www.Prozhe.com

گروه کامپیوتر

کارشناسی فناوری اطلاعات

عنوان پایان نامه

رمزنگاری در ارتباطات داده

استاد راهنما

مهندس خسرو سلمانی

نگارش

حمیده داوری فر

خرداد 1392

www.Prozhe.com

www.Prozhe.com

سپاسگزاری

از استاد راهنما، مهندس خسرو سلمانی که در طول انجام این

پایان نامه مرا راهنمایی و یاری کردند کمال تشکر و سپاسگزاری را دارم.

www.Prozhe.com

چکیده

شبکه های کامپیوتری از دیدگاه اجتماعی یک پدیده ی فرهنگی و از دید مهندسی کامپیوتر یک تخصص وعلم به شمـــــار می رود .در جهان امـروز توسعـه و پیشرفـت دانش به توسعه و گسـترش شبـــکه های کامپیوتری وارتباطات وابسته شده است.

هدف اصـلـی در فناوری اطلاعات تولیـــد دانش جدیـد از دانش های گردآوری شده می باشد ومنظـــور از این دانش مفاهـیم نظـری نمی باشند بلکه کلیـه ی آگا هی ها و دانش هایی می باشد که از طریـق آن ها می توان دانشی جدید پدید آورد.

موضـوع مورد تحقـــیق در این مقـاله امنیـــت در ارتباطـات داده می باشد و روش و شیـوه های متفاوتی از آن توضیح داده شده است از جملـــه این روش ها رمزنـگاری داده ها در برقـراری ارتباطات داده می باشد.

اهمیت رمزنگاری در حفظ برقراری امنـیت روز به روز در حال توسعه و گسـتـــرش می باشد و همگـــان در این زمینه را بر آن داشته تا به دنبال روش ها وشیوه های جدید باشند تا از نفوذ بد اندیـشان و مجـرمین اینـترنتی به اطلاعات دیگران و سو استفاده از این اطلاعات را جلوگیـری کنند.

بررسی الگوریتم های رمزنگاری محدودیت هایی دارد از آن جمله که بایستی پیاده سازی شود و اگر سعـــی در شکستـن این الگوریتـم ها وجود داشتـه باشد و هدف متخصص حمـله به این الگوریتم ها باشد بایستـی امکان آن فراهم باشد .

مثلاً برای شکستـن الگوریتم DES حدود چهارده هزار رایانه به کار گرفتـه شد تا این الگوریتم شکسته شود.

چارچـوب نظری این مقـاله مطالعه و و تحقیق در زمینه ی رمزنگاری ،الگوریتـم های کشف شده ی آن و نقاط ضعف این الگوریتم ها می باشد .

الگوریتم های زیـادی در زمینـه ی رمزنگاری کشف شده است که هـر کدام به نوبه ی خود و در زمان خودشان از محبوبیت بسیاری برخودار بودند ولی به محض شکسته شدن و حملـه به آن ها شهرت خود را از دست دادند تا جاییکه سعی در پدیدآوردن الگوریتم های جدیدی در این زمینه میشد.

با پیشرفـت شبکـه های کامپیوتری و فناوری اطلاعـات، رمزنگاری نیز در حال توسعـــه و پیشرفـت می باشد و ممکـــن است زمانـــی الگوریتـم هایی کشف شود که تا مدت ها و یا قرن ها دوام بیـاورد و به راحتـی شکستـه نشود.برای مثال متخصصان به دنبال این هستند که کلمه ی عبور در رایانه ها به فکر عبور تغییر کنند یک هکر نمی تواند امواج مغز شما را هـک کند و وقـــتی شما از طریق امواج مغزتان وارد حساب کاربـــری یا هر گـــونه اطلاعـات شخصی می شوید یک هکر نمی تواند به هیچ طریقی امواج مغز شما را هـــک کند و به اصطـلاح فکر شما را بدزدد و به اطلاعات محرمانه ی شما دست یابد.

www.Prozhe.com

فهرست مطالب

بخش اول : مقدمه

مقدمه 1

فصل اول : مفاهیم اصلی در ارتباطات داده..... 2

1-1 : ارتباط داده 2

1-2 : انتقال داده 2

1-3 : اینترنت 4

1-4 : ارتباطات داده و نظام اقتصادی 5

1-5 : Data communication concepts 7

1-6 : مدهای انتقال داده 9

1-7 : VPN 9

1-8 : Firewall 12

1-8-1 : عملکرد کلی و مشکلات استفاده از یک دیوارآتش 13

1-8-2 : اجزای جانبی یک دیوار آتش 13

1-9 : تفاوت بین فایروال های سخت افزاری و نرم افزاری..... 15

فصل دوم : امنیت در ارتباطات داده 18

2-1 : امنیت شبکه 19

فصل سوم : تاریخچه ی رمزنگاری 23

www.Prozhe.com

3-1 : نمونه هایی از روش های رمزنگاری در تاریخ.....23

3-2 : رمزنگاری در کشورها 25

3-2-1 : مخابره بوسیله ی پرچم.....25

3-3 : رمزنگاری داده 26

3-4 : رمزنگاری پیشرفته 27

3-5 : رمزنگاری سخت افزاری.....29

3-5-1 : اصول ششگانه ی کرکهف 30

3-6 : ارتباط رمزنگاری با داده کاوی 31

3-6-1 : پروژه ECHELON 31

3-6-2 : پروژهPRISM 31

3-7 : تفاوت شنود و داده کاوی 31

3-8 : Steganography.....33

3-8-1 : تفاوت رمزنگاری با نهان نگاری 33

بخش دوم : کارهای مرتبط

فصل چهارم : الگوریتم های سنتی رمزنگاری.....34

4-1 : الگوریتم ها.....34

4-2 : روش های جانشینی 35

4-2-1 : نقاط ضعف روش های جانشینی 36

4-3 : روش های جایگشتی.....37

www.Prozhe.com

4-3-1 : مثال از روش های جایگشتی.....38

4-3-2 : نقاط ضعف روش های جایگشتی 39

4-4 : توابع بدون کلید 40

4-4-1 : hash.....41

4-4-2 : موارد استفاده از Hash 42

4-4-3 : انواع Hash 43

4-4-3-1 : MD5 43

4-4-3-2 : پیاده سازی الگوریتم MD5 45

4-4-3-3 : نمونه کدهای الگوریتم MD5 45

4-5 : توابع مبتنی بر کلید.....47

بخش سوم : متن تحقیق

فصل پنجم : الگوریتم های متقارن در رمزنگاری 48

5-1 : الگوریتم های متقارن 48

5-1-1 : رمزهای دنباله ای و قطعه ای 49

5-1-2 : شرح الگوریتم های رمزنگاری متقارن 49

5-1-2-1 : رمزگذاری DES 52

5-1-2-2 : پیاده سازی الگوریتم DES در C#.Net.....55

5-1-2-3 : ECB(Electronic code book).....57

5-1-2-4 : استاندارد پیشرفته ی رمزنگاری(AES).....59

www.Prozhe.com

5-1-2-5 : پیاده سازی الگوریتمAES 60

فصل ششم : الگوریتم های نامتقارن در رمزنگاری 62

6-1 : الگوریتم های نامتقارن..... 62

6-1-1 : الگوریتم های رمزنگاری نامتقارن..... 62

6-2 : شیوه ی رمزگذاری کلید خصوصی 63

6-3 : مقایسه ی الگوریتم های رمزنگاری متقارن و نامتقارن..... 65

6-4 :RSAروشی جهت پیاده سازی رمزگذاری کلید عمومی..... 66

6-4-1 : موارد استفاده از الگوریتمRSA..... 73

فصل هفتم : انواع پروتکل های رمزنگاری 75

7-1 : پروتکل تبادل کلـید دیفـی،هلمن..... 75

7-2 : SSL..... 76

بخش چهارم : نتیجه گیری

فصل هشتم : آینده ی ارتباطات داده و رمزنگاری..... 77

8-1 : نتیجه گیری از مباحث 77

8-2 : رمزنگاری کوانتوم-آینده ی رمزنگاری 79

REFRENCES 81

پیوست..... 83

www.Prozhe.com

بخش اول مقدمه

نوآوری در شاخـه های مختـلف علم کم نبوده و نیست و بیش تر این نوآوری ها در صـــدد بهبودسطح زندگی و راحت تر کردن زندگـــی انسان هـــا می باشد .در این مقالـــه سعی بر آن است که یکی از این نوآوری ها که در صـدد آسان کردن زندگی انسان ها می باشد شـــرح داده شود. امنیت هدفی است که همواره در زندگی بشر از اهمیـت فراوانی برخودار است و این مقوله امنیت جانی،مالی و... را شامل می شود .این مقالـــه امنیت داده هـا کـــه امـــروزه راحـت بودن زندگـــی بشریت به آن وابسته است را تشریـح می کند و از موارد حفـــظ برقـــراری امنیـت در اطلاعات شخصی و داده ها می توان به اصول رمزنگاری در شبکـــه های کامپیوتری،اینترنت و... اشاره کرد. این مقاله در مورد تاریخچه ی رمزنگـاری و اینکه این مبحث مهـم از کـــی و به چه شیوه هایی در زندگی انسان ها وجود داشته و تاثیری که این مبحـث در برقـــراری امنیت داده ها دارد را تشریح می کند. رمزنگاری چه در گذشتـه و چه در حال و چه در آیـــنده از مباحـث مهـــم و ویـــژه در امنیت داده ها و امنیت در ارتباطـــات داده میـباشد و مبحـثی می باشد که متخصصان در این زمیـــنه بایستـــی روز به روز همگام با پیشرفت علـوم کامپیوتری و همگام با پیشرفـــت فنـاوری در صدد بهبود الگوریتم هـــای آن بکوشـند. در این مقاله روش های سنتی رمزنگـاری، الگوریتـــم هـــای کنونـی رمزنگـــاری اعـــم از متقـــارن و الگوریتم های رمزنگاری نامتقارن تشریح شده است . هـمچنیـن نقـاط ضعـف هرکدام از این روش هـــا و اینکـــه جهت بهبود هرالگوریتم و هر روش چه تدابیری اندیشیده شده است نیز بیان شده است. هـــم چنین تفاوت الگوریتـم هـای رمزنگاری و اینکـه هر کـــدام در چه زمیـنه هـــایی کاربـرد بیش تر و بهینه تری دارند نیز به طـــورکـامل ذکر شده است. نتایـج این پایـــان نامه نشان می دهد که الگوریتـم های رمزنگـــاری در جهـــت پیـــشرفته شدن رو به جـلو حرکـــت می کنند و بدیـن ترتیب بد اندیشان و مجرمین اینترنتی را ناکام خواهند گذاشت.

www.Prozhe.com

فصل اول : مفاهیم اصلی در ارتباطات داده

1-1: ارتباط داده

ارتباطات داده به سه مبحث زیر وابسته است:

1.فیزیک 2.ریاضیات 3. الکتریسیته

از طرفی ارتباط داده با دو مفهوم اصلی زیر تکمیل میشود:

1) Data transmission

2) Data switching

1-2: انتقال داده

انتقال داده شامل المان های اصلی زیر می باشد:

1) Source of the information(مبدا)

2) Destination of information(مقصد)

3) Channel for the transmission of the information(کانال انتقال)

www.Prozhe.com

همچنین در بعضی مواقع داده ها جهت کشف و تصحیح خطا کد میشوند. کانال انتقال داده میتواند از نوع سری یا موازی باشد.در نوع سری بیت ها یکی بعد از دیگری انتقال داده می شوند ولی در نوع موازی چندین بیت در آن واحد انتقال می یابند.

معمولاً کانال های از نوع موازی برای مسیر های کوتاه مورد استفاده قرار می گیرند(کمتر از 100متر)و کانال های از نوع سری برای مسافت های طولانی تر استفاده می شوند. امروزه کامپیوترها در بیشتر ادارات و منازل در دسترس هستند بنابراین نیاز به اشتراک گذاشتن اطلاعات روز به روز در حال افزایش است همچنین با پیشرفت تجهیزات ارتباطی داده، ارتباط بین کامپیوترها افزایش یافته است.

هم اکنون کاربری از هر کجای دنیا می تواند با هر کامپیوتر ازراه دوری توسط کانال ارتباطی ارتباط برقرارکند. هدف این پروژه معرفی جنبه های متنوع ارتباطات داده و شبکه های کامپیوتری است و بیش ترین تمرکز آن بر روی امنیت داده و رمزنگاری در مقوله ی ارتباطات داده است .

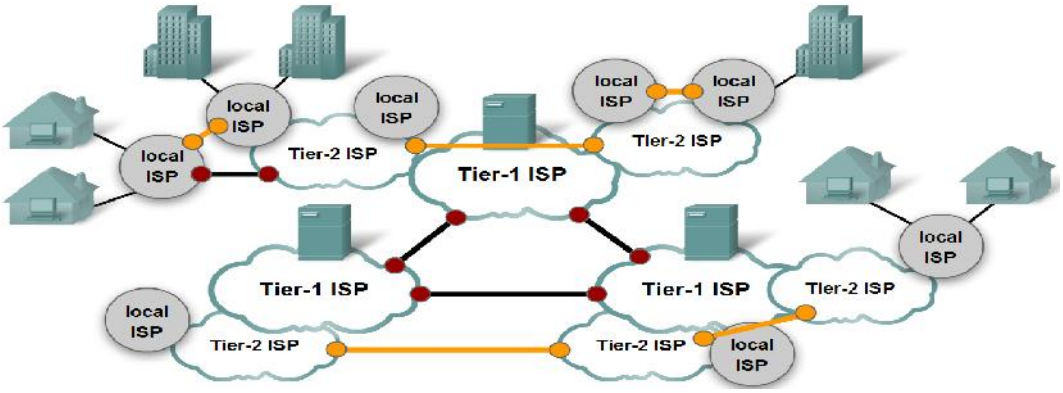
www.Prozhe.com

1-3: اینترنت

در سال های 60 هنگامیکه جنگ سرد بین آمریکا و شوروی مطرح بود آمریکـا به تدریج به شبکه هایش جهت انجام امور نظامی وابسته شد ولی همیشه از این بیم داشت که اگر جنـگ به وجود آید قسمتی از شبکه هایش از دست برود به همین دلیل به این فکر می کردند که کـاری انجام دهند که اگر قسمتی از شبکه از بین رفت بقیه بتوانند به کار خود ادامه دهند و خیـلی به هم وابسته نباشند.

دانشگاه های دولت آمریکا در صدد این بودند که ایده ای جهت حل مشکل مطرح کنند سر انجام یک سری خطوط طراحی کردند راه حلی که مطرح کردند این بود که هر یک از کامپیوتر ها به دو تا سه تا از کامپیوترهای دیگر ضرورتاً متصل باشد تا اگر یکی خراب شود ، بقیـه آن ها کار کنند ارتباط در اینجا اتصال گرا نبود چرا که چیزهای ثابت را نمی پذیرفت و الگوریتم هایی پویا تقاضا می کردتا بسته به شرایط ارتباط برقرارکند . به همین صورت تحقیقات انجام می شد تا به تدریج استانداردهایی در زمینه ی شبکه های کامپیوتری مطرح شد .

از جمله ی این استاندارد ها می توان به OSIو TCP/IPاشاره کرد.



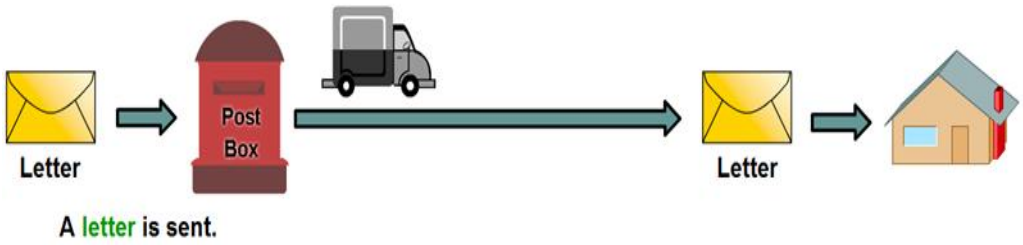
www.Prozhe.com

1-4: ارتباطات داده و نظام اقتصادی

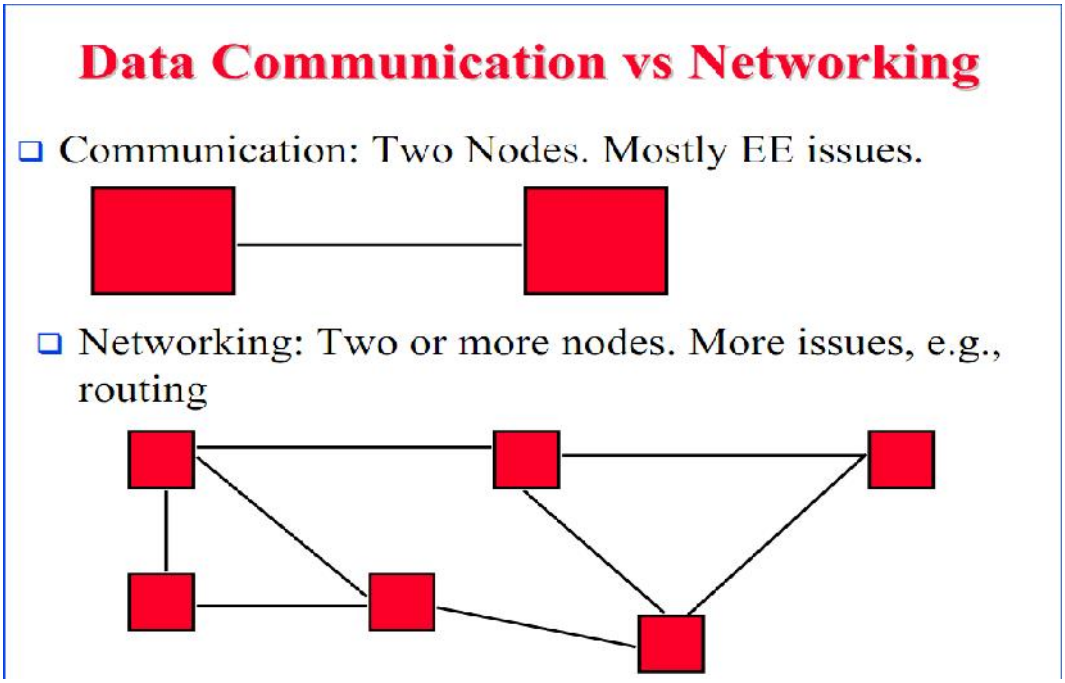
ارتباطات، مقوله ای که تمامی تکنولوژی های رسانه ای و دیجیتالی به آن ختم می شوند بخشی از نظام اقتصادی نیست بلکه خودش نظامی اقتصادی است منظور از این نظام اقتصادی کامپیوترها نمی باشد چرا که خیلی وقت است که دوره ی اقتصادی کامپیوترها به سر آمده و آن چه که نظام اقتصادی جدید در آن می گنجد حول محور ارتباطات عمیق وگسترده به گردش در می آید.

به همین جهت است که شبکه های کامپیوتری این چنین مهم جلوه می کنند ارتباطات و به دنبال آن رایانه ها سرگذشتی ویژه در تاریخ نظام اقتصادی دارند و این بیش تر به دلیل تاثیرات فرهنگی- اجتماعی و تکنولوژی و مفهومی می باشد که ریشه در زندگی انسان های امروز دارد.

عظمت تاثیر ابداع های شبکه های کامپیوتری به عظمت تاثیر ابداعات و اکتشافات مالی و شاید به گونه ای از آن هم بزرگ تر باشد . نظام اقتصادی آمیخته ای است از شیوه های مختلف تجارت،بازرگانی و مبادلات اجتماعی.



www.Prozhe.com



ارتباطات داده و شبکه های کامپیوتری از دیدگاه اجتـماعی یک پدیده ی فرهنگی و از دید مهندسی کامپیوتر یک تخصص و علم به شمار می آید.امروزه پیشرفت و توسعـــه ی مرزهـــای دانش به گسترش شبکه های کامپیوتری وابسته شده است هدف اصلـــی در فناوری اطلاعـــات گردآوری،سازمان دهی و فرآوری داده ها و دانش پراکـنده در سطـــح دنیـــاست به گونه ای که بتوان از این دانش گردآوری شده ،معرفـت و دانش جدید تولید کرد.بالطبع موثرترین ابزار برای جمع آوری ،سازمان دهی و پردازش داده های پراکنده،شبکه های کامپیوتری است.

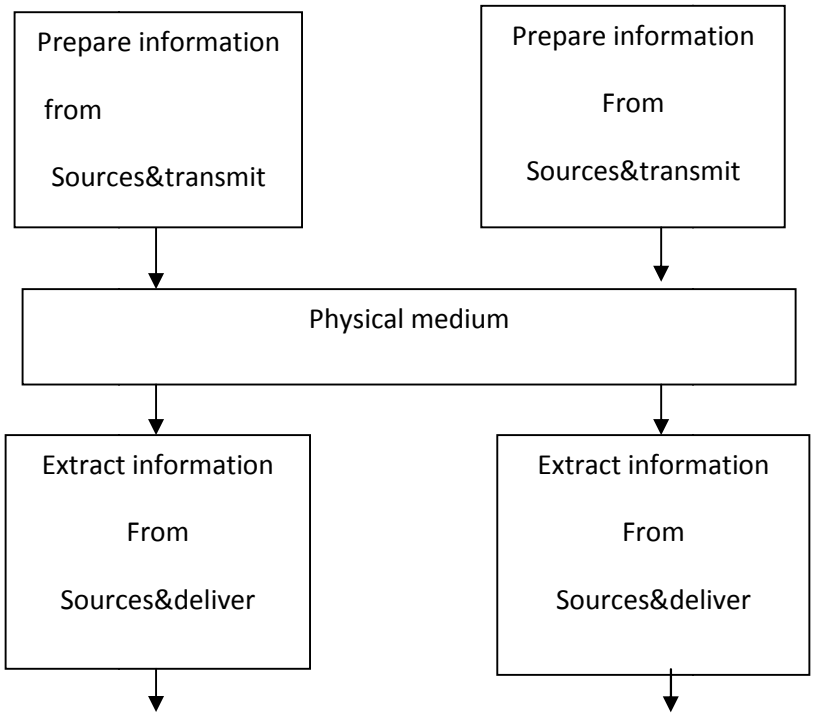
تنها دانش در اینترنت عرضه نمی شود بلکه چیزی که در اینترنت وجود دارد در یک مفهوم عام دانایی و آگاهی است به عنوان مثال اگاهی از نرخ سهام یا نتیجه ی یـک مسابقه یا اخبـــار حوادث را شاید نتـــوان در حوزه ی دانـش و علوم طبقه بندی کرد ولی نوعاً آگـــاهی محـسوب می شود.

www.Prozhe.com

Data communication concepts : 1-5

به منظور درک بهتر مفهوم ارتباط داده تصور کنید که یک سیستم ارتباطی متشکل از چند مبدا داریم این سیستم اجازه می دهد که هر مبدا، اطلاعـاتی را به مقصـدهای متفـاوت بفرستد این طور به نظر می رسد که ارتباط در این سیستم ارتباطی از یک دستور ساده و خاصی پیروی میکند.

هر مبدا به مکانیزمی جهت جمع آوری اطلاعات ،آماده کردن اطلاعات جهت انتقال وانتقال اطلاعات از بیـن یک وسیـله ی فیزیکـی نیاز دارد. به طور مشابه مکـانیزمی جهت گـشایش اطلاعات برای مقصد و فرستادن اطلاعات نیز وجود دارد.



در حقیقت ارتباط داده بسیار وسیع تر و پیچـیده تر از آن چیزیست که در دیاگرام مشاهده کردید زیرا اطلاعات می توانند از مبدا های متفاوت فرستاده شوند بنابراین تکنیک هایی که این مبداها را قبـل از فرستادن اطلاعـات اداره میکنند اهمیـت دارند همچـنین اطلاعـات باید به

www.Prozhe.com

صورت دیجیتالی فرستاده شوند علاوه بر این اطلاعاتی جهت مقابله با خطاهای احتمالی بایستی به داده های ما اضافه شوند.

همچنین در صورتیکه محرمانه بودن اطلاعات مد نظر قرار می گیرد بایستی اطلاعات رمزنگاری شوند. به منظور فرستادن زنجیره ای از اطلاعات از بین کانال ارتباطی از چندین مقصد متفاوت اطلاعات بایستی شناسایی شوند بنابراین مکانیزمی جهت شناسایی هر مقصد نیاز می باشد همچنین این مکانیزم بایستی تضمین کند که اطلاعاتی که از یک مبدا خاص به یک مقصد مشخص فرستاده می شوند با اطلاعاتی که از یک مبدا دیگر به همان مقصد مشخص فرستاده شده است اشتباه نمی شوند.

ارتباط داده:برای ارتباط اطلاعات و پیام ها از تلفن و سیستم های ارتباطی پستی استفاده می شود.به طور مشابه داده و اطلاعات از یک کامپیوتر میتواند به سایر کامپیوترها در بین مسیرهای جغرافیایی انتقال داده شوند.

انتقال داده:حرکت اطلاعات با استفاده از متدهای استاندارد در صورتیکه کامپیوترها به کانال ارتباطی وصل شوند داده ها و اطلاعات ،فایل ها و برنامه های کامپیوتر می توانند به سایر کامپیوترها فرستاده شوند. شکل مدرن ارتباطات مثل ایمیل و اینترنت فقط به خاطر شبکه های کامپیوتری ممکن شده است.

در مبحث ارتباط داده چهار مفهوم مورد استفاده قرار می گیرد:

1.داده:مجموعه ای ازحقایقی خام که بعد از پردازش به اطلاعات تبدیل می شوند.

2.سیگنال: کد کردن داده ها به صورت الکتریکی و الکترومغناطیسی

3.سیگنالینگ:انتشار سیگنال ها از میان سیستم ارتباط

4.انتقال:ارتباط داده حاصل شده از پردازش سیگنال ها

www.Prozhe.com

1-6 : مدهای انتقال داده

سه راه جهت انتقال داده از یک نقطه به سایر نقاط وجود دارد:

1)simplex:

ارتباط می تواند به صورت ساده باشد بدین صورت که شامل یک مسیر میباشد.گیرنده می تواند سیگنال ها را از دستگاه انتقال دریافت کند.در این مد جریان اطلاعات تـــک مسیره است یعنی یک طرف همیشه فرستنده و طرف دیگر همیشه گیرنده است در این صورت همیشه یک طرف در حال ارسال اطلاعات و طرفی دیگر در حال دریافت اطلاعات است.

2)Half-duplex:

دراین مد کانال ارتباطی در دو جهـت عمـل میکند اما در یک زمان. مسیر دو طرفه است بدین مفهوم که هر دو طرف میتوانند هم فرسـتـنده و هم گـیرنده باشند ولی نه همزمان.یعنی در یک زمان یک طرف فرستنده و طرفی دیگر گیرنده است و و در زمانی دیگر بالعکس .

3)Full-duplex:

در این مد کـانال ارتباطی در دو جهـت عمل میکـند به صورت همزمان.هـــمزمان هر دو طرف می توانند هم فرستنده و هم گیرنده باشند مثل خطوط تلفن.

(5) 1-7 : VPN[1]

VPN به زبون خودمونی شبکـــه خصوصی مجازی است که ارتباط کاربران رادر یک فضـــای خاص ایـجاد می کند برای مثـــال فرض کنیم که یـــک شرکـت بزرگ داریم که شعـــبه هایی درشهرهـــای مختلف دارد، وقتی کـــامپیوترهـــای این شرکت ها بخواهند با هـــم اطلاعـــات رد و بدل کنند یـــا حتـــی از یک اتوماسیون اداری یکـــسان استـــفاده کنند بایـد از طـــریق شبکـــه این کار را انجام بدهند. امّا استـــفاده از شبکـــهٔ جهانـی مثل اینترنت امنیـــت ندارد و

[1] Virtual Private Network

www.Prozhe.com

ترافیـک بالایی هم دارد و همچنین آدرس هـــایی را که در شبکـه داخلی خـودمان استــفاده میکنیم در شبکـــه اینترنت معـــتبر نیست که بخواهـــند از مسیـریاب ها رد بشوند.

از شبکه های گستردهٔ دیگری مثل:

OC3 وISDN هم میشود استفاده کرد. اما زیر ساخـت های زیـادی لازم دارد و هزینهٔ بالایی بایدپرداخت شود.

بنابراین از یک راه فرعی به نام VPN استفاده میشود.

VPN یک شبکهٔ خصوصی در دل شبکهٔ WANبه وجود می آورد که ترافیـک بالای اینترنت را نداردودرواقع سرعت بالاتر و امنیت بیشتری دارد. این یک کانال خصوصی برای ارتباط راحت تر و سریع ترمی باشد. به عبارتی ساده تر:

VPNیک تونل ایجاد میکند یعنی مثلاً شما وقتی در جاده از تونل رد میـشوید در حقیقـت در حال عبور از بستـر کوه هستید اما محـــتوای شما با محـــتوای کوه فرق دارد ، شما از هوا دارید عبور میکنید نه سنگ و این برای کوه قابل درک نیست و به همین دلیل اطلاعـات شما هم در اینترنت به همیـــن شکـــل خواهـــد بود ، شما فرض کنید اطلاعـــات خود را داریـــد با شکـــل مثـــلث ارسال میکنید و این در حالی هست که اطلاعات در اینترنت به شکل مستـطیل هستند و این باعث میـــشود که اطلاعـــات شما برای دیگران که در اینترنت هستند غیـــر قابل درک و نامفهوم شود که این خود امنیت است.

www.Prozhe.com

برای پیاده سازیVPNچندین پروتکل وجود دارد:

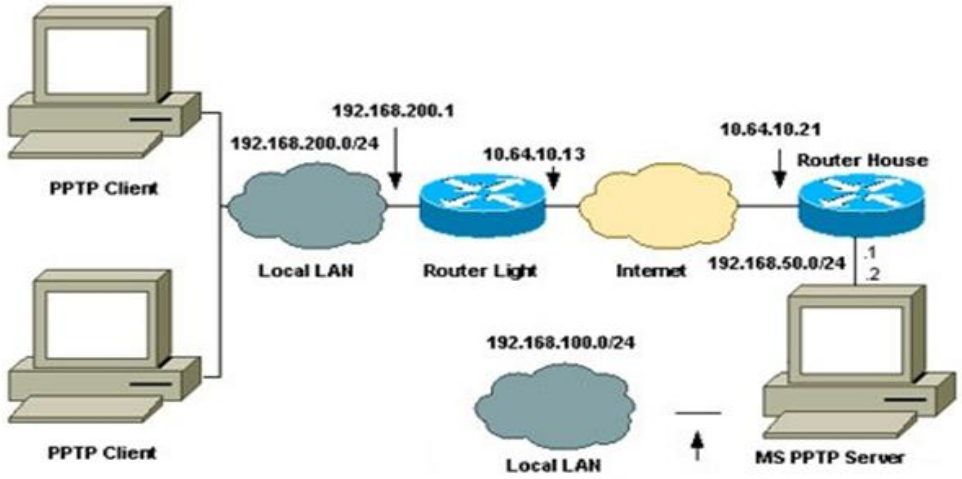
PPTP[2] :

ایـــن پروتکل برای انتقال داده هایی مثل (Net Beui) (داده هایی که دارای آدرس غیر IP هستند)روی یک شبکه ی پایه یIP استفاده می شود.

PPTP روی لایه ی دو مدل OSI پیاده سازی میشود و داده ها را روی FRAMهایی از طریق پروتکل نقطه به نقطه بسته بندی می کند.

البته PPP (point to point protocol) ویژگی هایی مثـل تخصیص آدرس پویا (DHCP) و تعیین اعتبار کاربر و فشرده سازی داده هـــا را دارد PPTP هـــم امکـــان رمز گـــذاری 40 بیتی و هم 128 بیتی را دارد.

شیوه های امنیتی به کار گرفته در این پروتکل کافی نیست.



میتوان گفت VPNنوعی معجزه در دنیای شبکه است.

[2] Point to Point Tunneling Protocol

www.Prozhe.com

این معـــجزه امروزه به صورت گسترده در دستیابی به شبکه هـای اجتماعی فعـــالیت می کند. VPN دارای پارامترهای امنیتی خاصی می باشد که باکنترل آن ها به آن سخت نفوذ می شود.

Firewall : 1-8

هـــر سیســتم امنیتی بر حسب نوع پارامترهایی که در داخلش استفاده میشود ممکن است که به آن نفوذ شود و مورد هجوم قرار گیرد.

VPN هم از این قضیه جدا نیست VPNدارای تنظیمات امنیتی ویژه می باشد که توانایی حفظ محرمانگی اطلاعات و امنیت را بالا می برد این شبکـه نیز همانند شبکه های دیگر قابلیت نفوذ دارد و بایستی تا جایی ممکن امنیت این شبکه را افزایـــش داد برای این کـار روش های زیادی وجود دارد از جمله: دیواره ی آتش و رمزنگاری

دیوار آتش

دیوار آتش سیستمی است که در بین کاربران یک شبکه ی محلی و شبکه ی بیرونی (مثلاً اینترنت) قرار میگیرد و ضـــمن نظارت بر دسترسیها،در تمـــام سطوح،ورود و خروج اطلاعات را تحت نظر دارد .

در این ساختـار هر سازمان یا نهادی که بخواهد ورود و خروج اطلاعات شبکه اش را کنترل کند موظف است تمام ارتباطات شبکه ی داخلی خود را با دنیای خارج قطـــع کرده و هرگـــونه ارتباط با دنیای خارج صرفاً از طریق یک دروازه که به شکل دیوار می باشد انجام گیرد.

www.Prozhe.com

1-8-1 : عملکرد کلی و مشکلات استفاده از یک دیوارآتش

بسته های IPقبل از مسیریابی روی شبکه ی اینترنت ابتدا وارد دیـــوار آتش می شوند و منتـظر می مانند تا طبق معیارهای حفاظتی و امنیتی پردازش می شوند.

پس از پردازش و تحلیل بسته سه حالت ممکن است اتفاق بیفتد:

1)اجازه ی عبور بسته صادر شود.(Accept Mode)

2)بسته حذف گردد.(Blocking Mode)

3)بسته حذف شـــده و پاسخ مناسـب به مبدا آن بسـته فرستاده شود.(Response Mode)

به طور کلی دیوار آتش محـــلی است برای ایست و بازرسی بسته های اطلاعاتی به گونه ای که بسته ها بر اساس تابعی از قواعد امنیتی و حفاظتی،پردازش شده و برای آن ها مجوز عبور یا عدم عبور صادر گردد.

1-8-2 : اجزای جانبی یک دیوار آتش

دیوار آتش یک سیستم امنیـتی است کـــه سیاست هـای مسئول شبـکه را پیاده و اعمال میکند. بنابراین دیوار آتش بایستی از طریق یک ورودی سهل و راحت قواعد را از مسئول شبکه دریافت نماید و همواره فعالیت موجود روی شبکه را به مسئول شبکه گزارش بدهد. بـــه همین دلیل اصولاً یک سیستم دیوار آتش دارای اجزای زیر می باشد:

واسط محاوره ای و ساده ورودی/خروجی:برای تبادل اطلاعات و سهولت در تنظیم قواعد امنیتی و ارائه یک گزارش به یک واسط کاربر[3] که ساده ودرعین حال کارآمدباشد، نیاز است.

معـــمولاً واسط کاربر مستقل از سیستم دیوار آتش است تـا حـــجـــم پردازش اضافی روی سیستم تحمیل نکند یعنی معمولاً دیـــوار آتش دارای دستگاهی به عنوان صفحه نمایش نیست

[3] User Interface

www.Prozhe.com

بلکه از طـریق وصل یک ابزار جانبی مثل ترمینال ساده یا یک کامپیوتر شخصی، فرمان میگیرد یا گزارش میدهد.

سیستم ثبت(Logger):برای بالاتر بـــردن ضریب امنیت و اطمینان در شبکه ،دیوار آتش باید بتواند حتی در صورت هرگـونه حمـله یا نفوذ بتـوان مسئـله را پیگیری کرد .در یک دیوار آتش ،کاری کـه سیستم ثبت می تواند انجام دهـد آن است که مبـدا و مقصـد بسته هـای ورودی و خروجی،شماره پورت هـای مبـدا و مقصـد، سرآینـد یـا حتی محتوای پیام در لایه ی کاربرد را (برای تمـام مبادلات خارج از شبکه ی محلی) ذخیـره کند و لحظه به لحظه مبادله ی اطلاعات تمام کـاربران و حتی مسئـول شبـکه را در محلی درج کند .ایـن اطلاعات می تـواند بـه عنوان سندی بر علیه فـرد خاطی استفاده شود یـا بـــه یافتن کسیکه کـه در خـارج از شبـکه مشغول اخلالگری است کمک کند.

سیســتم هشداردهنده:در صورت بروز هرگونه مشکل یا انتقال مشکوک،دیوار آتش می تواند مسئول شبـکه را مطلع و در صورت لـزوم کسب تکلیف کند . عملیات مشـکوک در هر سه لایه تعریف میشود:مثل تقاضای ارتباط با:

IPآدرس هـــای مسـدود،آدرس هـای پـورت مســـدود،اطلاعات مشـکوک در لایـه ی کـاربـرد (صفحات وب یا نامه حاوی کلمات مشکوک) ارتبـاط مشـکوک را می تـوان مصـداق ارتبـاطاتی دانست که بی هدف یا مکرر در طی روز برقرار میشود یا آنکه اطلاعات ارسالی مفهوم یا مضمون خاصی نداشته یا آنکه رمز شده باشد.در این حالت دیوار آتش ضمن کسب تکلیف می تواند یک آدرس مشکوک را به عنوان آدرس غیرمجاز مسدود کند.

راه حل نهایی:با تمام نظارتی که بـر تردد بستـــه های اطلاعاتی حین ورود و خـروج از شبـــکه می شود باز هم می توان زیرکانه از مرز دیـوار آتش عبور کرد و بهترین حفاظت برای جلوگیری از فاش شدن اطلاعات محرمانه به دنیـای خارج نابود کردن خط ارتباطی شبکه به دنیای خارج

www.Prozhe.com

است !چـرا که می تـــوان اطلاعات سری را رمز و فشرده کرد و آن را به عنوان بیت کم ارزش از نقاط تصویر یک گل رز بـه عنوان کـــارت پستال تبریک سال نو ارسال نمود. به این روش نفوذ استیگانوگرافی گفته میشود.

در حقیقت سیستم دیوار آتش فقط یک ابزار محـدود کننده است و اطمینان صد در صد ندارد.

1-9(5) : تفاوت بین فایروال های سخت افزاری و نرم افزاری

در اصطلاح کـــامپیوتری واژه فـــایروال به سیستمی اطلاق می شود کـه شبکه خصوصی یا کامپیوتر شخصی شمـــا را در مـــقابل نفوذ مهاجمین ، دستـرسی های غیر مجاز ، ترافیک های مخـرب و حملات هکری خارج از سیستم شما محافظت می کند . فایروال ها می توانند ترافیک ورودی بـــه شبکه را کنترل و مدیریت کرده و با توجه به قوانینی که در آنها تعریف می شود به شخص یـــا کـــــاربر خاصی اجازه ورود و دسترسی به یک سیستم خاص را بدهند . مثلاً شما می توانید برای فایروال خود که از یک شبکه بانکی محافظت میکند:

با استفاده از قوانینی که در آن تعریف می کنید بخـــواهید که بهX در ساعتYاجازه دسترسی به کامپیوتر Z کاربر که درون شبکه ی داخلی شما قرار دارد را بدهد.

فایـــروال های سخت افزاری معمولاً بصورت زیـــر ساخت هایی هستند کـه توسط شرکت های تولید کننده بر روی بـــردهای سخت افزاری نصب و راه اندازی شده اند و معمولاً در قالب یک روتر در شبکه فعالیت می کنند، یک روتـــر نیز می تواند در یک شبـــکه به عنوان یک فـایروال سخت افزاری فعالیت کند . یک فایـــروال سخت افزاری می تـــواند بصورت پیش فرض و بدون انجام هـــرگونه تنظیمات اولیه در حـــد مطلوبی از ورود داده ها و ترافیک نـاخواسته به شبکه محافظت کرده و اطلاعات ما را ایمن نگه دارد .

www.Prozhe.com

اینگونه فایروال ها معمولاً در قالب :

packet filtering فعالیت می کنند وHeader هـای مربوط بـه مبدا و مقصد بسته هـا را به دقت بـــررسی کرده و در صورتیکه کـــه محتویات بسته با قوانینی که در فایروال انجام شده است مغـــایرت داشته باشد بلافاصله از ورود آن به شبکه جلوگیری کرده و آنرا بلوکه می کند . بسته اطلاعاتی در صورتیکه مغایرتی بـــا قوانین موجود در فایروال نـداشته باشد به مقصد مورد نظر هدایت خواهد شد . کاربر باید به راحـتی از تنظیمات پیش فرض انجام شده در آن استفاده کند ، تنها بعضی از تنظیمات پیشرفته امنیتی در اینگونه فایروال ها هستند کـه نیـاز به داشتن دانش تخصصی فراوان بـــرای انجام دادنشان دارند . اما این را در نظر داشته باشید کـــه فایروال های سخـــت افزاری می بایست توسط یک کـــارشناس متـــخصص امنیـــت آزمایش شده تا از کـــارکرد آنها اطمینان حاصل شود . فایروال های سخت افزاری بار ترافیکی و لود کاری کمتری برای شبکه ایجـــاد می کنند و طبیعتاً سرعت و کـارآیی بهتری در شبکه دارند اما از نظر هزینه بیشتر از فایروال های نرم افزاری هزینه دارند.

فایـــروال های نـــرم افزاری در حقیقت نـرم افزار هایی هستند که بر روی سیستم عامل ها نصب شـــده و ترافیک ورودی و خروجی به شبکه یا سیستم عا مل را کنترل می کنند . اینگونه فایروال ها بیشتر استـــفاده های خانگی و سازمان ها و شرکت های کوچک و متوسط را به خود اختصاص داده اند . فـایروال های نـــرم افزاری سیستم ها را از خطرات معمولی که در اینترنت وجود دارند اعـم از دسترسی های غیرمجاز ، تروجان ها و کدهای مخرب ، کرم های کامپیوتری و بسیاری دیـــگر از این موارد حفاظت می کنند . اکثر اینگونه فایروال ها به کاربران این قابلیت را می دهنـــد کـــه بتوانند بـــرای به اشتراک گذاشتن منابع خود از جمله پرینتر و پوشه ها در قوانین فـــایروال تغییرات دلخواه خـــود را اعمـــال کـرده تا بتوانند از امکاناتی که مد نظر دارند استفاده و بهره کافی را ببرند . در بـرخی اوقات، فـــایروال های نرم افزاری ابزارهای جانبی را در

www.Prozhe.com

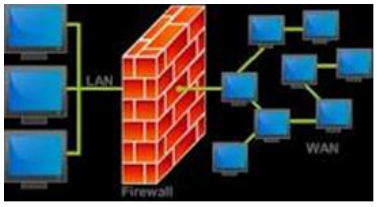
اختیار ما قرار می دهند که توسط آنها میتوانید تنظیمات محرمانگی و فیلترینگ خاصی را برای خود یا کاربران دیــگر اعمال کنید. اینگونه فایروال ها در دو نوع شبکه ای و تک محصولی ارائه می شوند ، فــایروال های نــرم افزاری تحت شبــکه روی یک سیستم عامل نصب می شوند و می توانند از آن محافظت کنند.

تنوع فایروال های نرم افزاری بسیار زیاد است.

امــا همیشه در نــظر داشته باشید کـه بهترین فایروال نرم افزاری فایروالی است که ضمن اینکه در پس زمینه سیستم شما فعالیت می کند از کم ترین منابع سیستمی استفاده کند و بار سیستم را زیاد نکند.

فایروال های نرم افزاری ترافیک و لود کـاری بیشتری در شبکه ایجاد می کنند امــــا به نسبت فایروال های سخت افزاری از هزینه ی قابل قبول تری برخوردارند.

هر سازمانی که می خواهد از فایروالی استفاده کند ابتدا می بایست شرایط کاری خود را در نظر گـــرفته و بداند که با توجه به این شرایــط بایــستی از کدام نوع فایـــروال استفاده کند سخت افزاری یا نرم افزاری.همان طور که گــفته شد فایـــروال هــای سخت افزاری لود کاری کــمتری در شبکه ایجاد می کنند ولی به نسبت فایـــــروال هـای نرم افزاری گران قیمت ترند ولی فایـــروال هــای نرم افزاری ارزان تر ولی لود کاری بیش تری در شبکه به وجود می آورند بنابراین بسته به نیاز و شرایط بایستی بهترین فایروال را انتخاب نمود چرا که در صورت انتخاب درست فایروال نیاز امنیتی شبکه ی سازمان تا حدی برطرف می شود.



نمایی ساده از یک دیوار آتش

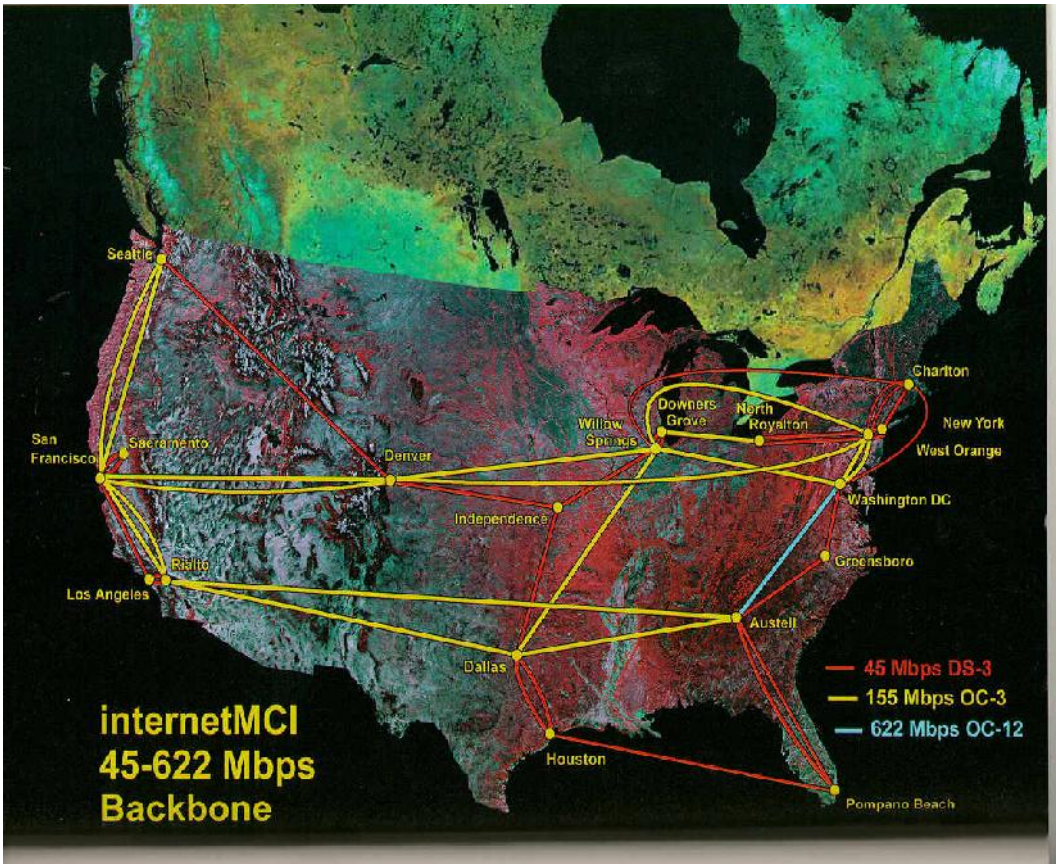
www.Prozhe.com

فصل دوم : امنیت در ارتباطات داده

با گسترش روز افزون استفاده از کامپیوتر و وسایل الکترونیکی بـه تدریج استفاده از شبکه های کامپیوتری نیز افزایش چشمگیری یافت .

با گسترش شبکه های کامپیوتری و انبـــوه حجم اطلاعات قسمت زیادی از امور روزمـره به شبکه های کامپیوتری و شبکه ی جهانی وابسته شده است بـه طوریکه اکثر کارهای روزمره ی زندگی توسط شبکه های کامپیوتری و یا در بستر اینترنت انجام می شود.

آن چه کـــه مهم است تبادل اطلاعات از طـــریق شبکه های کـــامپیوتری می باشد که این تبادل اطلاعات چالش های زیادی را برای صاحبان آن ها از نظر امنیتی به وجود آورده است.



www.Prozhe.com

بـــه طور یقین هرکس حفظ امنیت اطلاعات خود را خواستار است و هیچ کس نمی خواهد اطلاعاتش مـــورد سواستفاده قرار گیرد ولی بـــا توجه به اینکه شبکه های کامپیوتری با تعداد زیادی از کاربران سروکار دارد بنابراین حفظ امنیت اطلاعات و امنیت داده ها از مقوله های مهم در ایـــن مبحث به شمار می رود. اگـر مـــردم تا دیروز از افراد دزد و راهزن بـــه عنوان افرادی بی سواد می ترسیدند امروزه با گسترش اطلاعات بـــاید از افراد باهوش و باسواد حتی نابغه در علوم کامپیوتری ترسید چـــرا که هستند کسانی که بسیار باهوشند ولی از هوش خود در جهت نـــادرست استفاده میکنند این افـراد می توانند به راحتی به شبکه های کامپیوتری نفوذ کرده و اطلاعات دیگران را بدزدند و یا از آن ها سواستفاده کنند که بس بدتر از راهزنی و دزدی مالی می باشد .

2-1 : امنیت شبکه

امنیت شبکه ها شامل:

چگونه افراد بداندیش می توانند شبکه های کامپیوتری را مورد حمله قرار دهند؟

چگونه می توان شبکه های کامپیوتری را در برابر حملات ایمن نگه داشت؟

چه ساختارهایی می توان جهت مقابله با حملات طراحی و استفاده کرد؟

www.Prozhe.com

اینترنت ذاتاً با امنیت زیادی طراحی نشده است.

به چه دلیل ما به امنیت در اینترنت نیاز داریم؟

زیرا:

شبکه های کامپیوتری آسیب پذیری زیادی دارند و تهدیدبرانگیزند.

یک هــکر بداندیش می تواند از راه دور به ماشینی وارد شده و به راحــتی اطلاعـات آن را نابود کند.

یک برنامه ی بدجنس می تواند سبب از بین رفتن حجـم زیادی از اطلاعات در صدها کامپیوتر شود.

رشد سریع اینترنت سبب ایجـاد تغییرات زیادی در سبک زنـــدگی انسان ها،فعـالیت های کاری و شغلی آن ها همچنین تغییر در نحوه ی فعالیت های سازمان ها و موسسات شده است.

کاربران اینترنتی اطلاعـات زیاد و البته مهمی را بارهـــا و بارهـــا ارسال و یا دریافت می کنند.

www.Prozhe.com

افـــراد غیـرمجاز سعی در دستیابی به اطلاعات کاربران اینترنتی و سواستفاده از این اطلاعات را دارند و آن چه امروزه برای کاربران اینترنتی از اهمیت فراوان برخوردار است اطمینان از عـــدم دستیابی این افراد در توزیع اطلاعات است.

اطلاعاتی که کاربران در مـــورد آن ها حساس هستند و تمایل به مشاهده ی این اطلاعات توسط افراد دیگر را ندارند موارد زیادی را شامل می شود کـــه در ذیل به چند نمونه ی آن ها اشاره شده است:

اطلاعات خصوصی

جزئیات شخصی

رمزهای عبور

اطلاعات کارت های اعتباری

اطلاعات مربوط به حساب های بانکی

اطلاعات مهم و حیاتی در سازمان ها

تاکنون برای برقـــرای امنیت اطلاعـات بر روی کامپیوتر ویا اینترنت از روش های متفاوت و مخـتلفی استفاده شده است. یکی از این روش های حفظ اطلاعات و برقراری امـنیت که بسیـار ساده نیز می باشد ذخیره سازی قابل انتقال نظیر فلاپی دیسک ها می باشد.

متداول ترین روش امنیت اطلاعات رمزنمودن آن ها می باشد.

تشخیص اطلاعاتی که به صورت معمولی در کامپیوتر ذخیره می شوند و فاقد هرگونه روش علمی رمزنگـــاری می باشند به راحتی و بدون داشتن تخـــصـصی خاص انجـــام خواهد شد در صورتیکه دستیابی به اطلاعات رمز شده توسط افراد غیرمجاز امکـــان پذیر نبوده و فقط افرادی که دارای کلید رمز هستند قادر به استفاده از اطلاعات می باشند.

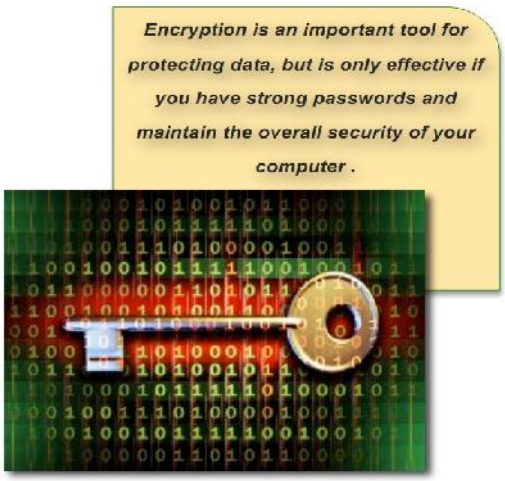
رمز نمودن اطلاعات حساس سبب حفظ حریم خصوصی افراد می شود.

www.Prozhe.com

امروزه با محـــول شدن امور مالی و اداری به شبکه های کامپیوتری زنگ خطر برای همگان به صـــدا در آمده و برخلاف گـــذشته که مردم از ترس دزدی و راهـزنی به در خـــانه خود قفل می زدند امروزه به دنبال قفل زدن بر اطلاعات شخصی خود می باشند .

امروزه امنـیت ملی و اقتدار سیاسی و البته مهـــم تر از همه اقتصادی به طور باورنکردنی به امنیت اطلاعات گـره خورده است و نه فقط دولت ها و سیاسیون بلکه تک تک افراد یک جامعه نیز به دنبال برقراری حفظ امنیت می باشند .

هیچ کس در جهان امروز نمی تواند اهمـیت امنیت اطلاعات را منکر شود برای مثال اگر به شخصی بگـویند که به حساب بانکی اش دستبرد زده شده و حساب خالـــی می باشد بعد از آن همیشه مراقب اطلاعات شخصی و بانکی خود خواهد بود و سعـــی در حفظ محرمانگـــی آن ها خواهد کردو به اهمیت امن ماندن اطلاعات خود پـی خواهد برد همچنان که حفظ امنیت برای همه مهم وحیاتی است شیوه های برقرای امنیت نیز مهـــم می باشد و هرکس به دنبال بهترین شیوه می گردد تا به بهترین نحو ممکن از اطلاعات خود حفاظت کند.



www.Prozhe.com

فصل سوم : تاریخچه ی رمزنگاری

3-1(4) : نمونه هایی از روش های رمزنگاری در تاریخ

جاسوسان یونـــــانی در ایـــران پیام های خـــود را روی سر تراشیده ی غلامان و بردگان می نوشتند و پس از بلند شدن مویشان آن ها را به یونان می فرستادند.

رمز و کاربرد آن حتی در قرآن هم مشاهده می شود حروف مقطع قرآن که در شروع بعضی سوره ها آمده مانند یک کلید رمز مقابل چشم مسلمانان قرار داشته و مسلمین فت آزمایی های زیادی برای حل آن ها به خرج دادند به عنوان مثال شیعیان از اتصال این حروف مقطعه جـمله "صراط علی حق تمسکه" را ساختند و حکام دیگر از هـــمان قدیم پی بردند که در سوره هایی که حروف رمز در آن ها وجود دارند،درصد تکرار آن حروف از حروف دیگر بیشتر است.

در تاریخ، قرامطه به تیـن نام خوانده شدند به این دلیل که با زبان رمزی نگـــارش می کـــردند.

توماس جفرسون چرخ رمز را ابداع کرد این رمز بعدها گسترش پیدا کرد و در جنگ جهانی دوم استفاده شد.

تینی چالسی اولین شرح رمز را برای رمزهای توموگرافیک نوشت.

الکساندر کوخ رمز استوانه ای را ابداع کرد.

لستر هیل مقاله ی زیبایی در رابطه با رمزنگاری در جبر حروف منتشر کرد.

در جنـگ جهانی دوم آلـــمان هـا از ماشینی به نام ماشین رمز انگـــیما استفاده می کردند این ماشیـن با استفاده از موتورهـــای الکتریکی عملیات رمزنگاری را با سرعـت بالا انجام میداد این ماشین از روش رمزنگاری میله ای استفاده میکرد. (4)

برای اولیـن بار در سال 1991 رمز کوانتومی توسط بنتووبراساد مطرح شد.آن ها از یک فوتون جهت انتقال کلید استفاده کردند در این رمزنگـاری فرستنده و گیرنده بایستی دارای کابل فیبر اپتیکی باشند.(4)

www.Prozhe.com

در سال های 1921 هوگ هیرن کدهای الکتریکی را ابداع کرد.

ویلیام فردریک به عنوان پدر علم رمز آمریکا شناخته می شود.

جوفری چاوسر رمزی نوشت که ترکیبی از علائم و جا به جایی حروف و کد بود.

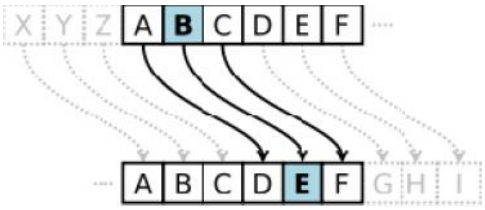
در تاریخ ائـــمه ی معصومین هم مواردی از کـاربرد رمز و استفاده ی از آن مشاهده می شود به عنوان مثال امام صادق(ع) هر بار که می خواستند از بنی عـباس با کـنایه یاد کنند از آن ها به صورت اولاد سابع یاد می کردند که معکوس کلمه عباس است.

محـققان بریتانیایی در آکسفورد و دانشگاه ساتمتون روشی را کـشف کرده اند که می توان عکـس هـــای دقیق از دست نوشته هـــای قدیمی برداشت. نامه های قدیمیتر که در سالهـــای 3000 و 3200 قبل از میـــلاد در ایران برای حسابرسی استفاده می شده است و تاکنون رمز گشایی نشده است. عکس های تهـیه شده بر روی سایت دانشگاه آکسفورد قرار داده خواهد شد تا متخصصان بتوانند بر روی آن کار و ترجمه کنند.

زمانیکه ژولـیس سزار نامه ای را برای فرمانده ی خود در جنگ می فرستـاد از ترس کـشته شدن پیک و یا خیانت پیک تمامی متن نامه را رمز مـی نمود به این صورت که هر حرف را به سه تاحرف بعدازآن شیفت میداد مثلاً (به جای حرفA از حرفD و به جای B از حرفE) استفاده می کرد.

در این صورت حتـــی در صورت کشته شدن پیک توسط دشمن و یا خیانت پیک از فاش شدن اطلاعات محرمانه جلوگیری میکرد و فقط کسی می توانست پیام را بخواند که به رمز آن آگاهی داشت و به قولی کلید رمز را می دانست.

روش سزار شاید امروزه بسیار ساده به نظر برسد ولی در زمان خودش بسیار پرکاربرد بوده است و بایستی توجه کرد قدمت رمزنگاری به همان دوران برمی گردد.



www.Prozhe.com

از روش هـای رمزنگـــاری در زمان های گذشته پیچیدن یک نوار کاغذی بر روی استوانه ای با قطر مشخص و سپس نوشتن پیام بر روی آن بوده است واضح است بدون دانستن اندازه ی قطر استوانه خواندن پیام کـار دشواری بوده و تنها کسانی که نمونه های یکسانی از استوانه را داشته باشند می توانستند پیام را متوجه شوند.

3-2 : رمزنگاری در کشورها

رمزنگـــاری علـمی است که شاید بتوان گفت در اکثر امور روزمره زندگـــی با مواردی از آن مواجه هستیم حتی کشورهای مختلف در ریزترین موارد برای حفـــظ امنیت اطلاعات و یا بیان مفاهیم مهم در کشورشان از رمزاستفاده می کـردند و هم اکنون نیز هـــمان مسیر ادامه دارد و استفاده از شیـــوه های رمزنگاری حتی در کـــوچک ترین مـــوارد نیز مـــتداول و رایـــج است.

از نمونه های بارز رمزنگـــاری در همه ی کشورها که به وسیله ی آن مفهـــومی را به سایر ملل می رسانند استفاده از شیوه هـــای رمزنگاری در پـــرچم کشورهـــای مـــلل مختلف است.

به گزارش اختصاصی ایران ویج ، استفاده از پرچم ها حتی از قبل از تاریخ بشر مرسوم بوده است. همه ی کشور هـای جهان دارای پرچم هستند، بعضی از آنها عجیب هستند، برخی زیبا و حتی برخی کسالت آور. در ذیل به نمونه ای از آن ها اشاره شده است.

3-2-1 : مخابره بوسیله ی پرچم

صحبت کردن و حرکـت دادن بدن تنهـــا روش هـای استفاده از زبان نیستند. پرچم هـــای مخـابره یا فرستادن پیام نیز یک راه انتقال اطلاعـــات از راه دور است که با استفاده از گـــرفتن پرچم، میله، سپر، پارو وگاهـــی حـتی با استفاده از دستان هـــم صورت می گیرد. حالت هـــای مختلف پرچم هـــا کد گذاری شده و وقتی پرچم در حالـــت ثابت قرار گـــیرد رمـــز آن خوانده

www.Prozhe.com

می شود. این روش در اوایل قرن نوزدهم در دریانوردی بسیار معمول بوده و کاربرد داشته است. این سیستم هنوز هم در دریا نوردی کاربرد دارد و در مواقع اضطراری برای برقراری ارتباط استفاده می شود؛ اگر نیاز باشد در شب پیامی فرستاده شود از مشعل های روشن بجای پرچم استفاده می شود.

با استفاده از رمزنگاری سه سرویس امنیتی فراهم می شود:

محرمانه سازی: اطلاعات به هنگام ارسال یا ذخیره شدن از دید افراد غیر مجاز پنهان می مانند.

تمامیت: تغییرات اعمال شده در اطلاعات ارسالی مشخص می شوند.

اعتبار سنجی: می توان منبع اطلاعات را اعتبار سنجی کرد.

3-3 : رمزنگاری داده

رمزنگاری داده به مباحث ریاضی و الگوریتمی بر می گرددومقوله ای است که در آن یک متن ساده به فرم متنی رمزنگاری شده در می آید ودر طول این رمزنگاری از یک کلید رمز استفاده می شود که توسط آن کلید، متن ساده رمز می شود و توسط همان کلید یا کلیدی دیگر متن رمزنگاری شده به شکل ساده و اولیه اش باز می گردد.

با رشد روزافزون و چشمگیر استفاده از اینترنت از جمله خرید اینترنتی،پرداخت اینترنتی، انجام امور بانکی توسط اینترنت و سرویس های دیگری که اینترنت ارائه می دهد حتی کاربران ساده ی منازل از رمزنگاری داده ها مطلع و آگاه می باشند.

www.Prozhe.com

3-4 : رمزنگاری پیشرفته

با پدیدارشدن رایانه‌ها و افزایش قـــدرت محاسباتی آنها، دانش رمزنگـــاری وارد حوزه علوم رایانه شد و این پدیده، موجب بروز سه تغییراساسی در مبحث رمزنگاری گردید.

1. شیوه های رمزنگاری که تا قبل از آن اصولاً برای رمز کردن پیام به کار می‌رفتند، کاربردهای جدید و متعددی پیدا کردند.

2. تا قبل از رایانه ها، رمزنگاری عمدتاً روی اطلاعات متنی و با استفاده از حـــروف الفـــبا انجام می‌گرفت؛ اما ورود رایانه باعث شد که رمزنگاری روی انواع اطلاعات و بر مبنای بیت انجام شود.

3.وجود قدرت محاسباتی بالا این امکان را پدید آورد که روش‌هـــای پیچیده‌تر و مؤثرتری برای رمزنگاری به وجود آید.

رمزنگاری امری تاریخی می باشدکه از هل دادن حـــروف و برعکـــس نوشتن آن ها از زمان قدیم شروع شده است و هرروز با رشد کامپیوتر و فناوری اطلاعـــات روشی نوین برای آن یافت می شود.

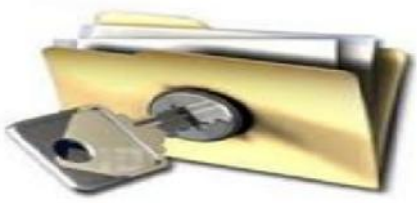
هنگـــامی که با مبحث تبادل داده و اطلاعـات سروکار داریم نیاز به تایید هویت فرستنده و گیرنده پیام داریم به گونه ای با مقوله ی احراز هویـت روبه رو هستیم این احراز هویت از زمان های دور نیز وجود داشته است و از روش های رمزنگـــاری برای محرمانه نگه داشتن پیام هایی

www.Prozhe.com

که بین فرماندهـان،جاسوسان و حـــتی عشاق رد وبـــدل می شده استفاده شده است به همین جهـــت می توان رمزنگاری را هـــنری دانست که از دیرباز در بین انسان هـا وجود داشته است. اطلاعـــات به سـوی پیشرفته شدن پیش مـی روند از طـــرفی پیشرفته شدن تکـــنولوژی های کـــامپیوتری سبب رشد و ارتقای علم رمزنگاری شده است و از طـــرفی دیگر نیاز به روش های جدیـــد ومطمئن تر در حوزه ی فناوری اطلاعات علم رمزنگـــاری را بر آن داشته تا نیاز هـــای موجود در این حوزه را به بهترین شکل ممکن مرتفع نماید. امنیت هـــدف نیست بلکه یک سفر دائـــمی است اغلـب می شنوید ایجـاد امنیت پایان پذیر نیست چرا که وقتی امنیت یک شبکه را در نظر بگیریم همیشه بایستی مراقب باشیم که یک گـام از مجرمان اینترنتی جلوتر باشیم و باید بدانیم هـمیشه نمی توان در یک سطح از امنیت باقـــی ماند و درجـــا زد چرا که مجـرمان اینترنتی هـــر روز به دنبال بهبود روش های خود جهـت نفوذ به شبکه ی شما هستند و بدیهی است که اگر شما یک گام از آن ها جلوتر نباشید آن ها یک گـــام از شما جلوتر هستند و شبکه شمـا هر روز با تهدیدهای آن ها مواجه خـواهد بود و آن ها هر روز و هرروز بر خـــلاقیت خـود می افزایند تا به شبکه ی شما راه پیدا کرده و به اطلاعات شما دست یابند.

در نتیجه:

همیشه یک گام جلوتر از مجرمین اینترنتی باشید .



www.Prozhe.com

علم رمزنگـاری با اصــول ریاضی و منطقی اطلاعــات را رمز کرده و اطلاعــات رمز شده را رمزگـشایی می کند. متضـاد رمزنگــاری ((تحـلیل رمز)) است کـه روش هــای شکـستن رمز اطلاعــات و کشف کلید رمز را مورد تجزیه و تحلیل قرار می دهد.

اوصولاً در دنیای شبکه های کامپیوتری رمزنگاری به سلسله ای از عملیات منطقی و ریاضی اطـلاق می شود کـه مجموعــه ای از اطلاعات خاص و با معنا را به مجموعــه ای از اطلاعــات نامفهوم و بی معـنا تبدیل می کند به طوریکه فقط گیرنده ی اصلـی بتواند آن را از حـالت رمز خارج کرده و از آن استفاده نماید.

3-5 : رمزنگاری سخت افزاری[4]

در ادامه در مورد پروتکــل ها و الگوریتم های رمزنگــاری مباحـثی را مطرح می کنیم.

مختصری در مورد الگوریتم های رمزنگاری:

الگوریتـم های رمزنگــاری را مــی توان هم به صورت سخـت افزاری و هم به صورت نرم افزاری مطـرح کرد. از الگوریتم های رمزنگاری سخت افزاری به منظور سرعت بالاتر و از الگوریتم های رمزنگاری نرم افزاری به منظور انعطاف پذیری بیش تر استفاده می کنند . از جمله این روش ها مــی توان به روش های جانشینی و جایگشتی اشاره کرد که می توانند توسط یک مدار ساده ی الکترونیکی پیاده سازی شوند.

P-BOX ابزاری که برای جایگشت یک بیت های ورودی هشت بیتی کاربرد دارد.

با برنامــه ریزی و سیم بندی درونی این ابزار قادر است هرگونه جایگشت بیتی را با سرعتی نزدیک به سرعت نور انجام می دهد چون هیچ گونه انجام محاسبه ای لازم نیست و فقط تاخیر انتشار سیگنال وجود دارد .

[4] Hardware Cryptography

www.Prozhe.com

این طراحـــی از اصول ششگانه ی کرکـــهف پیروی می کند به این معنا که مهاجم از روش عمومی جایگـشت بیت ها مطلع است آن چه که او نمی داند آن است که کـــدام بیت به کـدام بیت نگاشته می شود **کلید رمز همین است**.

1-5-3: اصول ششگانه ی کرکهف

آگوست کرکهف دو مقاله با عنوان رمزنگاری نظامی در سال 1883 منتشر کرد . در هردوی این مقالات شش اصل اساسی را به عنوان اصول پایه ای رمزنگاری بیان کرد که اصل دوم آن به عنوان اصلـــی اساسی دررمزنگـــاری هنوزهـم مورد استفاده ی دانشمندان در قوانین رمزنگاری پیشرفته مورد استفاده قرار می گیرد:

1.سیستم رمزنگاری نه به لحاظ تئوری بلکه در عمل غیرقابل شکست باشد.

2.سیستم رمزنگاری بایستی هیچ نکته ی گنگ و پنهان و نا مفهـــومی نداشته باشد تنها چیزی که پنهان است کلید رمز است.

3.کـلید رمز را بایستی به گونه ای انتخاب کرد کـه اولاً براحتی قابل تعویض باشد ثانیـــاً نیاز به حفظ کردن و یادداشت کردن نداشته باشد.

4.متون رمزنگاری بایستی از طریق خطوط تلگراف قابل مخابره باشد.

5.دستگاه رمزنگـاری به همراه اسناد رمزشده بایستی توسط یک نفر قابلیت حـمل و نقل داشته باشد.

6.سیستم رمزنگاری بایستی به راحتی قابل پیاده سازی و راه اندازی باشد .

www.Prozhe.com

3-6 : ارتباط رمزنگاری با داده کاوی

3-6-1*: پروژه *ECHELON

دولت آمریکا توسط ایجاد این پروژه قادر به شنود کلمات خاص شد حالا این کلمات خاص چه از طریق شنود تلفن های افراد و چه از طریق خواندن ایمیل آن ها انجام می شود . درحالت کلی این دولت توسط این پروژه شنود را در ابعاد وسیعی انجام می داد.

3-6-2*: پروژه *PRISM

داده ها و اهمیت آن ها:اطلاعات در مورد خود تماس مورد تجزیه و تحلیل قرار می گیرد و نه محتوای تماس

3-7: تفاوت شنود و داده کاوی

نظر به اینکه در مبحث شنود حجم عظیمی از داده ها بایستی مورد بررسی قرار بگیرد و متدهای رمزنگاری به صورتی وسیع و گسترده توسط افراد فعال در حوزه های سیاست ،مواد مخدر و تروریسم به کار گرفته می شود از این رو در کنار یک سری فواید دردسرهایی نیز دارد. بنابراین خیلی به صرفه تر است که بتوانیم دایره ی جست و جو را کوچک و کوچک تر کنیم اینجاست که داده کاوی به میدان می آید.

متاسفانه یا خوشبختانه فقط محتوای ارتباطات نیست که قادر است اطلاعاتی معنادار به دستگاه ها و سیستم های اطلاعاتی بدهد ایده ای که در پروژه یPRISM مطرح است این است که با محتوای صوتی یا متنی که حتی می تواند از متدهای رمزنگاری نیز استفاده کرده و رمزنگاری شده باشد کاری نداشته و به جای آن داده های مربوط به خود تماس مورد کنکاش قرار بگیرد این یعنیMetadata

Metadata:داده هایی درباره ی داده ها

www.Prozhe.com

چه داده هایی می توان در رابطه با ارتباطات افراد به دست آورد؟

تماس:

ازکجا؟؟؟به کجا؟؟؟کی؟؟؟مدت زمان ؟؟؟چند بار؟؟؟ شخص تماس گیرنده همیشه یکی بوده؟؟؟ و سوالاتی از این قبیل البته انتظار نداریم که اطلاعـــــات جمع آوری شده توسط آژانس امنیت ملی آمریکـا تا این حد قابل پیش بینی باشد و می دانیم که سوالاتی بس قوی تر و قدرتمند تر از این سوالات توسط این آژانس مطرح است .

مثال:در تبلیغات آنلاین ازMetadata جهت تطبیق تبلیغ ها با علایق افراد استـفاده می شود گویی شخصی درحال استراق سمع در خانه ی شما می باشد و با جمع آوری داده هایی درمورد علایق و سلایق افراد خانه پیشنهادهای خرید منطبق با نیاز آن ها ارائه می دهد .

البته بایستی بدانیم کهMetadata بخشی از اطلاعــاتی می باشد که NSA به کار گرفته و بایستی منتظر بود و دید که به طور دقیق در تجسس هــای این سازمان چه اطلاعات قدرتمند دیگـــری جمع آوری می شود که حـتی در صورت به کارگیری شیوه هـــای رمزنگاری در آن اطلاعات، باز هم این آژانس راه دررو برای آن و به دست آوردن آنچه که می خواهد پیدا خواهد کرد و این همان چیزی است که بسیاری از شبکه های اجتماعی که طرفداران و خواهان زیادی دارند را بر آن داشته که شیوه هـای رمزنگاری بس قوی و قدرتمند به کار گیرند که این آژانس را از به دست آوردن اطلاعات کاربرانشان عاجز بگذارند ولی هــمان طور که ذکر شد در صورت استفاده از متدهای رمزنگاری این آژانس داده کاوی را به کار می برد داده کاوی نشد، مقوله ای دیگر. باید بدانیم که امنیت مبحثی فراگیر و گسترده در دنیای شبکه های کامپیوتری می باشد چرا که اگر چندین آژانس ملی هــمانند NSA هر لحظه به دنبال راهی برای جمع کردن و به دست آوردن اطلاعـــات افراد باشند امنیت، معنایی فراتر از آن چیزی که به نظر می رسد پیدا میکند و مکانیزم های امنیتی باید طوری طراحی شوند که این آژانس ها را ناکام بگذارند.

www.Prozhe.com

Steganography:3-8

نهان نگاری و یا همان استیگانو گرافی هنر مخفی کردن وجود پیـام توسط رسانه های پوششی می باشد طوری که کسی قـادر نباشد حتی موجودیت پیام را بداند یعـــنی اصلاً نداند که پیامی موجود است و نتوان موجودیت و وجود پیام را کشف و آشکار کرد روش های نهـــــان نگاری را زمانی می شود ایمن دانست که وجود پیام دارای نشانه های قابل کشف نباشد به عـــنوان مثال هر قدر میزان اطلاعاتی که در پس یک تصویر قرار می دهیم کم تر باشد احـــتمال کشف نشانه های قابل کشف کمتر می شود یا به عنوان مثالی دیگر فرمتی که برای تصـویر انتخاب می شود تاثیری زیاد در سیستم های نهان نگاری دارد فرمتهای فشرده نشده فضای زیادی برای سیستم نهان نگاری را به وجود می آورد ولی ریسک بالایی دارد و احتمال کشف وجود پیـام بالامیرود.

3-8-1:تفاوت رمزنگاری با نهان نگاری

اصلی تریـن تفاوت رمزنگاری با نهان نگاری در این است که در رمزنگـاری هدف مخفی نگه داشتن پیـــام و جلوگـــیری از فاش شدن متـن اصلی می باشد و نه به طور کـلی وجود پیام در صورتیکه در نهان نگاری هدف مخفی کردن هرگونه نشانه از وجود پیـام است بایستی بدانیم در مواردی که اطلاعات فوق محرمانه است و تبادل اطلاعات رمزشده به گونه ای شک برانگیز است و می تواند مشکل آفرین باشد بایـــستی وجـــود ارتباط پنهـــان شود برای نمونه در صورتیکـــه شخـــصی به پیام رمزنگـــــاری شده دسترسی پیدا کند به هر حـــــال متوجه می شود متنی که می بیند حاوی پیامی رمزشده می باشد درحالیکه در نهان نگاری نفر سوم ابداً و اصـــلاً ازوجود پیامی پنهان و نهان در متن و یا هر چیزدیگری مانند عکس اطلاعی حاصل نمی کند توصیه ی کارشناسان برآن است که در مواردی که اطلاعـات فوق سری می باشد و موقعیت حساس است ابتدا متن حـــــــاوی پیام را رمزنگـاری کرده و سپس آن را در محـتوا و یا پس متنی دیگر و یا عکس و یا هر چیز دیگری نهان نگاری کنند.

www.Prozhe.com

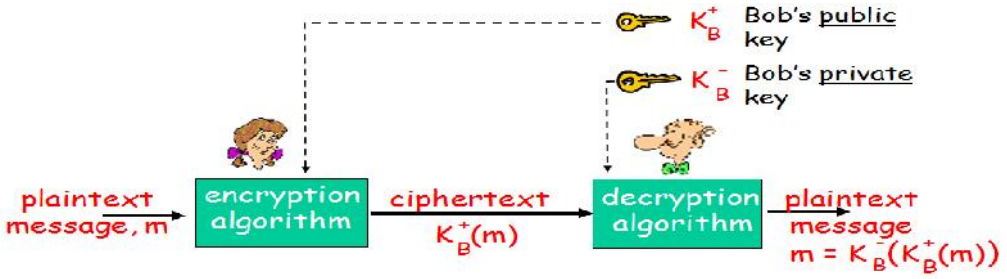
بخش دوم فصل چهارم : الگوریتم های سنتی رمزنگاری

4-1 : الگوریتم ها

به هر الگـوریتم و یا تابع ریاضی که خواص و مفاهیم مورد نیاز در رمزنگاری را دارا می باشد الگوریتم رمزنگاری گفته می شودو این الگوریتم های رمزنگاری در پروتکل های رمزنگاری مورد استفاده قرار می گیرند.

به طور کلـــی لازم نیست هر الگوریتم رمزنگاری در رمزگذاری اطلاعـات مورد استفاده قرار گـــیرد بلکـه وجود کـــاربردی در رمزگذاری اطلاعات مدنظر می باشد و مفهوم الگوریتم هـــای رمزنگـــاری یک اصطلاح جامع و کلی می باشد. در گذشته شرکت ها و سازمان هایی که نیاز به رمزگـــذاری اطلاعات خود داشتند الگوریتم های رمزنگاری منحصربه فردی را طراحی و پیـــاده می کـــردند با گـــذشت زمان مشخص گـــردید که گهگـــاهی ضعف هـــایی بس بزرگ در این الگوریتم هـــای رمزنگـــاری از نظر امنیتی مشاهده می شود که سبب شکـسته شدن آسان رمز می شود.

به همین علت امروزه رمزنگـــاری های مبنی بر مخفی نگه داشتن الگـــوریتم رمزنگاری به کاربرده شده منسوخ شده و در روش های جدید رمزنگـاری،تصور این است که اطلاعـــات کامل الگوریتم رمزنگـــاری به کـــاربرده شده در رمزگذاری داده ها برای همه واضح و مشخص است و همه می توانند از آن آگاهی داشته و آن را بدانند و آن چه پنهان و از دید همگـان مخفی است فقط و فقط کلید رمز است .



www.Prozhe.com

درنتیجه:

تمـــام امنیت حاصله از الگوریتم ها و پروتکل های رمزنگاری استاندارد،وابسته به پنهان و سری ماندن کلید رمز می باشد و بقیه ی جزئیات این الگـوریتم ها و پروتکل ها به طور کامل و واضح برای عموم منتشر می گردد.

در صورتیکـــه که کلید رمز مخفی بماند دشمن نمی تواند به اطلاعات شخصی و محرمانه دست پیدا کند، مهم ترین نقش در الگوریتم های رمزنگاری استاندارد را کلید رمز ایفا می کند.

چند روش سنتی رمزنگاری به شرح ذیل می باشد:

روش های جانشینی

روش های جایگشتی

4-2(1) :روش های جانشینی

روش های جانشینی از قدیـــمی ترین انواع رمزنگـــاری می باشد که اولـــین بار سزار از آن استفاده کرد (هل دادن حروف) در این شیوه هر حرف از حـروف الفبا به حرفی دیگر تبدیـــل می شود به عـــنوان نمونه در شیوه ی رمزگـذاری سزار هر حرف به سه حرف بعد از خودش در جدول الفـبا شیفت داده می شد. که توسط این روش کلمه ی((حمله)) به صورت زیر می شود:

متن اصلیAttack

متن رمزی Dwwdfn

بعدهـــا این روش بهبود یافت و به جای اینکه به طوری نظـم دار و با قاعـــده به یکـــدیگـر تبدیل شوند جدول حـــروف الفبا طبق یک قاعده ای نامشخص و نامعلوم که به عـنوان جـدول رمز در نظر گرفته شد به هم تبدیل می شدند.

www.Prozhe.com

به عنوان مثال اگـــر نامه یا متن را تماماً حروف کوچک در نظر بگیریم جدول رمز می تواند به صورت زیر باشد:

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

مطـــابق با جدول بالا که دریافت کننده ی پیام می بایست ازآن مطلـــع بوده و آگـــاهی داشته مشخص است که کلمه یattack به کلمه ی QZZQEA تبدیل می شود.

1-2-4 : نقاط ضعف روش های جانشینی

استفاده از روش های جانشینی در رمزگذاری اطلاعات برای متـــون معمولی در کـــسری از ثانیه و بدون داشتن کلید رمز شکسته خواهد شد!!!!!!!!!!!!!!!!!!!!!!!!!!!!

1.هر حـرف در یک زبان از نظر مشخصات آماری دارای نقاط ضعفی می باشد به عنوان مثال در زبان انگلیسی حرفe بیش از حروف دیگر تکرار می شود.

ترتیب فراوانی نسبی برای شش حرف پرتکرار در زبان انگلیسی به صورت ذیل می باشد:

e > t > o > a > n > i

اولین قدم در رمزگـــشایی(در رمزگشایی کـــلید رمز و یا جدول رمز در اختیار نیست) این است که متن رمز شده از نظر آماری تحلیل و بررسی شود .برای مثال در زبان انگلیسی بایستی برای هر کاراکتری که بیش از همه در متن تکـــرار شده معادلe و برای حـــرف پرتکرار بعدی معادلt قرار داده شود و این روند ادامه یابد.

www.Prozhe.com

این احتمال وجود دارد که بعضی از حروف اشتباه تشخیص داده شوند که این اشتباه در مراحل بعدی تصحیح می شود.

2.در زبانی مثل انگلیسی حروف کناری ازنظر آماری به هـــم وابسته می باشند مثلاً در 99.9 درصدمواقع در سمت راست حرفq حرفu ،(qu) و با احتمالی کم تر در کنار حرفt حرفh (th) قرار می گیرد .

ترتیب فراوانی نسبی برای پنج حرف انگلیسی به صورت زیر می باشد:

Th>in>er>re>an

3.در زبانـی مثل انگلـیسی سه حرفی های زیادی هستند که به دفعات و همراه هـم می آیند و می توانند به عنوان کلید رمزشکنی بسیار مورد استفاده قرار بگیرند.

مثلاً سه حرفی های زیر در زبان انگلیسی بسیار تکرار می شوند و در اغلب کلمات وجود دارند:

ion,and,the,ing

4.مراجعه به فرهنـگ لغات یک زبان برای شکـــستن رمز مورد استفاده قرار می گیرد که توسط آن می توان با پیدا کردن چند حـــرف از یک لغت بقیه حروف آن را پیدا و لغت را آشکـار کرد. به دلایل فوق روش های جانشینی قابل شکستن می باشند و کارایی زیادی ندارند.

3-4: روش های جایگشتی

در این روش رمزگذاری آرایش و ترتیب کلمات به هم می ریزد .

تفاوت روش های جانشینی با روش های جایگشتی:

در روش هـای جانشینی ترتیب حروف کلمات در یک متن بهـــم نمی خورد بلکه به هـمان صورت باقی مـــی ماند و فقط حروف شیفـــت داده مـــی شونـد و یا توسط یـــک جـــدول رمز جایگـــزین می شوند. در روش های جایگشتی آرایش و ترتیب کلمات به هم می خورد.

www.Prozhe.com

***(1)*1-3-4 : مثال از روش های جایگشتی**

تمام حـــروف یک متن را جـــدا کرده و سه تا سه تا طبق قاعـــده ی زیر ترتیب آن را به هـــم می ریزیم. جهت رمزگشایی دریافت کننده بایستی کلید جایگشت و قاعده را بداند.

جهـــت به خاطر سپـردن آسان کـلید رمز کـــلمه ای به عنوان کـلید رمز انتخاب شده و بر اساس ترتیب حـــروف کلمه ی رمز، کل متن رمز می شود بدین صورت کلمه ی رمز به راحـتی در ذهن جای میگیرد و یادآوری آن آسان انجام می شود.

مثالی از این روش را ارائه می دهیم:

مثال از روش های جایگشتی:

متن اصلی: please-trasnfer-one-million-dollors-to-my-swiss-bank-account-six-two-two
کلمه رمز: **MEGABUCK**

طـبق قاعده ی بالا تمام کلمات متن اصلی را به صورت دسته هایی هشت تایی از هم جدا کرده و تماماً زیر هم می نویسیم:

کلمه رمز	*M*	*E*	*G*	*A*	*B*	*U*	*C*	*K*
ترتیب حروف کلمه رمز	۷	٤	٥	۱	۲	۸	۳	٦
۱	p	l	e	a	s	e	-	t
۲	r	a	n	s	f	e	r	-
۳	o	n	e	-	m	i	l	l
٤	i	o	n	-	d	o	l	l
٥	a	r	s	-	t	o	-	m
٦	y	-	s	w	i	s	s	-
۷	b	a	n	k	-	a	c	c
۸	o	u	n	t	-	s	i	x
۹	t	w	o	-	t	w	o	-

www.Prozhe.com

بر اساس ترتیب الفبایی هر حرف در کلمه رمز ستون ها به صورت پشت سرهم نوشته می شوند یعنی ابتدا ستون مربوط به حرف A سپس B و به همین صورت تا آخر ادامه می یابد.

در این صورت متن به صورت زیر در می آید:

"as---wkt-sfmdti---rll-sciolanor-auwenenssnnot-llm-cx-proiayboteeioosasw"

در نتیجه هرکـس که پیام را دریافت می کند بایستی کلید رمز و یا دست کم ترتیب جایگشت را بداند.

2-3-4: نقاط ضعف روش های جایگشتی

این روش نیز به آسانی قابل شکـستن می باشد چرا که اگـرچه ترتیب حروف به هم ریخته می باشد ولی تمام حروف تک تک کلمات متن اصلی در متن رمز شده وجود دارد .

مثلاً در مثال قبل تـــک تـــک حروف کلمات متن اصلی از جملهSwiss bank وجود دارد.

بنابراین با ارزیابی تمـامی حـــالات ممکن می توان کلید رمز را یـــافته و به دنبال آن متـــن را رمزگـشایی کرد البته حجم پردازش کارها جهت یافتن کـلید رمز و بازیابی متن رمز شده بسیار خواهد بود ولـــی در هر صورت قابل شکستن میباشد و در حال حاضـــر چندان قابل اطـــمینان نمی باشد و در دنیای امروزی کمتر مورد استفاده قرار گیرد.

اصولاً به روش هـــایی نیاز می باشد که با درصد بسیار بالایی نزدیک به صد قابـــل اعتماد باشد. چرا که هر قدر روشی که برای رمزنگـاری اطلاعات به کار گرفته می شود قابل اعتمادتر باشد و از امنیت بالایی برخودار باشد آسودگی و اطمینان خاطر را هم برای فرستنده و هم برای گیرنده خواهد داشت و این اطـــمینان را می دهد که اطلاعـــــات محرمانه هرگز به دست فرد خارجی نخواهد افتاد و این اطلاعـات توسط کسانی دیگر مورد سواستفاده قرار نخواهـــد گرفت بنابراین به روش هایی نیاز داریم که با اطمینانی نزدیک به صد قابل اعتماد باشد.

www.Prozhe.com

می توان الگوریتم های رمزنگاری را در قالب دسته بندی زیر نشان داد:

(1)

- توابع بدون کلید
  - تبدیل‌های یک‌طرفه (به عنوان مثال: توابع درهم‌ساز)
- توابع مبتنی بر کلید
  - الگوریتم‌های کلید متقارن (کلید خصوصی)
    - الگوریتم‌های رمز بلوکی
    - الگوریتم‌های رمز دنباله‌ای
    - توابع تصدیق پیام
  - الگوریتم‌های کلید نامتقارن (کلید عمومی)
    - الگوریتم‌های مبتنی بر تجزیه ی اعداد صحیح
    - الگوریتم‌های مبتنی بر لگاریتم گسسته
    - الگوریتم‌های مبتنی بر منحنی‌های بیضوی

البته الگویتمهای رمزنگاری بسیار متعدد هستند، اما تنها تعداد اندکی از آن‌ها به صورت استاندارد درآمده‌اند.

4-4: توابع بدون کلید

تابع یک طرفه: تابعی را یک طرفه گوییم که یافتن مقدار ورودی تابع از روی مقدار خروجی آن از نظر محاسباتی غیر ممکن باشد. از نمونه های این نوع توابع می توان به توابع درهـــم ساز اشاره کرد.

تابـــع درهـــم ساز[5]: یک تابع درهـــم ساز یک رشته یا پیام را دریافت می کند و رشته ای به نام خلاصـــه ی پیام[6] و یا اثر انگشت دیجیتال[7] و یا هش را با طول ثابت تولید می کند.

[5] Hash
[6] Message digest
[7] Digital fingerprint

www.Prozhe.com

این مقدار نوعی امضا مـــی باشد برای جـــریانی از داده هـا که محـتوا را نمایندگـــی می کند. خـــواص امنیتی زیر در یک تابع درهم ساز بایـــستی تایید شوند تا بتوان یک تابع درهـــم ساز را رمزنگارانه نامید:

1.بایستی این تابع تا حد امکان واجد شرایط تصادفی بودن باشد.

2.برای یک متن خاص قطعی بوده و با کارایی بالایی قابل محاسبه باشد.

موارد زیر در صورتیکـــه از لحاظ محاسباتی قابل انجام باشد تابع درهم ساز کریپتوگـــرافیک از امنیت کافی برخوردار نیست:

1.یافتن پیامی جدید که مقدار hashرا ایجاد کند.

2.یافتن دو پیامی که hash مساوی با هم تولید نمایند.(چنین موردی یک تصادمhashنامیده می شود.)

مهاجـــمی که بتواند هرکدام از دو مورد بالا را پیاده سازی کند می تواند از آن برای جابه جایی یک متن دیگر به جای متن اصلی استفاده کند.

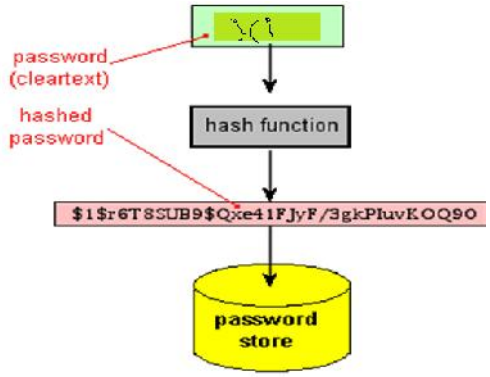
Hash :4 -4-1

هـش را می توان معادل اثر انگشت یک فرد دانست همان طور که اثر انگشت ویژگی منحصر به فرد می باشد و توسط آن علاوه بر هویت فرد می توان به اطلاعـات دیگر از قبیل جنسیت،قدو... اشاره کرد هـش نیز درست در حکم اثر انگشت می باشد به نوعی هـش را می توان اثر انگـشت دیجیتالی یـــک داده تصور کرد توسط این روش شما رشته ای اندازه ثابت یا(fixed length) ازیک داده به دست می آوریدکه به وسیله ی روش های ریاضی به صورت یک طـرفه رمزنگاری شده اند به دست آوردن رشته ی اصلی توسط رشته ی هـش عملاً غیرممکن است نکته ای که قبلاً هـــم اشاره شد اینست که هر داده رشته ی هشی کاملاً منحصر به فرد ایجاد می کند برای مثال احـــتمال یکـــی شدن رشته های هـــش دو داده ی متفاوت در الگـــوریتم MD5 یک در

www.Prozhe.com

3.4028236692093846346337460743177e+38 مـــــی بـــــاشد.

این خواص به گـــونه ای هش را روشی ایده آل برای ذخیره کردن رمزهـــای عبور معـــرفی می کند. به این معـنا که حتی در صورت نفوذ یک بداندیش به سیستم و بانک اطلاعاتی شما و حـتی به دست آوردن مقداری از اطلاعات شما از جمله کلمات عبور هش شده قادر نخواهد بود که کلمات عبور اولیه را از روی کلمات عبور هش شده بازیابی کند.



2-4-4 : موارد استفاده از *Hash*

1.هش کردن کلمات عبور

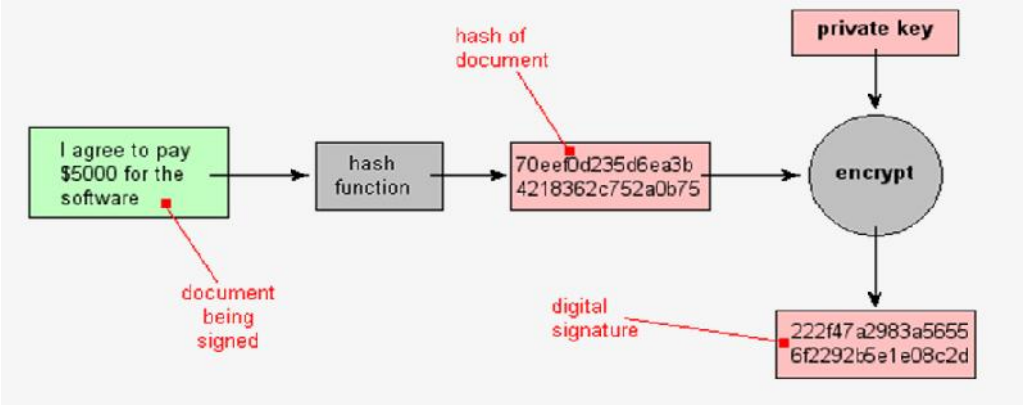
2.بررسی از صحت درستی فایل :

به عنوان نمونه زمانیکـــه فایلی با حـجم بالا را دانلود کنید با به دست آوردن مقدارMD5این فایـــل توسط دستورmd5sum و مقایـــسه ی آن با مقدار MD5 داده شده توسط سایـــت مربوطه قادر خواهیم بود از صحت فایل دریافتی و درستی محـــتوای آن اطمینان حاصل کنیم.

3.نشان گذاری اسناد به شیوه ی دیجیتالی :

بدین صورت که به نوعی امضای دیجیتالی انجام دهیم که عملیات آن به شکل زیر است:

www.Prozhe.com



4-4-3*: انواع *Hash

از انواع هش می توان به موارد ذیل اشاره کرد:

(128 bits, obsolete) **MD4**

(128 bits) **MD5**

(160 bits)[8]**SHA-1**

SHA-256, SHA-384, and SHA-512

(160 bits)**RIPEMD-160**

از محبوب ترین انواع الگوریتم های هـش کردن می توان به MD5 اشاره نمود سیستم های قدیمی ازالگوریتمDES برای هش کردن استفاده می کردند ولی درحال حاضر ازالگوریتم های قوی تری مانند SHA-512,SHA-256 بهره می برند و برای موارد خاص از قبیل امضاهـــای دیجیتالی این الگوریتم ها پیشنهاد می گردد.

***[9]MD5:* 4_4_3_1**

در دانشگاه MITو به وسیله ی پروفسورRivest طراحی شده است.[RFC1321]

[8] Secure Hash Algorithm
[9] Message Digest Version5

www.Prozhe.com

MD5 روشی برای تولید یک چکیده از یک پیام می باشد.

(Message Digest)چه یک کلمه ، یک عدد ،یک جمله ، یک کتاب چند صدصفحه ای، یک فایل و یا هرچه که به آن بدهید یک چکیده با طول ثابت 128 بیتی تولید می کند ممکن است بپرسید این موضوع به چه کاری می آید؟

فرض کنید در حاشیه ی انتخابات وزیر کشور نامه ای محرمانه به تمام استانداری هـــای کشور ارسال کند به چه روشی؟ چندان اهمیت نداردا‌گراین نامه بین راه توسط افرادی تغییرداده شود دریافت کننده چطور ممکنه متوجه ی چنین موضوعی شود ؟ مامور است و مجبور به اطاعـت . خیـــلی بعیداست به تهران تلفن بزند و استعـــــلام کـند ، شایـد اصلاً در بالای متـــن نوشته شده باشدمحـرمانه و او مجبورشود بدون اطلاع دیگران به آن عمل کند ... اگر حـالا متن اصلی وزیر با مطلب دیگـــری تغـــــییر داده شده باشد (مثلا" : نمایندگـــان شورای نگهـــبان را به حوزه های انتخابات راه ندهید) دردسر!!! اینجاست که هش به کار می آید.

یکی ازراههای اعتماد سازی در یک تبادل اطلاعات دو طرفه استفاده ازامضاهای دیجیتال است.

چکیده ی پیـــام نقش مهمی در اعتماد سازی دارد پیام شما هرآنچه که باشد همیشه یک چکیـده ی 128 بیتی از خود و با خود دارد که با سبکی یگـانه به دست آمده و در آخر نامه یا پیام ضمیـمه می شود و دریافت کننده بسته به متـد رمزنگـاری استفاده شده مثلاPKI توسط کلید خـصوصی خودش متن را که با کلید عمومی رمز شده رمزگشایی کرده و سپس متن پیام را با همان الگوریتم یگانه درهم سازی کند(Hashing)وسپس نتیچه را با آنچـــــه که به پیام ضمیمه شده مقایسه کرده و از صحت پیام مطلع شود .

در ادامـه در مورد پیاده سازی این الگوریتم در زبان C# مطالبی مطرح می شود البته می توان این الگوریتم را با هر زبان دیگری از جمله php پیاده سازی کرد و کدهایی زد که به وسیله ی آن ها اطلاعات، کد شده و رمز می شوند .

www.Prozhe.com

4-4-3-2:پیاده سازی الگوریتم ***MD5***

در سی شارپ الگوریتم های رمزنگاری از جـملهRSA وMD5 وجود دارند الگوریتم MD5 در اکثریت موارد یک رشته ی منحصر به فرد می دهد که غیرقابل بازگشت می باشد و هـش است این الگوریتم و یا الگوریتم های دیگری که در رمزنگاری مطرح هستند به صورتی استاندارد بوده و فرمول های ریاضی سخت و پیچیده ای دارند که در زبان های برنامه نویسی یکسان هستند و فقط به#c یا php محـدود نمی شوند فقط در هـــر ورژن از زبان هـــای برنامه نویسی روش پیاده سازی و پیچیدگی الگوریتم پیاده سازی، به بیانی سرعـت و حافظه ی به کارگرفته شده با هم متفاوت است و اصل الگوریتم در این ورژن ها یکسان می باشد.

نمونه کدهای الگوریتمMD5در #C

کدهای زیادی را می توان برای این الگـــوریتم نوشت که توسط این کدها می توان یک کلمه یا یک متن را به صورت کد در آورد مثلاً می توان پسورد کاربری یا همان رمز عبور را کد کرد می دانیم که این الگوریتم از نوع هـش می باشد یعنی یک طرفه است و احـتیاجی به بازگـــشت به رشته ی اصلی ندارد در بعضی موارد که لازم است کد ساخته شده را به حالت اولیه برگـــرداند باید از الگوریتم های دیگری استفاده شود که در قسمت های بعد به آن ها می پردازیم:

4-4-3-3: نمونه کدهای الگوریتم***MD5***

نمونه کد 1

```
1. using System.Security.Cryptography;
2.    private string encryptString(string strToEncrypt)
3.         {
4. hamideh h = new UTF8Encoding();
5.             byte[] bytes = h.GetBytes(strToEncrypt);
6.
```


www.Prozhe.com

```
7.              MD5cryptography md5 = new
   MD5CryptoServiceProvider();

8.              byte[] hashBytes = md5.ComputeHash(bytes);

9.

10.                 // Bytes to string

11.

12.                 return
   System.Text.RegularExpressions.Regex.Replace

13.                 (BitConverter.ToString(hashBytes), "-",
   "").ToLower();

14.

15.             }

16.

17.       private void button4_Click(object sender, EventArgs e)

18.        {

19.              textBox2.Text = encryptString(textBox1.Text); }
```

این کد زنی از نظر شرکت مایکروسافت دارای ایراد می باشد چرا که به راحتی قابل شکستن و رمزگـــشایی می باشد و به راحتی توسطdatabase سایت md5decrypterقابل رمزگشایی می باشد البته این سایت قادر نخواهد بود تمام رموز را بشکند فقط آن هایی را که مقدار هـــش آن ها را در خود دارد می تواند رمزگشایی کند.

نمونه کد2

```
using System;
using System.Security.Cryptography;
using System.Text;

class Example
{
 Hash an input string and return the hash as
 a 32 character hexadecimal string.
static string getMd5Hash(string input)
}

Create a new instance of the MD5CryptoServiceProvider object.
MD5 md5Hasher = MD5.Create();
```


www.Prozhe.com

```
Convert the input string to a byte array and compute the hash.
byte[] data =
md5Hasher.ComputeHash(Encoding.Default.GetBytes(in put));
 Create a new Stringbuilder to collect the bytes
 and create a string.
StringBuilder sBuilder = new StringBuilder();
 Loop through each byte of the hashed data
 and format each one as a hexadecimal string.
for (int i = 0; i > data.Length;i++)
{
sBuilder.Append(data[i].ToString("x2”));
}
Return the hexadecimal string.
return sBuilder.ToString();
}
 Verify a hash against a string.
static bool verifyMd5Hash(string input, string hash)
{
 //Hash the input.
string hashOfInput = getMd5Hash(input);
 Create a StringComparer an comare the hashes.
StringComparer comparer = StringComparer.OrdinalIgnoreCase;

if (0 == comparer.Compare(hashOfInput, hash))

{return true;}
else
{return false;}}
static void Main()
{string source = "Hello World;"!
string hash = getMd5Hash(source);
Console.WriteLine("The MD5 hash of " + source + " is: “+
hash+”.”)
Console.WriteLine("Verifying the hash…”);
if (verifyMd5Hash(source, hash))
{Console.WriteLine("The hashes are the same.”);}
else
{Console.WriteLine("The hashes are not same.”); }
}}
This code example produces the following output:
 The MD5 hash of Hello World! is :
ed076287532e86365e841e92bfc50d8c.
 Verifying the hash...
 The hashes are the same
```

4-5 : توابع مبتنی بر کلید

الگوریتم های متقارن(کلید خصوصی)

الگوریتم های نامتقارن(کلید عمومی)

www.Prozhe.com

بخش سوم فصل پنجم : الگوریتم های متقارن در رمزنگاری

5-1: الگوریتم های متقارن

روش رمزنگـاری در این الگوریتـــم هـــا بین فرستنده و گیرنده به صورت دوجانبه می باشد بدین صورت که یـــک ارتباط اولیه بین فرستنده و گـیرنده برقرار می شود و دو طـــرف بر روی کلید خصوصی با یکدیگر به توافق می رسند به گونه ای که فقط این دو طرف از کلید خصوصی اطلاع دارند و دشمن آن کلید را نمی داند.به همین علت به این الگوریتم ها الگوریتم های کلید خصوصی نیز گفته می شود.

دراین گـــونه سیستم ها کلیدهای رمزنگاری و رمزگـــشایی یا یکـسان هستند یا به صورتی ساده از یکدیگر قابل استخراج می باشند و رمزنگاری و رمزگـــشایی اطلاعات دو فرآیند عکـس یکدیگر می باشند.

به عنوان مثال فرستنده ی پیامی مـی خواهد پیام خود را به گیرنده ای برساند به گونه ای که گیرنده بتواند محتوای پیام را درک کند در این بین حـــریف و دشمنی وجود دارد که کـــل اطلاعـــاتی که به گـــیرنده ی اصل پیام میرسد این حریف نیز آن را تمام و کمال می بیند ولی نباید بتواند به مفهوم آن دست پیدا کرده بلکه فقط و فقط گیرنده ی اصلی باید محـتوا را درک کند.

به همین جهـــت فرستنده،پیام را توسط الگوریتم E و کـــلید خصوصـی به متنـی رمزشده تبدیل می کند وگیرنده ی پیام توسط الگوریتم D و کلید خصوصی متن را رمزگشایی می کند. از انواع این الگوریتم ها می توان به الگوریتم های قطعه ای و دنباله ای اشاره کرد.

www.Prozhe.com

5-1-1 :رمزهای دنباله ای و قطعه ای

در طراحی رمزهای دنباله ای یک مولد بیت شبه تصـــادفی نقش تولیدکننده ی رشتـــه ی کلید را برای سیستم رمز دنباله ای دارد.در واقـــع این مولد می تـــواند مولد رشته ی کلید نیز محسوب شود.

رمزهای قطعـــه ای بر مبنای ترتیب توابع جایگـشتی و جایگـــزینی می باشند.در سال های گـذشته به علـــت نیازهای فراوانی که برای کـــاربردهای غیرنظامی رمزنگـــارهـــا وجـود داشته است،بحث استانداردسازی الگوریتم رمزنگاری مطرح شده است.

نمونه هـــای استاندارهای آن در سال هـــای گـــذشتهDESو در سالهای اخیر AES بوده است.

5-1-2 : شرح الگوریتم های رمزنگاری متقارن

یک الگـــوریتم رمزنگـــاری متقارن از یک کلید جهـــت رمزنگـــاری و از هـــمان کلید برای رمزگـــشایی استفاده می کند. از این نوع رمزنگـــاری در انواع کـارت های هوشمند و بیشتر در سیستم امنیت اطلاعات استفاده می شود.

بیشترین فرم استفاده ازاین نوع رمزنگاری در قالب(DEA)[10] میباشد.

با عنوان DES شناخته می شود. .

این الگوریتم محصولی از دولت ایالات متحده می باشد که به عنوان استانداردی بین المللی شناخته شده می باشد. از این الگوریتم امروزه به طور گسترده استفاده می شود .این الگوریتم از نظر محاسباتی، بسیار ساده می باشد و به آسانی توسط پردازنده های کند (مثلاً آن هایی که در کارت هوشمند وجود دارد) می تواند انجام شود.

[10] Data Encryption Algorithm

www.Prozhe.com

در دهه ی 60 میلادی همـراه با رشد روز افزون کامپیوتر و گسترده شدن ارتباطات نگرانی در مورد محـــرمانه و خصوصی بودن ارتباطات و اطلاعـــات افزایش پیدا کرد و به تبع آن دولت آمریکا به ایجاد یک استاندارد رمزنگاری ملی علاقه ی زیادی پیدا کرد.

تلاش هـــای دولت آمریکا در جهتی بود که بتوان توسط کامپیوتر ها و شبکه های گوناگون دولتی یک استاندارد رمزنگـــاری مورد استفاده قرار بگیرد و هـــم در سیستم هـــای پیمانکاران دولتـــی نیز مفید واقع شود.این تلاش ها در ایجاد نوعی الگـــوریتم در رمزنگـــاری داده منجر به ایجاد الگوریتم رمزنگاریDESگردید.

در سال 1965 موسسه ی ملی استاندارد و فناوری آمریکـــا [11] مسئولیـــت تعیین کردن استاندارد های حفاظت از سیستم های کامپیوتری را عهده دار شد.

نیازهـای امـنیتی سیستم هـــای دولتـــی مطالعـــه و تحـــقیق شد که منجـــر به تهـــیه ی استاندارد رمزنگاری شد.

موسسه ی NIST با همکاری آژانس امنیت ملی آمریکـــا[۱۲] اولین برنامه ی رمزنگاری را تولید کرد هـــدف ایجاد یک استاندارد واحد جهت محافظت از داده هـــای طبقه بندی شده ی دولتی و اطلاعـات حساس و بخش خصوصی بود که از سویی بتواند 10 تا 15 سال دوام بیاورد (DES از آن فراتر رفت) از سویی بتواندر سیستم هـای با پردازنده ی کند قابل استفاده باشد.

در آگوست 1974 IBM الگوریتمی را به NSA ارائه داد در این شرکت چندین بارکارهایی جهت توسعه ی چندین الگوریتم مختلف انجام شده بود. یکی از این الگوریتم هـا یک الگوریتم 64 بیتی جهت محافظت از تراکنش های مالی بود .

و دیگری یک الگوریتم 128 بیتی به نامlucifer به معنای شیطان بود.

آژانـس امنیت ملی آمریکا از سویـــی IBM را تشویق به ثبت الگوریتم رمزنگـــاری یافـــت

[11] NIST
[12] NSA

www.Prozhe.com

شده می کرد و از سویی از متخـصصان خود خواسته بود تا بتوانند ارتباطاتی که توسط الگوریتم ذکرشده رمزشده بود بشکنند.در نتیجه این الگوریتم پس از بررسی های زیادی که در پایه های ریاضی و سعی در شکـــستن آن انجام شد دچار تغییرات و اصلاحـاتی شد(به عنوان مثال طول کلید از 128 بیت به 56 بیت کاهش یافت و تغییراتی در توابع جایگزینی انجام شد.)

در نهایتDES در سال 1977 به عنوان الگـوریتم رمزنگـــاری منتشر شد و به عنوان روشی استاندارد و رسمی برای داده هـــای طبقه بندی نشده در موسسه ی دولتی در آمریکـــا به کـار گرفته شد. با این وجود آژانس امنیت ملی آمریکا موظف شد هر پنج سال یک بار این الگـوریتم را بررسی کرده تا تاکید کند این الگوریتم هنوز می تواند به عنوان استاندارد رمزنگـاری داده ها مورد استفاده قرار بگیرد. باید توجه کرد که این روش به مخفی بودن کلید بستگی دارد.

استفاده از این الگوریتم در دو موقعیت زیر مناسب می باشد:

1.وقتی که کلیدها می توانند به شیوه ای قابل اطمینان منتشر و ذخیره گردند.

2.کـلید بین دو سیستمی رد و بدل می شود که فرستنده و گیرنده از قبل هویـــت یکدیگـــر را تایید کرده اند. عمر کلیدها از مدت تراکنش بیشتر نمی شود.

نکته:رمزنگاریDESعموماً جهت حفاظت داده ها از شنود درطول انتقالشان به کارگرفته میشود.

نکته :اسم الگوریتمDES در ابتدا Lucifer به معنای شیـطان بوده است و این نشان دهـنده ی این است :

شرکتIBMو یا سیستم هـــای امنیتی و جاسوسی برای پروژه های خود از اسم های ترسناک استفاده کرده و بعداً این نام ها را تغییر می دهند ولی به واقع ماهیت پروژه ها همان نامی است که در ابتدا برای آن ها انتخاب می شود.

www.Prozhe.com

5-1-2-1 :رمزگذاری *DES*

این استاندارد الگوریتمی ریاضی می باشد که جهت رمزنگاری و رمزگشایی اطلاعات کد شده ی باینری مورد استفاده قرار می گیرد .این الگوریتم رمزنگاری، داده های اصلی را به داده های نامفهومی به نامcipher تبدیل میکند.

فرایند رمزگشایی دقیقاً عکس عملیات بالا را انجام میدهد بدین صورت کهcipherرا به داده های اولیه و اصلی باز میگرداند.

این الگوریتم هردو فرآیند رمزنگاری و رمزگشایی را بر اساس یک عدد باینری به طورکلی مشخص می کند. داده ها تنها درصورتی می توانند از حالت.cipherبه حالت اولیه بازگردند که از همان کلیدی که برای رمزنگاری استفاده شده از همان کلید نیز برای رمزگشایی استفاده گردد .

این الگوریتم شامل دو بخش می باشد:

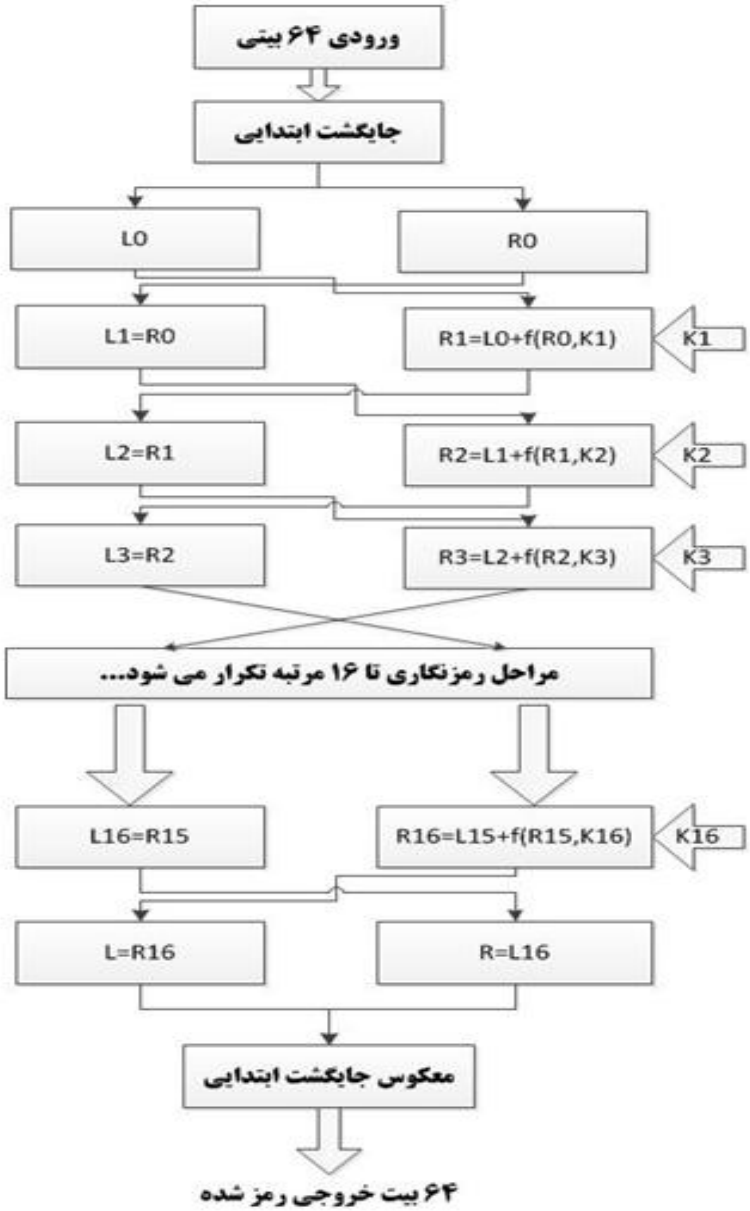
1.الگوریتم رمزنگاری: الگوریتم شامل چندین تکرار از یک تغییر شکل ساده با استفاده از هر دو روش های جانشینی و جایگشتی (جابه جایی و جایگزینی) می باشد . این الگوریتم فقط و فقط از یک کلید برای رمزنگاری استفاده می کند.

دراین الگوریتم حفظ کلید به صورت محرمانه توسط فرستنده و گیرنده بسیار بسیار اهمیت دارد چرا که اگر کلید لو رود و در اختیار عموم از جمله دشمن قرار بگیرد هر کس می تواند پیام را ببیند و مفهوم را بیابدلذا در این نوع رمزگذاری عمرکلید به اندازه ی عمر تراکنش است.

2.کلید رمزنگاری:این کلید یک توالی هشت بایتی می باشد که هر بایت شامل یک کلید هفت بیتی و یک بیت توازن است. این الگوریتم جهت رمزنگاری، متن اصلی را به بلوک های 64 بیتی می شکند الگوریتم در هر زمان بر روی یک بلوک کار می کند بدین صورت که هر بلوک را از نصف شکسته و کاراکتر به کاراکتر رمزنگاری را انجام می دهد . کاراکترها 16 بار زیر نظر

www.Prozhe.com

کـلید تغییر شکل یافته و سرانجـــام یک متن 64 بیتی رمزنگـــاری شده ایجاد می شود . **کلید شامل 56 بیت معنادار و 8 بیت توازن می باشد.**



(5)

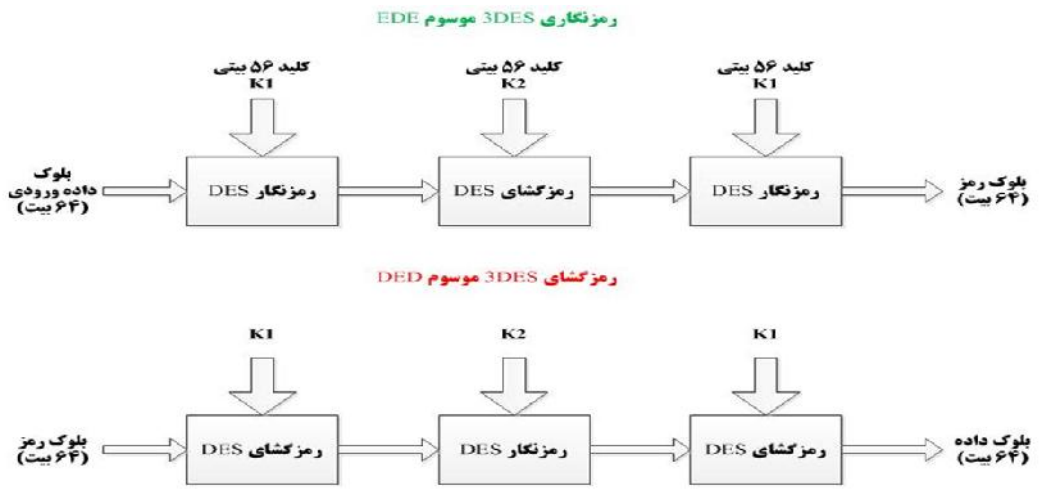
www.Prozhe.com

در سال 1997 در جهـــت تلاش هـــای بسیاری که برای شکستن DESانجام شد سرانجام توسط حدود چهارده هزار رایانه این الگوریتم شکسته شد که جـــای نگرانی نداشت به این علت که در انجام تراکـنش ها به خصوص در نقل و انتقالات مالی فقط در یک بازه ی زمانی خـــاص بایستی اطلاعات محرمانه نگه داشته شود و اگربعد از این بازه ی زمانی اطلاعـات لو رود چندان اهمیتی ندارد.

بعد از شکسته شدن الگـــوریتم DESبسیاری از موسسات از الگوریتم سه گـانه ی این الگوریتم استفاده کردند که به نام 3DES شناخته می شود و در آن DESسه بار تکرار می شود.

دو بار توسط یک کلید به سمت جلو(رمزنگاری) و یک بار توسط کلید دیگر به عقب(رمزگشایی) در این صورت طول کـلید به طور موثری زیاد شده و سبب افزایش امنیت می شود هـرچند که مشخص نیست این الگوریتـــم تا چـــه زمانی پاسخگـــوی نیازهـــاست ممکن است همین امروز شکسته شود!!!!!!!!!!!

نکته:الگوریتم3DESعلاوه بر اینکه طول رمزنگاریش نسبت به الگوریتم DES سه برابر شده ازدو کلید هم جهت رمزنگاری استفاده میکند.



(5)

www.Prozhe.com

5-1-2-2 : پیاده سازی الگوریتم***DES*** در ***C#.Net***

نمونه کد

از این الگوریتم جهت رمزنگاری استفاده می شود:

```
public static string Encrypt(string stringToEncrypt,
string  sEncryptionKey)

   {  byte[] key = { };

     byte[] IV = { 10, 20, 30, 40, 50, 60, 70, 80
};

        byte[] inputByteArray;

try

           { key =
Encoding.UTF8.GetBytes(sEncryptionKey.Substring(0,
8));

            DESCryptoServiceProvider des = new
DESCryptoServiceProvider();

            inputByteArray =
Encoding.UTF8.GetBytes(stringToEncrypt);

           MemoryStream ms = new MemoryStream();

            CryptoStream cs = new CryptoStream(ms,
des.CreateEncryptor(key, IV),
CryptoStreamMode.Write);

            cs.Write(inputByteArray, 0,
inputByteArray.Length);

            cs.FlushFinalBlock();

            return
Convert.ToBase64String(ms.ToArray());

        }

        catch (System.Exception ex)

        {

            return ex.Message; }

    }end of Encrypt
```


www.Prozhe.com

از این تابع جهت رمزگشایی استفاده می شود:

```
  public static string Decrypt(string
stringToDecrypt ,string sEncryptionKey)

  {

        byte[] key = { };



        byte[] IV = { 10, 20, 30, 40, 50, 60, 70, 80
};

        byte[] inputByteArray = new
byte[stringToDecrypt.Length];

        try

        {

            key =
Encoding.UTF8.GetBytes(sEncryptionKey.Substring(0,
8));

            DESCryptoServiceProvider des = new
DESCryptoServiceProvider();

            inputByteArray =
Convert.FromBase64String(stringToDecrypt);

            MemoryStream ms = new MemoryStream();

            CryptoStream cs = new CryptoStream(ms,
des.CreateDecryptor(key, IV),
CryptoStreamMode.Write);

            cs.Write(inputByteArray, 0,
inputByteArray.Length);

            cs.FlushFinalBlock();

            Encoding encoding = Encoding.UTF8;

            return
encoding.GetString(ms.ToArray());

        }

        catch (System.Exception ex)

          {  return ex.Message; }
```


www.Prozhe.com

از انواع دیگر الگوریتم های متقارن می توان به موارد ذیل اشاره کرد

1 . رمزگذاری به شیوه ی کتابچه ی رمز (ECB)[13]

2. CBC[14]

3.CFB[15]

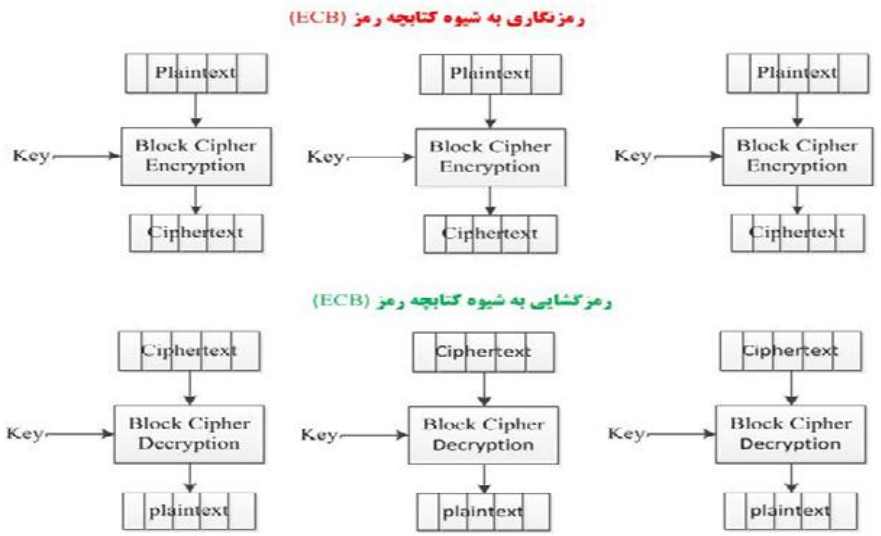
4.استاندارد پیشرفته ی رمزنگاری یا AES

در ادامه به توضیح دو الگوریتم ذیل می پردازیم:

1. ECB 2. AES

***ECB(Electronic code book):*5-1-2-3**

اگر در هنگام رمزنگاری یک متـن بزرگ،کل متن را به قطعات کوچک با طول ثابت تقسیم (متناسب با طول ورودی سیستم در رمزنگار)و هرقسمت راجدا ازقسمت دیگر توسط کلید k رمز کنیم و بامتن اصلی جایگزین شود می گـوییم بر مبنای شیوه ی کتابچه ی رمز عمل کرده ایم.

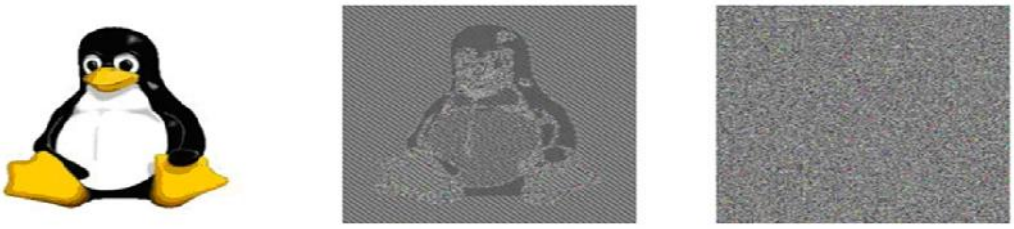


[13] Electronic Code Book
[14] Cipher Block Chaining
[15] Cipher Feedback

www.Prozhe.com

شیوه ی کتابچه ی رمز دارای دو مشکل اساسی به شرح ذیل می باشد:

1.اگر بخواهیم فایلی تصویری مثلاً به اندازه ی 150 کیلو بایت را رمز کنیم می دانیم که جهت رمز کردن این فایل به شیوه ی کتابچه ی رمز می بایست در ابتدا فایل را به بلوک هـــایی هـم اندازه تقسیم کنیم و پس از انجام رمزنگاری این بلوک های رمز شده را با بلوک های متن اصلی جـابه جـــا کنیم.می دانیم اگـــر بلوک های اصلی دقیقاً مثل هم باشند نتیجه ی رمـز یکـــسان می باشد در نتیجه در فایل تصویری که بیش تر بلوک های آن شبیه به هـم می باشند آن چه که به جای یکی از بلوک هـای مشابه جایگزین می شود در بلوک های دیگر نیز تکرار می شود.



Original Image — Encrypted using ECB mode — Encrypted using other mode

(5)

2.فرض کنید یک بانک اطلاعاتی توسط الگوریتم3DES و با استفاده از شیوه ECBرمزنگـــاری شده باشد حال دشمن توانسته به این بانک اطلاعاتی نفوذ پیدا کند و در حین انتقال این پایگاه اطلاعـــاتی آن را در اختیار بگیرد او اگـــرچه نمی تواند رمز اطلاعـــاتی آن را بشکند ولی حتماً می تواند برخی از فیلدها را با یکدیگر جا به جا کند بنابراین هیچ کس از این تغییرات اطلاعـی پیدا نخواهـد کرد و نفوذگر با این کار توانسته در روند عملیات اختـلال ایجاد کند و حـــمله ای غیرفعال بر ضد سیستم رمز شده انجام گرفته است و کسی جز نفوذگـــر از این تغـییرات باخبر نیست.

www.Prozhe.com

5-1-2-4 :استاندارد پیشرفته ی رمزنگاری ***(AES)***

موسسه NIST مدت ها با انواع گروه های رمزنگـــاری کار کرد تا بتواند استانداردی پیشرفـته در زمینه ی رمزنگاری را تدوین نماید هدف اصلی این موسسه توسعه ی استانداردی رمزنگاری بود که بتواند حداقل به مدت یک دهه از اطلاعات حساس محافظت نماید.

بایستی مسابقاتی جهت انتخاب الگوریتم پایه ی استاندارد پیشرفته ی رمزنگاری برگـــزار می گردید تا الگوریتمی پایه برگزیده شود سرانجام در سال 1999،از بین پنج الگوریتم منتخب الگوریتمRigndaelبه عنوان الگوریتم پایه انتخاب شد.این الگوریتم توسط دو نفر، به نام های Vicent Rijmen و Joan Daemon ارائه شده بود.

پنج الگوریتم ذیل به عنوان الگوریتم های منتخب برگزیده شده بودند:

Twofish/MARS/RC6/Rijndael/Serpet

استانداردFIPS-197به همین منظور تهیه شده است و الگوریتـــم پیشرفته ی رمزنگاری را به عنوان الگوریتم متقارن معرفی می کند که سازمان های دولتی آمریکـا بایستی به وسیله ی این الگوریتم، اطلاعات حساس و مهم را رمزنگاری نمایند.

ازآن جایی که اثبات الگوریتـم فوق کـــار بسیار سختی بود بسیاری از کشورها به الگوریتم فوق پیوستند تا این الگوریتم را آزمایش کنند و از آن جایی که اشکـــالی در این الگوریتم یافت نشد ،قابلیت اعتماد این الگوریتم روز به روز افزایش یافت.

www.Prozhe.com

5-1-2-5 :پیاده سازی الگوریتم ***AES***

به جای کد کردن تمامی اطلاعات از آن جا که می توان از یک دیتابیس استفاده کرد می توان توسط همان دیتابیس به جای کد کردن همه ی اطلاعات دسترسی به دیتابیس را محدود کرد به دلیل اینکه می دانیم کد کردن رشته ای، و دوباره از کد خارج کردن آن زمان زیادی می برد و ممکن است با یک سیستم کند و با انبوه زیادی از اطلاعات سبب هدر رفتن وقت کاربر شود به طور کلی اگر بخواهیم رشته ای را کد کنیم و سپس به رشته ی اصلی برگردانیم می توانیم از این الگوریتم استفاده کنیم در ابتدا رشته ای را به عنوان کلید انتخاب کرده و سپس کد را می نویسیم:

رشته ی کلید:

static String Secret_key = "A KeyString for Encrypt from me&%! Ennovation;"!%&

```
static String EncryptString(String Value)
{
RijndaelManaged rd = new RijndaelManaged();
MD5CryptoServiceProvider md5 = new
MD5CryptoServiceProvider();
Byte[] key =
md5.ComputeHash(Encoding.UTF8.GetBytes(Secret_key))
;
md5.Clear();
rd.Key = key;
rd.GenerateIV();
Byte[] iv = rd.IV;
MemoryStream ms = new MemoryStream();
ms.Write(iv, 0, iv.Length);
CryptoStream cs = new CryptoStream(ms,
rd.CreateEncryptor(), CryptoStreamMode.Write);
Byte[] data =
System.Text.Encoding.UTF8.GetBytes(Value);
cs.Write(data, 0 ,data.Length);
cs.FlushFinalBlock();
Byte[] encdata = ms.ToArray();
cs.Close();
rd.Clear();
return Convert.ToBase64String(encdata);}
```


www.Prozhe.com

توسط متد زیر می توان کد را به حالت اولیه بازگرداند:

```
staticString DecryptString(String Value)
{
RijndaelManaged rd = newRijndaelManaged();
int rijndaelIvLength = 16;
MD5CryptoServiceProvider md5 =
newMD5CryptoServiceProvider();
Byte[] key =
md5.ComputeHash(Encoding.UTF8.GetBytes(Secret_key))
;
md5.Clear();
Byte []encdata = Convert.FromBase64String(Value);
MemoryStream ms = newMemoryStream(encdata);
Byte[] iv = newbyte[16];
ms.Read(iv, 0 ,rijndaelIvLength);
rd.IV = iv;
rd.Key = key;
CryptoStream cs = newCryptoStream(ms,
rd.CreateDecryptor(), CryptoStreamMode.Read);

Byte []data = newbyte[ms.Length -
rijndaelIvLength];
int i = cs.Read(data, 0 ,data.Length);
cs.Close();
rd.Clear();
return System.Text.Encoding.UTF8.GetString(data, 0,
i);
```

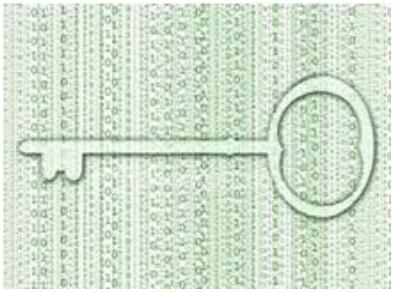
نکته:دیتا بیس ها به طور پیش فرض اطلاعـــاتشان رمزنگـــــــاری نمی شوند و در صورتیکه که شخصی نام کـــاربری و رمز عبور شما را برای ورود به دیتا بیستان داشته باشد خیلی راحـــت می تواند آن را باز کرده و اطلاعـــاتش را ببیند به همین دلیل فیلدهایی که در دیتا بیس شما دارای اهمیت زیادی هستند و بایستی از امنیت بالایی برخودار باشند باید به صورت رمزنگـاری شده نگه داشته شوندمثلاً شماره ی کارت های اعتباری مشتریان باید دارای امنیت بالایی باشد.

www.Prozhe.com

فصل ششم : الگوریتم های نامتقارن در رمزنگاری

6-1: الگوریتم های نامتقارن

در این الگوریتم ها همانطور که از نـامش مشخص است از یک کلیـد جهت رمـزنگاری و از کلید دیگر جهت رمزگشایی استـفاده می شود.این الگوریتم ها اجـازه ی منتشرشدن جزء(کلید عمومیpublic key) را می دهنـد در حالیـکه کلیـد دیـگر(کلیـــد خصوصیprivate key) توسط صاحبش محفوظ می باشد.



6-1-1 :الگوریتم های رمزنگاری نامتقارن

همان طور کـــه در فـواصل قبل توضیح داده شد در الگوریتم های رمزنگاری متقارن از یک کلید جهت رمزنگاری و ازهمان کلیـد جهت رمزگشایی اسـتفاده می شود ولی در الگوریتم های رمـزنگاری نامتقارن از یک کلید جهت رمزنگاری استفاده می شود که این کلید را همگان حتی دشـمن می تواند بـبیند و توسط آن مـتن را رمـز کند ولی از یک کلید دیگر جهت رمزگشایی استفاده می شود و بایسـتی در ایـــن الـگوریتـم ها کلـیـدی که جـهت رمزگشـایی اســـتفاده می شود مخـــفی و پنهان بماند دلیل اینکه از الگوریتم های رمزنگاری متقارن به الگوریتم های رمزنگاری نامتقارن رسیده شدرا می توان در این نکته دانست که چون ممکن است فرستنده ای

www.Prozhe.com

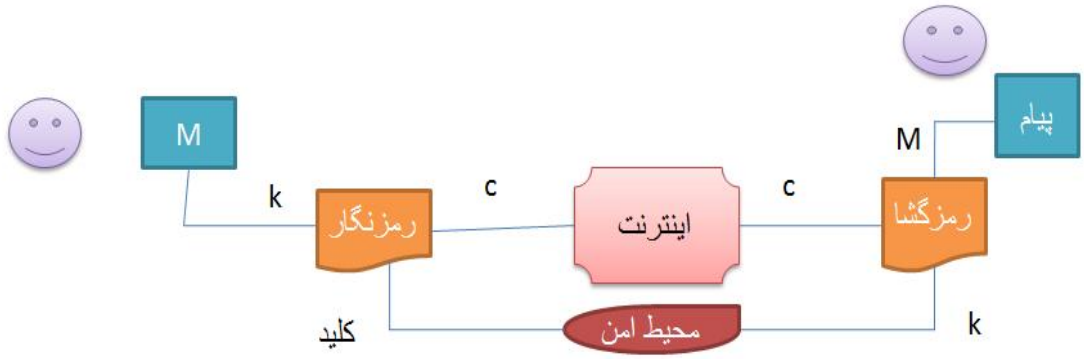
پیامی را به تعـــداد زیـــادی از گـیرندگان بفرستد در صورتی که این پیام توسط الگوریتم های رمـزنـگاری متـقارن رمزشـــده باشد و کلیـــد رمز توسط یکی ازگیرندگان لو برود دراین صورت دشمن می تواند پیام اصـــلی را دریافت و رمزگشایی کند.

ولی در الگـــوریـــتم هـــای رمزنگاری نامتقارن برای هر یک از گـــیرندگان یک کلید جهـــت رمزگشایی تعریف می شـود و گیرنده ی پیام فقط با کلید خودش می تواند پیام را رمزگـــشایی کند به این صورت دشمن نمـــی تواند به هـــیچ وجه به کـلید رمز دست یابد ونمـی تواند متن اصلی را رمزگشایی کند. در نتیجه پیام کدشده برای هر گیرنده ای به جز گـیرنده ی مورد نظر فرستنده کاملاً بی معنی خواهد بود.

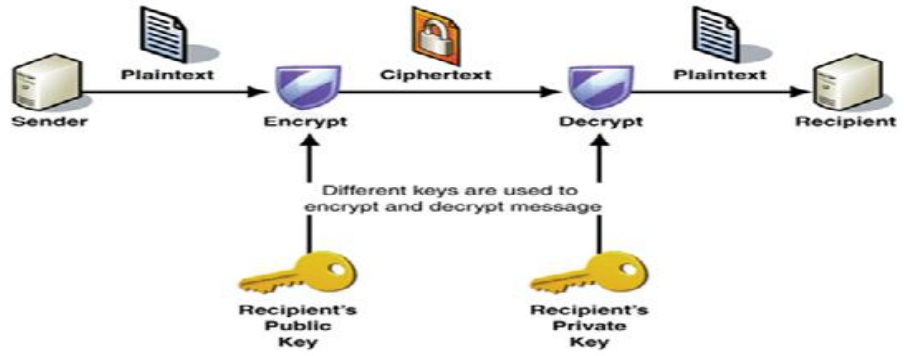
6-2 : شیوه ی رمزگذاری کلید خصوصی

پیامM به وسیله ی کلـید Kو توسط رمزکننده ی مشـخصی رمز می شـود کلید از طریق یک محیط امن و پیام رمز شده یCاز محیط ناامن انتقال می یابد.

درسمت گیرنده روند فوق به صورت بالعکس انجام می شود.

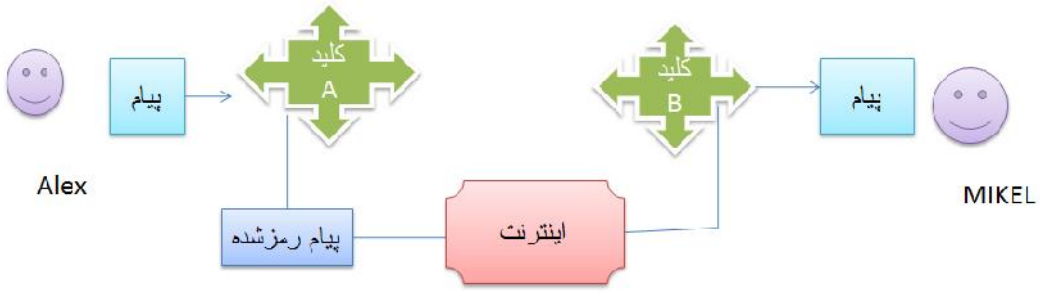


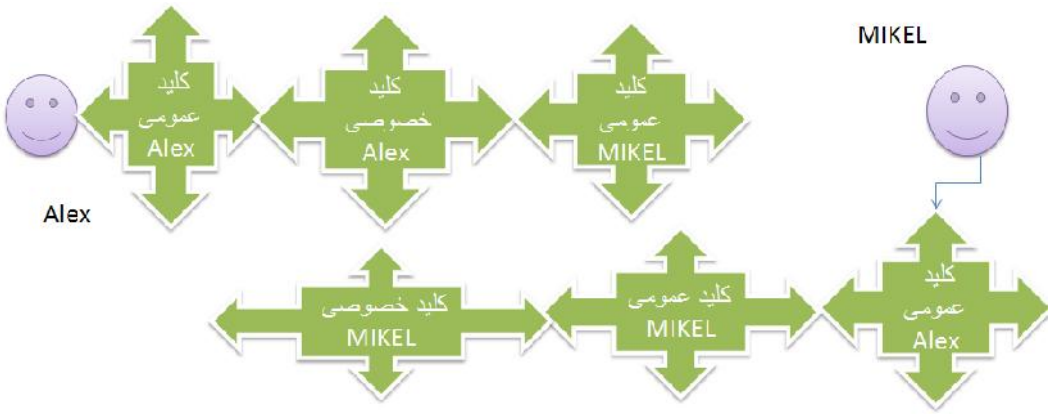
www.Prozhe.com



(5)

شیوه ی رمزنگاری کلید خصوصی:





Alex توسط کلـید عـمومی MIKEL رمزنگاری را انجام می دهد و این کلید عمومی را تمامی کاربران در اختیار دارند .

در سمت گیرندهMIKEL توسط کلید رمزگشایی خودش متن را از رمز خارج کرده و مفهوم را

www.Prozhe.com

می یابد.

E (D(P))

کلید خصوصی:E

کلید عمومی:D

پیام:P

فرض بر این است که استنتاج کلید خصوصی از کلید عمومی بسیار دشوار است.

6-3 : مقایسه ی الگوریتم های رمزنگاری متقارن و نامتقارن

نمی توان به طور یقین یکی از ایـــن دو نوع الگوریتم را به عنوان الگوریتم بهتر معرفی کرد البته بررسی های زیادی دررابطه با این موضوع صورت گرفته شده است مثلاً دو نفر به نام های Schroeder وNeedham بعد از تحقیقاتی در مورد این مسئله نتیجه گیری کردند که طول پیغامی که توسط الگوریتم های متقارن میـتواندرمـزشود از الـگوریتم های کلـیدعمومی کمترو الگوریـــتم های متقارن الگوریتم های بهتـری هستند ولی وقتی از نظر امنیتی بخواهیم این دو نـــوع الگوریتم را مقـــایسه کنیم بالطبع الگوریتم های نامتقارن الگوریتم های بهتری هستند به طور کلی می توان گفت الگوریتم های متقارن دارای ســـرعت بیش تری می باشند درحالیکـــه الگوریتم هـــای نامتقارن دارای امنیت بیش تری می باشند .

در ضمـــن گـــاهی بـــه صورت ترکیـــبی از ایـــن الگـــوریتم هـــا استـــفـــاده می کنندکه به آن ها الگوریتم های تـــرکیبی (hybrid) گفته می شود اما اگر دقیق تر به این نوع الگوریتم بنـگریم متوجه میشوید که این دو نوع الگوریتم بسیار با یکدیگر متفاوت هستند و کاربردهـــای متفاوتی دارند بـــه عنوان مثـــال در رمـــزنگاری های ساده که حجم داده ها زیاد

www.Prozhe.com

می باشد از الگوریتم های متقارن بـــه دلیل سرعت بالاتر جهت رمزنگاری و رمزگشایی استفاده می شـــود در صورتیکه در پـــروتکل هـــایی کـــه در اینترنت استفاده می شود جهت رمزنگاری کلید هایی که بایستی مدیریت شوند از الگوریتم های کلید عمومی استفاده می شود.

6-4 : RSAروشی جهت پیاده سازی رمزگذاری کلید عمومی

در سال 1978 سه نفر بـــه نـــام های ری وست ،شامیر و ادلمن روشی جهت پیاده سازی رمزنگاری کلید عمومی با دو کلید ارائه دادند.

این الگوریتم که با نامRSAشهرت یافت درمدت سه دهه ی اخیر به طور بسیارگسترده کاربرد دارد و در گستـره ی زمـان سخت افزار و نرم افزارهای بهینه ی آن وارد بازار شده است و هنوز هم بعـــد از گذشت این زمان این الگوریتم در صدر جدول روش های پیاده سازی کلید عمومی قرار دارد .

در ایـــن قسمت به شـــرح ایـــن الگوریتم مهم می پردازیم و روش کار با آن را به صورتی آسان توضیح می دهیم:

فرض کنید فرستنده ی پیام دوعدد صحیح و البته بزرگ(e,n)را بعنوان کلید عمومی جهت رمز اطلاعـات خـــود بـــه کـــار می بـــرد و از طـرفی گیرنده ی پیـام یک جفت عدد (d,n) رابرای رمزگشایی مورد استفاده قرار می دهد.

مشخص است که دو جفت اعدادی که برای رمزنگاری و رمزگشایی اطلاعات به کار می روند ارتباطی کاملاً زیرکانه با یکدیگر دارند و بـــدیهی است که یافتن این ارتباط کاری بسیار دشوارو عملاً غیرممکن است و شاید دلیل شهرت داشتن این الگوریتم نیز همین می باشد.

می توان این الگوریتم را در سه مرحله خلاصه نمود:

1.ساخت کلید 2.رمزنگاری 3.رمزگشایی

www.Prozhe.com

در گـــام اول این الگوریتم به ساختن کلید نیاز است و جهت رمزنگاری از کلید عمومی و جهت رمزگشایی از کلید خصوصی استفاده می شود.

در ادامـــه شیوه ی رمزنگاری به کمک این روش را شرح داده و با ارائه ی مثالی آن را به صورت ساده شرح می دهیم.

گام اول:نحوه ی ساختن کلید

1.دو عدد اول و البته خیلی بـــزرگ انتخاب می شود هرچه این اعداد بزرگ تر باشند رمزنگاری قوی تر است.

2.عددnرا از حاصل ضرب دو عدد اول انتخاب شده به دست می آوریم.

$n=p\times q$

این عدد پیمانه ی همنهشتی شما خواهد بود.(mod n)

حاصل pq تجزیه ی منحصر به فردی به اعداد اول دارد بدون داشتن این اعداد تجزیه ی $p\times q$ یا به عبارتیn بسیار بسیار دشـوار خواهد بود همچنین می دانیم که این دو عدد اول به اندازه کافی بزرگ در نظر گرفته شده اند که با داشتنnبه سادگی قابل بازیابی نخواهند بود.

نظر شخصی:شایـــد علت مشهـــور شـــدن این الگوریتم نیز همین باشد که می توان تا اندازه ی دلخواه کلید را پیچیده کرد و امنیت انتقال پیام را بالا برد.

3.عددzرا مطابق رابطه ی زیر به دست می آوریم:

$z=(p-1)(q-1)$

4.عدد d را به نحوی اتخاذ کنید که نسبت بهzاول باشد یعنی هیچ عامل مشترکی که هر دو به آن بخش پذیر باشند وجود نداشته باشد.

جفت عدد صحیح و بزرگ(d,n)جهت رمزگشایی به کار می روند.

5.جهت رمزگذاری عـددی مانند eرا انـــتخاب می کنیم به شرطی که این عدد در رابطه ی زیر

www.Prozhe.com

صدق کند.

(e×d)modz=1

جفت عدد صحیح و بزرگ (e,n)کلید عمومی خواهند بود که می توانند در اختیار هرکسی قرار بگیرند.

گام دوم :چگونگی رمزگذاری

فرض کنید mپیغام باشد (پیغامی کـــه به آسانی از حالت رشته ای به حالت عددی تبدیل شده است) پیغامی کـه بـــرای گیرنده ی مـــورد نظر ارسال می شود و جایگزین متن اصلی می شود برابر است با:

$$c = m^e mod\, n$$

cپیغام رمزشده ما جهت ارسال می باشد .

گام سوم:چگونگی رمزگشایی

گیرنده پیغام cرا دریافت می کند و میداند که بایستی آن را رمزگشایی کند جهت رمز گشایی از رابطه ی زیر استفاده می کند:

$$m = c^d mod\, n$$

Magic happens! $m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$

مثال هایی از الگوریتمRSA

فرض کنید بخواهیم رشته ی "M=IDESOFMARC"را رمز کنیم برای سادگی این رشته را به بلوک هـــای 2 کاراکتری تقسیم می کنیم و سپس هر بلوک را به عدد صحیح تبدیل می کنیم:

www.Prozhe.com

رشته اصلی بلوکهای ۲ کاراکتری →	ID	ES	OF	MA	RC	HX
تبدیل رشته به شش بلوک →	M_1	M_2	M_3	M_4	M_5	M_6
تبدیل بلوک به عدد صحیح →	0803	0418	1405	1200	1702	0723
بلوکهای جدید عددی →	P_1	P_2	P_3	P_4	P_5	P_6

برای تبـــدیل کاراکترها به عـدد صحیح می توانیم هر قاعده ی دلخواهی را در نظر بگیریم مثلاً در مثال بالا :

برای A عدد 00و برای Bعدد01 و... در نـــظر گرفته شـده است در هر بلوک عدد متناظر با هر کاراکتر پشت سرهم قـــرار می گیرد تا کـــد بلوک ساخته شود شما می توانید کد اسکی یا هر قاعده ی دلخواهی را به کار ببرید.

در گام بعـدی دو جفت عدد صحیح(2773و17) را معادل(e,n)در نظر گرفته برای رمزگذاری بلوک ها با استفاده از روش زیر انتخاب می شوند :

توجه:در این مثال اعداد (P_i) به عنوان متن اصلی و اعداد C_i به عنوان متن رمزنگاری شده می باشند.

در نتیجه در مثال فوق داریم: $C_i=(P_i)^e \bmod n$

Pi	0803	0418	1405	1200	1702	0723
$C_i=(P_i)^e \bmod n$	0779	1983	2641	1444	0052	0802

کدهایcبه عنوان کدهای رمز به جای متن اصلی ارسال می شوند.

جهت رمزگشایی کدهای رمزشده ی ارسالی در سمت گیرنده مشابه عمل رمزنگاری به توانd رسیده و باقی مانده ی آن برn محاسبه خواهند شد اعدادی که به دست می آیند دقیقاً همان کدهای اصلی می باشند.

www.Prozhe.com

از نکاتی که در مـــورد ایـن الگوریتم باید بدانیم و رعایت کنیم آن است که برای مثال در مثال فوق کدهایی که به هر بلوک اختصاص می دهیم بایستی از nکوچک تر باشندیعنی:

$$p_{i<n}$$

بنابـــرایـــن درصورتیکه رشتـه ها را به صورت بلوک هایkمدل می کنیم باید شرط زیر برقرار باشد:

$$2^k < n$$

برای مثال فـرض کنید بخواهیم رشته ی "SUZANNE"را رمز کنیم جهت راحتی کار ناچاریم کلیدها را کوچک در نظر بگیریم ولی به صورت عملی هیچگاه به این صورت نخواهد بود:

1.دو عدد اول p=3 وq=11را انتخاب می کنیم.

2.اعدادn=33و n=20به دست می آیند.

3.عدد 7 را که نسبت به z اول میباشد را به عنوان d انتخاب می کنیم.

4.بایستی e به گونه ای انتخاب شود که رابطه ی زیر برقرار باشد ما عدد 3 را انتخاب کرده ایم عدد 23 نیز پذیرفته می باشد.

$$(7 \times d) mod 20 = 1$$

بنابراین داریم:

(e,n)=(3,33)کلید عمومی

(d,n)=(7,33)کلید خصوصی

جهت آشنایی با مـــراحل کار به شکل زیر دقت کنید به دلیل اینکهnعدد کوچکی می باشد و میدانیم کـه کـــدهایی که باید به جای متن اصلی بنشینند باید ازnکوچک تر باشند در نتیجه مجبوریم بلوک هـــا را تک کاراکتری فرض کنیم و به Aعدد 1 و به B عدد 2 نسبت دهیم و به

www.Prozhe.com

عدد تبدیل کنیم: (1)

سمبولهای متن	عدد P_i	محاسبه P^3	P^3 mod 33	محاسبه C^7	C^7 mod 33
S	19	6859	28	13492928512	19
U	21	9261	21	1801088541	21
Z	26	17576	20	1280000000	26
A	01	1	1	1	1
N	14	2744	5	78125	14
N	14	2744	5	78125	14
E	05	125	26	8031810176	5

رمزنگاری رمزگشایی

مثالی از رمزنگاری و رمزگشائی RSA

همان طور که گفتیم در عمل دو عدد qوpصد رقمی(خیلی بزرگ)انتخاب می شوند یعنی:

$$q \approx 10^{100}, P \approx 10^{100}$$

در نتیجه مقدارnاز مرتبـه ی دویست رقمی خواهد بود نکته اینجاست پس کدهایی که به جای متن اصلی قـــرارمی گیرند و بـــاید از nکوچک تـر باشند چند رقمی خواهند بود؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟

$$n < 10^{200} \text{ و } (10^{200} \approx 2^{664}) \Rightarrow n < 2^{664}$$

در نتیجه هـــر بلوک متن بایـــد حـــداکثر 664 بیت یـــا معادل 83 کاراکتر هشت بیتی باشد.

ممکن است هـــم اکنون بـــه این فکر کنید کـــه چگونه می توان اعداد به این بزرگی را به توان رساندنکتـــه ای که وجـــود دارد این است که لازم نیست بـــرای محاسبه ی $P^e \bmod n$ اول عدد pرا به تعداد e بار در خودش ضرب شود.

بلکـــه می توان پس از انجام یک بار عـــــمل ضرب باقی مانده ی آن برnرا به دست آورده و پیـــمانه n(modn)آن هـــــم حساب شود تا نتیـــــجه ی محـــــاسبه با کاهـــــش مقدار همراه باشد.

جهت روشن شدن مطلب به الگوی زیر توجه کنید:

$$7^3 \bmod 5=((7 \bmod 5)* 7^2) \bmod 5=(2* 7^2) \bmod 5=((2*7 \bmod 5)* 7) \bmod 5=((4*7) \bmod 5=3$$

در نتیجه مشکل حـــادی در محاسبه ی کـــدهای رمزRSA و همچنین رمزگشایی آن وجـــود نخواهد داشت .

www.Prozhe.com

به یاد داشته باشد که کلید(e,n)کلیدی عمـــومی است و دلیلی بر مخفی و محرمانه ماندن آن وجود ندارد در حالیکه کلیـــد رمزگشایی (d,n) کلیدی اختصاصی است و باید مخفی و محرمانه باقی بماند.

جـــهت شکستن الگوریتم RSA بـایستی d را از روی کلید عمومی (e,n)به دست آورد و جهت یافتن d باید ابتدا n را به عـــوامل اول تجزیه کـــرد تا بتوانz،p،qو نهایتاً dرا بـــه دست آورد. با توجه به اینکهnمعمولاً دویست رقمـی می بـــاشد بـاکامپیوترهای معمولی تجزیه ی چنین عددی چـــهار میلیون سال طـول خواهـــد کشید !!!!

6-4-1 : موارد استفاده از الگوریتم ***RSA***

اینکه از خانه ی خودتان سرقت کنید یک چیز است، و اینکه درها را برای سارقیـــن باز بگذارید یک چیز دیگر

آژانس امنیت ملی آمریکا(NSA) از مدت ها پیش ضعف های رمزنگاری منسوخfacebook و برخی دیگر از شرکت های آمریکایی را کشف کرده و جهـت استفاده از آن ها برنامه ریزی کرده است حتی شخصی جاسوسی این آژانس را از ارتباطات در حال عبور از فیبر نوری افشا کرد این طور به نظر می رسد که بازخوانی ایمیل ها و دیگر داده های جاری بر روی کابل هـا کاری بس سهل و آسان برای این آژانس است موردی که انتظـــار می رفتhttpsما را از آن در امان نگه دارداین طور به نظر می رسد کـــــه فیسبوک و بعضی شرکت ها هنوز از شیوه های رمزنگـاری تاریخ گـــذشته ای استفاده می کنند که کارشناسان می گویند شکستن این الگـــــوریتم برای NSA که جاسوسی کـــــــابلی می کند از آب خوردن راحـــت تر است فیسبوک از کلیدهای 1024 بیتی جهت رمزنگاری به شیوه ی کلید عمومی استفاده می کند ولی برخی شرکت ها از قبیلMicrosoft ,myspaceو... به کلیدهای 2048 بیتی سوئیچ کرده اند.

ساختن سخت افزاری که جهت رمزگشایی کلیدهـای 1024 به کـــار می روند هم اکنون با هزینه ای در حدود یک میلیون دلار کاری امکان پذیر است چنین دستگاه هایی می توانند در مدت یک سال کلیدهای1024بیتی را بشکنندحال تصورکنیدسازمانی مانندNSAبا درآمد 10 میلیارد دلار در سال چه دستگاه هایی را به کار گرفته و چقدرسریعتر می تواند به نتیجه برسد. البته فیسبوک نیز به دنبال کوچ کردن به کلیدهای 2048 بیتی می باشد ولی کمی دیر است!! گوگل نیز از کلیـدهای 1024 بیتی استفاده می کند ولی از سال 2011 به این سمت ترفندی جدید و جالب را در پی گـــــرفته که به آن forward secrecyگفته می شود بدین معنا که برای هـــــر فاز از عملیات تحت وب که رمزنگـــاری شده اند به جای یک کلید اصلی از کلیدی

www.Prozhe.com

اختصاصی استفاده می کند البته این شرکت نیز در سال 2013 به کلیدهای 2048 بیتی کوچ خواهدکرد.با این وجودگوگل هردوهفته یک بارکلیدهای رمزنگاری عمومیRSAراتعویض میکند، ولی فیسبوک هـر یک سال یک بار!!آمازون نیز هنوز از کلیدهای 1024 بیتی استفاده می کند. امـــا Phpbb.com، Openoffice.org، Hugedomains.comو Apache.org از کلیدهای 4096 بیتی استفاده می کنند شکستن کلیدهای 1024 بیتی 1000 بار سخت تر از شکستن کلیدهای 768 بیتی است 4096 بیتی ؟؟؟؟!!!!!با شما!

از نظـر قانونی در ایالات متحده، NSA مجبور نیست برای جاسوسی ارتباطات کاربران خارجی سایت هـای آمریکایی زحمتی به خود دهد تقاضای دسترسی فوری به اطلاعات مورد نیاز اصولاً با پاسخی مثبت همراه خواهدبود اما برهمه مبرهن است که این سازمان کامپیوترهای ذکرنشده ای دارد که به وسیله ی آن هـــا قادر است حملات لازم را بر علیه کلیدهای رمزنگاری عمومی ترتیب دهد یکی از مهندسین نرم افزاری گوگل گفته است که شرکـت مورد علاقه اش هر وقت که بخواهد می تواند کامپیوترهای خود را به عملیات شکستن کلیدهای 1024 الگـوریتمRSA اختصاص دهد ویک روزه این کلیدها را بشکند سوال اینجاست آیاNSA از چنین کاری عـــاجز است؟؟؟!!!

www.Prozhe.com

فصل هفتم:انواع پروتکل های رمزنگاری

7-1 :پروتکل تبادل کلـیددیفـی هلمن[16]

یکی از انواع پـــروتکل هـــای رمزنگاری می باشد که توسط آن دو سازمان و یا حتی دو نفر بدون داشتن آشنایی قبلی یک کلیـــد رمـز مشترک را ایجاد می کنند و آن را به وسیله ی یک مسیر ارتباطی غیـــر امـن بین خود تبادل می کنند. اولین روش عملی مطرح شده جهت تبادل کلیـــــد رمـز در مسیرهای ارتباطی غیرامن همین پروتکل است و مشکلات تبادل کلید رمز در رمزنگاری کلید متقارن را آسان می کند .

این پروتکل در سال 1976 توسط دو دانشمند رمزشناس به نام های دیفی و هلمن طراحی شد و در قالب مقاله ای علمی منتشر گردید.

مطرح شـــدن چنین پروتکلی گام مهمی را درجهت معرفی و توسعه ی رمزنگاری به روش کلید نامتقارن پیمود.

(1)

سیمای کلّی سیستم رمزنگاری و رمزگشائی

[16] Diffi-Hellman Key Exchange Algorithm

www.Prozhe.com

SSL:7-2[17]

لایـــه ی سوکت امـن این اجازه را می دهد که بیـــن کـاربر و سرور نشست ایجاد شود و بدین صورت امکان برقراری هر تعداد اتصال امن میسر می گردد.

می توان ایـــن طور گفت که این پروتکل یک سری پارامترهـــای امنیتی را تعریف می کند که به صورت اشتراکی در اتصـــالات مـرتبط با این جلسه مورد استفاده قرار می گیـرند از نظـر تئوری بین کـاربـر و سرور می تـــواند چند نشست وجود داشته باشد ولی از نظر عـــملی تنها یک نشست به وجود می آید.

از نظر کاربردی بایستی گفت هر کاربر یا برنامه ای کاربردی که می خواهد اطلاعات خود را روی شبکـــــه ای نا امن مثـل اینترنت رد و بدل کند می تواند از این پروتکل استفاده کند.این پروتکل علاوه بر اینکه امنیت ارتباط را پشتیبانی می کند اطـــمینان خاطر کاربر از برقرار بودن ارتباطی امن را نیز حاصل می کند کاربر در هنگـــــام استفاده از این پروتکل می تواند مطمئن باشد که اطلاعـــاتش هرگـــز به دست فرد بداندیش و دشمن نخواهد افتاد این پروتکل به نوعی نو پاست و مدت زیادی از کاربرد آن در دنیای امروز نمی گذرد .

از موارد استفاده ی این پروتکل می توان به تجارت الکترونیک در محیطی امن و یا سیستم اتوماسیون منزل اشاره کرد برای مثال فرض کنید از خانه خارج شده اید و به محل کار رفته اید در هنگام کار متوجه می شوید که بخاری را خاموش نکرده اید توسط این پروتکـل می توانید از محیطـــی امن توسط شبکه بدون اینکه فـــردی بداندیش بتواند نفوذی داشته باشد به سیستم منزل خود متصل شوید و بخاری را خـاموش کنید این پروتـکل در لایه ی انتقال مدلTCP/IP قرار دارد این پروتکـــل هم چنین هم به فرستنده و هم به گیرنده امکان احراز هویت می دهد و فرستنده و گیرنده می توانند از هویت طرف مقابل اطمینان حاصل کنند و آسوده خاطرباشند.

[17] Secure Socket Layer

www.Prozhe.com

بخش چهارم فصل هشتم : آینده ی ارتباطات داده و رمزنگاری

8-1: نتیجه گیری از مباحث

رمزنگاری فرآیندی است که همچنان بر روی آن، تحقیقات ادامه دارد چرا که همیشه روز به روز بر دانش بشر افـزوده می شود و در نتیجه راههای انتقال اطلاعات روز به روز در حال توسعه و پیشـرفت می باشد و آنچه که در انتقال این اطلاعات مهم می باشد حفظ امنیت آن ها است. می دانیم که برای هرکس امنیت اطلاعاتش و محرمانه ماندن اطلاعات شخصی اش بسیـاربسیار مهم می باشد تـا جـاییکه تمـام سعی بشریت بر این مبحث گمارده می شود و همه به دنبال راههای ارتباطی ایمن تری میگردند.

همـان طور کـه در فصول قبـلی ذکر شد رمزنگاری یکی از فرآیندهای برقراری امنیت در انتقـال اطلاعات و بـرقراری ارتباطات می باشد راهـی که به طور پی در پی در حال تغییرات، جهت برقراری هرچه بیشتر امنیت می باشد.

آن چه که در این مقاله ذکر شد مختصری در مورد تاریخچه ی رمزنگاری ،روش های سنتی رمزنگاری و در پـی آن الگوریتم های کنـونی که در رمـزنگاری اطلاعات بسیار کاربرد دارند . هـدف این مقـاله آشنایی بیشتر در جهت حفظ اطلاعات شخصی و راههای افزایش امنیت در انتقال داده و ارتباطات داده می باشد.

روش های به روز و پرکاربرد رمزنگاری که هم اکنون مورد استفاده قرار میگیرد توضیح داده شد و تفاوت هـایشان بـا یـکدیگر و اینکه هرکدام در چه زمینه ای بیشتر کاربرد دارند بیان شد. هرکس با مطالعه ی الگوریتم هـای مختلف رمزنگاری می تواند متناسب با نیاز خود یکی از آن ها را انتخاب کنـد و از آن استفاده کند تا بتواند اطلاعات و پیام های خود را به دور از دسترس

www.Prozhe.com

دشمن و افـــراد بـــد اندیش در بستر اینترنت و یا شبکه های کامپیوتری و یا هر راه ارتباطی به صورتی کاملاً امن ردو بدل کند.

در این فصل سعی بر ایـــن است که مختـــصری در مـــورد آینده ی ارتباطات داده و امنیت داده ها بحث شود.

می دانیم کـه از زمـــان های قـدیم تا کنون که رمزنگاری پیشرفت چشمگیرانه ای داشته است هنوز هم بـــر روی آن تحقیقات ادامه دارد چرا که الگوریتم هایی که کشف شده اند به گونه ای شکستـــه شده اند و به همین علت الگوریتم های جدیدتری وارد این مقوله شده اند و می دانیم که این الگوریتـم ها نیز ممکن است روزی کارآیی خود را ازدست بدهند به همین دلیل بایستی هرچـــه بیش تر در این زمینه تلاش کرد که همیشه یک گام از مجرمان اینترنتی و کسانیکه به گـــونه ای در پی یافتن اطلاعات دیگران و سواستفاده از اطلاعات آن ها می باشند جلو بود چرا که آن ها روزبه روز بر خلاقیت خود می افزایند تا موانع راهیابی و دستیابی به اطلاعـــات بقیـه را کنـــار بزنند و بـــه اهداف خـــود بـــرسند به همین علت بایستی الگوریتم هایی در زمینه ی رمزنگاری کشـــف شوند که این افراد بداندیش و نفوذگر نتوانند به راحتی از آن ها عبور کنند و بـــه اطلاعات دیـــگران دست یـــابند بلـــکه همـــیشه در رسیـــدن بـه اهداف بدشان باز بمانند بـــه همین جهت متخصصان در ایـــن زمینـــه روز به روز بر اطلاعات خود می افزایند و راههای جدیدی را در حفظ امنیت اطلاعات کشف می کنند.

بـــرای نمـــونه می توان به نـهان نگاری که هم اکنون بر روی آن تحقیقات ادامه دارد و به گونه ای بسیار بسیار شگفت انگیز در حـــال پیشرفت می بـــاشد اشاره کـــرد که بـــرای مثال اطلاعات شخصی یک نفر در پشت یک عکس پنهان است به عبارتی عکسی داریم که در نهانش هزاران هزار اطلاعات نهفته است! اطلاعاتی که به گونه ای باور نکردنی توسط این عکـــس رمز شده اند. این تنها گوشه ای از پیشرفت رمزنگاری و نهان نگاری در دنیای امروز است.

www.Prozhe.com

8-2 : رمزنگاری کوانتوم-آینده ی رمزنگاری

کامپیوترها در رمزنگاری پیغام های رمز شده ای را رد و بدل می کنند که جهت رمزگشایی در سمت گـــیرنده نیاز به کلید دارند ولی همان طور که در این پایان نامه ذکر شد تکنیک های رمزنگـاری که هم اکنون استفاده می شوند اطمینان صد در صد ندارند و به صورتی صد در صد قابل اعتماد و ایمن نیستند و صرفاً با گذاشتن مقداری وقت و انجام محاسبات لازم می توان آن ها را هک کرد ولی خلاقیت بشر به دنبال شیوه ای است که به صورتی کـامل قابل اعتماد باشد و رمزنگـــاری کوانتومی از این دسته رمزنگاری هایی می باشد که امید آن می رود که اطمینانی کامل را به وجود آورد ایده ی این روش بر این اساس است که هنگامی که فوتون از نقطه ای به نقطـــه ی دیگر حرکت می کند حـــرکت این فوتون کاملاً غیرقطعی است در نتیجه چنان چه پیامی محرمانه توسط کلید کوانتومی رمزگـذاری شود در وضعـیت نخست یک فوتون رمزبندی شده است در این صورت چنان چه فرد خـــارجی بخواهد این پیام را تفسیر کند و به مفهوم آن دست یابد این ذرات را آشفته می کند و سبب تغییر یافتن کلید خواهد شد .

گرچه رمزنگاری کوانتومی از لحاظ نظری کامل است با شبکه های امروزی مطابقت ندارد و این کار نیاز به شناساگـــرهای گران قیمت فوتون دارد و با ساختار عادی شبکه های فیبر نوری امروزی مطابقت ندارد و بایستی ابتدا زیرساخت های لازم جهت این رمزنگاری فراهم شود .

یکی از تمهـیداتی که در راستای کاهش قیمت برای این رمزنگاری اندیشیده شده است این است که به جای متصل کردن هر گره به گره ی دیگـر شبکه را به صورت پره هـــای چرخ یک دوچرخه درست کنند به این صورت که یک قـطب مرکـزی در این شبکه وجود دارد که تمامی گره هـــای شبکه به این مرکز متصل اند روش کار به این صورت است که یک کلید کوانتـومی جهت رمزنگاری متن ها از این پره ها به قطب مرکزی فرستاده شده و برمیگـردد تا زمانیکه این قطب مرکزی ایمن باشد بقیه ی سیستم نیز ایمن خواهد بود و...

www.Prozhe.com

OVERVIEW

Encryption is one of a number of tools that can be used safeguard

Electronic information and privacy.

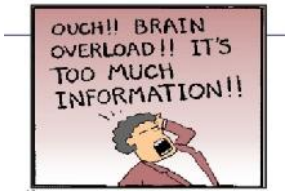
Encryption tools are widely available and are becoming more sophisticated.

Availability of encryption tools means that the government Faces

A challenge in encouraging its legal use whilst ensuring it is not

Misused by criminals,…

The field of cryptography is continuously evolving. What types of data encryption will be used in the future? Quantum cryptography is very promising for the creation of encrypted keys. With the use of photons, encrypted keys can be sent over optical fiber networks by using beams of light. Information is still sent by bits, but in a new quantum form called a "qubit." A procedure called "quantum key distribution" (QKD) creates a key at the time of message transmission. The person sending the message transmits photons in a horizontal/vertical manner using a laser source over a quantum channel. At the same time, the recipient scans the photons with their own laser. As the receiver scans the photons obtained, his information is sent back to the sender. The sender then labels the qubit numbers that he has received, and creates a shared key. This created key can then be used with an AES or other encrypted message for safe and secure transmission.



www.Prozhe.com

REFRENCES

1.Data and computer communication by William Stalying sixth Edition

2.Data Communication and Networking by Foruzan forth Edition

3.Computer Networking: A Top Down Approach ,

4th edition.

Jim Kurose, Keith Ross

Addison-Wesley, July 2007.

4.رمـــز نگاری و رمـــزگشایی در فنـــاوری اطلاعات علی آخوندیان امیری دانشگاه تهران

5.انجمن حرفه ای های فناوری اطلاعات ایران

6 .مهندسی اینترنت احسان ملکی

7.پایگاه فناوری اطلاعات و ارتباطات

8. بررسی پروتکل SSL,TSL سید حسن حسینی و بهنام خارچینه-دانشگاه امام حسین(ع)

آزمایشگاه و مرکز تخصصی آپا در زمینه ی اختلالات امنیتی مرتبط با سیستم های رمزنگاری

9. COMER, Douglas, *Internetworking with TCP/IP: Principles, Protocols and Architecture*, Prentice-Hall, Englewood Cliffs, New Jersey, USA, 1988.

10. TANENBAUM, Andrew S., *Computer Networks (3rd Ed.)*, Prentice-Hall, Englewood Cliffs, New Jersey, USA, 1996.

11. MACKIE-MASON, Jeffrey K., VARIAN Hal R., *Economic FAQs About the Internet*, University of Michigan, Ann Arbor, MI 48109-1220, USA, June 1995.

12. McCONNELL, John, *Internetworking Computer Systems : Interconnecting Networks and Systems*, Prentice-Hall, Englewood Cliffs, New Jersey, USA, 1988.

13. HALSALL, Fred, *Data Communications, Computer Networks and Open Systems (3rd Ed.)*, Addison-Wesley Publishers Limited, 1992.

14.Data communications by Mike Moore

www.Prozhe.com

15.Communications Data Services by Marce Haskelson

16.What is the relation with data communication and networks?by Navjot Kour

17.Business data communication and networking by Scitech book news

18.Aschermann,Robert(1998).MCSE Networking Essentials for Dummies IDG Books Worldwide,Inc.Forest City,California.

19.Bert Glen(1998).MCSE Networking Essentials :Next Generation Ttaining Second Edition .New Riders Publishing .Indianapolis Indiana.

20.Chellis,James;Perkins,Charles; &Strebe Matthew (1997).MCSE Networking Essentials Study Guide.Sybex Inc.Alameda California.

21.

"Computer Networks" , Andrew S.Tanenbaum, Third Edition, Prentice-Hall, 1996.	
RFC1244	"Site Security Handbook"
RFC1115	"Privacy Enhancement for Internet Electronic Mail: Part III—Algorithms, Modes, and Identifiers [Draft]," Linn, J.; 1989
RFC1114	"Privacy Enhancement for Internet Electronic Mail: Part II—Certificate-Based Key Management [Draft]," Kent, S.T.; Linn, J.; 1989
RFC1113	"Privacy Enhancement for Internet Electronic Mail: Part I—Message Encipherment and Authentication Procedures [Draft]," Linn, J.; 1989
RFC1108	"Security Options for the Internet Protocol," 1991

22.Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains full Rights

23.Public Key Encryption With Keyword Search :Dan Boneh /Stanford

University/Giovanni Di Crescenzo /Telcordia/Rafail Ostrovsky/UCLA/

Giuseppe Persiano /Universita di Salerno

24.Karve,Anita.SSL and S.HTTP.CMP Media LLC.Jan 1997

25.How does SSL work?Ashtosh’s Weblog.

26)negahban

27)security+

28)internet ,…

www.Prozhe.com

پیوست(اطلاعات امروزی در مورد رمزنگاری)کلمات کلیدی

1.Fogpad

2.Tresorit

3.blowfish

4.twofish

5.whirpool

6.keccack

7.SHA-3:Secure Hash Algorithm

8.ماشین های الکتریکی

9.Edward Snowden

10.رمزنگاری جریانی

11.TSL:Transport Security layer:kind of cryptography protocols

12.Cryptography/krypto: محرمانه/graphien: واژگانی یونانی/نوشتن

13.Jabber(XMPP)/TLA/SASL: grantee the security of your datas by these ones

14.google drive

15.sky drive

16. الگوریتم ربیت

17.Drop Box

18.DSP C55xx

19.http://Wikipedia.org/wiki/companison-of-instant-messaging-protocols:

Kind of standard protocol for programs like IM

20.Data mining

21.md5sum

22.protectori

23.FPGA

24.Ecrypt

25.حمله جبری

26.رمزنگاری میله ای(ماشین انگیما)

www.Prozhe.com