بسم الله الرحمن الرحيم

دانشگاه تهران

دانشکده علوم

به اشتراک گذاری رمز در رمز نگاری

نگارش: سعید صامت

استاد راهنما: دکتر هایده اهرابیان

استاد مشاور: دکتر حسین قدوسی

پایان نامه برای دریافت درجه کارشناسی ارشد در رشته

علوم کامپیوتر

خرداد ۱۳۸۲

جمهوری اسلامی ایران

دانشگاه تهران

دانشکده علوم

بسمه تعالی

اداره کل تحصیلات تکمیلی دانشگاه

احتراماً به اطلاع میرساند که جلسه دفاع از پایان نامه دوره **کارشناسی ارشد علوم کامپیوتر آقای سعید صامت** تحت عنوان:

به اشتراک گذاری رمز در رمزنگاری

در تاریخ ۸۲/۳/۱۸ در **گروه ریاضی و علوم کامپیوتر دانشکده علوم دانشگاه تهران** برگزار گردید.
هیأت داوران بر اساس کیفیت پایان نامه، مقالات انتشار یافته، استماع دفاعیه و نحوه پاسخ به سؤالات، **پایاننامه** ایشان را برای دریافت **درجه کارشناسی ارشد** در **رشته علوم کامپیوتر** معادل با ٦ واحد با نمره ۱۸/۵ با درجه **عالی** مورد ارزشیابی قرار داد.

هیأت داوران

سمت	نام و نام خانوادگی	مرتبه دانشگاهی	دانشگاه	امضاء
۱. استاد راهنما	**دکتر هایده اهرابیان**	استادیار	تهران	
۲. استاد داور	**دکتر حسن یوسفی آذری**	استادیار	تهران	
۳. استاد داور	**دکتر محمدابراهیم شیری**	استادیار	امیرکبیر	

معاون تحصیلات تکمیلی گروه
دکتر سیامک یاسمی

مدیر گروه
دکترعمید رسولیان

معاون تحصیلات تکمیلی دانشکده
دکتر مجید مدرس

این پایان نامه را تقدیم می کنم به همسر مهربانم که پیشرفت های خود را

مدیون زحمات بی دریغ او می دانم.

چکیده

در این رساله یکی از مباحث مهم مطرح شده در اصول رمزنگاری [1] بنام "به اشتراک گذاری رمز [2]" بررسی می گردد. ابتدا در مقدمه لزوم به اشتراک گذاری رمز، مثالها و کاربردهای عملی آن در دنیای واقعی بیان می شوند. سپس به کمک مقاله استینسون [3] [۱] بطور کامل به بررسی طرح آستانه ای شامیر [4] که برای اولین بار این مسئله را بصورت تئوری مطرح و راه حل آن را ارائه کرده است می پردازیم و همچنین طرح کلی به اشتراک گذاری رمز، مدل ریاضی آن و نیز یکسری تعاریف قراردادی را ارائه می نماییم. در ادامه یکی از طرح های به اشتراک گذاری رمز بنام "طرح هندسی" را که به دو صورت متفاوت توسط بلیک لی [5] و سیمونز [6] مطرح شده شرح می دهیم. پس از آن طرح به اشتراک گذاری رمز پیوسته بررسی می شود. سپس طرحهای به اشتراک گذاری فعال و قابل صحه گذاری توضیح داده خواهند شد و همچنین تقلب در طرح آستانه ای توسط شرکاء بهمراه راه حلی برای آن بررسی می گردد. فصل آخر نیز به پیاده سازی الگوریتم های مطرح شده و مقایسه آنها اختصاص داده شده است.

۱- *Cryptography*

۲- *Secret Sharing*

۳- *Stinson*

۴- *Shamir*

۵- *Blakley*

۶- *Simmons*

پیشگفتار

یکی از مسائلی که در مکانهای حساس مانند بانکها، پایگاههای نظامی، بانکهای اطلاعاتی و غیره مطرح است مسئله نحوه نگهداری رمزها و کلیدهای دسترسی و همچنین دسترسی به این مکانها و اطلاعات می باشد. اگر این اطلاعات بصورت یکجا و در نزد یک فرد یا دستگاه خاص قرار داده شود ضریب امنیتی به دلایل مختلف کاهش می یابد. یکی از این دلایل امکان مصالحه فرد نگهدارنده رمز با دشمن و فاش ساختن رمز دسترسی به اطلاعات، منابع و یا وسائل حساس و یا دسترسی دشمن به دستگاه نگهدارنده رمز می باشد. دلیل دیگر اینکه در صورتیکه فرد نگهدارنده رمز به هر علت حضور نداشته باشد و یا دستگاه نگهدارنده رمز از کار بیفتد، امکان دسترسی از بین خواهد رفت.

بطور کلی در دنیای امروز راه اندازی یک سیستم، از کار انداختن آن و یا امکان دسترسی به اطلاعات و منابع حساس نباید متکی به یک فرد و یا دستگاه خاص باشد. بهمین علت به اشتراک گذاری رمز و کلیدهای دسترسی بسیار ضروری می باشد.

مطمئنا به اشتراک گذاری رمز و یا کلید دسترسی بصورت مکانیکی و فیزیکی از زمانهای بسیار دور متداول بوده و می باشد. مانند تقسیم کردن نقشه یک گنج بین چندین نفر در گذشته و یا صندوقهای امانات بانکها در حال حاضر که دارای دو کلید و یا بیشتر هستند. اما بصورت تئوری اولین بار شامیر [۲] در سال ۱۹۷۹ این مسئله را مطرح و راه حلی برای آن ارائه کرد. او طرح خود را طرح آستانه ای[1] نامید. پس از او طرحهای دیگری نظیر طرحهای هندسی، فعال، پیوسته و ... توسط افراد مختلف ارائه گردید و همچنین مشکلاتی که طرحهای به اشتراک گذاری با آن روبرو هستند نظیر تقلب در به اشتراک گذاری توسط شرکاء و راه حلهای آنها مطرح شده است.

در این رساله سعی شده است به اشتراک گذاری رمز، تعدادی از طرحهای گوناگون و مشکلاتی که این طرحها با آنها مواجه هستند توضیح داده شود.

۱- *Threshold Scheme*

در فصل اول طرح آستانه ای شامیر، حالت عمومی طرح به اشتراک گذاری رمز، مدل ریاضی آن و همچنین تعدادی تعریف در رابطه با اشتراک گذاری به تفصیل شرح داده می شوند. در فصل دوم به بررسی طرح هندسی آن می پردازیم و با ارائه تعدادی مشاهده و مثال، ساخت هندسی طرحهای به اشتراک گذاری را بیان می کنیم.

در فصل سوم به بررسی یکی از طرحهای پیشرفته تر بنام به اشتراک گذاری پیوسته که مشکل حذف و یا اضافه شدن شرکاء به سیستم را بدون اینکه رمز اصلی و یا سهم های شرکاء موجود تغییر یابند حل می کند می پردازیم.

در فصل چهارم ابتدا طرح به اشتراک گذاری قابل صحه گذاری که وظیفه کنترل صحت سهم های توزیع شده بین شرکاء توسط توزیع کننده را بعهده دارد و سپس طرح به اشتراک گذاری فعال که برای رمزهای حساس و با طول عمر دراز بکار می رود بررسی می شوند.

در فصل پنجم تقلب در طرح آستانه ای به اشتراک گذاری رمز بیان شده و راه حلی برای آن ارائه خواهد شد و در فصل پایانی به پیاده سازی و مقایسه الگوریتم های مختلف مطرح شده در فصل های قبل پرداخته می شود.

فهرست مطالب

فصل اول

شرحی بر طرح های به اشتراک گذاری رمز

دراین فصل ابتدا به بیان چند تعریف پرداخته و سپس به کمک یکی از مقالات استینسون با طرح آستانه ای شامیر، طرح عمومی و مدل ریاضی طرح به اشتراک گذاری رمز آشنا می شویم.

۱-۱ تعاریف اولیه

تعاریف ریاضی:

هم نهشتی به پیمانه m : فرض کنیم m یک عدد طبیعی باشد. دو عدد صحیح a و b به پیمانه m هم نهشت اند هر گاه: $a-b=mk$ که در آن $k\in Z$ می باشد.(Z مجموعه اعداد صحیح است.)

دسته هم نهشتی: دسته هم نهشتی a به پیمانه m عبارتست از مجموعه $\{x \mid x\overset{m}{\equiv}a\}$

Z_m**:** مجموعه کلیه دسته های هم نهشتی متمایز به پیمانه m را با Z_m نشان می دهیم یعنی:

$$Z_m=\{0,1,...,m-1\}$$

گروه: ساختمان جبری $(G,*)$ را گروه گویند هر گاه در شرایط زیر صدق کند:

۱- شرکت پذیری $\forall a,b,c\in G:(a*b)*c=a*(b*c)$

۲- وجود عضو بی اثر $\exists e\in G;\forall a\in G:a*e=e*a=a$

۳- وجود عضو متقابل (وارون)

$\forall a \in G, a \neq e; \exists a' \in G : a * a' = a' * a = e$

گروه آبلی[1]: گروهی که دارای خاصیت جابجائی باشد گروه آبلی می نامند.

$\forall a, b \in G : a * b = b * a$

میدان: ساختمان جبری $(F,+,\times)$ میدان است اگر و تنها اگر:

۱- $(F,+)$ گروه آبلی باشد.

۲- $(F-\{0\},\times)$ گروه آبلی باشد.

۳- ضرب نسبت به جمع توزیع پذیر باشد.

میدان گالوا[2]:فرض کنیم p یک عدد اول و $n \in Z^+$ باشد. میدان با $q = p^n$ عضو، میدان گالوا از مرتبه $q = p^n$ نامیده می شود و با $GF(q)$ نشان داده می شود.

گراف[3]: گراف مجموعه ای است از نقاط و خطوطی که تعدادی (و شاید هیچکدام) از نقاط را به یکدیگر متصل می کنند. نقاط گراف معمولاً رأس و خطوط نیز یال نامیده می شوند.

گراف کامل[4]: گراف کامل گرافی است که هر جفت از رئوس آن توسط یک یال به یکدیگر متصل باشند. یک گراف کامل با n رأس دارای $\binom{n}{2} = \frac{n \times (n-1)}{2}$ یال می باشد.

ابر گراف[5]: گرافی که یالهای آن دو یا بیش از دو رأس را به یکدیگر متصل کنند ابرگراف نامیده می شود.

۱- *Abelian Group*

۲- *Galois Field*

۳- *Graph*

۴- *Complete Graph*

۵- *Hypergraph*

تعاریف و اصطلاحات رمزنگاری:

فرستنده: طرفی از یک سیستم ارتباطی می باشد که اطلاعات صحیح را ارسال می کند.

دریافت کننده: طرفی از یک سیستم ارتباطی می باشد که اطلاعات را دریافت می کند.

دشمن[1]**:** طرفی از یک سیستم ارتباطی می باشد که نه فرستنده است و نه دریافت کننده ولی سعی دارد امنیت ارتباطی بین فرستنده و دریافت کننده را مختل ساخته و یا از بین ببرد.

سندیت[2]**:** به دریافت کننده پیغام کمک می کند تا صحت هویت فرستنده را بررسی کند.

حمله فعال[3]**:** تهاجم دشمن به سیستم به قصد ایجاد وقفه در ارتباط، تغییر اطلاعات در حال ارسال و یا ارسال اطلاعات جعلی از طرف خود دشمن می باشد.

حمله غیر فعال[4]**:** تهاجم دشمن به سیستم به قصد بدست آوردن اطلاعاتی که در حال ارسال می باشد.

اطلاعات محرمانه[5]**:** اطلاعاتی که بصورت امن نگهداری شده و یا ارسال گردد را محرمانه می نامند.

اطلاعات عمومی[6]**:** اطلاعاتی که بصورت آشکار نگهداری شده و یا ارسال گردد را عمومی می نامند.

۱- *Adversary*

۲- *Authenticity*

۳- *Active Attack*

۴- *Passive Attack*

۵- *Private*

۶- *Public*

کلید محرمانه [1]: پارامتر K که به کمک آن پیغام به رمز درآمده و ارسال می گردد را کلید محرمانه می نامند.

به رمز در آوردن [2]: عمل اولیه معکوس پذیر در رمز نگاری که پیغام مورد نظر برای ارسال را به صورتی دیگر تبدیل می کند. اگر پیغام را با M و به رمز درآورده شده آن را با C و کلید لازم برای به رمز درآوردن پیغام را با K نمایش دهیم آنگاه داریم: $C = E_K(M)$ که در آن E نشاندهنده عمل به رمز درآوردن پیغام می باشد.

بازگشائی رمز [3]: عمل عکس به رمز درآوردن پیغام را که معمولا توسط دریافت کننده انجام خواهد شد بازگشائی رمز می نامند و آن را به صورت زیر نمایش می دهند.

$$D_K = E_K^{-1}$$

$$D_K(C) = E_K^{-1}(E_K(M)) = M$$

امنیت بدون شرط [4]: یک سیستم رمز نگاری دارای امنیت بدون شرط می باشد هرگاه دشمن نتواند با انجام محاسبات نامحدود امنیت سیستم را برهم زند.

روش های مرسوم رمز نگاری: روش های گوناگونی برای به رمز درآوردن متن ارائه شده است که تعدادی از آنها به شرح زیر است:

استگانوگرافی [5]: در این روش قدیمی پیغامها به طرق گوناگونی به رمز درآورده می شدند. از جمله:

۱- *Secret Key*

۲- *Encryption*

۳- *Decryption*

۴- *Unconditional*

۵- *Steganography*

۱- استفاده از جوهر نامرئی

۲- ایجاد سوراخهای ریز روی حروف مورد نظر

۳- استفاده از ریبون دستگاه تایپ

روشهای کلاسیک:

۱- روش سزار[1]**:** در این روش سزار هر حرف پیغام را با سه حرف جلوتر در حروف الفبا تعویض می نمود.

۲- روش انتقال[2]**:** حالت کلی روش سزار می باشد که در آن هر حرف متن با K ($1 \le K \le 26$) حرف جلوتر در حروف الفبا تعویض می گردد.

۳- روش های مونو آلفابتیک[3]**:** در این روش ها هر حرف متن پیغام بر اساس یک جایگشت با یکی از حروف الفبا تعویض می گردد.

۴- روش های پلی آلفابتیک[4]**:** در این روش ها هر حرف متن پیغام بسته به اینکه در کدام موقعیت در متن قرار داشته باشد، با یکی از حروف دیگر جایگزین می شود. معروفترین این روش ها روش ویجینر[5] می باشد.

۱- *Caesar*

۲- *Shift cipher*

۳- *Monoalphabetic cipher*

۴- *Polyalphabetic cipher*

۵- *Vigenere cipher*

روشهای مدرن:

۱- **روش استاندارد**[1]: در این روش به کمک ترکیبی از تعدادی جایگشت و جابجائی و انتقال، متن پیغام به رمز درآورده خواهد شد.

۲- **روش آر-اس-ا**[2]: این روش بر خلاف روشهای قبل که تنها از کلید محرمانه استفاده می کردند علاوه بر کلید محرمانه از کلید عمومی نیز بهره می برد. در واقع فرستنده توسط کلید عمومی متن پیغام را به رمز در می آورد و دریافت کننده به کمک کلید محرمانه رمز را بازگشائی می کند. به طور خلاصه مراحل این روش را شرح می دهیم:

الف- دریافت کننده دو عدد اول متمایز و بزرگ p و q را انتخاب می کند.

ب- N و $\varphi(N)$ را به کمک معادلات زیر محاسبه می کند.

$$N = p \times q$$

$$\varphi(N) = (p-1) \times (q-1)$$

پ- کلید عمومی k را با شرط $0 \le k \le \varphi(N)$ بطوریکه بزرگترین مقسوم علیه مشترک k و $\varphi(N)$ یک باشد، به صورت تصادفی انتخاب می کند.

۱- *DES*

۲- *RSA*