امیرحسین شریف ۹۴۱۴۳۰۱۶

رمز طاهر الجمال

مقدمه

در سال ۱۹۸۴ ، یک رمز نگار مصری به نام طاهر الجمال یک شیوه ی رمز نگاری مطرح کرد که بر پایه پروتکل تبادل کلید دیفی – هلمن می باشد. این شیوه رمز نگاری نامتقارن است.

طاهر الجمال یک رمز نگار که دارای ملیت مصری است و در حال حاضر در قید حیات می باشد و او را به نیز عنوان پدر SSLنیز می شناسند. ایشان در زمینه های کلید عمومی،لگاریتم گسسته و چند زمینه دیگر تحقیقاتی را انجام داده است.

الگوریتم رمز طاهر الجمال

هر رمز یا الگوریتم رمزنگاری نامتقارن دارای ۳ بخش می باشد که عبارت اند از : الگوریتم تولید کلید،الگوریتم رمز گذاری و الگوریتم رمز گشایی، که در ادامه این ۳ بخش را با یک مثال توضیح می دهیم. فرض کنید دو کاربر به نام های Alice و Bob داریم که Bob می خواهد پیامی را برای Alice بفرستد،با استفاده از الگوریتم رمز الجمال.

الگوریتم تولید کلید

برای تولید کلید مراحل زیر را به ترتیب انجام می شود.

مرحله اول – یک عدد p که یک عدد اول بزرگ می باشد را انتخاب می کنیم. برای مثال p = ۳۱ در نظر می گیریم و بعد از آن عدد xرا از بازه ی [۲,p-۱] به صورت رندوم انتخاب می کنیم. در این مثال،x=۲۰ انتخاب کردیم.

مرحله دوم – عدد a را از بازه ی [۲,p-۲]، به صورت رندوم انتخاب می کنیم. در مثال a = ۲۵ می گیریم.

مرحله سوم- A را با استفاده از فرمول زیر حساب می کنیم.

$A = x^a \pmod p \Rightarrow A = ۲۰^{۲۵} \bmod ۳۱ = ۵$

پس در اینجا کلید خصوصی یا رمز گشا برای کاربر Alice برابر با مقدار a و کلید های رمز گذار یا کلید عمومی آن A , x است که آن ها برای همه منتشر می کنیم که این کلید های عمومی برای ارسال پیام به Aliceاست و هرکس می خواهد پیامی به آن ارسال کند باید از کلید های عمومی آن استفاده کند.حال فرض کنید کاربر Bob می خواهد پیامی را برای Aliceبفرستد.

الگوریتم رمز گذاری

مقادیر A,x را برای Bob داریم و فرض کنید که پیام اصلی Bob را با X نمایش بدهیم.

مرحله اول – یک مقدار مانند b به صورت رندوم از بازه [۲,p-۲] انتخاب می شود.b=۱۳ انتخاب شده است.

مرحله دوم و سوم – مقادیر زیر را با استفاده از فرمول های که در زیر آمده حساب می کنیم.

$B = x^b \pmod p \Rightarrow B = ۲۰^{۱۳} \bmod ۳۱ = ۱۰$

$Z = A^b \pmod p \Rightarrow Z = ۵^{۱۳} \bmod ۳۱ = ۵$

مرحله چهار- برای رمز گذاری حال باید پیام اصلی Bob که X هست را در Z ضرب کرده و mod pبگیریم.

در این مثال پیام اصلی Bobرا X=۱۵ در نظر گرفته شده.

$Y = X*Z \pmod p \Rightarrow Y = ۱۵ * ۵ \bmod ۳۱ = ۱۳$

مرحله پنجم – حال مقادیر Y که همان پیام رمز شده است و B را از طرف Bob به سمت Alice ارسال می کنیم.

الگوریتم رمز گشایی

در اینجا مقادیر Y,B را داریم.

مرحله اول – مقدار Z` را محاسبه کرده با استفاده از فرمول زیر

$Z` = B^a \pmod p \Rightarrow Z` = ۱۳^{۲۵} \bmod ۳۱ = ۵$

مرحله دوم – برای رمز گشایی و بازیابی مقدار X ، مقدار Y را در معکوس ضربی `Z ضرب کرد.معکوس ضربی را $(Z`)^{-1}$، نمایش می دهند.

$X = Y*(z`)^{-1}$ => X= ۱۳*۲۵ mod ۳۱ = ۱۵

نکاتی در مورد الگوریتم رمز طاهر الجمال

۱- این الگوریتم چون بر پایه ی پروتکل تبادل کلید دیفی – هلمن است پس امنیت آن وابسته لگاریتم گسسته می باشد و این لگاریتم گسسته در واقع تلاش برای به دست آوردن کلید خصوصی یا رمز گشا می کند، که این مسئله سختی است چون این الگوریتم به نوعی نمایی است ، می توان به نوعی گفت که برای پیدا کردن کلید خصوصی باید روش بروث فورس استفاده کرد که به صرفه نمی باشد.

۲- مقدار b که در اینجا مطرح شده،مقداری یکبار مصرف می باشد،یعنی اگر چند بار یک پیام را این روش رمز کنید،هر بار مقدار رمز شده متفاوت خواهند به دلیل b های متفاوت آن،که این مقدار کلید میانی هم گفته می شود. این مقدار محرمانه برای کاربری که این مقدار انتخاب می کند،می ماند و طرف دیگر برای رمز گشایی به آن احتیاجی پیدا نمی کند،پس حتی اگر یک نفوذگر هم آن مقدار پیدا کند،محرمانگی زیر سوال نمی رود.

۳- به مانند الگوریتم تبادل کلید دیفی – هلمن ، باید عدد p اول و بزرگ باشد،می توان از مولد های شبه تصادفی برای تولید عددp استفاده کرد،اگر این عدد به درستی انتخاب نشود،می تواند امنیت این الگوریتم را به طور کامل به مخاطره بیاندازد.

۴- برای پیدا کردن معکوس ضربی از الگوریتم اقلیدس تعمیم یافته استفاده می شود.معکوس ضربی همیشه در این الگوریتم بین مقادیر pو `Z است.

۵- Z,Z`، همان کلید مشترک بین دو کاربر است.

الگوریتم پیدا کردن معکوس ضربی در میدان های متناهی(Z)

از الگوریتمی به نام الگوریتم اقلیدس تعمیم یافته استفاده می شود،برای فهم آسان تر و سریع تر این الگوریتم از یک مثال استفاده می شود.فرض کنید می خواهیم معکوس ضربی ۲۵ در میدان $Z_{۳۱}$ پیدا کنیم.

بنابراین دو عدد ۳۱ و ۲۵ را داریم ، ابتدا عدد بزرگ را نوشته و عدد دوم زیر آن در همان ستون جدول و زیر آن نوشته می شود،حال به شکل عمل می کنیم که باقی مانده تقسیم دو عدد زیر عدد دوم در همان ستون می نویسیم و عدد خارج قسمت تقسیم را در جلو عدد دوم نوشته و حال عدد دوم مانند عدد اول در نظر گرفته و تقسیم را تا جایی که به عدد ۱ در این ستون برسیم ادامه می دهیم. حال در ستون سوم در سطر اول آن عدد صفر را نوشته ،در ستون همان ستون،سطر دوم را عدد ۱ را نوشته و سپس محاسبات بقیه ستونی که در بالا یادشده، برای مثال سطر سوم این ستون می شود،مقدار دو تا بالاتر این ستون که عدد صفر است،منهای ضرب مقدار سطر دوم ستونی که در آن هستیم در سطر دوم ستون دوم ، همین روال برای بقیه محاسبات بقیه سطر های ستون انجام می دهیم تا به سطر آن ستون یاد شده با مقدار ۱ در یک سطر قرار بگیرد آن گاه مقدار ستون سوم که در یک ردیف با ۱ است می شود،معکوس ضربی. توضیحات شاید کمی پیچیده به نظر برسد،به همین دلیل با استفاده از این جدول که در زیر می بینید می توانید راحت و بهتر متوجه ترتیب و محاسبه معکوس ضربی بشوید.

i	r_i	q_i	$t_i=t_{i-۲}-q_{i-۱}t_{i-۱}$
۱	۳۱		۰
۲	۲۵	۱	۱
۳	۶	۴	۰-۱*۱=-۱
۴	۱	۶	۱-۴*(-۱)=۵

در نهایت ۵ در میدان متناهی ۳۱ می شود،معکوس ضربی ۲۵.

فقط سه نکته باید به آن توجه شود:اولا،دو عددی که برای آن معکوس ضربی پیدا می کنیم باید نسبت به یک دیگر اول باشند،دوما،اگر جواب معکوس ضربی منفی شد،آن با مقدار عدد میدان که در که در این مثال ۳۱ می باشد،جمع می کنیم تا عدد حاصل مثبت شود. سوما،اگر در الگوریتم های دیگری نیاز شد،که معکوس ضربی گرفته شود،از همین الگوریتم استفاده می شود و شیوه نشان

دادن گرفتن معکوس ضربی در میدان متناهی به این شکل است که عدد یا متغییر را به توان ۱- نوشته می شود.

پیاده سازی الگوریتم طاهر الجمال در نرم افزار Cryptool

در پیاده سازی الگوریتم طاهرالجمال ، مقادیر p,x,a,b را به صورت دستی وارد می شوند،دو مقدار p,x نیز با استفاده از store variable ذخیره شده و در جای مورد نیاز با استفاده load variable مقدار را استفاده کرده ، با استفاده از چند number operation مقادیر را محاسبه کرده، برای سادگی پیام اصلی X را به صورت دستی و فقط عدد در فایل طراحی این الگوریتم گذاشته که البته می توان برای تغییر آن از string encode وstring decode استفاده کرده تا به توان متن را به decimal و برعکس تبدیل کرده و در نهایت برای این که اطمینان حاصل شود که به درستی رمز نگاری انجام می شود، رمز گشایی را نیز انجام می شود تا آن مقدار با مقدار X مقایسه بشود و هم چنین از comparatorبرای مقایسه این که دو کلید مشترک که دو کاربر محاسبه می کنند یکی باشد،نیز از Boolean استفاده شده است.

نتیجه گیری

الگوریتم طاهر الجمال یکی از الگوریتم هایی است که بر پایه ی پروتکل دیفی – هلمن به وجود آمده است.به نظر اینجانب ، یکی از الگوریتم ها یا پیشرفت هایی است که به کمک تبادل کلید دیفی – هلمن کرده این الگوریتم، کاربرد الگوریتم نیز به مانند الگوریتم دیفی – هلمن البته با تفاوت این که ارسال پیام نیز می تواند صورت پذیرد در آن.

منابع

Wikipedia

ویدیو های آموزشی درس رایانش امن