

رمزنگاری Cryptography

رامین غرباء

Ramin_electro@yahoo.com

دانشگاه صنعتی مالک اشتر - دانشکده برق

امید مهدی نژاد

Omid_electro@yahoo.com

دانشگاه صنعتی مالک اشتر - دانشکده برق

چکیده :

هنر رمزنگاری از قدیم الایام مورد علاقه انسان بوده است . با پیشرفتهای علمی در قرن بیستم و توسعه و ساخت وسایل الکترونیکی پیچیده و سریع العمل ، هنر رمز نگاری به صورت علم رمز نگاری در آمده است و این علم دربر گیرنده زمینه های مختلف علمی مانند تئوری اطلاعات ، تئوری اعداد ، آمار، الکترونیک و می باشد . علم رمز نگاری در طی جنگها میان ملل مختلف عامل مهمی در پیروزی برخی از این ملل بوده است .

واژگان کلیدی : رمزنگاری ، سیستم ورنام ، آلگاریتم ، رمزگشایی ، سیستم جانشینی

۱- مقدمه

ارتباطات نظامی و سیاسی ایجاب می کرد که پیام فقط برای فرد یا افراد خاصی قابل فهم باشد و سایرین نتوانند اطلاعاتی از آن بدست آورند . به موازات تکامل این هنر عده ای کنجکاو و یا « دشمن » تلاش می نمودند از پیام رمز شده به محتوای اصلی آن دست یابند .

سازندگان رمز (code makers) و شکنندگان رمز (code breakers) همواره در کنار هم به تلاش خود ادامه دادند و در حقیقت دو روی یک سکه بوده اند . امروزه علاوه بر کاربردهای نظامی و سیاسی ، علم رمز نگاری در تجارت ، ارتباطات کامپیوتری ، ارتباطات خصوصی و..... نیز بکار می رود و حتی در بعضی از آنها نقش اساسی ایفا می کند .

اگر چه پیک خصوصی و یا پست سفارشی را می توان به عنوان وسایل امنی برای ارتباطات قلمداد نمود لیکن سرعت عمل ، عامل مهمی در ارتباطات است و در کاربردهای نظامی و مانند آن نیز بعضاً امکان استفاده از وسایل

رسمی مانند پست و پیک خصوصی میسر نیست و به همین دلیل علم رمز نگاری در این گونه موارد نقش خود را هویدا می کند .

۲- تکامل رمز نگاری (Development Cryptography)

به طور کلی روند تکامل رمز نگاری را می توان به چهار مرحله زیر تقسیم نمود :

مرحله اول: که از سیستمهای ساده جانشینی و جابجایی برای رمز نگاری استفاده می شد. در این مرحله بیشتر قلم و کاغذ و ماشینهای ساده مکانیکی مورد استفاده قرار می گرفتند (مانند سیستم سزار و اسپارتان) .

مرحله دوم: که از آغاز قرن بیستم شروع و تا دهه ۱۹۵۰ ادامه می یابد . در این مرحله از وسایل پیچیده مکانیکی و الکترومکانیکی استفاده شده و به تبع آن سیستمهای رمز نگاری پیچیده تری ابداع گردید. (مانند سیستم M 209 و یا ماشین Hagelin) .

مرحله سوم : که با انتشار مقالات بسیار مهم شانون در سالهای ۱۹۴۸ و ۱۹۴۹ و پیشرفت سریع در صنایع میکرو الکترونیک در دهه ۱۹۶۰ شروع می شود و هنر رمز نگاری به علم رمز نگاری مبدل می گردد.

مرحله چهارم : که از اواخر دهه ۱۹۷۰ با پیشنهاد سیستمهای رمز نگاری با کلید همگانی شروع می شود . [1]

۳- تعاریف اساسی (Basic Definitions)

رمز نگاری (cryptography) : علم و مطالعه روشهای مختلف نوشتن سرّی و مبادله اطلاعات امن را رمز نگاری گویند .

رمز کردن (cipher) : روش سرّی نوشتن .

متن اصلی (clear text) : پیام یا متننی که باید پس از رمز شدن برای گیرنده خاصی ارسال شود .

متن رمز شده (cipher text = cryptogram) : متن رمز شده که توسط یک کانال ناامن ارسال می شود . فرایند تبدیل متن اصلی به متن رمز شده را رمز گذاری (encryption = encipherment) نامند .

آلگاریتم (Algorithm) : روشی را که رمز کننده برای رمز کردن متن اصلی به کار می برد آلگاریتم نامیده می شود .

کلید (Key) : آلگاریتم عموماً متکی به یک کلید است که باید برای دریافت کننده متن رمز شده معلوم باشد و سایرین از آن اطلاعی نداشته باشند . گیرنده با استفاده از کلید متن اصلی را از متن رمز شده استخراج می نماید . عمل استخراج متن اصلی از متن رمز شده را رمز گشایی (Deciphering) گویند .

کد (Code) : نحوه ارسالی است که به کلید خاصی بستگی ندارد و فقط به Code book وابسته است ، یعنی فقط یک کلید دارد . بنابر این کد را فقط به صورت سیستمی که به کلید وابسته نیست تعریف می کنیم .

دشمن (Cryptanalyst) : کسی که حق فهمیدن پیام را ندارد اما در جستجوی آن است .

شکستن رمز (cryptanalysis) : دانش و مطالعه روشهای مختلف بدست آوردن پیام توسط دشمن را گویند .

Cryptology : دانش رمز نگاری (cryptography) و رمز شکنی را (cryptanalysis) را کلاً Cryptology نامند .

سیستم قابل شکست (Breakable) : سیستم را قابل شکست گوئیم هر گاه امکان دست یابی به کلید از روی

متن رمز شده و یا از روی متن رمز شده و متن اصلی باشد . [1]

۴- امنیت یک سیستم (Security of System)

به طور کلی دو نوع امنیت برای سیستمهای رمز نگاری تعریف می شود :

الف- امنیت بدون شرط : در صورتیکه علیرغم توان زیاد محاسباتی دشمن ، نتواند بر اساس متن رمز شده سیستم را بشکند سیستم را امن بدون شرط نامند .

ب - امنیت محاسباتی : در صورتی که شکستن سیستم رمز عملاً و از نظر محاسباتی پیچیده و طولانی باشد سیستم را به مفهوم محاسباتی امن می گوئیم .

تنها سیستم بدون شرط امن شناخته شده تاکنون سیستم " ورنام " (Vername) یا سیستم " One time pad " است که در آن متن اصلی با کلید کاملاً تصادفی با طول مساوی طول متن اصلی ترکیب می شود . در این روش متن اصلی با یک دنباله باینری به طول m نمایش داده می شود که این دنباله با دنباله کاملاً تصادفی باینری به طول n (کلید) XOR می شود . این کلید فقط برای یک بار مورد استفاده قرار می گیرد . در این سیستم دشمن با 2^n متن که یکی از آنها متن اصلی است روبه روست که این 2^n متن هیچ گونه اطلاعاتی در مورد متن اصلی به دشمن نمی دهد .

بدیهی است هر چه طول متن رمز شده در اختیار دشمن بیشتر باشد در حال کلی اطلاعات بیشتری در مورد شکستن سیستم در دست دشمن خواهد بود . حداقل طول متنی را که اگر در اختیار دشمن باشد سیستم شکسته می شود . فاصله قابل شکست (unicity Distance) گویند که اولین بار توسط شانون بکار گرفته شد . این مقدار برای سیستم " One time pad " برابر با ∞ است ($N_0 = \infty$) . [1]

۵- معیارهای پنج گانه ارزیابی شانون

معیارهای پنجگانه زیر برای ارزیابی یک سیستم توسط شانون در دهه ۱۹۴۰ پیشنهاد شد که علی رقم گذشت حدود نیم قرن از زمان پیشنهاد آنها هنوز کارایی خود را از دست نداده اند .

۵-۱- میزان ایمنی سیستم:

امنیت بعضی از سیستمها کامل است ($N_0 = \infty$) و دشمن نمی تواند به هیچ صورتی آنها را بشکند . بعضی از سیستمها به دشمن اطلاعاتی می دهد که ممکن است این اطلاعات به " جواب یکتایی " منجر شود و در مورد آنها نیز که منجر به جواب یکتا خواهند شد پیچیدگی محاسبات و زمان لازم برای شکستن از اهمیت خاصی برخوردار است .

۵-۲- اندازه کلید :

کلید باید به طریق مطمئن و غیر قابل دسترس دشمن در اختیار گیرنده قرار گیرد . (مثلاً در مواردی لازم است کلید بخاطر سپرده شود) بنابراین داشتن کلیدی حتی الامکان کوچک و ساده مطلوب است .

۵-۳- پیچیدگی عملیات رمز گذاری و رمز گشایی :

عملیات رمز گذاری و رمز گشایی باید حتی الامکان ساده باشد و در زمان کوتاه و با هزینه کم انجام پذیرد .

۵-۴- انتشار خطا :

ممکن است که ارتکاب یک خطا در رمز کردن یا ارسال پیام رمز شده باعث ایجاد خطاهای زیادی در موقع گشودن رمز شود و به دنبال آن باعث از دست رفتن مقدار زیادی اطلاعات گردد. بنابراین باید حتی الامکان از انتشار خطا در سیستم جلوگیری نمود .

۵-۵- بسط یا گسترش پیام :

در پاره ای از سیستمها اندازه پیام بعد از عمل رمز کردن بیشتر می شود . مثلاً در سیستمهایی مایل به از میان بردن

"فرکانس طبیعی سمبلها" هستیم که ممکن است از سمبلهای خنثی و یا تکرار سمبلهای جانشین شده استفاده شود و این امر برای سیستمهای مخابراتی مطلوب نیست پس باید حتی الامکان از گسترش پیام جلوگیری نمود . [1] , [5]

۶- امضاء دیجیتال

از مسائل مهم در ارتباطات رمز نگاری اعتبار اطلاعات دریافتی است بگونه ای که :

اولاً: گیرنده مطمئن باشد که پیغام از منبع فرستنده است .

ثانیاً: امکان تغییر پیام توسط گیرنده یا دیگری نباشد .

ثالثاً: فرستنده نیز بعداً نتواند ارسال پیام را انکار کند .

حال فرض کنید که منبع A بخواهد پیام امضاء شده M را برای منبع B ارسال نماید در این صورت شرایط زیر باید برقرار باشد :

الف) B می باید مطمئن باشد که پیغام متعلق به A است یعنی قادر به تأیید صحت امضاء A باشد .

ب) جعل امضای A برای هر فرد و از جمله خود B باید غیر ممکن باشد . یعنی هیچ منبع دیگری نتواند پیامی را به نام منبع A برای B ارسال کند و حتی B هم نتواند پیامی غیر از M را بعنوان پیامی از جانب A ارائه دهد .

ج) منبع A نباید قادر به انکار ارسال پیام باشد . و باید هر مرجعی با بررسی پیام دریافتی بتواند براحتی منبع ارسال آن یعنی A را مشخص کند .

می توان اثبات نمود که سیستمهای با کلید همگانی را می توان به راحتی برای امضای دیجیتال پیام مورد استفاده قرار داد . در حقیقت کلید خصوصی D_A نقش امضاء را به عهده خواهد گرفت . منبع A پیام M را با

کلید خصوصی D_A رمز کرده و برای B ارسال می نماید. متن رمز شده $C = D_A(M)$ توسط B دریافت شده و B با استفاده از کلید همگانی A یعنی E_A اعتبار پیام و تعلق آن به A را کشف و پیام را دریافت می کند .

بنابر این $D_A(M)$ پیام امضاء شده A است و $E_A(C) = E_A(D_A(M)) = M$ توسط B کشف می شود . در صورت بروز اختلاف بین A , B مرجع سوم می تواند ادعای B مبنی بر ارسال پیام توسط A را با بررسی متن

کد شده یعنی $D_A(M)$ بررسی کند . در حقیقت چون $E_A(C) = M$ و هیچ منبعی جز A اطلاع از کلید D_A ندارد بنابراین پیام M متعلق به A میباشد . و A نمی تواند ارسال آن را انکار کند .

البته هرکل (Herkle) روشی را برای امضاء در سیستمهای کلاسیک مطرح نمود ولی در اینجا یک منبع سوم مورد اعتماد برای A , B لازم است که این منبع باید کلیدهای رمز گشایی و رمز گذاری A , B را بداند .

فرض کنید منبع O مورد اعتماد است و کلید محرمانه D_A , E_A را می داند . برای ارسال پیام امضاء شده M از سوی A برای B ، منبع A پیام رمز شده $C = D_A(M)$ را ارسال می نماید . برای بررسی اعتبار پیام ، B ، پیام

رمز شده C را برای B می فرستد و S صحت آن را با محاسبه $E_A(C) = M$ مشخص کرده و پیام M را با استفاده از کلید محرمانه B می فرستد و B پیام M را رمز گشایی می کند. [2]

۷- تئوری کدینگ (Coding Theory)

بطور کلی کدینگ در سیستمهای مخابراتی به دلایل متفاوتی به کار می رود. در اینجا به لحاظ اینکه معمولاً در سیستمهای رمزنگاری برای تبدیل یک منبع اطلاعات پیوسته به یک منبع اطلاعات گسسته از کد کننده های منبع استفاده می شود. مختصری در این زمینه توضیح خواهیم داد.

کد کننده منبع (Source Encoder) خروجی منبع را به دنباله ای از رقمهای باینری تبدیل می کند. در کد کننده منبع باید به این دو نکته اساسی توجه شود که اولاً تعداد ارقام مورد نیاز (بیت) بر واحد زمان که برای نمایش خروجی منبع لازم است حداقل باشد و ثانیاً بازسازی خروجی منبع توسط دنباله باینری بدون ابهام امکان پذیر باشد.

البته نوع دیگری از کد کننده موسوم به کد کننده کانال (Chanel Encoder) نیز وجود دارد که در آن دنباله خروجی منبع را به یک دنباله دیگر کد مناسب برای ارسال روی کانال است (غالباً باینری) تبدیل می کند. عملیات کنترل خطا (تشخیص یا تصحیح خطا) در اینجا صورت می پذیرد. [2]

۸- تئوری اطلاعات (Information Theory)

شانون در سال ۱۹۴۹ تئوری رمز نگاری را بر اساس تئوری اطلاعات بیان کرده است. وی امنیت سیستم رمزنگاری را با محاسبات ابهام موجود در متن اصلی پس دریافت متن رمز شده اندازه گیری می کند. شانون سیستم را با امنیت کامل تعریف کرده است. هر گاه متن رمز شده (مستقل از مقدار متن) هیچ گونه اطلاعاتی از مقدار متن اصلی ندهد. در حال کلی با افزایش طول متن رمز شده اطلاعات بیشتری در مورد متن اصلی پیدا می شود. و امکان شکستن رمز بیشتری می گردد (سیستمهای غیر کامل) به این ترتیب اغلب سیستمهای رمز نگاری قابل شکست است (از نظر تئوری) ولی در پاره ای از موارد برای شکستن سیستم به چند صد رقم متن رمز شده نیاز است و اگر چه سیستم از نظر تئوری قابل شکستن است ولی از نظر زمانی با زمان غیر قابل قبولی روبرو خواهیم بود که در این موارد سیستمها از نظر محاسباتی غیر قابل شکست نامیده می شود. [2]

۹- سیستمهای رمز نگاری کلاسیک

بطور کلی سیستمهای رمز نگاری به دو دسته بزرگ قابل تقسیم اند:

۱- سیستمهای جانشینی (Substitution Systems)

۲- سیستمهای جابجایی (Transportation Systems)

و خود سیستمهای جانشینی نیز به دو دسته اند :

الف : سیستمهای جانشینی ساده و تک حرفی

ب : سیستمهای جانشینی چند حرفی

هر یک از سه نوع سیستم فوق را جداگانه بررسی خواهیم کرد.

۹-۱- سیستمهای جانشینی ساده و تک حرفی:

یکی از اولین سیستمهای رمز نگاری سیستمی است که توسط جولیس سزار بکار رفته و به نام خود او یعنی به سیستم رمز نگاری سزار معروف است. در این سیستم به جای هر حرف حرفی که به فاصله سه حرف بعد از آن قرار دارد انتخاب و ارسال می شود و دریافت کننده پیام برای رمز گشایی به جای هر حرف دریافتی حرفی را که سه حرف قبل از آن است انتخاب می کند.

به عنوان مثال فرض کنید که بخواهیم کلمه cryptography را به روش سزار رمز کرده و ارسال کنیم. در سیستم سزار الفبای متن اصلی و متن رمز شده به صورت زیر است.

Plain : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

بنابر این کلمه مورد نظر بصورت زیر رمز می شود:

Plain : C R Y P T O G R A P H Y
Cipher : F U B S W R J U D S K B

سیستمهای فوق مبنای پیدایش سیستمهای جانشینی است که اکنون به بررسی آن می پردازیم.

۹-۱-۱- سیستمهای جانشینی ساده:

سیستمی است که در آن هر حرف با یک حرف دیگر عوض می شود. و این تبدیل یک رابطه یک به یک خواهد بود یعنی با معلوم بودن هر حرف متن اصلی، حرف متناظر متن رمز شده معلوم و بالعکس با معلوم بودن حرف متن رمز شده حرف متن اصلی متناظر با آن معلوم خواهد بود. در حقیقت کلید این سیستم الگاریتم تبدیل است:

$$f : m \rightarrow c, \quad f(P) = c \leftrightarrow f^{-1}(c) = P$$

در حقیقت در این روش فضایی c فضای جابجایی شده m است و f یک نگاشت یک به یک از هر حرف m به حرف متناظر آن در c است.

۹-۱-۲- سیستمهای جانشینی چند حرفی

روشهای رمز نگاری که تا به حال مورد بحث قرار گرفت علیرغم پیچیدگی احتمالی آنها همواره به صورت تک حرفی روی حروف متن اصلی عمل می کرد. برای از بین بردن خواص آماری حروف متن اصلی و نقاط مشخصه آن از سیستمهای جانشینی چند حرفی استفاده می کنیم. در این سیستمها هر n حرف از متن اصلی به عنوان یک واحد در نظر گرفته شده و به طور یک جا و با یک تبدیل به n سمبل از متن رمز شده تبدیل می شود. اگر $n = 2$ باشد سیستم را دو حرفی (Diagraphic) گویند. [2],[3],[4]

۹-۲- سیستمهای جابجایی

در این روش رمز نگاری بر خلاف سیستمهای جانشینی هیچ حرفی تغییر شکل نمی دهد و فقط محل قرار گرفتن آن در متن رمز شده نسبت به متن اصلی تغییر می کند. در حقیقت ابتدا تعدادی از حروف متن اصلی انتخاب شده (d حرف) و سپس یک جایگشتی بین این d حرف صورت می پذیرد. d را می توان دوره تناوب سیستم نامگذاری کرد. [2]

۱۰- نتیجه گیری

امروزه فناوری رمزنگاری یکی از اساسی ترین علوم بوده که در کشورهای توسعه یافته مورد استفاده قرار می گیرد و همواره سیر تکاملی خود را طی می کند . با توسعه روزافزون علم الکترونیک و مخابرات انتظار می رود که رمزنگاری به عنوان یکی از زیر شاخه های این علوم نقشی اساسی را در امنیت کشورها ایفا نماید . با توجه هر چه بیشتر به این علم و وجود استعداد های فکری در میهن عزیزمان امید است کشور ما نیز بتواند در این زمینه پیشرفت داشته باشد .

۱۱- مراجع

- [1] « Cipher systems »
By : H.beker & F.piper _ Northwood Books , 1982
- [2] « Cryptography and Data Security »
By : D.Robling Denning – Addison – wesley , 1982
- [3] « Elementary Cryptanalysis , A Mathematical Approach »
By : A.sinkov – Random house , 1968
- [4] « Cryptography A primer »
By : A.Konheim – John Wiley & sons , 1981
- [5] « Comunication Theory of secrecy systems »
By : Shannon , BSTJ , Vol 28 , PP: 656-715 , Oct . 1947