

فهرست مطالب

۵	۱ مبانی کامپیوتر
۵	۱.۱ الگوریتم چیست؟
۵	۱.۱.۱ ویژگی های الگوریتم
۵	۲.۱ فلوچارت چیست؟
۶	۱.۲.۱ نماد های قراردادی در فلوچارت
۷	۲.۲.۱ مثالهایی از الگوریتم و فلوچارت
۳۳	۳.۱ کامپیوتر چیست؟
۳۳	۴.۱ سخت افزار چیست؟
۳۴	۵.۱ اجزای سخت افزاری کامپیوتر
۳۴	۱.۵.۱ Case
۳۴	۲.۵.۱ Power Supply
۳۵	۳.۵.۱ MotherBoard
۳۶	۴.۵.۱ CPU
۳۷	۵.۵.۱ RAM
۳۷	۶.۵.۱ ROM
۳۸	۷.۵.۱ BUS
۳۸	۸.۵.۱ Video Card
۳۹	۶.۱ نرم افزار چیست؟
۳۹	۱.۶.۱ انواع گروه بندی نرم افزار
۴۱	۷.۱ سیستم عامل چیست؟
۴۲	۱.۷.۱ نمونه هایی از سیستم عامل های کامپیوترهای شخصی
۴۳	۲.۷.۱ نمونه هایی از سیستم عامل های تلفن های همراه
۴۴	۸.۱ برنامه نویسی چیست؟

۴۴	۱.۸.۱	انواع زبانهای برنامه نویسی
----	-------	----------------------------

۲ شبکه و اینترنت ۴۵

۴۵	۱.۲	شبکه ی کامپیوتری چیست؟
۴۵	۱.۱.۲	دلایل استفاده از شبکه
۴۶	۲.۱.۲	تقسیم بندی شبکه از نظر جغرافیایی
۴۷	۲.۲	انواع توپولوژی های شبکه
۴۷	۱.۲.۲	Bus
۴۸	۲.۲.۲	Ring
۴۹	۳.۲.۲	Mesh
۵۰	۴.۲.۲	Star
۵۰	۳.۲	سخت افزار های ایجاد شبکه
۵۰	۱.۳.۲	Hub
۵۱	۲.۳.۲	Switch
۵۲	۳.۳.۲	Router
۵۳	۴.۲	MAC Address
۵۳	۵.۲	اینترنت چیست؟
۵۳	۶.۲	IP Address
۵۴	۷.۲	انواع کلاسهای IP
۵۵	۸.۲	خلاصه ی کلاس های IP به صورت جدول
۶۱	۹.۲	ساختار IPv4
۶۱	۱.۹.۲	سرآیند (header)
۶۴	۱۰.۲	انواع پروتکل ها در شبکه
۶۴	۱.۱۰.۲	DNS
۶۷	۲.۱۰.۲	ICMP
۶۸	۳.۱۰.۲	ARP
۷۰	۴.۱۰.۲	TCP
۷۳	۵.۱۰.۲	UDP

۳ شبکه های اجتماعی ۷۷

۷۷	۱.۳	وبلاگ چیست؟
۷۸	۱.۱.۳	انواع و نمونه هایی از وبلاگ ها

۲.۳	تعریف شبکه اجتماعی	۸۱
۱.۲.۳	انواع و نمونه هایی از شبکه های اجتماعی	۸۱
۳.۳	پیام رسان چیست؟	۸۵
۱.۳.۳	انواع و نمونه هایی از پیام رسان ها	۸۵

۴ امنیت

۱.۴	تعریف امنیت	۸۹
۲.۴	تعریف حمله	۹۰
۱.۲.۴	انواع حمله ها	۹۰
۳.۴	بد افزار چیست	۹۳
۱.۳.۴	ویروس رایانه ای	۹۳
۲.۳.۴	تروجان ها	۹۶
۳.۳.۴	جاسوس افزارها	۹۷
۴.۳.۴	روشهای مقابله با بد افزارها	۹۷

فصل ۱

مبانی کامپیوتر

۱.۱ الگوریتم چیست؟

الگوریتم مجموعه ای از مرحله های محاسباتی پشت سر هم است که مقادیر ورودی را دریافت می کنند و به خروجی تبدیل می کنند

۱.۱.۱ ویژگی های الگوریتم

۱. تعداد دستورالعمل ها باید مشخص باشد
۲. ابتدا و انتهای الگوریتم مشخص باشد
۳. دستورالعمل ها بدون ابهام باشند
۴. دستورالعمل ها قابل اجرا باشند
۵. الگوریتم هدف مشخصی داشته باشد

۲.۱ فلوچارت چیست ؟

برای درک بهتر الگوریتم و سهولت در دنبال کردن دستورالعمل های آن از یکسری اشکال خاص برای نشان دادن الگوریتم استفاده می کنیم که به آن فلوچارت گفته می شود .
به عبارت ساده تر :

به مجموعه ای از علائم ساده که الگوریتم را به صورت نماد های تصویری یا نموداری تبدیل می کند ، فلوچارت گفته می شود .

۱.۲.۱ نماد های قراردادی در فلوچارت

علامت شروع و پایان ، بیضی می باشد

برای نشان دادن شروع و پایان الگوریتم استفاده می شوند .



علامت محاسبات و مقداردهی ، مستطیل می باشد

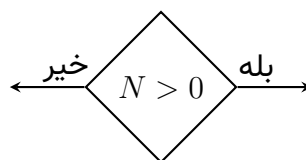
برای انجام محاسبات ریاضی و مقدار دهی به متغیر ها استفاده می شود



علامت ورودی گرفتن و چاپ در خروجی ، متوازی الاضلاع می باشد



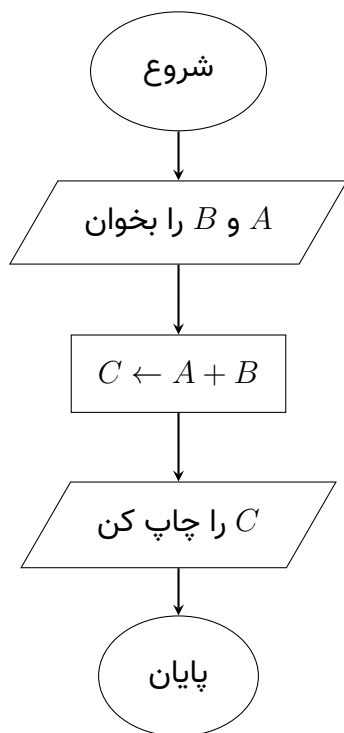
علامت بررسی شرط ، لوزی می باشد



۲.۲.۱ مثالهایی از الگوریتم و فلوچارت

مثال

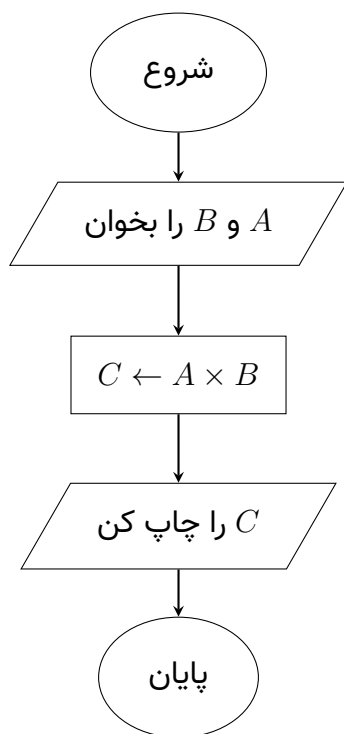
فلوچارتی رسم کنید که دو عدد A و B را به عنوان ورودی گرفته و حاصل جمع آنها را چاپ کند .



۱. شروع
۲. A و B را بخوان
۳. $C \leftarrow A + B$
۴. C را چاپ کن
۵. پایان

مثال

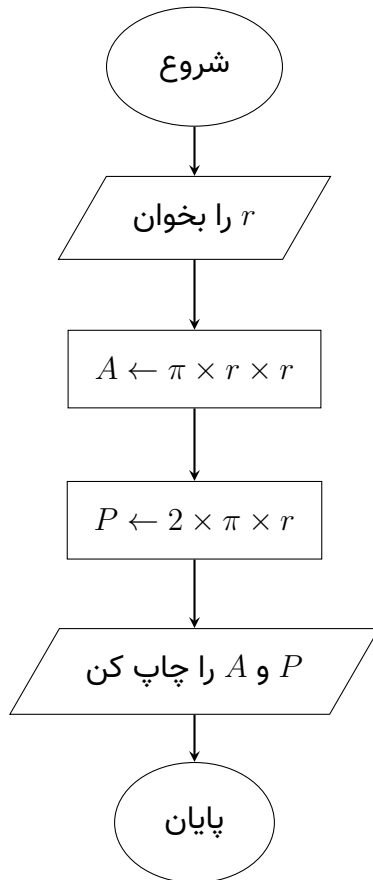
فلوچارتی رسم کنید که دو عدد را خوانده و حاصلضرب آنها را نمایش دهد



۱. شروع
۲. A و B را بخوان
۳. $C \leftarrow A \times B$
۴. C را چاپ کن
۵. پایان

مثال

فلوچارتی رسم کنید که شعاع یک دایره را خوانده و مساحت و محیط آن را نمایش دهد .



۱. شروع

۲. r را بخوان

۳. $A \leftarrow \pi \times r \times r$

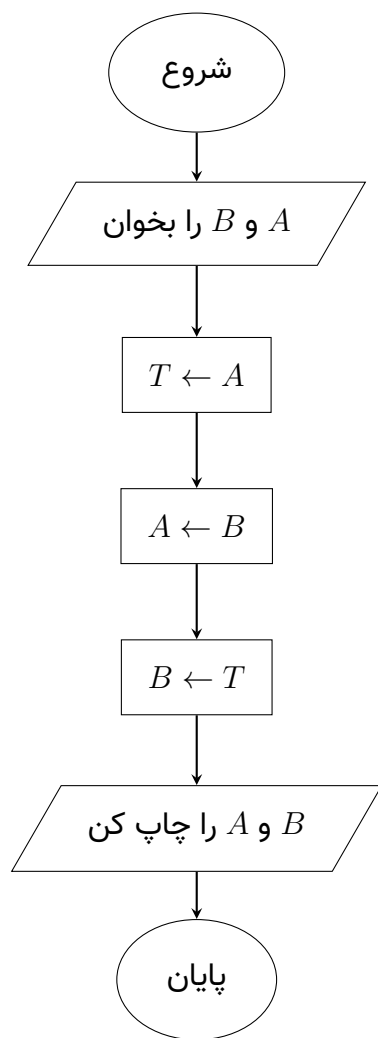
۴. $P \leftarrow 2 \times \pi \times r$

۵. P و A را چاپ کن

۶. پایان

مثال

فلوچارتی رسم کنید که دو عدد را خوانده و سپس مقادیر آن دو عدد را با هم جابه‌جا کند.



۱. شروع

۲. A و B را بخوان

۳. $T \leftarrow A$

۴. $A \leftarrow B$

۵. $B \leftarrow T$

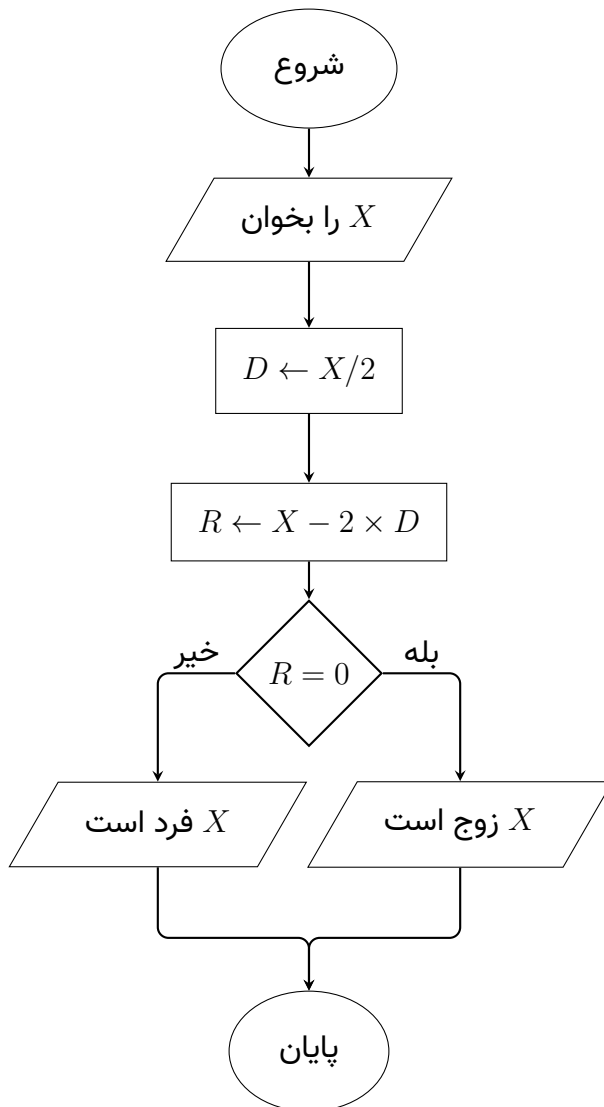
۶. A و B را چاپ کن

۷. پایان

مثال

فلوارتي رسم كنيد كه يك عدد را دريافت كند و مشخص كند كه عدد زوج است يا فرد

- يك عدد زوج است وقتي باقي مانده ي تقسيم آن عدد بر ۲ برابر صفر باشد
- يك عدد فرد است وقتي باقي مانده ي تقسيم آن عدد بر ۲ برابر با صفر نباشد



۱. شروع

۲. X را بخوان

۳. $D \leftarrow X/2$ ۴. $R \leftarrow X - 2 \times D$

۵. if $(R = 0)$ goto $\rightarrow 6$
 else goto $\rightarrow 7$

۶. X زوج است را چاپ كن
 goto $\rightarrow 8$

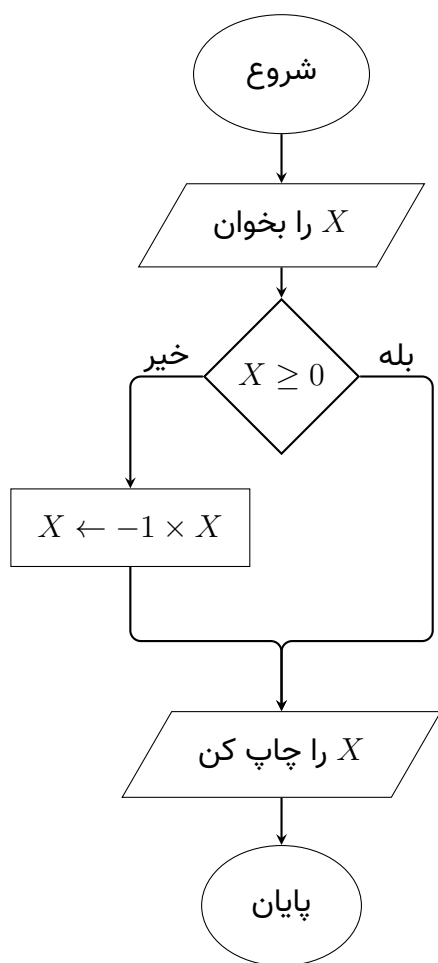
۷. X فرد است را چاپ كن
 goto $\rightarrow 8$

۸. پايان

مثال

فلوچارتی رسم کنید که عملکرد قدر مطلق را انجام دهد

$$|x| = \begin{cases} x \geq 0 & x \\ x < 0 & -x \end{cases}$$



۱. شروع

۲. X را بخوان

۳. if (X ≥ 0) goto → 5
else goto → 4

۴. $X \leftarrow -1 \times X$

۵. X را چاپ کن

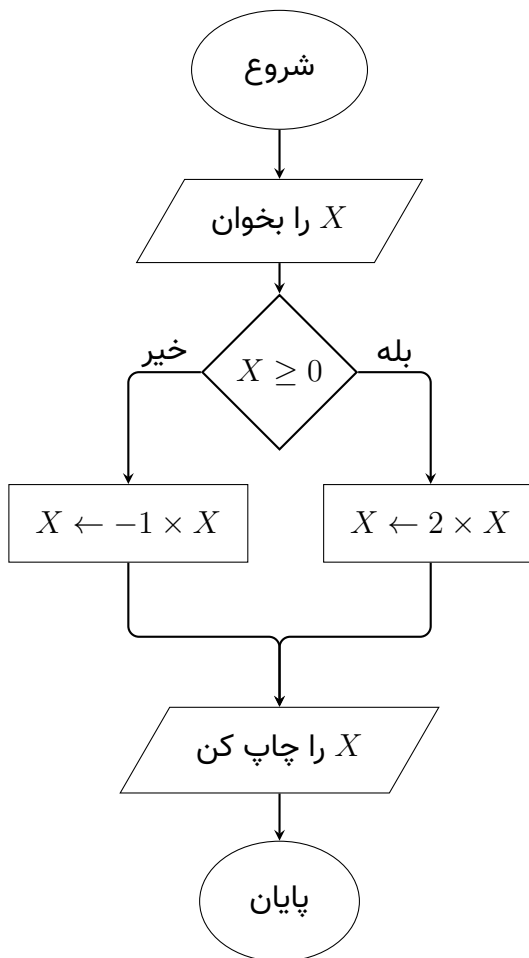
۶. پایان

مثال

فلوچارتی رسم کنید که عدد X را از ورودی بخواند و

• اگر X مثبت بود ، آن را در ۲ ضرب کند و چاپ نماید

• اگر X منفی بود قدر مطلق X را چاپ کند



۱. شروع

۲. X را بخوان

۳. if $(X \geq 0)$ goto $\rightarrow 5$
else goto $\rightarrow 4$

۴. $X \leftarrow -1 \times X$
goto $\rightarrow 6$

۵. $X \leftarrow 2 \times X$
goto $\rightarrow 6$

۶. X را چاپ کن

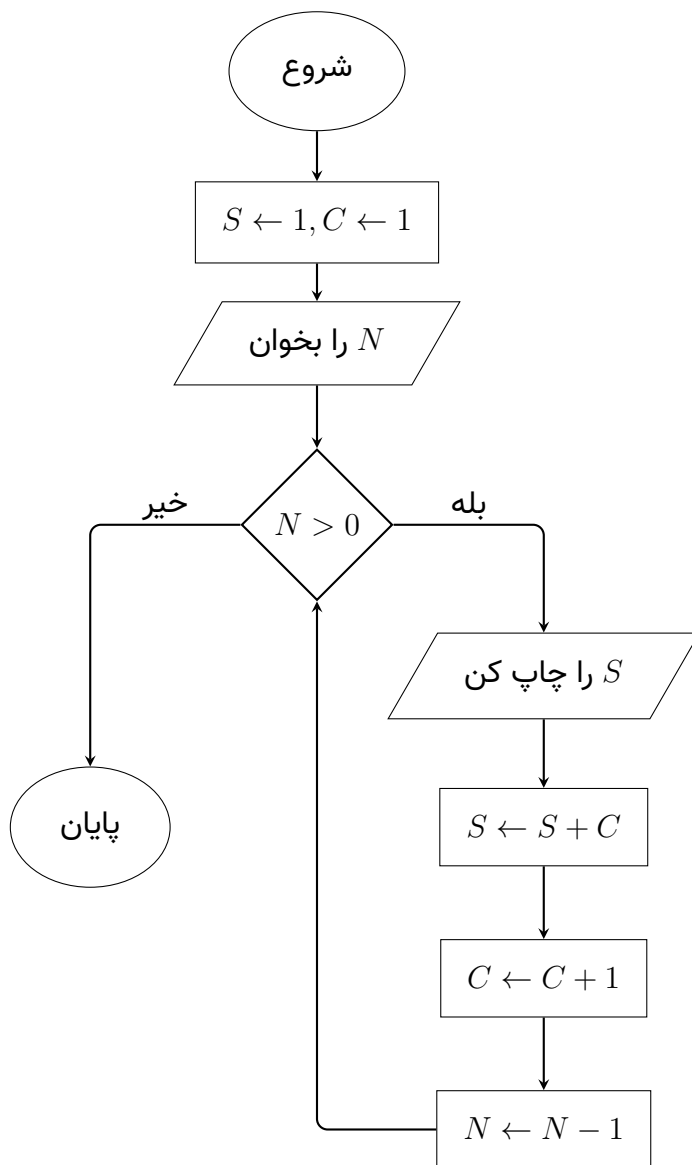
۷. پایان

مثال

فلوچارتی رسم کنید که عدد N را دریافت کند و N جمله ی اول دنباله ی

$1, 2, 4, 7, 11, 16, \dots$

را چاپ کند



۱. شروع

۲. $S \leftarrow 1, C \leftarrow 1$

۳. N را بخوان

۴. if ($N > 0$) goto $\rightarrow 5$
else goto $\rightarrow 9$

۵. S را چاپ کن

۶. $S \leftarrow S + C$

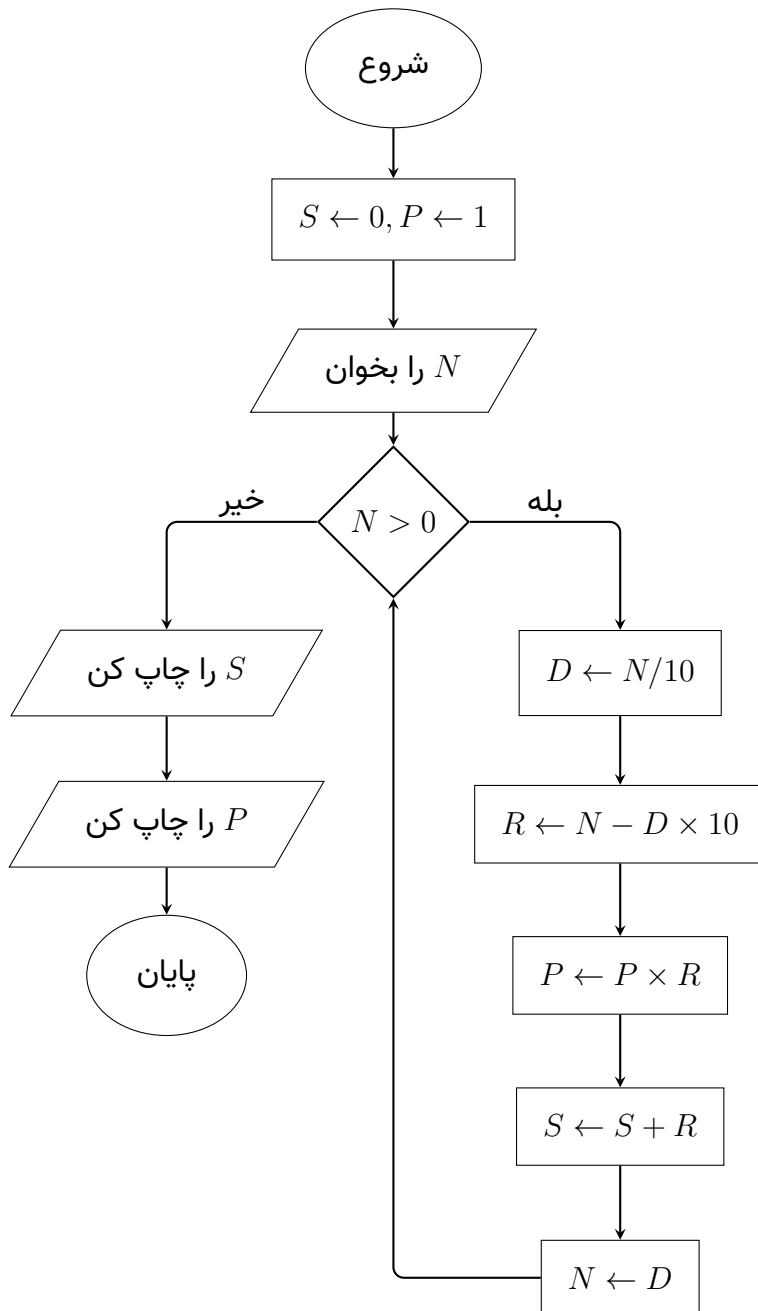
۷. $C \leftarrow C + 1$

۸. $N \leftarrow N - 1$
goto $\rightarrow 4$

۹. پایان

مثال

فلوارتي رسم كنيد كه عدد طبيعي N را از ورودی بخواند و مجموع و حاصل ضرب تعداد ارقام آن را محاسبه و چاپ نمايد



۱. شروع

۲. $S \leftarrow 0, P \leftarrow 1$ ۳. N را بخوان

۴. if $(N > 0)$ goto $\rightarrow 5$
 else goto $\rightarrow 10$

۵. $D \leftarrow N/10$ ۶. $R \leftarrow N - D \times 10$ ۷. $P \leftarrow P \times R$ ۸. $S \leftarrow S + R$

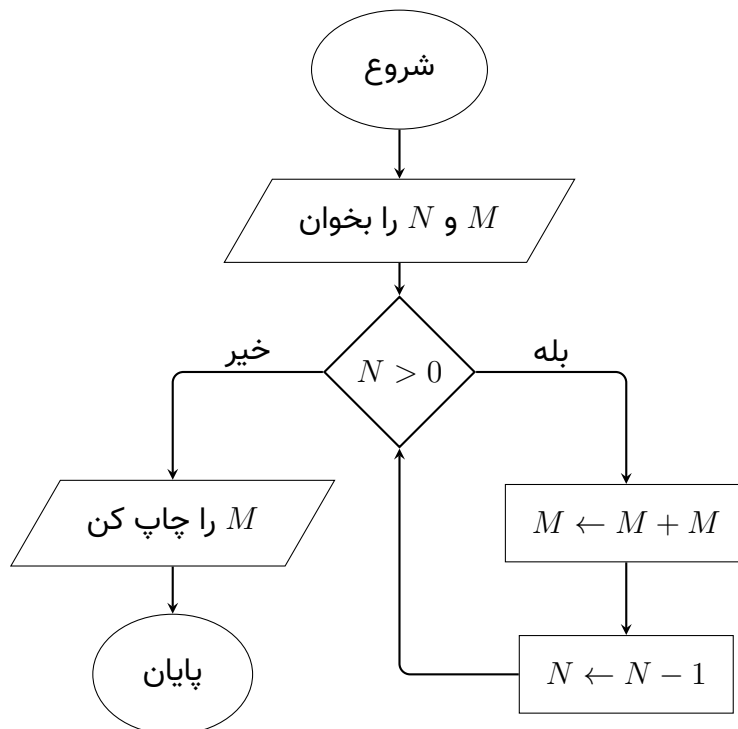
۹. $N \leftarrow D$
 goto $\rightarrow 4$

۱۰. S را چاپ كن۱۱. P را چاپ كن

۱۲. پايان

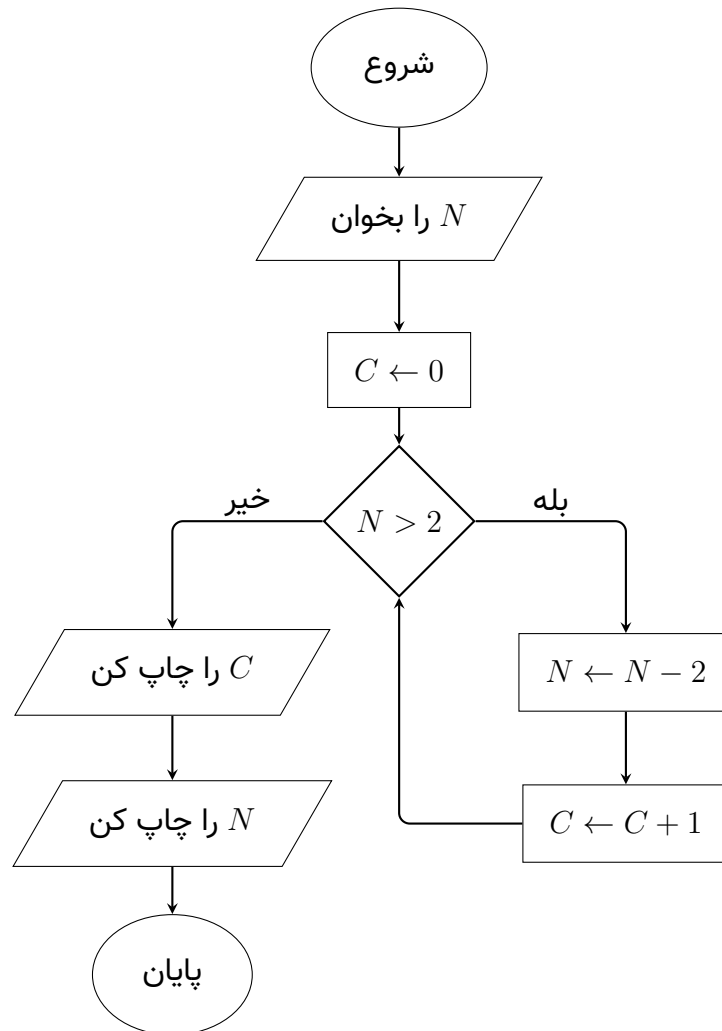
مثال

فلوچارتی رسم کنید که دو عدد طبیعی M و N را از ورودی بخواند و حاصل ضرب آنها را از طریق جمع های متوالی به دست آورد



مثال

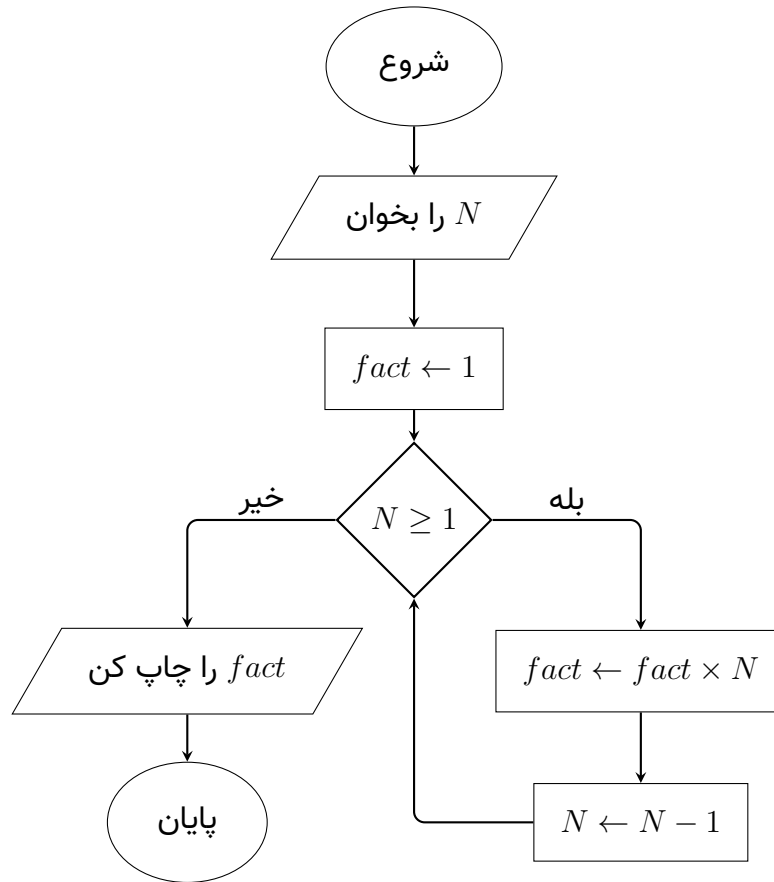
فلوچارتی رسم کنید که عدد صحیح و مثبت N را دریافت کند و باقی مانده و خارج قسمت تقسیم آن بر ۲ را از طریق تفریق های متوالی به دست آورد



مثال

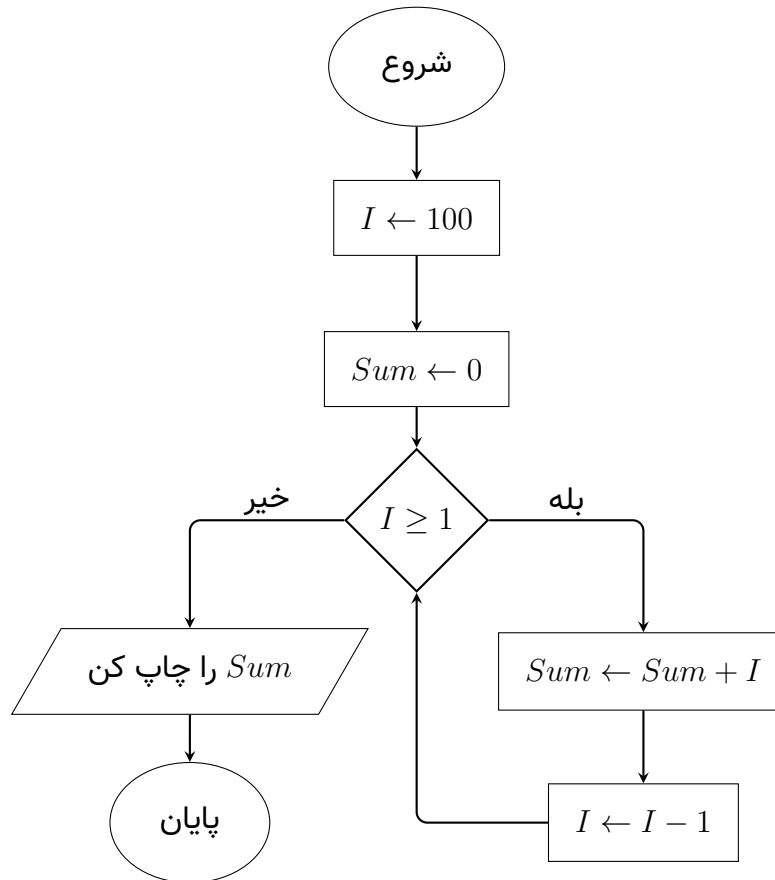
فلوچارتی رسم کنید که یک عدد را از ورودی بخواند و فاکتوریل آن را محاسبه کند .
فاکتوریل عدد n را با $n!$ نشان می دهند و برابر است با :

$$n! = n \times (n - 1) \times (n - 2) \times (n - 3) \times \dots \times 1$$



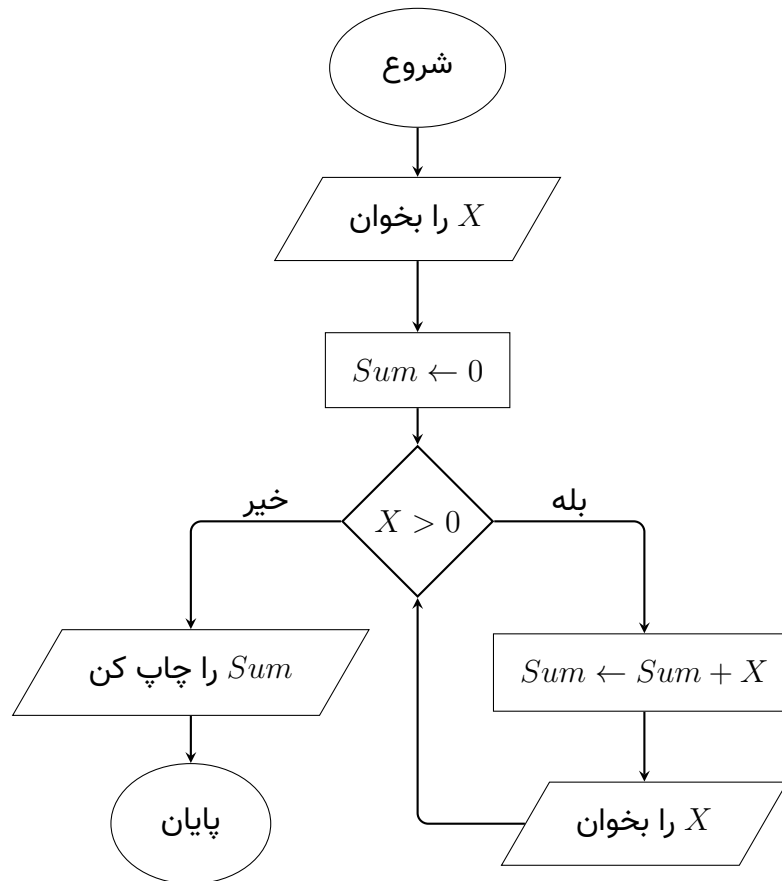
مثال

فلوچارتی رسم کنید که مجموع اعداد ۱ تا ۱۰۰ را چاپ کند .



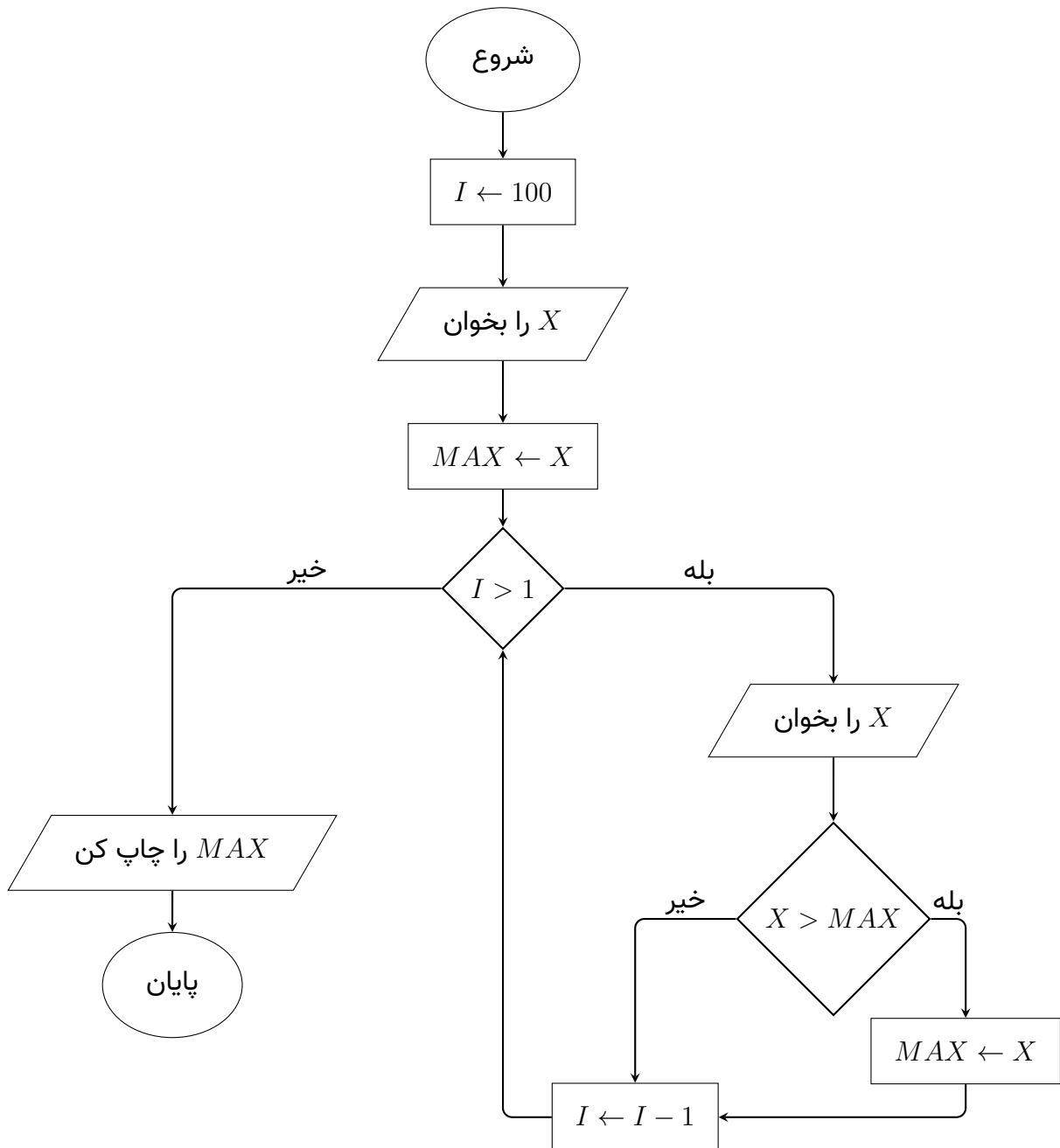
مثال

فلوچارتی رسم کنید که تا زمانی که ورودی بزرگتر از صفر باشد از ورودی اعداد را دریافت کند و در انتها مجموع اعداد را نشان دهد



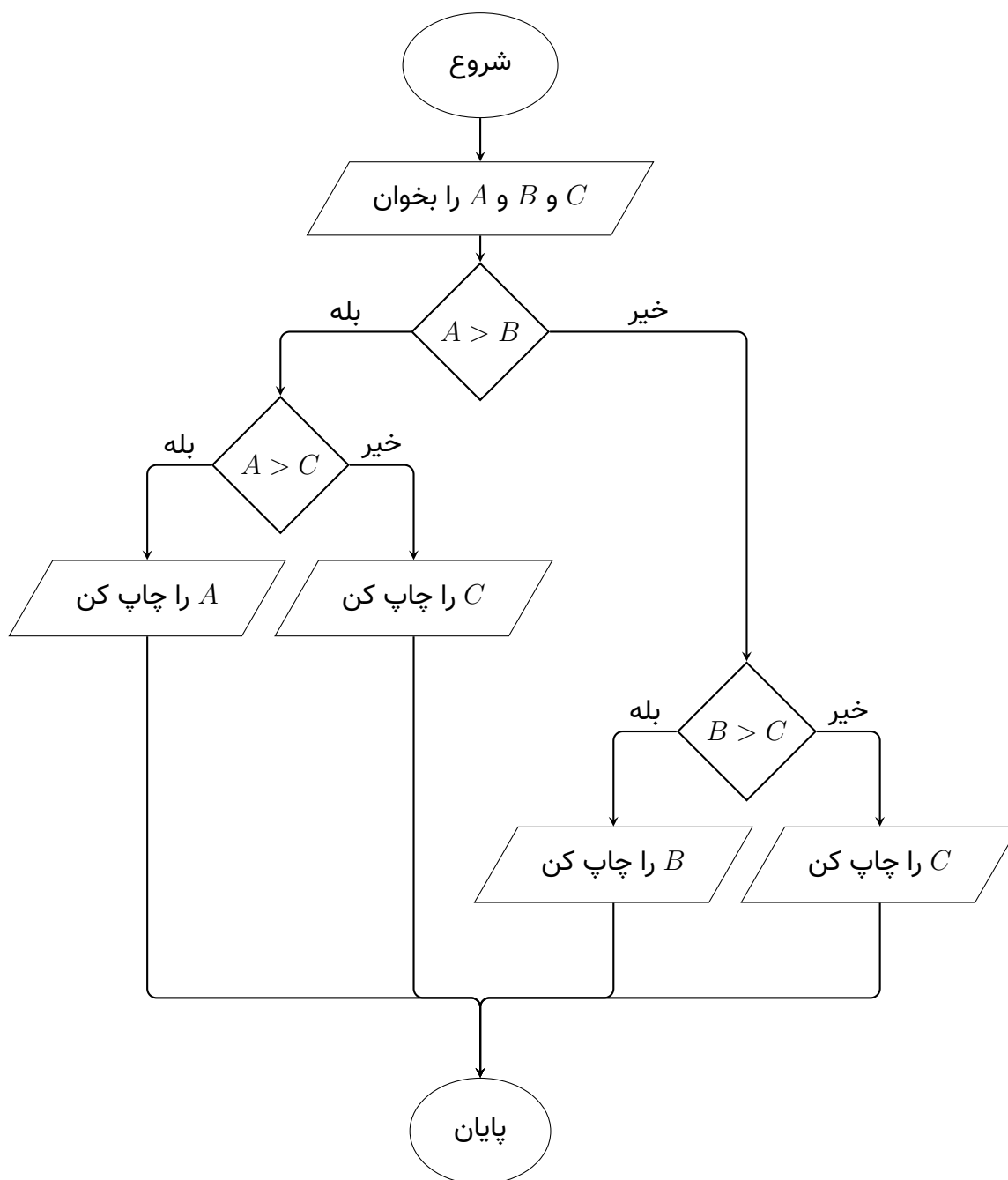
مثال

فلوچارتی رسم کنید که ۱۰۰ عدد را دریافت کند و بزرگترین آنها را نشان دهد



مثال

فلوچارتی رسم کنید که سه عدد را از ورودی دریافت کند و بزرگترین آنها را چاپ کند

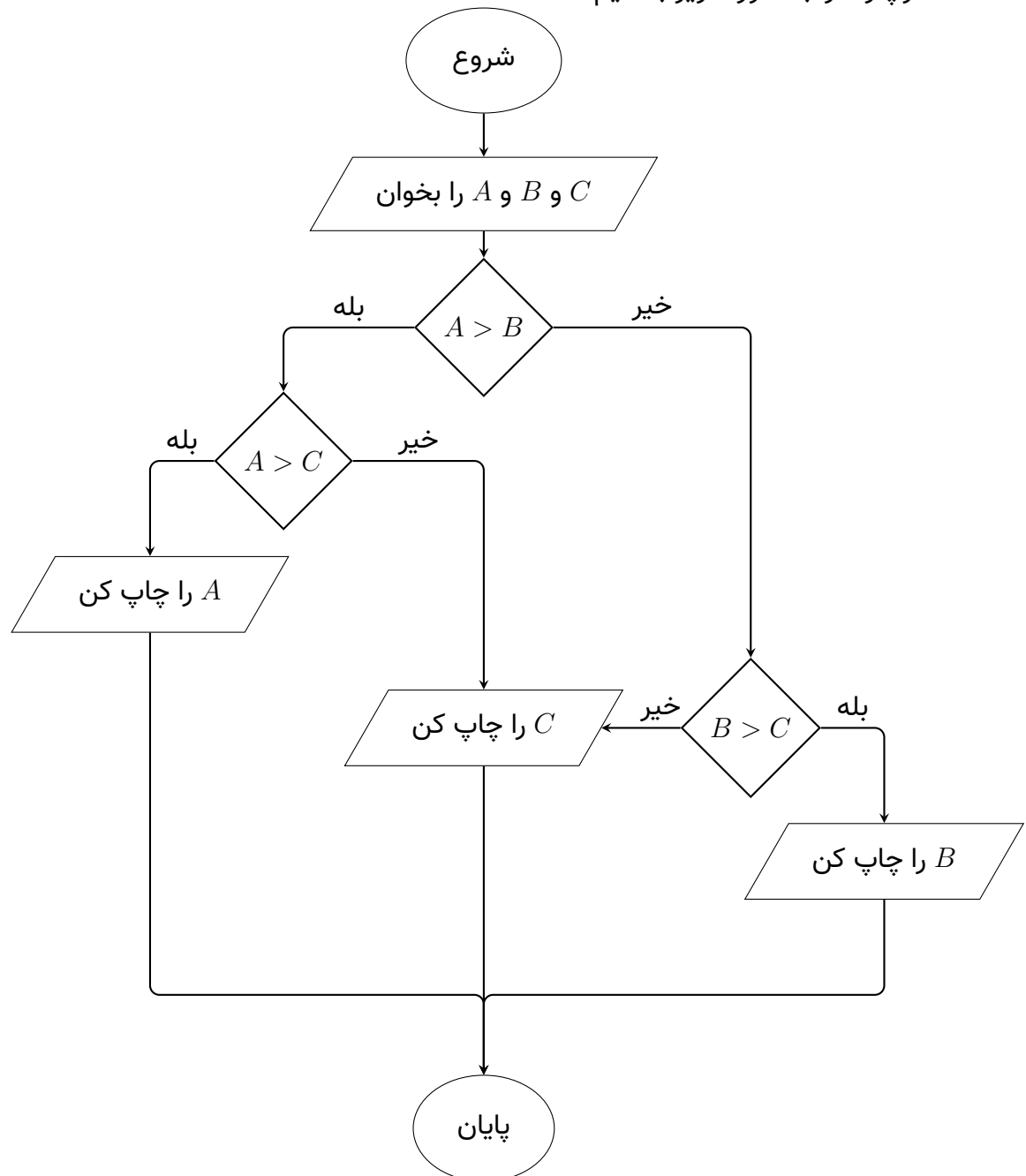


مثال

در مثال قبل برای اینکه دستور فلوچارت را به صورت زیر بکشیم .

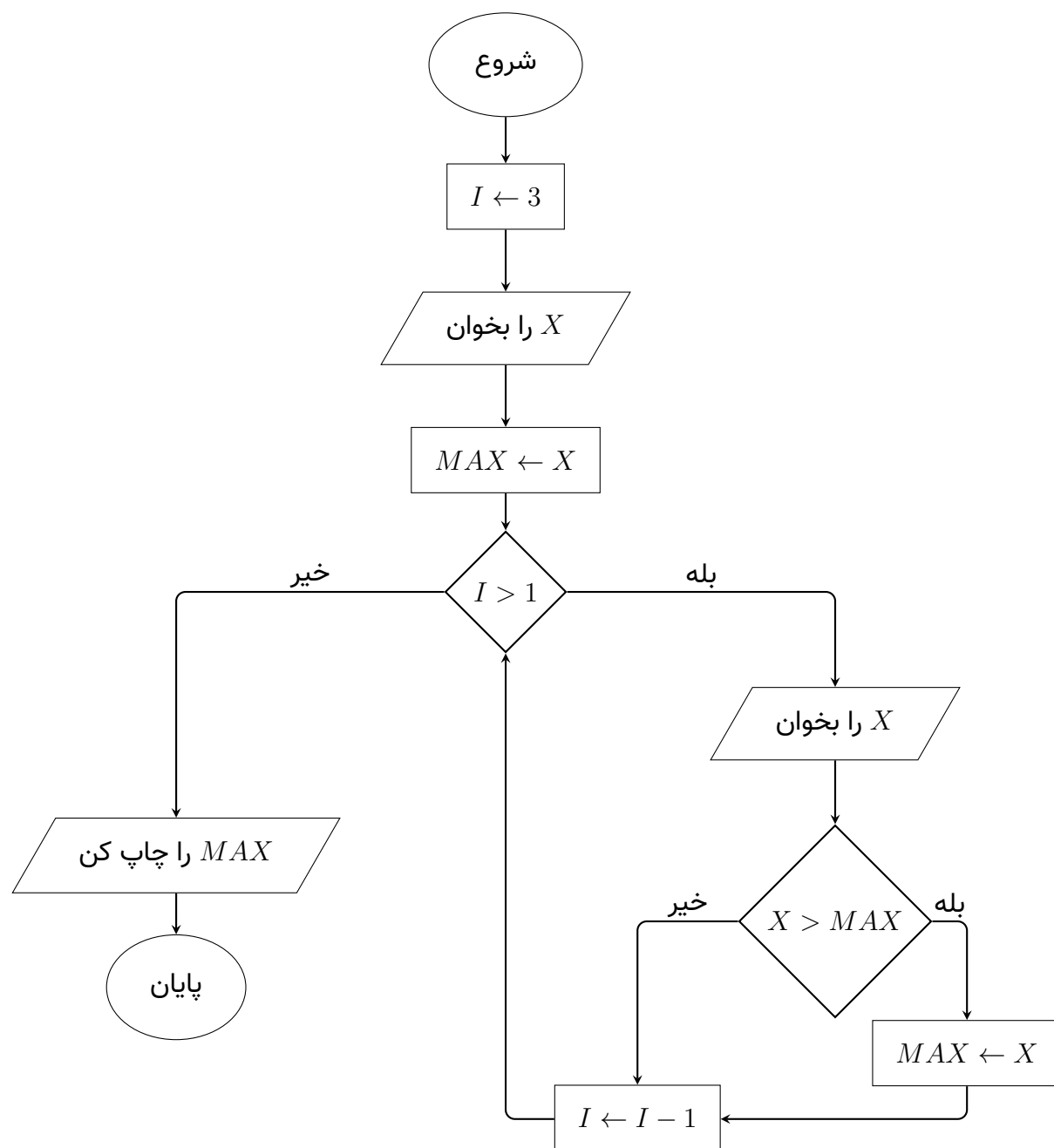
C را چاپ کن

را دوبار به کار ببریم می توانیم



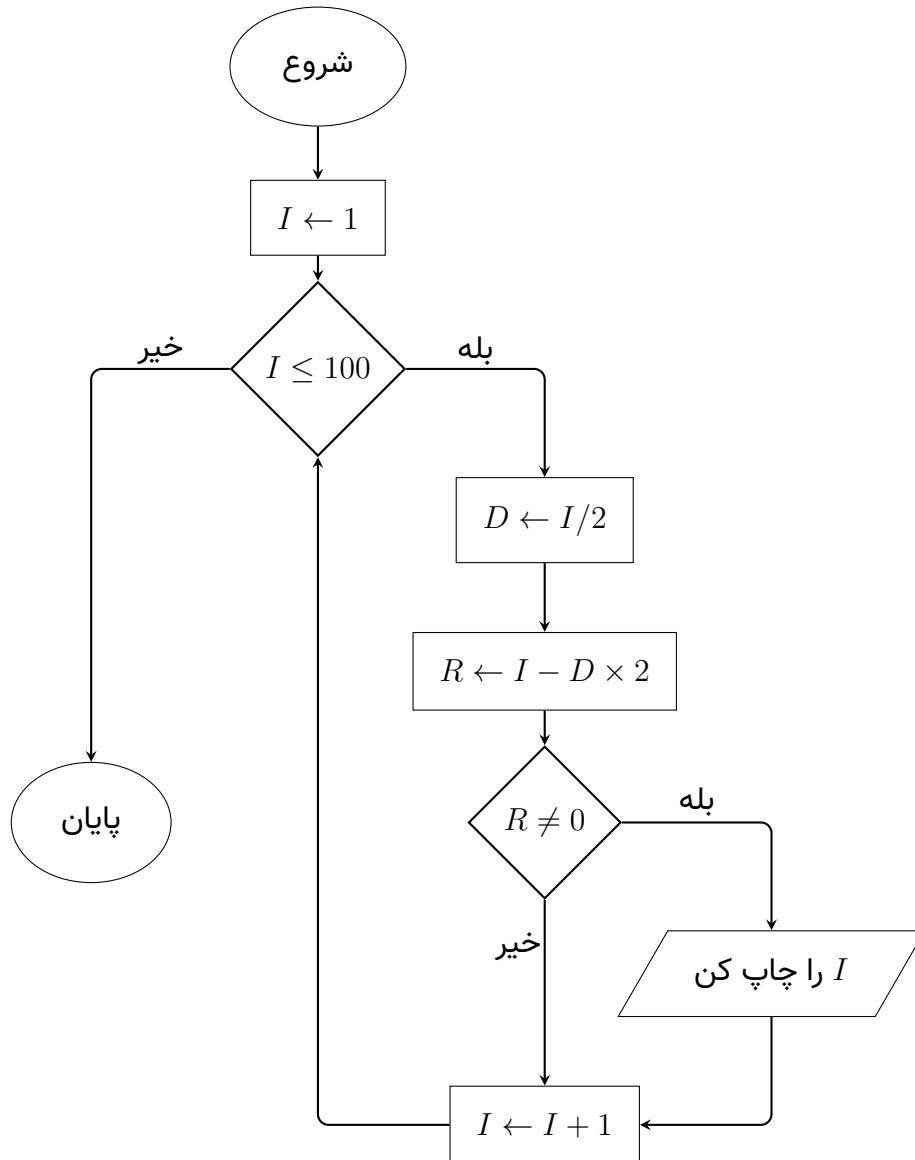
مثال

همچنین می توانیم مثال قبل را به صورت کلی حل کنیم و مقدار شمارنده را ۳ در نظر بگیریم



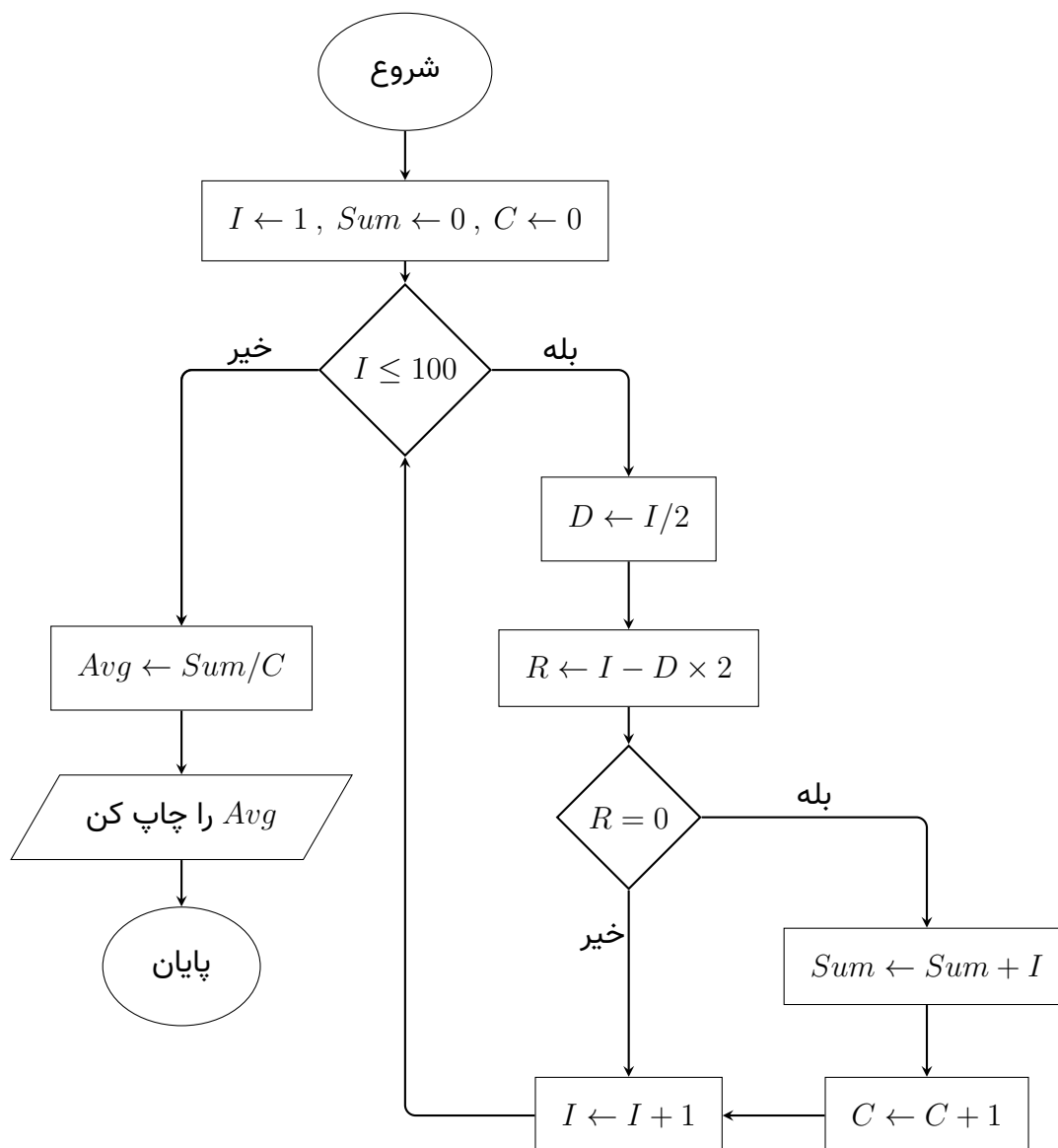
مثال

فلوچارتی رسم کنید که اعداد فرد بین ۱ تا ۱۰۰ را چاپ کند



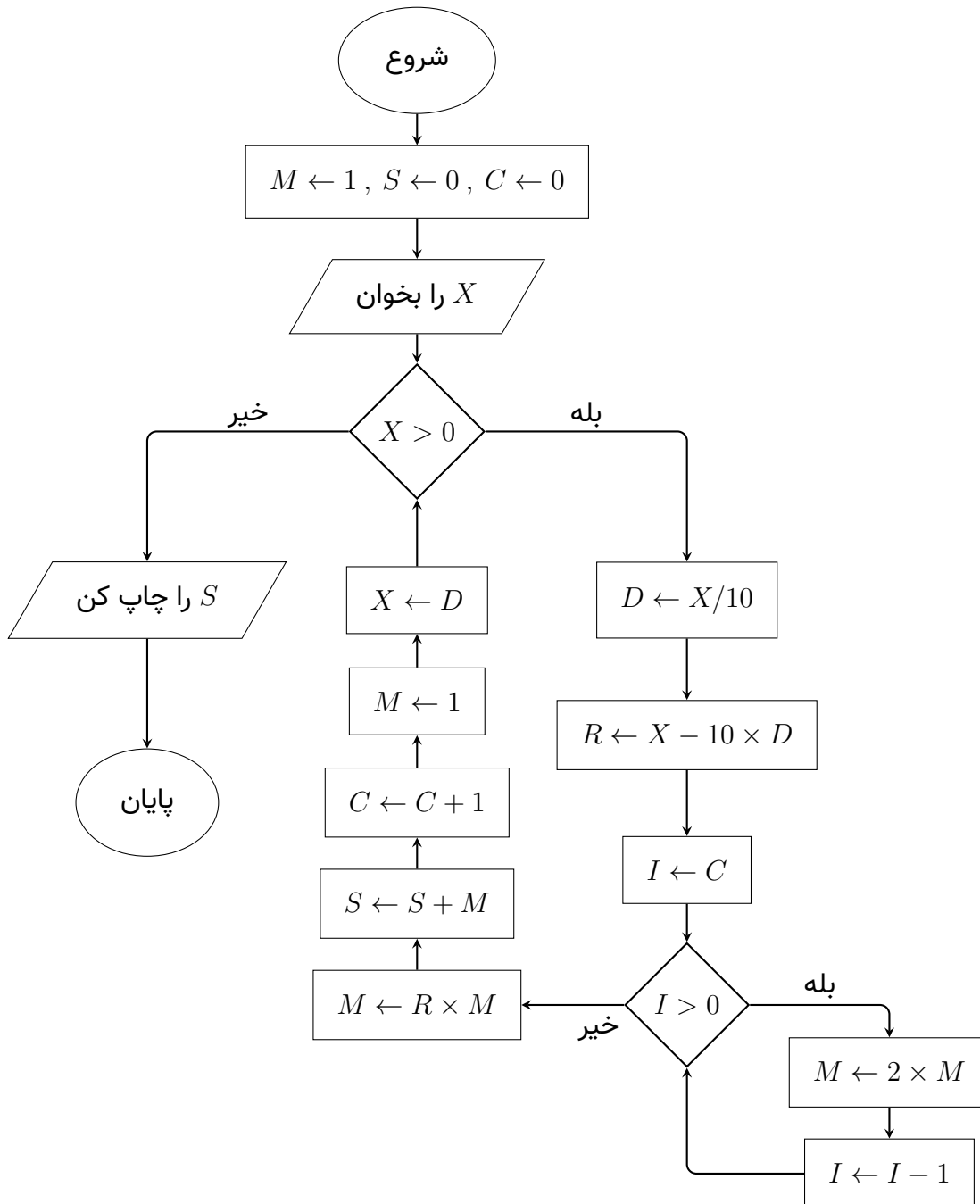
مثال

فلوچارتی رسم کنید که میانگین اعداد زوج بین ۱ تا ۱۰۰ را چاپ کند



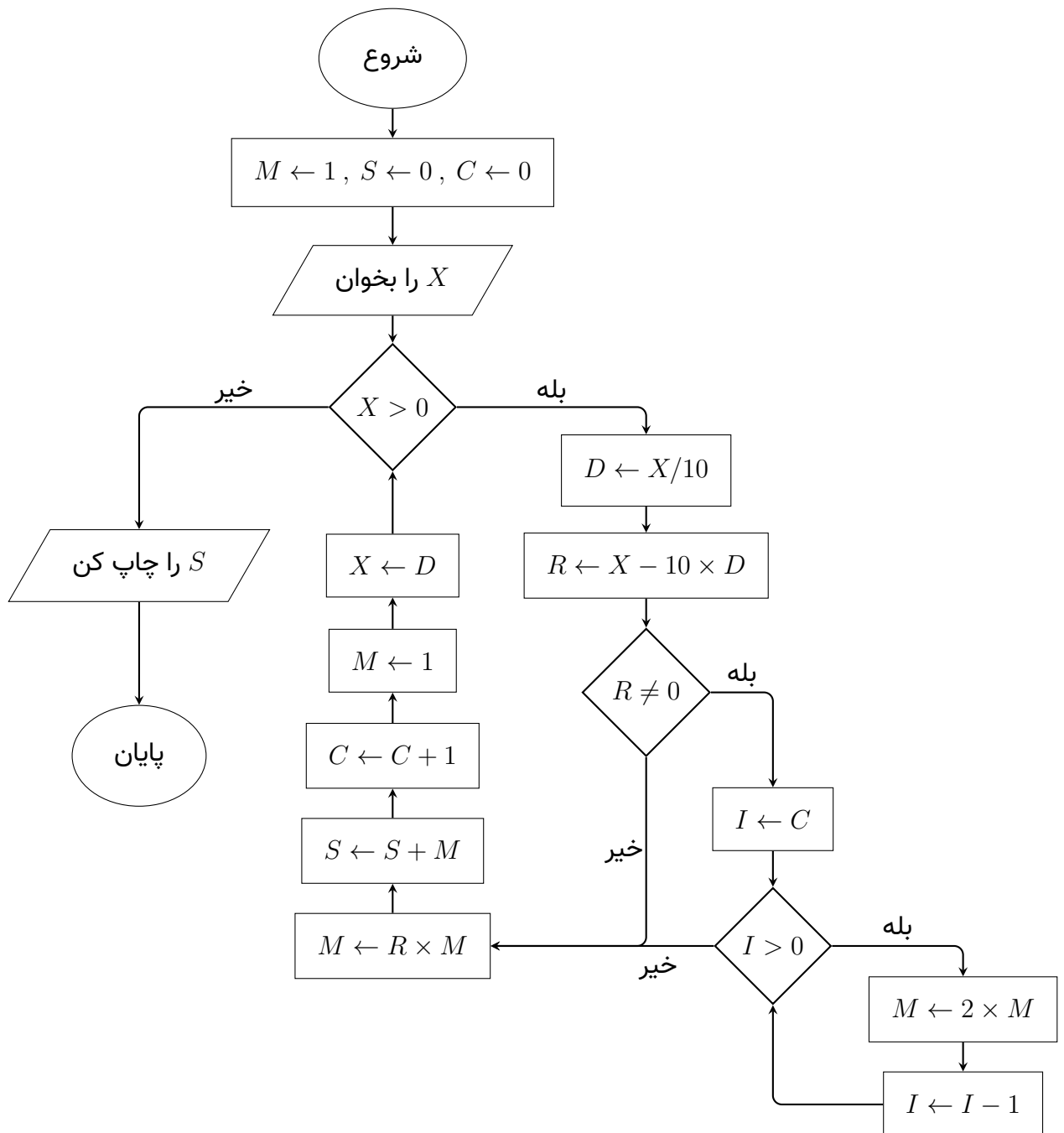
مثال

تبدیل از مبنای ۲ به مبنای ۱۰



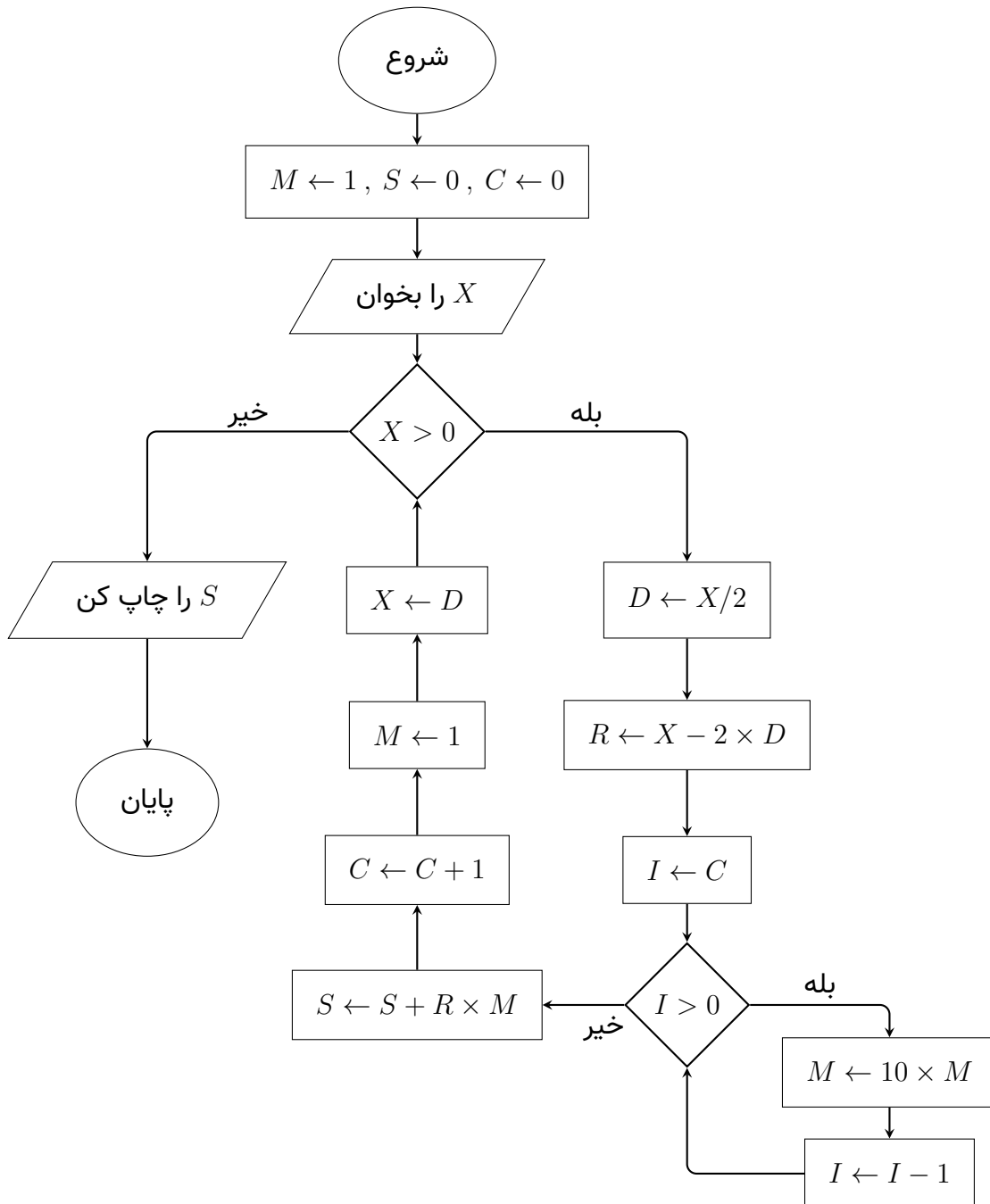
مثال

تبدیل از مبنای ۲ به مبنای ۱۰، به روشی بهینه تر (چرا ؟)



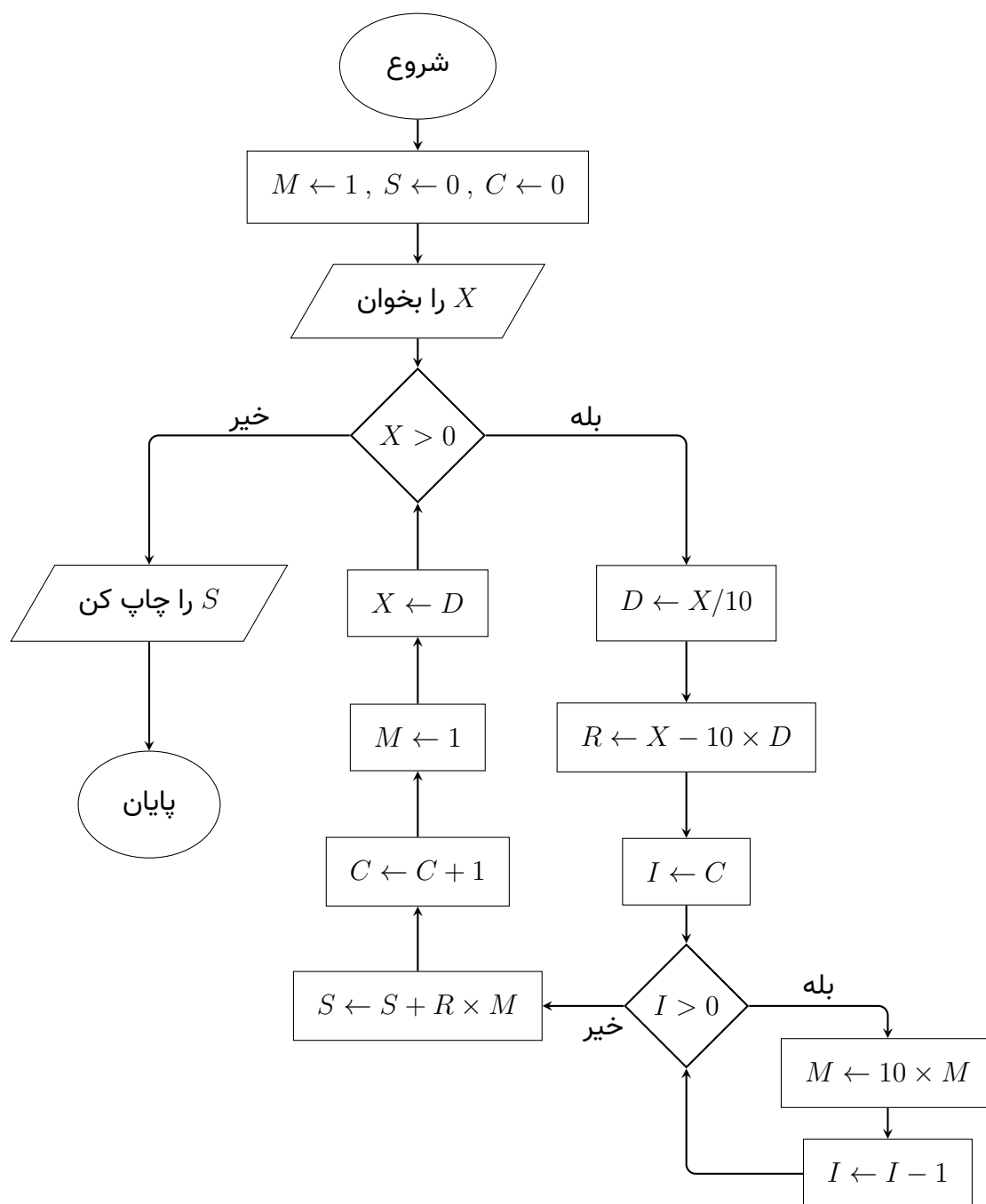
مثال

تبدیل از مبنای ۱۰ به مبنای ۲



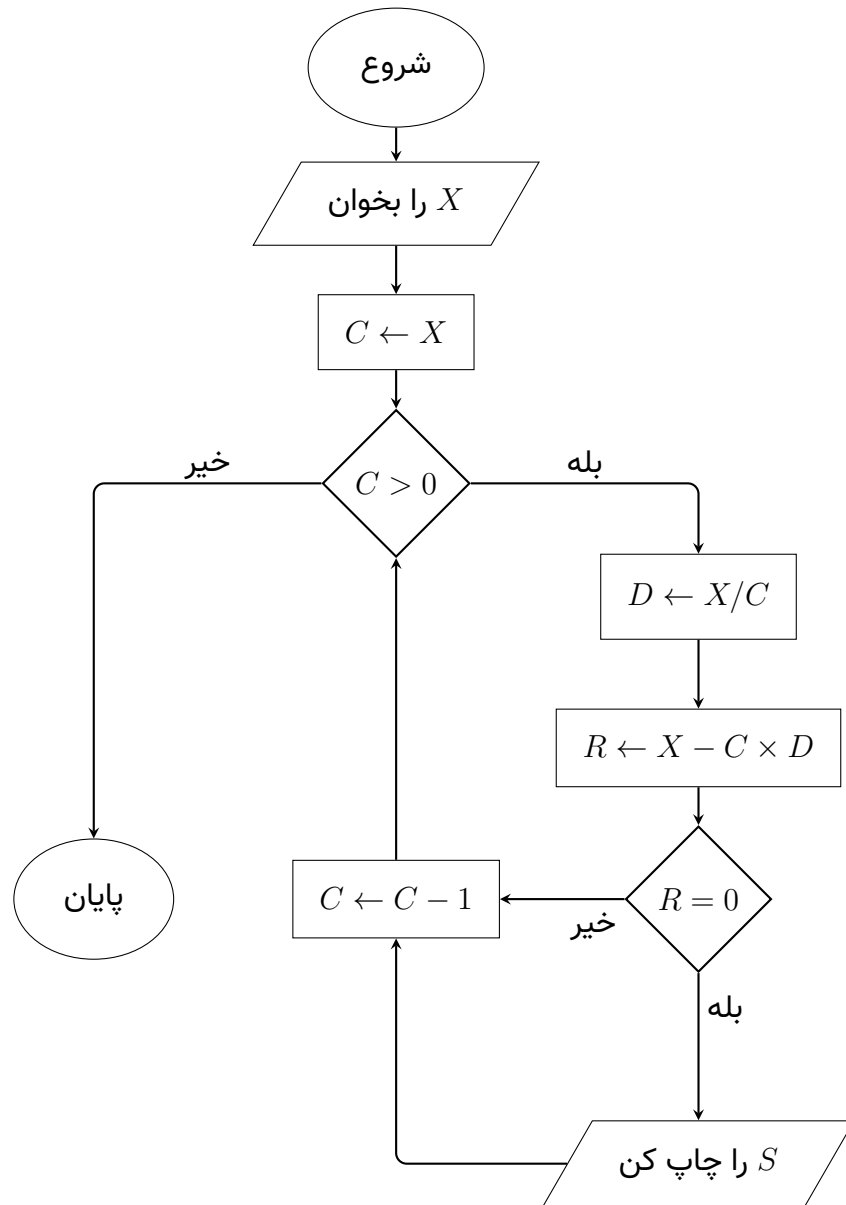
مثال

فلوچارتی رسم کنید که یک عدد صحیح را دریافت کند و مقلوب آن را چاپ کند. مثال :
مقلوب ۴۲۵ می شود ۵۲۴



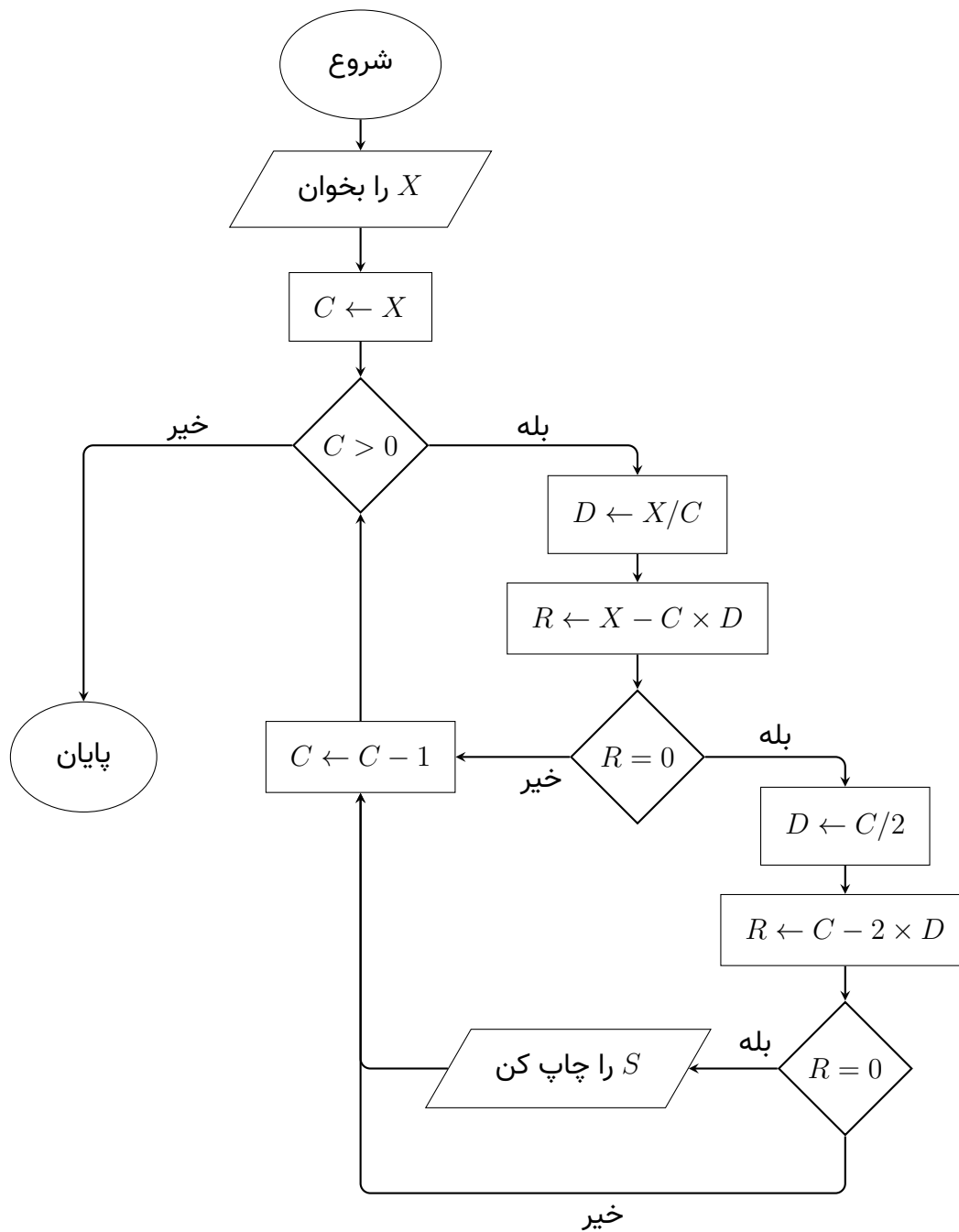
مثال

فلوچارتی رسم کنید که عدد طبیعی و دلخواه X را دریافت نماید و مقسوم علیه های آن را چاپ کند



مثال

فلوچارتی رسم کنید که عدد طبیعی و دلخواه X را دریافت نماید و مقسوم علیه های زوج آن را چاپ کند



۳.۱ کامپیوتر چیست؟

کامپیوتر ماشینی است که می تواند برای انجام عملیات محاسباتی و منطقی به کار گرفته شود .

یک کامپیوتر کامل شامل :

- سخت افزار
- سیستم عامل
- رابط های ورودی و خروجی
- می باشد .

۴.۱ سخت افزار چیست؟

سخت افزار کامپیوتر شامل اجزای فیزیکی و قابل لمس کامپیوتر می باشد ، مثل :

- CPU (Central Processing Unit)
- Motherboard
- Hard Disk
- Monitor
- Keyboard

۵.۱ اجزای سخت افزاری کامپیوتر

Case ۱.۵.۱








Case کامپیوتر ، قطعات سیستم کامپیوتری را در خود نگه می دارد و از آنها در برابر برخورد خارجی محافظت می کند، همچنین ساز و کاری را برای چرخش هوا و خنک سازی قطعات فراهم می کند .



Power Supply ۲.۵.۱

منبع تغذیه (Power Supply) ، ولتاژ AC برق شهری را به ولتاژ DC با اندازه های متفاوت و مناسب برای استفاده ی قطعات کامپیوتر فراهم می کند ، همچنین منبع تغذیه رابط های مختلفی را برای تغذیه ی برق قطعات مختلف کامپیوتر دارا می باشد .

منبع تغذیه ولتاژ مختلفی از جمله 5v و 12v و 3.3v و . . . تولید می کند که از طریق رنگ های مختلفی که به آنها نسبت داده شده اند می توان آنها را شناخت ، در جدول زیر لیستی از رنگ های مختلفی که در منبع تغذیه ی کامپیوتر برای تفکیک ولتاژهای مختلف استفاده می شود مشاهده می کنید .

Orange		+3.3 v
Red		+5 v
Black		Ground
Yellow		+12 v
Green		Power On
Purple		+5 v StandBy
Blue		-12 v



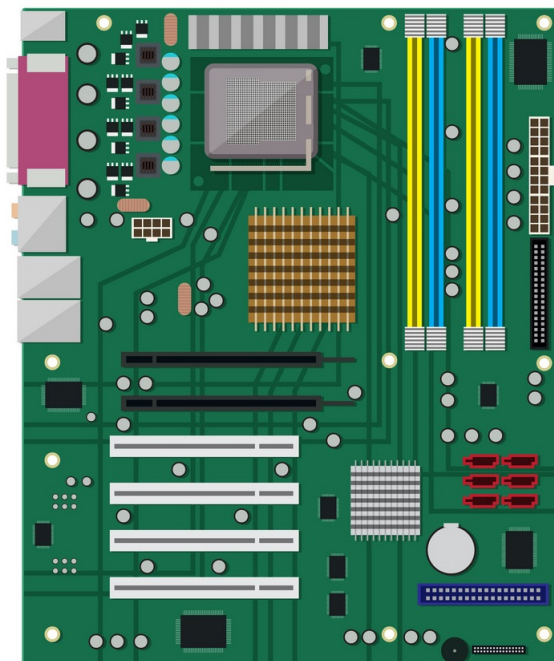
۳.۵.۱ MotherBoard

مادربورد (MotherBoard) قطعه ی اصلی سیستم کامپیوتری است و یک برد با مدار های مجتمع و درگاه هایی می باشد که قطعات مختلف کامپیوتر از جمله :

- CPU
- Hard Disk
- RAM

- CD & DVD Drive

را به هم متصل می کند .



۴.۵.۱ CPU

CPU اکثر اعمال محاسباتی را انجام می دهد که عملکرد کامپیوتر را محقق می سازد و به عنوان مغز کامپیوتر شناخته می شود .

CPU دستورالعمل های برنامه را برای اجرا از RAM دریافت می کند

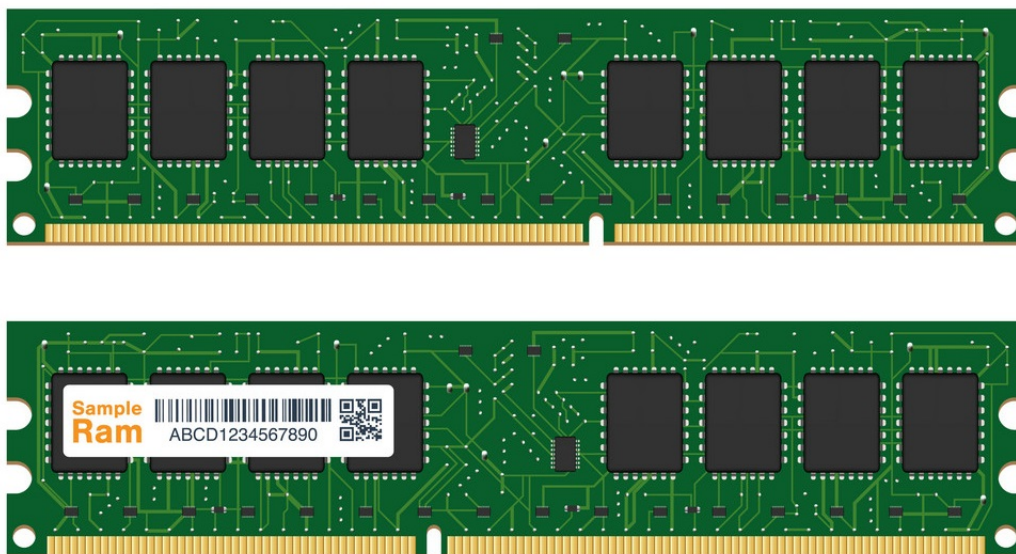
clock speed یکی از مشخصه های CPU می باشد که تعیین می کند دستورالعمل ها با چه سرعتی اجرا شوند و با واحد GHz بیان می شود .

CPU های مدرن قابلیت Overclock را فراهم می کنند که باعث افزایش عملکرد CPU می شود ولی دمای CPU را افزایش می دهد و بنابراین به سیستم خنک سازی بهتری نیازمند است .



۵.۵.۱ RAM

کد ها و داده هایی را که توسط CPU در حال استفاده و دسترسی هستند در خود نگه می دارد .



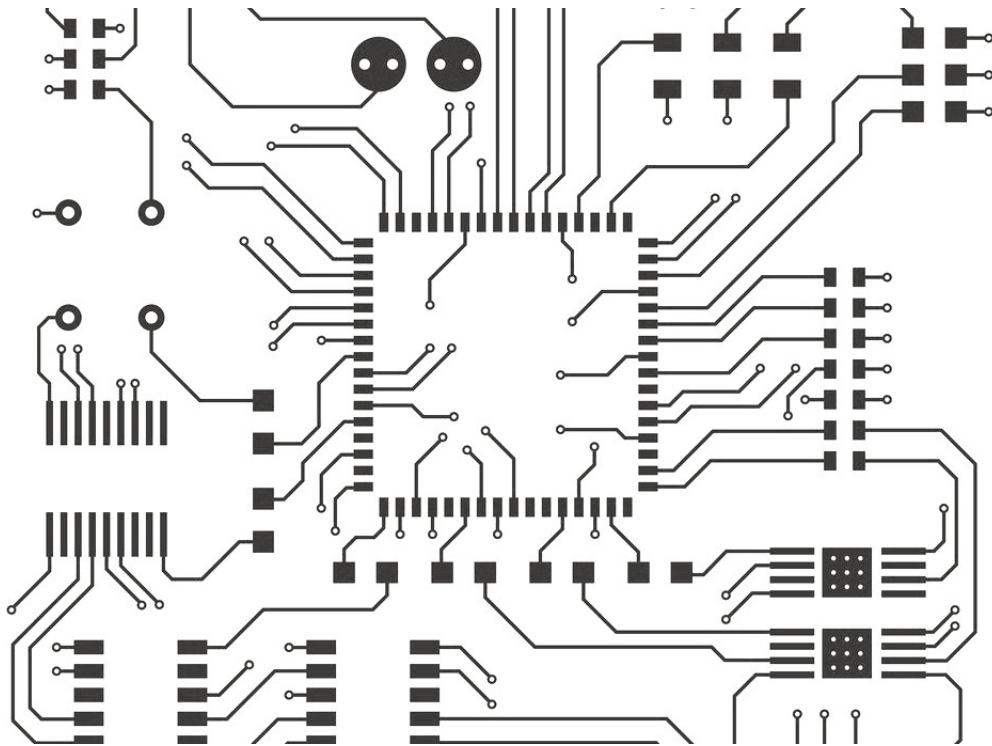
۶.۵.۱ ROM

ROM از نوع حافظه های غیر فرار است که در کامپیوتر و سایر قطعات الکترونیکی استفاده می شود . اطلاعاتی که در ROM ذخیره می شوند بعد از تولید حافظه دیگر قابلیت تغییر را ندارد . هر چند EPROM و EEPROM قابلیت پاک شدن و دوباره برنامه ریزی شدن را دارند . BIOS را در خود نگه می دارد که وقتی کامپیوتر روشن می شود اجرا می شود .

فرآیندی که هنگام روشن شدن کامپیوتر توسط BIOS انجام می شود ، Bootstrapping نام دارد .

BUS ۷.۵.۱

درگاه یا BUS ، CPU را به قسمت های مختلف کامپیوتر متصل می کند



Video Card ۸.۵.۱

کارت گرافیک یا Video Card محاسبات گرافیکی کامپیوتر را انجام می دهد و تصاویر خروجی را به دستگاه های نمایشگر ارسال می کند .



۶.۱ نرم افزار چیست؟

نرم افزار مجموعه ای از اطلاعات و دستورالعمل هایی است که می تواند توسط سخت افزار ذخیره و اجرا شود و تعیین می کند که کامپیوتر چه کاری را انجام دهد .

۱.۶.۱ انواع گروه بندی نرم افزار

- نرم افزارهای سیستمی
- نرم افزارهای زمان حقیقی
- نرم افزارهای تجاری
- نرم افزار های مهندسی و علمی
- نرم افزار های تعبیه شده
- نرم افزار های کامپیوترهای شخصی
- نرم افزارهای مبتنی بر وب
- نرم افزارهای هوش مصنوعی

نرم افزارهای سیستمی

مجموعه ای از برنامه هاست که برای سرویس دهی به برنامه های دیگر نوشته شده اند .
مثل :

- کامپایلر ها
- ویراستار ها
- برنامه های مدیریت فایل

مشخصه های نرم افزار های سیستمی

- بر هم کنش سنگین با سخت افزار کامپیوتر
- استفاده سنگین توسط چند کاربر
- لزوم زمان بندی برای انجام کارها
- مدیریت فرآیند و اشتراک منابع
- ساختمان داده های پیچیده
- واسطهای خارجی چندگانه

نرم افزارهای زمان حقیقی

نرم افزاری که رویداد های جهان واقعی را همانطوری که رخ می دهند، نظارت ، تحلیل و کنترل می کنند .

عناصر نرم افزار زمان حقیقی

- قطعه جمع آوری کننده داده ها
- ⊠ اطلاعات را از محیط خارجی جمع آوری و قالب بندی می کند .
- قطعه تحلیل کننده
- ⊠ اطلاعات را بنا به نیاز کاربردی انتقال می دهد .

• قطعه کنترل / خروجی

☒ به محیط خارجی پاسخ می دهد

• قطعه نظارت

☒ همه ی قطعات دیگر را هماهنگ می کند .

نرم افزار های تجاری

این نوع برنامه های کاربردی، داده های موجود را دوباره به شیوه ای سازماندهی می کند که عملیات تجاری و تصمیم گیری مدیریتی تسهیل شوند .

نرم افزارهای تعبیه شده

برای کنترل محصولات و سیستم های مربوط به بازارهای صنعتی و مصرفی به کار می رود .
مثل :

• صفحه کلید برای ماکروویو

• عملیات دیجیتال در خودرو

* کنترل سوخت

* صفحه نمایش داشبورد

* سیستم ترمز

۷.۱ سیستم عامل چیست؟

سیستم عامل برنامه ای است که سخت افزار کامپیوتر را مدیریت می کند ، همچنین سیستم عامل به عنوان یک رابط بین کاربر و سخت افزار کامپیوتر می باشد

۱.۷.۱ نمونه هایی از سیستم عامل های کامپیوترهای شخصی

- Microsoft Windows
 - Windows NT - 1993
 - Windows 98 - 1998
 - Windows Me - 2000
 - Windows XP - 2001
 - Windows Vista - 2007
 - Windows 7 - 2009
 - Windows 8 - 2012
 - Windows 10 - 2015
- MacOS
 - Mac OS X Kodiak - 2000
 - Mac OS X 10.2 Jaguar - 2002
 - Mac OS X Panther - 2003
 - Mac OS X Tiger - 2005
 - Mac OS X Leopard - 2007
 - Mac OS X Snow Leopard - 2009
 - Mac OS X Lion - 2011
 - OS X Mountain Lion - 2012
 - OS X Mavericks - 2013
 - OS X Yosemite - 2014
 - OS X El Capitan - 2015
 - macOS Sierra - 2016
 - macOS High Sierra - 2017
 - macOS Mojave - 2018

- macOS Catalina - 2019
- Linux
 - Debian
 - * Linux Mint
 - * Ubuntu
 - Fedora
 - * Red Hat

۲.۷.۱ نمونه هایی از سیستم عامل های تلفن های همراه

- Android
 - Android 1.5 Cupcake (API 3)
 - Android 1.6 Donut (API 4)
 - Android 2.0 Eclair (API 5)
 - Android 2.3 Gingerbread (API 9)
 - Android 4.0 Ice Cream Sandwich (API 14)
 - Android 4.4 KitKat (API 19)
 - Android 5.0 Lollipop (API 21)
 - Android 6.0 Marshmallow (API 23)
 - Android 7.0 Nougat (API 24)
 - Android 8.0 Oreo (API 26)
 - Android 9 Pie (API 28)
 - Android 10 (API 29)
- iOS
- Windows Phone

۸.۱ برنامه نویسی چیست؟

برنامه نویسی کامپیوتر فرآیند طراحی و ساخت یک برنامه ی اجرایی کامپیوتر است .
برنامه نویسی شامل موارد زیر می باشد :

- آنالیز مسئله

- طراحی الگوریتم

- پیاده سازی الگوریتم

هدف برنامه نویسی تولید یک مجموعه از دستورالعمل ها برای خودکار سازی انجام یک وظیفه می باشد .

۱.۸.۱ انواع زبانهای برنامه نویسی

انواع مختلفی از زبان های برنامه نویسی وجود دارد که هر کدام از آنها ویژگی ها و کاربرد های مختلفی دارند اما ساختار یکسانی دارند .

لزومی به دانستن همه ی زبان های برنامه نویسی نیست و در صورتی که شما یک زبان برنامه نویسی را خوب بدانید و چگونگی استفاده از متغیرها ، توابع ، کلاس ها و دیگر قابلیت های ارائه شده توسط یک زبان را بدانید در مدت زمان اندکی می توانید هر زبان برنامه نویسی دیگری را یاد بگیرید

- C
- C++
- C#
- Java
- Python
- PHP
- Javascript
- ...

فصل ۲

شبکه و اینترنت

۱.۲ شبکه ی کامپیوتری چیست؟

شبکه ی کامپیوتری یک شبکه ی ارتباطی دیجیتالی برای اشتراک گذاری منابع بین کامپیوتر هاست .

ارسال اطلاعات بین کامپیوتر ها توسط لینک های ارتباطی شامل کابل های فیزیکی مثل

:

- زوج های به هم تابیده

- فیبر نوری

و یا توسط روش های بدون سیم مثل

- Wi-Fi

- مایکروویو

- ماهواره

انجام می شود .

۱.۱.۲ دلایل استفاده از شبکه

- استفاده از منابع اشتراکی

- کاهش هزینه ها
- دسترسی آسان و سریع به منابع
- دسترسی از راه دور به منابع
- تبادل اطلاعات
- افزایش اطمینان

۲.۱.۲ تقسیم بندی شبکه از نظر جغرافیایی

Personal Aera Network (PAN)

شبکه های زیر ۱۰ متر با ۲ الی ۳ کامپیوتر

Local Aera Network (PAN)

شبکه های زیر ۵۰۰ متر با فاصله ی ۱ الی ۲ ساختمان

Campus Aera Network (CAN)

شبکه هایی در حد یک دانشگاه با چندین دانشکده در ساختمان های مختلف

Metropolitan Aera Network (MAN)

شبکه هایی در حد یک شهر که از اتصال چندین شبکه ی LAN به وجود می آید

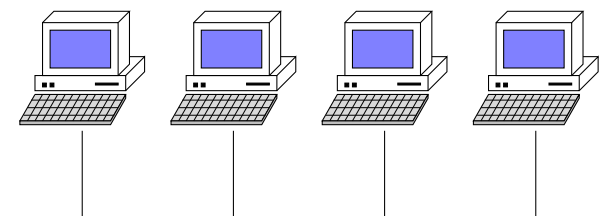
Wide Aera Network (WAN)

شبکه هایی در گستره ی یک کشور یا جهان

۲.۲ انواع توپولوژی های شبکه

۱.۲.۲ Bus

شبکه ای که از توپولوژی bus استفاده می کند ، معمولا از یک کابل تشکیل شده است که به کامپیوترها متصل است و هر کامپیوتر متصل به کابل می تواند سیگنال یا اطلاعات را در طول کابل بفرستد و بقیه ی کامپیوتر ها می توانند اطلاعات را دریافت کنند . ولی کامپیوتر ها باید طوری مدیریت شوند که در هر لحظه فقط یک کامپیوتر بتواند سیگنال بفرستد



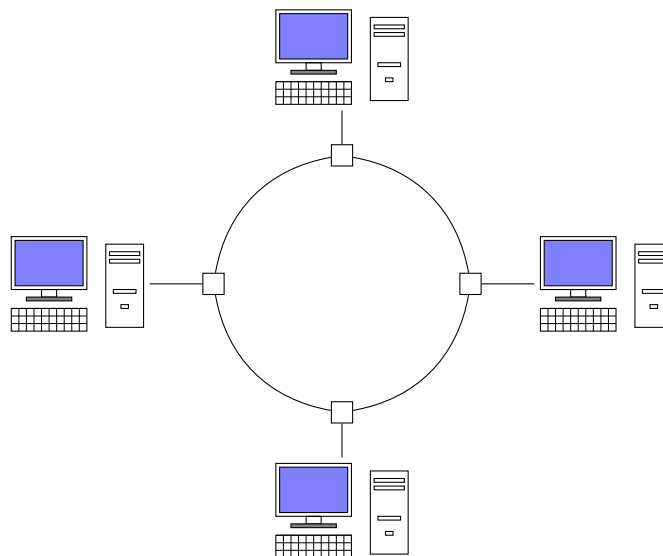
مزایا و معایب توپولوژی Bus

- هزینه ی راه اندازی پایین
- سرعت پایین، چون تنها یک مسیر وجود دارد
- تصادم اطلاعات باعث می شود داده ها از بین بروند

Ring ۲.۲.۲

شبکه ای که از توپولوژی ring استفاده می کند ، کامپیوتر ها را در یک حلقه ی بسته به هم متصل می کند به این صورت که کابلی کامپیوتر اول را به کامپیوتر دوم متصل می کند ، کابل دیگری کامپیوتر دوم را به کامپیوتر سوم متصل می کند و این روال به همین ترتیب ادامه می باشد تا زمانی که کابلی کامپیوتر آخر را به اولین کامپیوتر متصل کند .

بعضی از تکنولوژی ها برای پیاده سازی توپولوژی ring نیاز به این دارند که کامپیوتر به دستگاه کوچکی متصل شود ، مزیت استفاده از یک دستگاه مجزا این است که حتی اگر کامپیوتری ارتباط خود را از شبکه قطع کند ، حلقه همچنان پابرجاست



مزایا و معایب توپولوژی Star

- پهنای باند افزایش می یابد
- اضافه و حذف کردن کامپیوترها آسان است

Mesh ۳.۲.۲

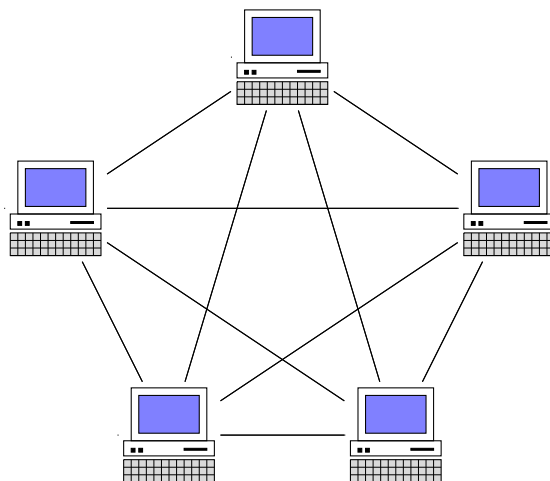
توپولوژی mesh بین هر دو کامپیوتر که در شبکه وجود دارد ارتباط مستقیم برقرار می کند ، هزینه ی بالا عیب بزرگ این توپولوژی می باشد .

شبکه ی mesh ای که n کامپیوتر را به هم متصل می کند ، به تعداد

$$\frac{n!}{(n-2)!2!} = \frac{n^2 - n}{2}$$

connection نیاز دارد

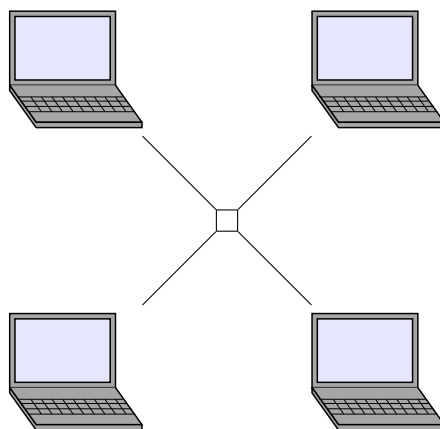
نکته ی مهمی که مشاهده می شود این است که تعداد connection هایی که برای توپولوژی mesh استفاده می شود از تعداد کامپیوتر های شبکه رشد بیشتری دارد و از آنجایی که هزینه ی برقراری هر ارتباط بالاست بنابراین LAN های کمتری از توپولوژی mesh استفاده می کنند



Star ۴.۲.۲

یک شبکه با توپولوژی star همه ی کامپیوتر ها را به یک نقطه ی مرکزی متصل می کند ، از آنجایی که شکل توپولوژی star شبیه بک چرخ می باشد ، مرکز چنین شبکه هایی hub نامیده می شود .

hub یک دستگاه الکترونیکی است ، که اطلاعات را از کامپیوتر فرستنده دریافت می کند و به مقصد مورد نظر تحویل می دهد .



۳.۲ سخت افزار های ایجاد شبکه

Hub ۱.۳.۲

hub یک سخت افزار شبکه برای ارتباط بین چندین دستگاه به یکدیگر است که باعث می شود همه ی آنها به عنوان یک مجموعه در نظر گرفته شوند .

hub دارای چندین port ورودی-خروجی است که در آن سیگنالی که به عنوان ورودی در یک port خاصی دریافت می شود به همه ی port های دیگر به غیر از خودش ارسال می شود .



۲.۳.۲ Switch

switch در شبکه یک دستگاه الکترونیکی پرسرعت است که اطلاعات را از ورودی دریافت می کند و به سمت مقصد ارسال می کند .
hub و switch از لحاظ شکل ظاهری بسیار شبیه به هم می باشند .

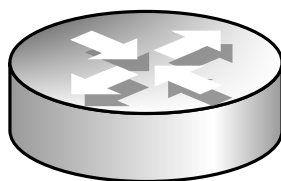


تفاوت switch و hub

در hub اطلاعات دریافت شده بدون توجه به آدرس مقصد به همه ی port های دیگر به غیر port دریافتی ارسال می شود ، ولی در switch اطلاعات فقط به port ای ارسال می شود که در آدرس مقصد تعیین شده است .

۳.۳.۲ Router

router سخت افزار شبکه است که تعدادی ورودی و خروجی دارد و بسته های اطلاعاتی را از ورودی ها تحویل گرفته و بر اساس آدرس مقصد یکی از کانال های خروجی را برای ارسال اطلاعات انتخاب نماید به طوری که بسته را به مقصد نزدیک نماید در واقع router عملکرد هدایت و مسیریابی اطلاعات را در اینترنت بر عهده دارد که با استفاده از جدول مسیریابی که در خود دارد ، تصمیم میگیرد که اطلاعات را به کدام شبکه ی بعدی بفرستد .

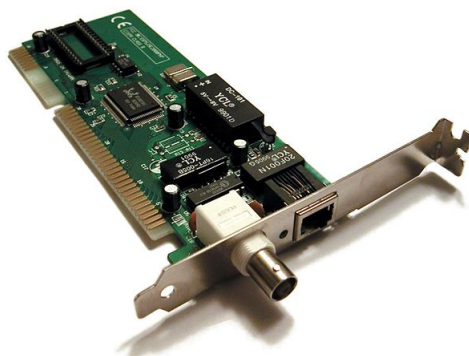


میزبان (Host)

عضوی از شبکه است که هیچ نقشی در هدایت بسته های اطلاعاتی در شبکه ندارد و فقط تولید کننده یا دریافت کننده بسته های اطلاعاتی است ، مثل : کامپیوتر شخصی یا تلفن همراه شما .

Network Interface Controller (NIC)

کنترلر واسط شبکه یا Network Interface Controller یک سخت افزار کامپیوتری است که کامپیوتر را به شبکه متصل می کند .



۴.۲ MAC Address

MAC Address یک شناسه ی منحصر به فرد است که به کنترلگر واسط شبکه نسبت داده می شود و به عنوان آدرس سخت افزاری میزبان در شبکه مورد استفاده قرار می گیرد . نمونه ای از MAC Address به صورت زیر است .

00:0a:95:9d:68:16

۵.۲ اینترنت چیست؟

اینترنت یک سیستم جهانی است که شبکه های کامپیوتری را به هم متصل می کند . در واقع اینترنت شبکه ای از شبکه هاست .

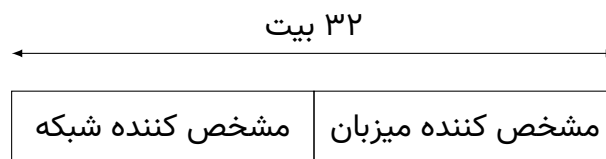
۶.۲ IP Address

آدرس پروتکل اینترنتی یا IP یک نماد عددی است که به هر دستگاه موجود در شبکه تخصیص داده می شود .

آدرس IP به دو قسمت اصلی تقسیم می شود :

• قسمت شبکه

• قسمت میزبان



مزیت استفاده از مدل دو بخشی آدرس شبکه و آدرس میزبان برای آدرس های IP ، کمینه کردن تعداد ورودی ها در جدول مسیریابی است . به جای اینکه برای هر میزبان در یک شبکه یک رکورد در جدول مسیریابی داشته باشیم، میتوان با استفاده از یک رکورد همه ی میزبان ها را در یک شبکه خلاصه کرد که فقط شامل قسمت آدرس شبکه است که پیشوند مشترک برای همه ی میزبان های شبکه می باشد .

۷.۲ انواع کلاسهای IP

• Class A با عدد 0 شروع می شود

$$\begin{aligned}
 0.0.0.0 &= \underbrace{00000000}_{Network} . \underbrace{00000000.00000000.00000000}_{Host} \\
 127.255.255.255 &= \underbrace{01111111}_{Network} . \underbrace{11111111.11111111.11111111}_{Host} \\
 &0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH
 \end{aligned}$$

• Class B با عدد 10 شروع می شود

$$\begin{aligned}
 128.0.0.0 &= \underbrace{10000000.00000000}_{Network} . \underbrace{00000000.00000000}_{Host} \\
 191.255.255.255 &= \underbrace{10111111.11111111}_{Network} . \underbrace{11111111.11111111}_{Host} \\
 &10nnnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH
 \end{aligned}$$

• Class C با عدد 110 شروع می شود

$$\begin{aligned}
 192.0.0.0 &= \underbrace{11000000.00000000.00000000}_{Network} . \underbrace{00000000}_{Host} \\
 223.255.255.255 &= \underbrace{11011111.11111111.11111111}_{Network} . \underbrace{11111111}_{Host} \\
 &110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH
 \end{aligned}$$

• Class D با عدد 1110 شروع می شود

$$\begin{aligned}
 224.0.0.0 &= 11100000.00000000.00000000.00000000 \\
 239.255.255.255 &= 11101111.11111111.11111111.11111111 \\
 &1110XXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX
 \end{aligned}$$

• Class E با عدد 11110 شروع می شود

$$240.0.0.0 = 11110000.00000000.00000000.00000000$$

$$255.255.255.255 = 11111111.11111111.11111111.11111111$$

$$1111XXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX$$

۸.۲ خلاصه ی کلاس های IP به صورت جدول

Class	Starting Bits	Size of network (bit)	Size of Host (bit)
Class A	0	8	24
Number of networks		Hosts per Network	
128 (2^7)		16,777,216 (2^{24})	
Total addresses in class		Start address	End address
2,147,483,648 (2^{31})		0.0.0.0	127.255.255.255

Class	Starting Bits	Size of network (bit)	Size of Host (bit)
Class B	10	16	16
Number of networks		Hosts per Network	
16,384 (2^{14})		65,536 (2^{16})	
Total addresses in class		Start address	End address
1,073,741,824 (2^{30})		128.0.0.0	191.255.255.255

Class	Starting Bits	Size of network (bit)	Size of Host (bit)
Class C	110	24	8
Number of networks		Hosts per Network	
2,097,152 (2^{21})		256 (2^8)	
Total addresses in class		Start address	End address
536,870,912 (2^{29})		192.0.0.0	223.255.255.255

یک شبکه کلاس C با آدرس 194.34.56.0 داده شده است، چند میزبان برای این شبکه وجود دارد ؟

$$194.34.56.0 \rightarrow \underbrace{11000010.00100010.00111000}_{Network} . \underbrace{00000000}_{Host}$$

$$2^8 - 2$$

یک شبکه کلاس B با آدرس 166.23.0.0 داده شده است، چند میزبان برای این شبکه وجود دارد ؟

$$166.23.0.0 \rightarrow \underbrace{10100110.00010111}_{Network} . \underbrace{00000000.00000000}_{Host}$$

$$2^{16} - 2$$

مثال

مشخص کنید که آدرس $192.168.1.18/24$ جزء کدام دسته کلاس آدرس می باشد و آدرس خود شبکه ، اولین میزبان ، آخرین میزبان و آدرس Broadcast را در این شبکه مشخص کنید ؟

- آدرس خود شبکه آدرسی است که تمام بیت ها در قسمت میزبان برابر با صفر باشد
- آدرس Broadcast آدرسی است که تمام بیت ها در قسمت میزبان برابر با یک باشد

$$192.168.1.18 \rightarrow 11000000.10101000.00000001.00010010 \Rightarrow \text{class } C$$

$$\underbrace{192.168.1}_{\text{Network}} . \underbrace{18}_{\text{Host}}$$

$$\text{Subnet} = 192.168.1.00000000$$

$$1st \text{ Host} = 192.168.1.00000001$$

$$Last \text{ Host} = 192.168.1.11111110$$

$$Broadcast = 192.168.1.11111111$$

مثال

مشخص کنید که آدرس 172.16.35.123/20 جزء کدام دسته کلاس آدرس می باشد و آدرس خود شبکه ، اولین میزبان ، آخرین میزبان و آدرس Broadcast را در این شبکه مشخص کنید ؟

- آدرس خود شبکه آدرسی است که تمام بیت ها در قسمت میزبان برابر با صفر باشد
- آدرس Broadcast آدرسی است که تمام بیت ها در قسمت میزبان برابر با یک باشد

$$172.16.35.123 \rightarrow 10101100.00010000.00100011.01111011 \Rightarrow \text{class } B$$

$$\underbrace{172.16}_{\text{Network}} . \underbrace{35.123}_{\text{Host}}$$

Subnet →	172.16.0010	0000.00000000
1st Host →	172.16.0010	0000.00000001
Last Host →	172.16.0010	1111.11111110
Broadcast →	172.16.0010	1111.11111111

Subnet →	172.16.32.0
1st Host →	172.16.32.1
Last Host →	172.16.47.254
Broadcast →	172.16.47.255

مثال

مشخص کنید که آدرس 172.16.129.1/17 جزء کدام دسته کلاس آدرس می باشد و آدرس خود شبکه ، اولین میزبان ، آخرین میزبان و آدرس Broadcast را در این شبکه مشخص کنید ؟

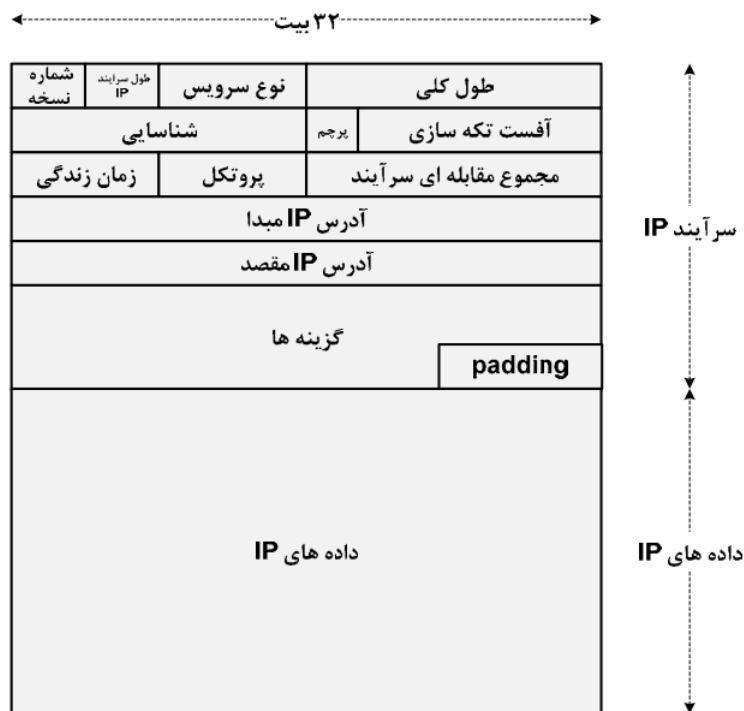
$$172.16.129.1 \rightarrow 10101100.00010000.10000001.00000001 \Rightarrow \text{class } B$$

$$\underbrace{172.16}_{\text{Network}} . \underbrace{129.1}_{\text{Host}}$$

Subnet →	172.16.1	00000000.00000000
1st Host →	172.16.1	00000000.00000001
Last Host →	172.16.1	11111111.11111110
Broadcast →	172.16.1	11111111.11111111

Subnet →	172.16.128.0
1st Host →	172.16.128.1
Last Host →	172.16.255.254
Broadcast →	172.16.255.255

۹.۲ ساختار IPv4



ساختار بسته های IP

یک بسته آی پی از دو بخش سرآیند (header) و داده تشکیل می شود

۱.۹.۲ سرآیند (header)

سرآیند بسته IPv4 از ۱۳ فیلد تشکیل می شود که ۱۲ تای آنها اجباری هستند. فیلد سیزدهم اختیاری است. این فیلدها به گونه ای در سرآیند بسته بندی می شوند که پرارزش ترین بایت در ابتدا بیاید.

شماره نسخه

نسخه: اولین فیلد در سرآیند یک بسته IP، فیلد ۴ بیتی نسخه است. مقدار این فیلد برای بسته IP نسخه چهار، ۴ می باشد.

طول سرآیند

این فیلد طول سرآیند بسته را بر حسب تعداد کلمه های ۳۲ بیتی مشخص می‌کند. از آنجا که در یک بسته IP نسخه ۴ طول فیلد اختیاری ثابت نیست، اندازه سرآیند در این فیلد ذخیره می‌شود (که برابر با محل شروع فیلد داده نیز هست). کمترین مقدار مجاز برای این فیلد ۵ است (RFC 791) که برابر با $32 \times 5 = 160$ بیت می‌باشد. و از آنجا که این فیلد ۴ بیتی است بیشترین مقدار آن ۱۵ کلمه یا $32 \times 15 = 480$ بیت است.

فیلد نوع سرویس

فیلد نوع سرویس، نوع سرویس دریافتی را از نظر پارامترهایی نظیر:

- میزان تقدم

- تاخیر

- گذردهی

- اطمینان

مشخص می‌کند.

فیلد طول کلی

فیلد طول کلی نشان دهنده ی طول بسته ی IP شامل سرآیند IP و داده بر حسب بایت می‌باشد. این فیلد ۱۶ بیت طول دارد.

فیلد شناسایی

فیلد شناسایی برای هر بسته به طور یکتا مقدار دهی می‌شود و نشان دهنده ی شماره ی بسته می‌باشد.

فیلد پرچم

فیلد پرچم ۳ بیت طول دارد . اولین بیت این فیلد همواره صفر است . بیت های دوم و سوم به ترتیب بیت های DF و MF می باشند . اگر مقدار پرچم DF برابر با ۱ باشد ، به این معنی است که نباید بسته تکه سازی شود . چنانچه پرچم MF برابر با ۱ باشد ، گیرنده متوجه خواهد شد که تمام تکه های بسته اصلی هنوز نیامده اند و تکه های دیگری در راه می باشند .

زمان زندگی (TTL)

فیلد زمان زندگی که بر حسب ثانیه اندازه گیری می شود نشان دهنده ی حداکثر زمانی است که یک بسته IP می تواند در شبکه زنده بماند . این فیلد ۸ بیتی از باقی ماندن بسته های سرگردان IP در شبکه جلوگیری می کند. مقدار این بسته توسط پیش فرض سیستم تعیین می شود و پس از عبور از هر مسیریاب یک شماره از این فیلد کم می شود. اگر این مقدار صفر شود مسیریاب بسته را حذف می کند و یک پیام ICMP به فرستنده بسته می فرستد و فرستنده متوجه می شود که عمر بسته پایان یافته است.

فیلد پروتکل

فیلد پروتکل برای مشخص کردن پروتکل لایه بالایی که باید داده های موجود در بسته IP را دریافت کند ، استفاده می شود .

مجموع مقابله ای سرآیند (Header Checksum)

این فیلد ۱۶ بیتی برای کشف خطا به کار می رود. در هر جهش (hop) باید مجموع مقابله ای سرآیند محاسبه و با مقدار این فیلد مقایسه شود. اگر این دو مقدار برابر نباشند به معنی بروز خطای انتقال است و بسته حذف می شود . نحوه ی محاسبه به این صورت است که مکمل ۱ تمام مقادیر ۱۶ بیتی موجود در سرآیند IP با هم جمع می شوند (به جز خود فیلد مجموع مقابله ای سرآیند) ، سپس مکمل ۱ مجموع محاسبه می شود ، اگر این دو مقدار با هم برابر باشند به معنی عدم وجود خطا در بسته می باشد . هر دو پروتکل UDP و TCP ، فیلد مجموع مقابله ای دارند.

فیلد گزینه و فیلد padding

از فیلد گزینه برای فراهم سازی برخی امکانات اضافی در پروتکل IP استفاده می شود چنانچه طول فیلد گزینه مضربی از ۴ نبوده ، به مقدار کافی در ناحیه ی padding بیت صفر اضافه می شود تا فیلد گزینه مضربی از ۳۲ بیت باشد .

۱۰.۲ انواع پروتکل ها در شبکه

DNS ۱.۱۰.۲

DNS مخفف Domain Name System یک سیستم سلسه مراتبی نام گذاری برای کامپیوترها، سرویس ها، یا منابع دیگر است که به شبکه اینترنت متصل هستند .

وقتی می خواهید وارد سایتی شوید باید آدرس IP آن را بدانید اما چون به خاطر سپردن آدرس های IP دشوار است ، هر آدرس IP به نام مخصوصی نگاشته می شود . کل نشانی های اینترنت درون بانک های اطلاعاتی توزیع شده ای هستند که هیچ تمرکزی روی نقطه ای خاص از شبکه ندارند.

روش ترجمه نام بدین صورت است که وقتی یک برنامه کاربردی مجبور است برای برقراری یک ارتباط، معادل نشانی آی پی از یک ماشین با نامی مثل cs.ucsb.edu را بدست بیاورد، قبل از هر کاری یک تابع کتابخانه ای را صدا می زند، به این تابع کتابخانه ای تابع تحلیلگر، نام (Name Resolver) گفته می شود.

تابع تحلیلگر، نام یک نشانی نمادین را که بایستی ترجمه شود، به عنوان پارامتر ورودی پذیرفته و سپس یک بسته درخواست (Query Packet) به روش UDP تولید کرده و به نشانی یک کارساز DNS (که به صورت پیش فرض مشخص می باشد) ارسال می کند. همه ماشین های میزبان، حداقل باید یک نشانی آی پی از یک سرویس دهنده ساناد را در اختیار داشته باشند. این «سرویس دهنده محلی» پس از جستجو، نشانی آی پی معادل با یک نام نمادین را برمی گرداند.

«تابع تحلیلگر نام» نیز آن نشانی آی پی را به برنامه کاربردی تحویل می دهد با پیدا شدن نشانی آی پی، برنامه کاربردی می تواند عملیات مورد نظرش را ادامه دهد.

روش های جستجو

همانگونه که اشاره شد، اسامی نمادین در شبکه اینترنت که خود در قالب حوزه ها و زیر حوزه ها سازماندهی شده اند، در یک فایل متمرکز ذخیره نمی شوند بلکه روی کل شبکه اینترنت توزیع شده اند، به همین دلیل برای ترجمه یک نام به نشانی آی پی ممکن است چندین مرحله «پرس و جو» صورت بگیرد تا یک نشانی پیدا شود.

طبیعی است که یک پرس و جو برای تبدیل یک نام حوزه همیشه موفقیت آمیز نباشد و ممکن است به پرس و جوهای بیشتری نیاز شود یا حتی ممکن است یک نشانی نمادین اشتباه باشد و هیچ معادل نشانی آی پی نداشته باشد.

سه روش برای پرس و جوی نام در سرویس دهنده های نام وجود دارد :

• پرس و جوی تکراری Iterative Query

• پرس و جوی بازگشتی Recursive Query

• پرس و جوی معکوس Reverse Query

پرس و جوی تکراری

در پرس و جوی تکراری قسمت اعظم تلاش برای تبدیل یک نام بر عهده سرویس دهنده محلی است؛ این DNS حداقل به نشانی ماشین، Root، به عنوان نقطه شروع نیاز دارد. وقتی یک تقاضای ترجمه نشانی به سرویس دهنده محلی ارسال می شود در صورتی که قادر به ترجمه نام به معادل نشانی آی پی آن باشد، معادل نشانی آی پی نام مورد نظر را به تقاضاکننده برمی گرداند. (این حالت وقتی است که سرویس دهنده محلی قبلاً آن نام را ترجمه و در یک فایل ذخیره کرده باشد) در غیر این صورت سرویس دهنده محلی خودش یک تقاضا برای DNS سطح بالا ارسال می کند. این سرویس دهنده، نشانی ماشینی را که می تواند برای ترجمه نام مورد نظر مفید باشد، به سرویس دهنده محلی معرفی می کند؛ سرویس دهنده محلی مجدداً یک تقاضا به ماشین معرفی شده در مرحله قبل ارسال می کند.

پرس و جوی بازگشتی

در این روش هر گاه برنامه ای بخواهد نشانی آی پی معادل یک نام مثل cs.yale.edu را بدست آورد، بگونه ای که قبلاً اشاره شد، «تابع سیستمی تحلیل نام» را فراخوانی می کند. این تابع یک ماشین را به عنوان سرویس دهنده محلی از قبل می شناسد و بنابراین تقاضای تبدیل نام

را به روش UDP برای آن ارسال کرده و منتظر جواب می‌ماند (پاسخ نهایی DNS طبیعتاً باید یک نشانی ۳۲ بیتی معادل نشانی آی‌پی یک ماشین باشد) دو حالت ممکن است اتفاق بیفتد:

ممکن است در بانک اطلاعاتی مربوط به سرویس دهنده محلی، نشانی آی‌پی معادل با آن نام از قبل وجود داشته و بالطبع به سرعت مقدار معادل نشانی آی‌پی آن بر می‌گردد. ممکن است در بانک اطلاعاتی سرویس دهنده محلی، معادل نشانی آی‌پی آن نام وجود نداشته باشد. مثلاً سرویس دهنده محلی در بانک اطلاعاتی خودش معادل نشانی آی‌پی نام cs.mit.edu را نداشته و طبیعتاً نمی‌تواند آن را ترجمه کند.

در چنین حالتی سرویس دهنده محلی موظف است بدون آنکه به تقاضا دهنده خبر بدهد، خودش رأساً به سرویس دهنده سطح بالاتر تقاضای ترجمه نشانی بدهد. در این حالت هم DNS سطح بالاتر به همین نحو، ترجمه نشانی را پیگیری می‌کند. یعنی اگر معادل نشانی آی‌پی آن نام را داشته باشد آن را برمی‌گرداند و در غیر اینصورت خودش از سرویس دهنده سطح پایینتر تقاضای ترجمه آن نام را می‌نماید و این مراحل تکرار می‌شود. در روش پرس و جوی بازگشتی ماشین سرویس دهنده محلی این مراحل متوالی را نمی‌بیند و هیچ کاری جز ارسال تقاضای ترجمه یک نشانی بر عهده ندارد و پس از ارسال تقاضا برای سرویس دهنده سطح بالا منتظر خواهد ماند.

بازهم تکرار می‌کنیم، روشی که DNS برای ترجمه نشانی بکار می‌برد می‌تواند بدون اتصال (UDP) باشد که این کار به سرعت عمل ترجمه نشانی می‌افزاید.

دقت کنید که در روش پرس و جوی تکراری نسبت به روش پرس و جوی بازگشتی، حجم عمده عملیات بر عهده سرویس دهنده DNS محلی است و مدیریت خطاها و پیگیری روند کار ساده‌تر خواهد بود و روش منطقی تری برای بکارگیری در شبکه اینترنت محسوب می‌شود. روش پرس و جوی بازگشتی برای شبکه‌های کوچک کاربرد دارد.

پرس و جوی معکوس

فرض کنید حالتی بوجود بیاید که یک سرویس دهنده، DNS نشانی آی‌پی یک ماشین را بداند ولی نام نمادین معادل با آن را نداند.

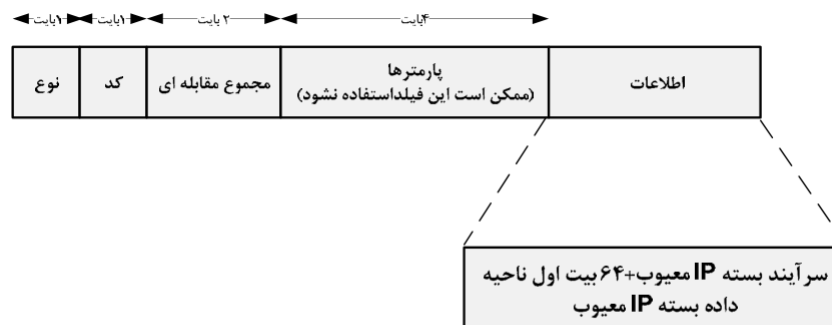
در چنین حالتی مسئله کمی حادث‌تر به نظر می‌رسد، چرا که برای ترجمه نامهای نمادین، چون این نامها دارای حوزه و زیرحوزه هستند، تحلیل نشانی‌ها ساده‌است؛ ولی ترجمه نشانی آی‌پی به معادل نام حوزه، از چنین روابطی تبعیت نمی‌کند؛ بعبارت بهتر هیچ ارتباط مستقیم و متناظری بین نشانی‌های آی‌پی و اسامی انتخاب شده در اینترنت وجود ندارد. برای یافتن نامهای متناظر با یک نشانی آی‌پی باید یک جستجوی کامل و در عین حال وقت گیر، انجام

بشود.

روش کار بدین صورت است که سرویس دهنده محلی یک تقاضا برای DNS متناظر با شبکه‌ای که مشخصه آن در نشانی آی‌پی، مشخص شده، ارسال می‌کند.

۲.۱۰.۲ ICMP

یکی از پروتکل‌های اصلی بسته پروتکل‌های اینترنت می‌باشد. مورد اصلی استفاده از آن در سیستم عامل‌های کامپیوترهای متصل به شبکه، برای ارسال پیام‌های خطا .



ساختار کلی پیام ICMP

ICMP متکی بر IP برای انجام کارهای خود است، و خودبخشی جدایی ناپذیر از IP می‌باشد.

از جمله خطاهایی که میتوان برای ارسال آن از ICMP استفاده کرد ، می توان به موارد زیر اشاره کرد .

- صفر شدن TTL
- عدم تحویل بسته به علت گم شدن یک تکه از بسته
- در دسترس نبودن یک پروتکل ، سرویس یا میزبان خاص در مقصد
- عدم توانایی پیش بردن یک بسته به خاطر عدم اجازه تکه سازی
- وقوع ازدحام در یک مسیر یا شبکه

پیام های ICMP برای اعلام وقوع خطا برای خود پیام های ICMP استفاده نمی شوند . زیرا پیام ها به شدت زیاد شده و به ترافیک شبکه اضافه می شود . هنگامی که یک مسیر یاب شبکه بسته ای را برای ارسال دریافت نماید ولی تشخیص دهد که مسیر یاب دیگری مسیر بهینه تری برای ارسال بسته به سمت مقصد دارد ، اقدام به ارسال پیام ICMP تغییر مسیر می نماید .

در حالت های زیر پیام ICMP تخطی زمانی فرستاده می شود .

- هر گاه مقدار فیلد TTL در بسته های IP به صفر برسد
- هرگاه یک تکه از بسته های IP تکه شده طی زمان مشخصی به مقصد نرسد ، مقصد یک پیام ICMP تخطی زمانی با مقدار کد ۱ ارسال می کند

پیام ICMP مشکل پارامتر

- چنانچه مسیر یاب متوجه مشکلی در پارامترهای سرآیند IP بسته های دریافتی شوند ، از پردازش بسته جلوگیری کرده و یک پیام ICMP مشکل پارامتر ارسال می شود .

پیام ICMP فرونشاندن مبدا

- هنگامی که یک مسیر یاب متوجه پر شدن ظرفیت حافظه ی خود می شود ، برای کاهش درخواست ها و کاهش ازدحام شبکه با حذف بسته های ورودی اضافی و فرستاده پیام ICMP فرو نشاندن مبدا به فرستندهایی که بیشترین درخواست ها را می فرستد از آن می خواهد که سرعت ارسال اطلاعات خود را کاهش دهند .

پیام های ICMP برای ارسال از بسته های IP استفاده می کنند ، و چون پروتکل IP تحویل پیام ها را ضمانت نمی کند بنابراین ممکن است پیام های ICMP گم شده و یا به خاطر ازدحام در مسیر یاب های میانی حذف شوند .

۳.۱۰.۲ ARP

Address Resolution Protocol یک پروتکل ارتباطی برای یافتن آدرس لایه پیوند، مانند MAC Address ، و ارتباطش با آدرس لایه شبکه (IPv4) است.

کاربرد و دلیل استفاده از پروتکل ARP

• از آنجاییکه در کامپیوتر مقصد، ابتدا لایه ی دوم قاب را از شبکه برداشته و بعد به لایه ی سوم که پروتکل IP است تحویل می دهد ، لذا دانستن تنها آدرس IP مقصد کفایت نکرده و باید آدرس سخت افزاری کامپیوتر مقصد نیز داشته باشیم ، به این علت از پروتکلی به نام ARP استفاده می کنیم . از پروتکل ARP برای استخراج آدرس لایه سخت افزاری که به آن MAC-Address گفته می شود از آدرس IP استفاده می شود .



قاب بسته ARP

محدودیت پروتکل ARP

• پروتکل ARP توسط پروتکل IP بسته بندی نمی شود ، بلکه مستقیماً توسط پروتکل لایه پیوند داده بسته بندی می گردد . این بدان معنی است که پیام های پروتکل ARP را نمی توان مسیریابی کرد، یعنی نمی تواند از مرز یک مسیریاب عبور کند .

به چه علت پیام درخواست ARP به صورت همه پخش می شود ؟

• در هنگام ارسال پیام درخواست ARP از آنجاییکه آدرس سخت افزاری مقصد هنوز معلوم نیست، بنابراین درخواست فوق در لایه ی دوم به صورت همه پخش می شود . شده طوری که همه ی میزبان های شبکه بتوانند آن را دریافت کنند .

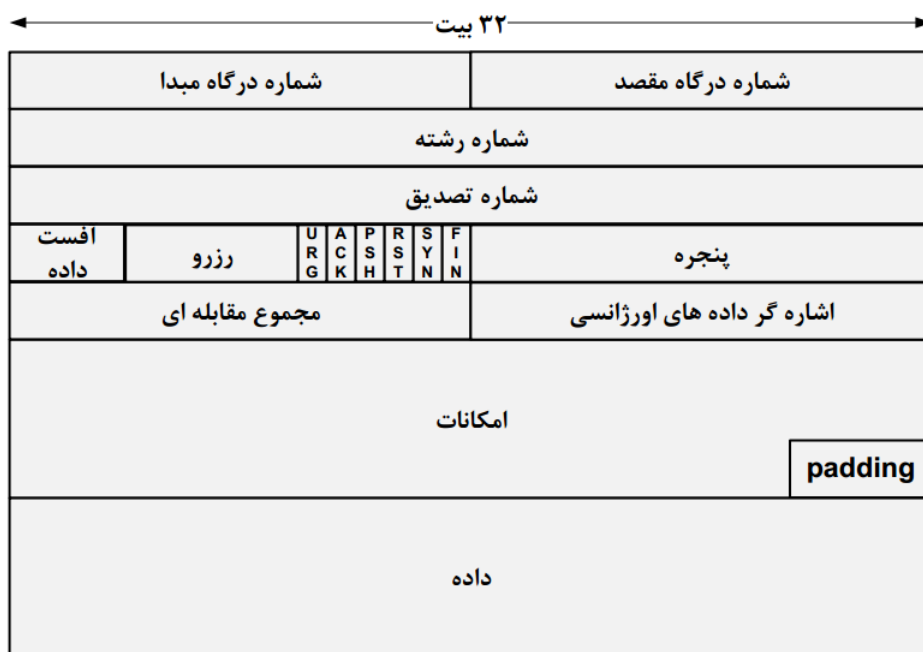
آیا پیام پاسخ ARP به صورت همه پخش می شود ؟ توضیح دهید ؟

• پاسخ ARP که توسط نود مقصد فرستاده می شود یک قاب همه پخش نیست ، زیرا این نود آدرس سخت افزاری را در پیام درخواست ARP دریافت کرده است . بنابراین در هنگام پاسخ دهی ، قاب پاسخ را به صورت تک پخش می دارد .

چگونه آزمون آدرس IP تکراری ARP انجام می شود ؟

- هر کامپیوتر در هنگام راه اندازی یک درخواست ARP را در شبکه منتشر می کند . در این پیام آدرس IP مقصد مساوی با آدرس IP فرستنده می باشد . در صورتی که فرستنده پاسخ پیام ARP را دریافت کند ، بدین معنی است که نود دیگری با این آدرس موجود می باشد که به معنای وجود آدرس های IP تکراری در شبکه می باشد .

۴.۱۰.۲ TCP



ساختار بسته TCP

Transmission Control Protocol که قرارداد کنترل انتقال یا پروتکل کنترل انتقال نیز گفته می شود؛ مجموعه ای از پروتکل های قراردادی است که پایه و اساس اینترنت می باشد. برای برقراری یک ارتباط گفتاری به وسیله اینترنت، در لایه انتقال از دو پروتکل TCP و UDP استفاده می شود. پروتکل TCP انتقال داده را با دقت و امنیت بالا انجام می دهد در حالیکه ویژگی پروتکل UDP انتقال سریع اطلاعات، بدون در نظر گرفتن اطمینان برای انتقال داده است

مهمترین وظیفه پروتکل TCP اطمینان از صحت ارسال اطلاعات است. پروتکل فوق اصطلاحاً «ارتباط اتصال‌گرا» نامیده می‌شود. علت این امر ایجاد یک ارتباط مجازی بین کامپیوترهای فرستنده و گیرنده، قبل از ارسال اطلاعات است. پروتکل‌هایی از این نوع، امکانات بیشتری را به منظور کنترل خطاهای احتمالی در ارسال اطلاعات فراهم نموده ولی به دلیل افزایش بار عملیاتی سیستم، کارایی آنان کاهش خواهد یافت. از پروتکل TCP به عنوان یک پروتکل قابل اطمینان نیز یاد می‌شود. به این علت که برای آگاهی از صحت اطلاعات ارسال شده، اطلاعات دیگری نیز به گیرنده فرستاده می‌شود. در صورتی که بسته‌های اطلاعاتی به درستی در اختیار فرستنده قرار نگیرند، فرستنده مجدداً اقدام به ارسال اطلاعات می‌نماید.

ویژگی های اصلی TCP را نوشته و به اختصار توضیح دهید ؟

• حمل داده پایه ای

* TCP توانایی حمل جریان پیوسته ای از بایت ها در هر دو جهت اتصال را دارد .

• اطمینان

* یکی از ویژگی های TCP تحویل مطمئن داده ها به صورت انتها به انتها است . برای مهیا سازی اطمینان TCP برای جبران داده های خراب ، گم شده از مدل ارسال مجدد تصدیق مثبت استفاده می نماید . در TCP سگمنت های جدید تنها زمانی فرستاده می شوند که سگمنت های قبلی ارسال شده تصدیق شده باشند .

* در TCP فرستنده با ارسال هر سگمنت ، منتظر دریافت پیام تصدیق مثبت (ACK) از طرف گیرنده می باشد . اگر ACK در یک بازه زمانی معین دریافت نشود ، سگمنت قبلی دوباره ارسال می شود .

* در TCP از مکانیزم شماره گذاری رشته برای مرتب کردن سگمنت هایی که خارج از نوبت دریافت شده اند و یا حذف سگمنت های تکراری استفاده می شود .

* در TCP در صورت وقوع خرابی در سگمنت های دریافتی ، با استفاده از فیلد مجموع مقابله ای در سرآیند بسته های TCP ، مشکل رفع می شود .

• کنترل جریان

* توسط مکانیزم کنترل جریان در TCP ، مقدار داده ارسال شده توسط فرستنده همواره کنترل می شود .

* پروتکل TCP از مکانیزم پنجره ی لغزان برای پیاده سازی کنترل جریان استفاده می کند .

• تسهیم سازی

* استفاده مشترک چندین فرآیند لایه کاربرد از امکانات TCP/IP ، تسهیم سازی نام دارد .

• اتصال انتها به انتها

• تقدم و امنیت

کاربرد فیلد های شماره رشته ارسال و شماره تصدیق را در بسته های TCP توضیح دهید ؟

• شماره رشته نشان دهنده ی اولین بایت داده در یک سگمنت TCP ارسالی می باشد .

• شماره تصدیق نشان دهنده ی شماره بایستی است که فرستنده ، انتظار دریافت آن از طرف مقابل را دارد .

• به عنوان مثال ، اگر فیلد شماره رشته ۱۰۰ باشد و فیلد شماره تصدیق ۲۰۰ باشد ، بدان معنی است که بسته ارسالی از بایت ۱۰۰ به بعد را شامل می شود و فرستنده تا بایت ۱۹۹ را به طرف مقابل می فرستد و منتظر بایت ۲۰۰ به بعد از طرف مقابل می باشد .

کاربرد هر یک از پرچم های TCP را توضیح دهید ؟

ACK هنگامی که ACK ، ۱ باشد نشان می دهد که فیلد شماره تصدیق معتبر است .

SYN برای نشان دادن باز شدن یک اتصال استفاده می شود

FIN برای قطع یک اتصال استفاده می شود

RST چنانچه در یک اتصال TCP خطای غیر قابل ترمیمی رخ دهد ، از بیت RST برای درخواست ری ست اتصال استفاده می شود .

PSH وقتی این پرچم برابر با ۱ شود گیرنده پیام باید فوراً آن را به لایه کاربرد تحویل دهد .

URG از این پرچم برای ارسال فوری داده ها بدون انتظار کشیدن تا گیرنده بایت های قبلی در جریان را پردازش کند ، استفاده می شود

مفهوم تسهیم سازی در TCP را توضیح دهید ؟

• در پروتکل TCP این امکان وجود دارد که به طور همزمان چندین سرویس ارتباطی بر روی یک کامپیوتر اجرا شود و همزمان داده های خود را برای ارسال به TCP تحویل می دهد . برای تفکیک این سرویس ها که از یک آدرس IP مشترک استفاده می کنند از شماره درگاه استفاده می شود . استفاده مشترک چندین فرآیند لایه کاربرد از امکانات TCP/IP ، تسهیم سازی نام دارد .

۵.۱۰.۲ UDP

قرارداد بسته داده کاربر یا پروتکل بسته داده کاربر User Datagram Protocol یکی از اجزاء اصلی مجموعه پروتکل اینترنت، مجموعه ای از پروتکل های شبکه که در اینترنت مورد استفاده قرار می گیرند، می باشد. رایانه ها با استفاده از UDP قادر به ارسال پیغام، که در این مورد آن را بسته داده یا Datagram می نامیم، به دیگر میزبان های موجود در پروتکل اینترنت (IP) می باشند. این پروتکل توانایی این را دارد که این کار را بدون برقراری ارتباط قبلی یا ایجاد کانال ها یا مسیرهای انتقال داده ویژه انجام دهد. پروتکل مزبور در سال ۱۹۸۰ توسط دیوید پی. رید ابداع گردیده و به طور رسمی در استاندارد RFC ۷۶۸ تعریف شد.

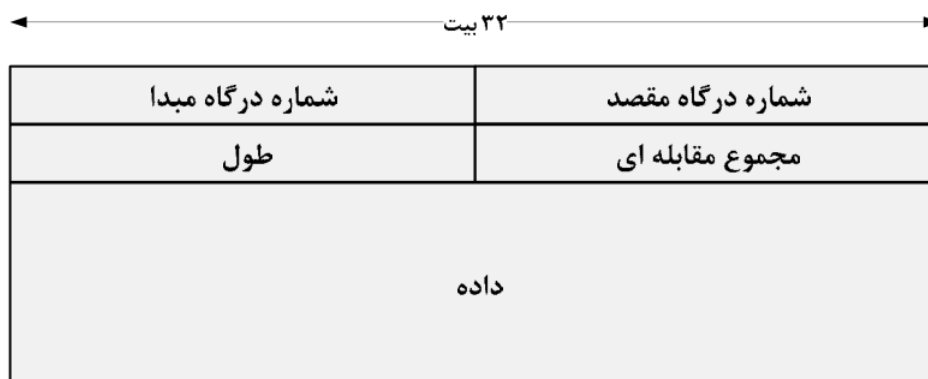
از مدل انتقال ساده بدون استفاده از تکنیک دست تکانی صریح که برای ایجاد قابلیت اطمینان (Reliability) ، مرتب سازی و یکپارچه سازی داده ها بکار می رود، بهره می جوید؛ بنابراین، UDP سرویس غیرمطمئنی را ارائه می دهد و ممکن است بسته داده ها نامرتب، تکراری بوده یا بدون اطلاع قبلی از دست بروند. UDP تشخیص می دهد که بررسی خطا و تصحیح آن با توجه به نوع کاربردی که دارد لازم نبوده یا نباید اجرا شود، بنابراین چنین بار اضافی پردازشی را بر شبکه تحمیل نمی کند. برنامه هایی که نسبت به زمان حساس هستند از UDP استفاده می کنند، زیرا از دست دادن بسته ها بهتر از منتظر ماندن برای بسته هاست؛ بنابراین پروتکل UDP بهترین گزینه برای سیستم های بی درنگ به حساب می آید. اگر برنامه ای نیاز به امکانات تصحیح خطا در سطح واسط شبکه داشته باشد، می تواند از قرارداد کنترل انتقال (TCP Transmission Control Protocol) یا پروتکل انتقال کنترل جریان (SCTP Stream Control Transmission Protocol) استفاده کند که به طور خاص برای این منظور طراحی شده اند.

ساختار بسته UDP

UDP کمینه‌ترین پروتکل مبتنی بر پیغام لایه انتقال است که جزئیات آن در RFC ۷۶۸ آورده شده‌است.

UDP هیچگونه تضمینی برای تحویل پیام به پروتکل لایه بالاتر را نمی‌دهد و پروتکل‌هایی هم که از UDP استفاده می‌کنند هیچ حالتی از پیغامی را می‌فرستند نگه نمی‌دارند. به همین دلیل، UDP را پروتکل بسته-داده غیر مطمئن می‌نامند.

UDP تسهیم‌سازی برنامه (از طریق شماره پورت) و بررسی یکپارچگی (با استفاده از مجموع مقابله ای سرآیند) سرایند و بخش داده‌ای را فراهم می‌آورد. اگر مطمئن بودن انتقال موردنظر باشد، بایستی این امکان در برنامه کاربر تعبیه شود.



قالب بسته های UDP

شماره درگاه مبدا

این فیلد شماره درگاه فرستنده را مشخص می‌کند و زمانی معنا پیدا می‌کند که برای پاسخ دادن احتیاج به شماره درگاه فرستنده داشته باشیم. اگر از آن استفاده نشود، عدد صفر در آن قرار می‌گیرد.

شماره درگاه مقصد

این فیلد شماره درگاه مقصد را نشان می‌دهد و وجود آن الزامیست.

طول

فیلدی که طول کل بسته داده را بر حسب بایت نشان می‌دهد.

مجموع مقابله ای

فیلد چک‌سام برای بررسی خطای سرایند و داده استفاده می‌شود. اگر هیچ چک‌سامی توسط فرستنده تولید نشود، این فیلد با صفر پر می‌شود. فیلد مزبور در IPv۶ اختیاری نیست.

در چه مواقعی بهتر است که از UDP استفاده کرد و در چه مواقعی از TCP ؟

- در مواقعی که نیاز است تا داده ها به یک برنامه کاربردی خاص در حال اجرا در یک ماشین فرستاده شود و یا در وضعیتی که نیاز است داده ها به صورت همه پخش ی چند پخش ی ارسال شوند ، از پروتکل UDP استفاده می گردد .
- برخی از برنامه های کاربردی اینترنت نیاز به همه ی توانایی های TCP نداشته و فقط به یک پروتکل حمل ساده که بتواند برنامه های کاربردی را در کامپیوتر شناسایی کند و یک بررسی خطای ساده مهیا سازد ، نیاز دارند .
- مزیت UDP برای کاربردهای همه پخش ی/چند پخش ی است . به این صورت که در TCP اگر یک بسته همه پخش ی باید به ۱۰۰۰ ایستگاه فرستاده شود ، فرستنده TCP باید ۱۰۰۰ اتصال را باز کرده و داده ها را به هر اتصال بفرستد و سپس ۱۰۰۰ اتصال را ببندد . سربار بازکردن این اتصالات بسیار بالاست . اما چنانچه از پروتکل UDP استفاده شود ، فرستنده می تواند داده را به ماژول IP با درخواست همه پخش ی / چند پخش ی بفرستد .

فصل ۳

شبکه های اجتماعی

۱.۳ وبلاگ چیست؟

وبلاگ نوعی وبسایت است که حاوی اطلاعاتی مانند: گزارش روزانه، اخبار، یادداشت‌های شخصی یا مقالات علمی مورد نظر طراح آن است. وبلاگ ترکیبی از دو کلمه «web» و «log» به معنای ثبت وقایع روزانه در وب است. مطالب وبلاگ بر مبنای زمانی که ثبت شده گروه‌بندی و به ترتیب از تازه‌ترین رخداد به قدیم ارائه می‌گردد.

وب‌نویس به گزارش مداوم رویدادها، خاطرات، یا عقاید یک شخص یا یک سازمان می‌پردازد. واحد مطالب در وبلاگ، پست است، معمولاً در انتهای هر مطلب، برچسب تاریخ و زمان، نام نویسنده و پیوند ثابت به آن یادداشت ثبت می‌شود. فاصله زمانی بین مطالب وب‌نوشت لزوماً یکسان نیست و زمان نوشته‌شدن هر مطلب به خواست نویسنده وبلاگ بستگی دارد.



شکل ۱.۳: Blogging

۱.۱.۳ انواع و نمونه هایی از وبلاگ ها

وب سایت های زیر به شما این امکان را می دهند که به راحتی بتوانید یک وبلاگ برای خود ایجاد کنید

WordPress



شکل ۲.۳: Wordpress

وب سایت wordpress.com پلتفرمی برای انتشار مطالب شخصی است ، مالکیت این شرکت به کمپانی Automattic تعلق دارد ، این وب سایت از موتور تغییر داده شده ی wordpress.org استفاده می کند . wordpress.com قابلیت میزبانی بلاگ را به صورت رایگان برای کاربرانی که ثبت نام کرده اند فراهم می کند، تامین مالی این وب سایت از طریق افزایش امکانات هر کاربر ، سرویس های VIP و تبلیغات است . تمامی ویژگی های اصلی وب سایت مانند پست گذاشتن به صورت رایگان هستند اما برای بعضی ویژگی های وب سایت باید پول پرداخت کرد مثل :

- نصب پلاگین های PHP
- شخصی سازی تم های CSS
- نوشتن کدهای Javascript
- حذف تبلیغات
- آپلود ویدیو

Wix

Wix یک کمپانی نرم افزاری اسرائیلی است که قابلیت توسعه ی وب سایت را برای کاربران فراهم می کند، این وب سایت به کاربران امکان ساخت وب سایت با استفاده از ابزار Drag & Drop را می دهد که برای desktop و mobile مناسب هستند . کاربران این امکان را دارند که به وب سایت هایشان امکاناتی از قبیل :



شکل ۳.۳: Wix

- پلاگین های شبکه های اجتماعی

- فروشگاه اینترنتی

- تماس با ادمین سایت

- انجمن ها

را اضافه کنند

Wix امکانات پایه ای وب سایتش را به صورت مجانی ارائه می دهد و کسب در آمد این وب سایت از طریق ارائه ی قابلیت های اضافی با دریافت مبلغی از کاربر است .

Tumblr

Tumblr یک شبکه ی اجتماعی آمریکایی و همچنین ارائه دهنده ی تولد وبلاگ است که توسط David Karp در سال ۲۰۰۷ ساخته شد و مالک کنونی آن شرکت Automattic می باشد . اسن سرویس به کاربران امکان پست محتوای متنی و چندرسانه ای را می دهد . کاربران می توانند بلاگ هایی که دوست دارند را follow کنند . قابلیت های وب سایت از طریق رابط کاربری dashboard قابل دسترسی است . تا سال ۲۰۱۹ Tubmlr ۴۷۵ میلیون وبلاگ را میزبانی کرده است .



شکل ۴.۳: Tumblr

Joomla

Joomla یک سیستم مدیریت محتوای رایگان و منبع باز (open source) برای انتشار مطالب وب می باشد که توسط شرکت Open Souce Matters ساخته شده است .



شکل ۵.۳: Joomla

کلمه ی Joomla از کلمه ی jumla که یک لغت سواحلی می باشد گرفته شده و به معنی "همه با هم" می باشد . Joomla برای طراحی و پیاده سازی از معماری MVC استفاده کرده است و به زبان برنامه نویسی PHP با تکنیک برنامه نویسی شی گرا نوشته شده است ، همچنین برای پایگاه داده ها از

MySQL یا PostgreSQL استفاده کرده است . در سال ۲۰۱۹ Joomla به عنوان چهارمین سیستم مدیریت محتوای (CMS) مشهور و محبوب در اینترنت شناخته شد .

Blogger

Blogger یک سرویس انتشار بلاگ است که این امکان را می دهد تا چند کاربر بتوانند بر روی یک بلاگ کار کنند، این سایت توسط Pyra Labs توسعه داده شد و در سال ۲۰۰۳ توسط Google خریداری شد . بلاگ ها توسط Google میزبانی می شوند و از طریق زیر دامنه ی blogspot.com قابل دسترسی است . همچنین بلاگ ها می توانند توسط دامنه ی دلخواه تعیین شده توسط کاربر تعیین شود . یک کاربر می تواند با هر اکانت تا ۱۰۰ بلاگ را تولید و مدیریت کند .



شکل ۶.۳: Blogger

۲.۳ تعریف شبکه اجتماعی

شبکه اجتماعی یا Social Network ساختاری اجتماعی است که در آن افراد می توانند با انتشار افکار ، عکس ها و ویدیو های خود در صفحات شخصی یا گروهی به تولید مطالب بپردازند همچنین در مورد مطالب منتشر شده نظرات دیگران را دریافت کنند و در مورد مطالب دیگران نظر بدهند

۱.۲.۳ انواع و نمونه هایی از شبکه های اجتماعی

از مشهورترین شبکه های اجتماعی که امکان عضو شدن و انتشار اطلاعات را به شما می دهند می توان به موارد زیر اشاره نمود .

Facebook

Facebook یک شبکه ی اجتماعی آنلاین است که در Menlo Park, California واقع شده است . این کمپانی توسط Mark Zuckerberg و به همراهی چند هم اتاقی اش در دانشگاه هاروارد به نام های Dustin Moskovitz ، Andrew McCollum ، Eduardo Saverin و Chris Hughes تاسیس شد . در ابتدا عضویت در Facebook به دانشجویان هاروارد محدود شده بود ، سپس به دانشگاه های MIT و دانشگاه های Boston و سپس بقیه ی دانشگاه ها گسترش داده شد . سپس دانشجویان دبیرستانی نیز به مجموعه ی Facebook اضافه شد . در سال ۲۰۰۶ هر کسی که بالاتر از ۱۳ سال سن داشت می توانست در Facebook ثبت نام کند .



شکل ۷.۳: Facebook

سرویس Facebook می تواند توسط هر دستگاهی که به اینترنت متصل باشد ، دسترسی پیدا کند : مثل کامپیوتر ، تبلت یا گوشی های هوشمند . بعد از ثبت نام در Facebook کاربران می توانند یک پروفایل حاوی اطلاعات شخصی خودشان داشته باشند . کاربران می توانند پست هایی شامل متن ، عکس و چند رسانه ای را با دیگر کاربران که با هم توافق کرده اند که به عنوان Friend باشند به اشتراک بگذارند ، یا در تنظیمات این قابلیت

را ایجاد کنند که هر کاربری بتواند کدام اطلاعات آنها را ببیند . به ادعای Facebook در سال ۲۰۱۸ این وب سایت بیشتر از ۲.۳ میلیارد کاربر فعال به صورت ماهانه دارد . اپلیکیشن Facebook بیشترین دانلود را در بین اپلیکیشن های موبایلی در دهه ی ۲۰۱۰-۲۰۱۰ داشته است

YouTube

Youtube یک پلتفرم اشتراک گذاری ویدیو است که دفتر مدیریت آن در , San Bruno California قرار دارد . سه کارمند سابق PayPal به نام های Chad Hurley ، Steven Chen و Jawed Karim این سرویس را در سال ۲۰۰۵ ساختند . Google این سایت را در نوامبر ۲۰۰۶ به قیمت ۱.۶۵ میلیارد دلار خریداری کرد .

Youtube به کاربران خود اجازه ی آپلود ویدیو ، مشاهده ی ویدیو ها ، اشتراک گذاری ویدیو ها ، مشترک شدن در کانال ها و . . . را می دهد . بیشتر محتوای Youtube را کاربران آن در وب سایت قرار می دهند . اما رسانه های خبری بزرگ مانند CNN ، CBS و . . . نیز از این سایت به عنوان تریبونی برای شبکه ی خودشان استفاده می کنند .



شکل ۸.۳: YouTube

کاربرانی که در وب سایت Youtube ثبت نام نکردند فقط می توانند ویدیو ها را تماشا کنند و قابلیت آپلود ویدیو را ندارند اما کاربرانی که در سایت ثبت نام کرده اند قابلیت آپلود بی نهایت ویدیو در این سایت را دارند ، همچنین می توانند از امکانات دیگری مثل ایجاد برنامه

ی زنده ، مشترک شدن در کانال ها ، نظر دادن درباره ی ویدیو ها و . . . برخوردار شوند . در فوریه ۲۰۱۷ در هر دقیقه ۴۰۰ ساعت ویدیو در Youtube آپلود می شود و روزانه یک میلیارد ساعت ویدیو در Youtube مشاهده می شود . بر اساس آمار Alexa در آگوست ۲۰۱۸ وب سایت Youtube به عنوان دومین وب سایت مشهور در جهان بعد از Google شناخته شد .

Instagram

Instagram یک شبکه ی اجتماعی است که به کاربران امکان اشتراک گذاری عکس ها و ویدیوهایشان را می دهد، مالک این وب سایت کمپانی Facebook می باشد . این اپلیکیشن توسط Kevin Systrom و Mike Krieger در اکتبر ۲۰۱۰ برای سیستم عامل تلفن همراه iOS طراحی شد . نسخه ی Android اینستاگرام در آپریل ۲۰۱۲ عرضه شد . در نوامبر همین سال رابط کاربری وب سایتی اینستاگرام به صورت محدودتری از امکانات رونمایی شد .



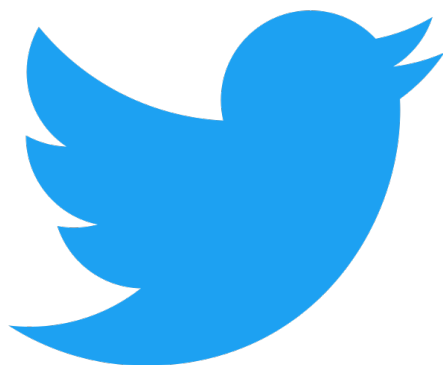
شکل ۹.۳: Instagram

بعد از ارائه ی Instagram در سال ۲۰۱۰ تعداد کاربران این اپلیکیشن به سرعت به ۱ میلیون کاربر رسید و در عرض یک سال به ۱۰ میلیون کاربر و در می ۲۰۱۹ به یک میلیارد کاربر . در آپریل ۲۰۱۹ کمپانی Facebook سرویس اینستاگرام را به مبلغ حدودی یک میلیارد دلار به صورت وجه نقد و سهام خریداری کرد . اپلیکیشن Instagram به کاربران امکان آپلود عکس و فیلم هایشان را با فیلتر ها و افکت های مختلفی ارائه می دهد ، پست های اینستاگرام می توانند به صورت مشاهده

ی عمومی یا خصوصی تنظیم شوند . کاربران می توانند عکس ها را like کنند یا بقیه ی کاربران را follow کنند تا پست های دیگران در قسمت Home آنان قرار گیرد . در ابتدا Instagram فقط اجازه ی آپلود عکس با نسبت (1:1) با پیکسل ۶۴۰ را می دهد که این محدودیت به خاطر عرض صفحه ی نمایش گوشی های iPhone در آن زمان بود . این سخت گیری در سال ۲۰۱۵ کمتر شد و قابلیت آپلود عکس های ۱۰۸۰ پیکسل را هم می داد . Instagram همچنین قابلیت فرستادن پیام ، آپلود چندین عکس در یک پست و ایجاد Story را هم می داد که به کاربران این امکان را می داد که عکس ها یا ویدیوهایشان را به مدت ۲۴ ساعت با دیگران به اشتراک بگذارند . در ژانویه ۲۰۱۹ روزانه ۵۰۰ میلیون کاربر از قابلیت Story استفاده می کنند . اینستاگرام به عنوان چهارمین اپلیکیشن با بیشترین دانلود در دهه ی 2010-2020 شناخته شده است .

Twitter

Twitter یک شبکه ی اجتماعی و بلاگ مانند می باشد که کاربران به صورت پیام هایی تحت عنوان tweet با هم در ارتباط می باشند . کاربرانی که در Twitter ثبت نام کرده اند می توانند پست کنند ، like کنند و retweet کنند اما کاربرانی که ثبت نام نکرده اند فقط می توانند آنها را بخوانند .



شکل ۱۰.۳: Twitter

کمپانی Twitter امکان استفاده از این اپلیکیشن را از طریق رابط کاربری وب سایت SMS ، و از طریق اپلیکیشن های گوشی موبایل به کاربران خود می دهد . مدیریت Twitter در San Francisco , California می باشد و بیشتر از ۲۵ دفتر در سرتاسر جهان دارد . Twitter در مارس ۲۰۰۶ توسط Jack Dorsey ، Evan Williams و Biz Stone ، Noal Glass ، ساخته شد و در جولای همان سال در معرض

استفاده قرار گرفت . سرویس Twitter به سرعت مورد استقبال قرار گرفت و در سال ۲۰۱۲ روزانه بیشتر از ۱۰۰ ملیون کاربر ۳۴۰ ملیون tweet می زنند . و روزانه تقریباً 1.6 میلیارد درخواست جستجو از سرور Twitter می شود . در سال ۲۰۱۳ وب سایت Twitter به عنوان دهمین وب سایت پربازدید شناخته شد و لقب "SMS اینترنتی" را به خود گرفت . در سال ۲۰۱۸ ، Twitter بیشتر از ۳۲۱ ملیون کاربر فعال داشته است .

۳.۳ پیام رسان چیست؟

پیام‌رسانی فوری (Instant Messaging) گونه‌ای از ارتباط مستقیم متنی بی‌درنگ (real time) بین دو یا چند فرد با استفاده از رایانه شخصی با دستگاه‌های دیگر و از طریق یک برنامه‌ی مشترک است. متن کاربر بر روی یک شبکه مانند اینترنت منتقل می‌شود. برنامه‌های نرم‌افزاری پیشرفته تر پیام‌رسانی رده بالاتری از جمله تماس تصویری یا صوتی را عرضه می‌کنند. پیام‌رسانی فوری با داشتن امکان جواب دادن آنی، ارتباطی مؤثر و کارآمد را برقرار می‌کند. در بعضی از موارد پیام‌رسانی فوری ویژگی‌های اضافی را ارائه می‌دهد که بر محبوبیت آن می‌افزایند. مثلاً به کاربران اجازه می‌دهد یکدیگر را از ببینند؛ یا مستقیماً و رایگان با یکدیگر حرف بزنند. بسیاری از برنامه‌ها امکان انتقال فایل‌های مختلف را فراهم می‌کنند.

۱.۳.۳ انواع و نمونه‌هایی از پیام رسان‌ها

از جمله پیام رسان‌های مشهور می‌توان به موارد زیر اشاره کرد

WhatsApp



شکل ۱۱.۳: WhatsApp

سرویس WhatsApp توسط شرکت What-Mountain View, sApp, Inc واقع در California تاسیس شد که در فوریه ۲۰۱۴ توسط کمپانی Facebook به ارزش ۱۹.۳ میلیارد دلار خریداری شد. این سرویس به مشهورترین اپلیکیشن پیام رسان در جهان در سال ۲۰۱۵ شناخته شد. WhatsApp قابلیت ارسال پیام متنی، عکس، صوت، ویدیو و برقراری تماس‌های صوتی و تصویری را دارد و بر روی پلتفرم‌های مختلف قابل

اجراست. اپلیکیشن سمت کاربر WhatsApp بر روی دستگاه‌های تلفن همراه اجرا می‌شود اما در صورتی که تلفن همراهتان را از طریق کامپیوتر تایید هویت کنید می‌توانید از طریق کامپیوتر هم به این اپلیکیشن دسترسی داشته باشیم. برای ثبت نام در سرویس WhatsApp کافی است که تنها یک شماره‌ی موبایل داشته باشید.

Facebook Messenger



شکل ۱۲.۳: Facebook Messenger

پیام رسان Facebook Messenger توسط کمپانی Facebook, Inc توسعه داده شده است. در ابتدا این برنامه به عنوان Face-Chat در سال ۲۰۰۸ به عنوان امکان پیام رسانی در وب سایت Facebook ساخته شد و در سال ۲۰۱۰ به صورت سرویس جداگانه در دسترس قرار گرفت. و در آگوست ۲۰۱۱ به صورت اپلیکیشن های iOS و Android عرضه شد. سپس Facebook یک وب سایت مستقل به نام Messenger.com را تاسیس کرد که به کاربران این امکان را

می دهد که از بین رابط کاربری وب سایت یا دانلود اپلیکیشن های iOS یا Android را برای استفاده از این سرویس انتخاب کند. در آوریل ۲۰۲۰ Facebook نسخه ی Desktop را برای Messenger عرضه کرد که سیستم عامل Windows 10 و macOS را پشتیبانی می کند. کاربران Messenger علاوه بر پیام های متنی، قابلیت ارسال عکس، ویدیو، Sticker، فایل های صوتی و هر نوع فایل دیگری را دارد. این سرویس همچنین از تماس های صوتی و تصویری نیز پشتیبانی می کند.

Telegram

Telegram یک پیام رسان اینترنتی است که برای سیستم عامل های iOS ، Android ، macOS ، Windows ، Windows Phone طراحی شده است . کاربران Telegram قابلیت ارسال پیام متنی ، عکس ، ویدیو ، Sticker و فایل های صوتی یا هر نوع دیگری از فایل ها را دارند . کد منبع سمت کاربر Telegram به صورت منبع باز است، اما کد منبع سمت Server به صورت بسته می باشد ، سرویس Telegram همچنین API های مختلفی را برای توسعه دهندگان فراهم کرده است که قابلیت ساخت ربات و برنامه های مختلفی را به توسعه دهندگان می دهد . در آپریل ۲۰۲۰ Telegram ۴۰۰ میلیون کاربر فعال به صورت ماهانه داشته و روزانه حداقل 1.5 میلیون کاربر جدید در Telegram ثبت نام می کنند



شکل ۳.۳: Telegram

Viber

Viber یک اپلیکیشن پیام رسان با قابلیت اجرا بر روی سیستم عامل های مختلف از جمله : Linux و macOS ، Windows ، iOS ، Android می باشد . این اپلیکیشن در سال ۲۰۱۰ توسط شرکتی به نام Viber Media در اسرائیل توسعه داده شد و در سال ۲۰۱۴ شرکت Rakuten این سرویس را خریداری کرد و از سال ۲۰۱۶ نام تجاری این اپلیکیشن به Rakuten Viber تغییر یافت . دفتر مرکزی این شرکت در Luxembourg واقع است اما در سایر نقاط دنیا از جمله : Paris ، London ، Barcelona ، Amsterdam و . . . نیز شعبه دارد . کاربران می توانند با یک شماره ی تلفن همراه در این اپلیکیشن ثبت نام کنند ، همچنین این سرویس از طریق کامپیوترهای شخصی و Laptop هم قابل دسترسی است . این سرویس علاوه بر پیام های متنی قابلیت ارسال عکس ها و ویدیوها را نیز دارد . تا سال ۲۰۱۸ بیشتر از ۱ میلیارد کاربر در این سرویس ثبت نام کرده اند .



شکل ۱۴.۳: Viber

فصل ۴

امنیت

۱.۴ تعریف امنیت

امنیت رایانه‌ای با نام‌های امنیت سایبری و امنیت فناوری اطلاعات نیز شناخته می‌شود. حفاظت از سامانه‌های اطلاعات در برابر دزدی یا آسیب به سخت‌افزار، نرم‌افزار، و اطلاعات نرم‌افزاری و محافظت در برابر حمله محروم‌سازی از سرویس (اختلال) و بات‌نت‌ها (گمراهی) نمونه پارامترهایی هستند که امنیت رایانه‌ای آنها را تأمین می‌نماید.

این سطح از امنیت شامل کنترل دسترسی فیزیکی به سخت‌افزار، و همچنین به صورت محافظت در برابر آسیب‌هایی که ممکن است با دسترسی به شبکه، داده‌ها و تزریق کد روی داده بکار گرفته می‌شود.

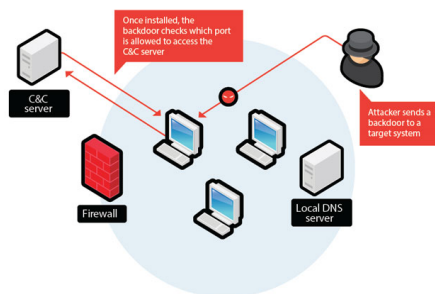
با توجه به افزایش وابستگی به سامانه‌های رایانه‌ای و اینترنت در بیشتر جوامع، شبکه‌های بیسیم مانند بلوتوث و وای فای، رشد دستگاه‌های هوشمند مانند تلفن هوشمند، تلویزیون، و دستگاه‌های کوچک مانند اینترنت اشیا امنیت رایانه‌ای اهمیت رو به رشدی پیدا کرده‌است.

برای حفظ امنیت رایانه، شناخت گونه‌ی حمله‌ها بسیار مهم است. در ادامه، نمونه‌ای از این حمله‌ها آورده شده‌اند:

۲.۴ تعریف حمله

۱.۲.۴ انواع حمله ها

در پشتی (Backdoor)



شکل ۱.۴: Backdoor

در پشتی در یک سامانه رایانه‌ای، یک سامانه رمزنگاری یا یک الگوریتم است. این مقوله به هر روش مخفی دورزدن اصالت‌سنجی عادی یا کنترل‌های امنیتی گفته می‌شود. درب‌های پشتی ممکن است به دلایل گوناگونی مانند طراحی اصلی و فقر پیکربندی وجود داشته باشند. این امکان وجود دارد که درب‌های پشتی توسط شخص مجاز که اجازه دسترسی‌های مشروع را می‌دهد یا توسط یک مهاجم به دلایل ویرانگر افزوده شده باشد.

حمله محروم‌سازی از سرویس (Denial-of-service attack)

حمله محروم‌سازی از سرویس به این منظور طراحی می‌شود که دستگاه یا منابع شبکه را از دسترس کاربران نهایی خارج کند.

مهاجمان می‌توانند خدمات‌رسانی به قربانیان منحصربفرد را رد کنند. مانند اینکه عمداً به صورت متوالی گذرواژه کاربر را اشتباه وارد می‌کنند تا حساب کاربری قربانی قفل شود یا ممکن است از توانمندی‌های دستگاه یا شبکه بیش از اندازه نرمال استفاده کنند. بگونه‌ای که در یک لحظه، استفاده از سرویس برای کاربران غیرممکن شود و همه کاربران را در یک لحظه بلاک کنند. می‌توان با افزودن یک رول مشخص در دیوار آتش، حمله‌ای که از سوی نشانی آی‌پی انجام می‌شود را بلاک کرد. اما این حملات می‌توانند به صورت توزیع شده از مناطق مختلف انجام شوند، به این حملات، «حمله دیداس»^۱ (DDoS attacks) نیز گفته می‌شود. یعنی در جایی که حمله از نقاط زیادی صورت می‌گیرد دفاع در برابر این نوع از حمله‌ها سخت‌تر می‌شود مانند حمله‌هایی که سرچشمه آن‌ها رایانه‌های زامبی است از یک بات‌نت هستند. ترتیبی از روش‌های ممکن دیگر می‌تواند شامل انعکاس و تقویت حمله‌ها باشند. مانند سامانه‌های بی‌گناهی که جریانی از ترافیک اینترنت را مانند سیل به سمت رایانه قربانی روانه می‌کنند.

^۱Distributed denial of service

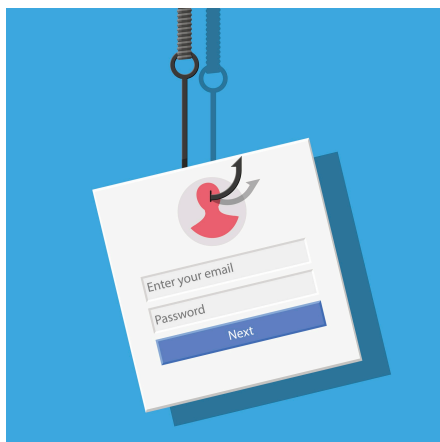
حمله‌های دسترسی مستقیم (Direct-access attacks)

یک کاربر غیرمجاز، دسترسی فیزیکی به یک رایانه را بدست می‌آورد؛ و به احتمال زیاد می‌تواند به‌طور مستقیم، داده‌ها را از روی آن کپی کند. ممکن است کاربر غیرمجاز، امنیت سامانه را با ایجاد تغییر در سیستم عامل، نصب کرم‌های نرم‌افزاری، کی‌لاگر، دستگاه شنود یا با استفاده از ماوس‌های بی‌سیم حتی زمانی که سامانه توسط تدابیر امنیتی مورد محافظت هستند در اختیار بگیرد. این حمله‌ها ممکن است به وسیله بوت شدن یک سیستم عامل دیگر یا اجرای یک نرم‌افزار از روی یک سی‌دی-رام و دیگر رسانه‌هایی که قابلیت بوت شدن به سمت رایانه قربانی انجام شوند. رمزنگاری دیسک و ماژول پلتفرم قابل اطمینان برای جلوگیری از این حمله‌ها طراحی شده‌اند.

شنود (Eavesdropping)

شنود به عمل مخفیانه گوش دادن به گفتگوی خصوصی دیگران بدون رضایت آن‌ها گفته می‌شود که در اینجا بین میزبان‌های درون یک شبکه رخ می‌دهد. برای نمونه، برنامه کارنیور و شرکت ناروس اینسایت توسط اداره تحقیقات فدرال (اف‌بی‌آی) و آژانس امنیت ملی ایالات متحده آمریکا برای شنود الکترونیک سامانه‌های تامین کننده ی خدمات اینترنتی بکارگرفته می‌شود. حتی اگر دستگاه‌های هدف، سامانه بسته باشد یعنی هیچ گونه ارتباطی با جهان خارج نداشته باشند. آن‌ها می‌توانند با امواج الکترومغناطیس ضعیفی که انتقال می‌دهند شنود شوند. تمپس (TEMPEST) مشخصه‌ای است که توسط آژانس امنیت ملی ایالات متحده آمریکا برای چنین حمله‌هایی مورد استفاده قرار می‌گیرد.

فیشینگ (Phishing)



فیشینگ روشی است که تلاش می‌کند تا اطلاعات حساس مانند نام کاربری، گذرواژه، و جزئیات کارت اعتباری را به‌طور مستقیم از کاربران بدست آورد. فیشینگ معمولاً توسط فرستادن ایمیل‌های متقلبانه و پیام‌رسان‌ها انجام می‌شود و بیشتر کاربران را به وارد کردن جزئیات در یک وب سایت دروغین که خیلی شبیه به وب سایت اصلی است هدایت می‌کند. در این حالت این اعتماد

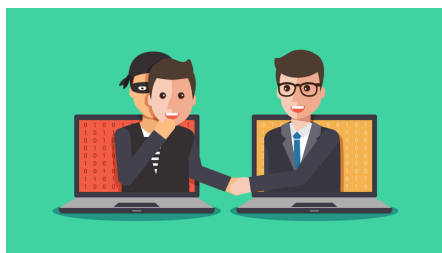
شکل ۲.۴: Phishing

قربانی است که شکار می‌شود. فیشینگ به عنوان نوعی از مهندسی اجتماعی دسته‌بندی می‌شود.

دزدی کلیک

دزدی کلیک به عنوان حمله واسط کاربری یا (User Interface Redress Attack) گفته می‌شود. این یک روش ویرانگر است که درست هنگامی که همان کاربر قصد دارد بر روی سطح بالای صفحه کلیک کند حمله‌کننده، کاربر را فریب می‌دهد تا بر روی دکمه یا پیوند یک صفحه وب دیگری کلیک کند. حمله‌کننده اساساً کلیک‌هایی که قرار است روی صفحه انجام شود را می‌رباید و کاربران را به سمت صفحات نامربوط که متعلق به اشخاص دیگری هستند هدایت می‌کند. این روش خیلی شبیه روشی است که از آن برای ربایش کلید استفاده می‌شود. تهیه نمونه دقیق یک پیش‌نویس از شیوه‌نامه‌ها، آی فریم‌ها، کلیدها، تکست باکس، باعث می‌شود کاربر به مسیر مورد اعتمادی هدایت شود که در آنجا گذرواژه یا دیگر اطلاعات را وارد کند درست هنگامی که به یک فریم پنهان وارد شده و آن فریم توسط شخص حمله‌کننده در حال کنترل است.

مهندسی اجتماعی (Social engineering)



شکل ۳.۴: Social engineering

هدف مهندسی اجتماعی این است که کاربر را متقاعد کند تا چیزهای محرمانه مانند گذرواژه یا شماره‌های کارت اعتباری اش را فاش کند. برای نمونه جعل هویت یک بانک، یک پیمانکار و یک خریدار می‌تواند از روش‌های مورد استفاده مهندسی اجتماعی باشد. در یک کلاهبرداری معمول و سودآور،

ایمیل‌هایی از سوی مدیرعامل دروغین یک شرکت برای بخش مالی و حسابداری همان شرکت فرستاده می‌شود. در اوایل سال ۲۰۱۶ اداره تحقیقات فدرال (اف‌بی‌آی) گزارش کرد که در زمینه کلاهبرداری در مشاغل در حدود ۲ سال بیش از ۲ میلیارد دلار آمریکا هزینه شده‌است. در مه ۲۰۱۶ میلواکی باکس یکی از تیم‌های اتحادیه ملی بسکتبال قربانی این روش با عنوان کلاهبرداری سایبری شد. این عمل با جعل هویت رئیس این تیم با نام پیتز فیگین انجام شد. در نتیجه فرم‌های مالیاتی دلیو - ۲ سال ۲۰۱۵ همه کارکنان تیم تحویل داده شد.

۳.۴ بد افزار چیست



شکل ۴.۴: malware

بدافزار (malware) برنامه‌های رایانه‌ای هستند که به علت آن که معمولاً کاربر را آزار می‌دهند یا خسارتی به وجود می‌آورند، به این نام مشهورند. برخی از آن‌ها فقط کاربر را می‌آزارند. مثلاً وی را مجبور به انجام کاری

تکراری می‌کنند. اما برخی دیگر سیستم رایانه‌ای و داده‌های آن را هدف قرار می‌دهند که ممکن است خسارتی به بار آورند. در عین حال، ممکن است هدف آن سخت‌افزار سیستم کاربر باشد.

ویروس رایانه‌ای تنها نوعی بدافزار است که خود را بازتولید می‌کند، اما اغلب کاربران رایانه به اشتباه به همه بدافزارها ویروس می‌گویند.

انواع بدافزارها

از انواع بدافزارها می‌توان به ویروس‌ها، کرم‌ها، اسب‌های تروآ، جاسوس‌افزارها، آگهی‌افزارها، روت‌کیت‌ها و هرزنامه‌ها اشاره کرد.

۱.۳.۴ ویروس رایانه‌ای



شکل ۵.۴: computer virus

ویروس رایانه‌ای (Computer virus) نوعی نرم افزار (program) است که در سیستم‌های رایانه‌ای باعث اختلال، جاسوسی و خرابی می‌شود.

ویروس، یک نوع نرم افزار (برنامه) کامپیوتری است که به دلیل ماهیت عملکرد مجرمانه آن به آن بدافزار می‌گویند. که در اغلب مواقع بدون اطلاع کاربر به سیستم

عامل وارد شده و آن را آلوده می‌کند و تلاش می‌کند خودش را تکثیر نماید. این عمل تولید مثل یا کپی‌سازی از خود بر روی یک کد اجرایی موجود، ویژگی کلیدی در تعریف یک ویروس است. معمولاً کاربران رایانه به ویژه آن‌هایی که اطلاعات تخصصی کمتری درباره کامپیوتر دارند، ویروس‌ها را برنامه‌هایی هوشمند و خطرناک می‌دانند که خود به خود اجرا و

تکثیر شده و اثرات تخریبی زیادی دارند که باعث از دست رفتن اطلاعات و گاه خراب شدن کامپیوتر می‌گردند در حالیکه طبق آمار تنها پنج درصد ویروس‌ها دارای اثرات تخریبی بوده و بقیه صرفاً تکثیر می‌شوند؛ بنابراین یک ویروس رایانه‌ای را می‌توان برنامه‌ای تعریف نمود که می‌تواند خودش را با استفاده از یک میزبان تکثیر نماید. بنابراین تعریف اگر برنامه‌ای وجود داشته باشد که دارای اثرات تخریبی باشد ولی امکان تکثیر نداشته باشد، نمی‌توان آن را ویروس نامید؛ بنابراین ویروس‌های رایانه‌ای از جنس برنامه‌های معمولی هستند که توسط ویروس‌نویسان نوشته شده و سپس به‌طور ناگهانی توسط یک فایل اجرایی یا جا گرفتن در ناحیه سیستمی دیسک، فایل‌ها یا کامپیوترهای دیگر را آلوده می‌کنند. در این حال پس از اجرای فایل آلوده به ویروس یا دسترسی به یک دیسک آلوده توسط کاربر دوم، ویروس به صورت مخفی نسخه‌ای از خودش را تولید کرده و به برنامه‌های دیگر می‌چسباند و به این ترتیب داستان زندگی ویروس آغاز می‌شود و هر یک از برنامه‌ها یا دیسک‌های حاوی ویروس، پس از انتقال به کامپیوترهای دیگر باعث تکثیر نسخه‌هایی از ویروس و آلوده شدن دیگر فایل‌ها و دیسک‌ها می‌شوند؛ لذا پس از اندک زمانی در کامپیوترهای موجود در یک کشور یا حتی در سراسر دنیا منتشر می‌شوند. از آنجا که ویروس‌ها به‌طور مخفیانه عمل می‌کنند، تا زمانی که کشف نشده و امکان پاکسازی آن‌ها فراهم نگردیده باشد، ماشین‌های هوشمند و قطعا برنامه‌های بسیاری را آلوده می‌کنند و از این رو یافتن سازنده یا منشأ اصلی ویروس مشکل است.

عملکرد ویروس

همان‌طور که گفته شد تنها پنج درصد از ویروس‌ها دارای اثرات تخریبی هستند و بقیه صرفاً تکثیر می‌شوند. با توجه به این مطلب این پرسش مطرح است که چرا ویروس‌ها به عنوان یک معضل شناخته می‌شوند و باید با آن‌ها مبارزه کرد؟ پاسخ به این پرسش در موارد زیر خلاصه گردیده است :

۱. بسیاری از ویروس‌ها دارای اثراتی هستند که هرچند تخریبی نمی‌باشد ولی می‌تواند برای کاربر ایجاد مزاحمت کند. مثلاً ممکن است پیغامی نمایش دهد، باعث ریزش حروف صفحه نمایش به پایین شود یا اینکه یک آهنگ پخش نماید. علاوه بر این برخی از ویروس‌ها به علت اشکالات نرم‌افزاری که ناشی از عدم دقت ویروس‌نویس می‌باشد، ممکن است دارای اثراتی غیرقابل پیش‌بینی باشند که گاهی این اثرات می‌توانند تخریبی نیز باشند. از دیدگاه کاربر اهمیتی ندارد که خسارت ایجاد شده به وسیله یک ویروس، یک کار عمدی پیش‌بینی شده توسط نویسنده ی ویروس باشد یا یک اشتباه برنامه نویسی .

۲. برخی از ویروس‌ها در حافظه کامپیوتر مقیم شده و از این طریق عملیات تکثیر خود را انجام می‌دهند. این عمل ممکن است به گونه‌ای باشد که جایی برای اجرای برنامه‌های دیگر نماند یا باعث ایجاد تأخیر یا وقفه در حین عملیات سیستم اعم از اجرای برنامه‌ها یا راه‌اندازی کامپیوتر گردد.

۳. فرض کنید که شما یک ویروس بر روی کامپیوتر خود داشته باشید. بسیار احتمال دارد که این ویروس به صورت غیرعمدی به یک دوست، همکار یا مشتری منتقل شود که این امر ممکن است باعث از بین رفتن اعتماد آن‌ها به شما و شرکت شما شود.

۴. ویروس‌ها و برنامه‌های مخرب زیادی وجود دارند که اقدام به سرقت اطلاعات و کلمات عبور کاربر می‌نمایند. بعضی از اینگونه برنامه‌ها با مقیم شدن در حافظه از عباراتی که توسط شما تایپ می‌شود گزارش گرفته و پس از اتصال رایانه شما به اینترنت این اطلاعات را برای مقصد خاصی ارسال می‌کنند. گیرنده این اطلاعات می‌تواند به راحتی از آن‌ها سوء استفاده‌های مختلفی نماید.

۵. علاوه بر همه این‌ها هیچ ویروسی کاملاً بی‌ضرر نیست و در خوشبینانه‌ترین حالت، آن‌ها وقت شما، وقت پردازنده و فضای دیسک شما را تلف می‌کنند.

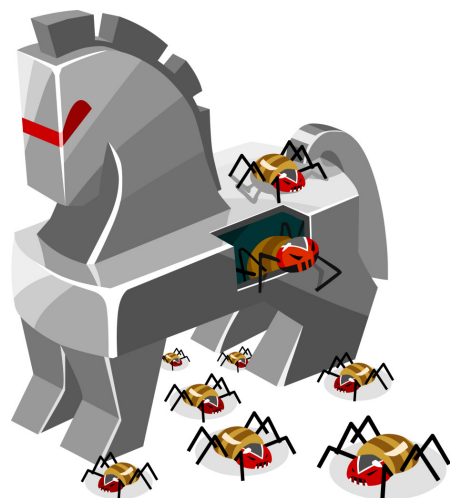
در مورد اثرات تخریبی ویروس‌هایی که آن‌ها را به صورت عمدی انجام می‌دهند می‌توان به موارد زیر اشاره نمود:

- تخریب یا حذف برنامه‌ها و اطلاعات بخش‌های مختلف دیسک‌ها
- فرمت کردن دیسک‌ها
- کد کردن اطلاعات و برنامه‌ها
- تخریب اطلاعات حافظه فلش‌ها

راه‌های ورود ویروس به سیستم عبارتند از:

- اینترنت
- حافظه‌های خارجی آلوده

۲.۳.۴ تروجان‌ها



شکل ۴.۶: Trojan

اسب تروجان (Trojan horse) یا تروجان یک برنامه نفوذی است که از نوع بدافزار است که به سیستم عامل، دسترسی سطح بالا پیدا کرده است در حالیکه به نظر می‌آید یک کار مناسب را در حال انجام است. یک داده ناخواسته روی سیستم نصب می‌کند که اغلب دارای یک در پشتی برای دسترسی غیرمجاز به کامپیوتر مقصد است.

این در پشتی‌ها گرایش به دیده نشدن توسط کاربران دارند اما ممکن است باعث کند شدن کامپیوتر شوند. تروجان‌ها تلاش برای تزریق به فایل‌ها مانند ویروس‌های

کامپیوتری را ندارند تروجان‌ها ممکن است اطلاعات به سرقت ببرند یا به کامپیوتر میزبان صدمه بزنند.

تروجان‌ها ممکن است به وسیله داندود نا خواسته یا نصب بازی‌های آنلاین یا برنامه‌های تحت شبکه یا به کامپیوتر هدف دسترسی داشته باشند. این موضوع از داستان اسب تراجان گرفته شده است و نوعی از مهندسی اجتماعی است.

تروجان ممکن است با دسترسی از راه دور نفوذگر، یک سیستم کامپیوتری را هدف قرار دهد. عملیات‌هایی که می‌تواند توسط یک هکر بر روی یک سیستم کامپیوتری مورد هدف اجرا شود شامل:

- از کار افتادن کامپیوتر
- صفحه آبی مرگ
- سرقت پول الکترونیکی
- سرقت اطلاعات
- داندود یا آپلود فایل‌ها بر روی کامپیوتر کاربر
- اصلاح یا حذف فایل

- کی لاگر
- تماشای صفحه نمایش کاربر
- تغییرات رجیستری
- نصب خود به خود برنامه‌ها

۳.۳.۴ جاسوس افزارها

جاسوس افزارها (Spyware) بد افزارهایی هستند که بر روی رایانه کاربر نصب می‌شوند و بدون اطلاع وی، اطلاعات مختلف در مورد او را جمع‌آوری می‌کنند. اکثر جاسوس افزارها از دید کاربرها مخفی می‌مانند و تشخیص و پیدا کردن آن‌ها در اغلب موارد مشکل است. برخی از جاسوس افزارها مانند کی لاگرها ممکن است توسط مسئول یک سازمان یا شرکت بر روی رایانه‌ها نصب شوند تا رفتار کاربران قابل ارزیابی و بررسی باشد.

جاسوس افزارها هر گونه اطلاعاتی را می‌توانند جمع‌آوری کنند. این اطلاعات می‌تواند اطلاعات شخصی یک کاربر مانند گشت و گذارهای وی بر روی اینترنت یا مشخصات حساب‌های مختلف وی مانند رمز عبور پست الکترونیکی و... باشد. علاوه بر این، جاسوس افزارهای می‌توانند در کنترل رایانه توسط کاربر اختلال ایجاد کنند. به عنوان مثال، جاسوس افزارهای می‌توانند کاربر را به بازدید از یک صفحه خاص اینترنتی مجبور کنند یا اینکه با تغییر تنظیمات رایانه وی، باعث کاهش سرعت اینترنت و دسترسی غیرمجاز به رایانه وی شوند.

۴.۳.۴ روشهای مقابله با بد افزارها

آنتی ویروس (Antivirus)

آنتی ویروس اصطلاحی است که به برنامه یا مجموعه‌ای از برنامه‌ها گفته می‌شود که برای محافظت از رایانه‌ها در برابر ویروس‌ها به کار گرفته می‌شود. این برنامه‌ها با بررسی محتوای پوشه‌ها، به دنبال ویروس‌ها یا کرم‌های رایانه‌ای می‌گردند و در صورت مشاهده از ورودشان به رایانه و اجرا شدنشان جلوگیری می‌کنند یا به شما هشدار



شکل ۷.۴: Antivirus

می‌دهند یا دستور می‌گیرند که ویروس را پاک کنند. گاه برای پاک کردن ویروس باید پوشه‌ی آلوده را پاک کرد و گاه نیز می‌توان خسارت‌هایی را که به آن وارد شده، ترمیم کرد. نرم‌افزار ضدویروس سه وظیفه‌ی عمده را انجام می‌دهند :

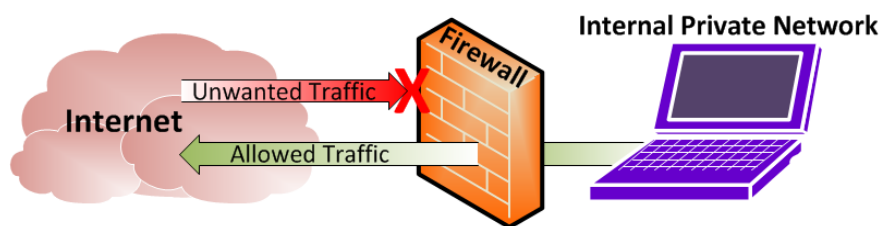
۱. بازرسی یا کشف

۲. تعیین هویت یا شناسایی

۳. آلودگی‌زدایی یا پاکسازی

شرکت‌های سازنده نرم‌افزارهای ضدویروس، با ساخته شدن ویروس‌های جدید، الگوهای نرم‌افزاری آن‌ها را کشف و جمع‌آوری می‌کنند و به همین علت اغلب لازم است تا این نرم‌افزارها هر از چندگاهی به‌روزرسانی (Update) شوند تا الگوهای جدید ویروس‌ها را دریافت کنند.

دیوار آتش (Firewall)



شکل ۴.۸: Firewall

دیوار آتش (Firewall) نام عمومی برنامه‌هایی است که از دستیابی غیرمجاز به یک سیستم رایانه جلوگیری می‌کنند. در برخی از این نرم‌افزارها، برنامه‌ها بدون اخذ مجوز قادر نخواهند بود از یک رایانه برای سایر رایانه‌ها، داده ارسال کنند. نوع دیگری از فایروال نیز وجود دارد که به آن فایروال معکوس می‌گویند. فایروال معکوس ترافیک خروجی شبکه را فیلتر می‌کند. فایروال‌ها صرفاً پورت‌های ضروری برای کاربران یا سایر برنامه‌های موجود در خارج از شبکه را در دسترس و قابل استفاده می‌کنند. برای افزایش ایمنی، سایر پورت‌ها غیرفعال می‌گردد.

تا امکان استفاده از آنان توسط هکرها وجود نداشته باشد. در برخی موارد و با توجه به نیاز یک برنامه می‌توان موقتاً تعدادی از پورت‌ها را فعال و پس از اتمام کار مجدداً آنان را غیرفعال نمود. اگر برای اتصال به اینترنت از وسیله‌ای مانند روتر بیسیم، دستگاهی که به شما امکان می‌دهد تا از اینترنت بیسیم استفاده کنید، داشته باشید احتمالاً هم‌اکنون نیز دیوار آتش دارید و نیازی به نصب جداگانه آن بر روی سیستم در بسیاری از مواقع وجود ندارد.