امیرحسین شریف ۹۴۱۴۳۰۱۶ رمز RSA

مقدمه

رمز RSA در سال ۱۹۷۷ یک سال بعد از انتشار الگوریتم تبادل کلید دیفی – هلمن ساخته شد،این الگوریتم توسط سه فرد به نام های رونالد ریوست ، ادی شامیر و لئونارد آدلمن ساخته شد، به همین علت به آن RSA گفته می شود. این سه فرد تلاش کردند که یک تابع را بیابند که یافتن معکوس آن تابع بسیار سخت باشد.

در سال ۱۹۷۷ این الگوریتم پایه ریزی و به این نام شناخته شد.

الگوریتم RSA

الگوریتم RSA که یک الگوریتم رمزنگاری با کلید نامتقارن است که دارای ۳بخش می باشد که با یک مثال آن را به طور کامل توضیح می دهیم. این ۳ بخش شامل، الگوریتم تولید کلید،الگوریتم رمز گذاری و رمز گشایی می باشد.

الگوریتم تولید کلید

مرحله اول- اعداد اول qوp را به صورت تصادفی با دو ویژگی ، باید فرد باشند و باید m بیتی باشند یعنی این اعداد نباید کوچک باشند،انتخاب می کنیم.

برای مثال فرض کنید که p = ۱۷ و q = ۱۱ باشد.

مرحله دوم – دو عدد qوp در هم ضرب کرده و مقدار حاصل در متغییری به نام n نگه داری کنید.

$n = p*q \quad => \quad n = ۱۷*۱۱ = ۱۸۷$

مرحله سوم - $\Phi(n)$ را با استفاده از فرمول زیر محاسبه می شود.

$\Phi(n) = (p-۱)*(q-۱) \quad => \quad \Phi(n) = ۱۶*۱۰ = ۱۶۰$

مرحله چهارم – مقدار e از بازه ی $[2, \Phi(n) - 1]$ به صورت تصادفی انتخاب می کنیم با این شرط که $\Phi(n)$ و e نسبت به هم اول باشند. در مثال ، e=۳ در نظر می گیریم.

مرحله پنجم – معکوس ضربی e را در میدان Z $\Phi(n)$محاسبه کرده و آن را d می نامیم.

زوج (n,e) به عنوان کلید رمز گذار و d به عنوان کلید رمز گشا در نظر بگیرید.

پس مقدار d = ۱۰۷ .

الگوریتم رمز گذار

اگرمتن رمز شده را Y و متن اصلی را X در نظر بگیریم . با فرمول زیر می توان متن رمز شده را به دست آورد

$Y = X^e \bmod n$

الگوریتم رمز گشا

اگرمتن اصلی را X در نظر بگیریم و متن رمز شده را Y . با فرمول زیر می توان متن اصلی را به بازیابی کرد :

$X = Y^d \bmod n$

حال باتوجه به مثال در قبل زده شده و مقادیری را به دست آمده ، اگر فرض کنیم که مقدار متن اصلی X=۲۰ باشد آن گاه

$Y = X^e \bmod n \Rightarrow Y = ۲۰^۳ \bmod ۱۸۷ = ۱۴۶$

$X = Y^d \bmod n \Rightarrow X = ۱۴۶^{۱۰۷} \bmod ۱۸۷ = ۲۰$

نکاتی در مورد الگوریتم RSA

۱- الگوریتم RSAمورد حملاتی زیادی بوده است که اگر آن ها را دسته بندی کنیم به ۳ دسته بندی کلی می رسیم که عبارت اند از :

- حملات مربوط به قرارداد،که معمولا برای زمانی است که این پروتکل دارای ضعف ساختاری باشد.
- حملات مربوط به کانال جانبی که استفاده درخت آسیب پذیری اتفاق می افتد که مربوط به ضعف پیاده سازی می باشد.
- حملات ریاضی که بهترین نوع حمله می باشد،که برای پیدا کردن مقدار d به کار می رود ولی باید زمان بهینه داشته باشد که با مسئله تجزیه به عوامل اول یا(integer factorization) روبه رو می شویم.

۲- قضیه باقی مانده چینی می باشد برای بدست آوردن برای بدست مقادیر x , e بکار می رود.

۳- الگوریتمی که در اینجا مطرح شده بیش تر برای آموزش است و باید خیلی مقادیر دیگر به متن X یا متن اصلی اضافه بشود تا بتوان یک رمز گذاری ایمن داشت .

۴- تابع Φ در این الگوریتم همان تابع فی اویلر می باشد.

۵- الگوریتم RSAچون از توان در ریاضیات استفاده می کند و گاهی اوقات این کار برای بعضی دستگاه ها که اولویت انرژی آن ها مطرح است،انرژی بسیار زیادی می گیرد،پس می توان مقدار eکوچک در نظر گرفت .

۶- باید در انتخاب p,q بسیار دقت کرد،به این دلیل که اگر درست و ایمن انتخاب نشوند امنیت این رمز به سادگی از بین خواهد رفت،از توابع و مولد های تولید اعدادشبه تصادفی می توان استفاده نمود.

نحوه ی پیاده سازی الگوریتم RSA در نرم افزار Cryptool

مقادیر pوe, q را بدست صورت دستی باید وارد کرد و پس از یک متن اصلی را باید وارد کرد،در این پیاده سازی در نرم افزار فقط اعداد در نظر گرفته شده اند. یعنی متن اصلی می تواند یک عدد باشد و مطابق الگوریتم این مقدار رمز می شود که می توان آن را مشاهده کرد و در نهایت رمز گشایی نیز روی آن انجام می شود تا به توان مقدار بازیابی شده را نیز دیده شود به عنوان خروجی و چند number operation برای محاسبات استفاده شده .خروجی یکی مقدار بازیابی شده متن اصلی،دیگری کلید خصوصی و اخرین نیز متن رمز شده می باشد.

اگر اعدادی که در مثال که برای فهم بهتر الگوریتم RSA نتیجه یکسان با مثال دریافت می کنیم.

نتیجه گیری

الگوریتم RSA یکی از پرکاربردترین رمز هاست که از آن استفاده می شود، اما چیزی در اینجا گفته شده بیش تر جنبه آموزشی دارد پس باید تغییراتی روی آن انجام بشود تا بتوان به عنوان یک رمز ایمن از آن استفاده کرد. در بعضی شبکه های کامپیوتری نیز آن استفاده می شود ولی چون رمز های نامتقارن کند تر از رمز های متقارن هستند برای رمز کردن داده های ارزشمند از این الگوریتم استفاده می شود.

منابع

Wikipedia

ویدیو های آموزشی درس رایانش امن