذیری به درستی استفاده نگردد برای مثال از این استاندارد در رابطه با روش های ارزیابی نامناسب، خواص امنیتی بی ربط یا محصولات فناوری اطلاعات نامناسب استفاده شود منجر به نتایج ارزیابی بی معنی و یا حتی گمراه کننده می گردد بنابراین باید متن استاندارد صریحا اینگونه موارد را ذکر کند مشکلاتی از این دست در استاندارد FIPS هم که استانداردی برای ارزیابی محصولات رمزنگاری می باشد، وجود دارد.

- عدم سلامت روحی و روانی و اجبار

امضاکننده در عدم سلامت روحی و روانی عمل امضا را انجام دهد و یا به اجبار این عمل را انجام دهد

فناوری اطلاعات رمزنگاری شده

عناصر مهمی که در رمزنگاری مورد استفاده قرار می گیرند، به شرح زیر هستند:(شفیعی،۱۴۰۱)

تعریف ۱: متن آشکار پیام و اطلاعات را در حالت اصلی و قبل از تبدیل شدن به حالت رمز، متن آشکار یا به طور اختصار پیام مینامند در این حالت اطلاعات بطور کامل برای همه قابل فهم است

تعریف ۲: متن رمز به پیام و اطلاعات بعد از تبدیل شدن به حالت رمز، متن رمز گفته میشود اطلاعات رمز شده توسط افراد قابل فهم نیست

تعریف ۳: رمزگذاری و رمزگذاری یا رمز کردن عملیاتی است که با استفاده از کلید رمز، متن آشکار را به رمز تبدیل میکند

تعریف ۴: رمزگشایی ۲ رمزگشایی عملیاتی است که با استفاده از کلید رمز، پیام رمزشده را به پیام اصلی باز میگرداند. از نظر ریاضی این الگوریتم عکس الگوریتم رمزگذاری است

تعریف ۵:کلید رمز کلید رمز اطلاعاتی معمولاً عددی و یا رشته ای از حروف الفبا است که به عنوان پارامتر ورودی به الگوریتم رمز داده میشود و عملیات رمزگذاری و رمزگشایی با استفاده از آن انجام میگیرد. معمولاً طول کلید بر زمان عملیات رمزنگاری و ضریب اطمینان عملیات تأثیرگذار می باشد. انواع مختلفی از کلیدها در رمزنگاری تعریف و استفاده میشود.

سرویس رمزنگاری

به طور کلی سرویس رمزنگاری به قابلیت و امکانی اطلاق میشود که بر اساس فنون رمزنگاری حاصل می گردد. قبل از ورود رایانه ها به حوزه ی رمزنگاری تقریباً کاربرد رمزنگاری محدود به رمزکردن پیام و پنهان کردن مفاد آن بوده است. اما در رمزنگاری پیشرفته سرویسهای مختلفی از جمله موارد زیر ارائه گردیده است:

- حفظ محرمانگی یا امنیت محتوا : ارسال یا ذخیره اطلاعات به نحوی که تنها افراد مجاز بتوانند از محتوای آن مطلع شوند که همان سرویس اصلی و اولیه ی پنهان کردن مفاد پیام است.

- حفظ صحت داده یا سلامت محتوا به معنای ایجاد اطمینان از صحت اطلاعات و عدم تغییر محتوای اولیه ی آن در حین ارسال است تغییر محتوای اولیه ی اطلاعات ممکن است به صورت اتفاقی در اثر مشکلات مسیر (ارسال و یا به صورت عمدی باشد.

- احراز هویت یا اصالت سنجی محتوا به معنای تشخیص و ایجاد اطمینان از هویت ارسال کننده ی اطلاعات و عدم امکان جعل هویت افراد میباشد.

- عدم انکار : به این معنی است که ارسال کننده ی اطلاعات نتواند در آینده ارسال آن را انکار یا مفاد آن را تکذیب نماید.

چهار مورد فوق سرویسهای اصلی رمزنگاری تلقی میشوند و دیگر اهداف و سرویسهای رمزنگاری، با ترکیب این چهار مورد قابل حصول میباشند این سرویسها مفاهیم جامعی هستند و میتوانند برای کاربردهای مختلف پیاده سازی و اجرا شوند. به عنوان مثال سرویس اصالت سنجی محتوا هم در معاملات تجاری اهمیت دارد و هم در مسائل نظامی و سیاسی مورد استفاده قرار می گیرد. برای ارائه کردن هر یک از سرویسهای رمزنگاری بسته به نوع کاربرد از پروتکلهای مختلف رمزنگاری استفاده می شود(مرادی،۱۴۰۰)

پروتکل رمزنگاری

یک پروتکل رمزنگاری مجموعه ای از قواعد و روابط ریاضی است که چگونگی ترکیب کردن الگوریتم های رمزنگاری و استفاده از آنها را به منظور ارائه ی یک . سرویس رمزنگاری خاص در یک کاربرد خاص، فراهم میسازد. معمولاً یک پروتکل رمزنگاری مشخص میکند که:

- اطلاعات موجود در چه قالبی باید قرار گیرند.

- چه روشی برای تبدیل اطلاعات به عناصر ریاضی باید اجرا شود.

- کدامیک از الگوریتم های رمزنگاری و با کدام پارامترها باید مورد استفاده قرار گیرند.

- روابط ریاضی چگونه به اطلاعات عددی اعمال شوند.

- چه اطلاعاتی باید بین طرف فرستنده و گیرنده ردو بدل شود.

- چه مکانسیم ارتباطی برای انتقال اطلاعات مورد نیاز است.

به عنوان مثال میتوان به پروتکل تبادل دیفی هلمن برای ایجاد و تبادل کلید رمز مشترک بین دو طرف اشاره نمود (صابری،۱۴۰۱)

الگوریتم رمزنگاری

الگوریتم رمزنگاری به هر الگوریتم یا تابع ریاضی گفته میشود که به علت دارا بودن خواص مورد نیاز در رمزنگاری در پروتکل رمزنگاری مورد استفاده قرار گیرد. اصطلاح الگوریتم رمزنگاری یک مفهوم جامع است و لازم نیست هر الگوریتم از این دسته به طور مستقیم برای رمزگذاری اطلاعات در مورد استفاده قرار گیرد، بلکه صرفاً وجود کاربرد مربوط به رمزنگاری مدنظر است. گذشته سازمانها و شرکتهایی که نیاز به رمزگذاری یا سرویسهای دیگر رمزنگاری داشتند، الگوریتم های رمزنگاری منحصر بفردی را طراحی مینمودند به مرور زمان مشخص گردید که گاهی ضعف های امنیتی بزرگی در این الگوریتمها وجود دارد که موجب سهولت شکسته شدن رمز میشود. به همین دلیل امروزه رمزنگاری مبتنی بر پنهان نگه داشتن الگوریتم رمزنگاری منسوخ شده است و در روشهای جدید رمزنگاری فرض بر این است که اطلاعات کامل الگوریتم رمزنگاری منتشر شده است و آنچه پنهان است فقط کلید رمز است. بنابراین تمام امنیت حاصل شده از الگوریتم ها و پروتکلهای رمزنگاری استاندارد متکی به امنیت و پنهان ماندن کلید رمز است و جزئیات کامل این الگوریتم ها و پروتکل ها برای عموم منتشر می گردد. تاکنون روشهای بسیاری برای فرآیند رمزنگاری پیشنهاد و اجرا شده است، این روشها را میتوان با توجه به نوع کلیدی که در آنها بکار میرود به دو دسته ی کلی رمزنگاری متقارن و رمزنگاری نامتقارن تقسیم بندی نمود(جرمین[5]،۲۰۲۳)

رمزنگاری کلید متقارن

رمزنگاری کلید متقارن یا تک کلیدی به آن دسته از الگوریتم ها و سیستمهای رمزنگاری گفته میشود که در آن هر دو طرف ردوبدل اطلاعات از یک کلید رمز یکسان برای رمزگذاری و رمزگشایی استفاده می کنند. در این نوع رمزنگاری باید یک کلید رمز مشترک بین دو طرف تعریف گردد. چون کلید باید کاملاً محرمانه باقی بماند برای ایجاد و رد وبدل کلید مشترک باید از کانالی امن استفاده نمود و یا از روشهای رمزنگاری نامتقارن استفاده کرد. واضح است که در این روشها رمزگذاری و رمزگشایی اطلاعات دو فرآیند معکوس یکدیگر هستند. نیاز به وجود یک کلید رمز به ازای هر دو نفر درگیر در رمزنگاری ،متقارن موجب بروز مشکلاتی در مدیریت کلید رمز میگردد(فیلیک[6]،۲۰۲۳)

رمزنگاری کلید نامتقارن

این روش رمزنگاری در ابتدا با هدف حل مشکل انتقال کلید در روش متقارن و در قالب پروتکل تبادل کلید دیفی- هلمن پیشنهاد شد. در این روش برخلاف روش متقارن، کلید رمزگذاری با کلید رمزگشایی یکسان نیست و به جای یک کلید مشترک از یک زوج کلید به نامهای کلید عمومی و کلید خصوصی استفاده میشود کلید عمومی برای رمزگذاری استفاده میشود و متن رمز شده توسط کلید خصوصی قابل رمزگشایی است. کلید خصوصی تنها در اختیار دارنده ی آن قرار دارد و امنیت رمزنگاری به محرمانه بودن کلید خصوصی بستگی دارد و کلید

[5] Jernin
[6] Filik

عمومی در اختیار کلیه ی کسانی که با دارنده ی آن در ارتباط هستند قرار داده می شود. دو کلید عمومی و خصوصی با یکدیگر متفاوت هستند و با استفاده از روابط خاص ریاضی محاسبه می گردند. رابطه ریاضی بین دو کلید به گونه ای است که کشف کلید خصوصی با در اختیار داشتن کلید عمومی، عملاً ناممکن است. صندوق پستی مثال ساده ای از این نوع رمزنگاری است. به مرور زمان به غیر از حل مشکل انتقال کلید در روش متقارن کاربردهای متعددی برای این نوع رمزنگاری مطرح گردیده است. اگر از کلید خصوصی برای رمزگذاری و از کلید عمومی برای رمزگشایی استفاده شود به الگوریتمی میرسیم که به امضای دیجیتالی معروف است(دیوید[7]،۲۰۲۱)

مطالعات صورت گرفته:

مطالعات داخلی:

نظری و همکاران(۱۴۰۱)در تحقیقی به بررسی تحلیل امنیتی جعل هویت در الگوریتمهای امضای دیجیتال به کار رفته در شبکه ای موردی بین خودرویی پرداختند در این پژوهش دو نسخه موجود از پروتکل NERA را بررسی شد و نشان داد نسخه بهبودیافته این پروتکل نیز دارای آسیب پذیری جدی است و مهاجم میتواند با استفاده از حمله مرد میانی امضای جعلی تولید کند و خود را به جای وسایل نقلیه دیگر جا بزند

رامینی و همکاران(۱۴۰۱)در تحقیقی به بررسی ارائه یک روش رمزنگاری بلوکی جهت استفاده در پروتکلهای امنیتی شبکه های بیسیم پرداختند در این تحقیق یک الگوریتم رمزنگاری امن بر پایه عملگرهای جبری پیما نهای جهت بالا بردن امنیت در مقابله حمله های بدخواهانه که الگوریتم AES در مقابل آن آسیب پذیر است، ارائه میشود که علاوه بر بالا بردن امنیت، سرعت را کاهش نداده و بدلیل نداشتن جداول Box-S الگوریتم های پیشین استفاده شده در پروتکلهای شبکه های بیسیم، حافظه را نیز بهبود میبخشد

دارابی و همکاران(۱۴۰۱)در تحقیقی به بررسی پیاده سازی سخت افزاری پردازشگر رمزنگار مبتنی بر الگوریتم استاندارد رمزنگاری پیشرفته پرداختند در طول تاریخ، رمزنگاری اطلاعات یکی از مهمترین مباحث علوم ریاضی بوده است. الگوریتم های رمزنگاری، همه با یک هدف مشترک طراحی شدهاند. تمامی این الگوریتم ها با هدف خصوصی ساز ی اطلاعات طراحی شده اند. الگیوریتم رمزنگیاری AES یکیی از متداول ترین الگوریتم های رمزنگاری استاندارد است. در پیاده سازی سخت افزاری، کاهش هزینه های تولید، افزایش توان عملیاتی و کاهش توان مصرفی، اهمیت بسیاری دارد .

منوچهری و همکاران(۱۴۰۱)در تحقیقی به بررسی ارزیابی و بهبود الزامات امضای دیجیتال پرداختند جهت بررسی این الزامات پرسشنامه ای تدوین شد که میزان آسیب پذیری هر یک از این الزامات را با توجه به آسیب ها و تهدیدات موجود در محیط های با تقسیم بندی پیشنهادی که شامل محیط معمولیPC ، ترمینال امن(مانند دفاتر دولت الکترونیکی) ترمینال و محیط امن (مانند ترمینال دفاتر الکترونیکی که شخص تایید هویت شده و سایر امکانات حافظتی نیز موجود است) و دفاتر اسناد رسمی می باشد، می سنجد. این تقسیم بندی محیط ها، پیشنهاد این پژوهش برای شرایط مختلف امضای دیجیتال می باشد.

مرادی و همکاران (۱۴۰۱)در تحقیقی به بررسی تحلیل امنیت و بهبود امضای دیجیتال وکالتی پرداختند با توجه به نتایج از آنجایی که، سیستمهای رمزنگاری بر پایه ی منحنی بیضوی بسیار کاراتر از سیستمهای رمزنگاری سپس، روش امضای وکالتی پیشنهادی در این تحقیق را تشریح کرده، و امن بودن و کارایی آن را ارزیابی بر پایه ی مسأله ی فاکتورگیری صحیح و مسأله ی لگاریتم گسسته میباشند. روش پیشنهادی در مقایسه با دیگر روشهای امضای دیجیتال وکالتی، از سرعت بالاتری برخوردار بوده و میتوان از آن در کاربردهای مختلف استفاده کرد. استفاده در نقل و انتقالات الکترونیکی و محیط هایی که از عاملهای سیار استفاده میکنند، از جمله کاربردهای آن می باشد.

[7] David

سلطان زاده و همکاران(۱۴۰۰)در تحقیقی به بررسی بهبود مکانیزم های پشتیبانی از کنترل انحصاری امضاکننده نسبت به داده امضا در امضای دیجیتال پرداختند هدف این پژوهش بهبود سطح کنترل انحصاری امضاکننده و اندازهگیری کمی آن است. در این راستا به مقوله کنترل دستگاهها و تجهیزات رمزنگاری پرداخته و مکانیزمهای تاثیرگذار در ایجاد و حفظ کنترل انحصاری بررسی و بهبود بخشیده شده اند. در ادامه مجموعه عوامل و شرایط عمل امضای دیجیتال، مورد بررسی قرار گرفته و با ترکیب مکانیزمهای موجود، مکانیزمی ارائه، که عوامل تاثیرگذار بیشتری را پوشش دهد. در نهایت نیز چارچوبی جهت ارزیابی سطح کنترل انحصاری با در نظرگرفتن جنبه های مختلف، شامل اعتماد به طرفهای موجود و ذینفعان، انتقال واگذاری اختیارات امضا به دیگری، تضمین امنیت تجهیزات و کنترل کاربرد ارائه شده است. در چنین چارچوبی با توجه به وزن دهی جنبه های فوق الذکر و تعیین سطح هر یک از آنها، کمیت کنترل انحصاری برای هر امضا قابل اندازه گیری میگردد. در این رابطه، جنبه های مورد نظر در یکی از زیرساختهای کلید عمومی موجود در کشور، وزن گذاری شده و میزان سطح کنترل امضاهای تولید شده به صورت کمی محاسبه شده است

نظری و همکاران(۱۳۹۹)در تحقیقی به بررسی بلاک چین و امضاهای دیجیتال پرداختند بلاک چین در دنیای امروز اهمیت زیادی پیدا کرده است و هر جا که به پایگاه داده یا سیستمی برای اشتراک داده نیاز بود، می توان از آن استفاده کرد و نیاز به اعتماد را از بین برد. امضاهای دیجیتال در بلاک چین بسیار پر استفاده هستند از این رو بهبودی در امنیت آن ها ایجاد شد لذا با تلفیق امضای دیجیتال با تسهیم راز تصویری الگوریتمی ارائه داد که امنیت قابل قبولی در برابر حملات کانال جانبی دارد

نصیری و همکاران(۱۳۹۹)در تحقیقی به بررسی بهبود مقیاس پذیری زنجیره بلوکی با استفاده از طرح های امضای دیجیتال آستانه ای امضای آستانه ای نوعی امضای دیجیتال است که تعداد مشخصی از اعضای گروه میتوانند با همکاری یکدیگر امضای معتبر ایجاد کنند به گونه ای که هیچ زیرمجموعه ای از اعضا با تعداد کمتر از آن مقدار، نمیتوانند آن را ایجاد کنند. استفاده از امضای دیجیتال آستانه ای میتواند معایب چند امضایی در زنجیره بلوکی را برطرف کند زیرا هم تراکنش حاوی امضا است و هم تایید آن زمان کمتری میطلبد.

مطالعات خارجی:

دارگون و همکاران(۲۰۲۳)در تحقیقی به بررسی چالش های حقوقی ، فناوری های دیجیتال در تجارت بین الملل پرداختند مطالعه تطبیقی قوانین تجارت بین المللی با قانون تجارت فناوری دیجیتال یونان و جهان گامی مؤثر در جهت شناخت کاستیهای قانون کشور یونان و تلاش در راستای ایجاد هماهنگی با قوانین بین المللی خواهد بود و در این مطالعه تطبیقی، آنچه که بیشتر ضروری مینماید، تأکید بر نقاط میان قراردادهای سنتی و الکترونیکی و دیجیتال در سیستمهای حقوقی مختلف است. و به رسمیت شناختن فناوریهای نوین ارتباطی در تشکیل قراردادها، نحوه تشکیل و اعتبار آنها، قابلیت انتساب اسناد الکترونیک، مسائل مربوط به امضای الکترونیک و.. از جمله مباحث مهم مطرح در این تحقیق می باشد

ریسون و همکاران(۲۰۲۳)در تحقیقی به بررسی میزان تأثیر عوامل موثر بر آمادگی سازمانی پرداختند برای استفاده از امضای دیجیتال در بانکداری الکترونیک امروزه بسیاری از مدیران بانکها نقش اساسی فناوری اطلاعات را در کسب مزیت رقابتی و دنبال نمودن اهداف استراتژیک سازمان درک نموده اند. با توجه به این که بانکداری الکترونیک یک الزام رقابتی است؛ پذیرش و استفاده از فناوری امضای دیجیتال می تواند اعتماد و امنیت تبادلات الکترونیک را بهبود بخشد. هدف اصلی این پژوهش مطالعه میزان تاثیر عوامل مؤثر بر آمادگی سازمانی برای استفاده از امضای دیجیتال در بانکداری الکترونیک است. بعد از بررسی گسترده در ادبیات موضوع، متغیرهای مؤثر بر آمادگی سازمانی برای استفاده از امضای دیجیتال شناسایی شدند و با استفاده از آزمون دوجمله ای، توسط نرم افزار Spss ۱۹ تحلیل شدند؛ که اثرات متغیرهای تأیید شده در قالب بعد ساختاری (فنی، مالی، امنیتی)، بعد رفتاری(مدیریت، فرهنگ سازمانی، دانش و آموزش) و بعد زمینه ای(مشتریان، رقبا، قانونی-سیاسی، اشخاص ثالث) دسته بندی شدند سایر یافته ها نشان داد، در بانک های دولتی عوامل زمینه ای با وزنی معادل٪۳/۳۱ مهمترین، و در بانک های خصوصی عوامل رفتاری با وزنی معادل ٪۱/۷۰ دارای بیشترین اهمیت را میباشد.

رامون و همکاران(۲۰۲۲)در تحقیقی به بررسی قواعد حقوقی حاکم بر استفاده از ارزهای رمزنگاری شده در تجارت بین الملل پرداختند استفاده از ارزهای رمزنگاری شده به طور اعم و بیت کوین به عنوان مهم ترین ارز رمزنگاری شده به طور اخص، روز به روز در حال گسترش است به طوری که سرمایه در گردش بازار بیت کوین امروزه به مرز ۱۷۰ میلیارد دلار رسیده است . دیدگاه مختلفی از جانب سیاستگذاران در مورد ممنوعیت یا مشروعیت به کارگیری ارزهای رمزنگاری شده در اقتصاد داخلی و تجارت بین الملل وجود دارد. تصمیم گیری درست در مورد اجازه ورود ارزهای رمزنگاری شده به چرخه اقتصاد و همسو نمودن نظام های مالی و اقتصادی با فناوری انتقال و نگه داری آن، نیازمند شناسایی ماهیت حقوقی و مزایا و معایب استفاده از اینگونه ارزها در تجارت بین الملل می باشد .از سوی دیگر ناشناس بودن هویت واقعی طرفین انتقال و انجام تراکنش ها به صورت نظیر به نظیر، موجبات ترویج استفاده اینگونه ارزها در جرائم مالی از جمله پولشویی، تامین مالی تروریسم و فرار مالیاتی را فراهم اورده است. مزیت ناشناسی و عدم وجود نهاد واسطه در ردیابی تراکنش ها در ارزهای رمزنگاری شده، به شرط ارزیابی تمامی ابعاد حقوقی و فنی این فناوری نوظهور، به نظر می تواند توسط کشورهای هدف تحریم به عنوان ابزاری در کاهش اثرات تحریم های اقتصادی و گردش سرمایه در بازار تجارت جهانی، به کار گرفته شد

دیوید و همکاران(۲۰۲۲)در تحقیقی به بررسی امکان سنجی ایجاد پول رمزنگاری شده ملی در بستر زنجیره های بلوکی پرداختند استفاده از فناوریهای روز یکی از مهمترین مسائل و مشکلات سر راه کارشناسان و محققین مالی و اقتصادی است. بلاکچین یکی از این تکنولوژیها هست که از آن به عنوان تکنولوژی قرن یاد میکنند. برخی از کارشناسان معتقدند که این تکنولوژی، منجر به حذف بانکهای مرکزی تا ۲۰ سال آینده خواهد شد.در این پژوهش، به بررسی امکان ایجاد پول رمزنگاری شده ملی در بستر زنجیره های بلوکی پرداخته میشود. برای انجام این مهم، ابتدا به بررسی ماهیت و مفهوم پول، تاریخچه آن، بررسی کارکردها و ویژگیهای الزم در هر پولی پرداخته شده و پس از تشریح تکنولوژی بلاکچین و کاربردهای آن ، به بررسی امکان طراحی و ساخت پول رمزنگاری شده پرداخته میشود. بر اساس نتایج این تحقیق برای طراحی پول رمزنگاری شده ملی در بستر زنجیره های بلوکی باید به ۱۱ شاخص توجه داشت. بر اساس مطالعات پژوهشگر ایجاد و طراحی پول رمزنگاری شده ملی از نظر این شاخص ها بلامانع است. همچنین برای اطمینان از نتایج تحقیق، پرسشنامه ای در اختیار خبرگان مالی و اقتصادی جهت ارزیابی شاخص ها قرار گرفت که بر اساس نظر خبرگان نیز، امکانِ طراحی و ایجاد پول رمزنگاری شده ملی در بستر زنجیره های بلوکی وجود دارد. این پژوهش از نوع کیفی، کاربردی و از حیث روش پژوهش توصیفی – تحلیلی و نظرخواهی از خبرگان میباشد.

رامون و همکاران(۲۰۲۱)در تحقیقی به بررسی رمزنگاری تصویر مبتنی بر سیستم های دینامیکی آشوبی پرداختند پیشرفت سریع فناوری اطلاعات و شبکه های مخابراتی در سالهای اخیر، موجب افزایش انتقال داده های دیجیتالی از جمله تصویر، فایلهای صوتی و تصویری شده است. از اینرو به منظور حفظ امنیت این دادهها و مصون ماندن آنها ازدید کاربران غیرمجاز، تحقیقات گستردهای توسط محققان انجام شده است. رمزنگاری یک راه بسیار مناسب برای رسیدن به امنیت بالا است. رمزنگاری تصویر به دلیل کاربردهای متنوعی که در مسائل نظامی و پزشکی دارد به یکی از حوزه های فعال و پرکاربرد تبدیل شده است. در این تحقیق به پیش زمینه و مفاهیم و اصطلاحات کاربردی در حوزه رمزنگاری پرداخته شد. سپس در مورد نظریه آشوب و کاربرد آن در رمزنگاری بحث کرده و خصوصیت های یک سیستم رمزنگاری ایمن را بیان شد. نظریه آشوب به دلیل ویژگی هایی مانند دوره ای بودن، حساس بودن به شرایط اولیه و پارامترهای کنترل محبوبیت بیشتری دارد. نتایج نشان میدهد که به منظور رسیدن به یک سطح امنیتی رضایت بخش فقط یک دور مورد نیاز است که در طرح پیشنهادی استفاده میشود، در حالیکه حداقل دو دور رمزنویسی در دیگر سیستمهای رمزنگاری قابل مقایسه اجرا شده است. بنابراین این مزیت منجر به افزایش سرعت طرح پیشنهادی در پایاننامه حاضر شده است.

بحث و نتیجه گیری:

رمزنگاری اساس و بنیاد تبادل اطلاعات در تکنولوژی‌های امروز در جهان گسترده اینترنت است. همچنین این روش به عنوان رمزنگاری نامتقارن نیز مطرح است زیرا کلیدی که برای رمزنگاری به کار می‌رود با کلیدی که برای رمز گشایی به کار می‌رود متفاوت است. در رمزنگاری ، هر کاربر یک جفت کلید برای رمزنگاری شامل یک کلید عمومی و یک کلید خصوصی است. کلید خصوصی به عنوان یک راز از سوی کاربر باید نگهداری شود و همه کاربران امکان استفاده از کلید عمومی را دارند و در اختیار همه قرار می‌گیرد. از رمز نگاری نامتقارن هم برای رمزنگاری استفاده می‌شود هم برای رمز گشایی استفاده می‌شود. پیام‌هایی که با کلید عمومی رمزنگاری می‌شوند فقط با کلید خصوصی مطابق قابلیت رمزگشایی را دارند. هرچند که کلیدهای عمومی و خصوصی مطابق با یکدیگر هستند ولی با استفاده از کلید عمومی نمی‌توان کلید خصوصی را به دست آورد. در طرح رمزنگاری متقارن فرستنده و گیرنده باید با یک کلید مشترک اضافه باشند تا بتوانند عملیات رمزگشایی و رمز نگاری را انجام دهند و به همین دلیل این طرح قابلیت اجرایی شدن کمتری نسبت به روش نامتقارن دارند زیرا روش متقارن یک پهنای باند ویژه جهت تبادل کلید اضافی نیاز دارد به همین دلیل از کارایی مناسبی برخوردار نیستند . دو شاخه اصلی رمزنگاری با کلید عمومی عبارتند از :رمزگذاری کلیدی عمومی: پیامی که با کلید عمومی رمزگذاری شده باشد فقط به وسیله صاحب کلید خصوصی مطابق با آن رمزگشایی می‌شود و این موضوع به همکاری فرستنده و گیرنده بستگی دارد و می‌تواند اعتماد را تا اندازه زیادی در این سیستم تأمین کند و همکاری کرد .امضاهای دیجیتال: در مورد امضای دیجیتال پیام با استفاده از کلید خصوصی فرستنده رمزگذاری می‌شود و با استفاده از کلید عمومی فرستنده نیز رمزگشایی می‌شود. رمزنگاری کلید عمومی در مقایسه با صندوق پستی مانند صندوق پستی قفل شده همراه یک دریچه است که این دریچه در دسترس عموم قرار دارد به‌طور مثال اطلاعاتی از قبیل محل خیابان در اختیار عموم قرار می‌گیرد. هرکس با دانستن آدرس خیابان می‌تواند به در مورد نظر مراجعه کرده و پیام مکتوب را از طریق دریچه می‌تواند ببیند ولی فقط شخصی که کلید باز کردن صندوق پستی را دارا می‌باشد می‌تواند پیام را بخواند. همچنین امضاهای دیجیتال شبیه پلمب یک پاکت نامه است که هرکس می‌تواند پاکت نامه را باز کند ولی پلمی فرستنده بر روی پاکت نامه به عنوان نشانی از فرستنده باقی خواهد ماند. مسئله اصلی برای استفاده از رمزنگاری عمومی ایجاد اطمینان در مسیر ارسال اطلاعات است.. با توجه به مثال‌های ذکر شده باید کلید عمومی برای هر شخص به درستی تولید شود تا از سوی شخص سومی مورد تهاجم واقع نشود و سلامت سیستم حفظ شود. یک شیوه مرسوم برای رسیدگی به این مسئله استفاده از یک سازمان کلید عمومی است که بتواند در مورد شخص سومی که وارد سیستم می‌شود یک دسترسی متناسب تعریف کند . تمامی تکنیک‌های قابلیت اجرای سریعتر نسبت به اجرای سیستم کلید خصوصی را دارند و می‌توانند به اندازه کافی برای برنامه‌های متنوع کلید تولید کنند .در عمل اغلب رمز نگاری با کلید عمومی با سیستم کلید خصوصی به کار می‌رود تا بتواند بازدهی بیشتری داشته باشد. چنین ترکیب‌هایی را سیستم رمزنگاری دو رگه می‌نامند. برای رمزنگاری، فرستنده پیام با استفاده از الگوریتم تولید کلید به‌طور تصادفی یک کلید تولید می‌کند و با استفاده از آن کلید تصادفی عملیات رمزنگاری با کلید عمومی را انجام می‌دهد. برای امضاهای دیجیتالی، فرستنده پیام با استفاده از تابع درهم‌سازی پیام را خرد می‌کنند و پس از تأیید محتوای نامه، آن را امضا می‌کند. همچنین گیرنده با استفاده از تابع درهم‌سازی محاسباتی را انجام می‌دهد و کدی را به دست می‌آورد و این کد را با کد حاصل از اعمال تابع درهم‌سازی بر روی امضا، مقایسه می‌کند و بررسی می‌کند که آیا پیام مورد حمله قرار گرفته‌است یا خیر

Challenges in implementing digital signature in cyberspace based on encrypted information technology

Ayda Nobakht Namin

Master Student of IT Business Management, Faculty of Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran

nobakht.ayda@gmail.com

Golnaz Rasouli

Master Student of IT Business Management, Faculty of Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran

golnazrasooli@gmail.com

Maryam Farshadivafa

Master Student of IT Business Management, Faculty of Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran

maryam.farshadivafa@gmail.com

Mohammad Reza Khosravi

Master Student of IT Business Management, Faculty of Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran

m.khosravi367@gmail.com

Abstract:

Digital signature is a scheme for checking the identification of a sender's message with the help of mathematical operations, which can be used as a strong tool to identify people and organizations, just like a manual signature. The sender of the message attaches the digital signature obtained from the text of the message with the help of the hash function and encryption function to his message. Unlike manual signature, digital signature changes with different messages. Digital signature guarantees that the content of the message is verified by the sender and has not been changed by someone else.

In this article, the issue of challenges in the implementation of digital signature in the cyber space based on encrypted information technology has been investigated. Currently, with the expansion of the use of electronic signatures, digital signatures can be used as an alternative to manual signatures. A digital signature is a type of electronic signature that contains a string of mathematical codes specific to a certain person. However, there are still security weaknesses that limit the use of digital signatures. In many electronic signature guidelines and guidelines, requirements for advanced electronic signatures, which are digital signatures, are stated. In this article, it is tried to take a step towards improving the security of digital signature by reviewing and improving these requirements.

Keywords: Digital signature, cyberspace, information technology, cryptography, digital transformation

منابع:

مرادی،(۱۴۰۱)" مقایسه دو استاندارد در زمینه امنیت محصولات رمزنگاری در شبکه های مخابراتی"، اولین کنفرانس ملی ایده های نو در مهندسی برق، دانشگاه آزاد تهران مرکز

صابری،(۱۴۰۱) مطالعه تطبیقی امضای الکترونیکی در حقوق ایران، مقررات آنسیترال و حقوق فرانسه"، نخستین کنگره بین المللی حقوق ایران، تهران

راستین،(۱۴۰۱)" بهبودمکانیزم های پشتیبانی از کنترل انحصاری امضاکننده نسبت به داده امضا درامضای دیجیتال"، پایان نامه ی کارشناسی ارشد، دانشگاه شاهد، تهران

شفیعی،(۱۴۰۱) امضای الکترونیک منطبق با حقوق فرانسه"، انتشارات بنیاد حقوقی میزان ،مجله دانش بنیان ش ۱۳

Neriso B, Kubiak.p(۲۰۲۳) Digital Signatures for Government – A Long-Term Security Architecture", LNICST 56, pp. 256–270, nstitute for Computer Sciences, Social Informatics and Telecommunications Engineering

Deris .E And Elkamchouchi.H,(۲۰۲۳) "Elliptic Curve Kleptography", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.6, June SCN 2010, LNCS 6280, pp 271-290

Jayson A Yung.M(۲۰۲۳) Digital signature in the way of law", International journal of electronics; mechanical and mechatronics engineering. Vol.2, Num.2, pp (172- 179)

David .P, Kubiak.P(۲۰۲۳) , "Digital Signatures", Publisher:Springer-Verlag New York Inc, New York, United States

Jernin V, Jonathan.S And John.R(۲۰۲۳) "Decision making - the analytic hierarchy and network processes (AHP/ANP)", Journal of systems science and systems engineering, Vol. 13, No. 1, pp1-35,
Filik(۲۰۲۳) "Supervised Usage of Signature Creation Devices", Inscrypt, Lecture Notes in Computer Science, vol 8567. Springer