مسیرهای جدید رمز شناسی

تهیه کنندگان :

یاشار خداقدیر مهرداد فردیار

آدرس پست الکترونیک : Yashar843@yahoo.com

چکیده

با گسترش روز افزون استفاده از کامپیوتر در زمینه های مختلف وافزایش تعداد کاربران آن در جهان اهمیت حفاظت از اطلاعات موجود در داخل کامپیوتر نیز افزایش یافته است . رمز گذاری اطلاعاتی که از راههای حفاظت اطلاعات است که بسیار مورد استفاده قرار می گیرد قرار دادن کلمه عبور برای دستیابی به اطلاعات و حتی رمز گذاری کردن اطلاعات داخل پرونده ها همگی از روشهای امنیتی هستند که به منظور پنهان نگه داشتن مطالب از دید نامحرمان صورت می گیرند. با این وجود هر روزه از گوشه و کنار دنیا خبر از افشا شدن اطلاعات سری بوسیله باز شدن قفلها و رمزها توسط افراد مختلف می‌رسد، افرادی که یا از روی سرگرمی یا از روی غرض اقدام به این گونه اعمال می کنند. پس اهمیت امنیت روشهای رمز گذاری کاملاً روشن است.

این مقاله چندین روش رمزگذاری و مخفی سازی اطلاعات را مطرح کرده است و در مورد مزایا و معایب ضریب امنیت آنها بحث کرده است. همگی این روشها مبتنی بر ریاضیات پیشرفته هستند که گاه درک این روشها برای خواننده مشکل می باشد،به همین خاطر در بعضی از موارد به اشاره ای کوتاه بسنده شده است. در بخش ضمیمه این مقاله،مقاله ای دیگر آمده است که در ارتباط تنگا تنگ با اطلاعات بخش اصلی است و در متن اصلی برای روشن شدن بیشتر مطالب در برخی نکات ، خواننده به بخش ضمیمه ارجاع داده شده است. مطالب ضمیمه ، به صورت کار بردی تر و عینی تر نسبت به مطالب بخش اصلی هستند و همگی به صورت اشاراتی کوتاه بیان گردیده اند ، لیکن لازمه درک آنها مطالعه بخش اصلی در ابتدا میباشد.

کلمات کلیدی:

دستگاه مخابره حروف رمز :dispenser

رمز گشایی کردن decipher: یادداشت یکبار مصرف: one – time pad:

دوسوئی- یک به یک bijective: محرمانه بودن secrecy:

کلید عمومی public key: ورود- اجازه ورود login:

کلمه عبور یکبارمصرف one – time password:

رمزگذاری encryption: زیست سنجی biometrics:

ناشناس ماندن:Anonymity به رمز درآوردن: encipher

اعتبار – صحت:authenticity رمز شناسی: cryptography

مقدمه

امروزه، با ارزان شدن سخت افزارهای دیجیتالی ، کاهش محدودیت های طراحی و کاهش هزینه ها از انواع روشهای گوناگون رمز گذاری در کاربرد های روزانه مانند تلگراف ، ترمینالهای کامپیوتری و .... استفاده می شود و هر روزه نیاز های جدیدی از این نوع سیستم ها احساس می گردد و این هنر باستانی (رمزگذاری مطمئن) را به شاخه ای از علوم تبدیل کرده است از طرفی توسعه کامپیوتر ها،ارتباطات شبکه ها را کنترل کرده و خبر ا ز ایجاد ارتباطات راحتتر ، ارزان تر و سریعتر میان افراد (یا کامپیوترهای) در آن سوی جهان داده است و این ارتباطات جایگزین بسیاری از سفرها و مکاتبات شده است. اما این ارتباطات باید در مقابل مسایلی نظیر استراق سمع و تزریق غیر مجاز اطلاعات امن باشد از طرفی رمز گذاری معاصر استفاده از شروطی را که باعث مزاحمت server ها بر روی سیستم کاربر و یا حذف از مزایای Teleprocessing شود نمی دهد.

مهمترین مسأله شناخته شده در رمزگذاری محرمانه بودن مطالب است یعنی از استخراج غیر مجاز اطلاعات در یک کانال نامطمئن جلوگیری شود به همین منظور رمزگذاری برا ی بیمه کردن امنیت اطلاعات به کار می رود اگر چه این پدیده نیاز به ارتباط میان اجزای ارتباطات دارد تا با این تقسیمات ، کلید رمزگذاری برای دیگران قابل شناسایی نباشد در حالت معمولی این کار با فرستادن یک کلید از طریق یک کانال مطمئن می باشد.

بخش سوم دو ابزار برای انتقال کلیدهای ارتباطی (تغییر شکل) از طریق کانالها مطرح می سازد روش رمزگذاری با کلید عمومی مخفی سازی E و کلید آشکار سازی D که از طریق جداگانه اداره می شود که محاسبه D از روی E تقریباً غیر ممکن است (مثلاً به $۱۰^{۱۰۰}$ دستور العمل نیاز دارد)

و با کاربرد این مطلب هر کار بری از سیستم می تواند پیغامی را به صورت محرمانه به شخصی دیگر بفرستد فقط و فقط به این قصد که او بتواند آن را آشکار کند. همچنین کلید عمومی رمزگذاری اجازه استفاده از چند نوع رمز را نیز می دهد.

وقتی شخصی پیغامی را به دیگری به صورت (رمز گذاری و ترکیب مخفی سازی) می فرستد گیرنده با استفاده از کلید عمومی ومخفی خودش آنرا رمزگشایی می کندهمچنین دراین مقاله روشهایی برای توسعه کلیدهای عمومی سیستم رمزگذاری مطرح می شود اما مسأله هنوز به صورت گسترده مطرح است.

سیستم های توزیع کلیدهای عمومی ابزارهای مختلفی را برای رفع نیاز به کانالهای توزیع کلید های امنیتی پیشنهاد می کند. مسأله دیگر استراق سمع کردن بر روی مبادلات (مثلاً کلیدها) می باشد که باید آن را پیدا کرد همچنین در مسئولیت را حل رمزگذاری ، مسأله

تشخیص صحت ها در انتقال اطلاعات در ارتباطات تجاری همزمان می باشد که باید قدرت انتقال ، ذخیره سازی قرار داد و امضا را داشته باشد و بتوان از آن در دادگاه استفاده کرد. به منظور داشتن یک جابجایی صرفاً دیجیتالی بجای ابزارهای کاغذی هر کابری باید پیغامی را ،ایجاد کند که صحت آن توسط کاربران دیگر قابل تشخیص باشد و در عین حال نتواند پیغامی را از طرف شخص دیگری حتی گیرنده ایجاد کند.

بخش چهارم در مورد مسأله ایجاد یک پیغام همراه با امضای معتبر بحث می کند وبه بررسی مسأله تشخیص صحت ارائه بعضی از راهکارها و همچنین در مورد انتقال کلید عمومی سیستم رمزگذاری از طریق سیستم تشخیص صحت می پردازد .

در بخش پنجم به رابطه شیوه های مختلف رمزگذاری و مسأله ایجاد تله های ورودی می پردازد از این رو افراد به دنبال کدهای کشف نشدنی در تحقیقات رمزگذاری می باشند مثلاً در سال ۱۹۲۰ one time pad سیستمی شکست ناپذیر محسوب می شد ولی ۲۵ سال بعد این نظریه نقض شد . از این رو با نتایج حاصل از نظریه ارتباطات و محاسبات امنیت سیستم ها ی کلاسه شده را ، برای زمانی (معین) افزایش داد د ربخش بعدی با اصطلاحات و تحدیدهای محیطی تعریف شده در سیستم های امنیتی آشنا می شوید.

قواعد رمزگذاری

رمزگذاری ، مطالعاتی از سیستم های ریاضی به منظور امنیت محرمانه بودن اطلاعات و درستی آنها می باشد این سیستم محرمانه ازتزریق یا استخراج اطلاعات بوسیله اشخاص غیر مجاز در کانال عمومی جلوگیری می کند و به فرستنده اطمینان می دهد که پیغام توسط شخص مزبور فقط خوانده می شود کانالی که به عنوان کانال عمومی در نظر گرفته می شود با توجه به نیازهای کاربرانش از امنیت کافی برخوردار نمی باشد.

و هر کانالی بسته به کاربردهای آن ممکن است توسط استراق سمع ، تزریق (یا استخراج اطلاعات) و یا هر دو ، مورد تحدید قرار گیرد. در بیشتر مواقع مسأله تشخیص صحت به دو قسمت تشخیص صحت متن و صحت کاربر تقسیم می شود که smart card نمونه ای از مسأله صحت کابر می باشد مثلاً در مورد شخصی که ادعا می کند شخص A می باشد سیستم تشخیص صحت فقط معلوم می کند که پیغام را چه کسی فرستاده است در اینجا فقط یک پیغام تلویحی نیز وجود دارد یعنی من کاربر A نمی باشم . این تفاوت رفتار محیطی بعضاً مشکلاتی را ایجاد می کند.

در این مباحث سه موضوع انتقال دهنده ، گیرنده و استراق سمع کننده وجود دارد مثلاً فرستنده یک plaintext و یا یک متن رمزگذاری نشده مانند P ایجاد می کند تا از طریق یک کانال (معمولاً نامطمئن) فقط به گیرنده حقیقی انتقال یابد برای اینکار فرستنده با ایجاد تبدیلی معکوس پذیر متن رمزگذاری شده C را ایجاد می کند یعنی ($C=S_K(P$) که کلید K فقط برای گیرنده حقیقی از طریق یک کانال امن ارسال می شود مادامی که گیرنده حقیقی کلید K را می داند می تواند C را با تبدیل معکوس رمزگشایی کند یعنی

$S_k^{-1}(c) = S_k^{-1}(S_k(p)) = p$ که P همان متن اصلی است

توجه به این نکته مهم است که برای انتقال خود P به علت تأخیر زمانی یا محدودیت ظرفیت کانال با خود کانال امن امکان پذیر نیست .

در $S_k : \{p\} \rightarrow \{c\}$ متن plaintext همان P و پیغام رمزگذاری نشده همان C و S_K تبدیلی معکوس پذیر می باشد و K کلید انتخاب شده می باشد در بیشتر مواقع که ما از سیستم های رمزگذار نام می بریم فقط به K اشاره می کنیم .

هدف نهای طراحی سیستم رمز گذاری $\{S_k\}$ارزان بودن عملگرهای رمزگذاری ،آشکار سازی و رمزگشایی می باشد در عین حال موفقیت عملکردهای آن بستگی به پیچیدگی و اقتصادی بودن آن دارد برای این موضوع دو ابزار وجود دارد .

۱- computionally secure

۲- unconditionally secure

می دانیم از مهمترین وظایف این سیستم ها محاسبه هزینه کشف رمز می باشد که سیستم اول در برابر حمله‌ای که منجر به محاسبات نامحدود شود از پا در خواهد آمد در صورتی که سیستم دوم مقاوم بوده و در برابر حمله اجازه محاسبات را نمی دهد .

سیستم unconditionally secure در بخش سه و چهار مورد بحث قرار می گیرد و قسمتی از تئوری اطلاعات است که نظریه شانون نامیده می شود نتایج unconditional secure حاصل چندین cryptogram می باشد این سیستم یکی از کابردهایش one time pad می باشد که یک متن را باعددی تصادفی به همان طول ترکیب می کند این سیستم تضمین کننده امنیت است ولی دربازه وسیع تر به تعداد زیادی کلید نیاز دارد از این رو برای بسیاری از کاربردها غیر عملی می باشد.

در این مقاله سیستم های compua tionally secure مادامی که کاربردهای کلی و وسیع دارد مورد بحث قرار می گیرد .

وقتی ما درباره نیاز به توسعه قابل اثبات (دست یافتنی) به سیستم های رمزگذاری امن می پردازیم عملاً سیستم هایی را که مانند one time pad کاربرد وسیعی ندارند کنار می گذاریم و به تعداد کمی سخت افزارهای دیجیتالی می اندیشیم که برای کلید فقط نیاز به چند

صد بیت دارند و همچنین ابزارهایی که از تعداد کمی سخت افزار دیجیتالی و یاچند صد خط نرم افزار تشکیل شده باشد ما این کار راcomputionally infeasible می نامیم اگر سنجش هزینه براساس مقدار حافظه بکار برده شده و یازمان اجرای محدود باشد. بسیاری از اصلاح خطای کدها بوسیله کدهای کانولشن و کدهای بلوک انجام می پذیرد . سیستم های رمزگذاری به دو طبقه جامع تقسیم می شوند:

۱- جریانی از رمزگذاری ۲- بلوکهایی از رمز گذاری

جریان رمزگذاری شامل قطعات کوچکی (از بیتها یا کاراکترها) می باشد که تولیدات ما از کنار هم قرار گرفتن ترتیبی بیت های تصادفی که به ماژول ۲ بیتیهای متن اضافه شده اند تشکیل می شود . بلوکهای رمزگذاری به عنوان ترکیب ضعیفی (کوچکی) از متد بلوکهای متن می باشند دراین روش تغییری کوچک در ورودی بلوک تغییرات اساسی در نتایج خروجی ایجاد می کند در این مقاله مقدمتاً در مورد بلوکهای رمزگذاری بحث می شود زیرا خصوصیت انتقال خطاها در بسیاری از کاربردهای تشخیص صحت قابل ارزیابی می باشد.

در یک سیستم قابل اعتماد رمزگذاری برای تضمین درستی پیغام دریافت شده از جانب گیرنده به کار می‌رود و از تزریق اطلاعات از جانب افراد فضول و همچنین از پیغام درکانال ارتباطی محافظت کند و یک سیستم رمزگذاری کلاً به تضمین خصوصی سازی توجه دارد.

برای تضمین صحت پیغام، اطلاعاتی از پیغام ، کلید مخفی ، تاریخ و زمان آن به یک تابع داده می شود به عنوان مثال: با دنبال کردن تاریخ ، زمان و رمزگشایی هر پیغام به صورت کاملاً ترتیبی ، پیغام حاصل می شود.این کار اطمینان می دهد فقط شخصی که پیغام را ایجاد کرده است تابع شامل تاریخ و زمان دقیق رمزگذاری میباشد باید توجه داشت که در این کار حتی تغییر ناچیزی در متن رمزگذاری شده تغییرات زیادی در نتایج (خروجی) ایجاد می کند باید در نظر داشت که اگر به متن در یک کانال نا امن noise تزریق شود متن تغییر و خطا انتقال می یابد.

اولین ارزیابی کافی بودن سیستم های رمزگذاری و طبقه بندی رفتارهای آنها در معرض موارد مختلف می باشد پیروی از این رفتارها می تواند برای هر یک از موارد مخفی سازی یا تشخیص صحت در سیستم های رمزگذاری به کار رود.

یک متن رمزی بخاطر کشف رمز مورد حمله قرار می گیرد و این عمل معمولاً تا کشف رمز ادامه دارد یک plain text به خاطر کشف رمزش مورد حمله قرار می گیرد و معمولاً تا کشف رمز ادامه دارد .در کشف نوشته رمزی معمولاً از اطلاعات آماری مثلاًدر زبان

انگلیسی ۱۳ در صد امکان دارد که حرف مورد نظر e باشد یا از کلمات ویژه ای که احتمالاً به کاربرده می شود (مانند نامه احتملاً با Dear sir آغاز می شود) برای طراحی یک سیستم رمزگذاری باید این نقاط ضعف را سازنده ، د رنظر داشته باشد .

به منظور اینکه سیستمی امن در نظر گرفته شود فقط اختصاص دادن یک مدل منطقی که توسط سیستم رمزگذاری اجرا شود کافی نیست . د رسیستم های مختلف از الگوریتم های مختلفی استفاده می شود اما باید حمله کاربران غیر مجاز به متن را تشخیص دهد .

برخلاف مزایای زیادی که برای سیستم های شناسایی identi fication)) درنظر گرفته می شود بعضاً خطاهای بزرگی رخ می دهد.

هدف اصلی سیستم های رمزگذاری شناسایی را حت تر و سریع تر است . معمولاً plain text که مورد حمله قرار می گیرد IFF نامیده می شود که ریشه این اصطلاح از جنگ جهانی دوم در شناسایی سیستم ها یا افراد دوست بوده است یک سیستم IFF که متعلق به رادار باشد می تواند بصورت خودکار دوست را از دشمن تشخیص دهد مثلاً رادار نوعی موج را به هواپیما می فرستد با توجه به مدت زمان رفت و برگشت موج فاصله هواپیما تشخیص داده می شود و خلبان در برابر موج پاسخ می دهد که معلوم می شود هواپیمای خودی می باشد هنگامی که هواپیمای دشمن به منظور انجام حملات تروریستی به ناحیه را دارد وارد می شود رادار موجی می فرستد و چون رمز مربوطه از طرف خلبان فرستاده نمی شود معلوم می گردد که هواپیمای دشمن است یعنی رادار نیز ترکیبی از سیستم تشخیص صحت و یک کلید می باشد در سیستم های رمزگذاری هم معمولاً از این ترفند استفاده می شود.

روشهای دیگری نیز برای تشخیص صحت (authentication) در قراردادهای رمزگذاری وجود دارد ولی ما نیاز به منابع جدید، ایده ها و تکنیکهایی داریم که در این مقاله توضیح داده خواهد شد. همچنین در مورد تکنیکهایی که درمقابل برداشت اطلاعات توسط افراد غیر مجاز از سیستم حمایت می کند و از انکار افراد جلوگیری می کند نیاز داریم. یعنی یک متن ممکن است فرستاده شود اما بعدها گیرنده یا انتقال دهنده منکر دریافت یا انتقال آن شود یا هر یک از اجزای پیغام فرستاده شده بی دلیل اظهار کنند که در زمان ارسال وجود نداشته اند بنابراین ما به امضاهای دیجیتالی حقیقی و اعلام وصول پیغام نیاز داریم به عنوان مثال یک دلال بورس متقلب تلاش می‌کند، با جعل سند با پول مشتری به خرید و فروش (غیرمجاز) بپردازد امامشتری هرگونه درخواستی (حقیقی) را رد کند در صورتی که بعداً می بیند از پولش کم شده است .

ما درمورد این مفهوم که به گیرنده اجازه می دهد که صحت و سقم پیغام را تأیید کند اما از ایجاد چنین پیغامی از طرف گیرنده جلوگیری کند. بنابراین از آنکار گیرنده و یا از سازش داده های authentication گیرنده جلوگیری می کند.

کلیدهای عمومی رمزگذاری

همانطور که می دانید رمزگذاری نوعی از ابزارهای امنیتی می باشد همین که یک کانال امنیتی در امتداد کلیدهایی که باید انتقال یابند بوجود می آید این کانال امنیتی می تواند به کانالهایی با ظرفیت بالا یا تأخیر کمتر توسعه پیدا کرده باشد. که نتیجه، انتقال پیغام از طرف آنها است.

علت اینکه از مزایای رمزگذاری در ارتباط میان افراد استفاده نمی شود مقید بودن این سیستم ها به وسایل زیادی برای امنیت رمزگذاری می باشد. بخاطر توسعه بیشتر امنیت سیستم های ارتباط از راه دور باید (موضوع تجهیزات فراوان این سیستم) تغییر کند.
اگر n کاربر وجود داشته باشد $\frac{(n^2-n)}{2}$ حالت وجود دارد که اشخاص با یکدیگر به صورت خصوصی ارتباط برقرار کنند.

اگر بخواهیم برای هر جفت از این کار بران که آشنایی زیادی باهم ندارند بوسیله ابزارهای فیزیکی کلیدهای ارتباطیشان را ارسال کنیم آنها مدت زمان زیادی معطل می مانند در صفحات بعد نویسنده ابزارهایی را که نیاز به خود روشهای جدید رمزگذاری ندارند اما باعث کاهش پیدا کردن امنیت ، مزاحمت و محدود یتهای شبکه های ستاره ای از لحاظ پروتکل های امضا کردن می باشد توضیح می‌دهد ما راه حلی را از سیستم توسعه یافته پیشنهاد می کنیم که شامل دو قسمت است وفقط از طریق یک کانال عمومی و کار برد یک تکنیک عمومی شناخته شده که می تواند یک ارتباط خصوصی ایجاد می کند، انجام می گیرد.

ما برای این مشکل دو ابزار را امتحان کرده ایم که کلید عمومی سیستم رمزگذاری و سیستم توزیع کلید های عمومی مجاز نامیده می شود که بخش اول بسیار نیرومند است و خودش راه حلی برای مسأله تشخیص صحت می باشد در صورتی که دومی به درک و فهم نزدیک تر است .

یک جفت از کلیدهای عمومی سیستم رمزگذاری خانواده از{K} E_K {K} و D_K {K}الگوریتم هایی از تبدیل معکوس می باشند:

D_k:{M}------{M E_K: {M}----{M}

یک متن محدود (از لحاظ فضا) مانند {M}

۱) برای هر K عضو مجموعه E_K (K({K}) معکوسی از D_K می باشد .

۲) برای هر K عضو مجموعه K و هر متن M عضو مجموعه M{}) الگوریتمهای D_K, و E_K به راحتی محاسبه می شوند.

۳) برای بیشتر k ها محاسبه D از روی E نشدنی می‌باشد

٤) برای هر عضو K مجموعه K{}) محاسبه معکوس E_K وD_K با K امکان پذیر می باشد.

E_K و D_K را تولید می کند که خروجی هستند . در یک چنین سیستمی مشکل کلیدهای توزیع ، زیادی نمونه‌ها می باشد هرکار بری یک جفت از تغییرات معکوس E وD را ایجاد می کند و تبدیل رمزگشایی D باید محرمانه باشد اما هرگز نیازی به ارتباط با کانالها ندارد.

کلید E کلید عمومی است که در یک فهرست عمومی در امتداد با نام و آدرس User می باشد.

از این رو کلید عمومی سیستم رمزگذاری می تواند در خصوص اجازه دستیابی چندین رمز باشد مثلاً شخص پیغامی را با توجه کلید، آن را کشف می کند و برای کابران دیگری فرستد شخص دیگر با توجه به آن کشف رمز نمی تواند متن های دیگر را ترجمه کند و حمایت از این کلید با توجه به ماهیت طبیعی فایل ها راحت است .

بنابراین یک سیستم رمزگذاری از دو قسمت تشکیل شده است .

خانواده ای از تغییر شکل های کشف نوشته رمزی و خانواده ای از راههای تغییر شکل رمزگشایی که به هر یک از اعضا، یک خانواده اختصاص داده می شود بنابراین دادن عضوی از یک خانواده (به خانواده دیگر) مطابق پیدا کردن عضوهای دیگر، شدنی می باشد.

اصل چهارم تضمین می کند که راهی برای محاسبه تبدیلات معکوس وقتی که عمل کشف رمز و رمز گشایی در فشار نباشند وجود دارد.

در عمل تجهیزات یک سیستم رمزگذاری باید شامل یک تولید کننده صحیح اعداد تصادفی باشد (به عنوان مثال در یک محیط noisy مانند دیود) این الگوریتم وروش protect write در مقایسهبا Protect Read مکانیزم اقتصادی است که به کار گرفته می شود.

به عنوان مثال یک کلید عمومی برای کشف plaintext با برداری باینری به ابعاد n در m و بوسیله ماتریس n*n نمایش داده می شود که $D=E^{-1}$ و برای عمل کشف رمز و رمزگشایی به n^2 عملگر نیاز داریم و محاسبه D از روی E ، با چنین ماتریسی ، مسأله سختی است و محاسبه معکوس ماتریس n^3 عمگر دارد نسبت زمان رمزگذاری (مثلاً محاسبه D از روی E) زمان برای کشف یا رمز گشای بیشتر از n و سایز بلوکها بیشتر از $۱۰^{۶}$ خواهد شد .

بیشترین مورد عملی برای یافتن E و D با استفاده از الگوریتم معکوس است و تحلیل تبدیل D به E در زبان سطح پایین مشکل است. مثلاً در برنامه هایی که از متغییرها و جملات اضافی و غیر ضروری استفاده می کنند تعیین الگوریتم معکوس می تواند خیلی پیچیده باشد. البته E هم می تواند به اندازه کافی پیچیده شده باشد تا از شناسایی ورودی و خروجی در امان باشد . کامپایلر راهی برای اجرای برنامه می باشد.کامپایلر راهی است که مراحل کامپایل را انجام می‌دهد اما جریان پردازش شدنی نیست (دراختیار افراد نیست و درکاربرد برنامه ها تنها سایز برنامه و زمان اجرا مهم نیست .

در بخش اول مطالعات جداگانه ای در مورد مسأله توزیع کلید ها از طریق یک کانال نا امن انجام گرفت که با کلید عمومی سیستم رمز گذاری که پیشنهاد شده است متفاوت است ولی به همه آنها سیستم توزیع کلید های عمومی اطلاق می شود.

هدف اصلی دو کاربر A و B انجام محرمانه تغییر کلید از طریق یک کانال نا امن می باشد پس این کلید از طرف هر دو کاربر در یک سیستم نرمال برای decipher و encipher به کار می رود.

Merkle روشی است که در یک سیستم که n کاربر مجاز وجود دارد هزینه به اندازه n^2 رشد می کند متأسفانه هزینه کاربران،بسیار بیشتر از زمان انتقال (مثلاً محاسبات) می باشد زیرا در پروتکل Merkle باید n کلید قبلاً انتقال یافته باشد تا براساس آن کلید فعلی با آن سنجیده شود بااین حال روش Merkle درعمل بسیار کارا می باشد اگر فقط یک مگا بایت فضا بر روی پروتکل setup باشد از این تکنیک می توان نسبت هزینه را تقریباً از ۱۰۰۰۰ به ۱ کاهش داد زیرا بسیاری از کاربردها (دستورات) کوچک تر می شود.

اگر یک باند با پهنای زیاد با اتصال داده ها درآن در دسترس و ارزان باشد نسبت بالا، از میلیون به یک کاهش می یابد و می توان کار بیشتری را انجام داد و این سیستم ، یک سیستم طبیعی می باشد.ما

ما حالا یک سیستم جدید توزیع کلیدهای عمومی را که چندین ویژگی دارد را پیشنهاد می کنیم اولاً به یک کلید نیاز دارد که قابل تغییر کردن است .ثانیاً : کوشش برای کشف رمز به صورت توانی،افزایش می‌یابد(برای n کاربر ،تعداد حالتها توانی از n می‌باشد)

ثالثاً : استفاده از فایل عمومی

یک فایل عمومی ساخته شده ذاتاً می تواند از روی حافظه خوانده شود و ارتباط کاربران باعث می شود که در بسیاری از زمانها برای کاربران زیادی درستی شناسه کاربر تأیید شود.

Rkle این تکنیک نیاز به کار برانی مانند A و B دارد که به صورت فعال همدیگر را با ابزارهای دیگری تأیید کنند. این تکنیک جدید صرفاً در محاسبات پیچیده لگاریتمی از طریق یک فیلد محدود GF(q) با عددی به نام q می باشد .

$$Y = \alpha^x \bmod q \quad , \quad 1 \le X \le q-1$$

که α یک مقدار ثابت ،از عنصر اولیه GF(q) می باشد پس حاصل لگاریتم Ymodq در مبنای α برابر X می باشد .

$$X = \log_{\alpha}^{Y \bmod q} \quad , \quad 1 \le Y \le q-1$$

بنابراین محاسبه Y از X آسان و برابر با حاصل ضرب $2X \log_2^q$ می باشد .

و برای محاسبه X از روی Y باید به انتخاب q بسیار توجه نمود.

امنیت این سیستمها بستگی به قطعیت امنیت محاسبات لگاریتمی q دارد. و اگر ترکیبی از $\log_2^q$ پیدا شود در آن صورت رمزگشایی آسان خواهد شد و به دلایل مختلف برای این الگوریتم،لگاریتم modq (عبارت) بهترین انتخاب ..... می باشد که ابزاری برای مسایل ترکیبی می باشد .

کاربران مختلف به صورت مستقل عددی را به صورت تصادفی از مجموعه {q.-1,.....,۱،۲} انتخاب می کنند که یک کلید مخفی مانند Xi ایجاد می شود.

در اینجا $Y_i = \alpha^{x_i} \bmod q$ فایل عمومی با نام و آدرس خودش می باشد وقتی کاربر i تمایل به ایجاد رابطه خصوصی دارد آنها از $k_{ij} = \alpha^{x_i x_j} \bmod q$. استفاده می کنند به عنوان کلیداستفاده میکنند.

و روابط زیر وجود دارد (برای کاربر) $k_{ij} = \alpha^{x_i x_j} \bmod q$ همین متد $k_{ij} = Y_j^{x_i} \bmod q = (\alpha^{x_j})^{x_i} \bmod q$. و در نتیجه برای کاربر j وجود دارد یعنی $k_{ij} = Y_i^{x_j} \bmod q$ و کاربر دیگر با محاسبه Yj ,Yi می تواند Kij را بدست آورد .

به عنوان مثال $k_{ij} = Y_i^{(\log yj)} \bmod q$.

بنابراین ما می بینیم اگر لگاریتم مد عبارت به راحتی محاسبه شود به راحتی نیز شکسته می شود می دانیم اگر q کمتر از ۲ باشد می توان آن را در n بیت نمایش داد و حاصل ضرب آن بیشتر از b 2 می باشد مثلاً b=200 باشد به بیشتر از ٤۰۰ بار عمل کردن برای محاسبه Yi از Xi یا Kij از Yi و Xj نیاز داریم .

اثبات صحت یک سویه

اثبات صحت قلب سیستمهایی است که با قراردادها و صورتحسابها سروکار دارند و بدون آن معاملات قابل انجام نیستند.

سیستمهای فعلی تأیید صحت الکترونیکی توانایی تأمین احتیاجات را برای امضاهای متنهای دیجیتال را بصورت کامل وغیر قابل جعل ندارند. آنها تنها می توانند از فعالیت بخش سوم جاعلان جلوگیری کنند. اما نمی توانند از بحثهای بین گیرنده و فرستند جلوگیری کنند.

به منظور توسعه یک سیستم که قادر به جانشینی معاملات نوشته شده جاری با چند ارتباط صرفاً دیجیتال باشد، ماباید دنبال یک وسیله دیجیتال باشیم که عملکردی مشابه امضای نوشتاری داشته باشد. بر همگان واضح است که امضا،یک وسیله تصدیق صحت می باشد و برای دیگران ایجاد آن امضا منع قانونی دارد. ما به چنین تکنیکی" اثبات صحت یک سویه" می گوییم .

مانند هر سیگنال دیجیتال دیگر که می تواند به دقت کپی شود، یک امضای دیجیتال واقعی هم باید بدون آنکه شناخته شود قابل تشخیص (مشخص شود که امضا متعلق به چه کسی است) باشد.

مفهوم اجازه ورود (login) در کامپیوترهایی که چند کار بر دارند . شخص وقتی که هزینه لازم برای استفاده را پرداخت،یک اسم رمز دریافت می کند که مستقیماً وارد دایرکتوری اسامی رمز سیستم میشود.هر بار که کاربر وارد می شود از او خواسته میشود تا اسم رمز خود را وارد کند. با مخفی نگه داشتن اسامی رمز از دید دیگران از ورود افرادغیر مجاز جلوگیری می شود. اگر چه فراهم کردن امنیت دایرکتوری اسامی رمز لازم است ، با توجه به اینکه اطلاعات داخل آن اجازه اعطای شخصیت به هر یک از کاربران را می دهد ، ولی مشکل زمانی ایجاد می شود که متصدیان سیستم دلایل قانونی برای دسترسی به این دایرکتوری داشته باشند. مجوز دادن به دلایل قانونی و منع کردن بقیه از دسترسی به این دایرکتوری تقریباً غیر ممکن است . این امر منجر به دستیابی به یک سری امکانات ظاهراً غیر ممکن برای این روش ورود جدید می شود که قادر باشد بین صحت اسامی رمز به قضاوت بنشیند. بدون آنکه آنها را بشناسد. وقتی یک کار بر برای اولین بار اسم رمز خود (PW) را وارد می کند، کامپیوتر به طور اتوماتیک و شفاف تابع F(pw) را محاسبه و آن را ذخیره می کند و نه همان PW را محل ذخیره سازی تابع F(pw) همان دایرکتوری اسامی رمز است. درهر ورود موفق ، کامپیوتر تابع F(X) را محاسبه می کند که در آن X اسم رمز پیشنهادی و سپس مقدار F(x) با مقدار ذخیره F(pw) مقایسه می شود، اگر و فقط اگر این مقادیر مساوی بودند کاربر مجوز ورود پیدا می کند. از آنجا که تابع F باید هر بار که کار بر قصد ورود دارد محاسبه شود پس زمان محاسبه آن باید کوتاه باشد. یک ملیون دستورالعمل برای محاسبه F(pw) شاید مناسب باشد چراکه اگر کسی بخواهد از روی دایرکتوری اسم رمز ها با محاسبه معکوس تابع F(F) به کشف رمز بپردازد مجبور به انجام محاسباتی معادل $۱۰^{۳۰}$ دستورالعمل خواهد بود و در نتیجه از این کار ناتوان خواهد بود .توجه کنید که :F(F(pw)) برای برنامه ورود به عنوان اسم رمز پذیرفته نیست تازمانی که F(F(PW)) به صورت اتوماتیک محاسبه شود که این مقدار هم دیگر با مقدار F(pw) که دردایرکتوری اسم رمز ذخیره گردیده برابر نیست.

فرض می کنیم که تابع f شامل یک سری اطلاعات کلی باشد که باعث پیچیدگی آن نشود تا محاسبه F^{-1} ساده باشد . این توابع ، توابع یک سویه خوانده می شوند . با دقت بیشتر مشخص می شود که تابع یک سویه ، تابعی است که به ازای هر X در دامنه آن محاسبه F(x) ساده باشد، به همچنین ، تقریباً برای تمام Y های موجود در برد این تابع محاسبه تساوی Y=F(x) برای پیدا کردن X مناسب ، غیر ممکن باشد دقت کنید که ما بدین طریق تابع F را تابعی معکوس ناپذیر تعریف کرده ایم . اما مسأله این است که چنین تابعی در ریاضی وارد کردن مقدار به آن و محاسبه آن ازدیگر توابع متفاوت است .

تابع F به طور معمول ، تابع >> معکوس ناپذیر << خوانده می شود. در واقع وقتی که به ازای هر Y موجود در برد تابع یک X یکتا در دامنه تابع وجود نداشته باشد (برا ی مثال $(f(x_1)=y=f(x_2$) ما تأکید می کنیم که این همان سختی در معکوس پذیری که مدنظر می باشد ، نیست . چراکه این کار (معکوس کردن تابع) باید بسیار مشکل باشد . اگر f یک تابع معکوس ناپذیر باشد این کار پیدا کردن یک تصویر معکوس از آن را ساده تر ممکن است بکند. یعنی اگر به ازای تمامی X های موجود در دامنه $F(x)= Y_0$ باشد پس $\{Y_0\}$ برد تابع F است و ما می توانیم هر X را به عنوان $(F^{-1}(Y_0$ بگیریم . پس به ناچار لازم است که تابع قابلیت فاسد شدن نداشته باشد (یعنی بتوان بعد از یک بار مصرف دوباره به آن مقدار داد) درجات خفیف توابع فاسد شدنی برای کار ما نسبتاً خوب است که در این مورد در بخشهای بعدی بحث خواهد شد چند جمله ای ها نمونه ای از توابع یک سویه را ارائه می دهند . به طور مثال پیداکردن ریشه X_0 در معادله $P(x)=y$ بسیار سخت تر است از پیدا کردن ریشه در $X_0=X$.توسط بعضی از دانشمندان استفاده از چند جمله ای های اسپارس با درجات بالا در زمینه های محدود توصیه شده است . در مورد مباحث ریاضی در این مورد بعداً بحث خواهد شد.

در هر حال، راه حل توابه یک سویه فقط بعضی از مشکلات ورود به سیستمهای چند کاربره را حل می کند. این تنها از مصالحه بخش تشخیص هویت سیستم واطلاعات در هنگامی که سیستم خاموش است خبر می دهد. اما همچنان نیاز به وارد کردن اسم رمز به طور صحیح توسط کاربران دارند. جلوگیری از ورود غیرمجاز نیاز به یک رمز گذاری اضافی دارد.

کلید اصلی رمزگذاری برای تولید یک تابع یک سویه واقعی به شرح زیر مورد استفاده قرار می گیرد.

اگر کاربر A بخواهد پیام M را به کاربر B ارسال کند آن را توسط روش کد گذاری خود، رمزگذری گذاری می‌کند و به این طریق کاربر B که پیام را دریافت می کند مطمئن می شود که پیام از کاربر A رسیده است .

اثبات صحت پیام های توابع یک سویه راه حل های جزئی دارند علت جزئی بودن راه حل آن است که تقریباً نیاز به بسط دادن به ۱۰۰ زمینه داده ای دارد. اگر چه یک تغییر جزئی مشکل گسترش را وقتی N یک مگا بیت یا بیشتر باشد را رفع میکند.

فرض کنید g یک تابع یک سویه از فضای دو دویی N به فضای دودویی n باشد جایی که n تقریباً ۵۰ بیت است . اجازه بدهید پیام N بتی m که تابع g روی آن اعمال شده است را بردارM بنامیم . سپس روش قبلی را برای ارسال M استفاده کنید و اگر $n=10^6$ و $n=50$ و ۱۰۰ باشد این عمل ۵۰۰۰ پارامتر اثبات صحت را به پیام می افزاید . بنابراین این متضمن ۵ درصد گسترش در طول انتقال است . حتی اگر تعداد زیادی از پیامهای دیگر موجود باشد(به طور میانین ۲^{n-N}) در یک مرحله اثبات صحت ، غیر قابل پیدا کردن و رمزگشایی می شود . در واقع تابع g از یک سویه معمولی قوی تر است . حتی اگر m نیز به آن داده شود پیدا کردن تصویر معکوس دیگری از m کار

سختی است . پیدا کردن چنین توابعی کمی با مشکل همرا ه است . یک راه حل جزئی دیگر برا ی توابع یک سویه موجود است . کاربر اسم رمزی را تولید می کند که برای خودش محفوظ است، اوبه سیستم $F^T(X)$ را می دهد ، جایی که یک تابع یک سویه موجود است .درزمان مشخص t تابع مناسب $F^{T-t}(X)$ است که میتواند چک شود توسط فراهم کرد $F^t(X)$ بوسیله سیستم .

به خاطر تابع یک سویه F ، پاسخها ارزشی برای جعل ندارند. مشکل این راه حل این است که نیاز به محاسبات زیادی برای یک ورود قانونی دارد. برای مثال t هر ثانیه افزایش پیدا می کند و سیستم باید کار کند برای یک ماه بر روی هر اسم رمز تا آنگاه T=2.6 شود . هم کاربر و هم سیستم با ید تابع F را بر هر ورود ۳/۱ ملیون بار تکرار کنند . پس این امکان عدم موفقیت استفاده از این روش را به طور آشکار رد می کند. مشکل قابل حل خواهد بود اگر ، یک روش ساده تر برای محاسبه $f^{(2^n)}$. برای n= 1,2 ... پیدا شود . به هر حال محاسبه سرعت محاسبه $F^{(n)}$ استفاده از روش توابع یک سویه را منتفی می کند.

مشکلات Trap Doors , Interrelation

در این بخش ، ما نشان خواهیم داد که بعضی از مشکلات رمزگذاری قابل کاهش خواهد بود. در بخش قبل گفتیم که سیستم رمزگذاری به امنیت کمک می کند البته فقط در برابر تهاجمات رده سوم جاعلان . این چنین سیستم رمزگذاری می تواند سایر بخشها را به خوبی ایجاد کند.

یک سیستم رمز گذاری که د ربرابر حملات یک main text شناخته شده بتواند مقاومت کند می تواند برای تولید توابع یک سویه نیز بکار رود.

بحث در مورد دلایل آن با جزئیات لازم نیست . برای یک تابع به طور اصولی این امکان پذیر است که از یک تحقیق از توابع ممکن درمجموعه توابع یک سویه یک بهره دهی خوب برای رمز گذاری داشته باشد. این مطلب بایک تابع نمایی مجزا امکان پذیر است . توابع یک سویه پایه های رمز های بلاکها و تولید کنندگان کلید هستند. کلید ساز، یک بیت ساز تصادفی است که خروجی آن رشته ای از کلیدها است که به یک پیام دودویی اضافه می شود(در تقلید از روش one-time-pad) کلید به عنوان بذری برا ی تعیین ترتیب تصادفی رشته ، کلیدها استفاده می شود. حمله متن رمز نشده plain text)) به حد تشخیص یک کلید از یک رشته کلید تقلیل پیدا کرده

است . برای سیستمی که می خواهد امن باشد، محاسبات لازم برای پیداکردن یک کلید از یک رشته کلید باید بطور قابل ملاحظه ای نشدنی باشد. البته در صورتی که ، سیستم قابل استفاده و مفید باشد این محاسبه باید ساده باشد.

بنابراین یک تولید کننده کلید خوب تقریباً یک تابع یک سویه تعریف می شود .

استفاده از هر روش رمزگذاری متضمن تحمل مشکلات کوچکی است . همان طوریکه قبلاً ذکر شد اگر تابع F به طور یکتا ، معکوس پذیر نباشد ممکن یا لازم نخواهد بود که مقدار واقعی X پیدا شود . هر X با هر تصویری کافی خواهد بود در حقیقت ضمانت اینکه روش رمزگذاری (مخفی سازی) تمام امکاناتش قابل استفاده باشد امکان پذیر نیست . در یک رمزگذاری خوب از نقش F می توان انتظار داشت که شخصیت یک انتخاب تصادفی از تمامی حالات ممکن Y به طور یکسان انتخاب شود. دراین مورد اگر X به طور یکسان انتخاب شود ویا پیامها و کلید در تعداد مساوی باشند آنگاه احتمال اینکه نتایج Y که K+1 فرم معکوس دارد تقریباً $e^{-1/k!}$ برای K=0,1,2,.... است این توزیع پوآسون برای $\lambda = 1$.است که یک واحد شیفت پیدا کرده.بنابراین تعداد گسترش یافته تصاویر معکوس فقط ۲ عدد می‌باشد.تا زمانیکه برای f ممکن است که دوباره تولید کند ،یک مخفی سازی خوب نخواهد بود .(در موارد اشتباه،اگر $f(x)=y_0$)برای چندینy_0 ما $S_k(p_0) \equiv c_0$ رادراریم که P_0 در کل به کلید بستگی ندارد. تا وقتی که ماعلاقه مند به پیدا کردن تابعی هستیم که برد و دامنه آن از لحاظ اندازه قابل مقایسه باشند، استثنای وجود دارد. در بخش قبلی مانیاز داشتیم که یک تابع یک سویه طولانی را به فرم کوتاهترش تبدیل کنیم . بوسیله استفاده از رمز بلاک ها که در آنها کلید ها طولشان از طول بلاک بزرگتر است، چنین تابعی می تواند در این تکنیک استفاده شود .یک راه دیگر نیز برا ی حل مشکل ساختمان تابع یک سویه از کلید بلاکها وجوددارد . این روش بهتر از انتخاب یک p_0 ثابت به عنوان ورودی است این روش از تابعی به شکل $F(x)=S_x(x$ استفاده می کند.

این یک روش دسترسی جذاب است چراکه حل این تساوی بدین شکل آسان است . حتی وقتی که خانواده S به طور قابل مقایسه ای ساده باشند . این امرباعث افزوده شدن پیچیدگی می شود، اگر چه خراب کند تساوی بین امنیت سیستم s در زیر حملات Plaintext و تابع یک سویه F را. یک سیستم مخفی سازی کلیدی عمومی می تواند برای تولید یک سیستم اثبات صحت یک سویه استفاده شود.

فقط با صحبت کردن کار درست نمی شود ، ایجاد ساختمان یک سیستم رمزگذاری کلیدی و عمومی مشکلات بیشتری از تولید یک سیستم اثبات صحت با تابع یک سویه دارد. به طور مشابه ، یک سیستم مخفی سازی کلیدی و عموی می تواند استفاده بشود به عنوان یک سیستم پخش کلید ولی نه بطور برعکس .

در یک سیستم کلیدی، عمومی ، سیستم عمومی که در آن E, D به شکل عمومی استفاده می شود. مشخصات E تعیین کننده یک الگوریتم کامل برای انتقال پیام ورودی به خروجی سیستم است. یک سیستم کلیدی عمومی متشکل از توابع یک سویه و trap - door ها است . البته این توابع واقعاً توابع یک سویه ای نیستند که در محاسبه معکوس وجود دارند .اما دادن یک الگوریتم برا ی پیش راندن توابع به اندازه کافی محاسبه معکوس آن را مشکل می کند. فقط ، اطلاعات یک trap- door ویژه (به طور مثال رشته تصادفی بیت که جفت E-D را تولید می کند) به سادگی می تواند تصویر معکوس را پیدا کند.

Trap-door ها تقریباً در پاراگراف قبلی بیان شدند. اما انواع دیگری نیز وجود دارند یک رمز Trap- door درمقابل کسانی که می خواهند وارد سیستم شوند و اطلاعات آنان در بخش اطلاعات Trap- door موجود نیست به شکل سختی مقاومت می کند این امر این امکان را برای طراح فراهم می سازد که سیستم را بعد از فروش به مشترک بتواند بشکند و به شهرت خود به عنوان یک سازنده سیستم های امنیتی بیافزاید .

این نکته قابل توجه وجود دارد که این زرنگی یا اطلاعات یک سیستم نیست که به طراح امکان اجرای اموری را می دهد که دیگران نمی توانند . اگر او اطلاعات trap- door را گم کند دیگر فرقی با دیگران ندارد. شغل او بدقت به قفلهای مخلوط وابسته است . هرکس که می تواند بداند که اختلاط می تواند در چند ثانیه روی دهد کاری که حتی یک قفل گذار برای انجام آن به ساعتها وقت نیاز دارد . ولی اگر اختلاط را فراموش کند دیگر هیچ سودی ندارد.

یک مخفی سازی Trap- door می تواند برای تولید یک سیستم پخش کلید استفاده شود برای A,B که بتوانند کلید اختصاصی خود را به اثبات برسانند یک کلید به طور تصادف انتخاب می شود ویک جفت مخفی ساز plaintext را برای B ارسال می کند. B رمز عمومی trap- door را می سازد ولی اطلاعات آن را از جفت plaintext برای حل کلید دورنگه می دارد. A,B حالا یک کلید معمولی در اختیار دارند. و این دلیل کوچکی برای الزام وجود رمزهای trap- door است .

از روی تعریف مانیاز خواهیم داشت که یک مشکل trap- door فراهم کننده مشکلاتی برای طراحی سیستم trap-door است واین دلیل استفاده از پیشوند (شبکه) برای نوع سوم ماهیت ها می باشد. برا ی مثال ،یک تابع شبه یک سویه یک ، تابع یک سویه واقعی نیست که محاسبه معکوس آن ساده باشد. اگر چه به شکل قابل محاسبه ای نشدنی حتی برای طرح که معکوس آن را پیدا کند. با این وجود یک تابع شبه یک سویه می تواند برجای یک تابع یک سویه واقعی استفاده شود بدون آنکه ضرری به امنیت برسد.

گم شدن اطلاعات trap- door در یک تابع یک سویه trap -door ایجاد یک تابع شبه یک سویه می کند. اگر توابع شبه یک سویه را از طبقه بندی توابع یک سویه خارج کنیم اشکالاتی بوجود خواهد آمد. این در واقع تعریف توابع یک سویه به صورت محدود یا وسیع است . به طور مشابه یک شبه رمز امنیتی ، رمزی است که می تواند مقاومت سیستم رمزگذاری را بالا ببرد حتی بوسیله طراح یا الگوریتم رمز گذاری . بار دیگر، از دید کاربردی تفاوت فاحشی بین یک رمز امنیتی ویک شبه رمز امنیتی وجود ندارد.

ما دیدیم که سیستمهای رمز عمومی به وجود توابع یک سویه trap- door اشاره دارند. برای اینکه یک تابع یک سویه trap-door مفید باشد باید دارای معکوس (مثلاً یک معکوس یکتا) باشد.

پیچیدگی محاسبات

مخفی سازی از دیگر زمینه های کوشش متفاوت است که در آنها سعی بر فراهم آوردن سهولت کار برای دسترسی به رضایت فراهم شده است . یک انتقال ساده می تواند یک متن قانونی را به یک متن در هم و برهم غیرقانونی تبدیل کند. شخص کاردان ، کسی که ادعا می کند معانی می توانند توسط مخفی ساز بازیابی شوند بایک نمایش دشوار روبه رو خواهد شد ، اگر بخواهد ثابت کند که نقطه نظرش صحیح است. تجربه نشان داده است ، با این وجود تعداد اندکی از سیستمها توانسته اند درمقابل حملات رمزگشایان ماهر مقاومت کنند ، ولی خیلی از آنها شکسته شده اند.

در نتیجه ، قضاوت درمورد ارزش یک سیستم جدید همیشه مورد علاقه مخفی سازان بوده است . در طول قرون شانزده و هفده ، مباحث ریاضی در مورد مخفی سازی بحث می کردند و به استناد ادامه این روشها کلیدهای ممکن به صورت اعداد نجومی پیدا می شد. اگر چه مشکلات سخت تر از آن بودند که توسط این روشهای ساده حل شوند . در طول این قرن ، جهت روشها عوض شد . تئوری اطلاعات برروی کاغذ متولد شد . شانون (ریاضی دان) نشان داد که سیستم یادداشت یکبار مصرف

(one –time pad system) که از دوازده سال قبل از آن شروع به استفاده شده بود پیشنهاد یک (ایمنی کامل) (مجموعه ای از امنیت های قطعی) را می دهد .

واژه امنیت تقریباً توسط شانون وارسی شده بود و او به آن روشها اعتماد داشت، این روشها هر روز با استقبال بیشتری که از آنها می شد، طولشان نیز به طور خطی افزایش پیدا می کرد.

ما توجه داریم که ، نه سیستم مخفی سازی عمومی و نه سیستم اثبات صحت یک سویه نمی توانند به طور قطعی ایمن باشند. به این دلیل که ، اطلاعات عمومی همیشه اطلاعات سری را مابین اعضای یک مجموعه محدود به طور یکتا تعیین می کنند با محاسبات نامحدود مشکلات به ناچار حل می شوند.

قرار است که پیچیدگی محاسباتی روشها محاسبه شود . تا بهترین و کوتاهترین الگوریتم را بتوان یافت .

تابعی به کلاس پیچیدگی P متعلق است (برا ی چند جمله ای) اگر بتواند بوسیله یک ماشین سازنده تعیین کننده در یک زمان که از بالا محدود شده است توسط چند ، چند جمله ای در طول ورودی خودش محاسبه شود . شاید به نظر برسد که این کلاس (طبقه) ، کلاس توابعی است که به طور ساده قابل مقایسه هستند، اما درست تر آن است که گفته شود تابعی که در این کلاس موجود نیست باید در نهایت محاسبه آن برای چند ورودی مشکل باشد.

درمسائل مهندسی مشکلات زیادی بوجود می آید که در زمان لازم برای حل چند جمله ای ها قابل حل نمی باشند مگر آنکه از کامپیوتر برای حل این مسائل استفاده شود تا چند عمل بتواند به صورت موازی انجام شود . این دسته از مسائل را در کلاس NP (nondeterministic , polynomial) طبقه بندی می کنند . آشکارا کلاس NP شامل P وناحیه بزرگ بازی از تئوری پیچیدگی است . در میان مشکلات شناخته شده ای که در زمان NP قابل حل هستند ، نه آنها که درزمان P قابل حل هستند . از نوع مسائل مرد فروشنده هستند، مسائل بهینه سازی مثل، مسئله کوله پشتی ، حلقه گرافهاو ....

ما می دانیم که این کمبود علاقه یا اثر نیست که مردم را از پیدا کردن راه حل ها در زمان P برا ی چنین مسائلی بازداشته است . پس قویاً باید باور کرد که در نهایت یکی از این مسائل نباید در کلاس P باشد ، پس بناچار کلاس NP به طور اکید از کلاس P گسترده تر است .

بعضی از دانشمندان یک رده فرعی را برای کلاس NP قائل شده اند به نام «NP کامل» با این توانایی که اگر هیچ کدام از آنها در کلاس P نبودند . انگاه همه مسائل NP داخل P هستند . در این دسته ازمسائل ۲۱ مسئله ذکر شده است که مسائل بالا نیز از آن جمله اند.

تا زمانی که مسائل طبقه NP کامل، قول استفاده از سیستم مخفی سازی را می دهند فهمیدن مشکلی آن به جز اشتباه در آنالیز چیز دیگری نیست . برای منظورهای مخفی سازی هزینه محاسبات معمولی باید قابل درک باشد. اگر ، ما زمان محاسبه موارد اشتباه را بازمان میانگین یا زمان محاسبه معمولی ، به عنوان اندازه پیچیدگی عوض کنیم دلایل جاری تساویها در میان مسائل NP کامل دیگر فاقد

اعتبار می شود. این مطلب زمینه های فراوانی را برای تحقیق می گشاید . اثر کلی و مفاهیم عمومی اطلاعات تئوری دارای نقشهای آشکاری دراین بازی دارند.

ما حالا می توانیم موقعیت مسائل مخفی سازی را درمیان بقیه مسائل محاسباتی پیدا کنیم .

مشکلی و سختی مخفی سازی یک سیستم که رمزگذاری آن می تواند در زمان P انجام بپذیرد نمی تواند از NP بزرگتر باشد. برای اینکه این مسئله روشن شود، مشاهده کنید که هر مشکل رمزگذاری میتواند با پیداکردن یک کلید حل شود، تصویر معکوس و غیره ..... انتخاب شده از یک دسته محدود. انتخاب یک کلید به صورت غیر معین از زمان P کاری صحیح است. اگر M کلید ممکن برای انتخاب وجود داشته باشد ، یک زمینه عملیات موازی M حالته باید استفاده شود. برای مثال در یک حمله plaintext , plaintext در زیر هر کلید به طور مشابه رمز گشایی می شود و توسط دستگاه مخفی ساز مقایسه می شود. از این رو ، با فزض اینکه رمز گذاری فقط زمان P را لازم داشته باشد . رمز گشایی به اندازه NP زمان لازم دارد. ما همچنین مشاهده می کنیم که مسائل اصلی مخفی سازی از نوع NP کامل هستند . و این بخاطر تعریف وسیع ما از مسائل مخفی سازی است . یک تابع یک سویه با تصاویر عکس در NP کامل ، جلوتر بحث خواهد شد.

مخفی سازی می تواند به طور مستقیم از تئوری پیچیدگی NP بوسیله آزمایش، راهی که در آن مسائل NP کامل می توانند برای مخفی سازی تطابق یابند منتج شود. برای نمونه ، مسئله کوله پشتی یک مسئله NP کامل است که به درد ساختمان توابع یک سویه می خورد . بگذارید $Y=F(x)=a....x$ باشد و a یک بردار شناخته شده عدد اینتیجر n و X یک بردار دودویی برای n باشد . محاسبه Y بسیار ساده است ، یک جمع از چند n اینتیجر .مسئله پیدا کردن معکوس F همان مسئله کوله پشتی است ، و نیاز به پیدا کردن یک زیر مجموعه دارد مثل $\{a_i\}_n\}$ که با Y جمع شود.

یک جستجوی کامل و جامع برروی ۲زیر مجموعه باعث رشد نهایی آن می شود و برای n های بزرگتر از ۱۰۰ تقریباً غیر قابل شمارش است. در آزمایش باید نهایت دقت را مبذول کرد تامطمئن شد که برای انتخاب پارامترهای مسئله راه کوتاهتری وجود ندارد. برای مثال اگر $n=100$ و هر a_i32 بیت طول داشته باشد و y و نیز در نهایت ۳۹ بیت باشد و f نیز به طور قابل ملاحظه ای قابل فساد باشد به طور میانگین نیاز به 2^{38} بار ، سعی برای پیداکردن راه حل لازم است. یک نکته جالب ، اگر $a_i=2^{i-1}$ آنگاه معکوس f برابر است با پیداکردن تجزیه y این مثال با دلیل، وجود احتمالات زیاد و میانبرهای قابل توجه را اثبات کرد.

تئوری پیچیدگی فقط به ما می گوید که مسئله کوله پشتی در بدترین حالات تقریباً مشکل است. و این دلیل برسخت بودن این مسئله برای همه ورودی ها نیست. این مطلب نشان می دهدکه با این وجود انتخاب $\{a_i\}$ به طور یکنواخت از $\{۰،۱،۲،...،۲^{n-1}\}$ مسئله را به یک حالت مشکل می برد که از جمله آنها این است که n به بی نهایت میل می کند.

دیگر استعداد بالقوه تابع یک سویه، کمک به آنالیز الگوریتم است.

دورنمای تاریخی

زمانی که سیستمهای رمزهای عمومی و اثبات صحت های یک سویه در این مقاله مطرح شدند هیچ صحبتی از چگونگی توسعه آنان تا این مرحله به میان نیامد. خوب است که در این قسمت کمی در مورد سابقه تاریخی این سیستمها صحبت شود که نتیجه طبیعی کوششها در جهت مخفی سازی است که قدمت آن به صدها سال پیش برمی‌گردد.

اختفا در قلب روشهای مخفی سازی قراردارد. چنانچه در روشهای امروزی به طور گیج کننده ای حتی مشخص نیست که سعی در اختفای چه شده است. سیستم های مخفی سازی مانند «رمزگذار سزار» (Caesar cipher) ، (در این رمزگذار Aبه Dو Bبه E تبدیل می شود) بسته به امنیتشان عملیات مخفی سازیشان سری تراست. بعد از اختراع تلگراف، فرق بین یک سیستم عمومی و یک رمز اختصاصی به سیستم عمومی این امکان را داد تا بتوان بوجود رخداد دزدی در این سیستم پی برد. مثلاً اگر یک دستگاه رمزگذاری دزدیده می شد، پیامهای بعدی به شکل جدیدی رمزگذاری می شدند. این کار برای اولین بار توسط کیرشهف (۱۸۸۱) انجام گرفت. در سال ۱۹٦۰سیستم های رمزگذاری در سرویسهایی به کار رفت که فرض می شد در مقابل حملات می توانند مقاومت کنند البته دیگر رمزهای قدیمی تر در متنها قابل استفاده نبود و حذف شدند.هر کدام از این پیشرفتها کاهش داد حجم قسمتهایی از سیستمها را که در دید عموم قرار داشت. هر گونه مقتضیات به دردنخور مثل پیش نویس نامه های دیپلماتیکی که هنوز ارسال نشده اند حذف نشد.

قبل از این قرن، رمز گذاری فقط به محاسباتی که توسط دست انجام می گرفتند و یا بوسیله وسایل بسیار ابتدایی، محدود می شد. اما در یک بازه زمانی بعد از جنگ جهانی اول انقلابی در روشها صورت گرفت که ادامه آن امروزه مورد استفاده قرار می گیرد. ماشینهای رمزگذاری برای مقاصد خاصی طراحی شدند. با وجود ساخت وسایل سخت افزاری دیجیتالی برای مقاصد عمومی همچنان رمز گذاری به علت سادگی اجرا و روشها به سخت افزارهای خاصی محدود شده بود. پیشرفت کامپیوترهای دیجیتالی روشهای رمزگذاری را از محدودیت خارج ساخت چراکه قبلاً این روشها با استفاده از چرخ دنده‌ها محدود شده بود.

اشکالات تلاشهایی که برای اثبات بی سروصدای سیستم های رمزگذاری به وسیله دلایل ریاضی صورت گرفت منجر به ساخت نمونه هایی از دستگاههای اثبات صحت برای مقابله با حملات رمزگشاها به وسیله کیرشهف در اواخر قرن قبل شد. اگرچه چند نقش اساسی پیشرفت یافته بود که به طراحان برای از بین بردن ضعف ها کمک کرد ولی آزمایش اصلی وقتی بود که سیستم توسط رمزگشاهای حرفه ای مورد حمله قرار گرفت. پیشرفت در زمینه کامپیوتر برای اولین بار باعث شد که الگوریتم های تئوری بتوانند نزدیک بشوند به مسائل مشکل تخمین زدن سختی محاسبات لازم برای شکستن رمزها. این باعث شد که دلایل ریاضی دوباره به عنوان بهترین روش رمزگذاری ظاهر شوند.

آخرین مطلبی که در این بخش باید به آن بپردازیم ، فرق بین یک رمزگذار حرفه ای و یک رمزگذار مبتدی است . مهارت در تولیدات رمزگذاری همیشه به شکل تنگاتنگ در کنار حرفه‌ای‌ها بوده است . اما ، نوآوری و طراحی روشهای جدید همیشه از طرف مبتدی ها بوده است. توماس جفرسون ، یک رمز گذار مبتدی روشی را اختراع کرد که در جنگ جهانی دوم مورد استفاده قرارگرفت.

در قرن بیستم که بیشترین توجهات به رمزگذاری معطوف بود چهار نفر مبتدی به طور جداگانه و مشابه ماشین چرخنده (rotor) را ساختند. ما امیدواریم که این تشویق کند دیگران را که در این زمینه کارکنند، که دولت ها و انحصارهای آنها از دخالت در این امر دلسرد شده اند.

نتیجه گیری

همان طور که خواندید چندین روش در مخفی سازی و رمزگذاری مطرح گردید و ازدیدگاهها ی مختلف مورد بررسی قرارگرفت،که هر کدام چه محسنات و چه مضراتی دارند. ولی با این وجود نمی توان گفت که چه روشی از دیگر روشها بهتر است،بلکه این امر همان طور که خواننده دریافته است وابسته به نوع کاری می باشد که می خواهد انجام بگیرد،مثلاً در بعضی از موارد ممکن است سرعت در عملیات ورود از اهمیت بیشتری نسبت میزان امنیت عملیات پردازش کلمه عبور داشته باشد و یابالعکس.

حتی، گاه ممکن است ترکیب چند روش با یکدیگر بهترین نتیجه را ارائه دهد. و این همان طور که گفته شد بستگی به اولویت پارامترهای موجود، برای هر نوع استفاده دارد.

این مقاله سعی کرد با دادن یک دید کلی به امر مخفی سازی و رمزگذاری ، خواننده را با این روشها آشنا کند. چرا که هر کدام از این روشها حاوی جزئیات بسیار زیادی می باشند. امیداست که این مقاله مورد پسند خوانندگان قرارگرفته باشد.

در آخر توجه خواننده را به مطلب موجود در بخش ضمیمه جلب می کنم که می تواند به درک مطلب به صورت ملموس تری کمک کند.

پایان

مراجع:

[۱] R. Merkle, "Secure communication over an insecure channel," submitted to *Communications of the ACM.* 1881 that the compromise of a cryptographic system should cause no inconvenience to the correspondents. About 1960 cryptosystems were put into service which were deemed strong enough to resist a known plaintext cryptanalytic attack, thereby eliminating the burden of keeping old messages secret. Each

[۲] D. Kahn, *The Codebreakers, The Story of Secret Writing.* New York: Macmillan, 1967.

[۳] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.,* vol. 28, pp. 656-715, Oct. 1949.

M. E. Hellman, "An extension of the Shannon theory of these [٤]
developments decreased the portion of the system **approach to cryptography," submitted to *IEEE Trans.*** which had to be protected from public knowledge, eliminating ***Inform. Theory,* Sept. 1975.** such tedious expedients as paraphrasing diplomatic dispatches
W. Diffie and M. E. Hellman, "Multiuser cryptographic [٥]
before they were presented. Public key systems are a natural **techniques, presented at National Computer Confer**-continuation
.of this trend toward decreasing secrecy. **ence, New York, June 7–10, 1976**
,D. Knuth, *The Art of Computer Programming, Vol. 2* [٦]
Semi-Numerical Algorithms.* Reading, MA.: Addison-** **[11] G. B. Purdy, "A high security log-in procedure," *Commu-nication
***.of the ACM,* vol. 17, pp. 442–445, Aug. 1974. Wesley, 1969**
The Art of Computer Programming, Vol. 3, Sort- **[12] W. ,———** [٧]
Diffie and M. E. Hellman, "Cryptanalysis of the NBS data encryption standard" submitted to *Computer, ing and*
***.Searching.* Reading, MA.: Addison-Wesley, 1973**
S. Pohlig and M. E. Hellman, "An improved algorithm for [٨]
computing algorithms in *GF*(p) and its cryptographic
.significance," submitted to *IEEE Trans. Inform. Theory*
M. V. Wilkes, *Time-Sharing Computer Systems.* New [٩]
.York: Elsevier, 1972
A. Evans, Jr., W. Kantrowitz, and E. Weiss, "A user [١٠]
authentication system not requiring secrecy in the com-
,puter," *Communication of the ACM,* vol. 17, pp. 437–442
.Aug. 1974
G. B. Purdy, "A high security log-in procedure," *Commu-* [١١]
nication
***.of the ACM,* vol. 17, pp. 442–445, Aug. 1974**
W. Diffie and M. E. Hellman, "Cryptanalysis of the NBS [١٢]
.data encryption standard" submitted to *Computer,* May 1976
A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The Design and* [١٣]
:*Analysis of Computer Algorithms.* Reading, MA
.Addison-Wesley, 1974
",R. M. Karp, "Reducibility among combinatorial prob-lems [١٤]
***Complexity of Computer Computations.* R. E. Miller and J.**
,Thatcher, Eds. New York: Plenum, 1972

www.cne.gmu.edu

www.edgereview.com

ضمیمه

همه کامپیوترها نیاز به ابزارهایی برای امنیت دارند و مکانیزم ابزارهای روش‌های امنیتی در این تحقیق مورد بررسی قرارمی‌گیرد که ما

آن را به هشت مورد اساسی به شرح زیر تقسیم می‌کنیم.

۱ – تقسیم بندی حافظه۲ – حالت‌های نظارتی و دستورالعمل‌های حساس ۳– کنترل اجازه دسترسی به فایل‌ها ٤ – login

٥ – پروتکل‌های رمز گذاری ٦– کلیدهای عمومی (certificate)

۷ – نتایج کنترل‌ها (در بعضی از سیستم‌های پایگاه داده‌ها) ۸– کنترل جریان داده‌ها (در بهضی از سیستم‌های امینتی نظامی)

روش‌ها در ارتباط با مکانیزم جداسازی

تغییر قوانین بدون تغییر دادن مکانیزم مانند کنترل اجازه دستیابی به فایل‌ها

سطوح مکانیزم (سه سطح)

سیستم عامل و سخت افزار (قسمت مرکزی)

یک شبکه مرتبط از کامپیوترها

اینترنت: به چه کسی یا به چه چیزی اطمینان کنیم

سطح اول – قسمت مرکزی

هدف کنترل اجازه دسترسی در همه قسمت‌های حافظه اصلی و حافظه ثانویه

- فقط توانایی پردازش موضوعاتی از حافظه که اجازه دستیابی به آنها سریعاً داده شده باشد
- عدم اجازه دسترسی به صورت پیش فرض (Defualt)

مفاهیم

تعاریف محدود کننده در Registerها و جدول‌ها

احضار جدول‌هایی از حافظه مجازی (تقسیم بندی منطقی)

محدودیت‌های دستورات حساس برای حالت نظارت

ورودی‌ها حفاظت شده از طریق تله‌ها

کنترل اجازه دسترسی به فایل‌ها و کپی بر روی (mapping table)

رسیدگی کردن (از لحاظ صحت و سقم) به اجازه دستیابی هر موضوع از طریق دستگاه کنترل مرکزی

توضیح بخش‌های گذشته "اساس کنترل اجازه دستیابی" روش استفاده اجازه دستیابی با استفاده از ماتریس ویژه

سطرها: نواحی حفاظت شده هستند

ستون‌ها: موضوعات (به انضمام نواحی)

- هر اجازه دسترسی به وسیله هسته کنترل می‌شود اگر دسترسی غیر مجاز محسوب شود سیستم در برابرا ین دسترس غیر مجاز با ایجاد وقفه محافظت می‌شود.
- ابزارها ماتریس دستیابی از طریق ستون‌هایش

ACL که مخفف (access control list) است لیست کنترل دستیابی‌ها که با موضوع در ارتباط است در نواحی ویژه و بسته به نوع اشاره اجاره دستیابی دهد.

- ماتریس دستیابی به طریق سطرها لیست موضوعات (لیست توانایی‌های) با نواحی در ارتباط است و اشیا ویژه‌ای قابلیت دستیابی دارند

- در عمل هر دو مورد به کار برده می‌شوند

اطلاعات ACL که از کتابچه راهنما است بر روی جداول صفحه یا سگمنت‌ها کپی می‌شود هسته (OS) و سخت افزار این جداول را به کار می‌برند و تک تک آدرس‌ها را تعیین و اجازه دستیابی‌ها را محدود می‌سازد.

- تعیین کردن جداول اشاره شده با استفاده از شناسایی نواحی Registerها در Stateword با CPU
- وقتی کابری از قفل استفاده می‌کند در واقع یک محدوده‌ای را تعیین می‌کند
- یک کاربرد می‌تواند به نواحی دیگر دسترسی داشته باشد اگر ماتریس دستیابی به او اجازه دهد.

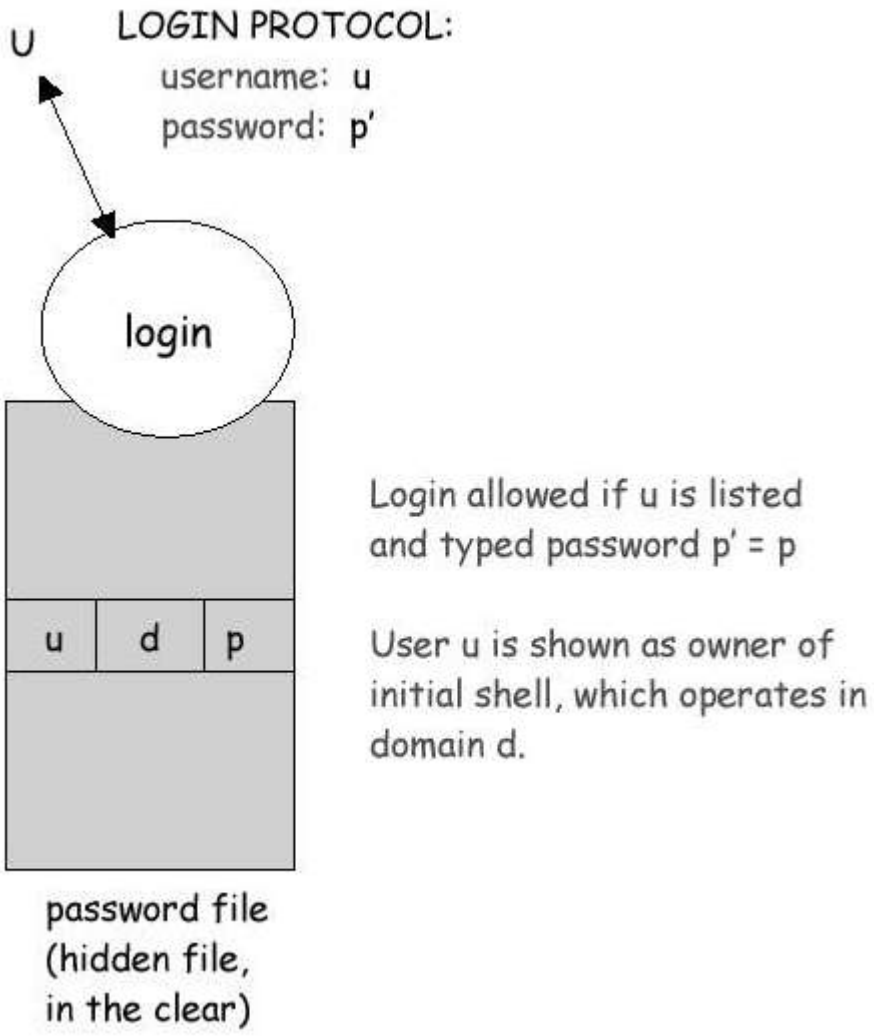
سطح دوم شبکه‌های محلی

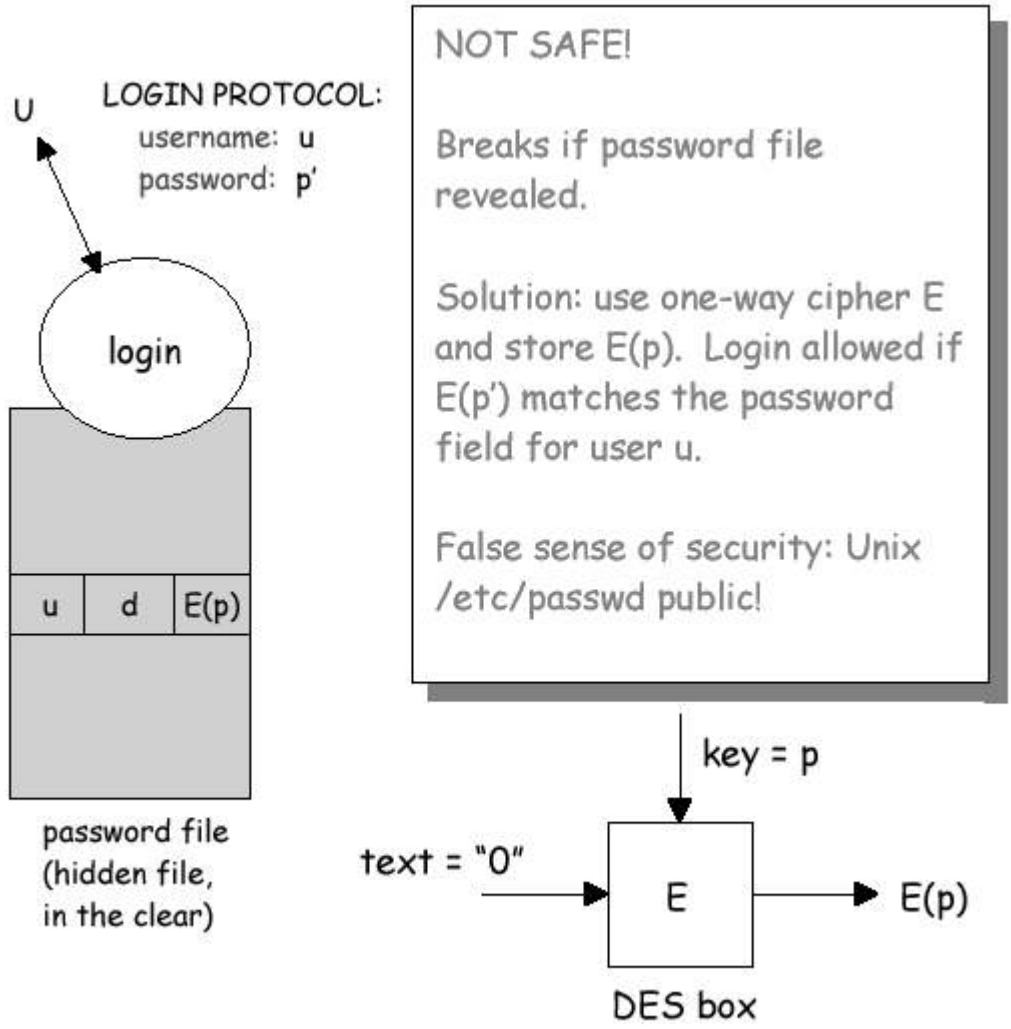
- فایل ها در سراسر یک مجموعه از ایستگاه‌ها (Work Station) و Serverها تقسیم شد و به وسیله یک شبکه محلی سریع به هم متصل شده‌اند

- **انتقال محلی**

  - فایل‌ها از طریق هر ایستگاهی قابل دید (دسترسی) هستند
  - کاربران می‌توانند برای هر ایستگاه از قفل استفاده کنند.

- صحت کاربر در (login) نقد مسأله امنیت است (کارایی سیستم). حمله کنندگان به دنبال گشودن حساب‌ها از طرق غیر مجاز هستند از دو طریق زیر
  - شکستن Password
  - پی بردن به Password


U
LOGIN PROTOCOL:
username: u
password: p'
login
u
d
p
Login allowed if u is listed and typed password p' = p
User u is shown as owner of initial shell, which operates in domain d.
password file (hidden file, in the clear)



Login هنوز مطمئن است

حمله کنندگان نمی‌توانند آنقدر فضای کلمه رمز را جستجو کنند تا Password متناسب با E(p) را بیابند. مثلاً اگر تعداد حروف Password 6 تا باشد 26^6 کلمه رمز امکان پذیر است و سایر این فضاب تقریباً 2^{30} است که غیر قابل استخراج به نظر می‌رسد.

اما کاربرانی که مایل هستند کلمات را به انگلیسی انتخاب کنند

- بیشترین احتمال شکستن کلمه رمز بر اساس حدس زدن تمام کلمه‌ها در یک فرهنگ انگلیسی است (تقریباً ۲۵۰۰۰۰ مدخل)
- استفاده از تقدم و تأخر در جابجایی اسامی (حروف) و تهیه دوکپی از نام و ...

- مطالعات زیاد نشان داده است که جمله یک فرهنگ لغات به شیوه مجازی که موفق به کشف فایل Password ب کمی یافتن

Password 100 کاربر موفقیت آیز بوده است که چندین ساعت زمان می‌برد.

- **روش های خنثی سازی**

- ساختن یک فایل Password غیر قابل دسترسی

- قطع ارتباط پس از سه کوشش ناموفق

- نیاز به پوشش از طریق اعداد و نقطه گذاری در Passwordها

- فرستادن اصطلاحات

- همه این‌ها هنوز مطمئن نیستند.

- سارقان پس از پی بردن به Passwordها از آنها نگه داری می‌کنند و دیگر نیازی به حدس زدن ندارند

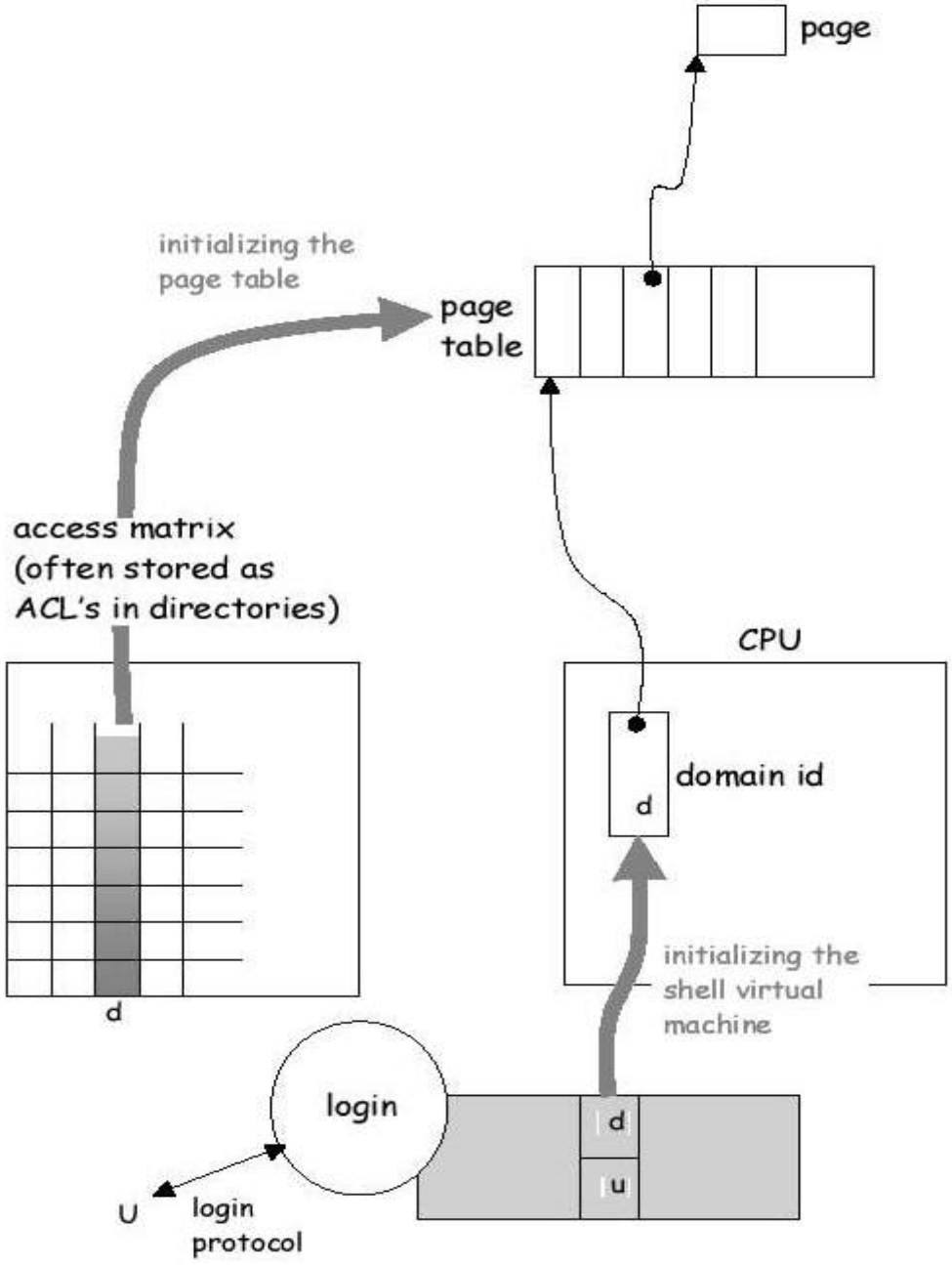
- **راه حل:**

هر کامپیوتری که بر روی شبکه کار می‌کند از یک رمز گذاری مربوط به صاحب کار که شامل نام کاربر و Password آن است تشکیل

شده است که آنها را به Server برای شناسایی می‌فرستند.

از بین بردن (مشکل) حمله به Passwordها

اختصاص کلیدی به Passwordها به طوری که این کلید قابلیت استفاده مجدد را داشته باشند


page
initializing the
page table
page
table
access matrix
(often stored as
ACL's in directories)
CPU
domain id
d
d
initializing the
shell virtual
machine
login
d
u
U
login
protocol

عددی که در پنجره قرار داده می‌شود ساعت زمانی رمز گذاری شده‌ای است که تحت یک کلید که در آنجا (پنجره) قرار داده و نگه داری می‌شود و محدوده و قرارگیری توسط سیستم مدیریت تعیین می‌گردد در این تغییرات هر یک ثانیه یکبار انجام می‌گیرد.

- وقتی که login کلمه عبور را می‌پرسد کاربر عددی را وارد می‌کند پس این عدد در پنجره قرار و نمایش داده می‌شود.
- سیستم عدد وارد شده را با آن چیزی که انتظار دارد چک می‌کند که این انتظار مربوط به زمان و کلید کاربر است.
- روش با تغییرات زمانی به وسیله نگه داشتن یک فاکتور تغییر کننده در جدول Passwordها برای کاربر u می‌باشد.
- اگر E(k,a*t) متناسب با آن آن چیزی که کاربر وارد کرده است باشد تأیید می‌شود.
- اگر متناسب نباشد یا با پارامتر $t-1$ (یا $t+1$) چک می‌شود اگر متناسب بود از $a=\frac{t-1}{t}$ یا $(a=\frac{t+1}{t})$ استفاده می‌شود.

مسأله مهم قیمت است

- اجازه ورود به عنوان مثال ۱۰ $ است
- مدیریت سنگین سراسری برای تعیین محدوده اجازه ورودی، فراخوانی اجازه ورود و جلوگیری از ورود غیر مجاز دزدی یک مشکل همیشگی نیست و این خطر احتمالی بدتر از دزدی کارت اعتباری است.

تحقیق و مطالعه پدیده‌های حیاتی

چه نوع پدیده حیاتی برای شناسایی سودمند است

Biometric کدام ویژگی‌ها در انسان یکتا است به عنوان مثال

اثر انگشت، اثر صدا، اثر شبکیه چشم، امضا

مزایا: سخت گول زدن (اما غیر ممکن نیست)

مشکلات: با تغییر Password و یا فرستادن اجازه ورود نمی‌توان دزدی این شناسه‌ها را بی اثر کرد

اینترنت سطح سوم

اینترنت باعث مطرح شدن مشکلات جدید و زیاد امنیتی شده است

گمنامی: بسیار سخت می‌توان محل servsr ایشتگاه‌های را شناسایی کرد و برای کاربران دادن نام‌های جعلی و برگرداندن آدرس‌ها

راحت است و اتصالات غیر قابل استخراج هستند.

- درجه بندی (وسعت) : هر کسی از ۱۰۰ میلیون کاربر می‌تواند اجازه دستیابی به موضوع را داشته باشد.

کم کردن محدودیت ها اینترنت برخلاف شبکه‌های محلی که به کاربرهای مجاز محدود است به روی همه باز است و چک کردن در خود

همان موضوع اجرا می‌شود.

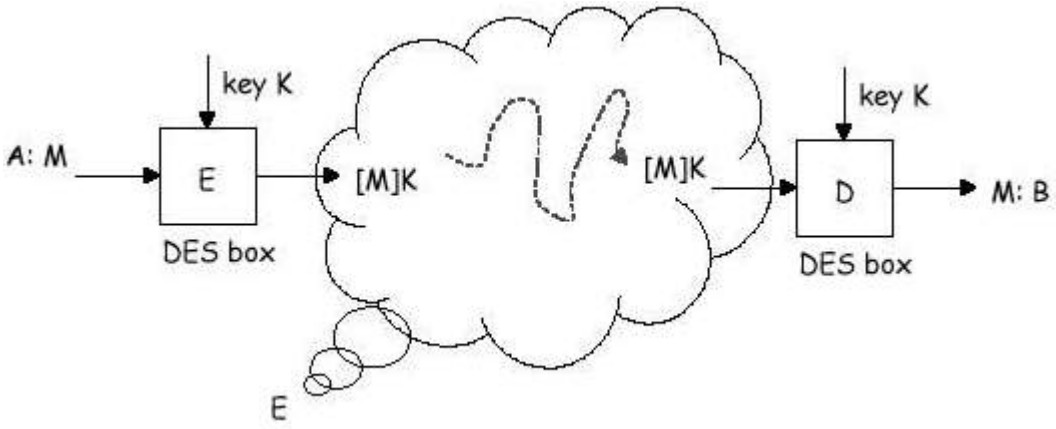
- استراتژی: حفاظت از موضوع به وسیله اجرای کنترل اجازه دسترسی محلی (یعنی در همان موضوع) و شناسایی علامت اجازه

  دسترسی وانجام این کار مستقل از شبکه به کار برده شده برای اتصال به آن موضوع می‌باشد.

- رمز گذاری به شیوه (end-to-end) پروتکل‌های از متد انتخاب هستند مبنای پروتکل‌ها عبارتند از :

کلید منفرد رمزگذاری : سریع اما از لحاظ مخفی سازی محدود شده است .

کلید عمومی رمز گذاری : که بسیار کندتر است اما قابلیت شناسایی و امضا کردن را دارد.



E can't find M in a reasonable time from [M]K. Knowledge of the E and D boxes doesn't help.

Problem: how do A and B agree on a key K?

کلید منفرد رمز گذاری

دو طرف مکالمه A (مثلاً Alice) و B (مثلاً Bob) هستند. آنها در پروتکل‌ها شریک هستند.

به منظور مخفی نگه داشتن مکالمات ابتدا یک کلید مخفی مانند K ایجاد می‌شود.

A متن مانند M را به وسیله یک تابع که بستگی به کلید K دارد به صورت رمز درمی‌آورد. [M] K = E (K,M)

B متن را به وسیله یک تابع که بستگی به کلید دارد رمز گشایی می‌کند

M = (K, M [K])

- استراق سمع کنندگان کسانی هستند که می‌خواهند M[K] را رمز گشایی کنند اما این کار بدون جستجو در همه کلیدهای ممکن امکان پذیر نیست. بنابراین بهتر است تا حد ممکن سایز کلید انتخابی بزرگ باشد . و این شیوه رمز گذاری هزاران سال قدمت دارد .
- ایجاد کلیدها نیاز به کانال امن دارد .

- نمونه مدرن رمز گذاری استاندار داده‌ها (Datu Encrytion Standard) یعنی DES حدود سال ۱۹۷۵ ایجاد شد.

- DES با استفاده از یک کلید ٥٦ بیتی بلوک‌های ٦٤ بیتی را رمز گذاری می‌کند.

در بیشتر مواقع انتقال جریان بیت‌ها از طریق یک مجموعه ١٦ دوری شامل انتقال ثبات و Sobox انجام می‌گیرد

چیپ‌های DES سرعتی حدود ١٠٠ Mbps و حتی بیشتر دارا هستندوDES به خوبی اعداد تصادفی (Random) ایجاد می‌کندو

DES یک تابع در هم ساز (hash function) خوب است .

- قرار دادن سه چیپ DES در یک حلقه feedback ظرفیت کلید را به ١١٢ بیت می‌رساند.

- شکستن کلیدی به این سایز حتی فراتر از کار کامپیوترها بزرگ و Parallel است

- مربوط به اینترنت: تعبیری از یک کلید امنیتی است که کانال‌های آن تغییر می‌کند.

نخستین شکست مربوط به DES حدس زدن کلیدها از طریق کامپیوترهای بزرگ جدا از هم بود در سال ١٩٩٨ یک موردی ساخته شد

که برای بررسی هر کلید ٢٤ ساعت وقت می‌گرفت

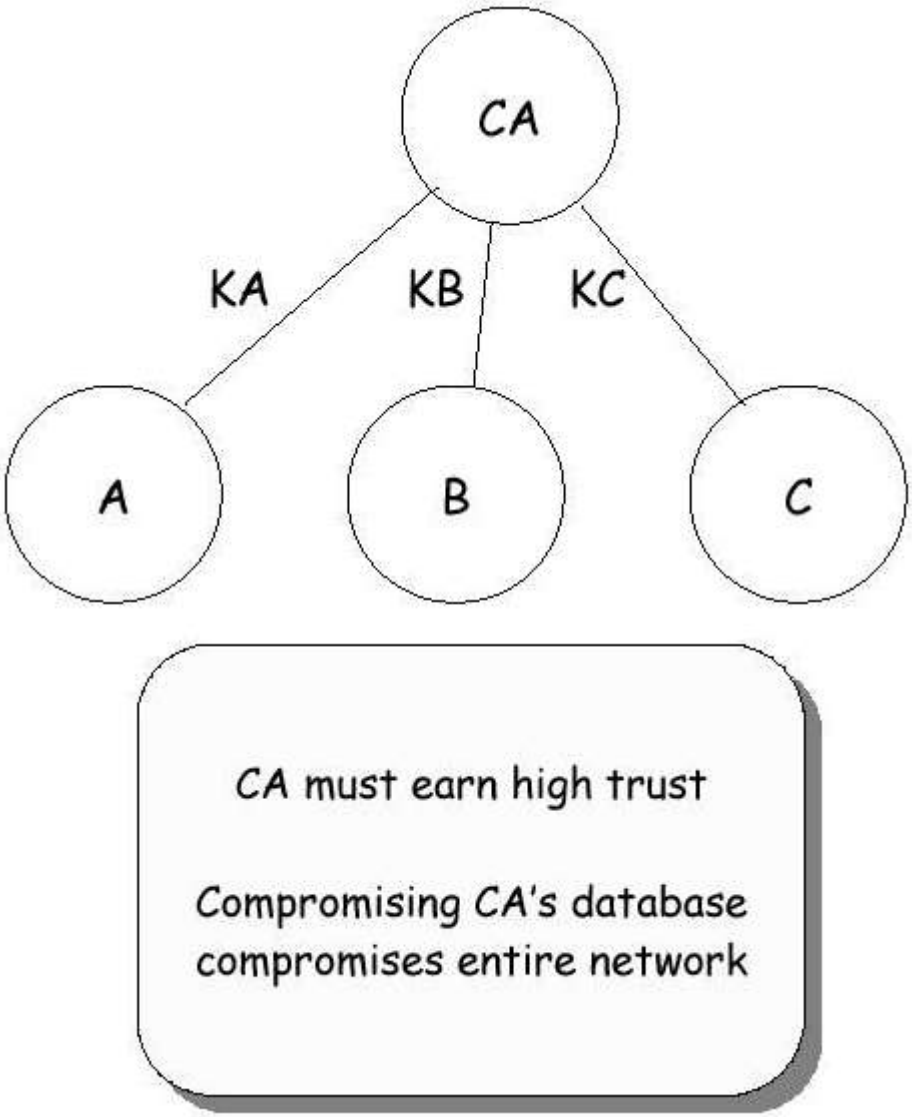
تأسیس کانال های امن

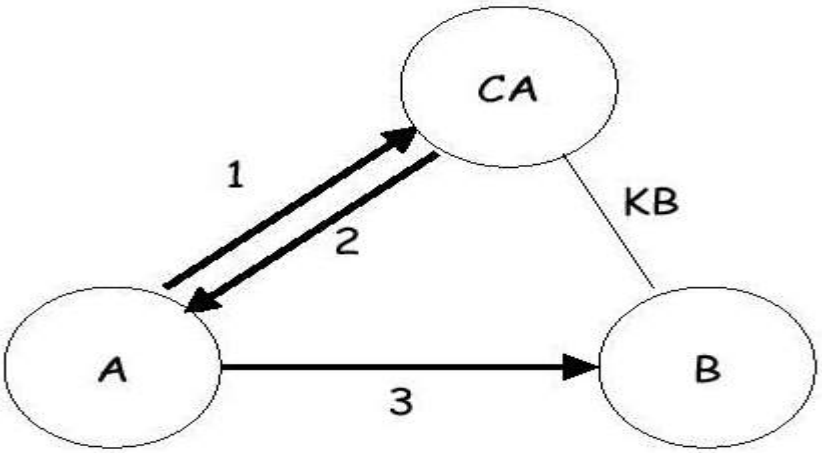
- مشخص کردن توانایی شناسایی صحت و سقم (Certification Authority)

- CA کلیدی مانند KA دارد که در ارتباط با کاربرد A است و فقط برای A و CA شناخته شده است

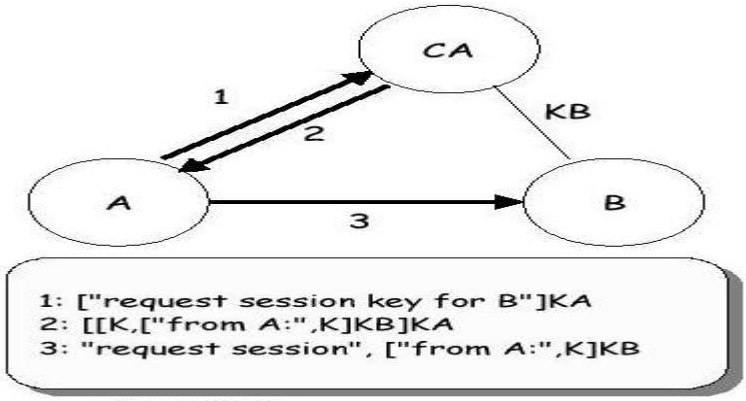
- کلید A با استفاده از کلید KA برای CA شناسایی می‌شود. کاربرد A می‌تواند از CA برای ایجاد کلید مانند K برای داشتن جلسه

  با B تقاضا کند و B متقاعد شود که فقط A و B کلید K را دارند.


CA
KA
KB
KC
A
B
C
CA must earn high trust
Compromising CA's database
compromises entire network

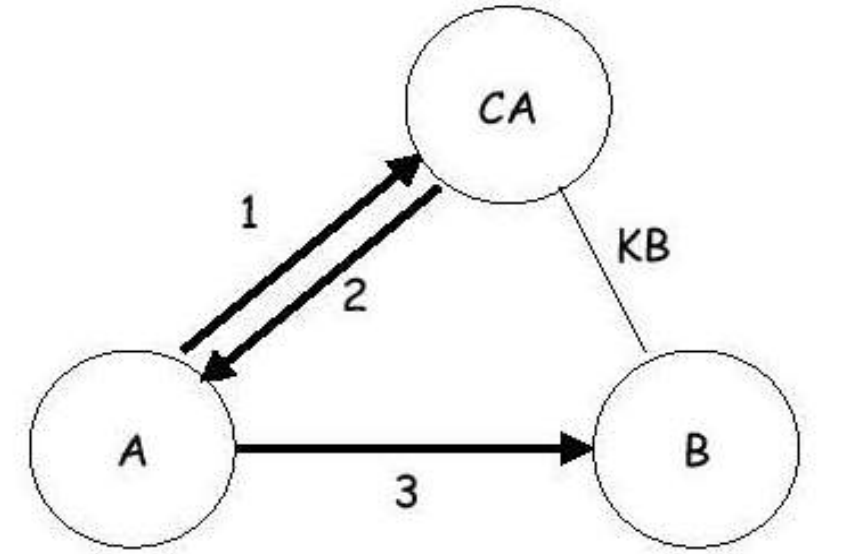


1: ["request session key for B"]KA
2: [[K,["from A:",K]KB]KA
3: "request session", ["from A:",K]KB



1: ["request session key for B"]KA
2: [[K,["from A:",K]KB]KA
3: "request session", ["from A:",K]KB

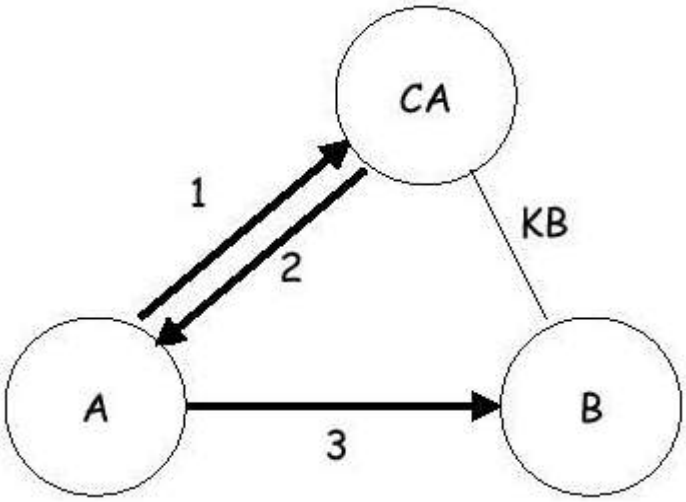
ANALYSIS:
1: A requests CA to generate K
no one else can say this
2: CA sends back K and a specia
certificate for B
3: A retains K and forwards
certificate to B
4: B opens certificate, see it's
from A and gets key K; onl



1: ["request session key for B"]KA
2: [[K,["from A:",K]KB]KA
3: "request session", ["from A:",K]KB

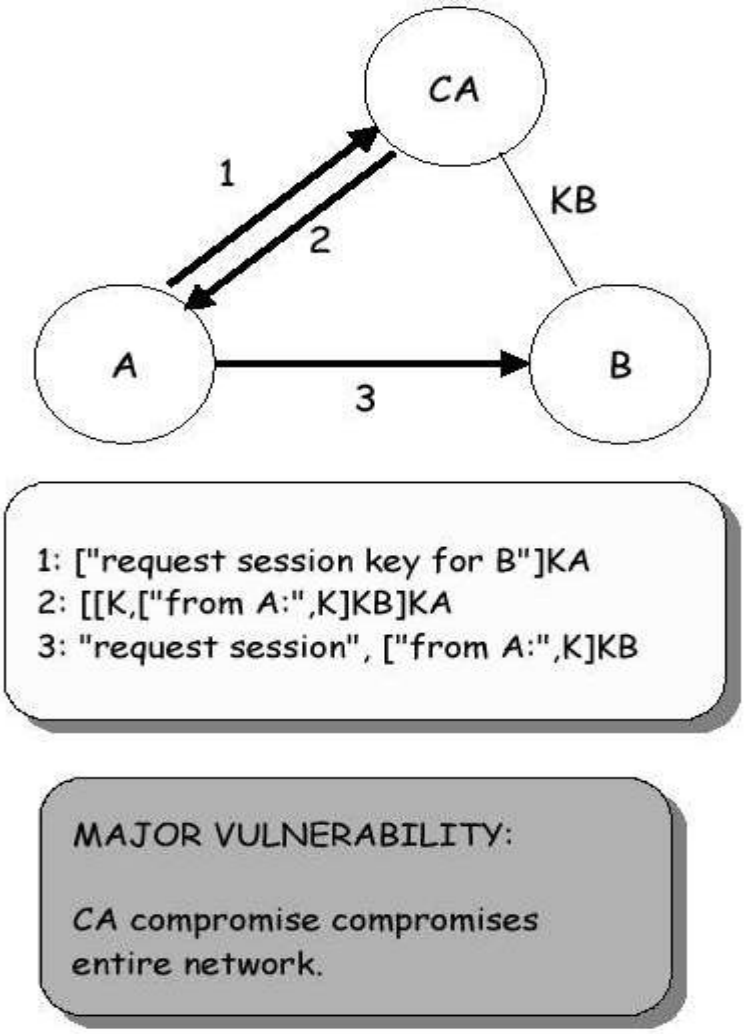
ANALYSIS:

1: A requests CA to generate K
no one else can say this
2: CA sends back K and a specia
certificate for B
3: A retains K and forwards
certificate to B
4: B opens certificate, see it's
from A and gets key K; only



1: ["request session key for B"]KA
2: [[K,["from A:",K]KB]KA
3: "request session", ["from A:",K]KB

OTHER:
Omitting KA in step 1 enables impostor of A to get K.
Omitting "from A" in step 2 deprives B of assurance A is sending the request.
Omitting certificate from step 3 deprives B of certainty that only A knows key K.
Add timestamps to prevent replay



سیستم های RSA

در ورژن اولیه یک محیط کاری امن توسط Rirest, Shamir, Adleman در سال ۱۹۷۷ اختراع شد و امروزه این روش رمز گذاری RSA نامیده می‌شود. اساس این روش انتخاب دو عدد بزرگ به صورت مخفی (مهمترین قسمت کار) مانند P و q می‌باشد (مثلاً p و q هر کدام ۲۰۰ رقم می‌تواند باشد) و قرار دادن حاصل ضرب p در q در n (n = pq)

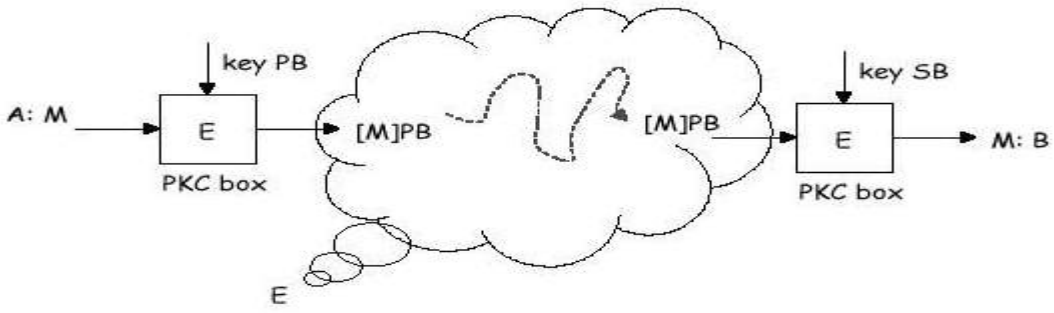
کلیدهای مخفی (d,n) هستند که d عدد صحیحی وابسته به (P – 1)(q – 1) می‌باشد

کلید عمومی (e,n) است بنابراین ۱ = ed Mod (p – 1) (q – 1) است

رمز گذاری M به C به شیوه زیر است $M^e \ Modn = c$

رمزگشایی C به M به صورت زیر است $C^d \bmod n = M$

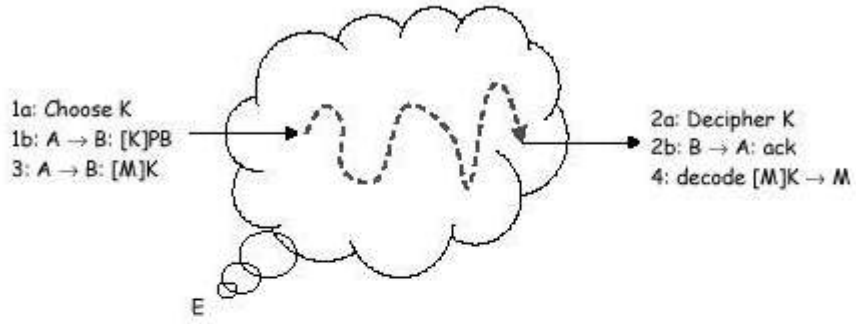
راهی پیدا نشده است که عاملی مانند nبا اعداد ترکیب شود به قسمتی که عامل اصلی آن یک چند جمله‌ای بر حسب زمان باشد مگر همه عامل‌های شناخته شده الگوریتمی از توان‌های بزرگ هستند مگر این که شما با استفاده از عامل n بتوانید d را از روی کلید عمومی پیدا کنید که این هم غیر ممکن است



Eavesdropper E cannot decipher [M]PB since SB is the only way to do that, SB is known only to B, and E cannot compute SB from PB.

DATA RATE of PKC box is much less than DES box -- on the order of 100Kb for PKC and 100Mb for DES.

Solution to Secure Key Channel Problem



A chooses a DES session key K and sends to B enciphered with B's public key. After that they can use DES to encipher all their messages.

PKC

(Public Key Crypthoyraph) اجازه امضا کردن را فراهم کرده که یک مفهوم جدید است

- [M]SA می‌تواند توسط هر شخص (با داشتن PA) رمز گشایی شود. اما فقط توسط A این پیغام می‌تواند ایجاد شود.

$$M = [[M]SA]P^A$$

- در اینجا مخفی سازی و تعیین صحت و سقم دو بخش عمده هستند

- مخفی سازی: رمز گذاری به وسیله کلید عمومی گیرنده (در رمز گذاری کلید عمومی)

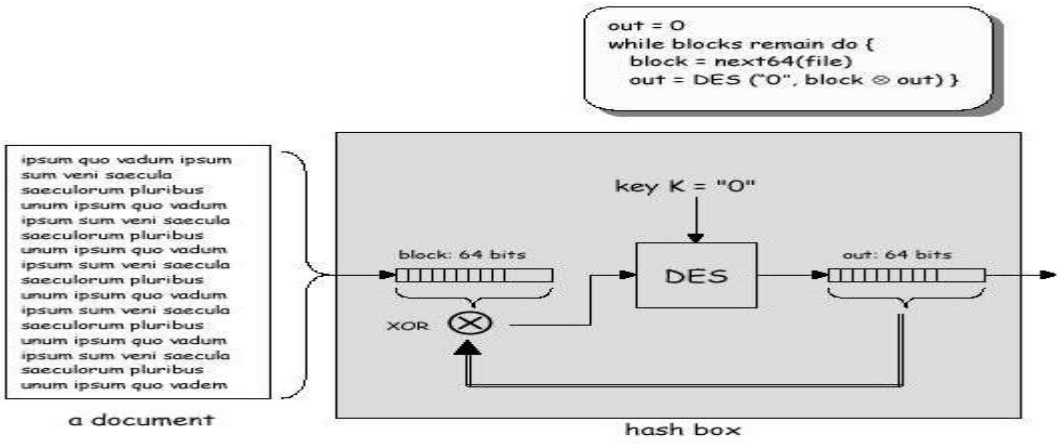
- تشخیص: رمز گذاری توسط کلید مخفی فرستنده

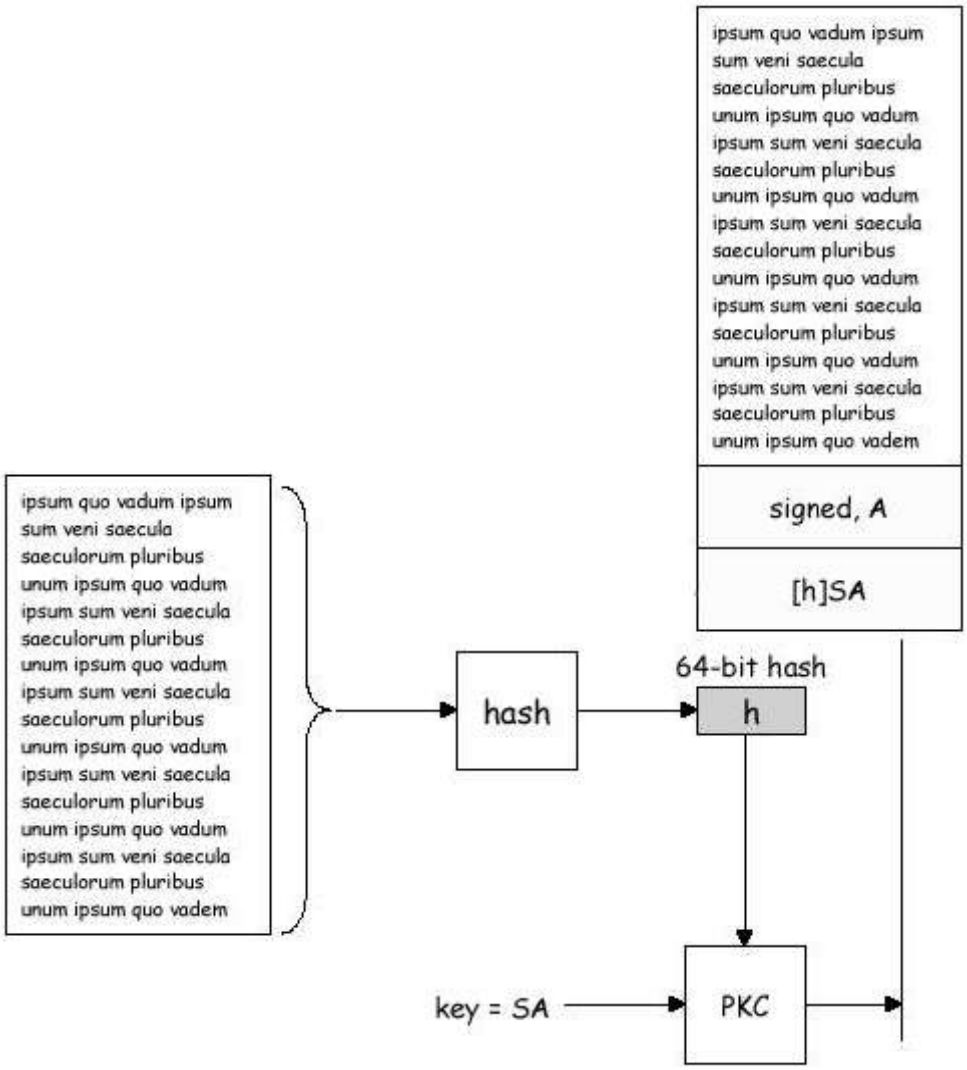
- ما در اینجا می‌توانیم از هر دو مورد استفاده کنیم وقتی که A به B پیغام می‌فرستد. در اینجا B فقط می‌تواند گیرنده و A فقط فرستنده است

[[M]SA]PB

- پهنای باند کم PKC باعث می‌شود که در متن‌های بزرگ، امضاها دوباره کد گذاری شوند

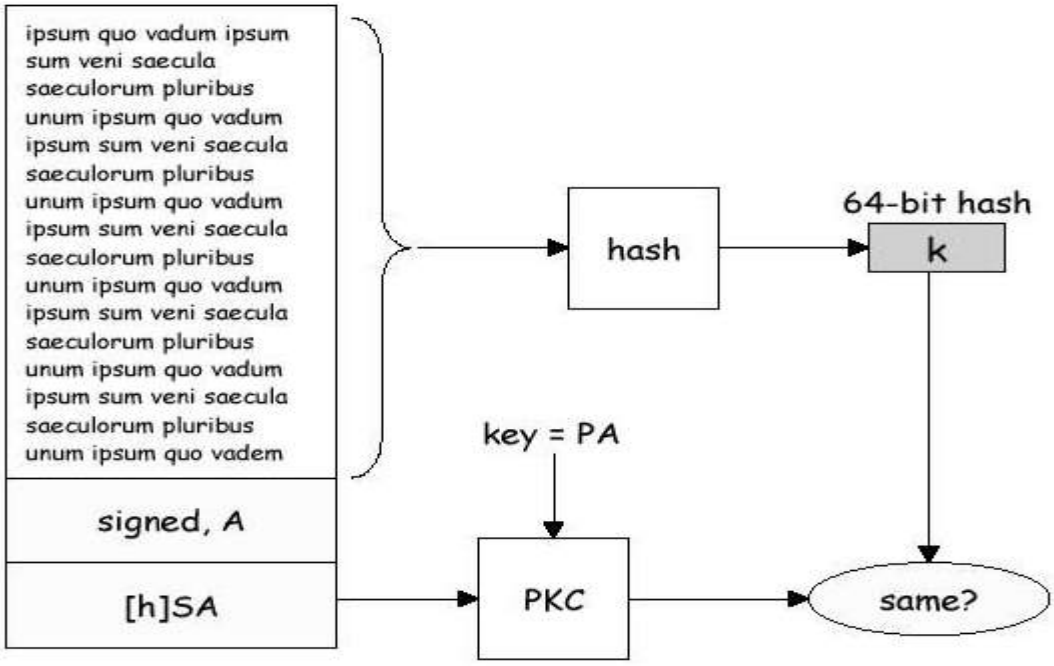
مورد عملی جالب: امضا کردن در متن (مانند email) وقتی که می‌خواهیم مطمئن شویم که شخص A آن را امضاء کرده است و شخص A نتواند آن را رد کند.





What A Does to Sign Document

What B Does to Verify Document Authenticity



The system PGP (Phil Zimmerman's Pretty Good Privacy) validates email this way.

شناسایی کلید عمومی (Public Key Certificates)

کلیدهای عمومی چگونه توزیع می‌شوند؟ باید مکانیزمی برای فراخوانی کلیدهای عمومی (PKI) در نظر گرفت.

صفحات یک پایگاه داده شامل چه نوع فرمی از (A,PA) است؟

این صفحات به دلایل زیر مطمئن نیستند:

۱- شخص B می‌تواند سفارشس را از طریق مدخل (A, PB) بفرستد بنابراین دیگران فکر می‌کنند که PB توسط PA به کار برده شده است. یعنی در اینجا B می‌تواند استراق سمع کننده باشد

۲- حتی اگر B زمانی نیاز به شناسایی خودش، در سفارشی داشت ممکن است این صفحات نتوانند کلید عمومی مربوط به B را شناسایی کنند.

- صحت شناسایی (CA): یعنی تأیید کردن این مطلب که PA کلید عمومی A است.

- به منظور اطمینان داشتن از این که A و PA متعلق به شخص A هستند CA باید A و هر کدام از آنها را شناسایی کند.

۱- CA در اینجا (PA,SA) را تولید می‌کند

۲- شخص A در این جا PA را ایجاد می‌کند و به مقایسه آن از طرف CA پاسخ می‌گوید برای تقاضای CA مثلاً در SA [challenge string] ذخیره می‌شود)

اما با کاربرد این روش‌ها نیز این روش کاملاً مطمئن نیست زیرا:

۱- پایگاه داده‌ها توسط حمله کنندگانی که به کلید مخفی CA دست یافته‌اند می‌تواند سازش کند یعنی می‌تواند Certificates را جابجا کند

تایید کردن کلیدهای عمومی:

۱- اعلان Aمبنی بر این که کلید عمومی او PAاست

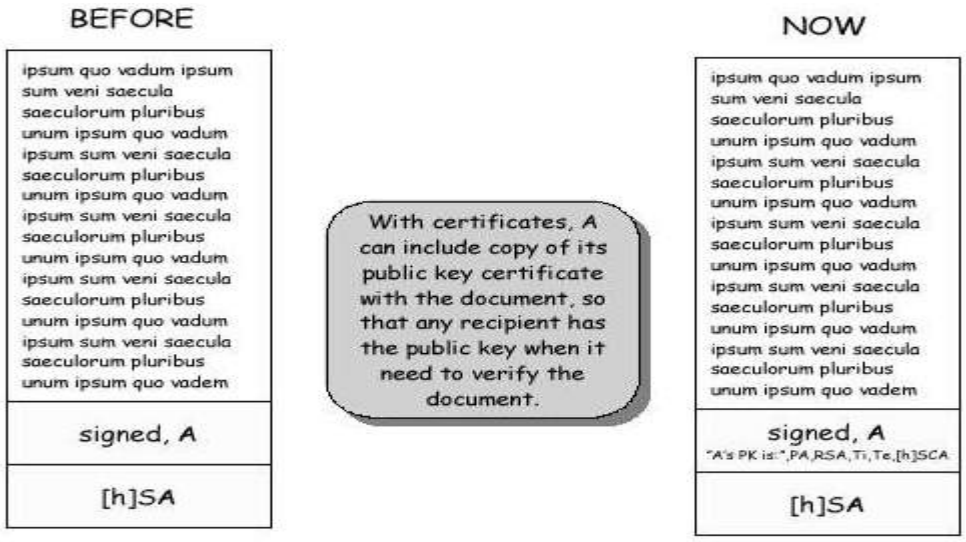
۲- PKC الگوریتمی است که به کار برده می‌شود و تاریخ انقضای آن .

توضیح:

certificate فقط می‌گوید که: شناسایی شخص مانند A بر اساس کلید عمومی او PA انجام گرفته و توسط CA علامت گذاری شده است

certificate نمی‌تواند اظهار کند که A حامل است حامل موضوع شخصی است که معامله را انجام می‌دهد و A را شناسایی می‌کند

یک certificate درست، بستگی به روال‌های شناسایی به کار برده شده از طرف CA و پردازش مراحل تشخیص صحت در آن زمان می‌باشد.



PKI

- شالوده (زیر بنای) کلیدهای عمومی: مجموعه‌ای از پروتکل‌ها، ارباب رجوع‌ها، Serverها و بازرگانان اجازه ارتباط با مشتری تأیید شده را می‌دهد

- درستی PKI بستگی به موارد زیر دارد

۱- با certificate PK صحیح (که توسط CA پیدا کرده است)

۲- درستی هر یک از مراحل پردازش تشخیص صحت

بیشتر مواقع PKI از طرف شرکت کارت‌های اعتباری به کار برده نمی‌شود

(مورد جدید کاربرد PKA در Microsoft است که شبیه امضا کردن است)