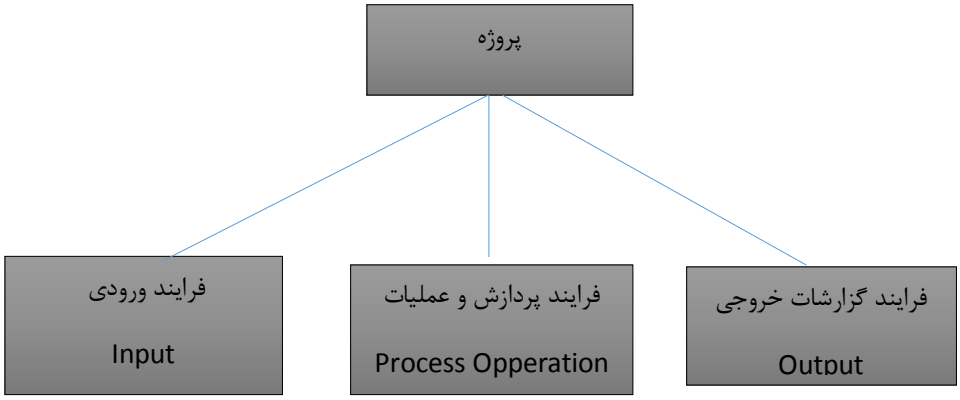
۱۵- در طراحی پروتکل لایه شبکه ۱۰ اصل کلی وجود دارد که بایستی هنگام طراحی در نظر گرفته شود؟

۱- اطمینان از عملکرد صحیح: یعنی مطمئن شویم که طراحی درست و دقیق انجام گرفته و در عمل به اشکال بر نمی خورد.
۲- پروتکل را ساده طراحی کنید: یعنی اگر ویژگی هایی اضافی و زائد است آن ها را حذف کنیم.
۳- تصمیمات روشن و شفاف بگیریم: یعنی از بین چند مدل طراحی یکی را بطور دقیق و شفاف انتخاب کنید.
۴- طراحی شما ماجولار باشد. منظور از ماجولاریتی این است که یک پروژه بزرگ به بخش های منطقی شکسته شود بطوریکه هر بخش در برگیرنده وظایف کاملا مشخص و مرتب و نزدیک به هم باشد مثلا یک پروژه اتوماسیون نرم افزاری می تواند بصورت زیر ماجولار شود.



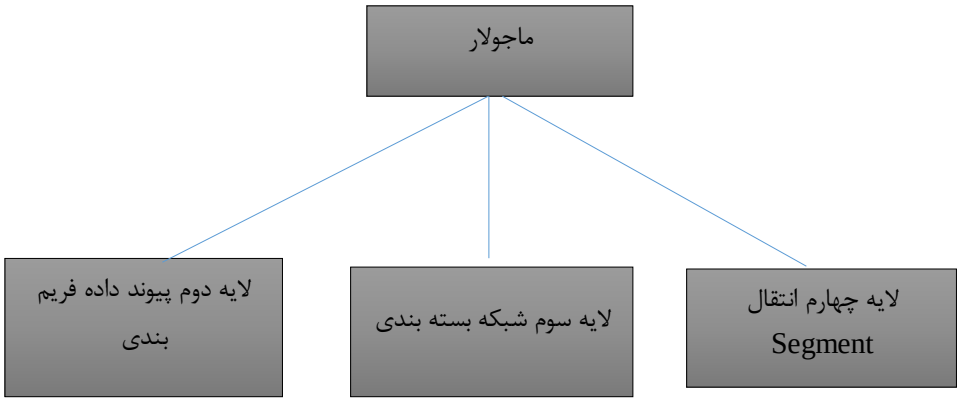

این ماجولار خوب است و کارها شکسته شده و انجام می شود.

نکته ۱ : ماجولاریتی می تواند سبب شفافیت و تقسیم پذیری یک پروژه بزرگ باشد و پیچیدگی آن تا حد امکان کم کند.

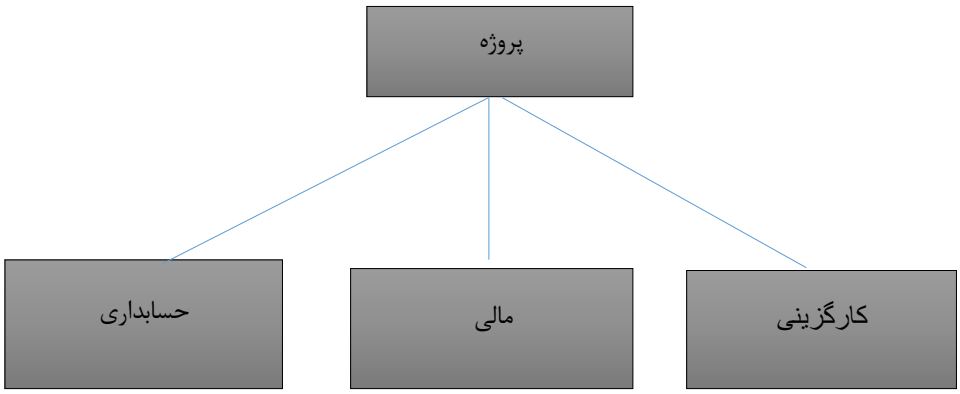
نکته ۲ : یک ماجولاریتی مطلوب آن است که دو ویژگی داشته باشد:

۱- اتصال یا انسجام داخلی Conesion : یعنی مولفه های داخلی لایه طراحی شده بطور مثال لایه شبکه کاملا مولفه های مرتبط به هم و دارای پیوستگی و انسجام بالا داشته باشند.

۲- جدا پذیری Coupling : یعنی مولفه های نامرتبط و دور از هم کاملا جداگانه و تفکیک یافته و بدون اشتراک طراحی شوند. بطور مثال در لایه شبکه لازم است که نام پروتکل شبکه و طول عمر بسته (TTL) و ورژن IP گفته می شود. اما لازم نیست که در این لایه مشخصات مربوط به فریم لایه ۲ یا Segment لایه ۴ چیزی درج شود. همچنین در لایه ۴مشخصاتی همچون شماره قطعه، پورت، ورودی و خروجی و مشخصات Ack.no و بافر مقصد می یابد و اما لازم نیست نوع پروتکل لایه شبکه و طول عمر بسته نیز اضافه شود. بنابراین هر لایه بطور جداگانه طراحی شده و در عین حال لایه های مختلف کاملا مستقل می باشند.




این ماجولار خوب است و کارها شکسته شده و انجام می شود.

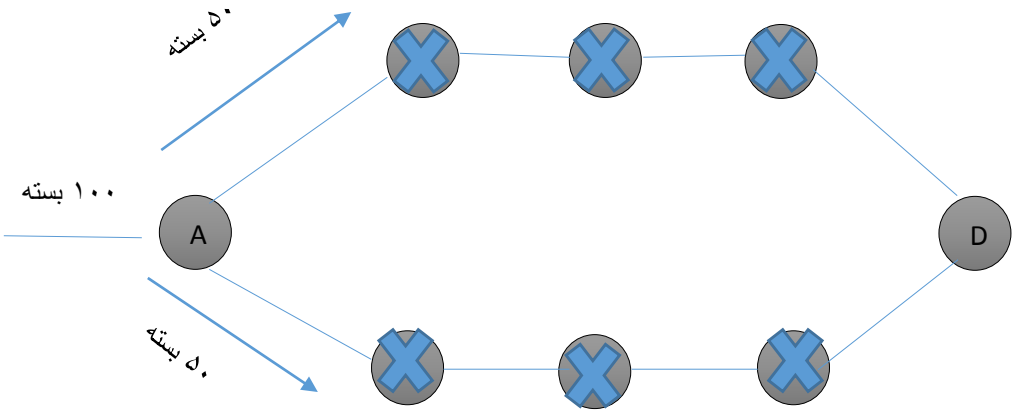



این نوع ماجولار درست نیست چون کارها بطور مستقل شکسته نشده اند و در هر بخش کارهای تکراری و وابسته به بقیه بخش ها وجود دارد و دارای ماجولارهای مشترک می باشند.

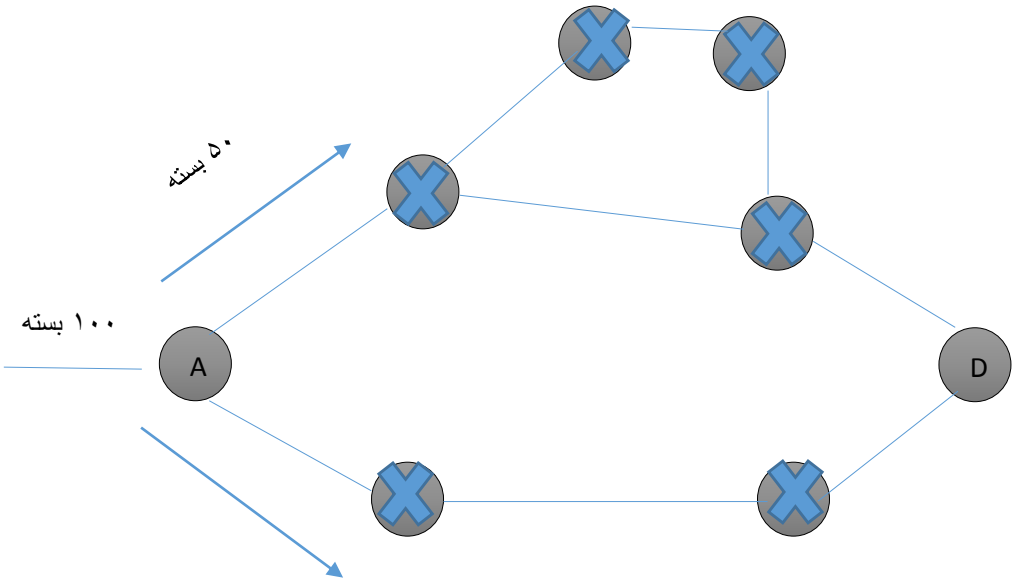
۵- ناهمگون بودن عناصر شبکه را در نظر بگیرید: زیرا در یک شبکه بزرگ سخت افزارها و امکانات مخابراتی و برنامه های کاربردی دارای ساختار و تکنولوژی متفاوتی می باشد و می بایستی که بصورت انعطاف پذیر و سازگار مدل مربوطه از این عناصر استفاده کنند.

۶- از گزینه ها و پارامترهای ثابت پرهیز کنید: زیرا این گزنیه ها می توانند برای نفوذگر اطلاعات خوبی را به آنها بدهد مثل اینکه طول حداکثر بسته ۶۵۰۰۰ بایت است یا TTL آن برابر ۲۰ باشد.

۷- دنبال طراحی خوب باشید: در واقع طراحی شبکه بایستی با حداقل هزینه و حداکثر بهروری باشد. مثلا اگر تعداد ۶ روتر یا مسیریاب داریم برای انتقال داده مسیریابی تپولوژی آنها به نحوی طراحی کنید که همه آنها در مسیریابی شرکت کنند مانند شکل زیر




شکل بالا دارای یک طراحی خوب است و بسته ها بطور مساوی از هر دو جهت عبور می کنند ولی در شکل زیر از طراحی مناسب برخوردار نیست چون در یک طرف حلقه ایجاد شده و همیشه در گره انتهایی ترافیک وجود دارد.




۸- هنگام ارسال بسته داده سخت گیر و مطابق استاندارد بفرستید و هنگام دریافت سعی کنید استانداردهای مختلف را بپذیرید.

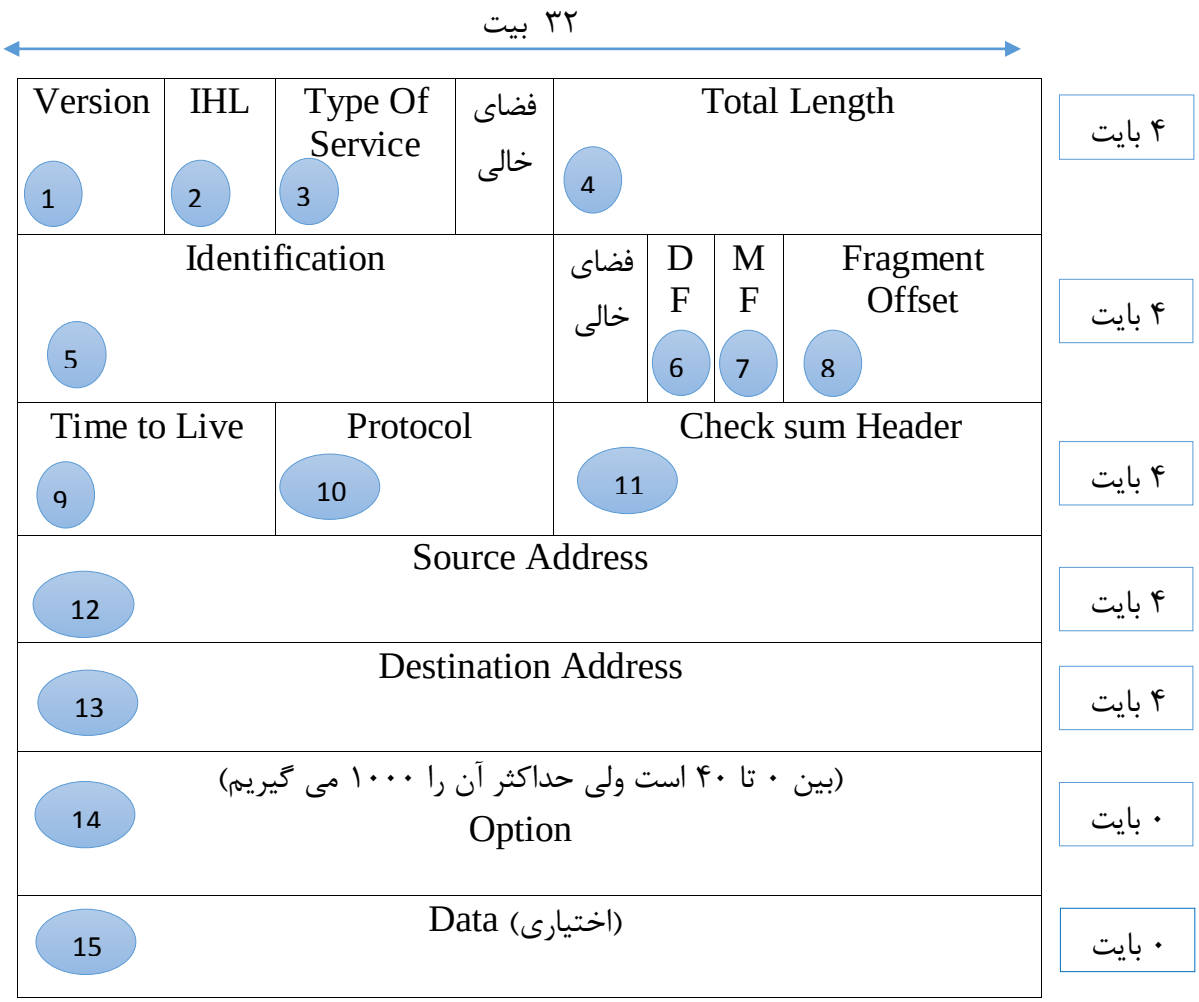
۹- در اندیشه قابلیت و گسترش و توسعه پذیری باشید: یعنی تلاش همواره پهنای باند بیشتر و سوئیچ های با پورت بیشتر و نرم افزارهای شبکه یا کاربران بیشتر بپذیرد.

۱۰- بکارایی و هزینه دقت داشته باشید: یعنی به ازای هزینه که می کنیم حداکثر بهروری و کارایی را داشته باشیم مثلا از توان سرور و حداکثر پهنای باند استفاده کنیم.

۱۶- پروتکل IP را بیان کنید؟

ساختار یک بسته IP شامل دو بخش می باشد مانند ساختار قطعه TCP یک بخش سرآیند و یک بخش محتوا دارد.

ساختار یک بسته IP ورژن ۴ در پروتکل اینترنت بصورت زیر می باشد:




سرایند ۲۰ بایت است و داده ۶۴ کیلو بایت معادل ۶۵۵۳۵

Version : این فیلد مشخص می کند که نتیجه پروتکل IP کدام است. IP ورژن ۴ یا ۶ است.

مطالعه در مورد IOT(Internet Of Things) که نفوذ در اینجا الان صورت می گیرد.

IHL : این عدد تقسیم بر ۴ می شود و اندازه سرایند را مشخص می کند. حداقل اندازه ۵ و حداکثر ۱۵ می باشد.

$$۵ < IHL < ۱۵ \qquad ۲۰ < IP\ Size < ۶۰$$

Type Of Service : نوع خدمات- این فیلد کلاس های مختلف خدمات را مشخص می کند. مثلا خدمات قابلیت اعتماد و سرعت را برای یک سیستم می توانیم تقاضا کنیم. بطور مثال برای انتقال موسیقی سرعت مهم تر از قابلیت اطمینان است. این فیلد شامل ۶ بیت است.

| Precedence | Delay | Throughput | Reliability |
|---|---|---|---|
| تقدم | تاخیر | ظرفیت یا توان خروجی | قابلیت اعتماد |
| ۳ بیت | ۱بیت | ۱بیت | ۱ بیت |

اولویت عمومی در ۶ حالت است اولی game و اخری بیت بالاترین اولویت و کنترلی است که در قسمت سه بیتی براساس آنچه که اولویت دارد مشخص می شود

000 ، 001 ، 010 ، 100 ، 101 ، 110 ، 111

احتمال ۱۱۱ امکان ندارد چون هر سه در کنار هم نشدنی است.

مثال: تاخیر و ظرفیت مهم نیست

| P | D | T | R |
|---|---|---|---|
| 001 | 0 | 0 | 1 |

مثال: تاخیر مهم نیست توان خروجی مهم و قابلیت اعتماد مهم نیست

| P | D | T | R |
|---|---|---|---|
| 001 | 0 | 1 | 0 |

مثال: موسیقی

| P | D | T | R |
|---|---|---|---|
| 010 | 0 | 1 | 0 |

موسیقی از طریق کابل باشد برای داده های تصویر و صوتی پرچم T باید ۱ باشد و D یک باشد و بی تاخیر باید باشد که صدا پشت هم باشد اما D صفر باشد یعنی مسیریابی دادهای صوتی بروی ماهواره ارسال می شود. ماهواره بخاطر مسافت تاخیر دارد.

مثال: داده های سند مالی

| P | D | T | R |
|---|---|---|---|
| 110 | 0 | 0 | 1 |

مثال: سیستم کنترلی جهت تنظیمات شبکه

| P | D | T | R |
|---|---|---|---|
| 111 | 1 | 0 | 1 |

اینجا همه اعداد باید یک باشد ولی چون در سطح شبکه امکان ندارد و چون توان خروجی از بقیه دارای اولویت پایین تر دارد اینجا صفر می شود.

Total Length : این فیلد طول کل بسته را شامل سرایند و داده مشخص می شود و حداکثر ۶۵۵۳۵ است و طول سرایند ۲۰ است.

Identification : این فیلد مشخص می کند که این قطعه به کدام دیتا گرام متعلق است.

نکته : تمام قطعات یک دیتاگرام واحد، دارای مقدار یکسان شناسه یا Identification می باشد.

مثال: دادهای فایل صوتی برای آلبوم بیداد دارای شناسه ۴۵۰ می باشد.

DF : Don’t Fragment به معنی آن است که قطعه نکن. بطور مثال اگر بسته داده وارد شده بزرگ است آن را به دو یا چند قسمت تقسیم نکن زیرا مقصد قادر بهم پیوستن آنها و یکی کردن آنها نیست.

مثال: می خواهیم تصویری از حافظه برای مقصد بفرستیم لذا بیت DF را ۱ می کنیم یعنی کل تصویر حافظه یکجا به مقصد برسد.

MF: More Fragment اگر این بیت ۱ باشد یعنی هنوز قطعات مربوط به یک برنامه ادامه دارد(قطعات دیتا دیاگرام)

نکته: آخرین بسته مربوط به یک دیاگرام بیت MF آن حتما صفر است.

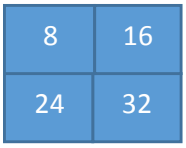
Fragment Offset : نشان می دهد قطعه جاری در کجای دیتاگرام اصلی واقع شده است. طول تمام قطعات حتما ضریبی از ۸ بایت است. طول این فیلد ۱۳ بیت است.

نمونه یک دیتاگرام بزرگ حداکثر به چند قطعه می توان تقسیم شود؟

$2^{13}$ = 8192*8 = 65536

یک بسته که به ۴ قسمت تقسیم می شود Fragment Offset ، MF ، DF و با Identification که ۱۰۰۰ است را نشان دهید؟


| Identification | DF | MF | Fragment Offset |
|---|---|---|---|
| 1000 | 0 | 1 | 1*8=8 |
| 1000 | 0 | 1 | 2*8=16 |
| 1000 | 0 | 1 | 3*8=24 |
| 1000 | 0 | 0 | 4*8=32 |




بسته ها می توانند تا ۸۱۹۲ تا تقسیم شوند و آخری آن MF برابر صفر است.

Time to Live : (TTL) شمارنده است که طول عمر بسته را تعیین می کند حداکثر اندازه آن ۲۵۵ می باشد و به ازای هر گام یا پرش (HOP) از مسیریاب یک واحد از آن کم می شود.

اگر یک بسته از دو مسیر مختلف ارسال شود و اولی TTL آن ۱۹۰ و دیگری ۲۰۰ باشد کدام مسیر انتخاب می شود؟

هر TTL ۲۵۵ است بنابراین

255-190 = 65 HOP

255-200 = 55 HOP

۵۵ مورد قبول است چون کمترین پرش مهم است.

فرمول کلی HOP-Count = 255 – TTL

نکته : اگر مقدار TTL به صرف برسد طول عمر آن تمام شده است و هر روتری که آن را دریافت کند آن بسته را می کشد و از بین می برد و پیام هشدار به ماشین مبدا تولید کننده پیام می دهد.

نکته : استفاده از فیلد TTL سبب می شود حلقه های که بی نهایت تولید نشده و شبکه دچار ازدحام غیر منطقی برای بسته های کهنه و سرگردان نشود.

Protocol : این فیلد نشان می دهد که بسته به کدام فرایند یا Protocol در لایه انتقال تحویل داده شود. مثلا بسته به پروتکل TCP یا UDP یا FTP تحویل داده شود.

Check sum Header : این فیلد جهت کشف خطا بکار می رود این فیلد فقط سرایند بسته را می گیرد و آن ها را در قالب دسته های ۱۶ بیتی زیر هم قرار می دهد و آنها را XOR می کند و بعد مکمل یک را حساب کرده (به این روش مکمل یک نیز می گویند) اگر سرایند بی خطا باشد بایستی مقدار محاسبه شده آن صفر باشد. البته در مقصد دوباره بخش Check sum سرایند دوباره محاسبه می شود.

فرض کنید سرایند دارای بیت های ۱۱۰۰۱۱۰۱۰۱۰۰ و به روش مکمل ۱ (One-Scomplement) مقدار Check sum مشخص کنید؟

برای هربیت داده مکمل ۱ آن را بدست می آوریم البته بعد از XOR کردن و Check sum را ۶ بیتی در نظر می گیریم.

$$\begin{array}{r} 010100 \\ \oplus\quad 110011 \\ \hline 100111 \end{array}$$

$$\begin{array}{r} 111111 \\ \text{مکمل یک}\quad 100111 \\ \hline 011000 \end{array}$$

حال در مقصد این بیت های داخل Check sum می رسد.

| Check sum |
| --- |
| 011000 |

$$\begin{array}{r} 010100 \\ \oplus\quad 110011 \\ \hline 100111 \end{array}$$

$$\begin{array}{r} 100111 \\ \oplus \quad 011000 \\ \hline 111111 \end{array}$$

نکته : اگر جمع حاصل XOR با Check sum همه یک باشد و یا & آن با Check sum صفر باشد یعنی طول سرایند طول مسیر تغییر نکرده است.

Source Address : آدرس IP مبدا قرار می گیرد.

Destination Address : آدرس IP مقصد قرار می گیرد.

Option : این فیلد طراحی شده است که بتوان اطلاعات اضافی از شبکه را در آن قرار داد مثلا طول صف مسیریاب یا میزان تاخیر جهت صف بندی یا بودن در صف و پردازش و .... است.

Data : این فیلد نشان دهنده اندازه داده است.

امنیت شبکه

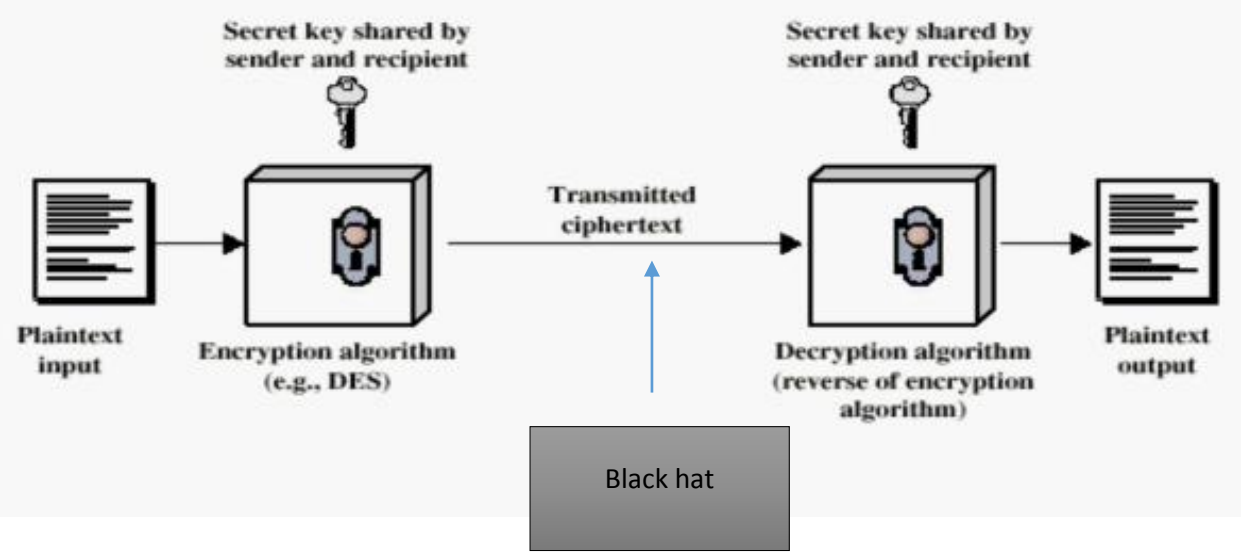
به منظور مقابله با نفوذگری در شبکه دو راه می توانیم انتخاب کنیم:

۱- استفاده از ابزارهای مناسب جهت ممانعت از ورود نفوذگران و کشف فعالیت های آنها است که این ابزارها و روش ها عبارتند از:

Firewall (دیواره آتش)- نرم افزارهایی مثل Honey bot ابزار نظارت و مدیریت و گزارش استفاده از پورت های باز سرور که Honey pot ابزار است به معنی ظرف عسل- آنتی ویروس- ضد جاسوس – سیستم تشخیص نفوذ IDS – سیستم پیشگیری از نفوذ IPS –

۲- استفاده از تکنیک های رمزنگاری برای افزایش امنیت داده

بطور کلی برای افزایش ظریب امنیتی داده ها هنگام ارسال داده ها از ماشین مبدا به ماشین مقصد بهتر است ماشین مبدا داده های خود را رمز نموده (Encryption) و سپس داده رمز شده را از طریق شبکه اینترنت راهی مقصد کند پس در مقصد بسته داده رمز شده ، رمزگشایی (Decryption) شود و داده های آن مورد استفاده قرار گیرد. شکل زیر موضوع را نشان می دهد.




انواع روش های رمزنگاری:

بطور کلی دو روش رمزنگاری داریم:

۱- با استفاده از کلید مشترک (متقارن)

۲- رمزنگاری با زوج کلید (نامتقارن)

رمزگذاری متقارن:

در این روش ماشین مبدا و مقصد بررسی یک کلید مشترک موافقت می کنند یعنی ماشین مشترک متن ساده را رمز می کند و ماشیم مقصد با استفاده از همان کلید متن رمز شده را رمزگشایی می کند.

روش های رمزنگاری کلید مشترک یا متقارن:

روش رمزگذاری سزار (کلید K ) :

در اینجا با فرض وجود الفیا انگلیسی از A تا Z که از ۱ تا ۲۶ است و داشتن کلید Kماشین مبدا متن نامه را به اندازه  بازنویسی کلمات متن اصلی بدست می آید.

مثال: می خواهیم کلمات زیر با کلید مشترک رمز گذاری سزار و با K=3 رمز کنید؟

HELLO KHOOR

Good Bye JRRGEBH

مشکلات این روش برای نفوذگران و هکرهای حرفه ای بسیار پیش پا افتاده است زیرا با توجه به الگوی کلمات و محل قرارگیری آنها در نامه به سادگی کد مشترک آنها کشف می شود.

روش جایگشتی الگوی کلمه:

در این روش رمزگذاری ابتدا متن مربوطه با توجه به تعداد حروف کلمه الگو بصورت دسته K حرفی زیر هم قرار می گیرند آنگاه بعد از قرار گرفتن تمامی متن بصورت ستونی متن مربوطه بر مینای حروف الفبا مرتب می کنیم و بدین ترتیب حروف و کلمات تغییر می کند. نکته مهم آن است که حتما بایستی تمامی سطرها و ستون ها کامل شوند زمانیکه متن رمز شده با این روش به مقصد می رسد ماشین مقصد الگوی کلمه را دارد و مراحل گفته شده بطور معکوس طی می شود تا متن اولیه تولید شود.

مثال : می خواهیم محتویات یک حواله بانکی را به روش جایگشتی و الگوی مگابایت MEGABUCK رمز گذاری کنیم مشخص کنید که چگونه این عملیات انجام می شود؟

Plain text: Please transfer two million toman from Tehran to swiss

Pattern: MEGABUCK

Decode:
AFLAHISEINRSTTORNALNMOTSESIMEWRWNOTBPAOTMOERIFAS

نکته: برای فشرده تر شدن متن فوق علائم سجاوندی (. ، : ، " ، و .....) حذف می گردد. همچنین تمامی حروف انگلیسی بوده و با حروف بزرگ نوشته می شود. اگر در سطر آخر کامل نشد می توانیم از حروف A تا Z استفاده کنیم.

الگوریتم:

۱- ابتدا الگوی MEGABUCK را بصورت جداگانه به عنوان سر تیتر می نویسیم.
۲- متن مورد نظر را به حروف بزرگ تبدیل کرده و بلنک های بین کلمات را حذف می کنیم و بصورت سطری زیر هم می نویسیم . در انتها اگر کامل نشد از A تا Z پر می کنیم.
۳- بر اساس ترتیب حروف الفبای MEGABUCK ستون به ستون حروف را برداشته و بطور سطری بطور متوالی می نویسیم.
۴- این متن رمز شده است و آن را در قالب یک بسته داده راهی ماشین مقصد می کنیم.

نکته: در الگو کلمات تکراری نداریم و عدد نباید بگذاریم.

نکته: الگوی جایگشتی باید بغیر از روش ارسال بسته صورت گیرد ( مثلا از طریق تلفن یا فکس و ....)

بسته ارسالی :

| H | MEGABUCK | Encryption Txt | T |
|---|---|---|---|

در مقصد ابتدا گیرنده الگوی MEGABUCK که شامل ۸ کارکتر است را می داند از طرفی تعداد کل کاراکتر های متن اصلی هم می داند که در اینجا ۴۸ است با تقسیم ۴۸ بر ۸ تعداد ستون بدست می آید ۶ تایی متن رمز شده را دسته بندی می کند و در ستون های آماده شده MEGABUCK به ترتیب حروف الفبا انجام می شود.

تمرین: اگر برای متن فوق از الگوی intermapow را انجام دهید؟

Plain text: Please transfer two million toman from Tehran to swiss

Pattern: INTERAPOW

Decode:TOMRAARNTIPSLROEWOHSLFIOSAINNCRMAABSTTESEEOMWNLFTD

روش Hill

در این روش هر حرف انگلیسی به ترتیب با عدد بین ۰ تا ۲۵ جایگزین شود.

A=0,B=1,…….,Z=25

سپس متن مربوط در قالب گروه های n حرفی به n حرف جدید نگاشته می شود.

رابطه زیر الگوی تغییر را نشان می دهد.

$$C = (K.p) \bmod 26$$

متن رمز شده — حرف کلید ماتریس n*n — متن اصلی

مثال: فرض کنید ماتریس کلید بصورت

$$K=\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

و متن اصلی P=”ACT”

( K.P ) Mod 26 = C

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}_{3*1} * \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}_{3*3} = \begin{bmatrix} 6*0+2*24+19*1 \\ 0*13+2*16+19*10 \\ 0*20+2*17+19*15 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

N=3

M*n . n*p = m*p

3*3.3*1=3*1

C=”POH”

در مقصد با حل یک معادله با حل یک معادله ماتریسی بصورت A.X = B که $X=A^{-1}.B$ مجددا حروف اصلی بدست خواهد آمد.

روش های جدید رمزنگاری

بطور کلی دو روش رمزنگاری : ۱- متقارن ۲- نامتقارن

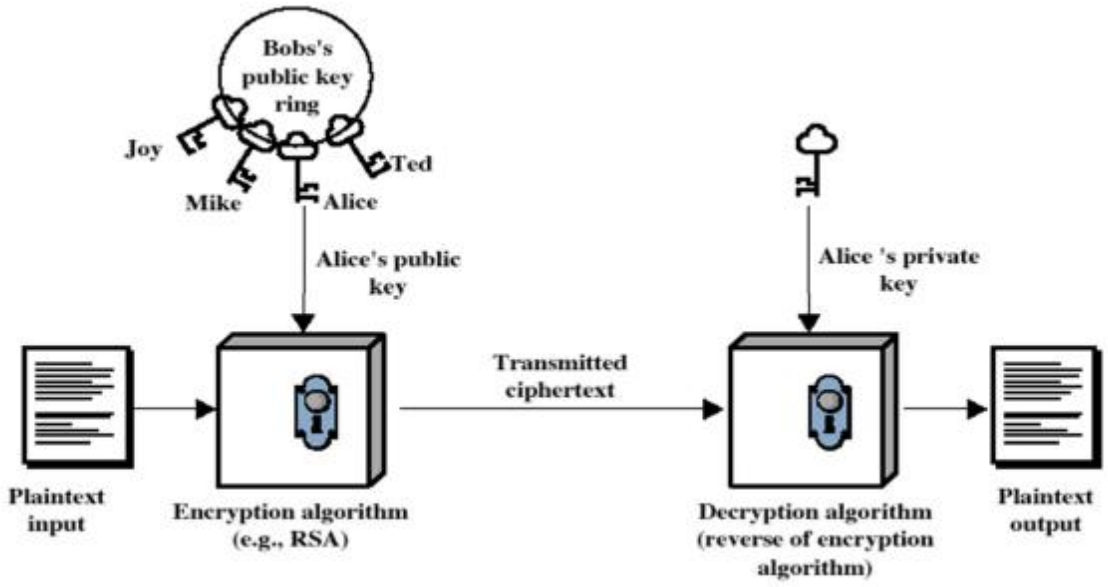
در رمزنگاری متقارن هر دو ماشین مبدا و مقصد از کلید مشترکی استفاده می کنند و مهم ترین این روش عبارتند از:

DES(Data Encryption Standard), AES(Advanced Encryption Standard),Blowfis

در رمزنگاری نامتقارن کاربر یک کلید عمومی و صاحب کلید یک کلید اختصاصی دارد. ابتدا فردی که صاحب رمز می باشد متن ساده خود را با کلید اختصاصی رمز می کند آنگاه متن رمز شده برای کاربر ارسال می شود و در مقصد کاربر با کلید عمومی می تواند آن متن رمز شده را باز کند.

(e,n) (d,n)

صاحب کلید کاربر




(e,n) (d,n)

و مرکز مجوز دهی کلیدها را مرکز CA(Certificat Assurance) مدیریت می کند.

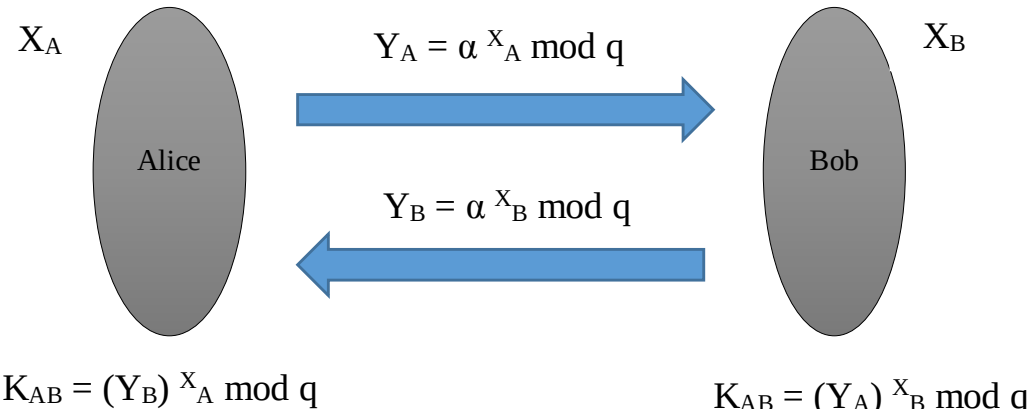
نکته: علت استفاده از امضاء دیجیتال که برگرفته از زوج کلید می باشد این است که طرفین نتوانند هویت خود را بعد از عقد قرارداد انکار کنند.

مهم ترین این الگوریتم ها عبارتند از:

RSA(Rivest – Shamir – Adleman),Diffi-Hellman,Elgamal

الگوریتم Diffi-Hellman

برای تولید زوج کلید با استفاده از لگوریتم Diffi-Hellman موارد زیر را انجام می دهیم.




۱- ابتدا بر روی مقادیر $\alpha$ و $q$ طرفین توافق می کنند.

۲- سپس Alice عدد تصادفی $X_A$ را انتخاب می کند و سپس رابطه زیر را محاسبه می کند.

$$Y_A = \alpha^{X_A} \bmod q$$

۳- در همین زمان Bob عدد تصادفی $X_B$ را تولید می کند و رابطه زیر را محاسبه می کند و ارسال می کند.

$$Y_B = \alpha^{X_B} \bmod q$$

۴- در دو طرف روابط زیر محاسبه می شود

$$K_{AB} = (Y_B)^{X_A} \bmod q$$

$$K_{AB} = (Y_A)^{X_B} \bmod q$$

نکته : در الگوریتم فوق کلید مشترک برابر $\alpha^{(X_A.X_B)} \bmod q$ است.

نکته : اکیدا توصیه می شود که عدد $\alpha$ ، $q$ ، $X_A$ و $X_B$ اعداد اول باشند.

مثال :

قدم اول فرض کنید که دو ماشین مبدا و مقصد بر روی اعداد $\alpha=3$ و $q=353$ توافق کردن

قدم دوم کلیدهای مخفی یعنی $X_A$ و $X_B$ به ترتیب توسط ماشین A و B بصورت زیر است:

کلید خصوصی---> $X_A=97$ کلید عمومی--> $X_B=233$

قدم سوم برای هر کلید عمومی $Y_A$ و $Y_B$ به ترتیب زیر است:

$$Y_A = 3^{97} \bmod 354 = 40$$

$$Y_B = 3^{233} \bmod 354 = 248$$

قدم چهارم کلید مورد توافق

$$K_{AB} = (Y_B)^{X_A} \bmod q = 248^{97} \text{ Mod } 354 = 160$$

$$K_{AB} = (Y_A)^{X_B} \bmod q = 40^{233} \text{ Mod } 354 = 160$$

مطالعه آزاد

تولید اعداد اول (غربال کردن) : فرض می کنیم می خواهیم اعداد اول بین $1<n<9999$

۱- ابتدا آرایه ای تشکیل می دهیم و اعداد از ۱ تا n را به ترتیب داخل آن می چینیم

۲- اعداد را $m=n/2$ که m میانه است که از $n/2$ برست می آید

۳-با استفاده از حلقه for به ترتیب از $i=2$ ..... m به پیش می رویم و سپس در حلقه داخلی دوم تمامی مضرب های i را تا رسیدن به عدد n تولید نموده و خانه آرایه آن را صفر می کنیم تا m

۴- سپس از انجام کار آنچه که در آرایه باقی می ماند عدد اول است.

نکات امتحان:

سوال ۲ مطالعه آزاد ، سوال ۷ مطالعه آزاد، صفحه ۶ و ۷ که سیگنال ها است مطالعه آزاد

سوال های ۱۴ و ۱۶ مهم است

با آرزوی موفقیت و سلامتی برای همه دوستان در تمامی مراحل زندگی و از همگی حلالیت می طلبم .