امیرحسین شریف ۹۴۱۴۳۰۱۶ رمز AES

مقدمه

به دلیل این که در رمز هایی مانند ...., DES ,۳DES دارای مشکلاتی بودند و حملاتی موثر علیه آن ها صورت می گرفت.یک مسابقه ای برای طرح یک رمز ایمن مطرح شد.در انتها رمز به نام rijndael که توسط دو رمز نگار بلژیکی به نام های ژوآن دیمن و وینست ریجمن ساخته شده بود،برنده مسابقه شد.البته در مسابقه مطرح شده رمز می بایست دارای شرایطی می بود،که در رمز rijndael رعایت شده بود،این رمز rijndael در سال ۲۰۰۱ مطرح شد و بعد از آن با تغییراتی که NIST روی آن انجام داد،به نام AES که مخفف Advanced Encryption Standard ، مطرح شد و به عنوان استاندار در حال مطرح شده است.

البته این رمز می تواند کلید های با اندازه های ۱۲۸و۱۹۲و۲۵۶بیت را پشتیبانی کند که کلید اندازه ی ۱۲۸ بیت آن به عنوان استاندار پذیرفته شده است.

الگوریتم AES

الگوریتم AES ، به مانند الگوریتم DES دارای مراحلی تکراری می باشد و شامل الگوریتم رمز گذاری و رمز گشایی و الگوریتم زمان بند کلید و تابع g و RC می باشد،که در ادامه آن را توضیح می دهیم.

این رمز از ساختار فایستل استفاده نمی کند. از محاسبات در میدان گالوا استفاده می کند. طول block متن اصلی در رمز AES،۱۲۸ بیت است و همین طور طول block خروجی. در رمز AES از یک S-box واحد استفاده می شود که برای آشنایی بیش تر با عملکرد آن می توانید در موردآن جست وجو کنید.

الگوریتم رمز گذاری

در الگوریتم رمز گذاری AES، ۴لایه در هر مرحله ی آن تکرار می شوند،به جز مرحله آخر که در ۳ لایه در آن می باشد. هر ۴ لایه یک مرحله است و مرحله آخر هم که ۳ لایه می باشد،اگر کلید را ۱۲۸ بیت در نظرگرفته شود،رمز گذاری شامل ۱۰ مرحله می شود،اگر ۱۹۲ بیت باشد،شامل ۱۲ مرحله و ۲۵۶ بیت شامل ۱۴ مرحله می باشد. ابتدا شروع به معرفی هر لایه می کنیم.

اولین لایه ، لایه ی جانشینی بایتی می باشدکه بلاک ورودی برابر ۱۲۸ بیت یا ۱۶ بایت است.عملکرد این لایه به این شکل است که در s-box مقدار تکراری وجود ندارد و در آن مقادیر به صورت hexهستند که سطر و ستون این s-box هشت تایی با نیبل است.ورودی که گرفته با توجه به عملکرد آن خروجی را گرفته ، خروجی این لایه است.

لایه دوم که نام آن،شیفت سطری می باشد،خروجی لایه قبل را گرفته به صورت ستونی و به ترتیب ، خروجی ۱۶ بایت را در یک ماتریس ۴*۴ می گذارد.تاکید می شود که اعداد به صورت hex می باشند. عملکرد این لایه این صورت است که شیفت چرخشی به سمت چپ می دهیم.البته همان طور که از نام این لایه پیدا است سطر های آن ماتریس این گونه شیفت می دهیم که سطر اول را بدون تغییر می گذاریم،سطر دوم را یک بایت به سمت چپ شیفت می دهیم،سطر سوم را دو بایت و سطر چهارم را سه بایت. حال خروجی به لایه ی بعدی می فرستیم.

لایه سوم که نام آن ترکیب ستونی نام دارد که مانند لایه دوم ، در یک ماتریس ۴*۴ به ترتیب و به صورت ستونی خروجی های لایه دوم را می نویسیم. حال یک ماتریس در یک بردار ضرب می شود و یک بردار می دهد. فقط نکته ای وجود دارد این است که بایت در بایت ضرب می شود،با کمک میدان های گالوا این ضرب را انجام می شود. برای راحتی کار این گونه فرض کنید بردار D خروجی این لایه است و بردار C خروجی لایه قبل و یک ماتریس که سطر اول آن به تغییر ضرب می شود و در سطر دوم یک بایت به سمت راست شیفت چرخشی می خورد و در سطرسوم،دو بایت و در سطر آخر،۳ بایت شیفت می خورد. فرمول آن به این شکل است:

$$\begin{bmatrix} D_i \\ D_{i+1} \\ D_{i+2} \\ D_{i+3} \end{bmatrix} = \begin{bmatrix} ۰۲ & ۰۳ & ۰۱ & ۰۱ \\ ۰۱ & ۰۲ & ۰۳ & ۰۱ \\ ۰۱ & ۰۱ & ۰۲ & ۰۳ \\ ۰۳ & ۰۱ & ۰۱ & ۰۲ \end{bmatrix} * \begin{bmatrix} C_i \\ C_{i+1} \\ C_{i+2} \\ C_{i+3} \end{bmatrix}$$

که در اینجا i=۰,۴,۸,۱۲ است. در این لایه خروجی ها را به ترتیب کنار هم می گذاریم.

لایه چهارم،که لایه آخر نیز می باشد،لایه اضافه کردن کلید نام دارد.(در مورد زمان بند کلید و توابع بعدا توضیحاتی داده خواهد شد)، خروجی لایه سوم وارد لایه اضافه کرد کلید شده و کلید مرحله XOR می

شود. با توجه توضیحاتی در بالا گفته شد،تعداد تکرار این چهار لایه می دانید،فقط در مرحله آخر همه ی این تکرار لایه ها،لایه ی ترکیب ستونی وجود ندارد.

در ابتدا متن اصلی و کلید وارد می شوند،ابتدا یک k_0 به متن اصلی اضافه می شود،k_0 همان کلید مرحله صفرام است در موردش توضیح داده خواهد و بعد مراحل ، که هر مرحله همان ۴ لایه هستند،تکرار می شود به اندازه ای که باید، با توجه اندازه کلید و بعد از آن خروجی همان متن رمز شده می شود.

زمان کلید و تابع g و RC

در رمز AES چون یک تبدیل لایه ی صفر داریم پس به تعداد تکرار+۱ کلید مرحله تولید می کنیم،یعنی اگر ۱۰ مرحله تکرار باشد،۱۱ کلید و اگر ۱۲ مرحله تکرار ۱۳ کلید و اگر ۱۴ مرحله ، ۱۵ کلید داریم. در ابتدا که متن اصلی وارد می شود، K_0 با آن XOR شده وسپس خروجی وارد مراحل می شودو کلید مرحله صفرم همان کلید اصلی است.

در زمان بند کلید از کلمات استفاده می شود،هرکلمه با توجه به معماری سیستم ۳۲ یا ۶۴ بیتی هستند،دراین جا فرض کنید هر کلمه ۳۲ بیتی است. پس برای طول کلید ۱۲۸ بیتی ، هر کلمه ۴ بایت است پس ، ۴ بایت ضرب در ۱۱ کلید فرعی می شود،۴۴ کلمه که برای تولید کلید ها برای الگوریتم AES نیاز می شود.برای ۱۹۲ و ۲۵۶ بیت نیز به ترتیب دارای ۵۲و۶۰کلمه است.

در اینجا در مورد AES که طول کلید آن ۱۲۸ بیت است،فقط در مورد آن در مورد تولید کلید های مرحله آن می گوییم،در مورد بقیه AES با طول کلید های ۱۹۲ و ۲۵۶ بیت می توانید جست و جو کنید،روش کار یکی است. حال زمان بند کلید AES-۱۲۸ به شرح زیر می باشد،

ابتدا کلمات را با w نمایش می دهیم.در ابتدا ما چهار کلمه w[۰],w[۱],w[۲],w[۳] را به طور مستقیم و بدون هیچ تغییری به عنوان کلید مرحله صفر ام که همان کلید اصلی نیز می باشد با متن اصلی XOR می کنیم و بعد از آن طبق این الگو که تا چند لحظه دیگر نوشته می شود،بقیه w ها را تولید کرده وکلید مراحل دیگر را می سازیم. الگو برای ساخت ، هر بار ۴ کلمه دیگر را به دست می دهد. الگو به شکل است که در w[۳] وارد یک تابع g می شود،(در مورد آن توضیح داده خواهد شد) و بعد خروجی آن با w[۰] ، XOR می شود و به w[۴] تشکیل می شود. w[۵] برابر می شود با w[۴]،XOR ،w[۱] و w[۶] می شود،w[۵]،XOR،w[۲]، و تا ۴ تا کلمه تشکیل شود سپس به عنوان مرحله استفاده می شود،یعنی این

روال این گونه ادامه می کند کلمات تشکیل شده با کمک تابع gوXOR کلمات و بعد به عنوان کلید مرحله استفاده می شود و تا تولید کلید آخرین مرحله.

حال تابع g ، در واقع ورودی ۳۲ بیت را گرفته به ۴ بایت می شکند و سپس یک شیفت چرخشی بایتی به سمت چپ می دهد و بعد از آن تک تک بایت ها به s-box یی که در مرحله جانشانی بایتی بود،دقیقا همین s-box را به هر بایت داده و خروجی را می گیریم،فقط در مورد چپ ترین خروجی بایک مقداری به اسم RC[i]، XORشده و سپس هر ۴ بایت را به هم می چسبانیم که این همان خروجی ۳۲ بیتی تابع g می باشد.

RC[i]، در واقع ضریب هر مرحله می باشد،که در استاندار AES دقیقا مقادیر آن وجود دارد وi یعنی مرحله i ام. در واقع یک ثابت مرحله می باشد.

الگوریتم رمز گشایی

فرض کنید کلید ها تولید شده اند و در جایی ذخیره شده باشند،فقط باید به ترتیب معکوس از آن ها استفاده بشود.معکوس عمل XOR خودش است،این می شودمعکوس لایه اضافه کردن کلید.

معکوس لایه ی ترکیب ستونی ، در واقع باید ضرب در معکوس ماتریس بشود تا این لایه معکوس شود،ماتریسی که در رمز نگاری AES استفاده می شود،معکوس پذیر است.

معکوس لایه انتقال سطری فقط باید مانند ترتیبی که در این لایه بود،معکوس آن یعنی شیفت چرخشی به سمت راست با همان ترتیب.

معکوس لایه جانشینی بایتی نیز چون s-box که در این رمز نگاری استفاده می شود معکوس پذیر با توجه آن می شود گفت که این لایه نیز معکوس شده است.

متن رمز شده را وقتی وارد می کنیم ابتدا ۳ مرحله داریم که معکوس لایه های اضافه کردن کلید و انتقال سطری جانشینی بایتی است و در بقیه مراحل لایه ترکیب ستونی بعد معکوس لایه اضافه کردن کلید و قبل از معکوس لایه ی انتقال سطری است. بعد از تکرار این مراحل به اندازه که باید،متن اصلی بدست می آید.

نکاتی در مورد رمز AES

۱- اگر طول بلاک متن ورودی مضرب صحیحی از طول بلاک نباشد از padding استفاده می شود و همین طور به مانند الگوریتم DES و ... از mode of operations می توان برای این رمز نیز استفاده کرد.
۲- این رمز امنیت CPA ندارد، این رمز deterministic یا قطعی می باشد.
۳- محاسبات ضرب و جمع آن در میدان گالوا $GF(2^8)$ است برای رمزAES
۴- تا به حال هیچ حمله تحلیلی علیه این رمز موفق نبوده و تا به حال کسی نتوانسته است که آن را به طور مستقیم رمز AES بشکند.
۵- در مورد زمان بند کلید تابع g که هست ، برای کلید ۲۵۶ بیت یک تابعh نیز می باشد.
۶- حمله جست و جو فراگیر برای این رمز قابل اجرا نمی باشد، به دلیل طول کلید آن،تلاش هایی برای بهبود آن شده ولی هیچ کدام موفقیت چشمگیری نداشته اند.
۷- برای امنیت کوتاه،میان و بلند مدت از طول کلید های ۱۲۸،۱۹۲،۲۵۶ رمز AES استفاده می شود.

پیاده سازی الگوریتم AES در نرم افزار Cryptool

در نرم افزار cryptool ، یک آیتم AES داریم که تنظیمات آن شامل،اولین برای است می خواهید از رمز AES استفاده کنید یا Rijndael،دومین برای نتظیم رمز گشایی یا رمز گذاری است،سومین تعیین اندازه کلید می باشد و در چهارم chaining mode یا همان mode of operations که گفته شد،آخرین نیز تنظیم نوع padding می باشد.

ورودی هایی که می گیرد این رمز hex یا باینری می باشد پس با استفاده از string decode متن اصلی را تبدیل کرده و بعد رمز می کنیم که می توان در نرم افزار مشاهده کرد و دیگر این که به مانند قبل از رمز گشایی با کلید یکسان استفاده می کنیم تا مطمئن شویم متن رمز شده،را بازیابی کرده و این که بتوانیم با متن اصلی نیز مقایسه بکنیم.

با استفاده یک آیتم دیگر از کلید اصلی به طور مستقیم استفاده با استفاده از آن ایتم که کلید تولید می کند از تابع hash sha-۲۵۶ نیز استفاده می کند. یعنی از یک تابع استفاده می کند و ورودی نیز گرفته و کلید تولید می کند.

نتیجه گیری

رمز AES یکی از رمز های امن در حال حاضر می باشد.اگر در جایی به صورت اصولی پیاده سازی بشود،تا سالها امنیت اطلاعات آن سازمان یا شرکت تضمین است و چون رمز آن از نوع متقارن نیز می باشد،پس سرعت نسبت بالایی برای رمز کردن داده ها نیز دارا است.

منابع

Wikipedia

ویدیو های آموزشی درس رایانش امن