عنوان مقاله : رمز نگاري

گروه مطالعاتی : امنیت

گروه کاری : امنیت

ارائه دهنده: افسانه کربلائي زاده

تاریخ ارائه: ۸۳/۱۱/۱۳

سرپرست گروه کاری: طیبه میرزائی

تاریخ اصلاح: ۸۳/۱۱/۱۵

اصلاح کننده : افسانه کربلائي زاده

مرجع: اینترنت

رمزنگاری اطلاعات

رمزنگاری علم کدها و رمزهاست بنابر این روشی مناسب به منظور حفاظت از اطلاعات حساس است. بدین ترتیب ، صرفا" افراد مجاز قادر به دستیابی و استفاده از اطلاعات خواهند بود.
هنگامی که با امنیت دیتا 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 دیتای 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 هنر نوشتن بصورت رمز است بطوریکه هیچکس بغیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.
رمزنگاری مخفف‌ها و اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از دیتای اصلی (*plaintext*)، آنرا با استفاده از یک کلید (رشته‌ای محدود از بیتها) بصورت رمز در می‌آوریم تا کسی که دیتای حاصله را می‌خواند قادر به درک آن نباشد. دیتای رمزشده (*ciphertext*) بصورت یک سری بی‌معنی از بیتها بدون داشتن رابطه مشخصی با دیتای اصلی بنظر می‌رسد. برای حصول متن اولیه دریافت‌کننده آنرا رمزگشایی می‌کند. یک شخص ثالث (یک هکر) می‌تواند برای اینکه بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمزنوشته *(cryptanalysis)* کند. بخاطرداشتن وجود این شخص ثالث بسیار مهم است.
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 بخودی‌خود 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.
دیتای اولیه اغلب قبل از رمزشدن بازچینی می‌شود؛ این عمل عموما بعنوان scrambling شناخته می‌شود. بصورت مشخص‌تر، hash functionها بلوکی از دیتا را (که می‌تواند هر اندازه‌ای داشته باشد) به طول از پیش مشخص‌شده کاهش می‌دهد. البته دیتای اولیه نمی‌تواند از hashed value بازسازی شود. Hash functionها اغلب بعنوان بخشی از

یک سیستم تایید هویت مورد نیاز هستند؛ خلاصه‌ای از پیام (شامل مهم‌ترین قسمتها مانند شماره پیام، تاریخ و ساعت، و نواحی مهم دیتا) قبل از رمزنگاری خود پیام، ساخته و hash می‌شود.
یک چک تایید پیام (Message Authentication Check) یا MAC یک الگوریتم ثابت با تولید یک امضاء برروی پیام با استفاده از یک کلید متقارن است. هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است. هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده می‌شود، منجر به ایجاد امضای دیجیتال (digital signature) می‌شود.

۲ – الگوریتم‌ها

طراحی الگوریتمهای رمزنگاری مقوله‌ای برای متخصصان ریاضی است. طراحان سیستمهایی که در آنها از رمزنگاری استفاده می‌شود، باید از نقاط قوت و ضعف الگوریتمهای موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیمگیری داشته باشند. اگرچه رمزنگاری از اولین کارهای شانون (Shannon) در اواخر دهه ۴۰ و اوایل دهه ۵۰ بشدت پیشرفت کرده است، اما کشف رمز نیز پابه‌پای رمزنگاری به پیش آمده است و الگوریتمهای کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند. بنابراین تعداد الگوریتمهای استفاده شده در سیستمهای کامپیوتری عملی و در سیستمهای برپایه کارت هوشمند بسیار کم است.

۲–۱ سیستمهای کلید متقارن

یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. بیشترین شکل استفاده از رمزنگاری که در کارتهای هوشمند و البته در بیشتر سیستمهای امنیت اطلاعات وجود دارد data encryption algorithm یا DEA است که بیشتر بعنوان DES شناخته می‌شود. DES یک محصول دولت ایالات متحده است که امروزه بطور وسیعی بعنوان یک استاندارد بین‌المللی شناخته می‌شود. بلوکهای ۶۴بیتی دیتا توسط یک کلید تنها که معمولا ۵۶بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. DES از نظر محاسباتی ساده است و براحتی می‌تواند توسط پردازنده‌های کند (بخصوص آنهایی که در کارتهای هوشمند وجود دارند) انجام گیرد.
این روش بستگی به مخفی‌بودن کلید دارد. بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستم مبادله می‌شوند که قبلا هویت یکدیگر را تایید کرده‌اند عمر کلیدها بیشتر از مدت

تراکنش طول نمی‌کشد. رمزنگاری DES عموما برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود.
کلیدهای DES ۴۰بیتی امروزه در عرض چندین ساعت توسط کامپیوترهای معمولی شکسته می‌شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شود. کلید ۵۶بیتی عموما توسط سخت‌افزار یا شبکه‌های بخصوصی شکسته می‌شوند. رمزنگاری DESسه‌تایی عبارتست از کدکردن دیتای اصلی با استفاده از الگوریتم DES که در سه مرتبه انجام می‌گیرد. (دو مرتبه با استفاده از یک کلید به سمت جلو (رمزنگاری) و یک مرتبه به سمت عقب (رمزگشایی) با یک کلید دیگر) مطابق شکل زیر:

این عمل تاثیر دوبرابر کردن طول مؤثر کلید را دارد؛ بعدا خواهیم دید که این یک عامل مهم در قدرت رمزکنندگی است.
الگوریتمهای استاندارد جدیدتر مختلفی پیشنهاد شده‌اند. الگوریتمهایی مانند Blowfish و IDEA برای زمانی مورد استفاده قرار گرفته‌اند اما هیچکدام پیاده‌سازی سخت‌افزاری نشدند بنابراین بعنوان رقیبی برای DES برای استفاده در کاربردهای میکروکنترلی مطرح نبوده‌اند. پروژه استاندارد رمزنگاری پیشرفته دولتی ایالات متحده (AES) الگوریتم Rijndael را برای جایگزیتی DES بعنوان الگوریتم رمزنگاری اولیه انتخاب کرده است. الگوریتم Twofish مشخصا برای پیاده‌سازی در پردازنده‌های توان‌پایین مثلا در کارتهای هوشمند طراحی شد.
در ۱۹۹۸ وزارت دفاع ایالات متحده تصمیم گرفت که الگوریتمها Skipjack و مبادله کلید را که در کارتهای Fortezza استفاده شده بود، از محرمانگی خارج سازد. یکی از دلایل این امر تشویق برای پیاده‌سازی بیشتر کارتهای هوشمند برپایه این الگوریتمها بود.
برای رمزنگاری جریانی (streaming encryption) (که رمزنگاری دیتا در حین ارسال صورت می‌گیرد بجای اینکه دیتای کدشده در یک فایل مجزا قرار گیرد) الگوریتم RC4 سرعت بالا و دامنه‌ای از طول کلیدها از ۴۰ تا ۲۵۶ بیت فراهم می‌کند. RC4 که متعلق به امنیت دیتای RSA است، بصورت عادی برای رمزنگاری ارتباطات دوطرفه امن در اینترنت استفاده می‌شود.

۲-۲ سیستمهای کلید نامتقارن

سیستمهای کلید نامتقارن از کلید مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستمها اجازه می‌دهند که یک جزء (کلید عمومی یا public key) منتشر شود در حالیکه دیگری (کلید اختصاصی یا private key) توسط صاحبش حفظ شود. فرستنده پیام، متن را با کلید عمومی گیرنده کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری میکند. بعبارتی تنها با کلید اختصاصی 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 کدشده برای هرگیرنده‌ای بجز گیرنده مورد نظر فرستنده بی‌معنی خواهد بود. معمولترین سیستم نامتقارن بعنوان RSA شناخته می‌شود (حروف اول پدیدآورندگان آن یعنی Rivest ، Shamir و Adlemen است). اگرچه چندین طرح دیگر وجود دارند. می‌توان از یک سیستم نامتقارن برای نشاندادن اینکه فرستنده پیام همان شخصی است که ادعا می‌کند استفاده کرد که این عمل اصطلاحا امضاء نام دارد. RSA شامل دو تبدیل است که هرکدام احتیاج به بتوان‌رسانی ماجولار با توانهای خیلی طولانی دارد:

- امضاء، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند؛
- رمزگشایی عملیات مشابه‌ای روی متن رمزشده اما با استفاده از کلید عمومی است. برای تایید امضاء بررسی می‌کنیم که آیا این نتیجه با دیتای اولیه یکسان است؛ اگر اینگونه است، امضاء توسط کلید اختصاصی متناظر رمزشده است.

به بیان ساده‌تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمزشده توسط کلید عمومی آن شخص که شما از آن مطلعید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشاندهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می‌شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمزشده نیستند بطوریکه با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود.

اساس سیستم RSA این فرمول است: $X = Y^k \pmod r$

که X متن کد شده، Y متن اصلی، k کلید اختصاصی و r حاصلضرب دو عدد اولیه بزرگ است که با دقت انتخاب شده‌اند. برای اطلاع از جزئیات بیشتر می‌توان به مراجعی که در این زمینه وجود دارد رجوع کرد. این شکل محاسبات روی پردازنده‌های بایتی بخصوص روی ۸ بیتی‌ها که در کارتهای هوشمند استفاده می‌شود بسیار کند است. بنابراین، اگرچه RSA هم تصدیق هویت و هم رمزنگاری را ممکن می‌سازد، در اصل برای تایید هویت منبع پیام از این الگوریتم در کارتهای هوشمند استفاده می‌شود و برای نشاندادن عدم تغییر پیام در طول ارسال و رمزنگاری کلیدهای آتی استفاده می‌شود.

سایر سیستمهای کلید نامتقارن شامل سیستمهای لگاریتم گسسته می‌شوند مانند Diffie-Hellman، ElGamal و سایر طرحهای چندجمله‌ای و منحنی‌های بیضوی. بسیاری از این طرحها عملکردهای یک‌طرفه‌ای دارند که اجازه تاییدهویت را می‌دهند اما رمزنگاری ندارند. یک رقیب جدیدتر الگوریتم RPK است که از یک تولیدکننده مرکب برای تنظیم ترکیبی از کلیدها با مشخصات مورد نیاز استفاده می‌کند. RPK یک پروسه دو مرحله‌ای است: بعد از فاز آماده‌سازی در رمزنگاری و رمزگشایی (برای

یک طرح کلید عمومی) رشته‌هایی از دیتا بطور استثنایی کاراست و می‌تواند براحتی در سخت‌افزارهای رایج پیاده‌سازی شود. بنابراین بخوبی با رمزنگاری و تصدیق‌هویت در ارتباطات سازگار است.
طولهای کلیدها برای این طرحهای جایگزین بسیار کوتاهتر از کلیدهای مورد استفاده در RSA است که آنها برای استفاده در چیپ‌کارتها مناسب‌تر است. اما RSA محکی برای ارزیابی سایر الگوریتمها باقی مانده است؛ حضور و بقای نزدیک به سه‌دهه از این الگوریتم، تضمینی در برابر ضعفهای عمده بشمار می‌رود.

تفاوت رمزنگاری با امضای دیجیتال

در رمزنگاری کلید عمومی همانند امضای دیجیتال از نرم افزاری نظیر PGP به منظور تبدیل اطلاعات با استفاده از الگوریتم های ریاضی استفاده می گردد . رمزنگاری کلید عمومی مبتنی بر کلیدهای خصوصی و عمومی است . علیرغم وجود برخی شباهت ها بین فرآیندهای رمزنگاری و امضای دیجیتال ، در این رابطه تفاوت هائی نیز وجود دارد
هدف رمزنگاری ، محرمانگی است . با ترجمه محتوای پیام به یک کد ، اطلاعات مخفی نگه داشته می شوند. هدف امضای دیجیتال، استحکام و واقعی بودن یک پیام است. بدین منظور بررسی لازم در خصوص فرستنده پیام و عدم تغییر محتوای آن ، انجام می شود . با این که رمزنگاری و امضای دیجیتال می توانند مستقل از هم استفاده شوند ، امکان امضای یک پیام رمز شده نیز وجود دارد
در زمان امضای یک پیام از کلید خصوصی استفاده می گردد و هر فردی که دارای کلید عمومی ارسال کننده پیام است ، قادر به بررسی صحت و اعتبار امضای دیجیتال است. (آشنائی با امضای دیجیتال) . در زمان رمزنگاری یک پیام از کلید عمومی فردی که اطلاعات برای وی ارسال می گردد ، استفاده شده و وی با استفاده از کلید خصوصی خود قادر به رمزگشائی پیام است . با توجه به این که افراد کلید خصوصی را نزد خود محرمانه نگه داشته و از آن با استفاده از رمزهای عبور، حفاظت می نمایند ، دریافت کننده یک پیام رمز شده ، تنها شخصی است که قادر به رمزگشائی و مشاهده پیام خواهد بود