
بسم الله الرحمن الرحيم

سمینار

عنوان

مطالعه و ارزیابی روش های رمزنگاری متقارن و نامتقارن

فهرست مطالب

عنوان | صفحه

چکیده ۱

فصل اول: مقدمه

۱-۱- مقدمه ۳

فصل دوم: مبانی نظری و پیشینه تحقیق

۲-۱- مقدمه ۷

۲-۲- سیستم‌های امنیتی ۸

۲-۲-۱- رمزنگاری ۱۰

۲-۲-۲- تاریخچه رمزنگاری ۱۰

۲-۲-۳- تفاوت پنهان‌نگاری و رمزنگاری ۱۳

۲-۲-٤- مثالی برای پنهان‌نگاری و رمزنگاری ۱٤

۲-۳- الگوریتم‌های آشکارسازی پیام ۱٦

۲-۳-۱- آشکارسازی ویژه ۱٦

۲-۳-۲- آشکارسازی کور (عمومی) ۱۷

۲-٤- رمزنگاری پیشرفته ۱۷

۲-۵- تعاریف و اصطلاحات ۱۷

۲-٦- پروتکل‌های رمزنگاری ۱۸

۲-۷- نیازمندی‌های امنیتی ۱۹

۲-۷-۱- محرمانگی داده‌ها ۱۹

۲-۷-۲- تمامیت داده‌ها ۱۹

۲-۷-۳- تازگی داده‌ها ۱۹

۲-۷-٤- احراز هویت ۲۰

۲-۸- طبقه‌بندی روش‌های رمزنگاری ۲۰

۲-۹- الگوریتم درهم ساز ۲۱

۲-۹-۱- MD5 ..... ۲۲
۲-۹-۲- SHA-1 ..... ۲۵
۲-۹-۳- RIPEMD ۲۶
۲-۱۰- الگوریتم‌های رمزنگاری متقارن و نامتقارن ۲۹
۲-۱۱- رمزنگاری متقارن ۳۰
۲-۱۱-۱- الگوریتم DES ۳۱
۲-۱۱-۲- الگوریتم AES ۳۱
۲-۱۱-۳- الگوریتم Blow Fish ۳۳
۲-۱۲- رمزنگاری کلید نامتقارن ۳۵
۲-۱۳- کلمات و اصطلاحات ۳۵
۲-۱٤- روش‌های ارائه شده برای رمزنگاری اطلاعات دیجیتال ۳٦
۲-۱۵- جمع بندی ۳۸

فصل سوم: نتیجه‌گیری و پیشنهادات

۳-۱- نتیجه گیری و پیشنهادت ۳۹

مراجع ٤۱

فهرست اشکال

شکل ۲-۱- نمای کلّی از سیستم‌های امنیتی ۱۰
شکل ۲-۲- مدل پایه‌ای رمزنگاری ۱۵
شکل ۲-۳- مدل پایه‌ای پنهان نگاری ۱۵
شکل ۲-٤- طبقه‌بندی الگوریتم‌های رمزنگاری ۲۲
شکل ۲-۵- ساختار درونی تابع درهم ساز ۲۳
شکل ۲-٦- ساختار کلی الگوریتم رمزنگاری MD5 ..... ۲٤
شکل ۲-۷- مدار داخلی HMD5 در روش رمزنگاری MD5 ..... ۲٤
شکل ۲-۸- تابع فشرده ساز در الگوریتم رمزنگاری MD5 ..... ۲۵
شکل ۲-۹- تابع فشرده ساز در روش SHA-1 ..... ۲٦
شکل ۲-۱۰- مدار داخلی تابع درهم ساز RIPEMD ۲۷
شکل ۲-۱۱- تابع فشرده ساز RIPEMD ۲۸
شکل ۲-۱۲- شماتیک کلی سامانه رمزنگاری متقارن ۳۱
شکل ۲-۱۳- الگوریتم رمزنگاری AES ۳۳
شکل ۲-۱٤- روند اجرای الگوریتم Blow Fish ۳٤
شکل ۲-۱۵- عملیات داخلی تابع F ۳۵

فهرست جداول

جدول ۲-۱- مقایسه بین پنهان نگاری و رمزنگاری ۱۷
جدول ۲-۲- بیت‌های ورودی ۲۵
جدول ۲-۳- مقایسه توابع درهم ساز ۲۹
جدول ۲-٤- برخی اصطلاحات سیستم‌های امنیتی ۳۷

چکیده

با گسترش فن آوری‌های مخابراتی و ارتباطی، رمزنگاری و مخفی‌سازی اطلاعات، یکی از ضرورت‌های ارتباطی شده است. در حال حاضر رمزنگاری اطلاعات تنها مختص اطلاعات نظامی و امنیتی نمی‌باشد، بلکه در بسیاری از حوزه‌های دیگر به کار می‌رود. رمزنگاری مدت طولانی است که توسط دولت و نیروهای نظامی به منظور برقراری ارتباط امن و یا بعضا مخفی استفاده می‌شود، اما درحال حاضر به طور معمول و در جهت حفاظت از اطلاعات در انواع مختلفی از سیستم‌های غیر نظامی نیز استفاده می‌شود. بنابراین رمزنگاری، ابزاری مناسب جهت حفاظت اطلاعات در کانال ناامن است. به این منظور، از دو روش رمزنگاری کلید متقارن و رمزنگاری کلید عمومی استفاده می‌شود. در این سمینار به مطالعه الگوریتم رمزنگاری متقارن و نامتقارن پرداخته می شود.

واژه‌های کلیدی: رمزنگاری، متقارن، نامتقارن، امنیت، کلید عمومی، کلید خصوصی.

فصل اول

مقدمه

۱-۱ مقدمه

رمزنگاری دانشی است که به بررسی و شناخت اصول و روش‌های انتقال یا ذخیره اطلاعات به صورت امن (حتی اگر مسیر انتقال اطلاعات و کانال‌های ارتباطی یا محل ذخیره اطلاعات ناامن باشند) می‌پردازد. هنگامی که با امنیت اطلاعات سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات اطلاعات مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند. اغلب این مساله باید تضمین شود که یک پیغام فقط می‌تواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده این مساله باشد "رمزنگاری" نام دارد. رمزنگاری استفاده از تکنیک‌های ریاضی، برای برقراری امنیت اطلاعات است. دراصل رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است، به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی از اطلاعات رمز شده باشد و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد، نتواند به اطلاعات دسترسی پیدا کند. دانش رمزنگاری بر پایه مقدمات بسیاری از قبیل تئوری اطلاعات، نظریه اعداد و آمار بنا شده‌است و امروزه به طور خاص در علم مخابرات مورد بررسی و استفاده قرار می‌گیرد. معادل رمزنگاری در زبان انگلیسی کلمه Cryptography است، که برگرفته از لغات یونانی kryptos به مفهوم «محرمانه» و graphien به معنای «نوشتن» است. بطور کلی هر عملی که امنیت اطلاعات را به مخاطره اندازد تهدید ایمنی اطلاعات نامیده می‌شود. بنابراین همانطور که گفته شد، یکی از روش‌های تامین ایمنی اطلاعات، رمزنگاری است. با رمزنگاری محرمانه ماندن و اعتبار پیغام حفظ می‌گردد. مشکل اصلی در رمزنگاری، ارائه روشی است که تهدید کننده نتواند از متن رمز شده متن اصلی را بدست آورد حتی نتواند با داشتن متن اصلی

مبدل رمزگشایی را پیدا کند. در این خصوص مقدار اطلاعات بدست آمده از متن رمز شده و روش رمزگذاری دارای اهمیت می باشند[1]. رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده‌اند. کلید، یک رشته از ارقام دودویی (صفر و یک)است که بخودی خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند. الگوریتم‌های رمزنگاری داده‌ها به طور کلی به دو دسته تقسیم می‌شوند. دسته اول الگوریتم‌های رمز متقارن[1] و دسته دوم الگوریتم‌های رمز نامتقارن[2] می‌باشند. الگوریتم‌های رمزنگاری با کلید نامتقارن از کلیدهای مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستم‌ها اجازه می‌دهند که یکی از کلیدها کلید عمومی[3] منتشر شود در حالی که دیگری کلید خصوصی[4] توسط صاحبش حفظ می‌شود. فرستنده پیام، متن را با کلید عمومی گیرنده، کد می‌کند و گیرنده آن را با کلید اختصاصی خود رمزگشایی می‌کند. بعبارتی تنها با کلید خصوصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کد شده برای هر گیرنده‌ای، به جز گیرنده مورد نظر فرستنده، بی‌معنی خواهد بود[2].

[1] Symmetric
[2] Asymmetric
[3] public key
[4] private key