مطالعات علوم کاربردی در مهندسی

دوره ۱۰، شماره ۱، بهار ۱۴۰۳

صفحات ۱۳۲-۱۲۰

Online ISSN: ۲۴۷۶-۴۵۰۷

Print ISSN: ۲۵۳۸-۲۰۵۵

www.irijournals.com

طراحی و پیاده سازی نرم افزاری مناسب یک الگوریتم رمز نگاری بلوکی بومی بر روی کارت هوشمند

عبدالوهاب کمالی

مهندسی تکنولوژی نرم افزار

چکیده

امروزه سامانه های مبتنی بر کارت هوشمند به طور گسترده در سراسر دنیا رایج گردیده اند. کارت های هوشمند در کاربردهایی از قبیل کنترل دسترسی، تجارت الکترونیک، احراز هویت و از این قبیل استفاده می گردند. به خاطر اهمیت این کاربردها، ملاحظات امنیتی برای تولید کنندگان و کاربران کارت هوشمند حیاتی است. استفاده کنندگان وقتی می توانند در یک فرآیند امن از خدمات مبتنی بر کارتهای هوشمند بهره گیرند که حداقل همه مخاطرات امنیتی در بکارگیری آنها را دانسته و برای مقابله با آنها تمهیدات لازم را تدارک دیده باشند . در این پژوهش ضمن آشنایی با ساختار سخت افزاری و نرم افزاری کارتهای هوشمند، مخاطرات امنیتی آنها شناسایی و استفاده از رمزنگاری بعنوان یکی از روشهای اصلی مقابله با این مخاطرات مورد بررسی قرار خواهد گرفت. عملیات رمزنگاری بر مبنای یک الگوریتم رمز انجام می گیرد. الگوریتمهای رمز با روشهای سخت افزاری یا نرم افزاری پیاده سازی و قابل بکارگیری می باشند. در این پایان نامه الگوریتم رمز aes با ساختار تغییر یافته، بعنوان الگوریتم رمز بومی در نظر گرفته شده و بصورت نرم افزاری بر روی کارت هوشمند top-imgx4 ساخت شرکت gemaltoپیاده سازی و با پیاده سازی های نرم افزاری الگوریتم aes که بر روی میکروکنترلر atmega163 و میکروکنترلر ۸۰۵۱ انجام شده است و همچنین پیاده سازی های سخت افزاری الگوریتم aes که بر روی تراشه fpga مدل xc2s515-6 و کارت هوشمند top-imgx4 انجام گردیده، مقایسه شده است. نتایج حاصله نشانگر آن است که پیاده سازی نرم افزاری الگوریتم رمز بومی برای همه کاربردهای غیر بلادرنگ مناسب بوده اما برای کاربردهای بلادرنگ صرفاً با افزایش منابع پردازشی و حافظه کارت هوشمند قابل استفاده خواهد بود.

واژه‌های کلیدی: طراحی، پیاده سازی، نرم افزار، الگوریتم، رمز نگاری، بلوکی بومی، کارت هوشمند

دوره ۱۰، شماره ۱، بهار ۱۴۰۳، صفحات ۱۳۲-۱۲۰

مقدمه:

در بررسی نخستین استفاده‌کنندگان از تکنیک‌های رمزنگاری به سزار (امپراتور روم) و نیز الکندی که یک دانشمند مسلمان است برمی‌خوریم، که البته روش‌های خیلی ابتدایی رمزنگاری را ابداع و استفاده کرده‌اند. به عنوان مثال، با جابجا کردن حروف الفبا در تمام متن به اندازه مشخص آن را رمز می‌کردند و تنها کسی که از تعداد جابجا شدن حروف مطلع بود می‌توانست متن اصلی را استخراج کند.یکی دیگر از شیوه‌های رمزنگاری ابتدایی، پیچیدن یک نوار کاغذی بر روی استوانه‌ای با قطر مشخص و سپس نوشتن پیام روی کاغذ پیچیده شده بوده‌است. بدیهی است بدون اطلاع از مقدار قطر استوانه، خواندن پیام کار بسیار دشواری خواهد بود و تنها کسانی که نسخه‌های یکسانی از استوانه را داشته باشند می‌توانند پیام را بخوانند.در قرن بیستم میلادی از همین روش به همراه موتورهای الکتریکی برای رمزنگاری با سرعت بالا استفاده شد که نمونه‌های آن در ماشین رمز لورنتز و ماشین رمز انیگما دیده می شود که در جنگ جهانی دوم توسط آلمان برای رمز کردن پیام‌های نظامی مورد استفاده قرار گرفته‌است.

وجود شاخصهای آماری برای دو یا سه حرفی ها، لستر اس.هیل را به این فکر واداشت که بایستی بیش از سه حرف را در هم ادغام کرد تا بلکه استحکام بیشتریدر مقابل حملات مبتنی بر شاخص های آماری متن، بوجود بیاید. این ریاضی دان از جبر ماتریسی بهره گرفت.آگوست کرکهف در سال ۱۸۸۳ دو مقاله با عنوان «رمز نگاری نظامی» منتشر کرد. در این دو مقاله شش اصل اساسی وجود داشت که اصل دوم آن به عنوان یکی از قوانین رمز نگاری هنوز هم مورد استفاده دانشمندان در رمز نگاری پیشرفته‌است:

- سیستم رمزنگاری اگر نه به لحاظ تئوری که در عمل غیر قابل شکست باشد.
- سیستم رمز نگاری باید هیچ نکته پنهان و محرمانه‌ای نداشته باشد. بلکه تنها چیزی که سری است کلید رمز است.
- کلید رمز باید به گونه‌ای قابل انتخاب باشد که اولا بتوان براحتی آن را عوض کرد و ثانیا بتوان آنرا به خاطر سپرد و نیازی به یاداشت کردن کلید رمز نباشد.
- متون رمز نگاری باید از طریق خطوط تلگراف قابل مخابره باشند.
- دستگاه رمز نگاری یا اسناد رمز شده باید توسط یکنفر قابل حمل و نقل باشد.
- سیستم رمزنگاری باید به سهولت قابل راه اندازی باشد.

با پدید آمدن رایانه‌ها و افزایش قدرت محاسباتی آنها، دانش رمزنگاری وارد حوزه علوم رایانه گردید و این پدیده، موجب بروز سه تغییر مهم در مسائل رمزنگاری شد:

۱. وجود قدرت محاسباتی بالا این امکان را پدید آورد که روش‌های پیچیده‌تر و مؤثرتری برای رمزنگاری به وجود آید.
۲. روش‌های رمزنگاری که تا قبل از آن اصولا برای رمز کردن پیام به کار می‌رفتند، کاربردهای جدید و متعددی پیدا کردند.
۳. تا قبل از آن، رمزنگاری عمدتاً روی اطلاعات متنی و با استفاده از حروف الفبا انجام می‌گرفت؛ اما ورود رایانه باعث شد که رمزنگاری روی انواع اطلاعات و بر مبنای بیت انجام شود.

گسترش و رشد بی سابقه اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، سازمانها و موسسات شده است. امنیت اطلاعات یکی از مسائل مشترک شخصیت های حقوقی و حقیقی است . اطمینان از عدم دستیابی افراد غیر مجاز به اطلاعات حساس از مهمترین چالش های امنیتی در رابطه با توزیع اطلاعات در اینترنت است . اطلاعات حساس که ما تمایلی به مشاهده آنان توسط دیگران نداریم، موارد متعددی را شامل می شود. برخی از اینگونه اطلاعات بشرح زیر می باشند:

- اطلاعات کارت اعتباری

- شماره های عضویت در انجمن ها
- اطلاعات خصوصی
- جزئیات اطلاعات شخصی
- اطلاعات حساس در یک سازمان
- اطلاعات مربوط به حساب های بانکی
- **متن ساده:** اطلاعات اولیه که هنوز رمز نگاری نشده اند
- **متن رمزی:** اطلاعاتی که رمز نگاری شده اند
- **الگوریتم رمز نگاری:** الگوریتمی که متن ساده را به متن رمزی تبدیل می کند
- **کلید رمز:** داده ای است که الگوریتم رمز نگاری متن ساده را به متن رمزی تبدیل می کند و برعکس
- **رمز نگاری:** فرایند تبدیل متن ساده به متن رمزی است
- **رمز گشایی:** فرایند تبدیل متن رمزی به متن ساده است

با استفاده از رمزنگاری سه سرویس امنیتی فراهم می شود:

محرمانه سازی: اطلاعات به هنگام ارسال یا ذخیره شدن از دید افراد غیر مجاز پنهان خواهد شد.

تمامیت: تغییرات اعمال شده در اطلاعات ارسالی مشخص خواهد شد.

اعتبار سنجی: می توان منبع اطلاعات را اعتبار سنجی کرد.

الگوریتم‌های رمزنگاری رامی توان هم به صورت سخت افزاری (به منظور سرعت بالاتر) و هم به صورت نرم افزاری (برای انعطاف پذیری بیشتر) پیاده سازی کرد. روشهای جانشینی و جایگشتی می‌توانند با یک مدار ساده الکترونیکی پیاده سازی شوند p-box.ابزاری است که برای جایگشت بیتهای یک ورودی هشت بیتی کاربرد دارد. با سیم بندی و برنامه ریزی درونی این p-box قادر است هر گونه جایگشت بیتی راعملاً با سرعتی نزدیک به سرعت نور انجام بدهد چرا که هیچ گونه محاسبه‌ای لازم نیست وفقط تأخیر انتشار سیگنال وجود دارد.این طراحی از اصل کرکهف تبعیت می‌کند یعنی: حمله کننده از روش عمومی جایگشت بیت‌ها مطلّع است آن چه که او از آن خبر ندارد آن است که کدام بیت به کدام بیت نگاشته می‌شود کلید رمز همین است.

به طور کلی، یک پروتکل رمزنگاری، مجموعه‌ای از قواعد و روابط ریاضی است که چگونگی ترکیب کردن الگوریتم‌های رمزنگاری و استفاده از آن‌ها به منظور ارائه یک سرویس رمزنگاری خاص در یک کاربرد خاص را فراهم می‌سازد.وظایف یک پروتکل رمزنگاری را می توان بصورت کلی به دسته های زیر طبقه بندی کرد:

- 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 الگوریتم‌های رمزنگاری و با کدام پارامترها باید مورد استفاده قرار گیرند.
- روابط ریاضی چگونه به اطلاعات عددی اعمال شوند.
- چه اطلاعاتی باید بین طرف ارسال‌کننده و دریافت‌کننده رد و بدل شود.
- چه مکانیسم ارتباطی برای انتقال اطلاعات مورد نیاز است.

به عنوان مثال می‌توان به پروتکل تبادل کلید دیفی-هلمن برای ایجاد و تبادل کلید رمز مشترک بین دو طرف اشاره نمود.

دوره ۱۰، شماره ۱، بهار ۱۴۰۳، صفحات ۱۳۲-۱۲۰

یک پروتکل رمزنگاری است که با استفاده از آن، دو نفر یا دو سازمان، می‌توانند بدون نیاز به هر گونه آشنایی قبلی، یک کلید رمز مشترک ایجاد و آن را از طریق یک مسیر ارتباطی غیر امن، بین خود تبادل نمایند. این پروتکل، اولین روش عملی مطرح شده برای تبادل کلید رمز درمسیرهای ارتباطی غیر امن است و مشکل تبادل کلید رمز در رمزنگاری کلید متقارن را آسان می‌سازد. این پروتکل، در سال ۱۹۷۶ توسط دو دانشمند رمزشناس به نام های ویتفیلد دیفی و مارتین هلمن طراحی شده و در قالب یک مقاله علمی منتشر گردیده است. مطرح شدن این پروتکل، گام مهمی در معرفی و توسعه رمزنگاری کلید نامتقارن به حساب می‌آید.

الگوریتم رمزنگاری، به هر الگوریتم یا تابع ریاضی گفته می‌شود که به علت دارا بودن خواص مورد نیاز در رمزنگاری، در پروتکل‌های 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 مورد استفاده قرار گیرد، بلکه صرفاً وجود کاربرد مربوط به رمزنگاری مد نظر است.در گذشته سازمان‌ها و شرکت‌هایی که نیاز به رمزگذاری یا سرویس‌های دیگر رمزنگاری داشتند، الگوریتم رمزنگاری منحصر به فردی را طراحی می‌نمودند. به مرور زمان مشخص گردید که گاهی ضعف‌های امنیتی بزرگی در این الگوریتم‌ها وجود دارد که موجب سهولت شکسته شدن رمز می‌شود. به همین دلیل امروزه رمزنگاری مبتنی بر پنهان نگاه داشتن الگوریتم رمزنگاری منسوخ شده‌است و در روش‌های جدید رمزنگاری، فرض بر این است که اطلاعات کامل الگوریتم رمزنگاری منتشر شده‌است و آنچه پنهان است فقط کلید رمز است.

بیان مسئله:

روش های رمزنگاری را در ساده ترین حالت ممکن به دو نوع رمزهای جانشینی و جایگشتی تقسیم بندی میکنیم، در ادامه توضیحاتی را در خصوص هر یک از این روش های رمزنگاری ارائه خواهیم داد.

در رمز جانشینی هر حرف یا گروهی از حروف به جای حرف یا گروهی از حروف دیگر قرار می گیرد تا پنهان سازی صورت گیرد. در این روش a به D ، b به E ، c به F ، .....و z به C تبدیل می شود.به عنوان مثال:عبارت attack به DWWDFN تبدیل می شود. در مثال ها متن ساده با حروف کوچک و متن رمزی با حروف بزرگ مشخص می شود.در این مثال کلید (k) برابر ۳ است که میتواند متغیر باشد.هر سیستم رمزنگاری که در آن یک سمبل با سمبل دیگر جایگزین می شود اصطلاحا سیستم جانشینی تک حرفی گفته میشود که در آن کلید رمز یک رشته ی ۲۶ حرفی است.

- متن ساده: a b c d e f g h I j k l m n o p q r s t u v w x y z
- متن رمزی: Q W E R T Y U I O P A S D F G H J K L Z X C V B N

مثال: طبق این الگو عبارت attack به متن QZZQEA تبدیل می شود. روش دیگر حدس زدن کلمه یا عبارت است به عنوان مثال متن رمزی زیر را از یک موسسه مالی درنظر بگیرید(به صورت گروههای پنج کاراکتری دسته بندی شده اند):

CTBMN BYCTC BTJDS QXBNS GSTJC BTSWX CTQTZ CQVUJ
QJSGS TJQZZ MNQJS VLNSX VSZJU JDSTS JQUUS JUBXJ
DSKSU JSNTK BGAQJ ZBGYQ TLCTZ BNYBN QJSW

یکی از کلماتی که ممکن است در موسسه مالی باشد financial است.با توجه به اینکه کلمه financial دارای حرف تکراری (i)است به طوری که چهار حرف دیگر بین دو وقوع i وجود دارد. حروف تکراری در متن رمزی را در این فاصله پیدا می کنیم.

۱۲ مورد وجود دارد که در موقعیت های ۶ و ۱۵ و ۲۷ و ۳۱ و ۴۲ و ۴۸ و ۵۶ و ۶۶ و ۷۰ و ۷۱ و ۷۶ و ۸۲ است.(از چپ به راست). فقط در دو تا از اینها یعنی ۳۱ و ۴۲ کاراکتر بعدی) متناظر با n در متن ساده (در موقعیت مناسبی تکرار شده است. از این دو تا فقط در موقعیت ۳۱ حرف a در موقعیت درستی قرار دارد لذا در می یابیم که financial از موقعیت ۳۰ شروع می شود. بنابراین با استفاده از تکرار آماری در متن انگلیسی به راحتی می توان به کلید پی برد.

اصولاً رمزنگاری کلید متقارن و کلید نامتقارن دارای دو ماهیت متفاوت هستند و کاربردهای متفاوتی نیز دارند. بنابراین مقایسه این دو نوع رمزنگاری بدون توجه به کاربرد و سیستم مورد نظر کار دقیقی نخواهد بود. اما اگر معیار مقایسه، به طور خاص، حجم و زمان محاسبات مورد نیاز باشد، باید گفت که با در نظر گرفتن مقیاس امنیتی معادل، الگوریتم‌های رمزنگاری متقارن خیلی سریع‌تر از الگوریتم‌های رمزنگاری نامتقارن می‌باشند.

لازم به ذکر است که رمزنگاری یک مبحث بسیار پیچیده است و در اینجا ما قصد توضیح پایه های ریاضی الگوریتمهای رمزنگاری یا باز کردن تمام جزئیات را نداریم و تنها به معرفی کلیات این مقوله خواهیم پرداخت. در قسمتهای قبلی تاریخچه مختصری از رمزنگاری، مفاهیم اولیه آن و کلیدهای رمزنگاری را توضیح دادیم. در این قسمت الگوریتم های رمزنگاری با استفاده از کلید متقارن و در قسمت بعدی الگوریتم های رمزنگاری با استفاده از کلید نامتقارن را شرح و بسط خواهیم داد.

یک الگوریتم متقارن از یک کلید برای رمزنگاری و ازهمان کلید برای رمزگشایی استفاده می‌کند. بیشترین شکل استفاده از این نوع رمزنگاری که در کارتهای هوشمند و البته در بیشتر سیستمهای امنیت اطلاعات وجود دارد Data Encryption Algorithmیا DEA است که بیشتر بعنوانDES شناخته می‌شود. الگوریتم DES یک محصول دولت ایالات متحده است که امروزه بعنوان یک استاندارد بین‌المللی شناخته شده و بطور وسیعی مورد استفاده قرار می گیرد.

بلوکهای ۶۴ بیتی دیتا توسط یک کلید تنها که معمولا ۵۶ بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. الگوریتم DES از نظر محاسباتی ساده است و به راحتی می‌تواند توسط پردازنده‌های کند (بخصوص آنهایی که در کارتهای هوشمند وجود دارند) انجام گیرد. در دهه ۶۰ میلادی، با رشد فزاینده فناوری کامپیوتر و نگرانی ها در مورد محرمانه و خصوصی بودن ارتباطات، علاقه به ایجاد یک استاندارد رمزنگاری ملی در آمریکا به شدت افزایش پیدا کرد.

تلاشها در جهت ایجاد استانداردی بود که بتواند توسط کامپیوترها و شبکه های متفاوت دولتی در آمریکا مورد استفاده قرار گیرد و همچنین در سیستم های پیمانکاران دولتی نیز مفید واقع شود. تلاشهای مذکور منجر به ایجاد استاندارد رمزنگاری داده یا Data Encryption Standard (DES) گشت که امروزه به صورت وسیعی در رمزنگاری مورد استفاده قرار می گیرد.

در سال ۱۹۶۵ موسسه ملی استانداردها و فناوری آمریکا که امروزه با نام NIST شناخته می شود، مسئولیت تعیین استانداردهای محافظت از سیستم های کامپیوتری را بر عهده گرفت. موسسه مذکور در فاصله سالهای ۱۹۶۸ تا ۱۹۷۱ به مطالعه و تحقیق در مورد نیازهای امنیتی سیستم های کامپیوتری دولتی پرداخت که در نهایت منجر به تهیه یک استاندارد رمزنگاری شد. موسسه NIST با همکاری NSA یا آژانس امنیت ملی آمریکا، نخستین برنامه رمزنگاری را تولید کرد.

در اوایل کار هدف ایجاد یک استاندارد واحد برای محافظت از داده های طبقه بندی شده دولتی و اطلاعات حساس بخش خصوصی بود که از طرفی بتواند بین ۱۰ تا ۱۵ سال دوام آورد) هدفی که DES بسیار پیشتر از آن رفت (و از طرفی نیز قابل استفاده در انواع سیستم های مختلف حتی سیستم های کند باشد.

در آگوست ۱۹۷۴، NSAاز تولید کنندگان الگوریتم های رمزنگاری برای بار دوم دعوت کرد تا روش های خود را اعلام کنند تا شاید در ایجاد یک استاندارد رمزنگاری عمومی با کیفیت بالا مورد استفاده قرار گیرد. در این زمان IBM الگوریتمی را ارائه

کرد که مورد قبول NSA واقع شد. در شرکت IBM تا قبل از آن کارهایی برای توسعه چندین الگوریتم متفاوت رمزنگاری انجام شده بود. یکی از آنها یک الگوریتم ۶۴ بیتی بود که برای محافظت از تراکنش های مالی به کار می رفت و دیگری یک الگوریتم ۱۲۸ بیتی به نام Lucifer بود.

آژانس امنیت ملی آمریکا در آن زمان از طرفی IBM را تشویق به ثبت الگوریتم Lucifer کرد و از طرف دیگر به متخصصان خود اجازه داد تا سعی کنند ارتباطات رمزنگاری شده توسط الگوریتم مذکور را بشکنند. لذا الگوریتم مذکور بعد از بررسی پایه های ریاضی و سعی در شکستن آن، دچار تغییرات و اصلاحاتی شد (برای مثال طول کلید از ۱۲۸ بیت به ۵۶ بیت کاهش یافت و تغییراتی در توابع جایگزینی انجام شد) تا به تولد DES منجر شد. بالاخره در سال ۱۹۷۷ این الگوریتم به عنوان استاندارد رمزنگاری داده منتشر شد و به عنوان روشی رسمی در محافظت از داده های طبقه بندی نشده در مؤسسات دولتی آمریکا مورد استفاده قرار گرفت.

در عین حال NSA موظف شد تا هر پنج سال یک بار این الگوریتم را مورد مطالعه قرار دهد و تأیید کند که هنوز می تواند به عنوان استاندارد به کار رود. قابل ذکر است که این روش بستگی به مخفی بودن کلید دارد. بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستمی مبادله می‌شود که قبلا هویت یکدیگر را تایید کرده‌اند. عمر کلیدها بیشتر از مدت تراکنش طول نمی‌کشد. رمزنگاری DES عموما برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود.

اهمیت وضرورت تحقیق:

استاندارد رمزنگاری داده (DES) یک الگوریتمی ریاضی است که برای رمزنگاری و رمزگشایی اطلاعات کدشده باینری به کار می رود. رمزنگاری داده ها را تبدیل به داده های نامفهومی به نام cipher می کند. رمزگشایی از cipher آن را به داده های اصلی بازمی گرداند. الگوریتم مذکور هر دو عملیات رمزنگاری و رمزگشایی را بر اساس یک عدد باینری به نام کلید مشخص می سازد. داده ها تنها در صورتی قابل بازیابی از cipher هستند که دقیقاً از کلیدی که برای رمزنگاری استفاده شده برای رمزگشایی نیز استفاده شود.الگوریتم DES دارای دو جزء است:

- **الگوریتم رمزنگاری**: الگوریتم DES منتشر شده شامل چندین تکرار از یک تغییر شکل ساده با استفاده از هر دو تکنیک جابجایی و جایگزینی است. این الگوریتم تنها از یک کلید برای رمزنگاری و رمزگشایی استفاده می کند و به همین جهت به آن رمزنگاری کلید اختصاصی نیز گفته می شود. در این حالت حفظ کلید به صورت محرمانه توسط فرستنده و گیرنده پیغام بسیار اهمیت دارد زیرا الگوریتم به صورت عمومی در اختیار همگان است و در صورت لو رفتن کلید، هر کسی می تواند پیغام محرمانه را ببیند. به همین جهت در رمزنگاری DES معمولاً عمر کلید به اندازه عمر تراکنش است.
- **کلید رمزنگاری**: کلید DES یک توالی هشت بایتی است که هر بایت شامل یک کلید هفت بیتی و یک بیت توازن است. در حین رمزنگاری، الگوریتم DES متن اصلی را به بلوک های ۶۴ بیتی می شکند. این الگوریتم در هر زمان بر روی یک بلوک کار می کند و آن را از نصف شکسته و کاراکتر به کاراکتر رمزنگاری می کند. کاراکترها ۱۶ بار تحت نظارت کلید تغییر شکل پیدا کرده و در نهایت یک متن رمزنگاری شده ۶۴ بیتی تولید می شود. کلید حاوی ۵۶ بیت معنادار و هشت بیت توازن است.
- در سال ۱۹۹۷ در یک تلاش همگانی و با استفاده از ۱۴هزار رایانه یک پیغام رمزنگاری شده توسط DES شکسته شد که البته چندان باعث نگرانی نیست. زیرا در بیشتر انتقال پیغام ها، به خصوص در نقل و انتقالات مالی، یک بازه زمانی وجود دارد

که در آن اطلاعات باید کاملاً محرمانه نگه داشته شود و بعد از آن فاش شدن آنها چندان اهمیت نخواهد داشت.بعد از سقوط DESبسیاری از مؤسسات از DES سه گانه استفاده کردند که به عنوان ۳ DESشناخته می شود و در آن DES سه بار تکرار می شود (دو مرتبه با استفاده از یک کلید به سمت جلو (رمزنگاری) و یک مرتبه به سمت عقب (رمزگشایی) با یک کلید دیگر). به این صورت طول کلید به طرز مؤثری افزایش پیدا می کند و منجر به ارتقای امنیت می شود، هر چند که هیچ کس مطمئن نیست این روش تا کی جواب می دهد.

- به هرحال DES به حیات خود ادامه می دهد زیرا اولاً هر کسی می تواند به راحتی از آن استفاده کند و ثانیاً قابلیت حفظ محرمانگی را برای مدت کوتاهی دارد که برای بسیاری از برنامه های کاربردی، زمان مناسبی محسوب می شود. رمزنگاری DESچهار مد مجزا را فراهم می کند که از لحاظ پیچیدگی و موارد کاربرد متفاوت هستند. در زیر هر کدام از مدها به صورت خلاصه شرح داده شده اند:
- هرگاه در رمزنگاری یک متن بزرگ، کل متن را به قطعات کوچک با طول ثابت (و متناسب با طول ورودی سیستم در رمزنگار) تقسیم کرده و هر بلوک مستقل از دیگری با کلید k رمز و جانشین متن اصلی شود، اصطلاحاً مبتنی بر "شیوه کتابچه رمز" یا (Mode Electronic Code Book (ECB عمل کرده ایم.
- الگوریتم هایی که به فاینال راه پیدا کرده بودند عبارتند ازMARS :، RC6، Rijndael، Serpentو .Twofish استاندارد FIPS-197 در همین رابطه تهیه شده است و الگوریتم مذکور را به عنوان یک رمزنگاری متقارن تعریف می کند که سازمان های دولتی آمریکا باید با استفاده از آن، اطلاعات حساس را رمزنگاری کنند. از آنجایی که اثبات قابل اعتماد بودن الگوریتم مذکور کار بسیار دشواری بود، بسیاری از کشورها و ملیت های دیگر نیز به پروژه AES پیوستند و به آزمایش این الگوریتم پرداختند و از آنجایی که مشکلی در این مورد پیدا نشد، الگوریتم مذکور روز به روز قابلیت اعتماد بیشتری را کسب کرد.

در قسمت قبلی در مورد الگوریتم‌های رمزنگاری متقارنDES ، ۳ DESو AES توضیح دادیم که از یک کلید برای رمزنگاری و رمزگشایی استفاده می کنند. در الگوریتم‌های مذکور در صورتی که کلید رمزنگاری به سرقت رود محرمانگی اطلاعات نیز از بین خواهد رفت.الگوریتم‌های رمزنگاری با کلید نامتقارن از کلیدهای مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستمها اجازه می‌دهند که یکی از کلیدها کلید عمومی یا (public key) منتشر شود در حالی که دیگری کلید خصوصی یا (private key) توسط صاحبش حفظ می‌شود.

فرستنده پیام، متن را با کلید عمومی گیرنده، کد می‌کند و گیرنده آن را با کلید اختصاصی خود رمزگشایی می‌کند. بعبارتی تنها با کلید خصوصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کدشده برای هر گیرنده‌ای، به جز گیرنده مورد نظر فرستنده، بی معنی خواهد بود.

معمول ترین سیستم نامتقارن به عنوان RSA شناخته می‌شود) .این حروف اول نام پدید آورندگان آن یعنی Rivest، Shamirو Adlemen است (این الگوریتم در سال ۱۹۷۸ در دانشگاه MIT ایجاد شده است و تأیید هویت (روشی برای مطمئن شدن از هویت ارسال کننده پیغام) را به خوبی رمزنگاری انجام می‌دهد. الگوریتم RSA از دو کلید برای رمزنگاری استفاده می‌کند: کلید خصوصی و کلید عمومی. در الگوریتم مذکور تفاوتی بین توانایی عملیاتی کلید عمومی و خصوصی وجود ندارد و یک کلید می‌تواند هم به عنوان کلید خصوصی به کار رود و هم به عنوان کلید عمومی.

کلیدهای RSA با استفاده از روش های ریاضی و با ترکیب اعداد اول تولید می‌شوند. بزرگترین عددها با ضرب اعداد کوچک به دست می آیند و این اعداد کوچک از لحاظ ریاضی به هم وابسته هستند و دانستن یکی از آن‌ها منجر به شناسایی دیگر اعداد اول به کار رفته در کلید می‌شود. این وضعیتی است که در استفاده از کلید های عمومی و خصوصی مورد نظر است. البته در صورتی که عدد خیلی بزرگ باشد، این کار به راحتی قابل انجام نیست و وضعیت های گمراه کننده بسیاری وجود دارند.

تنها ترکیب درست از اعداد اول موجود در کلید رمزنگاری، قادر به رمزگشایی پیغام است. امنیت الگوریتم RSA و الگوریتم‌های مشابه آن وابسته به استفاده از اعداد خیلی بزرگ است و بیشتر نسخه های RSA از اعداد ۱۵۴ رقمی یا ۵۱۲ بیتی به عنوان کلید استفاده می کنند. دسترسی به فاکتورهای اعداد اول اعداد خیلی بزرگ که بیش از ۱۰۰ رقم دارند کار بسیار مشکلی است. البته برخی از محققان توانسته اند با تلاش بسیار اعداد بزرگ را بشکنند ولی این کار برای هکرها جهت ورود به یک سیستم یا سر در آوردن از یک پیغام مقرون به صرفه نمی باشد.

برای پرهیز از پیچیدگی بحث فرض کنید فرستنده پیام جفت عدد صحیح و بزرگ (e,n) را به عنوان کلید عمومی برای رمزنگاری اطلاعات خود در اختیار دارد. در طرف مقابل، گیرنده نیز جفت عدد (d,n) را برای رمزگشایی پیام به کار می برد. بدیهی است که دو جفت عدد (e,n) و (d,n) با یکدیگر ارتباط زیرکانه ای دارند ولی این ارتباط یه گونه ای نیست که بتوان با در اختیار داشتن e و n براحتی d را استنتاج کرد. با فرض وجود چنین کلیدهایی، الگوریتم RSA در نهایت سادگی به صورت زیر بیان می‌شود:

- الف) پیامی که باید رمز شود به بلوک‌های k کاراکتری k) بایتی) تقسیم بندی می‌شود.
- ب) هر بلوک طبق قاعده ای کاملاً دلخواه به یک عدد صحیح با نام P تبدیل می گردد.
- ج) با جفت عدد (e,n) به ازای یکایک بلوک‌هایP ، اعداد جدیدی طبق رابطه زیر بدست می آید:

```
C=(P)^e mod n
```

- د) کدهای C به جای کدهای اصلی P ارسال می‌شوند.

روش رمزگشایی داده ها نیز مثل روش رمزنگاری است، یعنی با در اختیار داشتن جفت عدد (d,n) بلوک‌های رمز شده بصورت زیر از رمز خارج خواهند شد:

```
P=(C)^d mod n
```

حال برای درک بهتر به طرح یک مثال ساده و کوچک می پردازیم:

فرض کنید بخواهیم رشته ی "M="catsanddogs را رمز کنیم. برای سادگی این رشته ی کاراکتری را به بلوک‌های دوتایی تقسیم کرده و سپس هر بلوک را به یک عدد صحیح تبدیل می‌کنیم. قاعده تبدیل در این مثال عبارت است از: برای کاراکتر a عدد ۰۰، برای b عدد ۰۱، و به همین ترتیب تا z که عدد ۲۵ در نظر گرفته و جایگذاری می‌شود.

بحث وتحلیل:

رمزهای کلید خصوصی بر مبنای نوع عملکرد، چگونگی طراحی و پیاده سازی و کاربردهایشان به دو گونه رمزهای قطعه ای و رمزهای دنباله ای تقسیم می‌شوند. که در هر یک از آ نها عملکرد رمز نگاری به صورت یک عملکرد دوجانبه بین دو طرف

دوره ۱۰، شماره ۱، بهار ۱۴۰۳، صفحات ۱۳۲-۱۲۰

فرستنده و گیرنده می‌باشد که با ایجاد یک ارتباط اولیه با یکدیگر روی کلید خصوصی توافق می کنند به گونه ای که دشمن آن کلید را نداند.

فرستنده Sمیخواهد پیام m1,....miرا به گونه ای به طرف گیرنده R بفرستد که او بتواند به محتوای پیام دست یابد و در عین حال حریف مخالف A نتواند محتوای پیام را درک کند حتی اگر A تمامی آنچه بین R و S انتقال می یابد را دریافت نماید.به همین منظور فرستنده S هر متن روشن miرا به وسیله الگوریتم رمزگذاری E وکلید خصوصی به متن رمز شده تبدیل می‌کند ودریافت کننده نیز که متن رمز شده را دریافت کرده می‌تواند با الگوریتم رمز گشائی Dو کلید خصوصی متن اصلی را بدست آورد.

بحثهای زیادی شده که کدام یک از این الگوریتم‌ها بهترند اما جواب مشخصی ندارد. البته بررسی هایی روی این سوال شده به طور مثال Needham و Schroeder بعد از تحقیق به این نتیجه رسیدند که طول پیغامی که با الگوریتم‌های متقارن میتواند رمزنگاری شود از الگوریتم‌های کلید عمومی کمتر است و با تحقیق به این نتیجه رسیدند که الگوریتم‌های متقارن الگوریتم‌های بهینه تری هستند. اما وقتی که بحث امنیت پیش می آید الگوریتم‌های کلید عمومی کارایی بیشتری دارند. به طور خلاصه می‌توان گفت که الگوریتم‌های متقارن دارای سرعت بالاتر و الگوریتم‌های کلید عمومی دارای امنیت بهتری هستند.

در ضمن گاهی از سیستم ترکیبی از هر دو الگوریتم استفاده می‌کنند که به این الگوریتم‌ها الگوریتم های ترکیبی (hybrid) گفته می‌شود. اما اگر به طور دقیق تر به این دو نگاه کنیم آنگاه متوجه خواهیم شد که الگوریتم‌های کلید عمومی و الگوریتم‌های کلید متقارن دارای دو ماهیت کاملاً متفاوت هستند و کاربردهای متفاوتی دارند به طور مثال در رمزنگاریهای ساده که حجم داده‌ها بسیار زیاد است از الگوریتم متقارن استفاده می‌شود زیرا داده‌ها با سرعت بالاتری رمزنگاری و رمزگشایی می‌شوند. اما در پروتکل هایی که در اینترنت استفاده می‌شود، برای رمز نگری کلید هایی که نیاز به مدیریت دارند از الگوریتم‌های کلید عمومی استفاده می‌شود.

تکنیک‌های رمزنگاری پیچیده به راحتی از روش‌های جابه‌جایی یا جایگزینی استفاده نمی‌کنند. در عوض از یک کلید محرمانه برای کنترل یک توالی طولانی از جابه‌جایی و جایگزینی‌های پیچیده استفاده می‌کنند. کلیدهای رمزنگاری و الگوریتم‌های رمزنگاری با یکدیگر همکاری می‌کنند تا یک متن اولیه را به یک متن رمزی تبدیل کنند. در اغلب موارد الگوریتم رمزنگاری ثابت و شناخته شده است و این کلید رمزنگاری است که یک نسخه یکتا از اطلاعات رمزنگاری شده تولید می‌کند. در زیر انواع کلیدهای رمزنگاری توضیح داده شده‌اند.

سیستم‌های کلید محرمانه تنها از یک کلید برای رمزنگاری و رمزگشایی اطلاعات استفاده می‌کنند. در این شیوه رمزنگاری، لازم است که هر جفت فرستنده و گیرنده اطلاعات کلید جداگانه‌ای را برای رمزنگاری دارا باشند و حفظ کلید به صورت محرمانه بسیار اهمیت دارد. امنیت این روش در گرو حفظ امنیت کلید است. الگوریتم (Data Encryption Standard DES)یک نمونه از الگوریتم‌های کلید محرمانه است. چون فرض بر این است که الگوریتم شناخته شده و معلوم است، امن بودن انتقال و ذخیره کلید بسیار مهم است.

کارت‌های هوشمند معمولاً برای ذخیره کلیدهای محرمانه استفاده می‌شوند. در این حالت تضمین اینکه قلمرو کلید محدود است، مهم است: باید همیشه فرض کنیم که یک کارت ممکن است توسط افراد غیرمجاز با موفقیت تحلیل گردد و به این ترتیب کل سیستم در مخاطره قرار گیرد. در شکل زیر یک عملیات انتقال اطلاعات با استفاده از کلید محرمانه نشان داده شده

است که در آن یک کاربر بانک، اطلاعات را با استفاده از کلید محرمانه رمزنگاری می‌کند و برای کارمند بانک ارسال می‌کند. وی نیز اطلاعات را با کلید مشابهی رمزگشایی می‌کند.

سیستم‌هایی که از این نوع کلیدها استفاده می‌کنند، نامتقارن خوانده شده و در واقع دارای یک زوج کلید هستند: یک کلید عمومی و یک کلید خصوصی. در این سیستم هر کاربر دارای دو کلید عمومی و خصوصی است که لازم است کلید خصوصی محرمانه نگهداری شود ولی کلید عمومی در اختیار همگان است. در اینجا کلید عمومی و خصوصی به یکدیگر از لحاظ ریاضی وابسته هستند. کاربر می‌تواند با استفاده از کلید خصوصی که در اختیار دارد پیغام خود را رمزنگاری کرده و گیرنده آن را با استفاده از کلید عمومی رمزگشایی کند یا بالعکس.

امتیاز اصلی و مهم سیستم‌های کلید نامتقارن این است که آن‌ها اجازه می‌دهند که یک کلید (کلید خصوصی) با امنیت بسیار بالا توسط صاحب آن نگهداری شود در حالیکه کلید دیگر (کلید عمومی) می‌تواند منتشر شود. کلیدهای عمومی می‌توانند همراه پیام‌ها فرستاده شوند یا در فهرست‌ها لیست شوند. شروط و قوانینی برای کلیدهای عمومی در طرح فهرست پیام‌رسانی الکترونیکی .ITU X500 وجود دارد، و از یک شخص به شخص بعدی داده شوند.

مکانیسم توزیع کلیدهای عمومی می‌تواند رسمی (یک مرکز توزیع کلید) یا غیر رسمی باشد. یکی از نکات منفی سیستم‌های رمزنگاری با کلید عمومی توسط سناریوی زیر توضیح داده شده است. فرض کنید کاربر پیغام خود را با استفاده از کلید خصوصی رمزنگاری می‌کند. دریافت کننده پیغام می‌تواند از هویت فرستنده پیغام مطمئن باشد یعنی تأیید هویت به خوبی انجام می‌شود ولی مشکل اینست که هر کسی که دسترسی به کلید عمومی دارد

می‌تواند اطلاعات مذکور را رمزگشایی کند. لذا این روش محرمانگی اطلاعات را حفظ نمی‌کند. از طرف دیگر در صورتی که اطلاعات توسط کلید عمومی رمزنگاری شوند، از آنجایی که تنها دارنده کلید خصوصی قادر به رمزگشایی آن است لذا محرمانگی آن حفظ می‌شود ولی مشکل در اینست که چون هر کسی می‌تواند به کلید عمومی دسترسی داشته باشد تأیید هویت با مشکل روبرو می‌شود.

راه حل مشکل مذکور، استفاده ترکیبی از دو روش است به طوری که هم امکان تأیید هویت وجود داشته باشد و هم محرمانگی اطلاعات حفظ شود. فرستنده پیغام خود را با استفاده از کلید خصوصی که در اختیار دارد رمزنگاری می‌کند و سپس با استفاده از کلید عمومی که مربوط به گیرنده است آن را مجدداً رمزنگاری می‌کند. در این حالت لازم است گیرنده پیغام ابتدا با استفاده از کلید خصوصی خود پیغام را رمزگشایی کند و سپس نتیجه را با استفاده از کلید عمومی فرستنده مجدداً رمزگشایی کند تا به اصل پیغام دسترسی پیدا کند.

در این صورت پیغام رمزنگاری شده تنها با کلید خصوصی دریافت کننده قابل رمزگشایی است و در نتیجه هم مشکل تأیید هویت و هم حفظ محرمانگی اطلاعات برطرف شده است. در همه حالات فرض می‌شود که دارندگان کلید خصوصی مراقبت‌های لازم را برای حفظ امنیت کلید مزبور به انجام می‌رسانند. البته دو بار رمزنگاری و رمزگشایی همه پیغام لزوماً مورد نیاز نیست. از آنجایی که در صورت استفاده فرستنده از کلید عمومی گیرنده، محرمانگی اطلاعات حفظ می‌شود، در نتیجه رمزنگاری تنها بخش کوچکی از پیغام، برای تأیید هویت فرستنده کافی است. این قضیه ایده اصلی امضای دیجیتالی را تشکیل می‌دهد.

نتیجه گیری:

یکی از ایراداتی که به روش‌های پیشین وارد است، تعداد زیاد کلیدها است که طبیعتاً منجر به سخت‌تر شدن مدیریت کلید می‌شود. یک روش برای کاستن از تعداد کلیدهایی که باید منتقل و ذخیره شوند، مشتق گرفتن از آن‌ها در زمان مورد نیاز است. در یک برنامه اشتقاق کلید، یک کلید اصلی همراه با چند پارامتر مجزا برای محاسبه کلید مشتق شده استفاده می‌شود که بعداً برای رمزنگاری استفاده می‌گردد. برای مثال، اگر یک صادر کننده با تعداد زیادی کارت سروکار دارد.

می‌تواند برای هر کارت، با استفاده از کلید اصلی، شماره کارت را رمز کند و به این ترتیب کلید مشتق شده حاصل می‌شود و به آن کارت اختصاص داده می‌شود. شکل دیگری از کلیدهای مشتق شده با استفاده ازtoken ها به دست می‌آیند کهtoken ها محاسبه‌گرهای الکترونیکی با عملکردهای مخصوص هستند. ورودی آن‌ها ممکن است، یک مقدار گرفته شده از سیستم مرکزی، یک PIN وارد شده توسط کاربر و یا تاریخ و زمان باشد. خود token شامل الگوریتم و یک کلید اصلی است. چنین tokenهایی اغلب برای دسترسی به سیستم‌های کامپیوتری امن استفاده می‌شوند.

از آنجا که ارسال کلید یک نقطه ضعف از نظر امنیتی در سیستم‌ها بشمار می‌رود، رمز کردن کلیدها هنگام ارسال و ذخیره آن‌ها به شکل رمز شده منطقی به نظر می‌رسد. کلیدهای رمز کننده کلید هرگز به خارج از یک سیستم کامپیوتری (یا کارت هوشمند) ارسال نمی‌شوند و بنابراین می‌توانند آسان‌تر محافظت شوند. اغلب برای تبادل کلیدها الگوریتم متفاوتی از آنچه که برای رمز کردن پیام‌ها استفاده می‌شود، مورد استفاده قرار می‌گیرد. از مفهوم دامنه کلید (key domain) برای محدود کردن میدان کلیدها و محافظت کردن از کلیدها در دامنه‌شان استفاده می‌کنیم.

معمولاً یک دامنه، یک سیستم کامپیوتری خواهد بود که می‌تواند به صورت فیزیکی و منطقی محافظت گردد. کلیدهای استفاده شده در یک دامنه توسط یک کلید رمز کننده کلید محلی ذخیره می‌شوند. هنگامی که کلیدها می‌خواهند به یک سیستم کامپیوتری دیگر فرستاده شوند، رمزگشایی و تحت یک کلید جدید رمز می‌شوند که اغلب به عنوان کلید کنترل ناحیه (zone control key)شناخته می‌شوند. با دریافت این کلیدها در طرف دیگر، تحت کلید محلی سیستم جدید رمز می‌شوند. بنابراین کلیدهایی که در دامنه‌های یک ناحیه قرار دارند از دامنه‌ای به دامنه دیگر به صورتی که بیان گردید منتقل می‌شوند.

برای محدود کردن مدت زمانی که کلیدها معتبر هستند، اغلب یک کلید جدید برای هر نشست یا هر تراکنش تولید می‌شود. این کلید ممکن است یک عدد تصادفی تولید شده توسط ترمینالی باشد که در مرحله تصدیق کارت قرار دارد. اگر کارت قادر به رمزگشایی روش کلید عمومی باشد، یعنی کلید نشست می‌تواند با استفاده از کلید عمومی کارت رمز شود. بخشی از تراکنش که در آن کلید منتقل می‌شود اغلب در مقایسه با بقیه تراکنش کوتاه‌تر است؛ بنابراین بار اضافی این بخش نسبت به کل تراکنش قابل صرف نظر است.

چنانچه بقیه تراکنش به سبب استفاده از کلید متقارن (محرمانه) با بالاسری کمتری رمز شود، زمان پردازش برای فاز تایید هویت و انتقال کلید قابل پذیرش است (توضیح اینکه روش‌های رمز متقارن از نامتقارن به مراتب سریع‌تر هستند بنابراین می‌توان ابتدا یک کلید متقارن را با استفاده از روش نامتقارن انتقال داد و سپس از آن کلید متقارن برای انجام بقیه تراکنش استفاده کرد). شکل خاصی از کلید نشست، سیستم انتقال کلید است که در برخی سیستم‌های پرداخت الکترونیک و مبادله دیتای الکترونیک استفاده می‌شود. بدین صورت که در پایان هر تراکنش، یک کلید جدید منتقل می‌شود و این کلید برای تراکنش بعدی مورد استفاده قرار می‌گیرد.

دو سطح ارتباطی پایه وجود دارد که رمزنگاری می‌تواند در آن اجرا شود. رمزنگاری بر اساس این سطوح به دو دسته رمزنگاری مبدأ به مقصد و رمزنگاری انتقال تقسیم می‌شود. در رمزنگاری مبدأ به مقصد یا end-to-end که گاهی اوقات به آن رمزنگاری آفلاین هم گفته می‌شود، پیغام‌ها در مبدأ و در زمان ارسال رمزنگاری شده و سپس در مقصد رمزگشایی می‌شوند. در این سطح رمزنگاری نیازی نیست که شبکه از رمزی بودن پیغام آگاهی داشته باشد.

گاهی اوقات این نوع رمزنگاری می‌تواند توسط کاربر مورد انتخاب قرار بگیرد. پیغام در تمام طول انتقال رمز شده باقی می‌ماند، از ابتدا تا انتها. فایده این روش در این است که احتیاجی نیست در تمام گام‌های مسیر، تمام نقاط امن باشند. این اصلی است که امروزه در سیستم‌های شناخته شده رمزنگاری پیغام به شیوه تونل مانند SSL و TLS مورد استفاده قرار می‌گیرد. در رمزنگاری انتقال یا link encryption که گاهی به آن رمزنگاری آنلاین هم گفته می‌شود، مانند روش قبل پیغام در زمان ارسال رمزنگاری می‌شود ولی هر بار که به یک گره ارتباطی شبکه می‌رسد، رمزگشایی شده و دوباره رمزنگاری می‌شود. در این روش رمزنگاری از دید کاربر پنهان است و به عنوان بخشی از پروسه انتقال اعمال می‌شود. برای هر دو روش نقاط مثبت و منفی وجود دارد که در زیر آورده شده است.

نقاط مثبت روش مبدأ به مقصد

قابلیت انعطاف بیشتری دارد. کاربر می‌تواند تنها اطلاعات مورد نظر خویش را رمزنگاری کند و هر کاربر نیز می‌تواند کلید جداگانه‌ای داشته باشد.

- در این روش انتشار کلید و مدیریت آن ساده‌تر است.
- با استفاده از این روش، اطلاعات از ابتدا تا انتها و در کل شبکه محافظت شده باقی می‌مانند.
- روشی کارآمدتر است زیرا لازم نیست شبکه هیچ‌گونه تسهیلات خاص رمزنگاری را دارا باشد.

نقاط منفی روش مبدأ به مقصد

ممکن است نیاز به بررسی برخی از اطلاعات مانند اطلاعات سر آیند و یا مسیریابی به صورت رمزنگاری نشده باشد.

- هر سیستمی نیازمند اجرای نوع یکسانی از رمزنگاری است.
- این روش تنها محتویات پیغام را امن نگاه می‌دارد ولی نمی‌تواند این واقعیت را مخفی کند که چنین پیغامی فرستاده شده است.

نقاط مثبت روش انتقال

- راحت‌تر است زیرا لازم نیست کاربر هیچ کاری انجام دهد.
- استفاده از آن، در شبکه‌ای که گره‌های زیادی دارد راحت‌تر است.
- در صورتی که یکی از گره‌ها مورد سوء استفاده قرار گیرد تمام شبکه لو نمی‌رود زیرا هر جفت از گره‌ها از کلید جداگانه‌ای استفاده می‌کنند.
- در این روش تمام اطلاعات، حتی اطلاعات سرآیند و مسیریابی رمزنگاری می‌شوند.

نقاط منفی روش انتقال

- انتشار کلید و مدیریت آن بسیار مشکل خواهد بود زیرا همه گره‌های شبکه لازم است یک کلید دریافت کنند.
- نقاط آسیب پذیر بیشتری وجود دارد زیرا اطلاعات، چندین نوبت به حالت اولیه تبدیل می‌شود.

منابع:

۱. ارجمند، پرهام وهمکارن،۱۳۸۴ پایان‌نامه;کارشناسی ارشد، دانشگاه شیراز.

۲. زاهدی،عطا،۱۳۸۷، پایان‌نامهکارشناسی ارشد، دانشکده فنی مهندسی،دانشگاه تربیت مدرس .

۳. شجاعی، آرش، خواجه، روح الله، مروری بر مدل های توسعه خدمات نوین، ۱۳۹۴.

۴. عباداللهی، نواله، چشمه سهرابی، مظفر، نوشین فرد، فاطمه، ۱۳۹۳تحلیل عوامل فناورانه موثر بر پذیرش فناوری بر اساس نظریه اشاعه نوآوری راجرز: مورد پژوهشی نرم افزار نمایه نشریات، فصل نامه دانش شناسی، سال هفتم، صفحه ۷۹ الی ۹۲.

۵. فتحیان، محمد و همکاران، ۱۳۸۴، نقش مدیریت دانش در خلاقیت و نواوری، نشریه تدبیر، شماره ۱۶۴.

۶. منطقی، منوچهر، ثاقبی، فاطمه،۱۳۹۲، مدل های کسب و کار، مبانی، ارزیابی، نوآوری، فصلنامه تخصصی پارک ها و مراکز رشد، سال نهم، شماره ۳۵.

۷. محمودی،یعقوب وهمکاران،۱۳۸۹ پایان‌نامه کارشناسی ارشد، طراحی و پیاده‌سازی نرم‌افزاری مناسب یک الگوریتم رمزنگاری بلوکی بومی بر روی کارت هوشمند؛ دانشکده فنی مهندسی،دانشگاه تربیت مدرس.

۸. مارک داجسون، دیوید گان و آمون سالتر،۱۳۹۳، مدیریت نوآوری و تکنولوژی، چاپ اول، ترجمه: دکتر رضا سلامی و فرهاد شاه میری، تهران، انتشارات بازتاب.

1. Baykal, Nazife (2011). Identifying Factors THAT Facilitate The Use Of Multi-Purpose Smart Cards By University Students: An Empirical Investigation.

2. Baregheh,A., Rowley,J., Sambrook,S., "Towards a multidisciplinary definition of innovation," Management decision, vol. ۴۷, pp. ۱۳۲۳-۱۳۳۹, .۲۰۰۹

3. Crossan, M. M., & Apaydin, M. (2010). A Multi-Dimensional Framework of Organizational Innovation: A Systematic Review of the Literature.Journal of Management Studies, ۴۷(۶), .۱۱۵۴-۱۱۹۱

4. Geroski, PA.(2000) Models of thechnology diffusion. Research Policy,.۲۹,۶۰۳-۲۵

5. Griffiths, T.L. and J.B. Tenebaum (2006) Optimal predications in everyday cognition. Psychological Science, .۴۵,۵۶-۶۳

6. Gronroos, C. (2007). Service Management and Marketing Customer Management in Service Competition. West Sussex: John Wiley & Sons Ltd.