
بسم الله الرحمن الرحيم

دانشگاه صنعتی اصفهان
دانشکده برق و کامپیوتر

ارزیابی تحلیلی الگوریتمهای رمز قالبی با تاکید بر حمله خطی

پایان نامه کارشناسی ارشد مهندسی برق - مخابرات

قدمعلی باقری کرم

استاد راهنما

دکتر محمد دخیل علیان

۱۳۸۱

دانشگاه صنعتی اصفهان
دانشکده برق و کامپیوتر

پایان نامه کارشناسی ارشد رشته برق (مخابرات) آقای قدمعلی باقری کرم

تحت عنوان

ارزیابی تحلیلی الگوریتمهای رمز قالبی با تاکید بر حمله خطی

در تاریخ ۱۲/۷ /۱۳۸۱ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهائی قرار گرفت.

۱- استاد راهنمای پایان نامه — دکتر محمد دخیل علیان

۲- استاد مشاور پایان نامه — دکتر سید محمود مدرس هاشمی

سرپرست تحصیلات تکمیلی دانشکده — دکتر علیمحمد دوست حسینی

ای خوشا خاطر ز نور علم مشحون داشتن
تیرگیها را از این اقلیم بیرون داشتن

عقل و علم و هوش را با یکدگر آمیختن
جان و دل را زنده زین جانبخش معجون داشتن

بر خود لازم می دانم که از زحمات بی دریغ جناب آقای دکتر محمد دخیل علیان به خاطر راهنمایی های ایشان و همچنین از جناب آقای دکتر محمود مدرس هاشمی به خاطر همکاری صمیمانه با اینجانب و راهنمایی های ایشان صمیمانه تشکر کنم.

همچنین از جناب آقای دکتر مهدی برنجکوب و دکتر سعید صدری به خاطر قبول زحمت داوری این پایان نامه کمال تشکر را دارم.

از تمامی دوستانم در دانشکده برق و کامپیوتر که کمال همکاری را با اینجانب داشتند صمیمانه قدر دانی می کنم و از خداوند متعال آرزوی پیروزی و شادکامی همه آنها را خو استارم.

به یاد پدرم

و تقدیم به

مادر عزیزم

فهرست مطالب

عنوان | صفحه

فصل اول : مقدمه

۱- ۱- مقدمه ۲

۱-۲- ویژگی‌های یک سیستم رمزنگار قالبی ۵

۱-۳- شبکه های نیستل ۶

۱-۴- شبکه های غیر فیستل ۶

۱-۵- ساختار پایان نامه ۹

فصل دوم : حملات تفاضلی وخطی

۲- ۱- مقدمه ۱۱

۲- ۲- یک الگوریتم رمز قالبی SPN پایه ۱۲

۲-۲-۱- عملیات جانشینی ۱۲

۲-۲-۲- جایگشت ۱۴

۲-۲-۳- ترکیب با کلید ۱۴

۲-۲-۴- رمزگشایی ۱۴

۲- ۳- تحلیل تفاضلی ۱۵

۲-۳-۱- مرور کلی حمله تفاضلی ۱۵

۲- ۳-۲- تحلیل اجزاء الگوریتم رمز ۱۶

۲- ۳-۳- روش بدست آوردن مشخصه‌های تفاضلی ۱۹

۲- ۳-۴- استخراج بیتهای کلید ۲۲

۲- ۳-۵- پیچیدگی حمله تفاضلی ۲۴

۲- ۴- تحلیل خطی ۲۵

۲-۴-۱- مرور کلی بر حمله خطی ۲۵

۲- ۴-۲- قاعده سری کردن ۲۷

۲- ۴-۳- تحلیل اجزاء الگوریتم رمز ۲۹

۲- ۴-۴- روش بدست آوردن تقریب خطی برای کل الگوریتم ۳۱

۲-۴-۵- استخراج بیتهای کلید ۳۴

۲- ۴-۶- پیچیدگی حمله خطی ۳۶

۲- ۵- خلاصه و نتیجه گیری ۳۷

فصل سوم : امنیت قابل اثبات در برابر حمله خطی

۳-۱- مقدمه ۳۸
۳-۲- مدلSPN ۳۸
۳-۳- حمله خطی ۴۰
۳-۴- مشخصه‌های خطی ۴۲
۳-۴-۱- جداول تقریب خطی ۴۲
۳-۴-۲- مشخصه‌های یک دوری ۴۳
۳-۴-۳- مشخصه‌های چند دوری ۴۳
۳-۴-۴- انتخاب بهترین مشخصه ۴۴
۳-۵- هالهای تقریبا خطی ۴۵
۳-۶- متوسط مربع بایاس صحیح ۴۵
۳-۶-۱- تعاریف اولیه ۴۶
۳-۶-۲- توزیع بایاس برای S-boxهای فعال ۴۶
۳-۶-۳- شمارش مشخصه‌ها ۴۷
۳-۶-۴- نتیجه اصلی ۴۸
۳-۷- نتایج محاسبات ۴۸
۳-۸- خلاصه و نتیجه‌گیری ۵۰

فصل چهارم: تحلیل خطی الگوریتم IES80

۴-۱- مقدمه ۵۱
۴-۲- ساختار کلی الگوریتم ۵۲
۴-۳- روش تحلیل خطی ۵۳
۴-۴- تقریب خطی از S-box ها ۵۶
۴-۵- تقریب خطی الگوریتم IES80 ..... ۵۶
۴-۶- حمله متن اصلی معلوم روی IES80 ..... ۶۲
۴-۷- تحلیل IES80 با استفاده از تقریب خطی چندگانه ۶۵
۴-۸- معرفی حمله خطی تعمیم یافته و اثر آن روی IES80 ..... ۶۹
۴-۸-۱- حمله خطی تعمیم یافته ۷۱
۴-۸-۲- احتمال موفقیت حمله خطی تعمیم یافته ۷۲
۴-۸-۳- لم اتصال سری در حمله خطی تعمیم یافته ۷۳
۴-۸-۴- یک روند جهت یافتن مجموع سه لایه هوموروف موثر ۷۴
۴-۸-۵- ارزیابی الگوریتم IES80 از دیدگاه حمله خطی تعمیم یافته ۷۶

۴-۹- جمع بندی و نتیجه گیری ۷۶

فصل پنجم: ارزیابی تحلیلی الگوریتم رمز طارق۲

۵-۱- مقدمه ۷۷
۵-۲- تحلیلهای تفاضلی و خطی ۷۸
۵-۲-۱- تحلیل تفاضلی ۷۸
۵-۲-۲- تحلیل خطی ۸۰
۵-۳- الگوریتمهای رمز قالبی با امنیت قابل اثبات در برابر حملات تفاضلی و خطی ۸۱
۵-۳-۱- مقدمات ۸۲
۵-۳-۲- برخی نگاشتهای خاص ۸۳
۵-۴- ارزیابی تحلیلی الگوریتم طارق۲ ..... ۸۸
۵-۴-۱- عملیات بکار رفته در الگوریتم طارق۲ ..... ۸۸
۵-۴-۲- فرآیند رمزگذاری ۸۹
۵-۴-۳- تبدیل ابتدایی ۹۰
۵-۴-۴- تبدیل انتهایی ۹۱
۵-۴-۵- تابع دور رمزنگار f ۹۱
۵-۴-۶- تابع S و معکوس آن S^{-1} ۹۲
۵-۴-۷- ارزیابی الگوریتم ۹۴
۵-۵- خلاصه و نتیجه گیری ۹۷

فصل ششم نتیجه‌گیری و پیشنهادات

۶-۱- نتیجه گیری ۹۸
۶-۲- پیشنهادات ۱۰۰
ضمیمه الف ۱۰۱
مراجع ۱۰۳

چکیده

الگوریتمهای رمز قالبی در بسیاری از سیستمها و محصولات امنیتی عنصری اساسی و مهم به شمار می آیند.این الگوریتمها در موارد متعددی مورد استفاده قرار می گیرند که از آن جمله می توان به مولدهای شبه تصادفی،رمزنگارهای پی در پی،کدهای اعتبار پیام و توابع درهم،اشاره کرد.به علاوه این الگوریتمها می توانند نقش اساسی در تکنیکهای اعتبار پیام،مکانیزمهای درستی داده ها،پروتکلهای تصدیق اصالت و روشهای امضاء دیجیتال ایفا کنند.لذا امروزه بحث ارزیابی چنین الگوریتمهایی،در کنار روشهای طراحی آنها به طور گسترده مورد توجه محققان زیادی قرار گرفته است.مهمترین بحث در ارزیابی الگوریتمهای رمز قالبی،ارزیابی امنیتی این الگوریتمها می باشد.در یک دیدگاه کلی می توان ارزیابی یک الگوریتم رمز قالبی را به دو قسمت ارزیابی آماری و ارزیابی تحلیلی تقسیم کرد که در این تقسیم بندی،ارزیابی تحلیلی یک الگوریتم از جایگاه ویژه ای بر خوردار است.منظور از ارزیابی تحلیلی،بررسی امنیت الگوریتم در برابر حملات تحلیلی می باشد.از جمله مهمترین حملات تحلیلی شناخته شده به الگوریتمهای رمز قالبی می توان به حمله تفاضلی و حمله خطی اشاره کرد.هدف این پایان نامه ارزیابی تحلیلی دو الگوریتم رمز قالبی IES80 و طارق ۲ – کاندیداهای مسابقه ارزیابی انجمن رمز ایران- می باشد که تاکید بر روی حمله خطی است.در این پایان نامه ضمن معرفی حملات فوق الذکر امنیت قابل اثبات در برابر حمله خطی مورد بررسی قرار می گیرد.در ادامه حمله خطی به الگوریتم رمز IES80 اعمال می شود واثر حمله خطی تعمیم یافته و حمله خطی با استفاده از تقریبهای چندگانه روی این الگوریتم مورد بررسی قرار می گیرد و در ادامه امنیت الگوریتم طارق ۲ در برابر حملات خطی و تفاضلی مورد ارزیابی تحلیلی قرار می گیرد.

فصل اول
مقدمه

۱-۱-مقدمه

به منظور ایجاد سرویس محرمانگی در سیستم‌های اطلاعاتی از الگوریتمهای رمزنگاری استفاده می‌شود. یک الگوریتم رمزنگاری شامل یک سری تبدیلات معکوس پذیر، وابسته به پارامترهای متغیری به نام کلید است که برای تبدیل متن اصلی به متن رمز شده یا تبدیل متن رمز شده به متن اصلی به کار برده می‌شود. الگوریتمهای رمزنگاری از نظر کلید به دو دسته عمده زیر تقسیم می‌شوند :

الف- الگوریتمهای با کلید پنهان

ب- الگوریتمهای کلید عمومی

در یک الگوریتم با کلید پنهان عملیات رمزگذاری[1] و رمزگشایی[2] وابسته به یک کلید محرمانه که مورد توافق بین فرستنده و گیرنده قرار گرفته است صورت می پذیرد و اصالت[3] و محرمانگی[4] پیام به امنیت کلید بستگی دارد. در یک سیستم کلید عمومی، برخلاف دسته قبل، نیازی به توافق فرستنده و گیرنده بر روی یک کلید امن نیست، بلکه هر یک از فرستنده و گیرنده یک کلید عمومی(علنی) برای رمز کردن و یک کلید خصوصی(مخفی) برای گشودن رمز دارند.

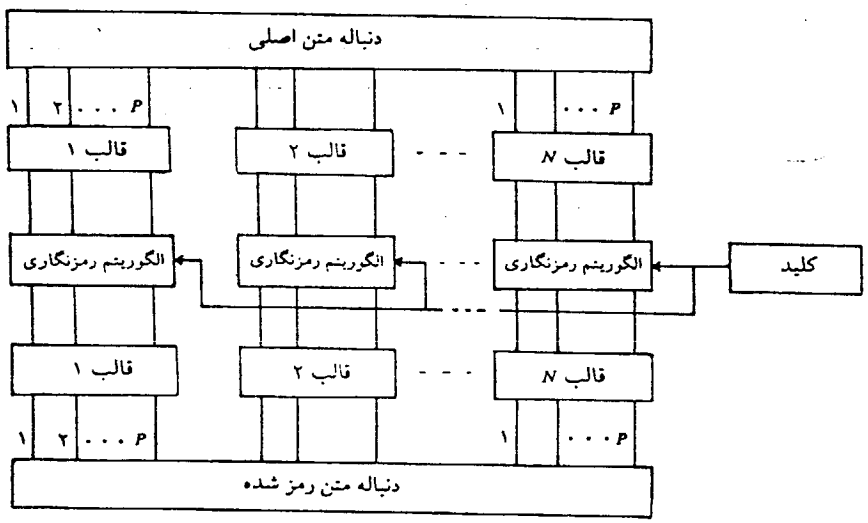
1.Encryption
2.Decryption
3.Authentication
4.Privacy

الگوریتمهای رمزنگاری با کلید پنهان، به دو گروه عمده زیر تقسیم می‌شوند :

الف- الگوریتمهای رمزنگاری قالبی[1]

ب- الگوریتمهای رمزنگاری پی‌درپی[2]

در یک الگوریتم رمزنگاری قالبی در طرف فرستنده، دنباله متن اصلی به تعدادی قالب با اندازه یکسان تقسیم می‌شود و این قالبها بطور جداگانه تحت یک الگوریتم رمزنگاری مشخص وابسته به کلید رمز شده و قالبهای متن رمز شده را می‌سازند. در طرف گیرنده، به طریق معکوس، قالبهای متن رمز شده جدا می‌شوند و الگوریتم رمزگشایی تحت همان کلید (مورد توافق)، قالب‌های متن اصلی را تولید می‌کند. بلوک دیاگرام کلی یک سیستم رمزنگاری قالبی با طول قالب P در شکل ۱-۱ دیده می‌شود.



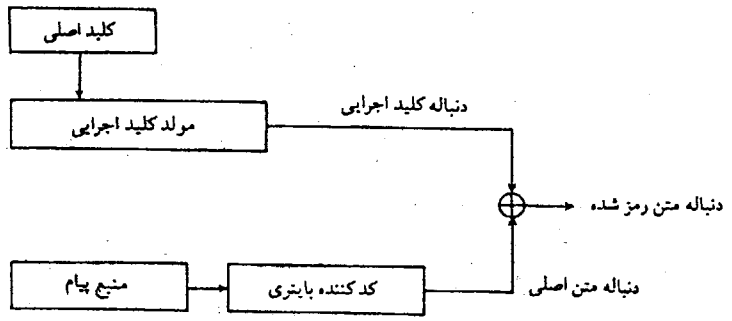
شکل ۱-۱ : بلوک دیاگرام یک سیستم رمزنگار قالبی

در یک سیستم رمزنگار پی‌درپی، دنباله متن اصلی با یک دنباله موسوم به کلید اجرایی بیت به بیت ترکیب شده و دنباله متن رمز شده را بوجود می‌آورد. دنباله کلید اجرایی نیز با یک الگوریتم مشخص از روی کلید اصلی تولید می‌شود. عمل ترکیب دنباله متن اصلی و دنباله کلید اجرایی، عمل جمع در هنگ ۲ یا XOR است و با نماد ⊕ نشان داده می‌شود. در گیرنده کافی است که مجدداً دنباله کلید اجرایی با دنباله متن رمز شده XOR شود تا متن اصلی را به وجود آورد. بلوک دیاگرام یک سیستم رمزنگاری پی‌درپی در شکل ۱-۲ دیده می‌شود.

1.Block ciphers

2.Stream ciphers

سیستم‌های رمزنگاری و بطور کلی ارتباطات محرمانه همواره از طرف فرد یا افرادی مورد تهدید قرار می‌گیرند. در مبحث امنیت به این افراد نام دشمن اطلاق می‌شود. دشمن کسی است که سعی می‌کند در ارتباط بین فرستنده و گیرنده اختلال ایجاد کند یا از این ارتباط جهت مقاصد خود اطلاعات کسب کند.



شکل ۱-۲ : بلوک دیاگرام یک سیستم رمزنگاری پی‌درپی

بعنوان مثال در یک سیستم مخابراتی که برای جلوگیری از آشکار شدن محتوای پیامهای حساس آنها را بصورت رمز شده ارسال می‌کنند دشمن سعی می‌کند با بدست آوردن کلید رمزنگاری از محتوای پیامها اطلاع پیدا کند و یا پیامهای جعلی را رمز کرده و ارسال کند تا گیرنده را با مشکل مواجه کند.

حملات علیه سیستم مخابراتی به دو نوع غیرفعال و فعال تقسیم می‌شوند. در حمله غیرفعال دشمن بصورت یک گیرنده غیر مجاز عمل می‌کند و در کانال غیر امن بین فرستنده و گیرنده استراق‌سمع می‌نماید. هدف در این نوع تهدید آن است که داده‌های ارسالی ضبط شوند و بعداً محتوای آنها کشف شود. در حمله فعال دشمن علاوه بر گیرنده غیرمجاز، فرستنده غیرمجاز نیز می‌باشد. یعنی توسط دستگاهی داده‌های ارسالی یا سیگنالهای کنترلی را عوض می‌کند و یا داده‌ها و سیگنالهای کنترلی جعلی تولید می‌کند. هدف دشمن در این حمله، دادن اطلاعات اشتباه به گیرنده و یا جلوگیری از ارسال اطلاعات به آن است.

تحلیلگر رمز[1] ممکن است خودی یا دشمن باشد که هدف خودی از تحلیل الگوریتم،بررسی نقاط ضعف الگوریتم به منظور اصلاح آن می باشد در صورتی که هدف دشمن دستیابی به کلید است. اعمالی که دشمن برای دستیابی به کلید یا متن اصلی انجام می‌دهد نام حمله بخود می‌گیرد. البته در بسیاری موارد

1.cryptanalyser

رمزشکنی و حمله بصورت مترادف بکار می‌روند. حملات به سیستم‌های رمزنگاری به سه نوع کلی تقسیم می‌شود :

۱- حمله نوع اول (یا حملهٔ فقط بر اساس متن رمز شده) : در این حمله دشمن الگوریتم رمزگذاری و رمزگشایی را می‌داند (ولی کلید را نمی‌شناسد) و متن رمز شده را نیز در اختیار دارد.

۲- حمله نوع دوم (یا حمله بر اساس متن اصلی معلوم) : دشمن در این حمله علاوه بر شناخت الگوریتم قسمتی از متن اصلی و متن رمز شده متناظر با آنرا در اختیار دارد.

۳- حمله نوع سوم (یا حمله بر اساس متن اصلی انتخاب شده) : دشمن در این حمله علاوه بر شناخت الگورینم، برای هر متن اصلی دلخواه خود، متن رمز شده متناظر با آنرا در اختیار خواهد داشت. بعبارت دیگر فرض بر این است که دشمن کلیه اطلاعات لازم برای شکستن سیستم را در اختیار دارد و فقط کلید را نمی داند.

میزان مقاومتی را که سیستم رمزنگاری در مقابل حملات دشمن از خود نشان می‌دهد، امنیت سیستم گویند.سیستمی را که از لحاظ تئوری و عملی، قابل شکست نباشد، سیستم با امنیت کامل نامند و سیستمی را که از لحاظ تئوری قابل شکستن باشد، ولی از لحاظ عملی نیاز به زمان یا هزینه شکستن بسیار بالایی داشته باشد، سیستم با امنیت عملی گویند.

۱-۲- ویژگی‌های یک سیستم رمزنگار قالبی

در یک سیستم رمزنگار قالبی (در حالت باینری) با طول قالب P، بعد فضای قالب‌های متن اصلی و متن رمز شده 2^P است. در واقع، قالب ورودی در این سیستم یک بردار باینری P بیتی بوده که تحت یک الگوریتم مشخص وابسته به کلید، به برداری P بیتی در خروجی تبدیل می‌شود.

سه ویژگی عمده یک سیستم رمزنگار قالبی خوب عبارتند از :

۱- بزرگ بودن اندازه قالب، به منظور جلوگیری از تشکیل یک جدول تناظر یک به یک بین قالب‌های ورودی، خروجی توسط دشمن.

۲- بزرگ بودن فضای کلید، به منظور جلوگیری از امکان جستجوی کامل فضای کلید توسط دشمن.

۳- پیچیدن بودن رابطه موجود بین قالب متن رمز شده و قالب متن اصلی و کلید، برای جلوگیری از امکان بدست آوردن قالب متن اصلی یا کلید از روی قالب متن رمز شده بصورت تحلیلی یا آماری از طرف دشمن.

برای پیچیده کردن رابطه بین قالب‌های ورودی و خروجی (ویژگی سوم)، از معیارهای شانون برای یک سیستم رمزنگاری خوب استفاده می‌شود. این معیارها عبارتند از[۱] :

۱- انتشار[1]

۲- درهم پیچیدگی[2]

منظور از انتشار آن است که هر بیت از کلید یا متن اصلی بر روی همه بیت‌های متن رمز شده تأثیر داشته باشد. یا بطور معادل هر بیت از متن رمز شده به تمام بیت‌های متن اصلی و کلید وابسته باشد.

درهم پیچیدگی به این معناست که رابطه آماری و تحلیلی موجود بین متن رمز شده و متن اصلی بقدر کافی پیچیده باشد تا دشمن را از حمله تحلیلی به سیستم مأیوس کند.

در یک تقسیم بندی کلی می توان ساختار سیستمهای رمزنگاری قالبی را به دو دسته عمده تقسیم کرد : شبکه های فیستل[3] و شبکه های غیر فیستل[4].

شبکه های فیستل نخستین بار توسط فیستل در طراحی رمزنگار لوسیفر[5][۲] ابداع گردید و در حال حاضر در طراحی بسیاری از رمزنگارهای قالبی بکار می رود.

در بخشهای بعدی به معرفی هر یک از ساختارهای فوق پرداخته می شود.

۱-۳- شبکه های فیستل

اغلب الگوریتمهای رمزنگاری قالبی از نوع شبکه های فیستل می باشند. شکل ۱-۳ یک شبکه فیستل را به طور عمومی نمایش می دهد.

در این نوع رمزنگارها، قالب ورودی متن اصلی به طول n بیت ابتدا به دو نیمه راست و چپ با نامهای R_0 و L_0 هر کدام به طول $n/2$ بیت تقسیم می شود. البته n باید زوج باشد. سپس عملیات زیر به صورت تکراری طی r دور متوالی روی نیمه های راست و چپ داده ها انجام می شود. در هر دور نیمه (زیر قالب) سمت راست داده ها به همراه زیر کلید همان دور در ورودی تابع رمزنگار f قرار می گیرند. خروجی تابع f به طول $n/2$ بیت با نیمه چپ داده ها XOR می شود و سپس جای دو زیر قالب راست و چپ عوض می گردد. تعویض جای زیر قالبهای راست و چپ در انتهای هر دور به جز دور آخر انجام می شود. در یک شبکه فیستل به صورت فوق خروجی i امین دور با استفاده از روابط زیر به دست می آید :

1.Diffusion
2.Confusion
3.Feistel networks
4.Non feistel networks
5.Locifer