دانشگاه زنجان

دانشکده مهندسی

گروه برق

پایان‌نامه کارشناسی

گرایش: الکترونیک

عنوان:

طراحی و پیاده سازی روش شمیر در به اشتراک گذاری سری تصاویر

استاد راهنما:

دکتر مصطفی چرمی

نگارش:

مهدی محمدی

شهریور ۱۳۹۴

به پاس تعبیر زیبا و انسانی‌شان از کلمه ایثار و از خودگذشتگی

به پاس عاطفه سرشار و گرمای امیدبخش وجودشان

به پاس قلب‌های بزرگشان که فریادرس است و سرگردانی و ترس در پناهشان به شجاعت می‌گراید

و به پاس محبت‌های بی‌دریغشان که هرگز فروکش نمی‌کند

این مجموعه را تقدیم می‌کنم به:

پدر و مادر بزرگوار و فداکارم

فهرست

چکیده

در این پایان نامه سعی شده است که رمزها وتصاویر را با استفاده از روش شمیر که یکی از الگوریتم‌های تسهیم محرمانه در رمز نگاری می‌باشد را تشریح و پیاده سازی کنیم. در روش شمیر رمز یا تصویر به n بخش تقسیم می‌شود و هر بخش در اختیار یک کاربر قرار می‌گیرد و زمانی که تعداد مشخصی از کاربران، اطلاعات خود را به اشتراک می‌گذارند، رمز یا تصویر محرمانه به طور مجدد تولید می‌شود.

۱- رمزنگاری[1]

هرکدام از ما وقتی به دنیای ماموران مخفی و جاسوسان فکر می‌کنیم چیزهای زیادی به ذهنمان می‌رسد: سفرهای خارجی، ماموریت‌های خطرناک، اسلحه‌های عجیب و ماشین‌های سریع، کمتر کسی درکنار این چیزها به ریاضیات فکر می‌کند، اما باید بدانیم ریاضیات در فهمیدن پیام‌های سری و شکستن رمزها نقش اساسی بازی می‌کند و در طول تاریخ ریاضیدان‌ها نتیجه نبردهای فراوانی را با شکستن رمزها تغییر داده‌اند.

نمیدانم فیلم "ذهن زیبا"را دیده‌اید یا نه؟ این فیلم زندگی واقعی یک ریاضیدان به نام جان نش[2] را به تصویر می‌کشد. این ریاضیدان ابتدا برای شکستن کدهای سری به استخدام سازمان سیا در می‌آید. ولی پس از مدتی به بیماری شیزوفرنی[3] دچار می‌شود. ولی پس از مدت‌ها بیماری دوباره به صحنه علم برمی‌گردد و جایزه نوبل اقتصاد را دریافت می‌کند.

۱-۲ رمز نگاری چیست؟

در رمزنگاری هدف ساختن طرح‌ها یا پروتکل‌هایی است که بتوان با کمک آنها حتی در حضور دشمن نیز کارهای خاصی را انجام داد. یک هدف اساسی در رمزنگاری این است که به افراد این امکان را بدهند که روی یک کانال ناامن با حفظ حریم خصوصی و اصالت داده‌هایشان به صورت کاملاً امن با هم ارتباط برقرار کنند. به عنوان مثال فرض کنید که آلیس بخواهد از طریق اینترنت پیامی را برای باب ارسال کند. در حالت ایده‌آل می‌خواهیم که هیچ حمله کننده‌ای نتواند هیچ اطلاعاتی درباره پیام آلیس به‌دست آورد و همچنین نتواند هیچ تغییری در پیام آلیس بدون اینکه باب متوجه شود، ایجاد کند. با وجود اینکه حفظ حریم خصوصی و اصالت داده‌ها یک هدف اصلی برای پروتکل‌های رمزنگاری است علاوه بر این امروزه علم رمزنگاری در

---

[1] Cryptography
[2] John Nash
[3] Schizophrenia

موضوعات بسیار زیاد دیگری مانند رأی‌گیری الکترونیکی، پول‌های الکترونیکی و مزایده‌های امن پیشرفت‌های قابل توجه‌ای کرده است و مسائل زیادی در این زمینه‌ها نیز مطرح شده است. در ادامه توضیح می‌دهیم که رمزنگاری چیست و چگونه می‌توانیم یک توجیه علمی برای امنیت طرح‌های رمزنگاری داشته باشیم.

۱-۳ شروع و توسعه رمزنگاری

اولین بار سزار امپراتور رم باستان برای آنکه بتواند بدون اطلاع دشمن با ا ارتشش در سراسر دنیا در ارتباط باشد نوعی رمز را بکار گرفت. این رمز به این شکل بود که برای فرستادن یک پیام جای هر حرف را با سومین حرف بعد از آن در الفبا عوض می کردند، مثلا به جای 'A' حرف 'D' و به جای 'X' حرف 'A' را می گذاشتند . بنابراین برای از کد خارج کردن پیام ها کافی بود دریافت کننده جای هر حرف را با سومین حرف بعد از آن در الفبا عوض کند. مثلا سعی کنید این پیغام سزاری را از رمز خارج کنید :

Hqhpb dssurdfklaj

Wkluwb ghdg

Uhwuhdw wr iruhvw

۱-٤ مدل کردن امنیت

چگونه می‌توانیم تضمین کنیم که یک طرح رمزنگاری امن است؟ برای اینکه بتوان امنیت را فرمول‌بندی کرد ابتدا باید توانمندی‌های دشمن را مشخص کرد (اینکه دشمن چه کارهایی را می‌تواند انجام دهد). همچنین باید شرایطی را که در آن یک حمله می‌تواند به طور موفقیت‌آمیزی انجام شود، مشخص کرد. به عنوان نمونه در مثالی که ابتدا مطرح کردیم، دشمن می تواند متن رمز شده آلیس را بخواند و آن را تغییر دهد. در این مثال حمله زمانی به طور موفقیت‌آمیزی انجام شده که حمله کننده بتواند اطلاعاتی را در مورد پیام آلیس به‌دست آورد و یا بتواند تغییری در پیام ایجاد کند بدون اینکه باب متوجه شود این تغییر از سوی آلیس نبوده است و یا دشمن پیامی برای باب بفرستد که باب تصور کند این پیام از سمت آلیس است.

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

بنابراین می توان گفت یک طرح رمزنگاری امن است اگر بتوانیم به صورت ریاضی ثابت کنیم هیچ حمله‌ای نمی‌تواند به‌صورت موفقیت‌آمیزی انجام شود، مگر با یک احتمال بسیار ناچیز.

۱-۵ رمزنگاری متقارن

در ساده‌ترین حالت ممکن، آلیس و باب می‌توانند، بدون اطلاع دشمن، کلید K را با هم به اشتراک بگذارند و از این کلید برای رمز کردن و از رمز خارج کردن متن مکاتباتشان استفاده کنند. کلید به اشتراک گذاشته شده معمولاً یک دنباله تصادفی k بیتی است که با یک توزیع احتمال یکنواخت انتخاب می‌شود. همانطور که در شکل ۱ نشان داده شده است، آلیس می‌تواند الگوریتمی را برای رمزکردن متن اصلی M با کمک کلید K به کار ببرد و متن رمز شده C را به‌دست آورد. متن رمزشده C برای باب فرستاده می‌شود. باب با کمک الگوریتمی متناظر با الگوریتم آلیس و با کمک کلید K می تواند متن C را از رمز خارج کند و متن اصلی M را به‌دست آورد. این طرح، طرح کلی رمزنگاری متقارن است، که در آن دو طرف مکاتبه کننده کلیدی را با هم به اشتراک می‌گذارند. در حالت کلی یک طرح رمزنگاری به صورت تصادفی است، بدین معنی که آلیس باید یک عدد تصادفی انتخاب کند و پیام C را از روی ورودی M، عدد تصادفی انتخاب شده و کلید K به‌دست آورد. در هر مرحله که الگوریتم رمزکردن انجام می‌شود یک عدد تصادفی جدید مورد نیاز است. تجدید این عدد تصادفی باعث می شود که اگر الگوریتم رمزکردن دوبار روی یک پیام M با یک کلید K اجرا شود متن‌های رمزشده متفاوتی داشته باشیم.