بررسی مباحث کلیدی متداول و رایج و وضعیت رمزنگاری

چکیده:

برنامه های کاربردی اینترنت بسیار سریع در حال رشد و پیشرفت می باشند. با توجه به پیشرفت تکنولوژی، ایمن ترین روش انتقال داده ها در اینترنت، تبدیل شدن به عملکردی پرسشی می باشد. افراد مزاحم داده ها را هک می کنند و از آن ها برای اهداف خود استفاده می نمایند. برای جلوگیری از این اقدامات نامناسب، از رمزنگاری برای تضمین امنیت پیام های مخفی و ایمن استفاده می شود.

1. مقدمه:

حجم داده ها در حال افزایش است و پیچیدگی آن ها نیز در حال رشد می باشد. بیش از 93٪ از تمامی داده ها، دیجیال می باشند. مقدار اطلاعاتی که سالانه وارد دنیای دیجیتال می شوند، حدودا برابر با 988 EB است. دنیای دیجیتال از ابتدای سال 2010 تا پایان سال 2020، تا 50 برابر رشد خواهد داشت. اطلاعات متعددی از منابعی مانند کتاب، کتاب های الکترونیکی، تصاویرف روزنامه ها و مجلات، مطالب تحقیقاتی، اسناد دولتی، پایگاه داده ها، و ... گرداوری شده اند. از اینرو، به امنیت این منابع و برنامه ها نیاز می باشد. امنیت داده ها یکی از عوامل مهم یک سازمان، برای حفظ اطلاعات از رقابت های مختلف سازمانی می باشد. این کار به تضمین حریم خصوصی اطلاعات شخصی کاربران از دسترسی سایر افراد کمک می کند. زمان و انتقال ایمن داده ها همیشه یکی از جنبه های مهم برای تمامی سازمان ها بوده است. امنیت سیستم در دو حالت رده بندی شده است که در شکل زیر نشان داده شده است.

شکل 1

الف: اهداف رمزنگاری:

رمزنگاری چند هدف دارد. این اهداف را می توان به طور همزمان در یک برنامه به دست آورد، و یا تنها به یکی از آن ها دسترسی پیدا کرد. این اهداف عبارتند از:

1. **احراز هویت:** برای اثبات هویت شخصی آن ها.
2. **محرمانه:** این مورد تضمین می دهد که هیچ کس، به جز کسی که رمز را می داند، نمی تواند پیام دریافتی را متوجه شود.
3. **ترکیب داده ها:** دریافت کننده، پیامی دریافت می کند که تغییر نیافته و یا اخطاری از منشاء خود نمی باشد.
4. **انکارناپذیری:** ثابت می کند که، فرستنده این پیام را ارسال کرده است، و پیغام توسط فرد خاصی دریافت شده است، بنابراین، گیرنده نمی تواند ادعا کند که پیغام ارسال نشده است.
5. **کنترل دسترسی:** که فرآیند جلوگیری از استفاده ی غیرمجاز از منابع می باشد.

ب: الگوی کلی و مفاهیم بنیادی:

رمز: زمینه ی مربوط به رمزگذاری و رمزگشایی که با این نام شناخته می شود.

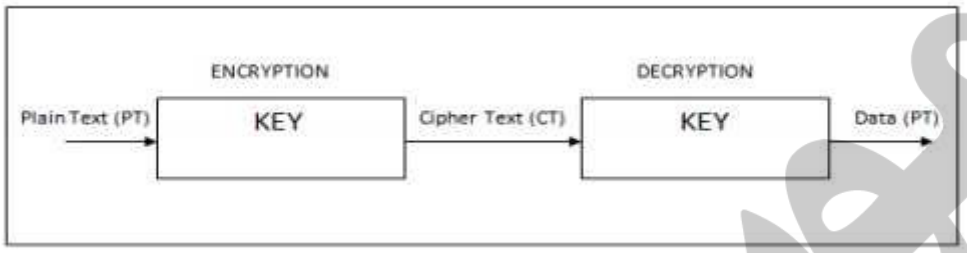
رمزگذاری: این مورد، انتقال داده های خواندنی و قابل درک به حالت دیگری است که نمی توان برای امنیت داده ها آن ها را درک کرد.

رمزگشا: فردی است که متخصص تجزیه و تحلیل و شکستن کدها می باشد.

2. بررسی آثار:

الف: معیارهای عملکردی:

معیارها و ضوابط عملکردی برای تحقیقات سرّی، امنیت و زمان می باشند. این الگوریتم ها باید موارد مربوط به فاش کردن و یا پنهان نمودن فایل های چند رسانه ای ورودی (متن و یا سایر موارد) را اجرا کنند. به همین دلیل، برخی از پارامترها و مقیاس ها را باید در نظر گرفت. این موارد عبارتند از: محاسبه ی زمان رمزگشایی، رمزگذاری، رمزگشایی کلید امنیتی، و اندازه ی آن.



شکل 2

نوع داده ها: نوع داده ها، رمزگذاری فایل ها را نشان می دهد و دارای انواع متعددی از این فایل ها می باشد.

اندازه ی داده ها: فضایی که توسط فایل موجود در دیسک اشغال شده است. فایل های صوتی و یا ویدیویی به صورت کلی، فضای بیشتری را نسبت به فایل های متنی در دیسک اشغال می نمایند.

حجم داده ها: مقدار اطلاعات مختلف ارائه شده در داده ها می باشد.

زمان رمزگذاری: زمان مورد نیاز برای پنهان کردن داده ها از متون ساده به متون رمزدار.

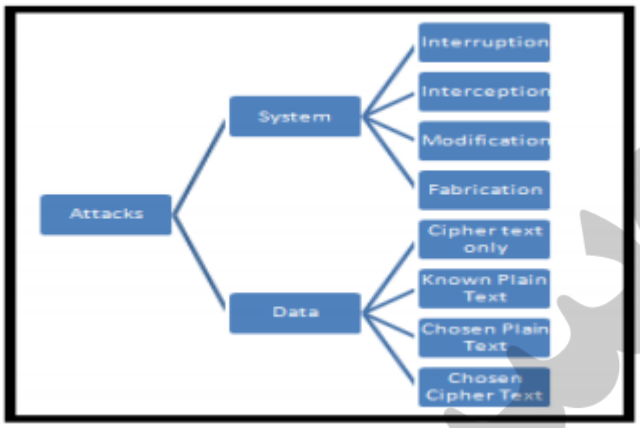
زمان رمزگشایی: زمان مورد نیاز برای برداشتن رمز داده ها.

ب: حملات رمزنگاری:

اساسا، دو نوع حمله وجود دارد. یکی از این حملات در سیستم رخ می دهد و دیگری، در داده های نشان داده شده در شکل 3 به وقوع می پیوندند.

حمله ی سیستمی: به طور کلی، جریان اطلاعاتی از یک منبع به یک مقصد وجود دارد. این حمله ممکن است در جریان اطلاعاتی رخ دهد که به عنوان حمله ی سیستمی شناخته می شوند.

حمله ی داده ها: اقدامات انجام شده در تجزیه و تحلیل داده ها و اطلاعاتبه عنوان حمله شناخته می شوند. سطح اطلاعاتی که رمزگذار می تواند از سیستم رمزگذاری استخراج کند، به 5 تقسیم گردیده اند که عبارتند از: حمله به متون رمزی، حمله به متون شناخته شده، حمله به متون منتخب.



شکل 3

3. انواع رمزگذاری:

اساسا، رمزگذاری به دو مکانیسم الف)رمزگذاری متقارن، و ب) رمزگذاری نامتقارن، تقسیم می گردد.

الف: رمزگذاری متقارن:

تنها از یک کلید برای رمزگذاری و یا رمزگشایی پیام استفاده می شود.

ب: رمزگذاری نامتقارن:

دو کلید وجود دارند که از ان ها برای رمزگذاری، و رمزگشایی استفاده می گردد.

4. مشاهدات:

مشاهدات زیر از بخش های قبل به دست آمده اند:

1) کلید کوتاه نمی تواند الگوی تضمینی را برای رمزگذاری ارائه دهد، و کلید بلند قادر به انجام این کار می باشد.
2) کلیدهای نامتقارن در سطوح امنیتی بالا اولویت دارند و مورد استفاده قرار می گیرند.
3) باید کلید مناسبی وجود داشته باشد تا به الگوی رمزگذاری ایمنی دست پیدا کنیم.

5. اهداف آتی:

امنیت الگوریتم های رمزی براساس مدل رمزهای مربوطه متفاوت می باشد. این موارد متعدد، برای برنامه های کاربردی مختلفی به کار می روند. سطح امنیت ممکن است براساس انواع برنامه ها متفاوت باشد.

Symmetric Algorithms	Rounds	Key Size	Block Modes
RC2	18	40 and 64-bit keys	ECB, CBC, CFB, OFB, CTR
RC4	256	1 to 256-bit keys	Stream Cipher
RC5	256	0 to 2040-bit keys	ECB, CBC, CFB, OFB, CTR
RC6	14	192, 256-bit keys	CBC, ECB, CFB, OFB, CTR
Blowfish	16	32 to 448-bit keys	ECB, CBC, CFB, OFB, CTR

جدول1

6. نتیجه گیری:

در این مقاله، مباحث انجام شده برای برخی از مفاهیم اولیه ی مربوط به رمزگذاری، معیارهای عملکردی، و برخی از پارامترهای مهمی ارائه شده اند که، در رمزگذاری مورد استفاده قرار می گیرند. در میان برخی از موارد ارائه شده، نکات مهمی وجود دارد که، در سیستم های رمزگذاری، مانند انتخاب کلید برای امنیت و رمزگذاری، فرآیند رمزگشایی به نسبت کمتر مورد بررسی قرار گرفته است. از اینرو، این مقاله ی تحقیقاتی بر چنین موضوعاتی توجه دارد. انواع رمزگذاری های متقارن و نامتقارن به طور خلاصه بیان شده اند. تمامی این موارد انواع روش های مختلف برای ایمن سازی سیستم جهت دستیابی به سطح بالایی از امنیت می باشند. برخی از انواع حملات نیز، مورد بحث قرار گرفته اند. بنابراین، انتخاب الگوریتم رمزگذاری مناسب، در سیستم های امنیتی بدست می آیند که، ممکن است حملات متعددی را سرکوب نمایند.