امیرحسین شریف ۹۴۱۴۳۰۱۶ رمز DES

مقدمه

الگوریتم DES که در دهه ی ۷۰ میلادی توسط آمریکا به عنوان یک استاندارد کد گذاری مطرح شد و می بایست این را برای نرم افزار ها شرکت های نرم افزاری برای محافظت از نرم افزار های تولیدیشان استفاده می کردند. DES مخفف Data Encryption Standard بود. این الگوریتم به سفارش سازمان NIST، توسط شرکت IBM ساخته شد.

البته هنوز هم اسناد آن منتشر نشده است،یعنی به چه علت هر کدام قسمت های الگوریتم به این شکل هایی ساخته شده اند،هنوز جامعه رمزنگار در مورد آن اطلاعی ندارد.

در حال حاضر استفاده از این رمز منسوخ شده به دلایلی که بعدا در همین گزارش مطرح گفته می شود.

الگوریتم رمز DES

الگوریتم DES از ساختار فایستل استفاده می کند. هر Block ورودی آن برابر ۶۴ بیت است. حال الگوریتم های رمز گذاری و رمز گشایی و زمان بند کلید را شرح می دهیم. این الگوریتم از ساختاری تکراری برای رمز گذاری و رمز گشایی استفاده می کند.

الگوریتم رمزگذاری

ابتدا متن اصلی یا plain text وارد می شود و یک جایگشت اولیه روی آن صورت می گیرد. متن اصلی به ۲ قسمت مساوی ۳۲بیتی تقسیم می شود. ۳۲ سمت راست یا کم ارزش را R_0 و L_0 را ۳۲ بیت سمت چپ یا پرارزش می نامیم. حال R_0بدون هیچ تغییری برابر با L_1 می گذاریم و برای ساخت قسمت R_1، به این صورت عمل می شود که R_0 و کلید مرحله ۱ و وارد یک تابع fمی شوند(در مورد کلید مرحله و تابع fبعدا توضیحاتی داده خواهد شد)،پس از آن خروجی تابع fبا مقدار L_0،XOR شده.

حال که L_1 , R_1 بدست آوردیم مانند بالا ، مراحل تکرار کرده تا L_2,R_2برسیم و این رویه آن را به اندازه ی ۱۶ ادامه داده و پس آن یک جایگشت که دقیقا معکوس جایگشت اولیه که متن اصلی وارد شده بود را انجام می دهیم و متن رمز شده بدست می آید. اگر دقت کرده باشید در واقع هر بار نصف از متن در مرحله رمز می شود.

الگوریتم زمان بند کلید و تابع f

کلیدی که در بالا گفته شده در واقع یک کلید اصلی ۶۴بیت وارد الگوریتم DES می شود، در ابتدا یک جایگشت اولیه انجام داده وسپس از هر بایت این کلید اصلی یک بیت به عنوان بیت parity در نظر گرفته و آن ها کنار می گذاریم پس حال ۵۶ بیت باقی مانده به عنوان کلید در الگوریتم زمان بند کلید استفاده می شود. بعد آن ها به دو قسمت ۲۸ بیتی شکسته می شود،قسمت سمت سمت چپ را C_0 و قسمت سمت راست را D_0 نام گذاری می کنیم. شیفت چرخشی برای هر یک از بیت های هر یک از قسمت های C_0,D_0 به سمت چپ انجام می شود و بعد ازآن C_0,D_0 تبدیل به D1C1 می شود و در این جا یک جایگشت دوم انجام شده و کلید مرحله اول وارد تابع f می شود و در اینجا این شیفت چرخشی برای این ۱۶ مرحله و بعد جایگشت انجام می شود تا کلید های ۱۶ مرحله تولید و استفاده بشوند.

شیفت چرخشی به سمت چپ برای مراحل ۱و۲و۹و۱۶ یک بیت باید باشد و برای مراحل دیگر به جز این مراحل باید دو بیت باشد.

تابع f در واقع تابعی بسیار مهم می باشد،چراکه امنیت رمز DES بسیار وابسته به انتخاب این تابع است اگر این تابع به درستی پیاده سازی نمی شد امنیت کل این رمز که در گذشته استفاده می شد،خطر می افتاد.

تابع f، به این شکل کار می کرد که کلید مرحله iام وارد می شد و همین طور R_{i-1} ولی چون R_{i-1}، ۳۲ بیتی بود و کلید مرحله برابر با ۴۸بیت بود نمی تواستند بایک دیگر XOR بشود پس ابتدا R را توسیع یا بسط داده تا به ۴۸ بیت برسد با تکرار کردن بعضی بیت ها،می توانید در اینترنت جست وجو کنید که کدام بیت ها باید تکرار بشوند،پس از آن با کلید مرحله XOR می شود.حال ۴۸ بیت را به ۸ قسمت ۶ بیتی تقسیم کرده و هر کدام در یک S-box به ورودی داده و ۴ بیت خروجی می گیریم از هر کدام و بعد آن ها را بهم چسبانده ۳۲ بیت تشکیل شده را و یک جایگشت به آن ۳۲ بیت داده و این می شود،خروجی تابع f.

درمورد s-box های و عملکرد آن ها دررمز DES می توانید در اینترنت جست و جو کنید و به طور دقیق درباره ی نحوه ی عملکرد آن ها ببینید.

الگوریتم رمزگشایی

مراحلی که در رمز گذاری را به طور عکس و همین طور کلید مراحل را به طور عکس استفاده کنیم،می-شود الگوریتم رمز گشایی DES.

نکاتی در مورد رمز DES

۱- در رمز های متقارن بیش تر مواقع متن اندازه ی صحیحی از block نمی باشد،برای این که این مشکل حل بشود،از padding استفاده می شود.
۲- امنیت رمز DES در زمان خودش قابل قبول بوده ولی چون طول کلید موثرآن ۵۶ بیت بوده ، با حمله جست و جو فراگیر به راحتی قابل شکستن بوده است. به دلیل طول کلید کوتاه به راحتی می توان آن را شکست و حتی اگر آن را ۶۴ بیت در نظر بگیریم.حملات جست و جو فراگیر تا ۱۲۸ بیت قابل قبول هست.
۳- در مورد رمز های متقارن به شکل Block برای این که بتوانند متن رمز شده نیز کمی پیچیده تر کنند از mode of operation هایی استفاده می شوند که عبارت اند از ECB,CBC,CFB,OFB می باشد. می توانید در مورد آن ها در اینترنت جست و جو کنید.

نحوه ی پیاده سازی رمز DES در نرم افزار Cryptool

همه ی رمز DES در یک آیتم این نرم افزار است،نتظیماتی که برای آن وجود دارد،شامل، برای رمز گذاری یا رمز گشایی استفاده بشود،chaining mode که همان mode of operation که پیش تر گفته شد،قابل نتظیم می باشد و همین طور نوع padding که استفاده می کنیم. ورودی ها بایدبه شکل بایت باشند،پس اگر متن ورودی به شکل text باشد باید با string decode آن تبدیل کرده و

سپس به عنوان ورودی به DES داده بشود،پس از آن که خروجی گرفته شد DES می توان بایک string encode ، آن به شکل های قابل نتظیم در آن به عنوان متن رمز شده نشان داد و برای اطمینان از این که این الگوریتم درست کار می کند در نرم افزار از خروجی رمز شده و کلید یکسان رمز گشایی را انجام داده و با متن اصلی وارد شده چک می کنیم. فقط برای این که از کلید اصلی به طور مستقیم استفاده نکنیم آن چیزی به عنوان کلید اصلی می دهیم از یک آیتم استفاده کردیم که کلید اصلی را گرفته و کلیدی اصلی دیگری برایمان بسازد و با کمی تغییر و این بشود،کلید اصلی ما.

نتیجه گیری

الگوریتم رمز نگاری DES ، دیگر امن نیست به چند دلیل :

۱- طول کلید کوتاه آن ،طول کلید موثر ۵۶
۲- اسنادی که براساس آن این الگوریتم ساخته شده ، هنوز هم منتشر نشده است.
۳- با توجه به قانون مور ، بعد از کمی پیشرفت با استفاده از روش brute-force به راحتی این رمز شکسته می شود.

منابع

Wikipedia

ویدیو های آموزشی درس رایانش امن