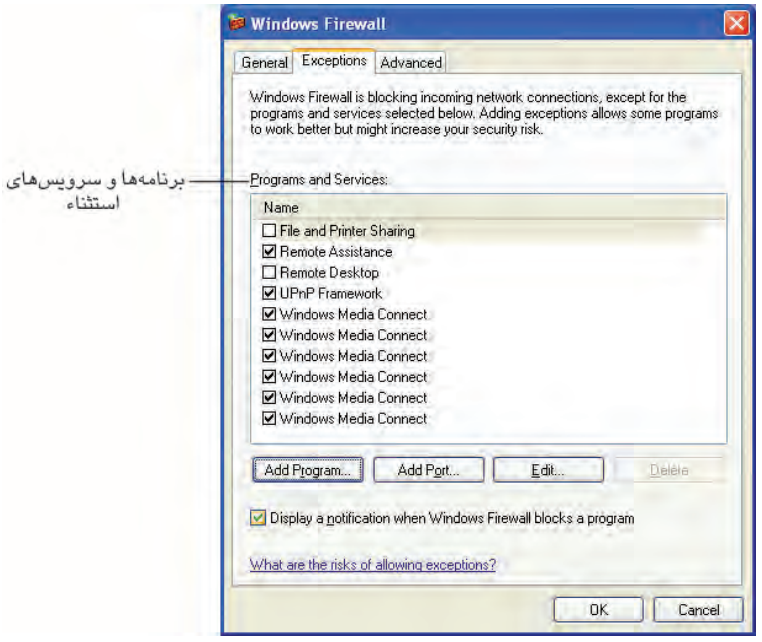
۳-۵ فعال کردن دیوار آتش و تعریف برنامه‌های استثناء

در شکل ۲-۵ با کلیک روی گزینه On(recommended) دیوار آتش فعال و با کلیک روی گزینه Off (not recommended) غیرفعال می‌شود.

گاهی اوقات ممکن است بخواهیم به برنامه یا سرویس مشخصی اجازه دسترسی به سیستم و ورود اطلاعات از طریق آن برنامه را بدهیم و در واقع راهی را برای آن برنامه یا سرویس باز نگه داریم. در این‌صورت می‌توانیم آن درگاه یا برنامه را به‌صورت استثناء تعریف کنیم.

به‌عنوان مثال ممکن است بخواهیم به یک بازی چند نفره تحت شبکه یا اینترنت بپردازیم. در این زمان با باز نگه‌داشتن درگاه مربوط به آن بازی، دیوار آتش به سیستم ما اجازه می‌دهد به اطلاعات بازی دسترسی داشته باشد.



شکل ۳-۵ تعیین استثناء برای دیوار آتش

در شکل ۳-۵ دکمه‌های Add Program و Add Port به ترتیب برای تعیین برنامه‌ها و درگاه‌های استثناء هستند. اگر می‌خواهید دیوار آتش عمل مبادله اطلاعات توسط یک برنامه مشخص را مسدود نکند، با استفاده از دکمه Add Program آن را به لیست برنامه‌ها و سرویس‌های استثناء اضافه کنید. اما برای مشخص کردن این استثناء از طریق شماره درگاه آن روی دکمه Add Port

کلیک کنید.

معمولاً برای هر برنامه‌ای که نیاز به مبادله اطلاعات از طریق شبکه یا اینترنت دارد یک شماره درگاه مشخص شده است، برای آگاهی از شماره درگاه هر برنامه کافی است به بخش راهنمای آن (Help) مراجعه کنید.

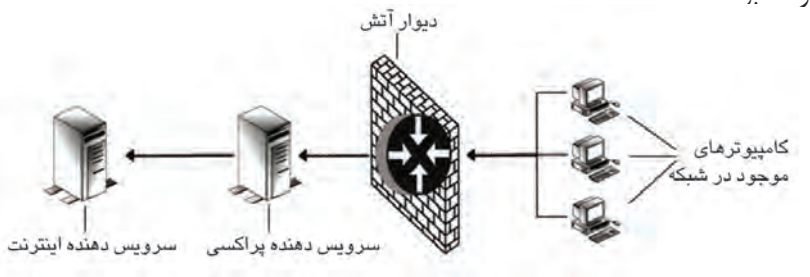
اگر در نظر داشته باشید هیچ استثنایی قائل نشوید و بخواهید دیوار آتش سیستم را در مقابل تمام برنامه‌ها و اطلاعات فاقد مجوز حفاظت کنید، در زبانه General (شکل ۲-۵) گزینه Don't allow exceptions را فعال کنید.

در نسخه SP3 و SP2 ویندوز XP، دیوار آتش به‌طور پیش‌فرض فعال است.

پراکسی (Proxy)

پراکسی ابزاری است که تا حدود زیادی مشابه دیوار آتش عمل می‌کند و معمولاً به‌صورت نرم‌افزاری قابل پیاده‌سازی است. پراکسی روی سرویس‌دهنده اینترنت یا روی سیستم دیگری نصب می‌شود اما از لحاظ عملکرد خود را بین کامپیوتر سرویس‌گیرنده و سرویس‌دهنده اینترنت قرار می‌دهد.

در صورتی‌که دیوار آتش نیز فعال شده باشد محل قرارگیری هرکدام از اجزای شبکه به‌صورت شکل زیر خواهد بود.



شکل ۴-۵ موقعیت سرویس‌دهنده پراکسی و سایر اجزا در شبکه

پراکسی‌ها داده‌های اینترنتی را در مسیر عبور و قبل از رسیدن به کامپیوتر می‌سنجند، اگر آن‌ها برخلاف سیاست‌های امنیتی سیستم باشند، آن‌ها را دور می‌ریزد و در غیر این‌صورت اجازه عبور از دیوار آتش و رسیدن به سیستم را به آن‌ها می‌دهد. پراکسی‌ها محتویات بسته‌های اطلاعات ارسالی

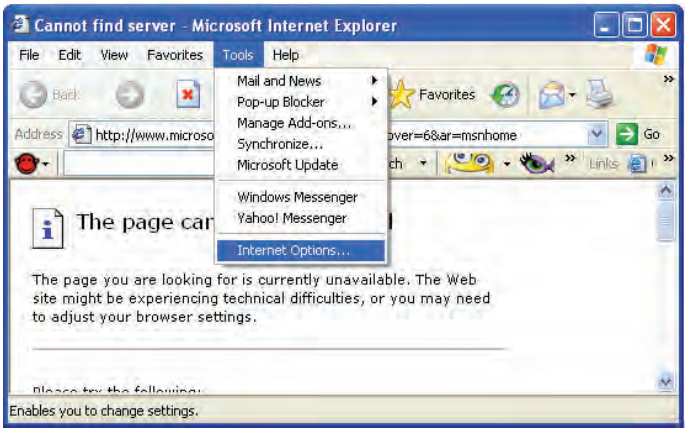
در اینترنت را به‌طور دقیق بررسی می‌کنند اما دیوارهای آتش محتویات اطلاعات را به‌طور کلی و بدون جزییات مورد بازرسی قرار می‌دهند.

پراکسی‌ها علاوه بر موارد فوق، کاربردهای دیگری نیز دارند:

- از طریق قواعد خاصی که برای آن‌ها تعیین می‌شود، برخی از سایت‌های غیرمجاز را فیلتر کرده و از دسترسی افراد به این سایت‌ها جلوگیری می‌کند.
- هر بار که به اینترنت متصل می‌شویم، سرویس‌دهنده پراکسی به ما یک آدرس IP منحصر به‌فرد اختصاص می‌دهد و تا زمانی‌که در اینترنت مشغول گشت و گذار هستیم، این IP با ما همراه است و به این ترتیب کامپیوتر ما در اینترنت دارای یک هویت می‌شود. سرویس‌دهنده پراکسی این آدرس IP را در دفعات بعدی ارتباط با اینترنت عوض می‌کند تا از سوء استفاده هکرها و افراد مزاحم جلوگیری کند.
- کاربرد دیگر سرویس‌دهنده پراکسی که امروزه کاربرد وسیعی دارد، Cache کردن اطلاعات است. سرویس‌دهنده پراکسی، اطلاعات سایت‌هایی را که بیشتر به آن‌ها مراجعه می‌شود، در یک حافظه جداگانه نگه می‌دارد، به‌طوری که برای مراجعه مجدد به آن‌ها نیازی به دریافت مجدد اطلاعات از طریق ارتباط با سرویس‌دهنده اینترنت نباشد و مستقیماً اطلاعات آن سایت‌ها از طریق پراکسی دریافت می‌شوند.

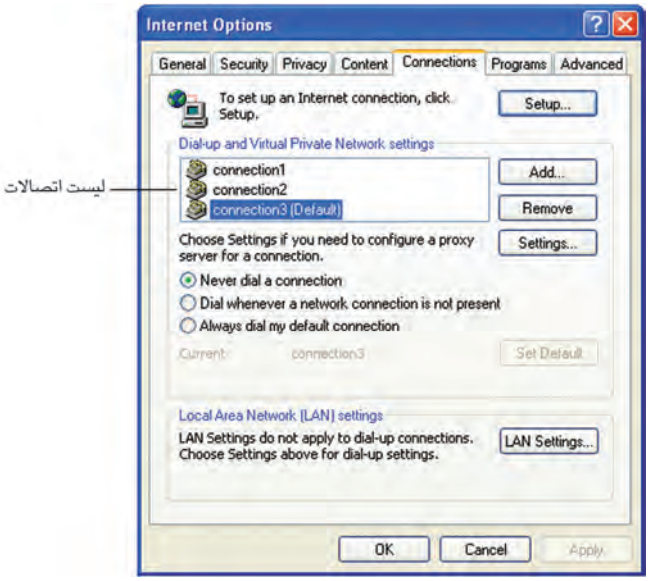
با استفاده از این قابلیت از یک طرف سرعت دسترسی به اطلاعات کمتر شده و از طرف دیگر پهنای باند موجود برای دریافت اطلاعات تکراری اشغال نمی‌شود و به برنامه‌های دیگر اختصاص پیدا می‌کند.

برای فعال کردن سرویس‌دهنده پراکسی در پنجره Internet Explorer، از منوی Tools گزینه Internet Options... را انتخاب کنید.



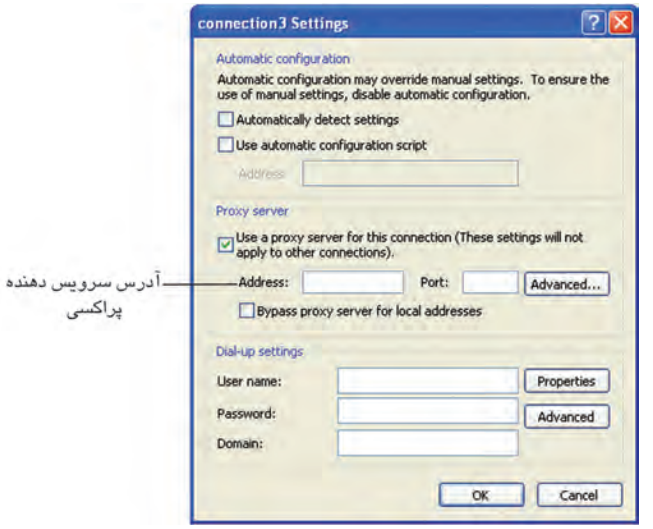
شکل ۵-۵ انتخاب گزینه Internet Options

در کادر محاوره Internet Options در زبانه Connections از لیست اتصالات، گزینه‌ای را که می‌خواهید پراکسی برای آن فعال شود انتخاب کنید.



شکل ۶-۵ انتخاب اتصال مورد نظر

سپس روی دکمه ...Settings کلیک کنید.



شکل ۷-۵ فعال کردن سرویس‌دهنده پراکسی

در کادرمحاوره ۷-۵ گزینه Use a proxy server... را فعال کرده و در مقابل Address، آدرس سرویس‌دهنده پراکسی را وارد کنید.

به‌عنوان مثال اگر آدرس سرویس‌دهنده پراکسی www.x.com باشد، این عبارت را مقابل قسمت Address وارد می‌کنیم یا اینکه در قسمت Port شماره درگاه آن‌را وارد می‌کنیم.

هنگام کار با اینترنت سرویس‌دهنده پراکسی از طریق سرویس‌دهنده اینترنتی که از آن استفاده می‌کنیم، تنظیم شده است و بدون نیاز به تنظیم توسط کاربر تمامی امکانات سرویس‌دهنده پراکسی قابل دسترسی هستند.

Learn in English

Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets: All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

واژه‌نامه

Access	دستیابی
Block	متوقف‌کردن
Combination	تلفیق
Criteria	معیار
Design	طراحی‌کردن
Enter	وارد شدن
Examine	آزمایش‌کردن
Exception	استثناء
Fire wall	دیوار آتش
Implement	قرارگرفتن
Intranet	اینترانت[1]
Pass through	خارج شدن از
Private	خصوصی
Recommended	توصیه شده
Specified	بخصوص
Unauthorized	بدون مجوز

۱- به یک شبکه خصوصی گفته می‌شود که برای مدیریت اطلاعات درون یک شرکت یا یک سازمان طراحی شده است.

خلاصه مطالب

- هنگام ارتباط با اینترنت یکی از مهم‌ترین مسائلی که بررسی می‌شود، حملات اینترنتی است که در نتیجه این حملات، ممکن است اطلاعات شخصی ما در دسترس افراد غیرمجاز قرار گرفته یا اینکه سیستم، مورد حمله انواع ویروس‌ها قرار بگیرد.
- سیستم عامل ویندوز روش‌هایی برای مقابله با این تهدیدات و حملات ارائه می‌دهد که از مهم‌ترین آن‌ها دیوار آتش و تنظیم پراکسی است.
- دیوار آتش مانند یک دیوار دفاعی از سیستم در برابر تهدیدات امنیتی محافظت می‌کند.
- پراکسی‌ها از امکانات پیشرفته‌تر ویندوز هستند و به عنوان یک رابط بین دیوار آتش و سرویس‌دهنده‌های اینترنتی قرار می‌گیرند.
- پراکسی‌ها بسته‌های اطلاعات ارسال شده از طرف شبکه را به‌طور دقیق بررسی کرده و به اطلاعات مشکوک یا اطلاعاتی که با قوانین امنیتی سرویس‌گیرنده مغایرت دارند، اجازه عبور نمی‌دهند. پراکسی‌ها همچنین می‌توانند سایت‌های خاصی را فیلتر کرده و به کاربر اجازه ورود به آن‌ها را ندهند.
- یکی دیگر از کاربردهای سرویس‌دهنده پراکسی Cache کردن اطلاعات است که با این عمل از اشغال پهنای باند اینترنت توسط اطلاعات تکراری جلوگیری می‌شود.

آزمون نظری

۱- در کدام‌یک از نسخه‌های ویندوز XP، دیوار آتش به‌طور پیش‌فرض فعال است؟

الف- SP1

ب- SP2

ج- SP2 و SP1

د- همیشه به‌طور پیش‌فرض دیوار آتش غیرفعال است.

۲- کدام‌یک از گزینه‌های زیر محتویات ارسالی از اینترنت را قبل از دریافت توسط کامپیوتر به‌طور دقیق‌تر بررسی می‌کنند؟

الف- دستگاه مودم ب- دیوار آتش ج- پراکسی د- نرم‌افزارهای ضد ویروس

۳- کدام‌یک از موارد زیر از وظایف پراکسی‌ها نیست؟

الف- فیلترکردن سایت‌ها

ب- تشخیص ویروس‌های روی سیستم

ج- Cache کردن اطلاعات

د- اختصاص IP منحصر به‌فرد در اینترنت

۴- محل قرارگیری دیوار آتش به‌طور فرضی کجاست؟

الف- روی کارت شبکه یا مودم

ب- بین کارت شبکه یا مودم و سرویس‌دهنده اینترنت

ج- بین کارت شبکه یا مودم و کامپیوتر

د- روی کامپیوتر

5- Which of the following sentences is not correct?

a- Some of the messages entering or leaving the Intranet pass through the firewall.

b- Firewalls can be implemented in both hardware and software, or a combination of both.

c- Firewalls are used to prevent unauthorized Internet.

d- Firewall is a system designed to prevent unauthorized access to or from a private network.

۶- انواع تهدیداتی را که هنگام اتصال به شبکه و اینترنت ممکن است به‌وجود بیاید، بیان کنید.

۷- امکاناتی که سیستم عامل ویندوز برای محافظت از سیستم در نظر گرفته، چیست؟

۸- نحوه عملکرد دیوار آتش را توضیح دهید.

۹- پراکسی چیست؟

۱۰- تفاوت اصلی دیوار آتش و پراکسی را بیان کنید.

۱۱- انواع کاربرد سرویس‌دهنده پراکسی را بیان کنید.

آزمون عملی

۱- بررسی کنید که در حال حاضر سیستم شما کدام‌یک از روش‌های محافظت از سیستم را استفاده می‌کند.

۲- دیوار آتش را فعال کنید.

۳- روی سیستم خود یک استثناء برای برنامه Windows Media Player تعریف کنید، طوری که دیوار آتش اطلاعات مبادله شده توسط این نرم‌افزار را مسدود نکند.

۴- برای سیستم خود یک سرویس‌دهنده پراکسی با آدرس www.a.com فعال کنید.

واحد کار ششم

توانایی اعمال محدودیت در حساب کاربری

هدف‌های رفتاری

پس از مطالعه این واحد کار از فراگیر انتظار می‌رود که:

۱- امکانات فایل سیستم NTFS را بشناسد.

۲- انواع مجوزها را برای محدود کردن اختیارات کاربران بشناسد.

۳- بتواند مجوزهای مختلف را برای کاربران تعریف کند.

۴- بتواند مفهوم خاصیت ارث‌بری را توضیح دهد و هنگام کار با مجوزها آن را اعمال کند.

۵- اختیارات مجوزهای خاص را بشناسد و بتواند با آن‌ها کار کند.

۶- مفهوم فشرده‌سازی و رمزنگاری را شناخته و آن را برای فایل‌ها و پوشه‌ها اعمال کند.

زمان (ساعت)

نظری	عملی
۴	۶

کلیات

به‌طور کلی به بخشی از سیستم‌عامل که با فایل‌ها سروکار دارد فایل سیستم گفته می‌شود. از مهم‌ترین وظایف فایل سیستم می‌توان به موارد زیر اشاره کرد:

۱- ایجاد، تغییر نام و حذف فایل

۲- نوشتن و خواندن از فایل

۳- کنترل دستیابی به فایل، مثلاً از تغییر فایل‌های Read only جلوگیری شود.

۴- تغییر محتویات فایل

۵- دیدن و تغییر دادن صفت فایل

شرکت مایکروسافت از زمان عرضه MS DOS تاکنون سه فایل سیستم FAT16، FAT32 و NTFS را به بازار عرضه کرده است. FAT16 اولین بار در سیستم‌عامل MS DOS مورد استفاده قرار گرفت. به علت یکسری معایب FAT16 مایکروسافت فایل سیستم جدیدی به‌نام FAT32 با امکانات بیشتر معرفی کرد. از زمان عرضه ویندوز ۲۰۰۰ تاکنون فایل سیستم NTFS [1] با مزایای بیشتری مورد استفاده قرار می‌گیرد.

هنگام نصب ویندوز، تعیین نوع فایل سیستم بسیار مهم است. شرکت مایکروسافت، فایل سیستم NTFS را برای درایو نصب ویندوز XP پیشنهاد می‌کند. در این واحدکار با امکانات NTFS آشنا می‌شوید. تمام فعالیت‌هایی که در این واحدکار انجام می‌گیرد تنها در NTFS قابل اجراست.

۱-۶ امکانات NTFS

NTFS مزایای بیشتری نسبت به FAT16 و FAT32 دارد. از مهم‌ترین آن‌ها می‌توان به موارد زیر اشاره کرد:

۱- پشتیبانی از فضای بزرگ‌تر از ۳۲ GB برای یک پارتیشن (حداکثر اندازه مجاز یک پارتیشن در FAT32، ۳۲ GB است اما NTFS تا اندازه ۲ TB برای یک پارتیشن را پشتیبانی می‌کند.)

۲- سرعت دسترسی بالاتر به محتویات فایل

۳- امکان فشرده کردن فایل‌ها برای صرفه‌جویی در فضای دیسک

۴- امکان رمزگذاری فایل‌ها برای بالا بردن امنیت

1- New Technology File System

۵- تعیین مجوز دسترسی به فایل‌ها

۶- تعیین سهمیه استفاده از فضای هر درایو تا GB ۲ برای کاربران، مثلاً می‌توان برای User1 محدودیت استفاده از درایو E تا سقف GB ۲ ایجاد کرد.

۶-۲ اعمال مجوز به حساب کاربری

در ویندوز مقدماتی با نحوه ایجاد حساب کاربری برای کسانی که به‌طور مشترک از یک کامپیوتر استفاده می‌کنند، آشنا شدید. همان‌طور که می‌دانید حساب‌های کاربری به دو دسته تقسیم می‌شوند: Administrator و Limited . Administrator یا مدیر سیستم دارای تمام اختیارات است اما کاربر از نوع Limited فاقد اختیاراتی چون نصب و حذف برنامه یا سخت‌افزار، ایجاد یک حساب کاربری جدید، مشاهده حساب‌های کاربری دیگران یا تغییر نوع حساب کاربری خود است. در حساب کاربری Limited همه فایل‌ها (به غیر از محتویات پوشه My Documents افراد دیگر) قابل مشاهده هستند و کاربر به راحتی می‌تواند آن‌ها را ویرایش یا حذف کند. با توجه به توضیحات بخش ۶-۱، به کمک فایل سیستم NTFS می‌توان برای دسترسی به فایل‌ها و پوشه‌های خاص در حساب‌های کاربری مختلف محدودیت ایجاد کرد. برای اعمال این محدودیت‌ها، مدیر سیستم مجوزهایی را به کاربران می‌دهد. در این بخش با نحوه تعریف مجوز دسترسی بیشتر آشنا می‌شوید.

۶-۲-۱ انواع مجوزها

ویندوز XP در فایل سیستم NTFS برای فایل‌ها و پوشه‌ها دو دسته مجوز به نام‌های مجوزهای استاندارد و مجوزهای خاص تعریف کرده است. یک مجوز استاندارد از یک یا چند مجوز خاص تشکیل شده است. مجوزهای استاندارد به شرح زیر هستند:

۱- **Read:** در این حالت می‌توان محتویات فایل یا پوشه، صفات آن‌ها یا حتی مجوز دسترسی به آن‌ها را مشاهده کرد. در کل هر چیزی که مربوط به دیدن باشد با این مجوز قابل انجام است.

۲- **Write:** به کمک این مجوز می‌توان محتویات یک فایل را تغییر داد، مثلاً محتوای فایل را پاک کرد یا چیزی به آن افزود. همچنین می‌توان فایلی ایجاد کرد و صفات آن را خواند یا تغییر داد. اگر این مجوز برای یک پوشه اعمال شود می‌توان داخل پوشه، پوشه‌های دیگری را ایجاد کرد. دقت کنید تنها با داشتن این مجوز نمی‌توان فایل یا پوشه مربوطه را حذف کرد.

۳- **List Folder Contents:** به کمک این مجوز می‌توان محتویات پوشه را مشاهده کرد اما امکان تغییر یا حذف درون آن وجود ندارد. همچنین می‌توان فایل‌ها را اجرا کرد و صفات آن‌ها را خواند.

۴- **Read & Execute:** علاوه بر داشتن امکانات مجوز Read، کاربر می‌تواند فایل‌های اجرایی را نیز اجرا کند.

در بسیاری از موارد برای اجرای یک فایل اجرایی باید محتوای چندین فایل دیگر خوانده شوند. مثلاً برای اجرای کامل فایل اجرایی برنامه فتوشاپ، محتوای فایل‌های زیادی باید خوانده شود. بنابراین تنها با داشتن مجوز Read نمی‌توان گروه زیادی از فایل‌های اجرایی را اجرا کرد.

۵- **Modify:** با داشتن این مجوز، علاوه بر فراهم بودن تمام امکانات مجوزهای بالا می‌توان فایل یا پوشه مربوطه را (در صورت نداشتن زیرپوشه) حذف کرد.

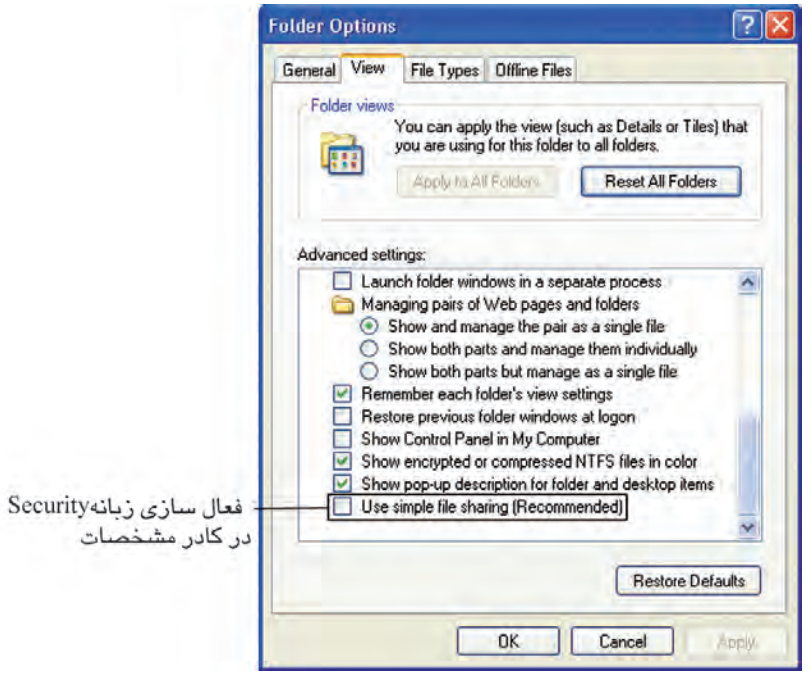
۶- **Full Control:** علاوه بر داشتن اختیارات Modify می‌توان مجوز دسترسی دیگر کاربران را به فایل یا پوشه مربوطه تغییر داد.

اعضای گروه Administrator از قاعده Full Control مستثنی هستند، یعنی چه دارای مجوز Full Control باشند و چه نباشند، می‌توانند مجوزهای دیگران را تغییر دهند.

در ویندوز XP قسمت دسترسی به مجوزها به‌طور پیش‌فرض غیرفعال است. برای فعال کردن آن باید این مراحل را طی کرد:

۱- در پنجره Control Panel روی Folder Options دابل کلیک کنید.

۲- در زبانه View گزینه Use simple file sharing (Recommended) را از حالت انتخاب خارج کنید تا زبانه Security در کادرمحاوره مشخصات فایل و پوشه‌ها فعال شود.



شکل ۱-۶ کادرمحاوره Folder Options

۲-۲-۶ نحوه اعمال مجوزها

برای انجام این کار مراحل زیر را طی کنید[۱]:

۱- روی فایل یا پوشه مورد نظر کلیک راست کرده و سپس گزینه Properties را انتخاب کنید.

۲- در کادر مشخصات، وارد زبانه Security شوید.

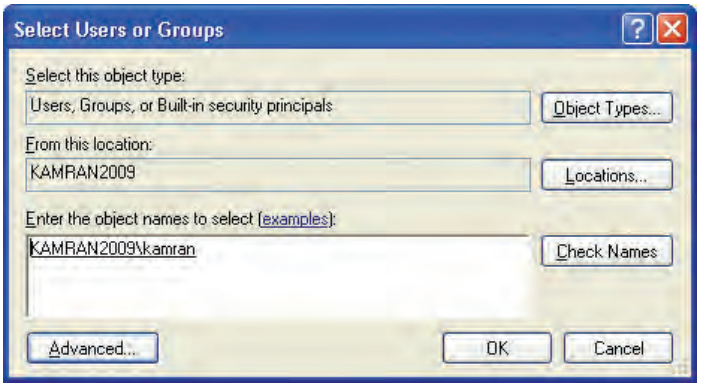
در این کادر مطابق شکل ۲-۶ دو قسمت اصلی برای تعیین نام کاربر و مشخص کردن مجوزهای دسترسی وجود دارد.

۱- همه تنظیمات انجام گرفته در شکل‌ها برای پوشه‌ای به نام class انجام شده است.

شکل ۲-۶ کادرمحاوره مشخصات پوشه class

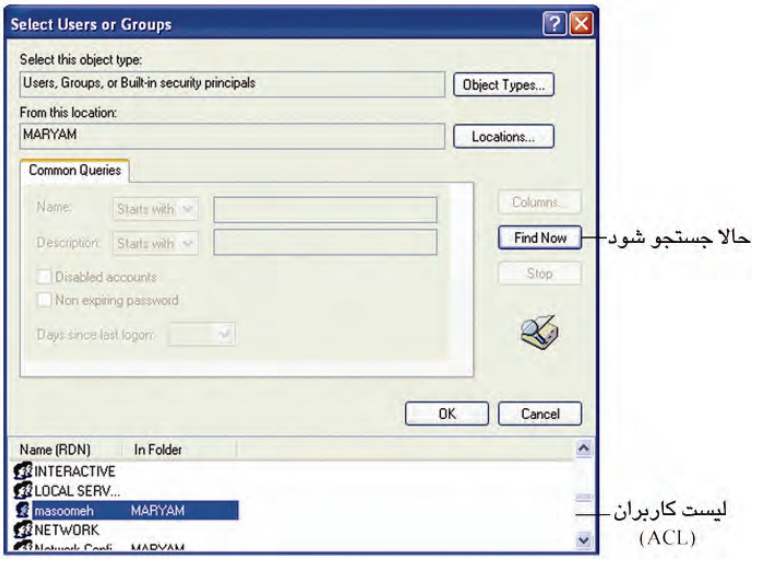
اگر بخواهید برای دسترسی یک حساب کاربری یا یک گروه محدودیت ایجاد کنید، باید نام آن را در کادر Group or user names انتخاب کنید. حال اگر اسم آن در لیست وجود نداشت می‌توان یکی از این دو روش را برای اضافه کردن استفاده کرد:

- در قسمت Group or user names روی دکمه Add... کلیک کرده تا کادر Select Users or Groups (شکل ۳-۶) ظاهر شود. حال نام کاربر را در کادر متنی From this location نوشته و سپس برای اطمینان گزینه Check Name را کلیک کنید تا صحت آن را بررسی کند، سپس روی دکمه OK کلیک کنید.



شکل ۳-۶

- اگر در کادرمحاوره Select Users or Groups روی دکمه Advanced و سپس روی دکمه Find Now کلیک کنید (شکل ۴-۶) ویندوز نام همه کاربران را جستجو کرده و نمایش می‌دهد. کاربر مورد نظر خود را انتخاب کرده و روی دکمه OK کلیک کنید تا نام کاربر در کادر Group or user names مشاهده شود، سپس روی دکمه OK برای تأیید نهایی کلیک کنید.



شکل ۴-۶ نحوه افزودن نام یک کاربر به کادر متنی **Group or user names**

۳- پس از انتخاب نام کاربری باید در قسمت ... Permissions for مجوزهای دسترسی را تعیین کنید. روبه‌روی هر مجوز دو گزینه با عنوان‌های Allow و Deny وجود دارد. Allow به معنای این است که کاربر یا گروه آن مجوز را دارد اما Deny یعنی کاربر یا گروه مجوز مربوطه را ندارد.

مثال: اگر در گروهی با تعداد کاربران زیاد بخواهید اختیارات یک کاربر خاص را محدودتر کنید چه باید کرد؟ اگر اختیارات گروه را محدودتر کنید اختیارات بقیه کاربران هم تغییر می‌کند. بهترین راه حل این است که پس از تعیین اختیارات گروه نام کاربر موردنظر را از لیست کاربران انتخاب کرده و سپس در قسمت تعیین مجوز به کمک گزینه Deny مجوزی را که می‌خواهید از او سلب شود، تعیین کنید. به علت بالاتر بودن اولویت Deny نسبت به Allow با وجود فعال بودن دو گزینه Allow و Deny، گزینه Deny غالب است. بدین صورت کاربر تمام مجوزهای گروه را خواهد داشت منهای مجوزی که به صورت اختصاصی از او سلب شده است.

اولویت گزینه Deny بالاتر از Allow است.

شکل ۵-۶ نحوه تعیین مجوز برای کاربر

پس از انجام تنظیمات روی دکمه OK کلیک کنید.

۳-۲-۶ ارث‌بری مجوزها

یکی از نکات جالب در مجوزهای دسترسی خاصیت ارث‌بری است. بدین معنی که پس از ایجاد یک

پوشه، تمام مجوزها از پوشه بالایی (پوشه پدر) به‌طور پیش‌فرض به او می‌رسد.

برای غیرفعال کردن این خاصیت باید:

۱- در زبانه Security روی دکمه Advanced کلیک کنید.

۲- در قسمت پایین کادرمحاوره باز شده گزینه ... Inherit from parent را از حالت انتخاب خارج کنید.

شکل ۶-۶ کادرمحاوره Advanced Security Settings برای انجام تنظیمات پیشرفته

ضمناً اگر گزینه ... Replace permission entries on را انتخاب کنید، مجوزهای در نظر گرفته شده برای پوشه، به تمامی زیر پوشه‌ها اعمال می‌شود. این حالت برای زمانی است که از قبل، قابلیت ارث‌بری بعضی از پوشه‌ها را غیرفعال کرده باشید و حال بخواهید تمام پوشه‌ها از یک مجوز خاص پیروی کنند.

مثال: فرض کنید که در پوشه class سه فایل به نام‌های a، b و c وجود دارد، اگر شما بخواهید برای این سه فایل، سه مجوز متفاوت تعریف کنید باید:

- در کادرمحاوره Advanced Security Settings for class هر سه فایل گزینه Inherit from parent ... را غیرفعال کرده و مجوزهای لازم را تعریف کنید.

حال اگر پشیمان شده و مجدداً بخواهید که این سه فایل از همان اختیارات تعریف شده برای پوشه class استفاده کنند می‌توانید یکی از روش‌های زیر را به‌کارگیرید:

- در کادرمحاوره Advanced Security Settings for class هر سه فایل گزینه Inherit from parent ... را فعال کنید.
- در کادرمحاوره Advanced Security Settings for class پوشه class گزینه Replace permission entries on ... را فعال کنید.

تمرین۱: زبانه Security را در کادر مشخصات فعال کرده و سپس برای پوشه‌ای خاص مجوز خواندن را برای کاربر مشخصی تعریف کنید.

تمرین۲: خاصیت ارث‌بری را برای فایل‌های درون پوشه غیرفعال کنید.

۶-۲-۴ مجوزهای خاص (Special Permissions)

آخرین گزینه کادر تعیین مجوز گزینه Special Permissions است (شکل ۶-۲). به کمک این گزینه می‌توان مجوزهای دقیق‌تری را بیان کرد. برای فعال کردن و کار با این گزینه مراحل داده شده را دنبال کنید.

۱- در قسمت پایین کادرمحاوره شکل ۶-۲ روی دکمه Advanced کلیک کنید. کادر Advanced Security Settings for class ظاهر می‌شود.

۲- در قسمت Permission entries نام کاربر را انتخاب و سپس روی دکمه Edit ... کلیک کنید.

۳- در کادر محاوره Permission Entry for class به کمک دکمه Change ... می‌توانید نام کاربری را که می‌خواهید مجوز برای آن تعیین کنید، تعویض کنید.

شکل ۷-۶ کادرمحاوره Permission Entry for class به منظور تعریف مجوزهای خاص برای پوشه class

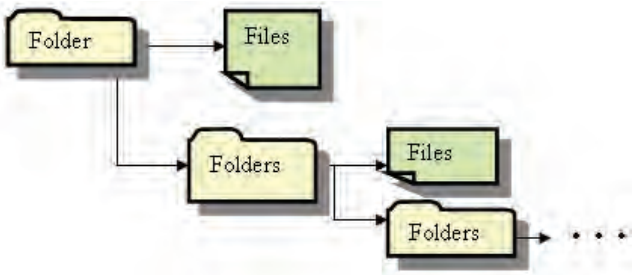
۴- در لیست بازشوی Apply onto باید مشخص کنید که این تنظیمات برای چه قسمتی اعمال شود.

برای درک بهتر گزینه‌های این قسمت، به جدول ۱-۶ دقت کنید.

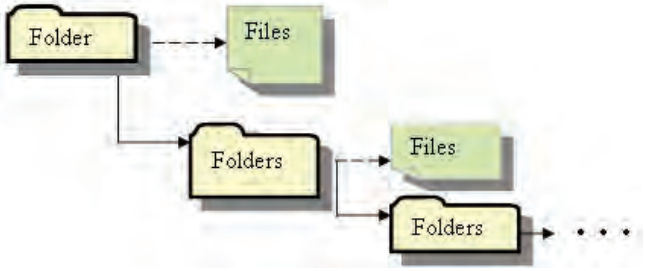
جدول ۱-۶ شرح گزینه‌های قسمت Apply onto

Apply onto	مجوزها برای پوشه جاری به‌کار رود.	مجوزها برای زیرپوشه‌های پوشه جاری به‌کار رود.	مجوزها برای فایل‌های پوشه جاری به‌کار رود.	مجوزها برای همه زیرپوشه‌های داخل زیر پوشه‌های پوشه جاری به‌کار رود.	مجوزها برای همه فایل‌های درون زیرپوشه‌های پوشه جاری به‌کار رود.
This Folder only	×				
The folder, subfolders and files	×	×	×	×	×
This folder and subfolders	×	×		×	
This folder and files	×		×		×
Subfolders and files only		×	×	×	×
Subfolders only		×		×	
Files only			×		×

مثال: براساس جدول ۱-۶ شکل‌های ۸-۶ و ۹-۶ به ترتیب بیانگر گزینه‌های This Folder, Subfolders and Files و This Folder and Subfolders هستند. اشکالی که کادر دور آن‌ها به‌صورت پررنگ‌تر نشان داده شده، بیانگر این است که مجوز برای آن‌ها اعمال می‌شود اما مجوز برای اشکالی که کادر دور آن‌ها کم‌رنگ‌تر است اعمال نمی‌شود. همچنین عبارت ... به معنای این است که اگر ساختار درختی ادامه یابد روال تکرار می‌شود. (در This folder, Subfolders and Files مجوز برای فایل‌ها و پوشه‌های داخلی‌تر به‌کار می‌رود اما در This Folder and Subfolder پوشه‌های داخلی‌تر مجوز دارند ولی فایل‌های داخلی‌تر مجوز ندارند.)



شکل ۸-۶ گزینه The Folder, Subfolders and Files



شکل ۹-۶ گزینه This Folder and Subfolders

۵- در قسمت Permissions مجوزها را مشخص کرده و سپس روی دکمه OK کلیک کنید.

مفهوم این مجوزها به شرح زیر است:

- **Traverse Folder/Execute File:** اگر پوشه‌ای دارای این مجوز باشد اجازه مشاهده پوشه‌های درون پوشه را خواهید داشت و اگر برای یک فایل اجرایی باشد می‌توانید فایل را اجرا کنید.
- **List Folder/Read Data:** اگر این مجوز برای یک پوشه باشد می‌توانید لیست محتویات پوشه را مشاهده کنید و اگر برای یک فایل باشد می‌توانید محتویات فایل را بخوانید.
- **Read Attributes:** به کمک این مجوز می‌توانید صفات فایل یا پوشه را بخوانید.
- **Read Extended Attributes:** به کمک این گزینه می‌توانید صفات گسترده فایل یا پوشه را مشاهده کنید. (صفات گسترده توسط برنامه‌ها ایجاد شده و ممکن است توسط آن‌ها هم تغییر کنند.) توضیح بیشتر درباره صفات گسترده خارج از محدوده این کتاب است.
- **Create Files/Write Data:** به کمک این مجوز می‌توان در پوشه فایل ایجاد کرد و اگر برای فایل استفاده شود می‌توانید محتویات فایل را تغییر دهید.

- **Create Folders/Append Data:** در صورت استفاده از این مجوز برای پوشه، می‌توان در آن پوشه ایجاد کرد و اگر برای فایل با محتویات متنی استفاده شود می‌توان به انتهای آن اطلاعات اضافه کرد ولی امکان تغییر محتویات از قبل نوشته شده یا حذف آن‌ها وجود ندارد.
- **Write Attributes:** توسط آن می‌توان صفات فایل یا پوشه را تغییر داد.
- **Write Extended Attributes:** می‌توان صفات گسترده فایل یا پوشه را تغییر داد.
- **Delete Subfolders and Files:** این مجوز برای پوشه استفاده می‌شود و به کمک آن می‌توان فایل‌ها یا زیرپوشه‌های آن را حذف کرد (حتی اگر فایل‌ها و زیرپوشه‌ها مجوز حذف نداشته باشند).
- **Delete:** اجازه حذف پوشه یا فایل را می‌دهد.
- **Read Permissions:** اجازه خواندن مجوزهای تعریف شده برای فایل یا پوشه را می‌دهد.
- **Change Permissions:** اجازه تغییر مجوزهای تعریف شده برای فایل یا پوشه را می‌دهد.
- **Take Ownership:** با این مجوز کاربر منتخب صاحب پوشه یا فایل می‌شود به این معنی که مانند مدیر سیستم اختیار کامل نسبت به فایل یا پوشه را دارد، همچنین در زبانه Owner کادر Advanced Security Settings نام کاربر به عنوان مالک ثبت خواهد شد.

مثال: فرض کنید پوشه Students تنها حاوی یک فایل به نام Hoda است. اگر بخواهید که User2 تنها اختیار بازکردن پوشه Students و خواندن محتوای فایل Hoda را داشته باشد باید مراحل زیر را دنبال کنید:

۱- در زبانه Security پوشه Students در قسمت Group or user names، گزینه User2 را انتخاب کنید.

۲- در قسمت Permissions دکمه Advanced را کلیک کنید.

۳- در کادر Advanced Security Settings در قسمت Permission entries پس از انتخاب گزینه User2 دکمه Edit را کلیک کنید.

۴- در قسمت Apply onto گزینه This folder and files را انتخاب کرده و در قسمت Permissions گزینه List Folder/ Read Data را فعال کنید سپس دکمه OK را کلیک کنید.

توجه: در تمرین عملی برای درک بهتر اختیارات مجوزهای خاص روی یک فایل یا پوشه، خاصیت ارث‌بری آن را غیرفعال کنید تا فقط از مجوزهایی که برایش مشخص شده است استفاده کند و مجوزهای پدر روی آن تأثیری نگذارد.

همان‌طور که قبلاً گفته شد مجوزهای استاندارد از یک یا چندین مجوز خاص تشکیل شده‌اند برای درک بهتر این موضوع، جدول ۲-۶ را مطالعه کنید.

جدول ۲-۶ اختیارات مجوزهای استاندارد برحسب مجوزهای خاص

	Traverse Folder/Execute file	List Folder/Read Data	Read Attributes	Read Extended Attributes	Create Files/Write Data	Create Folders/Append Data	Write Attributes	Write Extended Attributes	Delete Subfolders and Files	Delete	Read Permissions	Change Permissions	Take Ownership
Full Control	×	×	×	×	×	×	×	×	×	×	×	×	×
Modify	×	×	×	×	×	×	×	×		×	×		
Read & Execute	×	×	×	×							×		
List Folder contents	×	×	×	×							×		
Read		×	×	×							×		
Write					×	×	×	×			×		

مثال: براساس جدول ۲-۶ مجوز Write به معنای این است که:

۱- می‌توان فایلی ایجاد کرد یا محتوای آن را تغییر داد.

۲- پوشه‌ای در داخل پوشه موردنظر ایجاد کرد یا به محتوای فایل متنی اطلاعات اضافه کرد.

۳- صفات اصلی یا صفات گسترده فایل را تغییر داد.

۴- مجوزهای تعیین شده برای فایل یا پوشه را خواند.

۶-۲-۵ نکات لازم درباره مجوزها

در پایان بحث مجوزها لازم است دو نکته مهم گفته شود:

- مجوزها فقط برای سیستم‌عامل جاری روی فایل‌ها یا پوشه اعمال می‌شود و در سیستم‌عامل‌های دیگر مجوزهای تعیین شده دیده نشده و رعایت نمی‌شوند.
- اگر فایل یا پوشه‌ای که مجوزی برای آن تعیین شده است به یک درایو با فایل سیستمی از نوع FAT کپی یا انتقال داده شود، مجوزها دیگر اعمال نمی‌شوند.

۶-۳ فشرده‌سازی و رمزنگاری فایل‌ها و پوشه‌ها

یکی از امکانات فایل سیستم NTFS فشرده‌سازی و رمزنگاری فایل‌ها و پوشه‌هاست. فشرده‌سازی برای کم کردن حجم فایل‌ها و پوشه‌ها و رمزنگاری برای محرمانه‌کردن آن‌ها استفاده می‌شود. قبل از بیان مراحل کار لازم است چند نکته درباره رمزنگاری گفته شود:

۱- محتویات فایل یا پوشه رمزنگاری شده تنها توسط مدیر سیستم یا حساب کاربری که فایل یا پوشه در آن رمزنگاری شده، قابل مشاهده است. در ضمن تنها این افراد می‌توانند نام فایل یا پوشه رمزنگاری شده را تغییر دهند.

۲- هیچ‌گونه محدودیتی برای حذف فایل یا پوشه رمزنگاری شده وجود ندارد و کاربران می‌توانند آن را حذف کنند. (مگر اینکه مجوز حذف فایل یا پوشه رمزنگاری شده را نداشته باشند.)

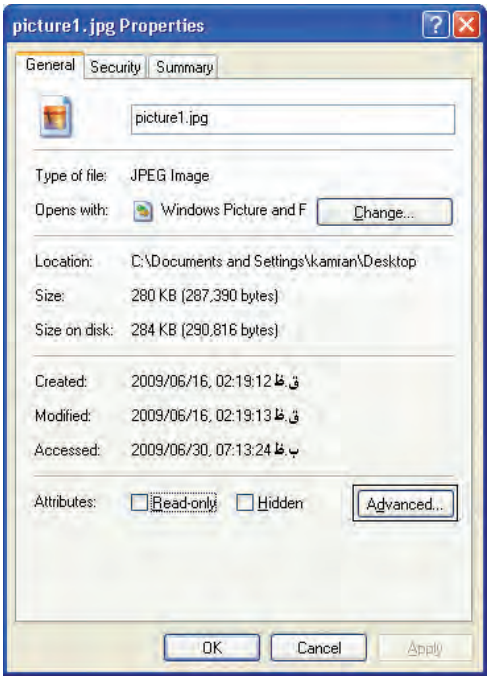
۳- فایل‌های سیستمی مانند فایل‌هایی را که در پوشه Windows درایو نصب ویندوز قرار دارند، نمی‌توان رمزنگاری کرد.

۴- اگر فایل یا پوشه رمزنگاری شده‌ای را به درایوی با سیستم فایل FAT کپی کنید، از حالت رمزنگاری خارج می‌شود.

برای انجام فشرده‌سازی یا رمزنگاری مراحل زیر را دنبال کنید:

۱- روی فایل یا پوشه کلیک راست کرده و روی گزینه Properties کلیک کنید.

۲- در زبانه General در قسمت Attributes روی دکمه Advanced کلیک کنید.

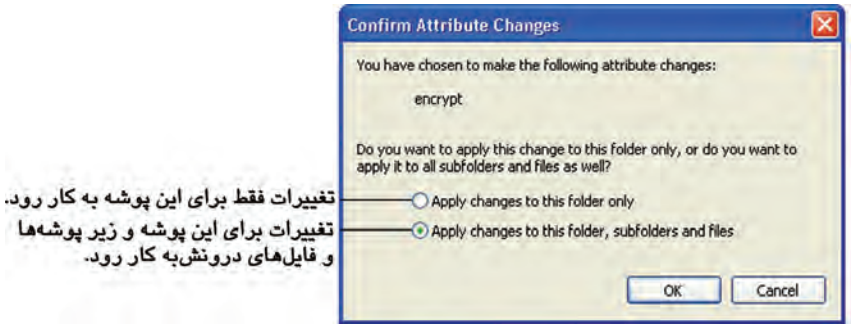


شکل ۱۰-۶

۳- مانند شکل ۱۱-۶ در قسمت Compress or Encrypt attributes به ترتیب مشخص کنید که فایل یا پوشه، فشرده یا رمزنگاری شود (امکان انتخاب هر دو با هم وجود ندارد) سپس روی دکمه OK کلیک کنید.

شکل ۱۱-۶ فشرده‌سازی و رمزنگاری فایل یا پوشه

۴- اگر عنصر موردنظر برای رمزنگاری پوشه‌ای باشد که خالی نیست، پس از کلیک روی دکمه OK در کادر Properties، یک کادرمحاوره مانند شکل ۱۲-۶ ظاهر می‌شود. در این کادر از شما سؤال می‌شود که این تغییر تنها روی پوشه اعمال شود یا در تمام زیرپوشه‌ها و فایل‌های داخل پوشه اثر بگذارد، پس از انتخاب روی دکمه OK کلیک کنید. اگر تنها پوشه رمزنگاری شود این رمزنگاری روی پوشه و فایل‌های موجود اثری نمی‌گذارد ولی اگر فایلی یا پوشه‌ای داخل پوشه ساخته شود به‌طور خودکار رمزنگاری می‌شود.



شکل ۱۲-۶ کادرمحاوره Confirm Attribute Changes

۵- اگر یک فایل را برای رمزنگاری انتخاب کرده‌اید، پس از کلیک روی دکمه OK در کادرمحاوره Advanced Attributes کادرمحاوره‌ای مانند شکل ۱۳-۶ ظاهر می‌شود. در این کادر سؤال می‌شود که آیا این تغییر تنها روی فایل اعمال شود یا پوشه پدر آن نیز رمزنگاری شود؟ اگر پوشه پدر هم رمزنگاری شود علاوه بر فایل رمزنگاری شده هر فایل یا پوشه درون پوشه پدر که پس از رمزنگاری ساخته می‌شود، به‌طور خودکار رمزنگاری می‌شود.

شکل ۱۳-۶ کادرمحاوره Encryption Warning

تمرین:

یک پوشه را همراه با محتویات آن رمزنگاری کنید.

یک فایل در درایو D را فشرده کرده و حجم آن را با حجم اولیه مقایسه کنید.

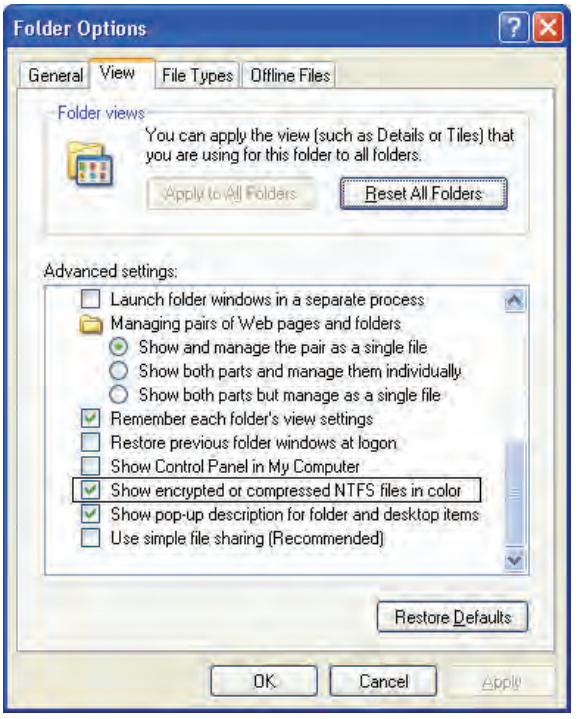
۱-۳-۶ نحوه رنگی کردن عنوان فایل‌ها و پوشه‌های رمزنگاری شده و فشرده

در ویندوز XP می‌توانید نام فایل‌ها و پوشه‌های رمزنگاری شده یا فشرده را رنگی کنید (رنگ سبز برای مشخص کردن فایل‌های رمزنگاری شده و رنگ قرمز برای فایل‌های فشرده).

برای انجام این کار مراحل زیر را دنبال کنید:

۱- در پنجره Control Panel روی Folder Options دابل‌کلیک کنید.

۲- در زبانه View گزینه Show encrypted or compressed NTFS files in color را از لیست Advanced settings انتخاب و سپس روی دکمه OK کلیک کنید.



شکل ۱۴-۶

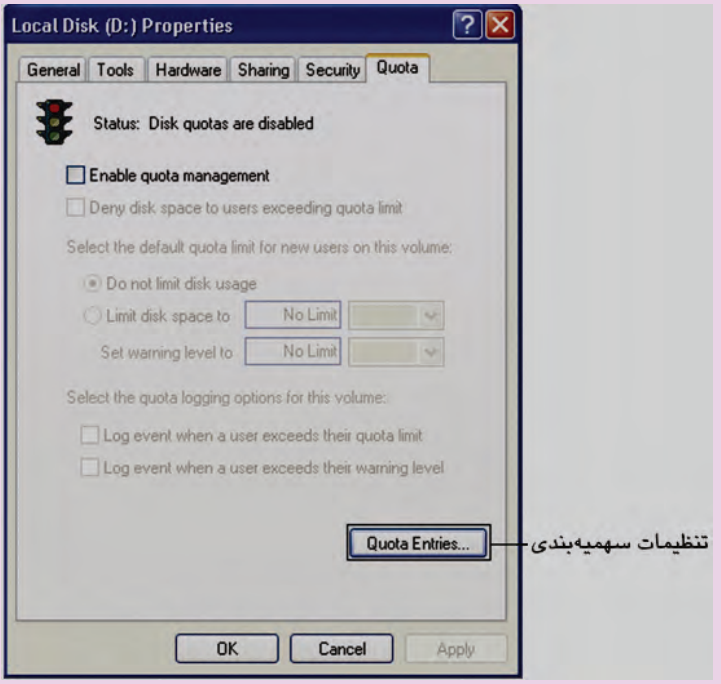
تمرین: خاصیت رنگی شدن فایل و پوشه رمزنگاری شده را غیرفعال کنید.

مطالعه آزاد

یکی از امکانات فایل سیستم NTFS در ویندوز XP تعیین سهمیه استفاده از فضای دیسک در هر درایو برای کاربران مختلف است. برای انجام این کار مراحل زیر را دنبال کنید:

۱- روی درایو موردنظر کلیک راست کرده و گزینه Properties را انتخاب کنید.

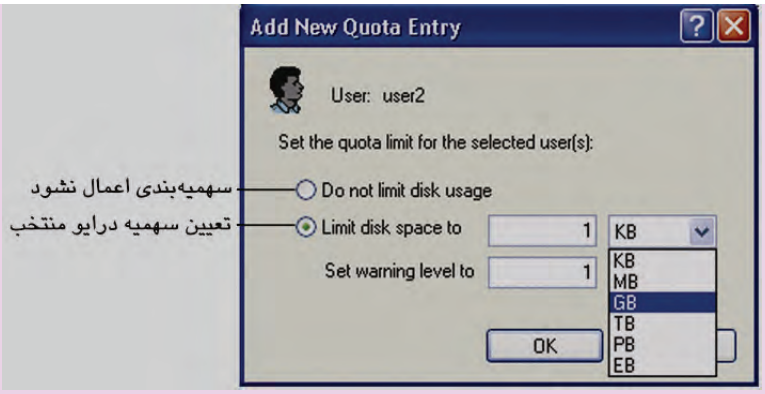
۲- در زبانه Quota مانند شکل ۱۵-۶ روی دکمه ...Quota Entries کلیک کنید تا وارد پنجره Quota Entries For Local Disk شوید.



شکل ۱۵-۶ زبانه **Quota** برای سهمیه‌بندی درایو

۳- از منوی Quota گزینه New Quota Entry... را انتخاب کنید.

۴- در این قسمت پس از تعیین نام کاربر در قسمت Advanced در کادرمحاوره Add New Quota Entry مانند شکل ۱۶-۶ گزینه Limit disk space to را انتخاب کرده و سپس ظرفیت استفاده از درایو را در کادر مقابل آن تعیین و روی دکمه OK کلیک کنید.



شکل ۱۶-۶

Learn in English

NTFS

Short for NT file system, one of the file system for the windows NT operating system (windows NT also supports the FAT file system). NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories and/or individual files. NTFS files are not accessible from other operating systems such as DOS.

واژه‌نامه

Access	دسترسی
Accessible	قابل دسترسی
Compress	فشرده کردن
Directory	دایرکتوری، فهرست
Encryption	رمزنگاری
Failure	اِشکال، خرابی
Feature	خصوصیات
Improve	اصلاح‌کردن
Individual	شخصی
Inheritance	ارث‌بری
Owner	صاحب، مالک
Parent	والدین
Permission	مجوز
Recover	بازیابی
Reliability	قابلیت اطمینان
Security	امنیت
Support	پشتیبانی کردن
Transaction log	آنچه تغییر و تحولات انجام شده در یک پایگاه داده‌ای را ثبت کرده و مبنایی را برای به‌روزرسانی فایل اصلی پایگاه داده و ردیابی کارهای انجام شده در آن فراهم می‌سازد.
Traverse	عبور کردن