امیرحسین شریف ۹۴۱۴۳۰۱۶ رمز triple DES

مقدمه

در ابتدا اگر در مورد فایل توضیحات مربوط به DES را نخوانده اید.اکیدا توصیه می شود،ابتدا آن را مطالعه کرده و بعد از به مطالعه این فایل بپردازید. رمز DES دارای مشکلاتی بود و جامعه رمز نگاری تلاشی برای رفع آن انجام می داد،الگوریتم های مختلفی اعلام شد،که یکی از آن ها توسط شخصی ساخته شده بود،۳DES یا tripleDES بود،بدین معنا که ۳ بار از رمز DES استفاده بشود.

رمز ۳DES

الگوریتم رمز گذاری و رمز گشایی و زمان کلید رمز DES است.فقط چند نکته را بیان می کنیم:

۱- در واقع متن ورودی وارد DES اول می شود با کلید K_1 بعد متن رمز شده ی خروجی به عنوان ورودی وارد DES دوم شده با کلید K_2 متن رمز شده خروجی وارد سومین شده DES با کلید K_3 رمز می شود.

۲- اما چون ساختار ۳DES، خیلی سخت افزار زیادی می خواست و هزینه بر در زمان خودش محسوب می شد،ساختاری که در نکته ی ۱ گفته شده به این شکل تغییر و پیاده سازی شد که در ابتدا متن ورودی با DES و کلید K_1 رمز می شود، سپس متن رمز شده با کلید K_2 رمز گشایی می شود و در نهایت متن رمز شده در این جا با کلید K_3 رمز گذاری می شود.

۳- هیچ کدام از کلید های K_1,K_2,K_3 نباید باهم برابر باشند،در غیر این صورت اگر دوتا دوتا باهم برابر باشند یعنی انگار فقط با یک بار با DES رمز گذاری شده است متن اصلی و اگر ۳ تا مثل هم باشند باز هم انگار که یک بار با DES رمز گذاری شده است،متن اصلی.

۴- طول بلاک ورودی و خروجی ۶۴ بیت و طول کلید ۱۶۸ بیت است.

۵- برای باید مراحل را برعکس کرده و متن رمز شده را به آن داده بشود.

نکاتی در مورد رمز ۳DES

۱- رمز ۳DES آسیب پذیر بود، حملات meet in the middle و جست و جو فراگیر برای آن موثر بود.
۲- در حمله جست و جو فراگیر اگر کلید را برابر $۲^{۱۶۸}$ در نظر بگیریم خیر ولی با توجه به یکسری محاسبات معلوم شد که کلید موثر درواقع $۲^{۱۱۲}$ می باشد و به راحتی می شود،این رمز را شکست.
۳- در مورد حمله ی meet in the middle نیز همین اتفاق باعث شد که این حمله نیز موثر واقع بشود.
۴- تلاشی برای سفید سازی کلید برای الگوریتم ۳des انجام شد ولی باز هم حملات بالا موثر بودند. اگر بعد از سفید سازی کلید ، کلیدی پیدا می شد،توسط نفوذگر که برای یک متن رمز شده که آن را به یک متن معتبر می رساند ولی پیام دیگری جواب نمی داد،به آن مثبت کاذب گفته می شد. با زیاد کردن تعداد پیام ها و استفاده از دو یا چند متغییر برای جواب گرفتن از کلید حدس زده شده ،می توانست احتمال رسیدن به مثبت کاذب را نفوذگر به نزدیک صفر برساند.

نحوه ی پیاده سازی رمز ۳DES در نرم افزار Cryptool

برای پیاده سازی از ۳ آیتم DES استفاده کرده و مانند همان چیزی که گفته شد از ۳ کلید استفاده شده که از ۳ آیتم HKDF sha-۲۵۶ برای تولید کلید استفاده شده که کلید ها تصادفی نیز باشند، ۳آیتم des اولی با کلید ۱ رمز می کند دومین با کلید ۲ رمز گشایی کرده و سومین با کلید ۳ رمز گذاری می کند. هر کدام از آن ها را می توان با استفاده از تنظیماتی که هر کدام DES ها دارند،تنظیماتی متفاوتی روی آن ها انجام داد برای اطمینان از این که رمز گذاری و رمز گشایی به درستی انجام می شود، حال کلید ها و DES ها به مانند رمز گذاری به صورت متوالی چیده فقط تنظیمات آن برای رمز گشایی و همین طور ترتیب وارد شدن کلید ها را برعکس می کنم تاعملیات رمز گشایی انجام شود،که در نرم افزار آن را انجام داده و می توان خروجی اش را با متن اصلی مقایسه و چک کرد.

نتیجه گیری

رمز ۳DES نیز به مانند رمز DES چون دارای آسیب پذیری بود،استفاده از آن در حال حاضر منسوخ شده است و رمز ناامن است.

منابع

Wikipedia

ویدیو های آموزشی درس رایانش امن