دانشکده‌ی علوم

پایان‌نامه‌ي کارشناسی ارشد در رشته‌ی ریاضی محض گرایش جبر و توپولوژی

بررسی سیستم‌های رمزنگاری کلید عمومی برپایه بعضی ساختارهای جبری

توسط

طاهره کاکایی

استادان راهنما

دکتر حبیب شریف

دکتر علیرضا کشاورز حداد

شهریور ماه ۱۳۹۰


بسم الله الرحمن الرحيم

به نام خدا

اظهارنامه

اینجانب، طاهره کاکایی (۸۸۰۶۰۰)، دانشجوی رشته‌ي ریاضی محض گرایش جبر و توپولوژی دانشکده‌ي علوم اظهار می کنم که این پایان نامه حاصل پژوهش خودم بوده و در جاهایی که از منابع دیگران استفاده کرده‌ام، نشانی دقیق و مشخصات کامل آن را نوشته‌ام. همچنین اظهار می‌کنم که تحقیق و موضوع پایان نامه‌ام تکراری نیست و تعهد می‌نمایم که بدون مجوز دانشگاه دستاوردهای آن را منتشر ننموده و یا در اختیار غیر قرار ندهم. کلیه‌ي حقوق این اثر مطابق با آیین نامه‌ي مالکیت فکری و معنوی متعلق به دانشگاه شیراز است.

نام و نام خانوادگی: طاهره کاکایی

تاریخ و امضا:

به نام خدا

بررسی سیستم‌های رمزنگاری کلید عمومی برپایه بعضی ساختارهای جبری

به کوشش:

طاهره کاکایی

پایان نامه

ارائه شده به تحصیلات تکمیلی دانشگاه شیراز به‌عنوان بخشی از فعالیت‌های تحصیلی لازم برای اخذ درجه‌ي کارشناسی ارشد

در رشته‌ی:

ریاضی محض

از دانشگاه شیراز

شیراز

جمهوری اسلامی ایران

ارزیابی شده توسط کمیته‌ی پایان نامه با درجه‌ی: عالي

دکتر حبیب شریف، استاد بخش ریاضی (رئیس کمیته) .....

دکتر علیرضا کشاورزحداد، استادیار بخش مهندسی برق (رئیس کمیته) .....

دکتر شهره نمازی، استادیار بخش ریاضی .....

دکتر عزیزاله جمشیدی، استادیار بخش مهندسی برق .....

شهریور ماه ۱۳۹۰

باسمه تعالی

خدای را سپاسگزارم که به من توفیق داد قدم در مرحله جدیدی از علم و معرفت بگذارم. هر چند که «العلم نور یقذفه فی قلب من یشاء» (علم نوری است که خدا در دل هر کس که بخواهد می تاباند)، اما تلاشم آن بوده است که با کوشش و تلاش ناچیز خود در علم را به اندازه وسع خویش بکوبم و گشایش این در جز به خواست خدا میسر نیست.

ای خدای پاک و بی انباز و یار — دست گیر و جرم ما را واگذار
هم دعا از تو اجابت هم ز تو — ایمنی از تو مهابت هم ز تو
یاد داه ما را سخن‌های رقیق — که تو را رحم آورد آن ای رفیق
گر غلط گفتیم اصلاحش تو کن — مصلحی تو ای تو سلطان سخن
این همه بیناگری‌ها کار توست — این همه اکسیرها ز اسرار توست

مولانا

تقدیم به:

مادرم که در همه فراز و نشیب های زندگی و در همه لحظات سامان یافتن این پایان نامه رفیقی شفیق و یاری همراه بود، و

پدرم که در همه مراحل زندگی و پیمودن طریق علم و عمل همواره راهنمایی بصیر و تکیه گاهی استوار بوده است.

سپاسگزاری

در اینجا بر خود لازم می دانم که از استاد بزرگوار جناب آقای دکتر حبیب شریف تشکر کنم، که اگر نبود تشویق و راهنمایی‌ها و صبر و حوصله ایشان، این پایان نامه هیچگاه به سرانجام نمی رسید. از دیگر استاد راهنما، جناب آقای دکتر علیرضا کشاورز حداد نیز بینهایت سپاسگزارم که وقت گذاری ایشان و نکات مهمی که یادآور می شدند در جهت پربار کردن پایان نامه کمک شایانی کرد.

چکیده

بررسی سیستم‌های رمزنگاری کلید عمومی

بر پایه بعضی ساختارهای جبری

به کوشش

طاهره کاکایی

در این پایان‌نامه،هدف بررسی سیستم‌های مختلف رمزنگاری کلید عمومی برپایه ساختارهای مختلف جبری و نحوه ساختن توابع یک‌طرفه برای رمزنگاری کلید عمومی است.در فصل اول مقدمات رمزنگاری بیان شده و سیستم‌های رمزنگاری معروفی چون RSA ،الجمال و پروتکل تبادل کلید دیفی- هلمن معرفی می‌شوند.فصل دوم به مطالعه بعضی مفاهیم رمزنگاری و نظریه گروه‌ها که در پایان‌نامه مورد استفاده قرار می‌گیرد اختصاص دارد.در فصل سوم با الهام از الگوریتم‌های دیفی- هلمن و الجمال الگوریتم‌های مختلفی برپایه ساختارهای مختلف جبری معرفی شده و کلی‌ترین تعمیم این الگوریتم‌ها به کلی‌ترین حالت‌های ممکن تحت عنوان حالت کلی دیفی- هلمن و حالت کلی الجمال معرفی می‌شوند.فصل چهارم یک حالت خاص از این تعمیم،یعنی برای عمل یک نیم‌گروه بر یک مجموعه بررسی شده و پیاده‌سازی آن در ساختارهای مختلفی چون ساختار ماتریس‌ها و طوقه‌ها بررسی می‌شوند.

فهرست مطالب

لیست الگوریتم‌ها

فصل اول

مقدمه

با گسترش علم و فناوری و تغییر شکل زندگی بشر نیازهای انسان و خطراتی که با آن روبرو می‌شود شکل تازه‌ای به خود می‌گیرد. گسترش حجم اطلاعات و افزایش ارتباطات، تهدیدات علیه اطلاعات را افزایش داده و منجر به پدید آمدن مبحث تازه‌ای در علم و تکنولوژی به نام *امنیت داده‌ها* شده است.

تهدیدهای امنیتی [۱] که برای یک سیستم ممکن است رخ دهد به سه دسته تهدیدهای طبیعی، تهدیدهای غیر عمد و تهدیدهای عمد تقسیم می‌شوند. تهدیدهای عمدی (که بیشترین خسارت و دشوارترین راه مقابله را دارند) عبارت از *هرگونه اقدام برنامه‌ریزی شده جهت افشا، نابودی یا تغییر در داده‌های حیاتی شبکه یا ایجاد اختلال در خدمات معمول سرویس دهنده‌ها* می‌باشد. هدف اصلی رمزنگاری مقابله با این نوع تهدیدها و به حداقل رساندن احتمال وقوع و یا خسارت ناشی از این نوع تهدیدهاست. هرگاه تهدیدی از قوه به فعل درآید اصطلاحا یک *حمله*[۲] رخ داده‌است؛ خواه آن حمله موجب خسارت به منابع شود و خواه یک تلاش نافرجام باشد.

عمده‌ترین خدماتی که برای برقراری یک ارتباط امن در شبکه‌های کامپیوتری بکار می‌روند عبارتند از:

- **محرمانه ماندن اطلاعات**[۳] به مجموعه مکانیزم‌هایی که تضمین می‌کند داده‌ها و اطلاعات مهم کاربران از دسترس افراد بیگانه و غیر مجاز دور نگاه داشته شود، *سرویس محرمانگی* اطلاق می‌شود. این سرویس‌ها عموما با روشهای رمزنگاری تحقق می‌یابند. روشهای مختلف رمزنگاری اطلاعات، زیربنای مابقی سرویسهای امنیتی است.
- **احراز هویت**[۴] مجموعه مکانیزم‌هایی که این امکان را فراهم می‌کند که بتوان مبدأ واقعی یک پیام، سند یا تراکنش [۵] را بدون ذره‌ای تردید یا ابهام مشخص کرد، *سرویس احراز هویت* نامیده می‌شود.

---

[۱] Security Threat

[۲] Attack

[۳] Confidentiality

[۴] Authentication

[۵] Transaction

- **تضمین صحت اطلاعات**[۶] مجموعه مکانیزم‌هایی که از هرگونه تحریف، دستکاری، تکرار، حذف یا آلوده سازی داده‌ها پیشگیری می‌کند یا حداقل باعث کشف چنین اقداماتی می‌شود، *سرویس تضمین صحت اطلاعات* نامیده می‌شود.

- **غیر قابل انکار ساختن پیام‌ها** [۷] مجموعه مکانیزم‌هایی که به پیامهاها و تراکنشها پشتوانه حقوقی می‌بخشد و اجازه نمی‌دهد که فرستنده به هر طریق ارسال پیام خود را انکار کند و یا گیرنده منکر دریافت آن شود به *سرویس غیرقابل انکار ساختن* پیامها شهرت دارد.

- **کنترل دسترسی**[۸] مکانیزمهایی که دسترسی به کوچکترین منابع اشتراکی شبکه را تحت کنترل درآورده و هر منبع را بر اساس سطح مجوز کاربران و پروسه‌ها در اختیار آنها قرار می‌دهد، *کنترل دسترسی* خوانده می‌شود.

تمام خدمات امنیتی با این فرض طراحی و پیاده سازی می شوند که تهدیدهای چهارگانه زیر همیشه وجود دارند و هر لحظه ممکن است اتفاق بیفتند:

- **استراق سمع**[۹] هرگاه یک شخص غیر مجاز به هر نحو بتواند نسخه‌ای از داده‌های در حال جریان بین مبدأ و مقصد را به نفع خود شنود کند حمله *استراق سمع* به وقوع پیوسته است.

- **دستکاری**[۱۰] هرگاه داده‌های در حال جریان بین مبدأ و مقصد توسط شخص غیر مجاز به هر نحو دستکاری یا تحریف شود، حمله *دستکاری داده‌ها* رخ داده است.

- **جعل**[۱۱] هرگاه یک شخص غیر مجاز اقدام به تولید پیامهای ساختگی کرده و ارسال

---

[۶] Integrity

[۷] Non-Repudiation

[۸] Access Control

[۹] Interception

[۱۰] Modification

[۱۱] Fabrication

آنها را به شخص مجاز دیگری نسبت بدهد، حمله *جعل و ارسال داده‌های ساختگی* به وقوع پیوسته است.

- **وقفه**[۱۲] هرگاه کسی بتواند سیستم یا سرویسی را در شبکه از کار بیندازد حمله *وقفه* رخ داده است.

۱ - ۱ کلیات رمزنگاری

رمزنگاری یا Cryptography از دو کلمه یونانی مشتق شده که اولی به معنای مخفی و پوشیده و دومی به معنای نگارش و ترسیم است. رمزنگاری عبارتست از یک *نظام* یا الگوی *ریاضی / منطقی* که بر اساس آن اطلاعات و مفاهیم آشکار و قابل فهم برای همگان، طبق روالی برگشت پذیر به اطلاعاتی نامفهوم و گنگ تبدیل می‌شود.

تعریف ۱ - ۱ - ۱. یک طرح رمزی یا دستگاه رمزنگاری یک پنج‌تایی $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ با خواص زیر است:

۱. $\mathcal{P}$ یک مجموعه است.این مجموعه فضای متن ساده نامیده می‌شود.اعضای آن متن ساده نامیده می‌شوند.

۲. $\mathcal{C}$ یک مجموعه است.این مجموعه را فضای متن رمز می‌نامند.اعضای آن متن رمز نامیده می‌شوند.

۳. $\mathcal{K}$ یک مجموعه بوده و فضای کلید نام دارد.اعضای آن کلید نامیده می‌شوند.

۴. $\mathcal{E} = \{E_k : k \in \mathcal{K}\}$ یک خانواده از توابع $E_{\mathcal{K}} : \mathcal{P} \longrightarrow \mathcal{C}$ است.اعضای آن توابع رمزگذاری نام دارند.

۵. $\mathcal{D} = \{D_k : k \in \mathcal{K}\}$ یک خانواده از توابع $D_k : \mathcal{C} \longrightarrow \mathcal{P}$ است.اعضای آن توابع رمزگشایی نام دارند.

[۱۲] Interruption

۶. برای هر $e \in \mathcal{K}$ عضوی چون $d \in \mathcal{K}$ وجود دارد که برای هر $p \in \mathcal{P}$ رابطه $D_d(E_e(p)) = p$ برقرار است.

۱-۱-۱ اصول ششگانه کرکهف

پروفسور *آگوست کرکهف* [۱۳] استاد زبان‌شناسی دانشسرای عالی مطالعات بازرگانی پاریس (۱۹۰۳ – ۱۸۳۵) در سال ۱۸۸۳ در دو مقاله با عنوان *رمزنگاری نظامی* در مجله علوم نظامی فرانسه، شش اصل اساسی را در رمزنگاری عنوان کرد که اصل دوم آن به عنوان یکی از قوانین اساسی در رمزنگاری مدرن مورد تأیید دانشمندان و زیربنای هر فعالیت و پژوهش قرار گرفت.در زیر اصول ششگانه کرکهف را معرفی می‌کنیم:

۱. سیستم رمزنگاری نه فقط به لحاظ نظری بلکه در عمل غیر قابل شکست باشد.

۲. سیستم رمزنگار باید هیچگونه نکته پنهان و محرمانه ای نداشته باشد، بلکه تنها چیزی که باید سری نگاه داشته شود کلید رمز است(اصل اساسی کرکهف). طراح سیستم رمزنگار نباید جزییات سیستم خود را حتی از دشمنان مخفی نگاه دارد.

۳. کلید رمز باید بگونه ای قابل انتخاب باشد که اولاً بتوان براحتی آنرا عوض کرد و ثانیاً بتوان آن را بخاطر سپرد و نیازی به یادداشت کردن آن نباشد.

۴. متون رمزنگاری شده باید از طریق خطوط تلگراف قابل مخابره باشند.

۵. دستگاه رمزنگاری یا اسناد رمز شده باید توسط یک نفر قابل راه اندازی و کاربری باشد. چنین سیستمی نباید به آموزش های مفصل و رعایت فهرست بزرگی از قواعد و دستورالعمل ها نیاز داشته باشد.

۶. سیستم رمزنگاری باید به سهولت قابل راه اندازی و کاربری باشد.چنین سیستمی نباید به آموزشهای مفصل و رعایت فهرست بزرگی از قواعد و دستورالعمل‌ها نیاز داشته باشد.

[۱۳] Kerchoffs

لازم به ذکر است که *رمزنگاری*(Cryptography یا Encryption) با *کدگذاری* (Encoding) تفاوت دارد: وقتی دو نفر با هم قرار می‌گذارند به جای کلمه «پول»» از کلمه «هویج» و به جای «پرداخت» از کلمه «گاز زدن» و نظایر آن استفاده کنند، یک نوع «کد گذاری» انجام داده‌اند.در فرآیند کدگذاری،کلمات،نمادها و افعال موجود در ادبیات زبانی، با مقادیر مورد توافق تعویض می‌شوند.

در رمزنگاری دنباله ای از بیتها یا بایتها بدون توجه به محتویات زبان‌شناختی آنها، طبق روالی معلوم و غیرسلیقه‌ای درهم و رمز می‌شود. در روال رمزنگاری دنباله داده‌ها، کلید رمز به عنوان پارامتر در متن داده‌ها تزریق می‌شود و چگونگی درهم شدن داده‌ها به مقدار کلید وابسته است. فرض بر آنست که داده‌هایی که بین گیرنده و فرستنده مخابره می‌شود به راحتی توسط بیگانگان قابل شنود و حتی قابل دستکاری است.

در حقیقت رمزنگاری مسئله سری نگه داشتن یک پیام با طول بزرگ و دلخواه را به مسئله سری نگه داشتن یک کلید کوتاه کاهش می‌دهد.

۱ - ۲ دسته بندی سیستم‌های رمزنگاری

معمولا در سیستم‌های رمزنگاری فرض بر این است که «آلیس» و «باب» میخواهند از طریق یک کانال ناامن با هم یک ارتباط رمزنگاری شده داشته باشند و «ایو» مکالمات آنها را استراق سمع می‌کند.آلیس، باب و ایو لزوما انسان نیستند.آنها می‌توانند رایانه باشند.

اگر آلیس بخواهد یک پیغام رمز شده را به باب بفرستد از یک کلید رمزگذاری e استفاده کرده و سپس باب کلید رمزگشای متناظر با آن را برای بدست آوردن متن ساده بکار می‌برد.

سیستم‌های رمزنگاری به دو رده کلی *رمزنگاری متقارن* [۱۴] و *رمزنگاری کلید عمومی* [۱۵] تقسیم بندی می‌شوند.

---

[۱۴] Symmetric Key Cryptosystem

[۱۵] Public Key Cryptosystem

۱-۲-۱ رمزنگاری متقارن

در یک سیستم رمزنگاری اگر همواره کلید رمزگذاری e برابر کلید رمزگشایی d بوده و یا d به سادگی از روی e قابل محاسبه باشد، آنگاه سیستم را متقارن می‌نامیم.اگر آلیس و باب از یک سیستم رمز متقارن استفاده کنند باید قبل از تبادل اطلاعات کلید مخفی e را مبادله کنند.مبادله محرمانه کلید یک مسئله اساسی است.کلید e باید محرمانه نگهداری شود زیرا هرکس که به آن دسترسی پیدا کند می‌تواند کلید رمزگشای d را بدست آورد.

در سیستم های رمزنگاری متقارن عموما فرآیند رمزگشایی و رمزنگاری تشابه کامل دارند با این تفاوت که فقط مقادیر متغیرها و ثابت ها عوض می‌شوند ولی در مجموع ذات ساختار الگوریتم رمزنگاری و رمزگشایی متحدالشکل و یکسان است.

در شبکه ای که جمعا n کاربر وجود دارد و دو به دوی آنها می‌خواهند با یکدیگر ارتباطی امن و رمزنگاری شده برقرار کنند به تعریف و توافق $\frac{n(n-1)}{2}$ کلید سری و متقارن نیاز است.

از آنجا که در روش های متقارن پیامهای بزرگ در قالب قطعات کوچک پردازش و رمز می‌شوند، لذا یا باید برای هر بلوک کلید رمز را عوض کرد (که چنین کاری در عمل ممکن نیست) و یا باید بلوک های رمز را به نحوی به یکدیگر زنجیر کرد. در غیر این صورت بلوک های مشابه از متن اصلی به بلوک های رمز شده مشابهی تبدیل می‌شوند. همین موضوع که یک اخلالگر در شنود غیرمجاز اطلاعات رمزشده را مشابه ببیند، ممکن است بتواند در مورد ماهیت آن دو بلوک حدس های درستی بزند. لذا جلوگیری از نگاشته شدن بلوک های مشابه متن اصلی به بلوک های رمز شده یکسان به عملیاتی مجزا نیاز دارد که به الگوهای زنجیره سازی بلوک های رمز مشهورند.

بعضی از روشهای متقارن و مدرن عبارتند از روشهای DES ، 3-DES ، AES(Rijndael) ، IDEA ،Serpent و RC6 .برای آشنایی با این روشها به مرجع [۲] مراجعه کنید.