وزارت علوم، تحقیقات و فناوری
دانشگاه تحصیلات تکمیلی علوم پایه
گاوازنگ - زنجان

طرح توزیع کلید توزیع شده

پایان‌نامهٔ کارشناسی ارشد

گل‌بس استادی

استاد راهنما: **دکتر علی طاهرخانی**

دی ۱۳۹۱


بسم الله الرحمن الرحيم

تقدیم به

پدر و مادرم

و

کسانی که عشق را هم ارز تعهد می دانند.

تشکر و قدردانی

خداوند بزرگ را شاکرم به سبب تمام نعمت‌هایی که به من عطا فرموده. از خانواده مهربانم به ویژه پدر و مادر عزیزم که همواره در سایه پر مهر وجودشان فرصت رشد و آموختن یافتم سپاس‌گزارم و بهترین‌ها را برایشان آرزومندم.

از استاد بزرگوارم جناب آقای دکتر طاهرخانی که در انجام و تدوین این پایان‌نامه با نهایت صبوری و مهربانی مرا یاری نمودند صمیمانه قدرانی می‌کنم و امیدوارم سپاس فراوان مرا بپذیرند.

سپاس خالصانه‌ام را تقدیم می‌نمایم به آقای رضا هاشمی بخاطر همراهی ایشان در طی این دو سال.

از دوستان خوبم که خاطرات زیبای بودن در کنارشان را هرگز از یاد و قلبم نخواهم برد و همچنین از آقای آرمین جمشیدپی که در یادگیری مفاهیم اولیه رمزنگاری کمک شایانی به بنده کردند سپاس‌گزارم.

چکیده

مرکز توزیع کلید (KDC) یک شبکه، کارگزاری است که قادر است ارتباط خصوصی بین گروهی از کاربرها را برقرار کند. هر کاربر یک کلید با مرکز به اشتراک می‌گذارد. وقتی یک کاربر می‌خواهد با اعضای دیگر ارتباط برقرار کند مرکز، سهم‌هایی را به شکل رمز شده به کاربرها می‌فرستد که بتوانند کلیدهای مخفی را برای رمزگذاری و رمزگشایی پیام‌ها، برای ارتباط با دیگر اعضای کنفرانس محاسبه کنند. یک مرکز توزیع کلید توزیع شده (DKDC) مجموعه‌ای از n کارگزار شبکه است که با هم مرکز توزیع کلید را تشکیل می‌دهند. در این پایان‌نامه طرح توزیع کلید توزیع شده را معرفی خواهیم کرد که در آن مرکز توزیع کلید، یک مجموعه از n کارگزار است. همچنین مدل‌هایی مانند پلکانی و ساختار دسترسی روی مجموعه کارگزارها را ارائه خواهیم کرد. در هر مدل کران‌های پایینی برای منابع مورد نیاز مانند بیت‌های تصادفی، حافظه ذخیره‌سازی و . . .، برای تنظیم و مدیریت یک طرح توزیع کلید توزیع شده (DKDS) را نشان می‌دهیم و سپس پروتکل‌هایی را بیان می‌کنیم که نشان دهنده‌ی اجرایی بودن این طرح‌ها هستند.

کلمات کلیدی. طرح توزیع کلید، طرح توزیع کلید توزیع شده، مدل پلکانی، طرح تسهیم راز.

فهرست

لیست تصاویر

پیش‌گفتار

با افزایش ارتباطات برای مقاصد مختلف، نیاز بیشتری برای تحقیق در راستای سریع‌تر و امن‌تر شدن آن‌ها احساس شد. این ارتباطات گاه برای انتقال اطلاعات نظامی، سیاسی، شخصی و ... صورت می‌گیرد. لذا ضرورت امن نگه‌داشتن این ارتباطات بیشتر احساس می‌شود. در این تبادل اطلاعات همواره اطلاعاتی وجود دارند که دارنده‌ی آن در صدد است تا تنها افرادی که مد نظر او هستند از آن آگاه شوند و هر فرد دیگری، قادر به دریافت این اطلاعات نباشد.

فرض کنید n کاربر برای برقراری ارتباط با یکدیگر از الگوریتم کلید عمومی استفاده کنند. لذا اگر یک کاربر بخواهد متن یکسانی مانند M را به n کاربر متفاوت بفرستد، باید n بار رمز شده متن M را با n کلید عمومی متفاوت محاسبه کند و سپس آن را به کاربرها بفرستد. مشکلی که در الگوریتم کلید عمومی وجود دارد این است که اگر تعداد کاربرهایی که می‌خواهند با هم مکاتبه کنند زیاد باشد، آنگاه هر کاربر برای فرستادن یک متن به اعضای دیگر کنفرانس نیاز دارد که یک متن را چندین بار با کلیدهای عمومی مختلف رمز کند. با توجه به اینکه الگوریتم‌های رمزگذاری و رمزگشایی با کلید عمومی، عملیات کندی هستند لذا این روش موثر نیست. پس سوال این است چطور می‌توان پروتکل کارآمدی تنظیم کرد که یک کلید مشترک را برای هر کنفرانس فراهم کند. یک راه حل معمول استفاده از مرکز توزیع کلید (KDC) است که در آن یک کارگزار مسئولیت توزیع و مدیریت کلیدهای محرمانه را به عهده دارد.

ایده استفاده از KDC به این صورت است که هر کاربر یک کلید مشترک با KDC به اشتراک می‌گذارد. وقتی که کاربر می‌خواهد به صورت محرمانه با کاربرهای دیگر ارتباط برقرار کند، یک پیام تقاضای کلید کنفرانس به KDC می‌فرستد. KDC عضویت کاربر در کنفرانس را بررسی می‌کند و

سپس کلید کنفرانس را به صورت رمزشده برای کاربر می‌فرستد. نیدهام [۱] و اسکرودر [۲] اولین کسانی بودند که در سال ۱۹۷۸ این روش را آغاز کردند [۱۳]. طرح اجرا شده توسط KDC برای نحوه توزیع کلید کنفرانس را KDS می نامیم. توزیع کلید مسئله‌ای است که در رمزنگاری به طور گسترده‌ای مطالعه شده است. مقاله‌های زیادی در این زمینه وجود دارند. انواع مختلفی از طرح‌های توزیع کلید تاکنون بررسی شده است مانند طرح‌های پیش توزیع کلید (KPS)، طرح‌های توافق کلید (KAS) و ...

در طرح توزیع کلید، KDC وظیفه توزیع کلید را به عهده دارد. وضعیت ناخوشایندی که وجود دارد این است که KDC همه‌ی کلیدهای مخفی کنفرانس‌ها را می‌داند. بنابراین باید مورد اعتماد باشد. به‌علاوه KDC می‌تواند یک نقطه شکست برای سامانه باشد. از طرفی همه‌ی کاربرها وقتی می‌خواهند کلید کنفرانس را به‌دست آورند باید با مرکز ارتباط برقرار کنند.

در این پایان‌نامه، توجه خود را روی یک مدل پیشرفته برای رفع ضعف یک KDC متمرکز می‌کنیم. یک راه حل قوی و موثر می‌تواند مرکز توزیع کلید توزیع شده (DKDC) باشد. یک DKDC مجموعه‌ای از n کارگزار شبکه است که با هم مرکز توزیع کلید را تشکیل می‌دهند.

یک کاربر برای ارتباط با اعضای کنفرانسی که عضوی از آن است، نیاز به کلید آن کنفرانس دارد. لذا یک پیام تقاضای کلید به زیرمجموعه‌ای مجاز از n کارگزار می‌فرستد. کارگزارهایی که مورد ارتباط واقع شده‌اند، با مقداری اطلاعات که کاربر را قادر به محاسبه کلید می‌سازد به کاربر پاسخ می‌دهند. در یک چنین مدلی یک کارگزار خودش به تنهایی کلیدهای مخفی را نمی‌داند چون کلیدها بین n کارگزار تقسیم شده‌اند. در این مدل محدودیت ارتباط حذف شده است چرا که هر کاربر می‌تواند همزمان یک

---

[۱] Needham

[۲] Schroeder

پیام تقاضای کلید را به کارگزارهای مختلف بفرستد و از این رو اتلاف وقت برای محاسبه کلید نیز وجود ندارد. اگر کاربرها قادر به ارتباط با برخی از کارگزارها نباشند همچنان می‌توانند کلیدهایی را که نیاز دارند، به‌دست آورند.

در فصل اول مقدمه‌ای از رمزنگاری ارائه خواهد شد. در فصل دوم که برگرفته از مرجع [۱۱] است به بررسی طرح توزیع کلید توزیع شده می‌پردازیم و کران‌هایی برای آن ارائه می‌دهیم. در فصل سوم که برگرفته از مرجع [۴] است مدلی دیگر از طرح توزیع کلید را مورد بررسی قرار می‌دهیم و کران‌هایی نیز برای آن ارائه می‌دهیم. در فصل‌های دوم و سوم، کران‌ها به کمک خواص آنتروپی محاسبه می‌شوند و در نهایت در فصل چهارم یک طرح توزیع کلید توزیع شده با ساختار دسترسی روی مجموعه کارگزارها را ارائه می‌دهیم. این فصل نیز با توجه به مرجع [۳] جمع‌آوری شده است. در این فصل برخلاف فصل‌های دوم و سوم برای به‌دست آوردن کران‌ها از خواص آنتروپی استفاده نخواهد شد بلکه با کاهش طرح توزیع کلید توزیع شده به طرح تسهیم راز، کران‌هایی را برای این طرح به‌دست می‌آوریم.

فصل اول

مقدمه‌ای بر رمزنگاری

از دیرباز تا کنون همواره تبادل اطلاعات به شیوه‌های گوناگون میان انسان‌ها رواج داشته است. در این تبادل اطلاعات، همواره اطلاعاتی وجود دارند که دارنده‌ی آن درصدد است تا تنها افرادی که مدنظر او هستند از آن آگاه شوند و هر فرد دیگری، قادر به دریافت این اطلاعات نباشد. اولین راه حلی که به ذهن می‌رسد این است که اطلاعات را دور از دسترس عموم نگه داریم. ولی قطعا در بسیاری از موارد این امکان وجود نخواهد داشت. به عنوان مثال فرض کنید فردی (آن را آلیس می‌نامیم) قصد دارد پیامی را به شخص دیگری (آن را باب می‌نامیم) در فاصله‌ای دور بفرستد. طبیعی است در این صورت مخفی نگه داشتن آن عملی نخواهد بود.

مطالعه روش‌هایی که شخص را قادر سازد از اطلاعات شخصی خود محافظت کند همواره مورد توجه بشر بوده است. رمزنگاری دانشی است که تلاش می‌کند تا با تبدیل اطلاعات به یک شکل غیرمتعارف از فاش شدن آن‌ها جلوگیری کند. در واقع اطلاعات به گونه‌ای ذخیره یا انتقال داده می‌شوند که با فرض قرار گرفتن در اختیار افراد دیگر قابل بهره‌برداری نباشد.

آنچه باعث پیشرفت روز به روز دانش رمزنگاری شده توسعه‌ی روز افزون روابط تجاری، اجتماعی، سیاسی و . . . است. در این فصل ابتدا رمزنگاری متقارن را مورد بررسی قرار می‌دهیم و برای درک بهتر آن مثالی ارائه می‌دهیم.

۱.۱ رمزنگاری متقارن

به منظور درک بهتر سامانه‌های رمزنگاری، این بخش را با مثالی ساده آغاز می‌کنیم.

فرض کنید آلیس و باب در یک مکان نیستند و قصد دارند به‌طور محرمانه با یکدیگر ارتباط برقرار کنند. از آنجایی که این ارتباط از راه دور است. لذا نیازمند واسطه‌هایی مانند اینترنت و . . . است (از این پس این واسطه‌ها را شبکه یا مجرای ارتباطی می‌نامیم). از طرفی فرض می‌کنیم این مجراهای ارتباطی به هیچ وجه امن نیستند. بنابراین با این فرض آلیس و باب در تلاشند از روشی استفاده کنند که اگر اطلاعاتشان در اختیار فرد دیگری (مانند اسکار) قرار گرفت قابل بهره‌برداری نباشد.

فرض کنید آلیس می‌خواهد متن زیر را برای باب بفرستد. با این فرض که مجرای ارتباطی کاملا ناامن است.

آدمی را آدمیت لازم است.

برای اینکه محتوای این پیام (آن را متن اصلی می‌نامیم) برای افراد دیگر قابل فهم نباشد، آلیس باید به دنبال راه حلی باشد. بنابراین در گام اول، آلیس حروف الفبای پیام فوق را طبق جدول صفحه بعد به اعداد تبدیل می‌کند. [۱]

[۱] در تبدیل یک متن به رمز، فاصله بین کلمات، نقطه و . . . حذف خواهد شد و همچنین حروفی مانند حمزه و نظایر آن به حروف مشابه مانند ی و . . . تبدیل می‌شوند.

الف	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش
۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶

ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی
۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰	۳۱	۳۲

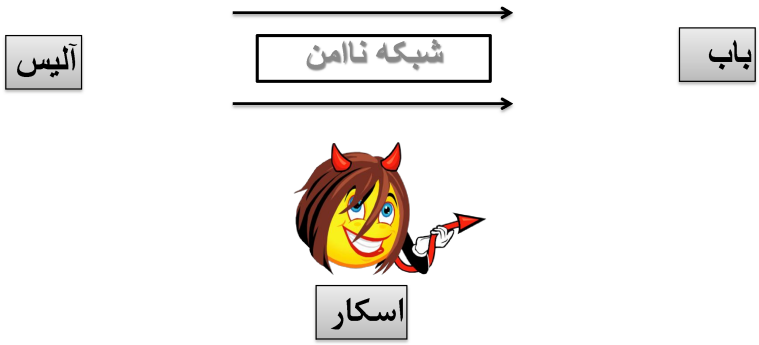
به عنوان مثال د به ۱۰، س به ۱۵ و م به ۲۸ تبدیل می‌شوند. سپس برای اینکه پیام را منتقل کند اعداد به‌دست آمده را با ۷ جمع می‌کند و حاصل را به پیمانه ۳۲ (روی حلقه $\frac{Z}{۳۲Z}$) حساب می‌کند و دوباره اعداد به‌دست آمده را با حروف الفبا جایگزین می‌کند. لذا پس از انجام این محاسبات، متن اصلی به صورت زیر خواهد بود.

حصپچطححصپچذبحظپحغذ [۱]

متن فوق همان متن رمز شده‌ای است که آلیس به باب خواهد فرستاد. افراد دیگری که این متن را می‌بینند به‌وضوح با متن به ظاهر بی‌معنی مواجه می‌شوند. حال با فرض اینکه باب تابع رمزنگار را بداند یعنی بداند یک حرف به حرف دیگر انتقال پیدا کرده است (آن را رمز انتقالی می‌نامیم)، برای اینکه از محتوای پیام آگاه شود کافی است بداند این انتقال به اندازه ۷ بوده است. آنگاه برای بازیابی متن اصلی، متناظر ۷+ یعنی ۷- را به مقدار عددی هر حرف اضافه می‌کند. پس موفق خواهد شد متن اصلی را به‌دست آورد.

متاسفانه همیشه عده‌ای در پی آن هستند که به متن اصلی دست پیدا کنند. فرض کنیم اسکار فردی باشد که تلاش می‌کند تا به متن اصلی دست یابد. در این مثال با فرض اینکه اسکار از تابع رمزگذار

[۱] به منظور اینکه متن رمزی اطلاعات کمی را فاش کند از گذاشتن فاصله خودداری می‌کنیم. چرا که تعداد حروف یک واژه می‌تواند به فهم متن کمک کند.



شکل ۱.۱ : سامانه رمزنگاری

آگاه باشد، تا زمانی که نداند انتقال به چه اندازه بوده است قادر به بازگشایی متن رمزی نخواهد بود. آنچه در اینجا نقش اصلی را به عهده داشت انتقال به اندازه ۷ بود که آن را کلید می‌نامیم و با k نمایش می‌دهیم. کلید در یک سامانه رمزگذار مولفه‌ای است که تابع رمزگذار را به طور صریح مشخص می‌کند. همان‌طور که مشاهده کردیم عدد ۷ در این مثال هیچ خاصیت ویژه‌ای نداشت و به راحتی می‌توانستیم هر عدد دیگری را با آن جایگزین کنیم. پس به نظر می‌رسد که هر سامانه دارای مجموعه‌ای از کلیدها است. اکنون که آمادگی لازم را ایجاد کردیم تعریفی برای سامانه‌های رمزنگاری ارائه می‌دهیم.

هر سامانه رمزنگاری مجموعه‌ای از علائم برای نمایش متن اصلی، مجموعه‌ای از علائم برای نمایش متن رمزی(که می‌تواند با مجموعه اول یکی باشد)، مجموعه‌ای از کلیدها و توابع رمزگذار و رمزگشا را در خود دارد.

تعریف ۱.۱.۱. [۱۵] سامانه رمزنگاری یک پنج تایی مرتب $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ است که دارای شرایط زیر است.

- $\mathcal{P}$ مجموعه‌ای ناتهی و متناهی از متن‌های اصلی

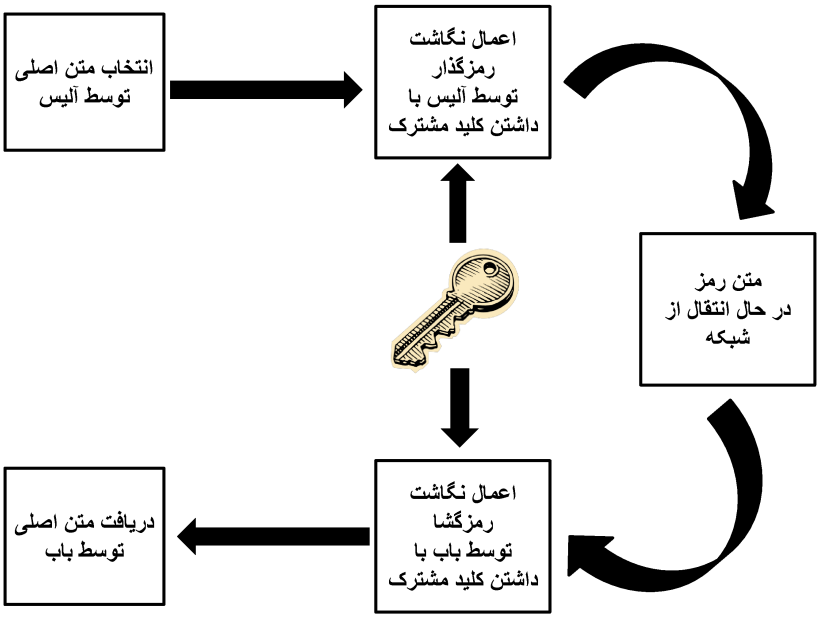
- $\mathcal{C}$ مجموعه‌ای ناتهی و متناهی از متن‌های رمزی
- $\mathcal{K}$ مجموعه‌ای متناهی از کلیدها که به آن فضای کلید می‌گوییم.
- به ازای هر $k \in \mathcal{K}$ تابع رمزگذار $e_k \in \mathcal{E}$ و متناظر با آن تابع رمزگشای $d_k \in \mathcal{D}$ وجود دارند که $e_k : \mathcal{P} \longrightarrow \mathcal{C}$ و $d_k : \mathcal{C} \longrightarrow \mathcal{P}$. همچنین برای هر $x \in \mathcal{P}$ داریم $d_k(e_k(x)) = x$.

برای ایجاد امنیت بالا در سامانه‌های رمزی، فرض می‌کنیم اسکار می‌داند آلیس و باب از کدام سامانه رمزنگاری استفاده کرده‌اند یعنی فرض را بر آن می‌گذاریم که اسکار تمام اطلاعات در مورد تابع رمزگذار و رمزگشا و حتی فضای کلید را می‌داند و از تنها چیزی که آگاهی ندارد این است که نمی‌داند از کدام کلید استفاده شده است. لذا در تمام حمله‌ها نیز این چنین فرض می‌کنیم که اسکار یا هر مجموعه افراد دیگری به دنبال به‌دست آوردن هرگونه اطلاعاتی در مورد کلید هستند.

اصل کرکهف. همواره فرض می‌کنیم که اسکار همه‌ی اطلاعات در مورد سامانه رمزنگاری به غیر از کلید را می‌داند. به عبارتی دیگر امنیت سامانه فقط وابسته به کلید است.

علاوه بر ایجاد امنیت بالاتر، حفاظت از اطلاعات با حجم کمتر همواره آسان‌تر و کم هزینه‌تر است. لذا حفاظت از کلید به نسبت آسان‌تر از حفاظت از کل سامانه رمزنگاری است. همان گونه که توصیف شد هرگاه آلیس و باب تصمیم داشته باشند که به‌طور محرمانه و خصوصی با هم ارتباط برقرار کنند در زمانی که کنار یکدیگر هستند و یا زمانی که یک مجرای ارتباطی امن وجود دارد دو کلید یکسان را انتخاب می‌کنند و هر کدام از آن‌ها یکی از کلیدها را نزد خود نگه می‌دارد. سپس در زمانی که کنار یکدیگر نباشند از آن‌ها استفاده خواهند کرد. روشی که شرح داده شد ایده‌ی رمزنگاری متقارن است. با توجه به توصیف‌های ذکر شده، در سامانه رمزنگاری متقارن، کلید رمزگذاری و کلید رمزگشایی یکسان(متقارن) هستند.

رمز انتقالی که در ابتدا مورد بحث قرار گرفت نمونه‌ای از رمز متقارن است. در ادامه معایب رمز



شکل ۲.۱: سامانه رمزنگاری متقارن

متقارن را توضیح خواهیم داد.

۱.۱.۱ معایب رمزنگاری متقارن

همان طور که در بخش قبل شرح داده شد در رمزنگاری متقارن، آلیس و باب باید قبل از اینکه در فاصله‌ای دور قرار بگیرند و در حالی که مجرای ارتباطی امن است، توافق کلید کنند. لذا در شرایطی که در زیر بیان خواهیم کرد رمزنگاری متقارن پاسخگوی نیاز ما نخواهد بود.

- فرض کنید آلیس و باب در فاصله‌ای دور قرار گرفته باشند و یا شبکه‌ای امن در دسترس نباشد. در این صورت برای تعیین یک کلید مشترک چگونه باید عمل کرد؟
- فرض کنید N نفر در یک شبکه قصد دارند دو به دو با هم ارتباط خصوصی برقرار کنند. آنگاه تعداد کلیدهای لازم $\binom{N}{2}$ خواهد بود. لذا نگهداری از چنین فضای کلید بزرگی به راحتی

امکان‌پذیر نخواهد بود. از طرفی هر فردی برای اینکه با $N-1$ فرد دیگر ارتباط برقرار کند باید $N-1$ کلید را نزد خود نگه دارد که این نیز چندان آسوده نخواهد بود.

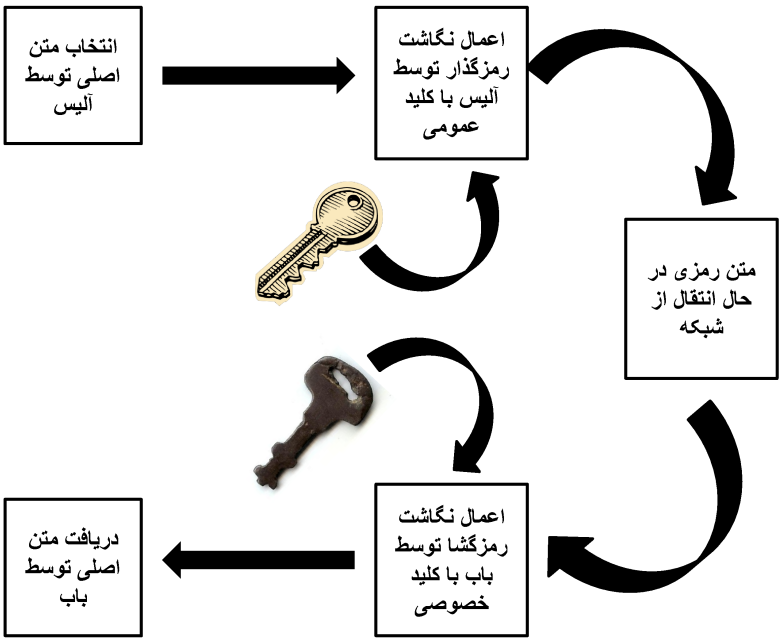
لذا به دنبال سامانه‌ای هستیم که این دو ضعف را نداشته باشد.

۲.۱ رمزنگاری نامتقارن یا کلید عمومی

در مدل‌های ابتدایی رمزنگاری، آنچه بررسی شد، آلیس و باب به‌طور محرمانه کلید مشترک k را انتخاب می‌کردند.

فرض کنید آلیس و باب در مکان‌هایی دور از یکدیگر قرار دارند و تصمیم دارند به طور محرمانه با هم ارتباط برقرار کنند. در چنین حالتی اگر آن‌ها به یک شبکه امن دسترسی نداشته باشند آلیس پیام خود را درون جعبه‌ای قرار می‌دهد و آن را با کلیدی که فقط خودش می‌داند، قفل می‌کند. سپس جعبه را برای باب می‌فرستد. باب که از کلید آلیس خبری ندارد قادر به باز کردن آن نخواهد بود. بنابراین قفل دیگری که فقط خودش کلیدش را می‌داند، به جعبه خواهد زد و آن را برای آلیس می‌فرستد. اکنون وضعیت آلیس را بررسی می‌کنیم. آلیس جعبه‌ای را در دست دارد که هم قفل خود و هم قفل باب بر آن زده شده است. لذا با کلیدی که در دسترس دارد قفل مربوط به خود را باز می‌کند و سپس جعبه‌ای که فقط قفل باب بر روی آن است بار دیگر برای باب می‌فرستد. باب نیز با کلیدی که در دسترس دارد به راحتی می‌تواند جعبه مذکور را باز کند و پیامی که آلیس در آن قرار داده بود را بخواند. الگویی که توصیف شد ایده‌ی رمزنگاری نامتقارن است.

در این سامانه دو نوع کلید وجود دارد یک کلید خصوصی و یک کلید عمومی. هرگاه آلیس قصد داشته باشد پیامی را برای باب بفرستد آن را با کلید عمومی مربوط به باب رمز می‌کند و سپس آن را



شکل ۳.۱: سامانه رمزنگاری نامتقارن

برای باب می‌فرستد. باب نیز برای اینکه محتوای پیام را مشاهده کند آن را با کلید خصوصی باز می‌کند. شکل فوق سامانه رمزنگاری نامتقارن را به تصویر می‌کشد.

ایده رمزنگاری کلید عمومی توسط دیفی [۱] و هلمن [۲] در سال ۱۹۷۶ پایه گذاری شد. سپس در سال ۱۹۷۷، ریوست [۳]، شمیر [۴] و ادلمان [۵] سامانه رمزنگاری RSA را ابداع کردند [۱۵]. چندین سامانه رمزنگاری نامتقارن تاکنون ارائه شده است. مانند سامانه رمزنگاری الجمال [۶]، دیفی-هلمن و . . . .

---

۱ Diffie

۲ Hellman

۳ Rivest

۴ Shamir

۵ Adleman

۶ ElGamal

اکنون سامانه رمزنگاری RSA را به عنوان یک سامانه رمزنگاری کلید عمومی مورد بررسی قرار می‌دهیم زیرا در زمانی که تاسیس شد بسیار مورد توجه قرار گرفت و به‌طور گسترده‌ای از آن استفاده شد. در حال حاضر به‌طور قطع می‌توان گفت معروف‌ترین سامانه رمزنگاری در تمام دوران است. اهمیت سامانه RSA از آن جهت است که امنیت آن بر پایه‌ی دشواری تجزیه اعداد بزرگ است [۱۶].

ابتدا باب دو عدد اول متمایز بزرگ p و q را به‌طور محرمانه انتخاب می‌کند و عدد $n = pq$ را تشکیل می‌دهد و n را که عمومی است به عنوان پیمانه قرار می‌دهد. دقت کنید که $\phi(n) = (p-۱)(q-۱)$. حال اگر باب تصمیم داشته باشد پیام x را برای آلیس بفرستد، $y = x^b$ را محاسبه می‌کند و برای او می‌فرستد. آلیس نیز برای اینکه به محتوای پیام دست یابد آن را به توان a می‌رساند. عددهای a و b دارای این خاصیتند که

$$ab \equiv ۱ \mod \phi(n).$$

لذا عددی مانند t وجود دارد که

$$ab = t\phi(n) + ۱.$$

حال بررسی می‌کنیم که چگونه آلیس قادر به رمزگشایی متن رمز شده می‌شود. فرض کنید $x \in \mathbb{Z}_n^*$ [۱]. بنابراین داریم

$$\begin{aligned}(x^b)^a &\equiv x^{t\phi(n)+۱} \mod n \\ &\equiv (x^{\phi(n)})^t x \mod n \\ &\equiv ۱^t x \mod n \\ &\equiv x \mod n.\end{aligned}$$

[۱] مجموعه اعداد عضو $\mathbb{Z}_n$ که نسبت به n اول هستند.