گروه آموزشی خرزان

محصولات آموزشی
تخصصی مهندسی شبکه

بر مبنای متد نوین
آموزش غیرحضوری

Microsoft
CERTIFIED
Systems Engineer

Mohammad H.Shirkhodaie
www.modir-shabake.com

www.ParsBook.org

www.modir-shabake.com

معرفی کتاب الکترونیکی

در این کتاب الکترونیکی مختص به دوره آموزشی (Windows XP & 7) قصد داریم به معرفی قابلیتی بپردازیم که با استفاده از آن می توانید امنیت مختص به اطلاعات ذخیره شده بر روی کامپیوتر را به طور چشمگیری افزایش دهید و یکی از دغدغه های اصلی که مربوط به حفظ اطلاعات و جلوگیری از دسترسی غیر مجاز به آنان می باشد را از همین طریق برطرف نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی کتاب الکترونیکی

چنانچه با مفاهیم مختص به اجازه هـای دسترسـی (Permission) آشـنایی داشـته باشـید، می دانید که یکی از راه های حفاظت از اطلاعات استفاده از Permission بر روی فایل ها و فولدرها می باشد، و از این طریق می توان تا حد بسیار زیادی از دسترسی به اطلاعات موجود بر روی کامپیوتر توسط سایر کاربران جلوگیری نمود.

ولی یکی از روش هایی که استفاده از آن به مراتب امنیت بـالاتری را مـی توانـد بـرای شـما فراهم آورد، بحث مختص به رمزگذاری (Encryption) می باشد، با اسـتفاده از ایـن قابلیـت می توانید تمامی اطلاعات موجود بر روی کامپیوتر را به صورت رمزنگاری شده تبدیل کرده و امکان دسترسی به اطلاعات خودتان را توسط سایر افراد به صفر نزدیک نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی کتاب الکترونیکی

در واقع شما می توانید اطلاعات را به طور کامل Encrypt کرده و بر روی هارد دیسک کامپیوتر نگهداری نمایید، در این حالت تنها شخصی که می تواند به محتوای اطلاعات دسترسی داشته باشد فقط خود شما خواهید بود.

حتی اگر یک فرد هکر اقدام به نفوذ به کامپیوتر شما نمایید باز هم فقط با اطلاعاتی مواجه می باشد که رمزگذاری شده اند و عملاً امکان استفاده از اطلاعات شما را نخواهد داشت.

بنابراین استفاده از Encryption یکی از راه های بسیار مفید برای حفاظت از اطلاعات می باشد و شما در زمینه های شخصی و یا حرفه ایی می توانید از آن در سطح وسیعی استفاده نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی کتاب الکترونیکی

ولی باید توجه داشته باشید که استفاده از این ابزار نیازمند شناخت مناسب از عملکرد آن می باشد و شما می بایست دارای دانش استفاده از علم رمزگذاری باشید تا استفاده از آن برای شما بسیار موثر و مفید تر واقع گردد.

در هر صورت در کتاب الکترونیکی پیش رو مختص به آموزش رایگان گروه آموزشی فرزان شما با تمامی مباحث و موارد مربوط به رمزگذاری اطلاعات در ابتدا به صورت از پایه آشنا شده و سپس چگونگی پیاده سازی و استفاده کاربردی از این ابزار در سیستم عامل های Windows XP & Windows 7 را فرا خواهید آموخت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

www.modir-shabake.com

معرفی کتاب الکترونیکی

با توجه به شیوه منحصر به فرد آموزش داده شده، این اطمینان وجود دارد که پس از مطالعه مفاهیم موجود در این کتاب بتوانید به آسانی و با سطح دانش و آگاهی بسیار مطلوبی از راهکار مختص به Encryption برای حفظ و رمزگذاری اطلاعات ارزشمند خودتان استفاده نمایید.

اینکه بتوانید اطلاعات خود را به صورت رمز شده مبدل نمایید و سپس راه های تهیه نسخه پشتیبان از اطلاعات خودتان را بیاموزید و از تمامی نکات و مسائل مختص به Encryption اطلاع پیدا کرده و از آنان به طور کاربردی و مفید استفاده نمایید از اهداف کتاب الکترونیکی پیش رو می باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی کتاب الکترونیکی

مطالعه مفاهیم این کتاب برای تمامی کسانی که می خواهند شرایطی را محیا نمایند تا از اطلاعات ارزشمند خودشان در برابر دسترسی افراد غیر مجاز جلوگیری گردد و همچنین تمامی کاربران عادی و متخصصی که قصد دارند از قابلیت رمزگذاری برای محیط های کاری و یا شخصی استفاده نمایند توصیه می گردد.

با تشکر

گروه آموزشی فرزان خرداد ۱۳۹۰

www.modir-shabake.com

www.ParsBook.org

معرفی کتاب الکترونیکی

برای دریافت جدیدترین کتاب های الکترونیکی منتشر شده توسط گـروه آموزشـی فـرزان بـه آدرس زیر مراجعه نمایید:

www.Modir-Shabake.com

www.ParsBook.org

WWW.SOFTGOZAR.COM

فهرست مطالب

قسمت اول: آشنایی با NTFS Encryption مفاهیم پایه

قسمت دوم: چگونگی استفاده و پیاده سازی NTFS Encryption در Windows XP

قسمت سوم: آشنایی با Recover Agent در Workgroup

قسمت چهارم: چگونگی استفاده و پیاده سازی NTFS Encryption در Windows 7

قسمت پنجم: غیرفعال نمودن قابلیت EFS در Domain & Workgroup تحت Windows XP & 7

www.ParsBook.org

WWW.SOFTGOZAR.COM

قسمت اول:

آشنایی با

NTFS Encryption

مفاهیم پایه

www.ParsBook.org

معرفی درس

بعنوان یکی از Features های مختص به NTFS Partition قصد داریم در ایـن درس بـا قابلیت Encryption آشنا شویم، در قسمت اول از این مبحث با مقدمات مفاهیم رمزگـذاری آشنا خواهید گشت و در درس بعدی به پیاده سازی مفاهیم فـوق خـواهیم پرداخـت، در درس پیش رو به طور مقدماتی و تحت مدل شبکه ایـی Workgroup بـا رمزگـذاری و Encrypt نمودن اطلاعات آشنا خواهید گشت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

آشنایی با رمزنگاری (Cryptography)

یکی از مفاهیمی که امروزه بسیار مورد توجه قرار گرفته است و لزوم استفاده از آن برای تمامی کاربران و متخصصان ضروری شده است، بحث مختص به مدیریت دسترسی افراد به دیتا می باشد که با استفاده از مکانیسم های متعددی قابل پیاده سازی می باشد، اعمال مواردی همچون مدیریت login کاربران به سیستم، مدیریت دسترسی کاربران به منابع کامپیوتر و ... نمونه هایی از این موارد هستند.

www.ParsBook.org

WWW.SOFTGOZAR.COM

آشنایی با رمزنگاری (Cryptography)

بعنوان مثال،

با یک نمونه بسیار قوی و مناسب تحت عنوان Permission در درس های قبل (از دوره آموزشی Windows XP & Windows 7) آشنا شده اید، ولی ممکن است اطلاعات به صورت فیزیکی مورد سرقت و دسترسی قرار گیرند، در این حالت روش هایی که در شبکه مورد پیاده سازی قرار می گیرد نمی تواند جلوی دسترسی غیر مجاز به اطلاعات را بگیرد.

چرا که با استفاده از اجازه های دسترسی می توانید مدیریت دسترسی کاربران را به منابع Share شده و یا منابعی که به صورت Local بر روی کامپیوتر قرار دارند مدیریت نمایید، مثلاً اجازه دهیدکه یکسری از کاربران به بعضی از فایل ها دسترسی داشته باشند و یکسری از اعمال را بر روی آنان انجام دهند.

www.ParsBook.org

WWW.SOFTGOZAR.COM

آشنایی با رمزنگاری (Cryptography)

بنابراین می بایست از متد و روشی استفاده گردد که یک لایه امنیتی بر روی خود دیتا ایجاد گردد که در واقع دیتا را به تنهایی و در همه حال امن و غیر قابل دسترس نمایید، فرض نمایید که یک دیتا به سرقت رفته و در صورتی که اصول محرمانگی (Confidentiality) بر روی آن فایل اعمال نشده باشد در این حالت ممکن است به راحتی در دسترس افراد غیر مجاز قرار گیرد، منظور از این محرمانگی به عدم امکان دسترسی به محتوای دیتا بر می گردد.

ولی می توان دیتا و به طور کلی اطلاعات را با استفاده از مکانیسم ها و روش های مختلف دیگری به صورت محرمانه (Confidential) درآورد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

آشنایی با رمزنگاری (Cryptography)

علم Cryptography در لغت به معنای رمز نگاری می باشد، علم رمزنگاری در واقع بر همین اساس و برای جلوگیری از دسترسی غیر مجاز به محتوای دیتا و بر پایه الگوریتم های پیچیده ریاضی ابداع شده است، اگر نگاهی گذرا به تاریخچه علم Cryptography داشته باشیم متوجه می شویم که نیازهای نظامی در ایجاد و پیشرفت این علم بسیار موثر بوده است.

ریشه لغت Cryptography از یونان می باشد و به معنای نوشتن به صورت پنهانی می باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

آشنایی با مفاهیم رمزنگاری

استفاده از دو مفهوم در علم Cryptography بسیار کاربردی و حائز اهمیت می باشد:

- **Encryption**
- **Decryption**

رمزگذاری و رمزگشایی را می توان دو مفهوم بسیار مهم و کاربردی در مباحث Cryptography دانست، هر نوع دیتا و اطلاعاتی در فرمت اولیه و ساده خود در این علم اصطلاحاً Plain نامیده می شود، در واقع دیتا و اطلاعات در شرایط نرمال در حالت واضح، آشکار، ساده قرار دارند بنابراین به این فرمت اصطلاحاً Plain Text گفته می شد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

آشنایی با مفاهیم رمزنگاری

یکی از اصلی ترین رسالت های ایجاد علم رمزنگاری ابداع و به کارگیری روش هایی است که بر اساس آن بتوان فرمت Plain Text از اطلاعات را به فرمتی رمز آلود و سری تبدیل نمـود، برای همین اساس مفهوم دیگری تحت لغت Cipher ابداع شده است. (که در لغت به معنـای رمز و ِسری شده نمی باشد)

براساس این مفهوم می توان اطلاعات و دیتا را که به فرمت Plain Text می باشد به فرمـت Cipher تبدیل نمود.

www.ParsBook.org

WWW.SOFTGOZAR.COM

آشنایی با مفاهیم رمزنگاری

در تعریف Cipher می توان گفت:

به روشی برای تبدیل plain text به صورتی که معنای آن پنهان باشد cipher گفته می‌شود، به بیان بسیار ساده قرار است اطلاعات از فرمت ساده و روشن که به صورت نرمال دارای آن می باشند به فرمتی رمزی و پیچیده تغییر فرم دهند، به این ترتیب در هر صورتی که در دسترس افراد غیر مجاز قرار گیرند خاصیت محرمانگی آنان حفظ می گردد، حتی اگر اطلاعات به صورت فیزیکی هم در دسترس قرار گیرند (مثلاً هارد دیسک به سرقت رود)، در این حالت باز هم فرد سارق با اطلاعات رمزگذاری شده روبه رو خواهد گشت، و عملاً امکان استفاده از دیتای سرقت شده را نخواهد داشت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی Encryption

در این متد اطلاعات را کدگذاری کرده تا از دسترسی افراد به آن جلوگیری گردد.

زمانی که دیتا و اطلاعات رمز می شود:

یعنی Encrypt می گردد به صورتی در خواهد آمد که تا زمان Decrypt شـدن بـی معنـی و غیر قابل استفاده می باشند، به طور مشخص Encryption بر مبنای دو متد و روش می تواند صورت گیرد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی Encryption

دو متد مورد نظر عبارتند از:

- **Symmetric**
- **Asymmetric**

روش نخست (Symmetric) بنام کد گذاری با کلید های متقارن شناخته می شود.

روش دوم (Asymmetric) بنام کد گذاری با کلید های نامتقارن شناخته می شود.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی Encryption

در رمزگذاری اطلاعات از کلید هایی استفاده می شود که با استفاده از آنان و بر اساس یکسری الگوریتم های ریاضی بتوان اقدام به رمزگذاری و رمز گشایی دیتا و اطلاعات نمود.

این کلید ها دو دسته می باشند که شامل:

- **Public Key**
- **Private Key**

کلید های عمومی و کلید خصوصی نامیده می شوند.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی Encryption

با استفاده از این کلید ها دیتا به صورت کد گذاری شده (Encrypt) و بـه صـورت رمزگشـایی شده Decrypt در می آید، در متدها و روش های مختص به متقارن و نامتقارن از کلید هـای فوق (Public or Private) استفاده می گردد.

در تعریف کلید ها می توان گفت:

به اطلاعات و الگوریتم هایی که با استفاده از آنان بتـوان Plain text را بـه Cipher text و بلعکس تبدیل کرد کلید گفته می شود.

www.ParsBook.org

WWW.SOFTGOZAR.COM

روش Symmetric

در روش Symmetric و یا متقارن از یک کلید برای Encrypt & Decrypt نمودن دیتا استفاده می گردد.

بعنوان مثال،

در این روش برای باز و بسته کردن یک در از یک کلید استفاده می گردد.

کلید مورد استفاده در این متد Public Key می باشد، در واقع کلید ها با هم متقارن می باشند و از همان کلیدی که برای رمزگذاری دیتا استفاده می شود از همان کلید برای رمزگشایی نیز استفاده می گردد.

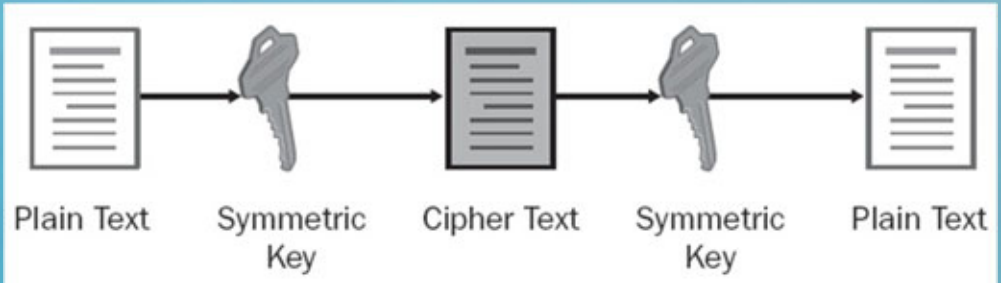
www.ParsBook.org

WWW.SOFTGOZAR.COM

روش Symmetric

در شکل مشاهده می نمایید که دیتا اولیه به صورت Plain Text می باشد که با استفاده از یک Symmetric Key رمزگذاری شده (Cipher Text) می گردد و کامپیوتر اول همان کلید را که استفاده کرده برای کامپیوتر دوم می فرستد.

کامپیوتر مقصد نیز با استفاده از همان کلید مجدداً اقدام به رمز گشایی به فرمت Plain Text می نمایید.



www.ParsBook.org

روش Symmetric

امنیت الگوریتم های مبتنی بر Symmetric خیلی نمی توانند بالا باشند ولی دارای سرعت مناسبی در انجام اعمال Encrypt نمودن اطلاعات می باشند، در بیشتر مواقع از این متد در نقل و انتقال اطلاعات استفاده می گردد، یکسری از الگوریتم های امنیتی زیر با متد کلید های متقارن کار می نمایند، از قبیل:

- **DES, 3DES, AES,...**

www.ParsBook.org

WWW.SOFTGOZAR.COM

روش Asymmetric

در این متد از هر دو کلید Public & Private برای رمزگذاری و رمز گشایی دیتا استفاده می گردد، در این روش از یک کلید برای رمزگذاری و از یک دیگر برای رمزگشایی استفاده می شود، در واقع در این روش از کلید هایی استفاده می نمایید که نامتقارن می باشند، برای درک بهتر از عملکرد این متد به مثالی در همین رابطه توجه نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

روش Asymmetric

فرض نمایید دو کامپیوتر تحت عنوان فرستنده و گیرنده وجود دارند، در این حالت کامپیوتر فرستنده با استفاده از Public Key کامپیوتر گیرنده اقدام به رمزگذاری دیتا می نمایید، سپس دیتا را برای کامپیوتر گیرنده ارسال می نمایید، در ادامه کامپیوتر گیرنده با استفاده از Private Key که مختص به خودش است اقدام به رمزگشایی دیتا می نمایید.

بنابراین کامپیوتر فرستنده فقط دارای Public Key کامپیوتر گیرنده می باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

روش Asymmetric

نکته جالب توجه در مثال این می باشد،

که با توجه به Encrypt شدن دیتا با استفاده از Public Key کامپیوتر گیرنده، فقط همین کامپیوتر (یعنی کامپیوتر گیرنده) می تواند دیتا را Decrypt نمایید، چرا که کلید مختص به Private Key را فقط خودش دارا می باشد.

www.ParsBook.org

روش Asymmetric

پس می توان گفت حتی کامپیوتر فرستنده که خودش دیتا را Encrypt کرده است هم نمی تواند اقدام به Decrypt کردن دیتا نمایید!!!

در دوره های آموزشی مختص به امنیت (Security) از محصولات فرزان با مفاهیم فوق به طور کامل آشنا خواهید گشت.

www.ParsBook.org

فرزان

معرفی EFS

در سیستم عامل ویندوز نیز یکی از روش هایی که بر اساس آن می توان اقـدام بـه Encrypt نمودن اطلاعات نمود مختص به روش EFS می باشـد، کـارکرد EFS در مـدل شـبکه ایـی Workgroup بسیار ساده و دارای مفاهیم قابل فهم و راحتی می باشد، ولـی کـارکرد و پیـاده سازی استفاده از EFS در محیط شبکه ایی دامین نیازمند یادگیری و شناخت مفاهیم متعـددی از جمله PKI و Certificateها می باشد.

در دوره آموزشی Windows XP و یا Windows 7 که مفـاهیم کتـاب الکترونیکـی فـوق مربوط به آنان می باشد، به طور کامل اقدام به بررسی و استفاده از EFS تحت مدل شبکه ایی Workgroup و کامپیوترها به صورت Local خواهیم نمود.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی EFS

پیاده سازی مفاهیم تخصصی مختص به EFS در دامین را به دوره های آتی واگذار می نمایم، ولی چگونگی استفاده و Encrypt نمودن دیتا را توسط کاربران در محیط دامین در دوره آموزشی Server 2003 or 2008 مورد بررسی قرار خواهیم داد.

در درس بعدی به پیاده سازی مفاهیم فوق و بررسی شرایط مختلف مختص به آن خواهیم پرداخت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

قسمت دوم:

چگونگی استفاده و پیاده سازی NTFS Encryption در Windows XP

www.ParsBook.org

معرفی درس

در ادامه مبحث درس قبل به بررسی شرایط مختص به پیاده سازی استفاده از قابلیت EFS در محیط های شبکه ایی Workgroup خواهیم پرداخت، همچنین در انتهای قسمت دوم از درس فوق به بررسی عملی موارد گفته شده خواهیم پرداخت.

در این درس به بررسی شرایط استفاده و پیاده سازی قابلیت فوق تحت سیستم عامل Windows XP خواهیم پرداخت و در درس های بعدی به بررسی این قابلیت در Windows 7 خواهیم پرداخت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی EFS

EFS مخفف Encryption File System می باشد و در مدل شبکه ایی Workgroup بر روی هر کامپیوتر به صورت مجزا قابل پیاده سازی می باشد، کاربرانی که از یک کامپیوتر مثلاً سیستم عامل Windows XP استفاده می نمایند، می توانند فایل ها خود را به سادگی به صورت Encrypt شده در آورند، برای این منظور می بایست چک مارک گزینه مختص به Encryption را انتخاب نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

پیاده سازی EFS

در شکل زیر نمایی از گزینه مختص به Encryption را مشاهده می نمایید:

بر روی تمامی فایل ها و فولدرها می توانید با گرفتن Properties و سپس وارد شدن به قسمت Advanced چک مارک گزینه فوق را انتخاب نمایید، فقط باید توجه داشته باشید که EFS از جمله توانمندی های مختص به NTFS File System می باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

پیاده سازی EFS

بنابراین پارتیشن های شما حتماً می بایست از نوع NTFS باشد تا فایل ها و فولدرهای داخل آن را بتوانید Encrypt نمایید، فایل ها و فولدرهایی که در ویندوز XP به صورت Encrypted شده درآمده اند دارای رنگ سبز می باشند:

www.ParsBook.org

WWW.SOFTGOZAR.COM

پیاده سازی EFS

توجه نمایید که در یک زمان یک فایل و یا فولدر را نمی توانید به صورت های Compress & Encrypted تبدیل نمایید، بلکه می بایست تنها یکی از دو گزینه فوق را در یک زمان انتخاب نمایید، با استفاده از دستور Cipher و Command Prompt هم می توانید اقدام به Encrypt نمودن دیتا نمایید.

برای این منظور می بایست از دستور Cipher به همراه سویچ های زیر استفاده نمایید:

- **/E**
- **/D**

سویچ مختص به /e برای Encrypt نمودن و سویچ مختص به /d برای Decrypt نمودن دیتا استفاده می گردد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

پیاده سازی EFS

سویچ مختص به F/ برای Force و اجبار بر روی تمامی فایل ها و فولدرهایی که حتی قبلاً ممکن است Encrypt شده باشند استفاده می گردد

(در این حالت آنهایی که از قبل Encrypt شده باشند Skip می شودند)

- **/F**

www.ParsBook.org

WWW.SOFTGOZAR.COM

پیاده سازی EFS

اگر دستور Cipher را به صورت خالی و بدون سویچ اجرا نمایید وضعیت مختص به فایل ها و فولدرهایی را که دستور در آن قرار دارد از لحاظ Encrypt بودن نمایش می دهد:

در شکل مشاهده می نمایید که فولدر Data در E: به صورت Encrypt می باشد.

```
C:\WINDOWS\system32\cmd.exe

E:\Data>cipher

 Listing E:\Data\
 New files added to this directory will be encrypted.
```

در شکل زیر نیز مشاهده می نمایید که فولدر Data با سویچ /d به صورت Decrypt درآمده است.

```
E:\>cipher e:\data /d

 Decrypting directories in e:\

Data [OK]

1 directorie(s) within 1 directorie(s) were decrypted.
```

www.ParsBook.org

WWW.SOFTGOZAR.COM

نقل و انتقال EFS

بعد از آنکه دیتا خودتان را به صورت Encrypt درآوردید تمامی کاربرانی که بر روی کامپیوتر دارای حساب کاربری می باشند امکان مشاهده محتویات دیتای شما را نخواهند داشت، پیغامی را که در شکل مشاهده می نمایید زمانی است که کاربر دیگری می خواهدمحتویات یک فایل Notepad را که Encrypt شد است را مشاهده نمایید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

نقل و انتقال EFS

همچنین کاربران دیگر نمی توانند فایل های Encrypted شده شما را Move or Copy نمایند، ولی باید توجه داشته باشید که فایل های Encrypted شده از Delete شدن توسط سایر کاربران درامان نمی باشد!!!

www.ParsBook.org

WWW.SOFTGOZAR.COM

استفاده از فایل های EFS

فرض نمایید دو کاربر بر روی یک کامپیوتر (Windows XP) تعریف شده اند، هر دو کاربر فوق عضو گروه Administrators می باشند.

یکی از کاربران فایل های خود را در :C به صورت Encrypt شده درآورده است در این حالت کاربر دیگر نمی تواند محتوای فایل های فوق را مشاهده نمایید و یا آنها را Move و یا Copy نمایید ولی می تواند فایل های فوق را Delete نمایید!!!

www.ParsBook.org

WWW.SOFTGOZAR.COM

استفاده از فایل های EFS

دلیل این امر به دارا بودن اجازه دسترسی Full Control است که به گروه Administrators به صورت پیش فرض به تمامی فایل ها و فولدرها بـر روی کـامپیوتر داده شـده اسـت، بـرای برطرف نمودن این مشکل در زمان ایجاد فایل ها و فولدرها بر روی کـامپیوتری کـه دارای دو Administrator می باشد می بایست گروه Administrators را از ACL لیست و Owner فایل ها و فولدرهایی که ایجاد کرده اید حذف نمایید.

با انجام عمل گفته شده در صفحه قبل، با Encrypt نمودن فایل ها و فولدرهای هیچ کاربری امکان مشاهده و یا Delete نمودن آنان را نخواهد داشت. (حتـی کـاربرانی کـه عضـو گـروه Administrators می باشند.)

www.ParsBook.org

WWW.SOFTGOZAR.COM

استفاده از فایل های EFS

باید توجه نمایید که کاربرانی که عضو گروه Users می باشند و در واقع کاربرانی محدود تلقی می شوند این کاربران نیز می توانند دیتا هایی را که خودشان ایجاد کرده اند را Encrypt نمایند، در این حالت حتی Administrator هم نمی تواند محتویات دیتا های رمزگذاری شده کاربران فوق را مشاهده نمایید!!!

ولی کماکان امکان Delete نمودن دیتا های کاربران محدود توسط Administrator وجود خواهد داشت!!!

www.ParsBook.org

WWW.SOFTGOZAR.COM

استفاده از فایل های EFS

بنابراین در صورتی که یک فایل Encrypt گردد به جز کاربری که آن را Encrypt نموده است هیچ کاربر دیگری نمی تواند به محتوای آن دسترسی داشته باشد، دسترسی و مشاهده محتویات یک فایل Encrypt شده به هیچ وجه حتی با داشتن Full Control Permission به آن فایل نیز میسر نخواهد بود.

در نتیجه مبحث مختص به Encrypt شدن یک فایل از مبحث اجازه دسترسی (Permission) داشتن به آن فایل متفاوت می باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

مثال

کاربر محدودی که عضو گروه Users می باشد یک فایل را در :C به صورت Encrypt شده درآورده است.

Administrator با حساب کاربری خود به همین کامپیوتر Login می نمایید در این حالت اعمالی که وی می تواند بر روی فایل رمزگذاری شده فوق انجام دهد را توضیح دهید؟

در جواب باید گفت:

Administrator نمی تواند فایل فوق را Open, Move, Copy نمایید و فقط می تواند فایل را Delete نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

موارد امنیتی EFS

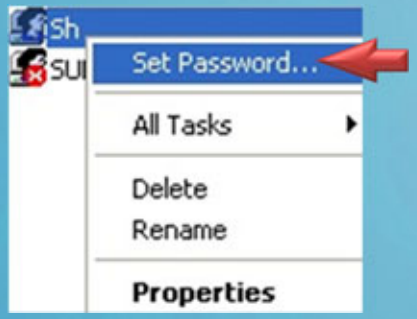
یکی از موارد مهم امنیتی که باعث ارتقای امنیت اطلاعات Encrypt شده می گردد مختص به عدم امکان مشاهده فایل های Encrypt شده توسط هکرها و افراد نفوذگر می باشد، همان طور که گفته شده فقط کاربری که دیتا را رمزگذاری کرده است می تواند دیتا خودش را مشاهده نمایید، در این حالت ممکن است یک فرد نفوذگر بتواند پسورد یک کاربر را Reset نمایید و با استفاده از نام کاربری وی وارد ویندوز گردد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

موارد امنیتی EFS

در چنین شرایطی که پسورد یک کاربر بنا به هر دلیلی Reset گردد، مثلاً به وسیله Administrator و با استفاده از کنسول Computer Manager:



و یا یک هکر اقدام به شکستن پسورد کاربر و Reset نمودن آن نمایید، در هر دو حالت فوق فایل هایی که به صورت Encrypt شده بر روی کامپیوتر مربوط به کاربر مورد نظر هستند به هیچ وجه امکان مشاهده را نخواهند داشت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

موارد امنیتی EFS

تنها را مشاهده مجدد فایل های رمزگذاری شده استفاده از همان پسورد قبلی کاربری می باشد که Account وی را Reset Password کرده اید، در این شرایط باید گفت اگر کاربر پسورد خود را فراموش کرده است و مجبور به Reset نمودن پسورد خود شده است، و یا Administrator سازمان به خاطر ترک نمودن کاربر از سازمان پسورد وی را Reset کرده باشد.

در تمامی موارد فوق می بایست برای همیشه با فایل های Encrypt شده مختص به کاربر مورد نظر خداحافظی نمایید!!!

www.ParsBook.org

WWW.SOFTGOZAR.COM

موارد امنیتی EFS

ولـــی ممکـــن اســـت شـــما بعنـــوان Administrator یـــک کـــاربر را از لیســـت Local Users & Group پاک نمایید، قبل از آنکه از وجود فایل های Encrypt شده توسط کاربر فوق اطلاع داشته باشید، در ایـن حالـت اگـر بـاز هـم کـاربری را کـه Account آن را Delete کرده اید به همان نام قبلی و با همان پسورد قبلی عیناً بسازید باز هـم مشـکل عـدم مشاهده و امکان دسترسی به فایل های Encrypt شده آن کاربر به قوت خـود بـاقی خواهـد ماند.

www.ParsBook.org

WWW.SOFTGOZAR.COM

موارد امنیتی EFS

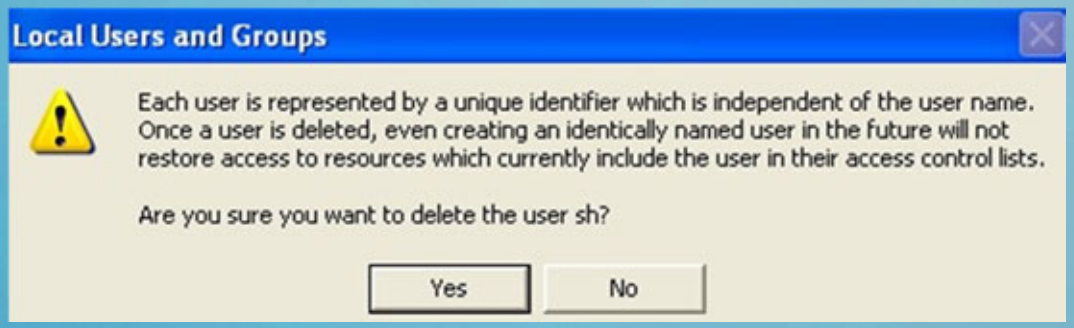
دلیل این امر به Unique بودن SID هر User Account بر می گردد، بنابراین می بایست در صورتی که فایل های Encrypt شده ایی بر روی کامپیوتر دارید به تمامی این شرایط و موارد امنیتی مختص به آن توجه داشته باشید، در زمان پاک کردن یک کاربر از دیتابیس کامپیوتر (SAM) نیز با پیغامی مبنی بر unique بودن SID هر User مواجه خواهید گشت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

موارد امنیتی EFS

در این پیغام به شما گفته می شود که در صورت Delete شدن یک کاربر مشخصات مختص به SID آن نیز پاک می شود و دیگر دسترسی به منابع کامپیوتر حتی در صورت ایجاد به همان نام قبلی میسر نخواهد بود:



www.ParsBook.org

WWW.SOFTGOZAR.COM

موارد امنیتی EFS

بنابراین در صورت دارا بودن دیتا به صورت Encrypt شده بر روی کامپیوتر می بایست بسیار توجه نمایید که Account کاربران Delete و یا Reset Password نگردند، در این شرایط نگه داری از سیستم عامل نیز بسیار مهم است چرا که کاربران بر روی Windows XP تعریف شده اند و باید مواظب خرابی این ویندوز نیز باشید!!!

www.ParsBook.org

WWW.SOFTGOZAR.COM

تهیه Backup از فایل های Encrypt شده

یک کاربر میتواند از اطلاعات و دیتا که خودش آنان را Encrypt کرده است یک Backup تهیه نمایید، در زمان Restore نمودن Backup فوق فایل به صورت همان حالت Encrypt شده بازیابی می گردد، توجه داشته باشید که Administrator می تواند فایل ها و فولدرهایی را که خود کاربران از آنان Backup گرفته اند را Restore نمایید.

ولی در هر حال بعد از Restore نمودن آنان باز هم به واسطه ماهیت Encrypt بودن این فایل ها و فولدرها Administrator نمی تواند به آنان دسترسی داشته باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تهیه Backup از فایل های Encrypt شده

بنابراین یک کاربر از فایل های خود Backup گرفته است (از فایل های Encrypt شده) سپس فایل Backup گرفته شده را به Administrator داده است، Admin هم اقدام به Restore کردن فایل ها کرده است، در نهایت باز هم به جز کاربر اولیه هیچ شخص دیگری نمی تواند به دیتا دسترسی داشته باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تهیه Copy از فایل های Encrypt شده

ممکن است کاربر بخواهد از اطلاعات و دیتا که خودش آنـان را Encrypt کـرده اسـت یـک کپی بر روی (CD, DVD, USB Flash) تهیه نمایید، در این حالـت بایـد توجـه نماییـد در صورت Copy و سپس Paste نمودن اطلاعات بر روی تجهیزات Removable Media و یا CDRW دیتا از حالت Encrypted شده خارج می گردد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تهیه Copy از فایل های Encrypt شده

فقط در دو صورت اطلاعات Encrypted شده را می توانید جابه جا نمایید و خاصیت Encrypt فایل های فوق نیز باقی بماند، روش نخست تهیه نسخه پشتیبان از فایل های Encrypt شده می باشد و سپس Copy نمودن فایل های فوق به تمامی External Storage Device ها از قبیل،(USB Flash, CD, DVD)

روش دوم کپی فایل های فوق بر روی External Hard Disk که برای سیستم عامل به منزله یک هارد دیسک تلقی می گردد، چنانچه بخواهید فایل های Encrypt شده خود را مستقیماً کپی نمایید می توانید این کار را با استفاده از هاردهای External انجام دهید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

بررسی مشکل استفاده از فایل های رمزگذاری شده

در هر صورت چه فایل های Encrypt شده را Backup گرفته و یا مستقیماً بر روی هارد دیسک External کپی نمایید، در هر دو حالت فوق فقط کاربری که فایل های فوق را Encrypt کرده است و فقط بر روی کامپیوتر و سیستم عاملی که این کار را انجام داده است می تواند به فایل های فوق دسترسی داشته باشد.

برای درک بهتر از موضوع به مثالی در همین رابطه در صفحه بعد توجه نمایید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

بررسی مشکل استفاده از فایل های رمزگذاری شده

فرض نمایید که کاربری از اطلاعات Encrypt شده خود یک نسخه Backup و یا Copy تهیه نموده است، سپس بنا به دلایلی سیستم عامل ویندوزی که کاربر فوق با آن کار می کرده است یک بار نصب مجدد شده است، در این حالت کاربر در زمانی که مجدداً فایل های Encrypt شده خود را از روی External Hard Disk و یا Backup های موجود مورد استفاده قرار می دهد، با پیغام Access is Denied مواجه می گردد و امکان باز نمودن این فایل ها برای وی به هیچ وجه وجود نخواهد داشت.

دلیل این موضوع به Private Key بر می گردد که هر کاربر مختص به خود دارد، در واقع دیتا های رمزگذاری شده فقط به وسیله کلید مختص به هر کاربر امکان Decrypt و رمز گشایی شدن را خواهند داشت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

بررسی مشکل استفاده از فایل های رمزگذاری شده

بنابراین می بایست از Private Key کاربری که اقدام به Encrypt نمودن دیتا های خود کرده است یک Backup و پشتیبان تهیه نمایید، تا در صورتی که به هر دلیل نرم افزاری و یا سخت افزاری مجبور به تعویض سیستم عامل و یا پاک کردن Account کاربر و یا Reset Password نمودن حساب کاربری آن شوید، و یا حتی اگر بخواهید دیتا Encrypt شده یک کاربر را از یک کامپیوتر به کامپیوتر دیگری و برای کاربر دیگری منتقل نمایید.

در همه این موارد از Private Key کاربری که قبلاً آن را Export کرده اید استفاده نمایید، به این ترتیب ریسک موجود برای از بین رفتن اطلاعات نزدیک به صفر درصد می شود!!!

www.ParsBook.org

WWW.SOFTGOZAR.COM

Export نمودن Private Key

برای این منظور می بایست اقدام به Export نمودن Private Key کاربر از کامپیوتر نمایید، راه های متعددی برای انجام عمل فوق وجود دارد که در این درس به بررسی چند نمونه از آنان خواهیم پرداخت.

نخستین راه حل برای Export نمودن استفاده از دستور Cipher می باشد، برای این منظور می بایست از دستور Cipher به همراه سویچ /R استفاده نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Export نمودن Private Key

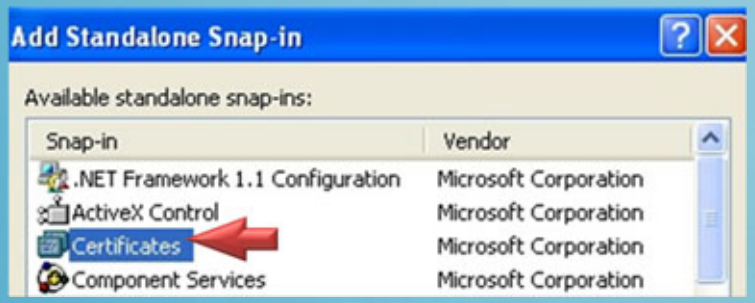
همچنین می توانید طریق MMC Certificates Console اقدام به Export نمودن Private Key کاربر نمایید، نخست می بایست با Account کاربری که قصد دارید Private Key آن را Export نمایید Login کرده و سپس وارد کنسول MMC شوید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Export نمودن Private Key

برای این منظور وارد کنسول MMC شده و سپس Certificates Snap-in را Add نمایید:



در ادامه گزینه My User Account را انتخاب نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Export نمودن Private Key

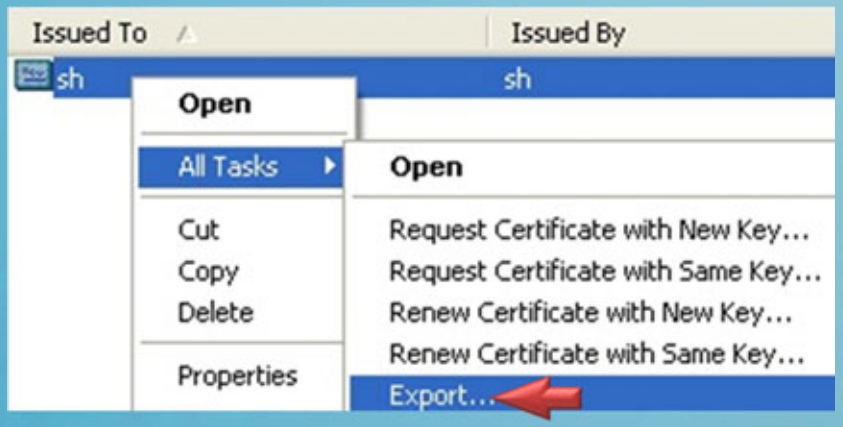
باید توجه داشته باشید که برای استفاده از روش فوق می بایست حداقل یک فایل بـه صـورت Encrypt شده توسط کابری که می خواهیـد Private Key آن را Export نماییـد بـر روی سیستم از قبل وجود داشته باشد، در ادامه وارد قسمت Personal Certificates شوید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Export نمودن Private Key

سپس بر روی Certificate که بنام کاربری که Login کـرده اسـت راسـت کلیـک کـرده و گزینه Export را انتخاب نمایید.



www.ParsBook.org

WWW.SOFTGOZAR.COM

Export نمودن Private Key

در ادامه می بایست یک Wizard را تکمیل نموده که در انتهای آن یک فایل با پسوند PFX مختص به Private Key ایجاد خواهد گشت:

فقط باید توجه داشته باشید که در طول پروسه Wizard حتماً می بایست گزینه Yes, export the private key را نیز انتخاب نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Import نمودن Private Key

فرض نمایید که از Data که Encrypt شده است Backup و یا Copy تهیه کرده اید و در مکان امنی آنها را نگه داری کرده اید، در این شرایط هارد دیسک کامپیوتر دچار مشکل خرابی می گردد و تمامی دیتا رمزگذاری شده به همراه سیستم عامل و کاربران تعریف شده در آن همگی از بین می روند، در این حالت شما نیز به انجام Disaster Recovery خواهیم داشت، در صفحه بعد به چگونگی انجام پروسه فوق خواهیم پرداخت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Import نمودن Private Key

برای رفع مشکل به وجود آمده می بایست یک بار دیگر سیستم عامل جدیدی را نصب نمایید (نوع و نگارش می تواند متفاوت با ویندوز قبلی باشد)، در ادامه می بایست با نام کاربری جدیدی که تعریف کرده اید (می تواند هم نام کاربر قبلی باشد و یا نام دیگری داشته باشد) به ویندوز جدید login نمایید.

سپس مجدداً وارد MMC شده و Certificates Snap-in را باز نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Import نمودن Private Key

وارد قسمت Personal Certificates شوید و با راست کلیک گزینه Import را انتخاب نمایید، در شکل زیر نمایی از وارد نمودن (import) شدن Private Key مختص به کاربر که در مرحله قبل کلید آن را Export کرده اید را مشاهده می نمایید:

در ادامه Wizard را دنبال کرده و مسیر مختص به فایلی را که قبلاً Export کرده اید را مشخص نموده و مراحل وارد نمودن کلید را کامل نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

نکته

در صورتی که بخواهید دیتا هایی را که یک کاربر به صورت Encrypt شده در آورده است را در کامپیوتر کاربر دیگری مشاهده نمایید، می بایست همین مراحل مختص به Import نمودن Private Key را بر روی کامپیوتر کاربران دیگر دنبال نمایید، ولی ممکن است بخواهید بر روی یک کامپیوتر که مثلاً دارای دو کاربر می باشد دیتا Encrypt شده یکی از کاربران را کاربر دیگر بتواند مشاهده نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

نکته

در این صورت تنها کافی است ابتدا با کـاربرل کـه دارای دیتـا Encrypt شـده اسـت Login نمایید و سپس کلید این کاربر را Export نمایید، در ادامه با کاربر دیگر Login نموده و اقدام به Import نمودن کلیدی مختص به کاربر اول نمایید، در اینصورت کاربر دوم هم می تواند به محتویات دیتا کاربر اولی که اطلاعات خود را Encrypt نموده است دسترسی داشته باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

اجازه دسترسی سایر کاربران به فایل های Encrypt شده

یکی از مواردی که ممکن است بخواهید بر روی یک کامپیوتر که همزمان چندین کاربر از آن استفاده می نمایند پیاده سازی نمایید، مختص به اجازه دسترسی سایر کاربران به فایل های Encrypt شده می باشد.

فرض نمایید بر روی یک کامپیوتر هر کاربر فایل های خود را رمزگذاری کرده است در این حالت ممکن است یکی از کاربران بخواهد به چندین کاربر دیگر اجازه دسترسی به فایل های رمز شده خودش را بدهد.

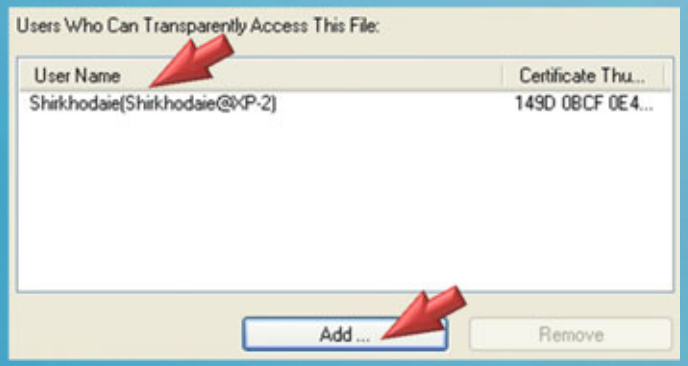
www.ParsBook.org

WWW.SOFTGOZAR.COM

اجازه دسترسی سایر کاربران به فایل های Encrypt شده

در این حالت می بایست از گزینه Details استفاده کرده و Certificate سایر کاربران را نیز در لیست افراد مجاز قرار دهید، برای این منظور در همان قسمت خواص های پیشرفته فایل بر روی گزینه Details کلیک نمایید:

در این قسمت لیستی از نام کـاربرانی را مشـاهده می نمایید که می توانند بـه محتـوای Encrypt شده فایل فوق دسترسی پیدا نمایید، برای اضـافه کردن سایر کاربران بر روی Add کلیک نمایید:

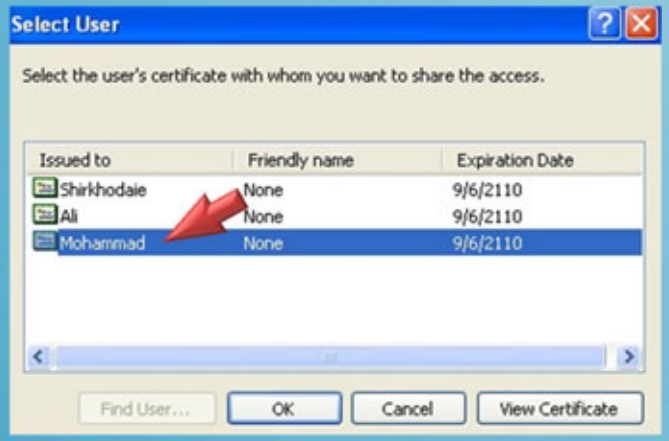


www.ParsBook.org

WWW.SOFTGOZAR.COM

اجازه دسترسی سایر کاربران به فایل های Encrypt شده

بعد از کلیک بر روی Add از لیست نمایش داده شده کاربران و یا کاربر مورد نظر را که می خواهید به فایل رمز شده شما دسترسی داشته باشد را انتخاب نمایید:



با انتخاب کاربر Mohammad وی می تواند به فایل که کاربر Shirkhodaie آن را Encrypt کرده است دسترسی داشته باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

اجازه دسترسی سایر کاربران به فایل های Encrypt شده

باید توجه داشته باشید که کاربر Mohammad در این مثال فقط به همان یک فایلی که کاربر Shirkhodaie به وی اجازه داده است می تواند دسترسی داشته و به سایر فایل های رمز شده کاربر Shirkhodaie دسترسی نخواهد داشت، بنابراین این روش Per File or Folder عمل می نمایید و باید برای هر کدام از فایل ها و یا فولدرهایی که رمز شده است دسترسی به سایر کاربران اعطا نمایید.

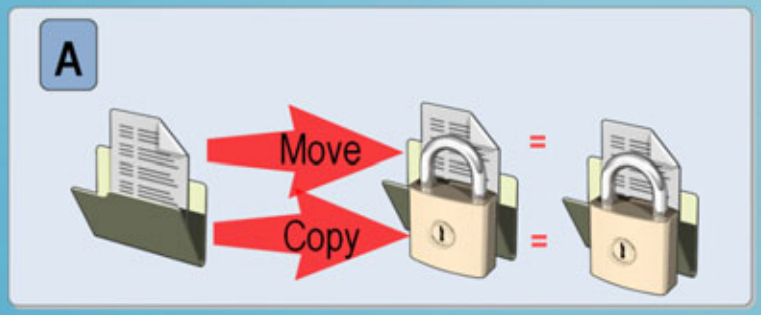
در درس سناریو عملی (در مالتی مدیا آموزشی) مثال فوق را مورد پیاده سازی قرار خواهیم داد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

شرایط مختص به نقل و انتقال Encryption Data

- کپی و یا Move کردن یک فولدر که Encrypt نمی باشد به فولدری که Encryptمی باشد.



در نتیجه فولدری که به یک Encrypted Folder منتقل و یا کپی شده است خود فولدر و محتویات آن همگی به صورت Encrypt شده در خواهند آمد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

نکته

در صورتی که فایلی را که دارای خواص Encrypt می باشد از یک NTFS Partition به یک FAT Partition منتقل نمایید، فایل هایی که به صورت Encrypt شده خواص رمز شده خود را از دست می دهند، فایل هایی که به صورت Encrypt شده می باشند را می توانید تغییر نام داده، Copy و یا move نمایید.

باید توجه داشته باشید که فایل های Encrypt شده را تنها کاربری می تواند مدیریت نمایید که خودش آنها را رمزگذاری نموده است.

بعنوان آخرین نکته توجه داشته باشید که فایل ها و فولدرهای سیستمی را نمی توانید Encrypt نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تمرین عملی

در تمرین عملی مربوط به مالتی مدیای آموزشی به بررسی مـوارد گفتـه شـده در طـول درس مختص به چگونگی Encrypt نمودن اطلاعات، بررسی انجام اعمال مختلف بر روی دیتاهای رمزگذاری شده خواهیم پرداخت، چگونگی تهیه کپی و Backup از فایل های فوق و مشاهده کلید Private Key را پیاده سازی خواهیم نمود.

همچنین برای درک بهتر از عملکرد اسـتفاده از کلیـدهای Private Key بـه درس سـناریو عملی در همین رابطه مراجعه نمایید.

www.ParsBook.org

تمرین عملی

- استفاده از قابلیت Encryption در ویندوز XP
- استفاده از دستور Cipher برای رمزگذاری و رمزگشایی دیتا
- بررسی اعمال مختلف بر روی دیتا های رمزگذاری شده
- استفاده از کپی و Backup از دیتاهای Encrypt شده
- مشاهده و دسترسی به Private Key های کاربران

www.ParsBook.org

قسمت سوم:

آشنایی با Recover Agent در Workgroup

www.ParsBook.org

معرفی درس

در درس های قبلی با مفاهیم پایه ایی مختص به Encryption آشنا شده اید و همچنین به طور کامل با چگونگی پیاده سازی قابلیت Encryption در محیط شبکه ایی Workgroup و Windows XP آشنا شده اید.

ولی یکی از مباحث مهمی که می بایست در رمزگذاری مورد توجه قرار دهید مختص به Recovery و بازیابی دیتا های Encrypt شده می باشد.

در این درس به مفاهیم مختص به آن خواهیم پرداخت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی Recovery

در قسمت قبل بیان شده که هر زمان بخواهید امکان دسترسی به دیتا رمزگذاری شده یک کاربر را داشته باشیم، تنها کافی است از Private Key مختص به آن کاربر یک Export تهیه نمایم و در ادامه آن را در هر کامپیوتر و سیستم عاملی که مورد نظر است Import نمایید، به این ترتیب امکان مشاهده دیتای (Encrypted) کاربر فوق را خواهیم داشت.

از این روش می توانید برای ارسال اطلاعات رمزگذاری شده خودتان نیز استفاده نمایید، ولی مشکلی که ممکن است به وجود آید مختص به زمانی است که تعدادی کاربر به صورت اشتراکی از یک Local Computer استفاده می نمایند، در این حالت هر کدام به صورت مجزا اقدام به Encrypt نمودن اطلاعات خودشان می باشند.

www.ParsBook.org

WWW.SOFTGOZAR.COM

معرفی Recovery

بنابراین با فرض اینکه از یک کامپیوتر سه کاربر استفاده می نماند و هر سه نیز اطلاعات خود را رمزگذاری می نمایند، بنابراین سه کلید Private برای هر کدام از آنان وجود دارد و می بایست Export گردد، هر کاربر می تواند شخصاً Private Key خود را از کامپیوتر Export نمایید، ولی اگر راه حلی باشد که یک کاربر خاص بتواند تمامی دیتا های Encrypt شده کاربران دیگر را مشاهده و مدیریت نمایید، و نیازی نباشد که همه کاربران جداگانه Private Key های خودشان را Export نمایند، در این حالت ضریب خطا و همچنین مباحث مختص به Recovery دیتا نیز راحت تر صورت می گیرد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

www.modir-shabake.com

معرفی Data Recovery Agent

مایکروسافت نام کاربری را که می تواند به تمامی دیتاهای سایر کاربران دسترسی داشته باشد، اصطلاحاً Data Recovery Agent نامیده است، این کاربر می تواند به اطلاعات Encrypt شده تمامی کاربرانی که بر روی یک کامپیوتر وجود دارد دسترسی داشته باشد.

در صفحه بعد به عملکرد مختص به این کاربر خواهیم پرداخت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

www.modir-shabake.com

بررسی عملکرد Data Recovery Agent

در عملکـرد Data Recovery Agent شـما مـی بایسـت نخسـت یـک کـاربر را کاندیـد (Designate) نمایید، سپس Certificate & Private Key کاربر فوق را Export کرده و در نهایت تحت عنوان مامور مختص به Data Recovery در کـامپیوتر وارد نماییـد، بعـد از انجام پروسه فوق این کاربر می تواند دیتا رمزگذاری شده تمامی کاربران را مشاهده و مدیریت نمایید (حتی می تواند دیتا سایر کاربران را Decrypt نمایید.)

www.ParsBook.org

WWW.SOFTGOZAR.COM

بررسی عملکرد Data Recovery Agent

کاربر موردنظر که در نقش مامور بازیابی اطلاعات خواهد بود و هر زمان که با استفاده از Credential خودش به کامپیوتر Login نمایید، می تواند به تمامی دیتاهای Encrypted شده بر روی کامپیوتر(از هر کاربر) دسترسی پیدا نمایید.

در اولین مرحله برای معرفی نمودن یک کاربر کاندید به عنوان Recovery Agent می بایست Certificate & Private key مختص به وی را Export نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Export کردن کاربر Data Recovery Agent

برای این منظور از دستور Cipher به همراه سویچ R/ برای Export نمودن کاربری که می خواهید در نقش Data Recovery Agent باشد استفاده نمایید، در شکل زیر نمایی از دستور مورد نظر را که برای کاربر کاندید اجرا شده است را مشاهده می نمایید:

```
C:\>cipher /r:c:\key\sh
Please type in the password to protect your .PFX file:
Please retype the password to confirm:


Your .CER file was created successfully.
Your .PFX file was created successfully.
```

www.ParsBook.org

WWW.SOFTGOZAR.COM

Export کردن کاربر Data Recovery Agent

در ادامه سویچ /r می بایست مسیر مختص به Export شدن را نیز مشخص نمایید، همان طور که در شکل صفحه قبل مشاهده گردید می توانید مسیر فولدری را که می خواهید برای Export در نظر گرفته شود را مشخص نمایید.

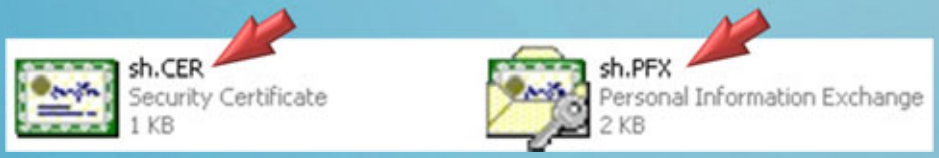
www.ParsBook.org

WWW.SOFTGOZAR.COM

Export نمودن Private Key

در نتیجه دستور صفحه قبل مشاهده گردید که:

در مسیر :C و در داخل فولدر key دو فایل بنام های (Sh.CER) و (Sh.PFX) ایجاد شده اند.



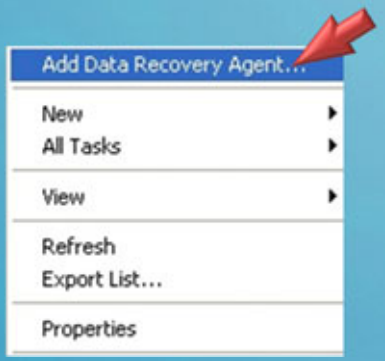
در ادامه می بایست فایلی را که دارای پسوند CER مـی باشـد را بعنـوان Data Recovery Agent معرفی نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تعیین Data Recovery Agent

برای این منظـور وارد Local Security Policy از Administrative Tools شوید سـپس مسـیر مشخص شده در شکل را باز نمایید.



در این قسمت گزینه

Add Data Recovery Agent

را مشاهده انتخاب نمایید:

www.ParsBook.org

تعیین Data Recovery Agent

در نخستین قسمت از Wizard می بایست به با کلیک بر روی گزینه Browse مسیر فـایلی *.CER را که در مرحله قبل Export کرده اید را مشخص نمایید:

در نهایت بعد از مشخص نمودن Certificate کاربر کاندید باید پروسـه Wizard را تـا انتهـا دنبال نمایید و گزینه Finish را در انتها انتخاب نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تعیین Data Recovery Agent

بعد از تکمیل پروسه می بایست یک Value جدید در قسمت مختص به Encrypting File System بنام کاربر کاندید ایجاد شده باشد:

Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	Administrator	9/2/2110	File Recovery

در قسمت Intended Purpose نیز حتماً می بایست عبارت File Recover را مشاهده نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تعیین Data Recovery Agent

در ادامه می بایست فایل دومی را که با دستور Cipher از آن خروجی گرفته شد(یعنی فایلی که دارای پسوند PFX) می باشد را اجرا و پروسه Wizard مختص به Import نمودن آن را طی نمایید، بعد از تکمیل نمودن پروسه Add کردن مامور بازیابی و اجرای فایل PFX مختص به کاربر فوق، می بایست یک بار کامپیوتر را Restart نمایید.

تا تغییرات صورت گرفته اعمال گردد، سپس براساس شرایط مختص به هر کدام از سناریو هایی که در ادامه درس بیان می گردد، می بایست مراحل مختص به Recovery دیتاهای رمزگذاری شده را انجام دهید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Recover نمودن دیتا های رمزگذاری شده

در دو سناریو مختلف می توان دیتاهای رمزگذاری شده را بازیابی نمود:

- نخست قبل از آنکه کاربری بر روی کامپیوتر دیتاهای خودش را به صورت Encrypt شده درآورده باشد یک Data Recovery Agent بر روی سیستم تعریف کرده باشید.

در حالت فوق کاربر Agent می تواند به تمامی دیتاهای کاربران بعد از آنکه دیتاهای فوق Encrypt گردید، دسترسی داشته باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Recover نمودن دیتا های رمزگذاری شده

در حالت مختص به سناریو یک:

فقط کافی است مامور بازیابی به کامپیوتر Login نمایید و فایل ها و فولدرهای Encrypt شده را باز کرده و محتوای آنان را مشاهده نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Recover نمودن دیتا های رمزگذاری شده

در سناریو دوم،

ممکن است قبل از معرفی کاربری بعنوان مامور بازیابی کاربران بر روی کامپیوتر دیتاهای خود را از قبل Encrypt کرده باشند.

- در حالت دوم باید هر کاربر بعد از تکمیل شده پروسه معرفی مامور بازیابی یک بار با Account خودش Login و سپس Logoff نمایید، سپس Recovery Agent با Account خودش login کرده و اقدام به باز کردن دیتاهای Encrypted شده کاربران نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Recover نمودن دیتا های رمزگذاری شده

در واقع در سناریو دوم،

یک مرحله اضافه تر مختص به login & logoff خود کاربران به کامپیوتر می بایست صورت گیرد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

نکته

پیشنهاد شده است همیشه کاربر کاندید برای Recovery Agent را Administrator انتخاب نمایید، چرا که دارای دسترسی های بسیاری به صورت پیش فرض نیز می باشد و می تواند گزینه مناسبی برای Data Recovery Agent نیز محسوب گردد، باید توجه داشته باشید که کاربران محدود (یعنی عضو گروه Users) را نیز می توانید تحت عنوان Data Recovery Agent معرفی نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

نکته

ولی برای انجام عمل فوق می بایست با یک کاربر که عضو گروه Administrators می باشد ابتدا Login کرده و سپس پروسه گفته شده را برای کاربر محدود انجام دهید، برای مشاهده اینکه آیا یک فایل دارای Recover Agent می باشد و یا خیر، می بایست به قسمت Details از Advanced Properties مراجعه نمایید:

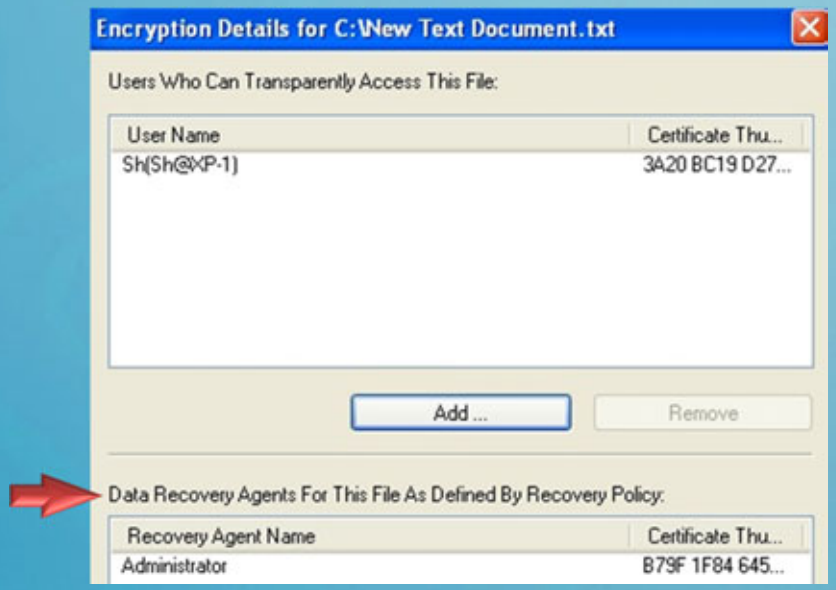
www.ParsBook.org

WWW.SOFTGOZAR.COM

نکته

در ادامه نام کاربری را که بعنوان مامور بازیابی مشخص شده است را می توانید مشاهده نمایید،

در شکل مشاهده می نمایید که نام Administrator بعنوان مامور بازیابی مشخص شده است.



www.ParsBook.org

WWW.SOFTGOZAR.COM

Recover Agent در محیط Workgroup

توجه نمایید که در محیط شبکه ایی Workgroup هیچ کامپیوتری به صورت پیش فرض دارای Recovery Agent نمی باشد، بنابراین می بایست بر روی کامپیوترهای فوق خودتان اقدام به معرفی کاربری به صورت مامور بازیابی نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

استفاده از EFS بر روی Network

توجه داشته باشید EFS به صورت Transparent و پشت صحنه فعالیت می نمایید همانند قابلیت Compression، در واقع خود سیستم عامل فایل های Encrypt را همانند فایل های Compress باز و استفاده می نمایید و مجدداً اعمال فوق را بر روی آنان صورت می دهد، در نتیجه نیازی نیست که خود کاربران در هر بار استفاده از دیتاهای رمزگذاری شده اقدام به Decrypt نمودن آنان و مجدداً Encrypt کردن نمایند.

در صورتی که دیتا های Encrypt شده را در شبکه به اشتراک بگذارید، فرمتی که آنان بر روی شبکه نقل و انتقال می گردند به صورت Clear Text می باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

استفاده از EFS بر روی Network

به این ترتیب اگر اطلاعات به وسیله یک فرد نفوذ گر در شبکه Sniff و سرقت شود می تواند به محتوای فایل دسترسی داشته باشد، بعنوان راه حل می بایست از Solution های دیگری مثل، IP Sec (IP Security) استفاده نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تمرین عملی

در تمرین عملی مختص به مـالتی مـدیای آموزشـی مـوارد گفتـه در طـول درس و همچنـین پیاده سازی دو سناریو فوق را به طور کامل انجام خواهیم داد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تمرین عملی

- اضافه نمودن کاربر کاندید بعنوان Data Recover Agent
- بررسی سناریوهای مختلف در رابطه با Recover نمودن اطلاعات رمزگذاری شده.

www.ParsBook.org

www.ParsBook.org

قسمت چهارم:

چگونگی استفاده و پیاده سازی NTFS Encryption در Windows 7

معرفی درس

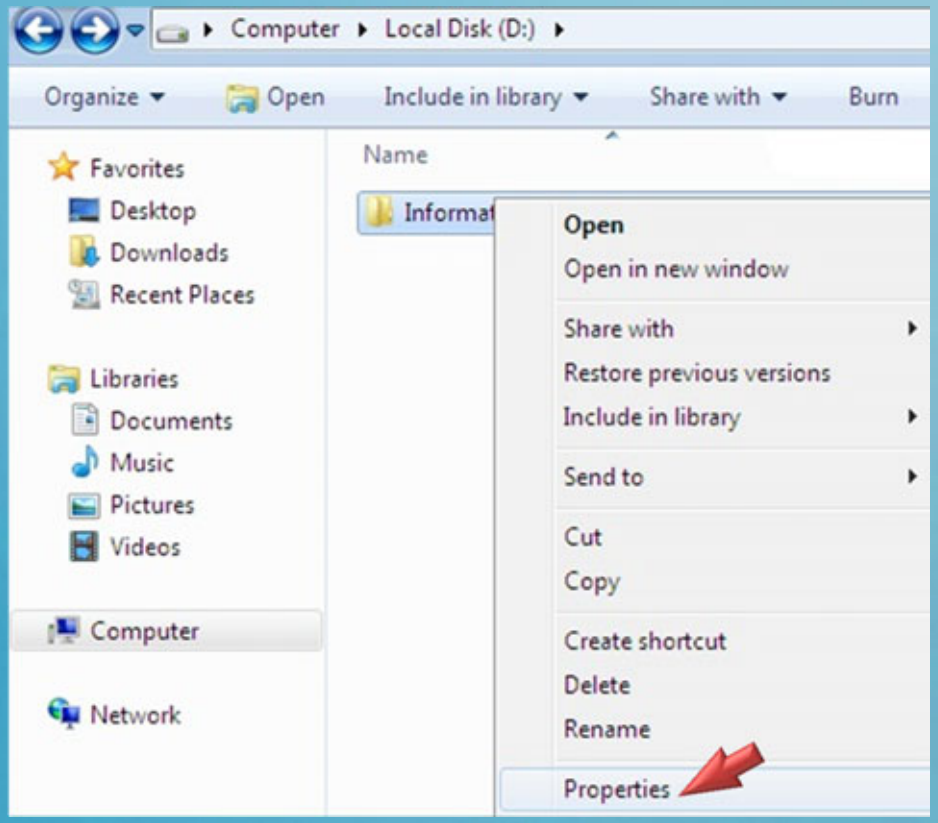
در Windows 7 شاهد تغییرات جزیـی در رابطـه بـا مبحـث رمزگـذاری نمـودن اطلاعـات می باشیم، بنابراین در این درس به بررسی چگونگی پیاده سازی و اسـتفاده از Encryption تحت سیستم عامل Windows 7 خواهیم پرداخت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

همانند Windows XP می بایست بر روی فایل و یا فولدر مورد نظر راست کلیک کرده و اقدام به گرفتن Properties نمایید:

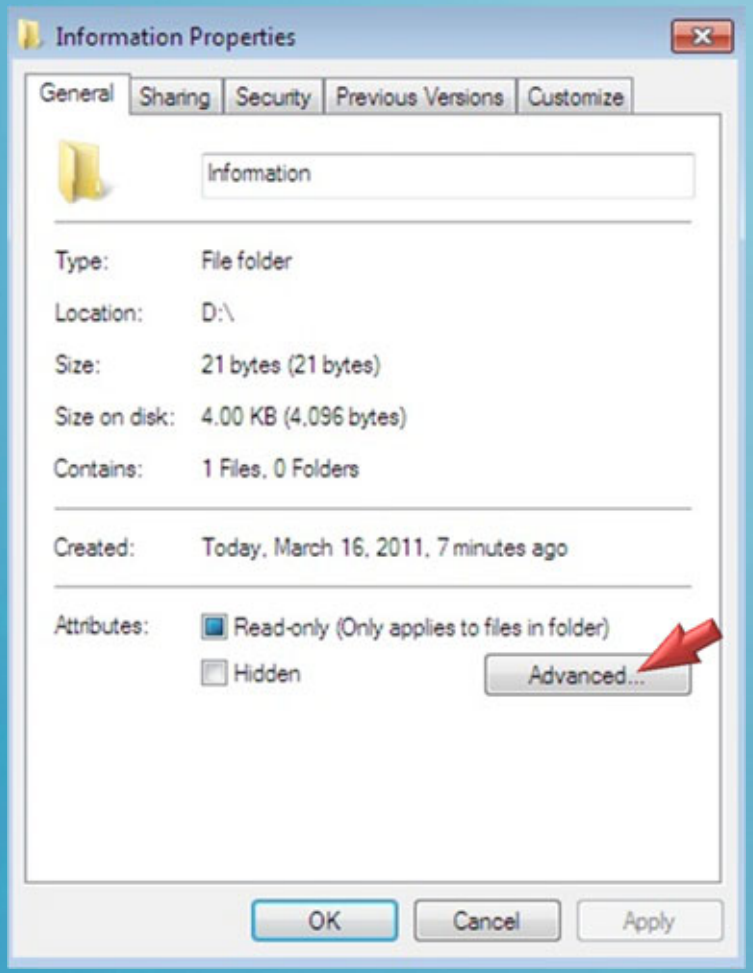


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در General Tab بر روی گزینه Advanced کلیک نمایید:

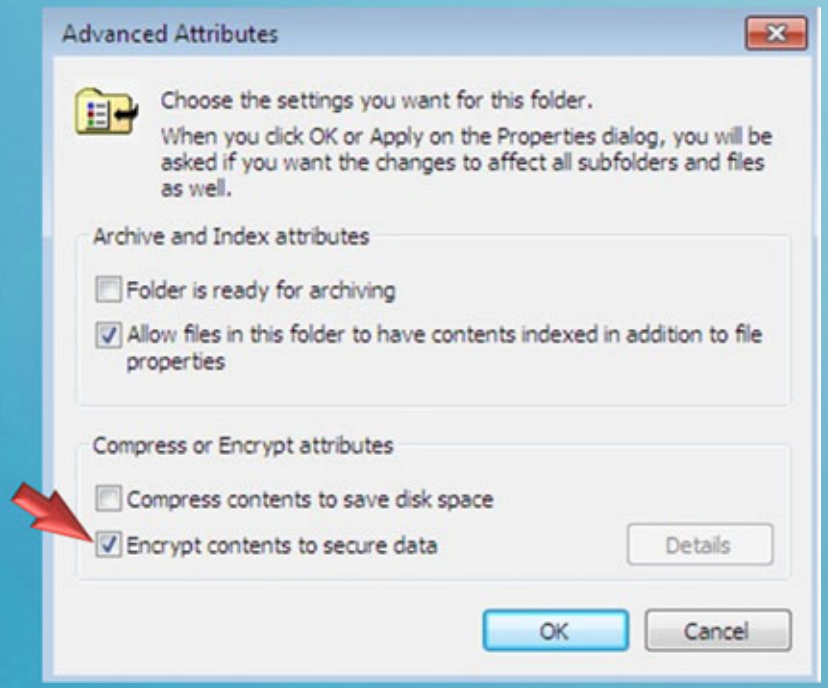


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

سپس می بایست چک مارک گزینه Encrypt content to secure data را مطابق شکل زیر انتخاب نمایید:

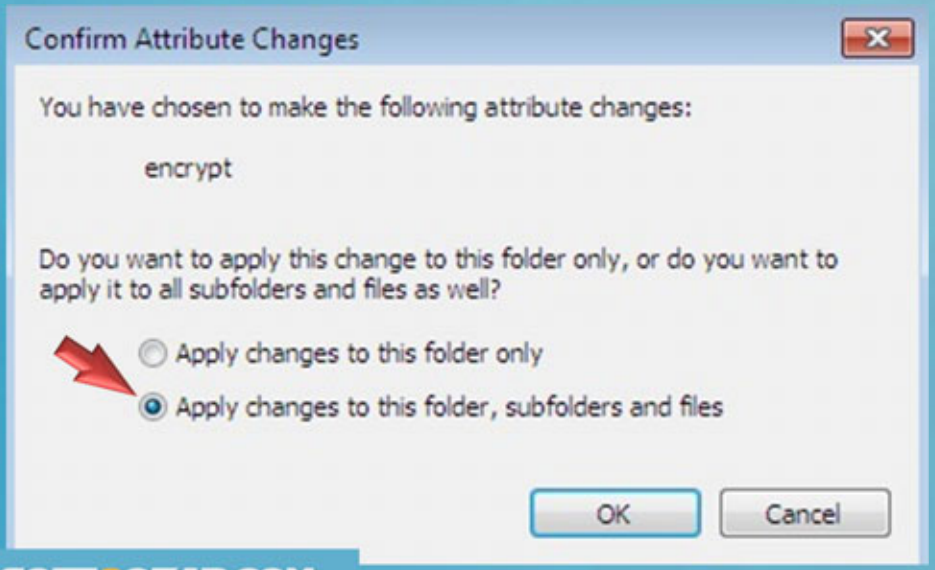


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

بعد از کلیک بر روی Ok و سپس Apply نمودن تنظیمات کادری باز شده و از شما در سوالی پرسیده می شود مبنی بر اینکه آیا می خواهید محتویات فایل های درون فولدر مورد نظر نیز Encrypt شوند که شما می توانید گزینه مشخص شده در شکل زیر را انتخاب نمایید تا تمامی فایل ها و زیر فولدرهای موجود همگی یکجا Encrypt گردد:

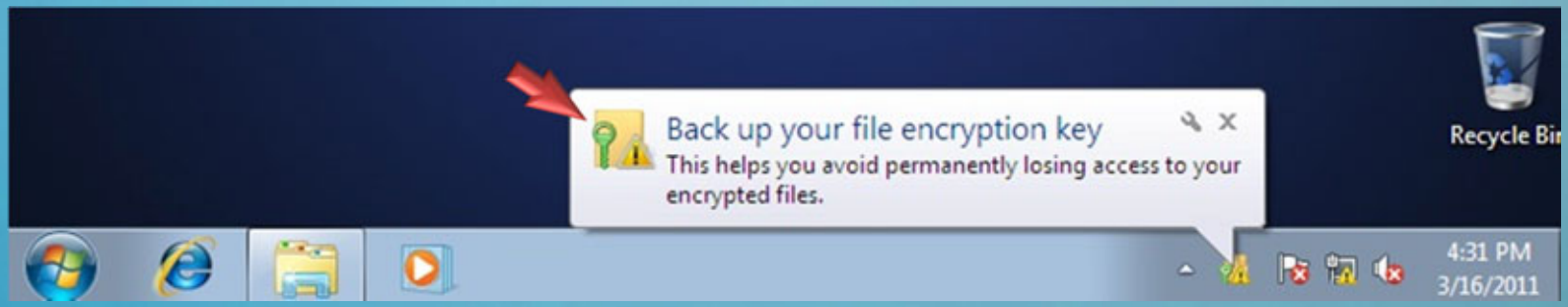


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

بعد از تکمیل نمودن پروسه مختص به Encrypt شدن فایل ها یک بالون در کنار ساعت ویندوز نمایش داده می شود، و از شما خواسته می شود که یک نسخه پشتیبان از فایل مختص به کلید رمزگذاری شده اطلاعات که مختص به خودتان می باشد تهیه نمایید:



www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

توجه داشته باشید چنانچه کامپیوتر Windows 7 در محیط Workgroup و در یک شبکه از کامپیوترها قرار داشته باشد، و یا اینکه در حالت اصطلاحاً Stand Alone قرار داشته باشید، در هر دو شرایط فوق، سیستم عامل اقدام به ایجاد نمودن یک Certificate می نمایید و شما می بایست از Certificate فوق فایل Backup تهیه نمایید.

در اینجا منظور از شرایط بیان شده حالتی است که کامپیوتر در یک شبکه Domain قرار ندارد و اصطلاحاً Join to Domain نمی باشد، مثلاً تمامی کامپیوترها، Laptop هایی که در حال استفاده به صورت شخصی می باشند همگی در حالت Stand Alone می باشند.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

بعد از اینکه فایل های خود را بر روی کامپیوتر به صورت Encrypt شده ست کردید، تنها شخصی که می تواند به اطلاعات شما دسترسی پیدا نمایید، فقط خود شما خواهید بود.

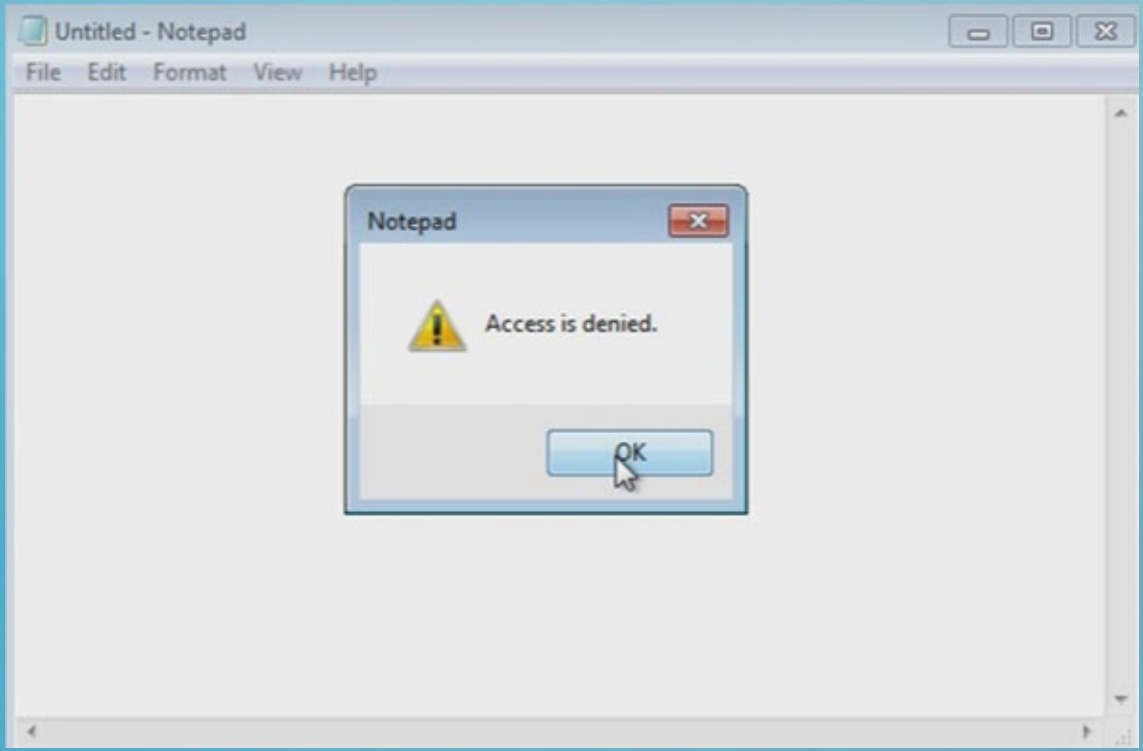
مثلاً اگر بر روی یک کامپیوتر خانگی برای تمامی اعضای خانواده User Account و حساب کاربری تعریف شده باشد، و شما فایل های خودتان را در پارتیشن D: به صورت Encrypt ست کرده باشید، فقط شما خواهید توانست فایل های رمز شده مربوط به خودتان را باز کرده و محتویات آنان را مشاهده نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

بنابراین سایر کاربران با پیغام Access is Denied مواجه خواهند شد در زمانی که بخواهند به اطلاعات رمزشده شما دسترسی پیدا نمایند:



www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

حتی اگر شما اجازه دسترسی (Permission) را نیز برای سایر کاربران مشخص کرده باشید باز هم آنان نمی توانند به محتویات فایل های رمزشده شما دسترسی پیدا نمایند.

برای اینکه امکان دسترسی به محتویات فایل های Encrypt شده خودتان را به سایر کاربران بر روی کامپیوتر بدهید، می بایست Certificate آنان را نیز بر روی فایل های خودتان اضافه نمایید.

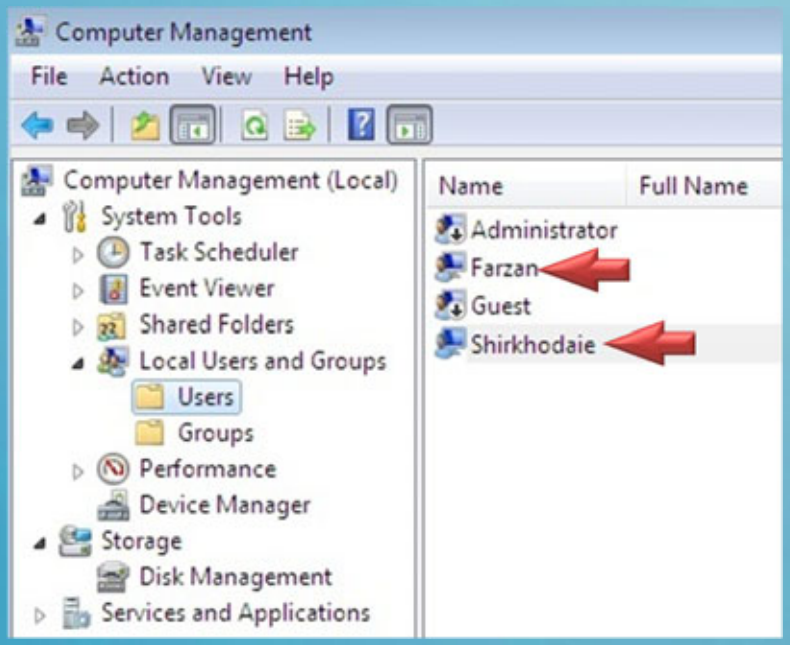
توجه داشته باشید که برای اینکه یک کاربر دارای Certificate باشد می بایست حداقل دارای یک فایل Encrypt شده مختص به خودش باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

برای اینکه در این درس شرایط مناسبی برای آموزش ایجاد گردد، بر روی سیستم عامل Windows 7 دو کاربر را ایجاد کرده ایم به نام های:



www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

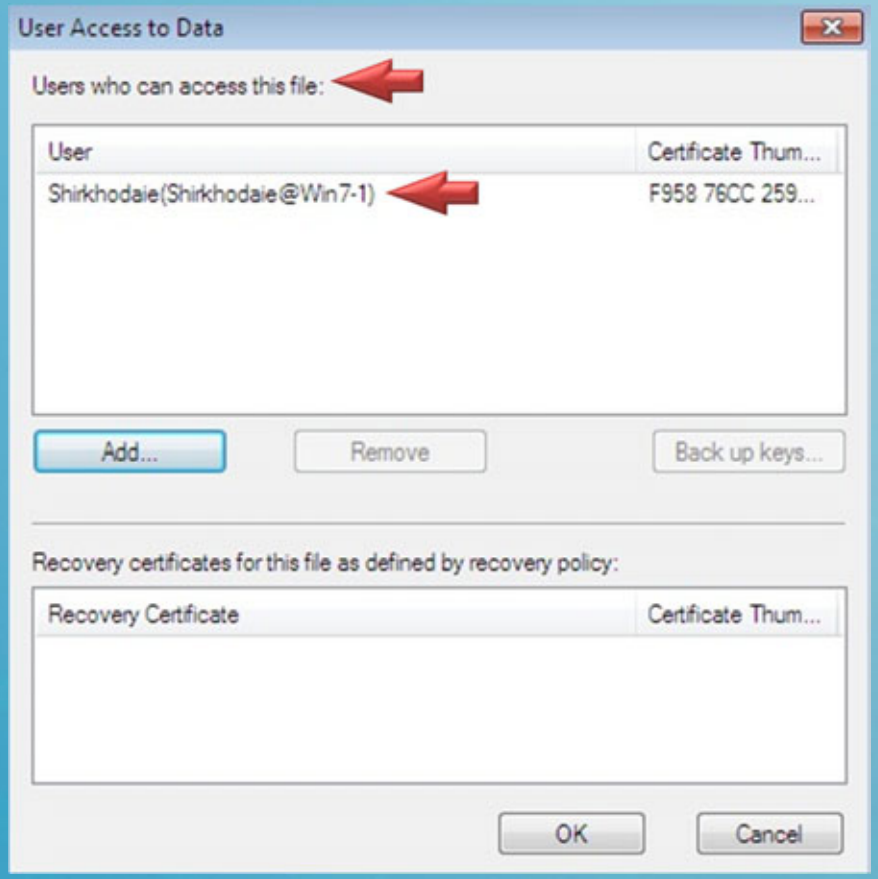
با هر کدام از کاربران فوق یک بار Login کرده و یک فایل را در داخل D: و بـرای هرکـدام به صورت مجزا Encrypt کرده ایم، سپس در ادامه قصد داریم امکان استفاده از فایل هـای Encrypt شده توسط کاربر Shirkhodaie را به کاربر Farzan اعطا نماییم.

برای این منظـور بـا کـاربر Shirkhodaie وارد کامپیوتر شده و بر روی فایل مـورد نظـر راسـت کلیک کـرده و گزینـه Properties را انتخـاب کرده و و بر روی Details کلیک نمایید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات



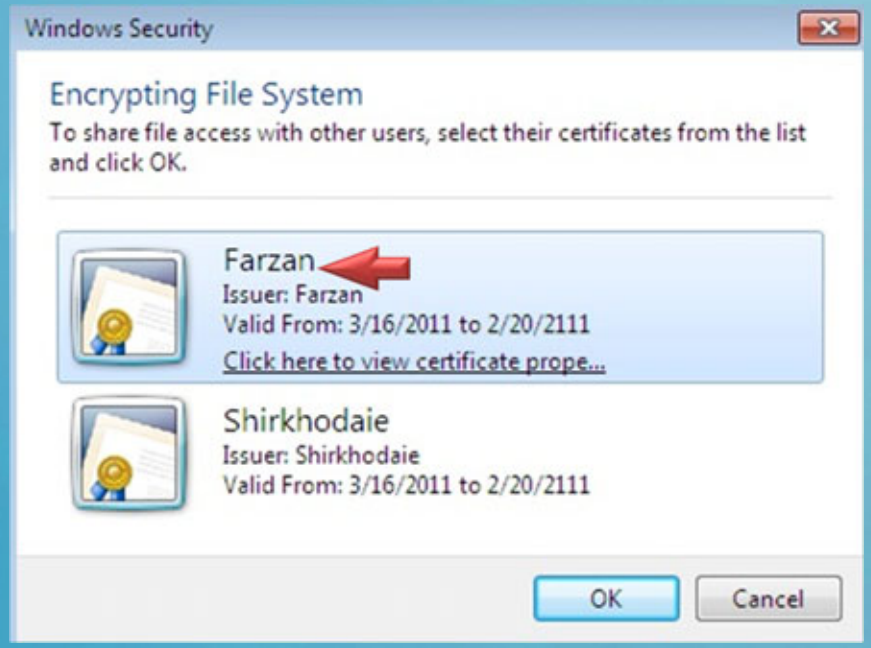
در ایـــن قســـمت Certificate کـــاربری را مشاهده می نمایید کـه بـه فایـل مـورد نظـر دسترسی دارد، و چون ما در این مثال با کاربر Shirkhodaie وارد شده ایم و فایل فـوق را به صورت Encrypt ست کرده ایم بنـابراین نام کاربر فوق را در تصویر زیر مشـاهده مـی نمایید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در ادامه کافی است بر روی گزینه Add کلیک کرده و کاربر مورد نظر را انتخـاب نماییـد، در اینجا قصد داریم کاربر Farzan را انتخاب نمایم:

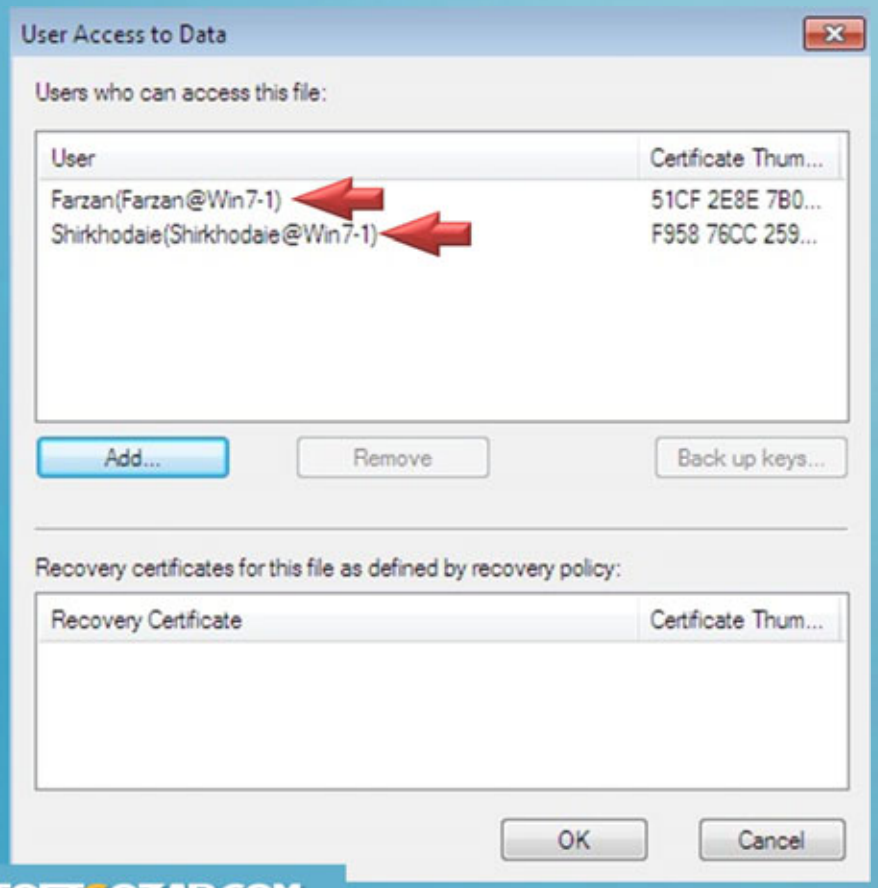


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در شکل زیر مشاهده می نمایید نام دو کاربر در لیست مشخص شده است، در نتیجه هر دو کاربر می توانند به محتویات فایل Encrypt شده دسترسی پیدا نمایند:

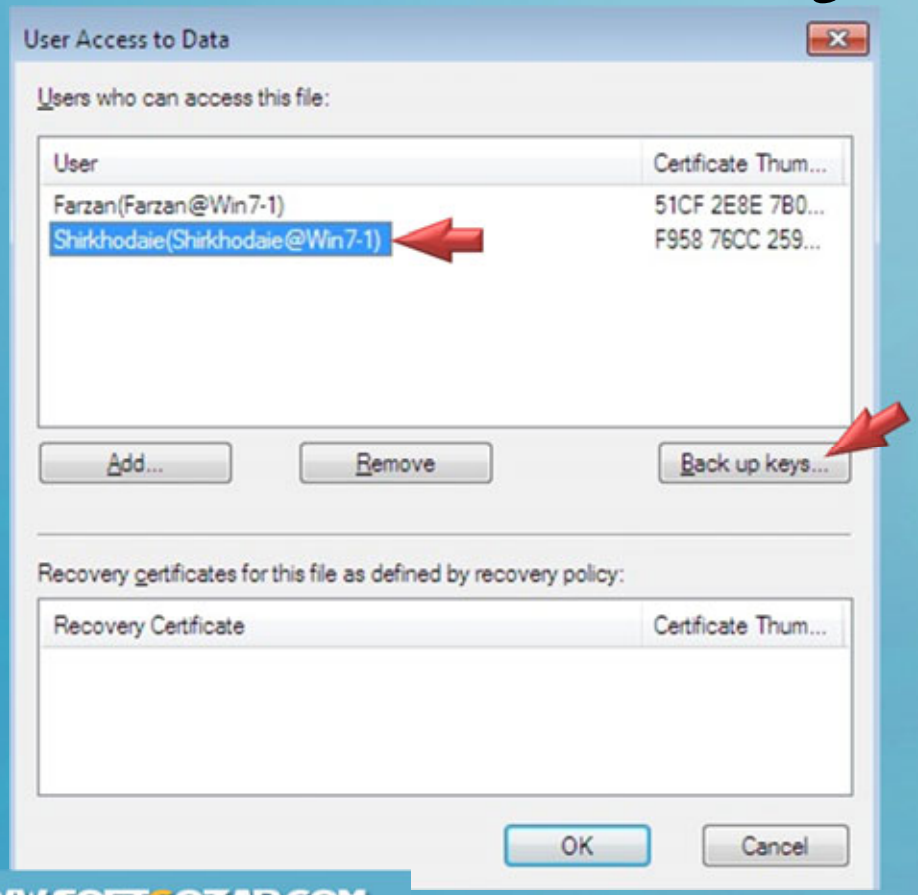


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در قسمت فوق همچنین می توانید بر روی نام یکی از کابران را انتخاب نمایید، و سپس اقدام به گرفتن Backup از Certificate مربوط به آن نمایید:



در شکل مشاهده می نمایید که قصد داریم از کاربر Shirkhodaie و Certificate مربوط به آن Backup تهیه نمایم.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

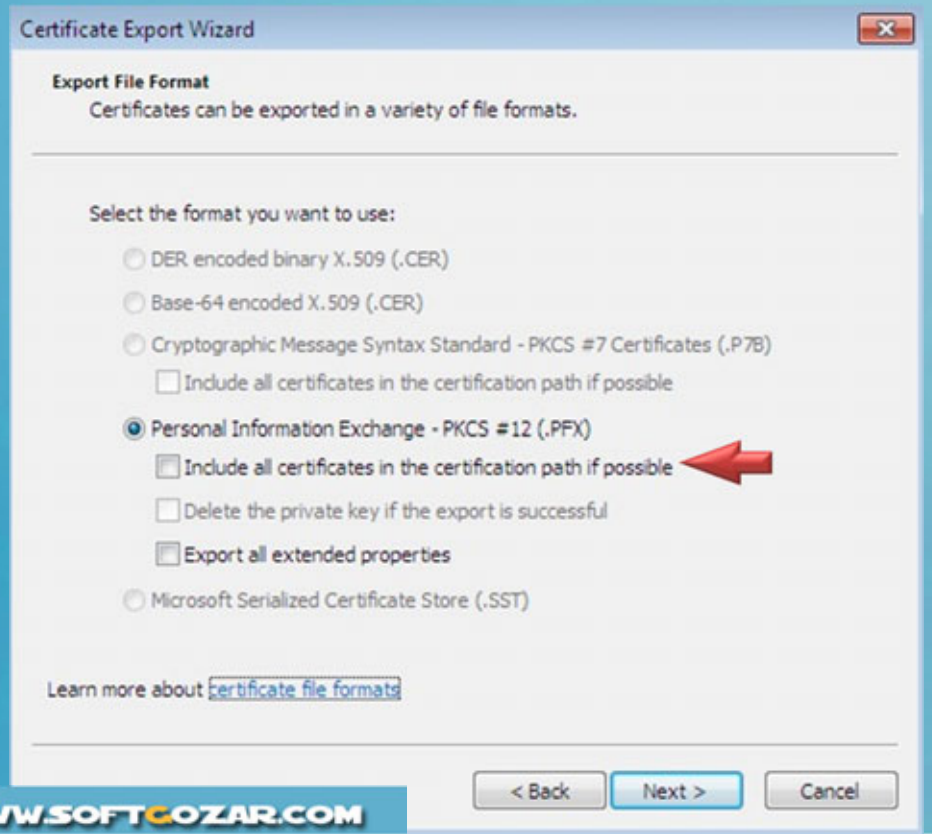
در شکل زیر اولین پنجره مختص به Wizard تهیه Backup را مشاهده می نمایید، ب روی Next کلیک نمایید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در ادامه می توانید از تمامی Certificate هایی که در کامپیوتر موجود می باشند Backup تهیه نمایید، که در اینصورت می بایست چک مارک گزینه Include all certificate in... را انتخاب نمایید:



در اینجا چون قصد داریم فقط از Certificate کاربر Shirkhodaie فایل Backup تهیه کنیم بر روی Next کلیک کرده بودن انتخاب گزینه های ممکن

www.ParsBook.org
WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

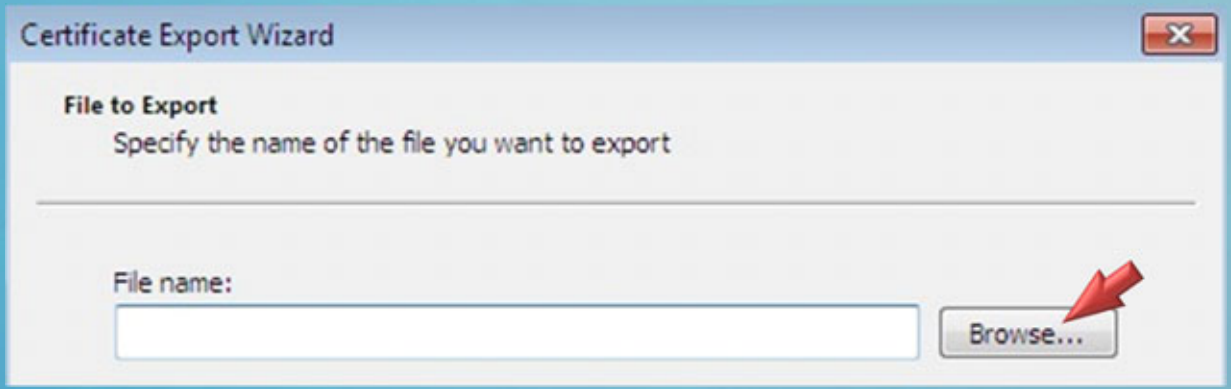
سپس می بایست یک پسورد برای فایل Backup مشخص نمایید تا در صورتی که شخصی فایل Backup مختص به Certificate شما را به دست آورد نتواند بدون دانستن پسـورد از آن استفاده نمایید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در ادمه مسیر فایل Backup را که قرار است در آنجا ذخیره شود را مشخص نمایید:



www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در آخرین قسمت Wizard شما اطلاعاتی را از گزینه های انتخابی مشاهده می نمایید:

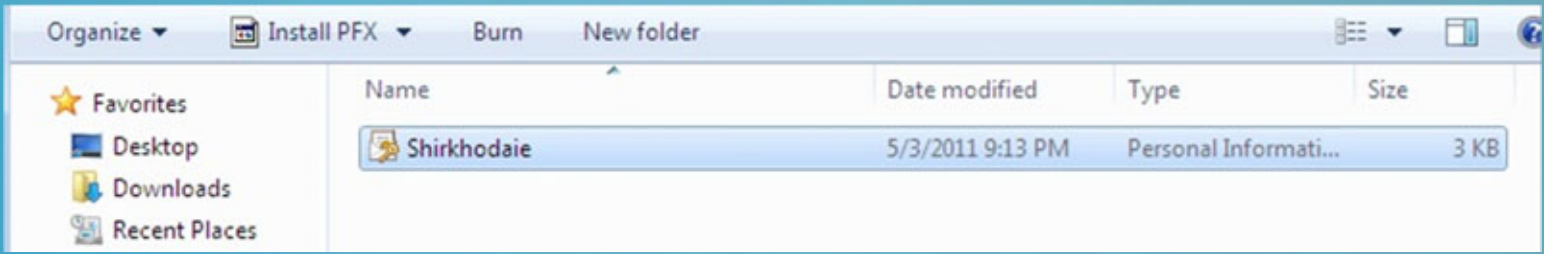
www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در آخر برای شما پیغـام موفقیـت آمیـز بـودن تهیـه Backup از Certificate نمـایش داده خواهد شد:

در شکل زیر نمایی از فایل خروجی را مشاهده می نمایید:



www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

همچنین می توانید از طریق کلیک بر روی بالون نمایش داده شده در کنار ساعت ویندوز از Certificate مختص به خودتان Backup تهیه نمایید:

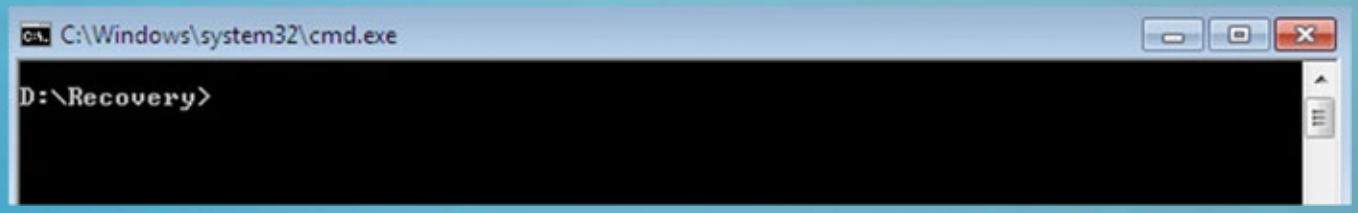
در هر دو روش می بایست Wizard توضیح داده شده را تکمیل نمایید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

همچنین شما می توانید یک Recovery Agent ایجاد نمایید تا کاربری که در آن نقش می باشد بتواند تمامی فایل های Encrypt شده همه کاربران را مشاهده و مورد دسترسی قرار دهید، برای این منظور یک فولدر در یکی از پارتیشن های کامپیوتر ساخته و سپس با دستور CD از طریق Command Prompt وارد آن شوید:



www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در ادامه دستور زیر را اجرا نمایید:

```
C:\Windows\system32\cmd.exe
D:\Recovery>cipher /r:Shirkhodaie
```

توجه نمایید به جای عبارت Shirkhodaie می توانید از نام دلخواه استفاده نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

سپس می بایست در ادامه یک پسورد برای فایل تعریف نمایید و در نهایت خروجی به صورت زیر خواهد بود:

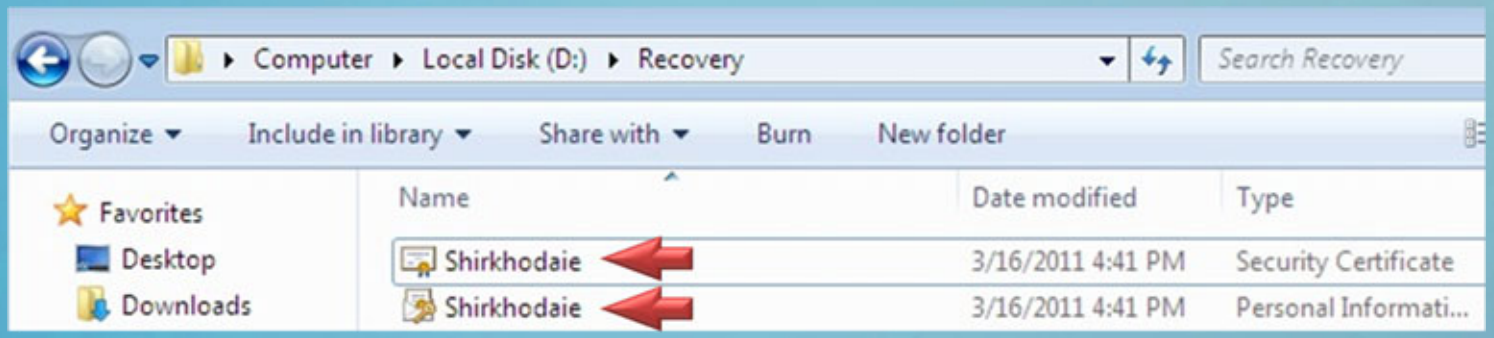
C:\Windows\system32\cmd.exe

```
D:\Recovery>cipher /r:Shirkhodaie
Please type in the password to protect your .PFX file:
Please retype the password to confirm:


Your .CER file was created successfully.
Your .PFX file was created successfully.

D:\Recovery>
```

www.ParsBook.org

چگونگی Encrypt نمودن اطلاعات

دو فایل در انتهای دستور فوق همانند شکل زیر برای شما نمایش داده می شود:

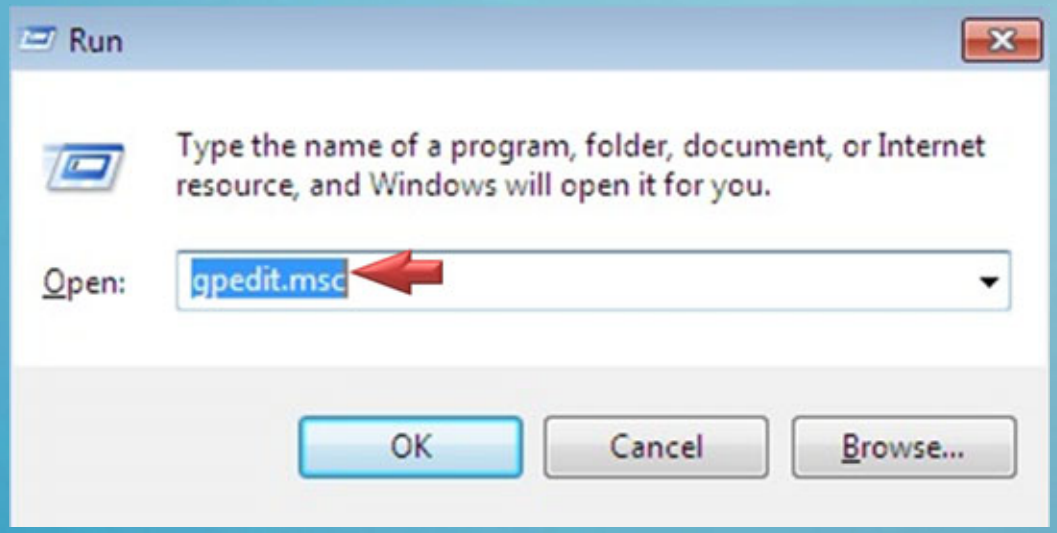


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در ادامه می بایست کاربر فـوق را در Local Group Policy بعنـوان Recovery Agent تعریف نمایید، نخست با دستور زیر وارد GP شوید:

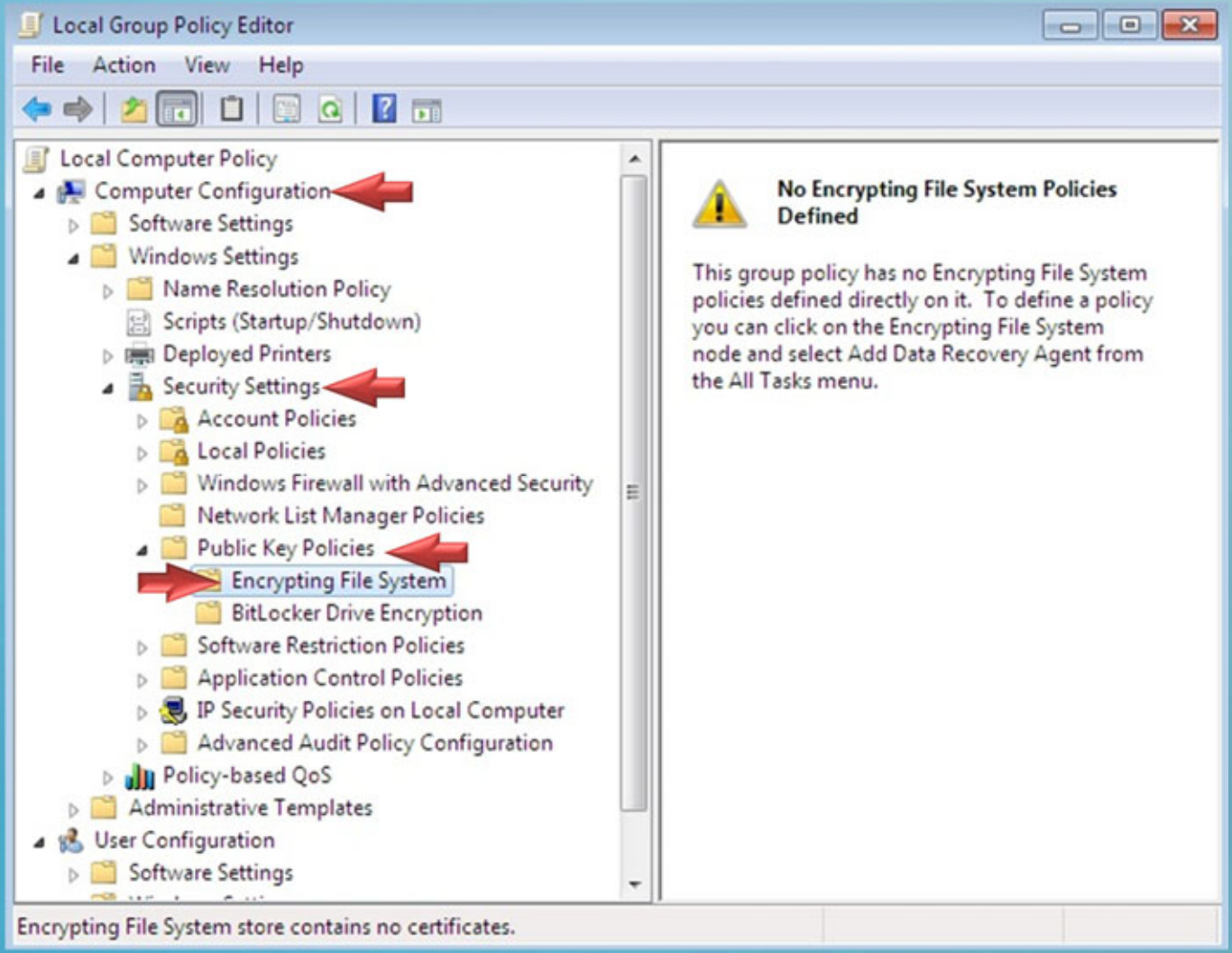


در ادامه وارد مسیر مشخص شـده در Group Policy در صفحه بعد شوید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

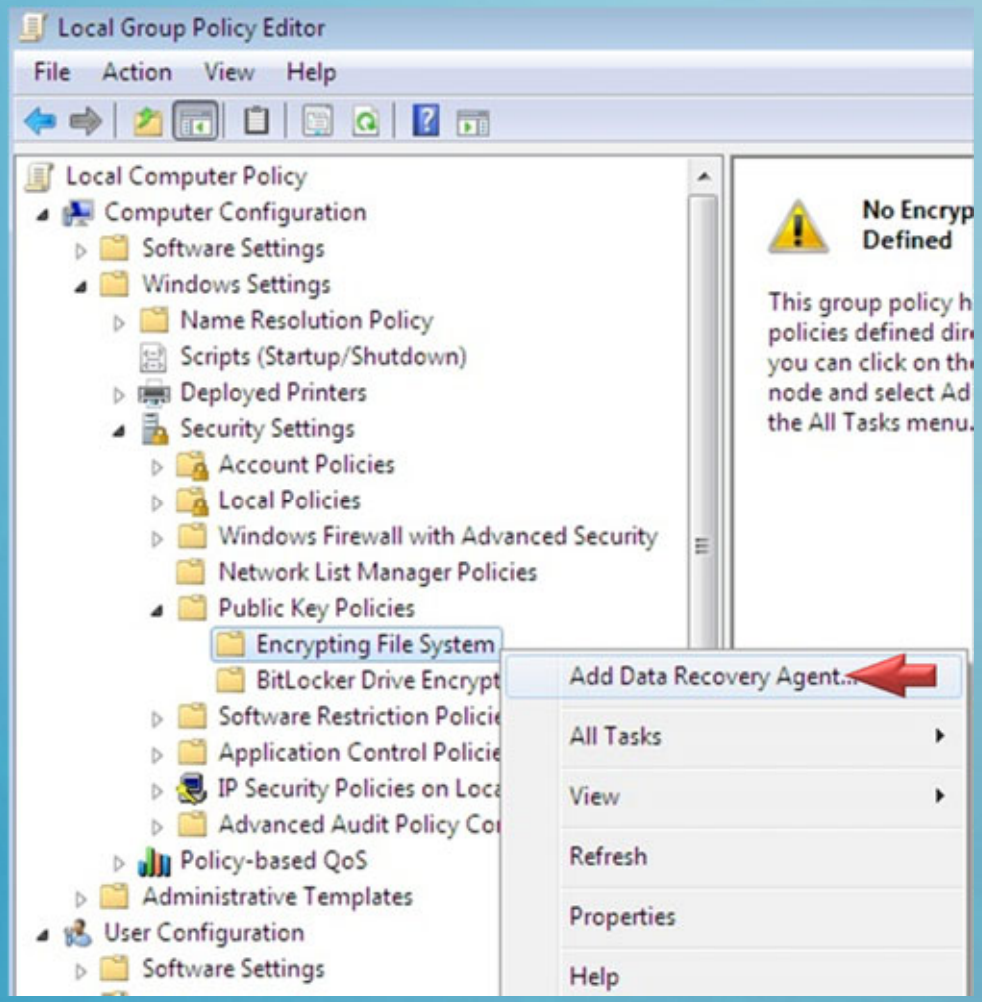
چگونگی Encrypt نمودن اطلاعات



www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات



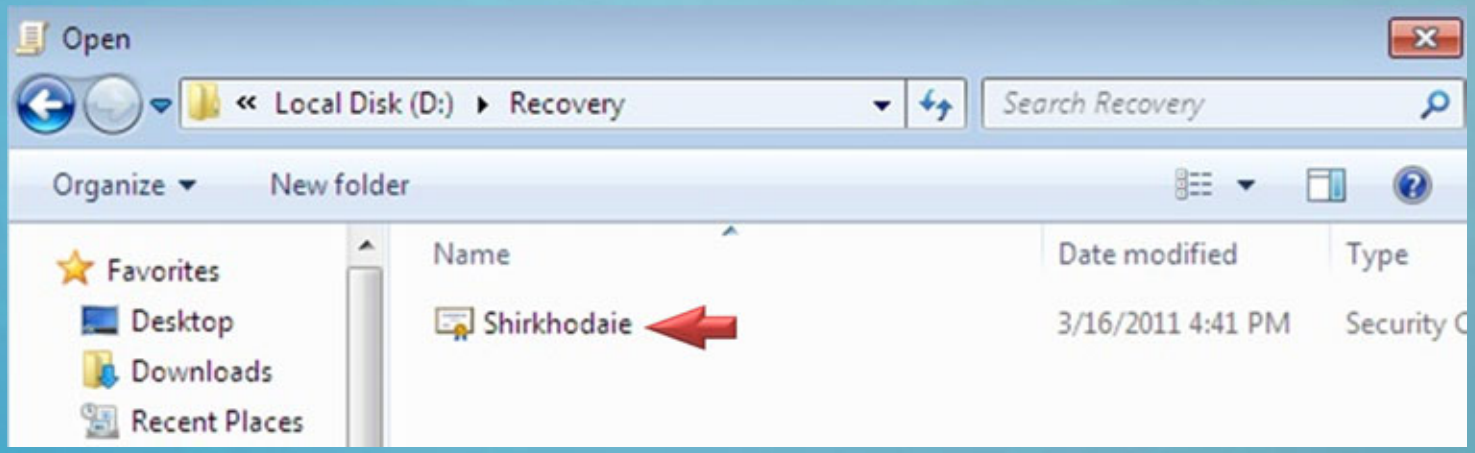
بر روی قسمت Encrypting File System کلیک راست کرده و گزینه Add Data Recovery Agent را انتخاب نمایید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

می بایست مسیر مختص به فایل Certificate را که برای Recovery Agent با استفاده از دستور گفته شده در صفحات قبل مشخص کرده اید را مسیر دهی نمایید:

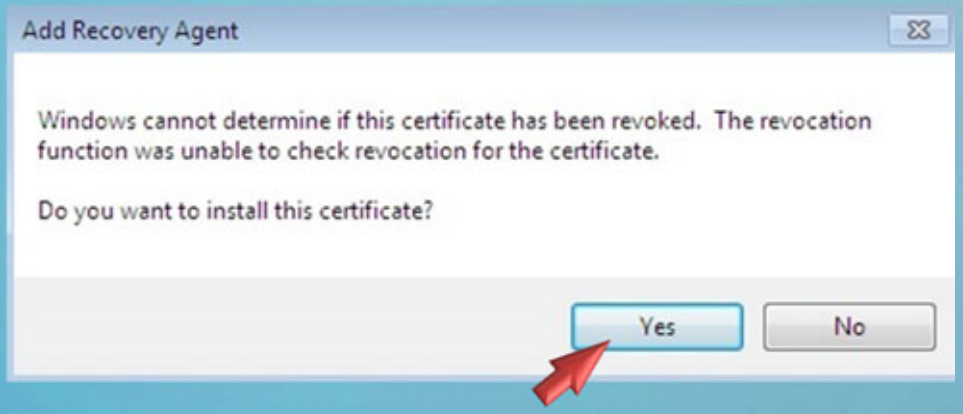


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

بعد از انتخاب فایل Certificate از شما یک سوال پرسده می شود که در جواب گزینـه Yes را انتخاب نمایید:

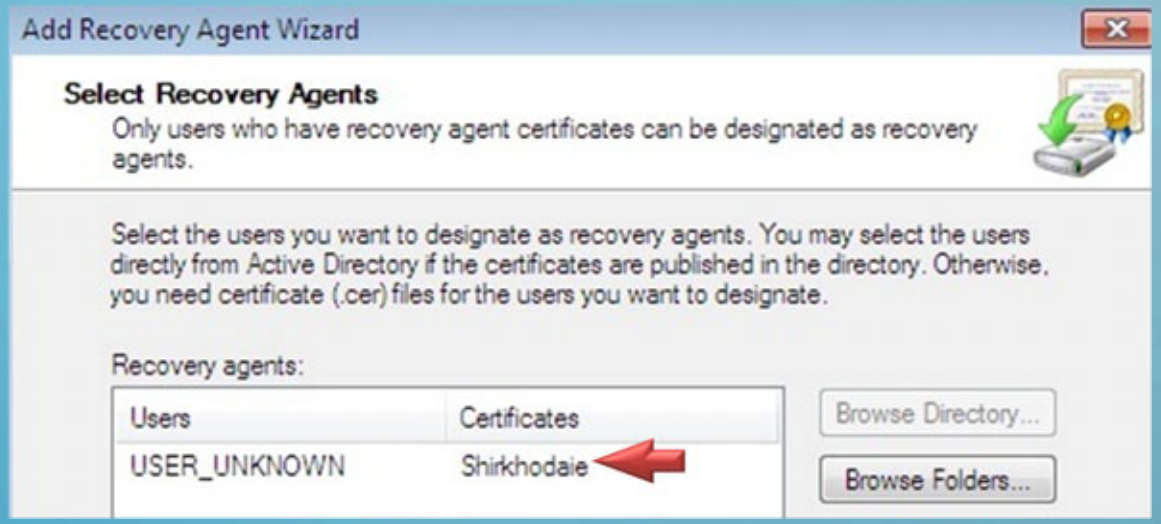


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

در شـــکل زیـــر نمـــایی از کـــاربر Shirkhodaie را مشـــاهده مـــی نماییـــد بعنـــوان Recovery Agents:

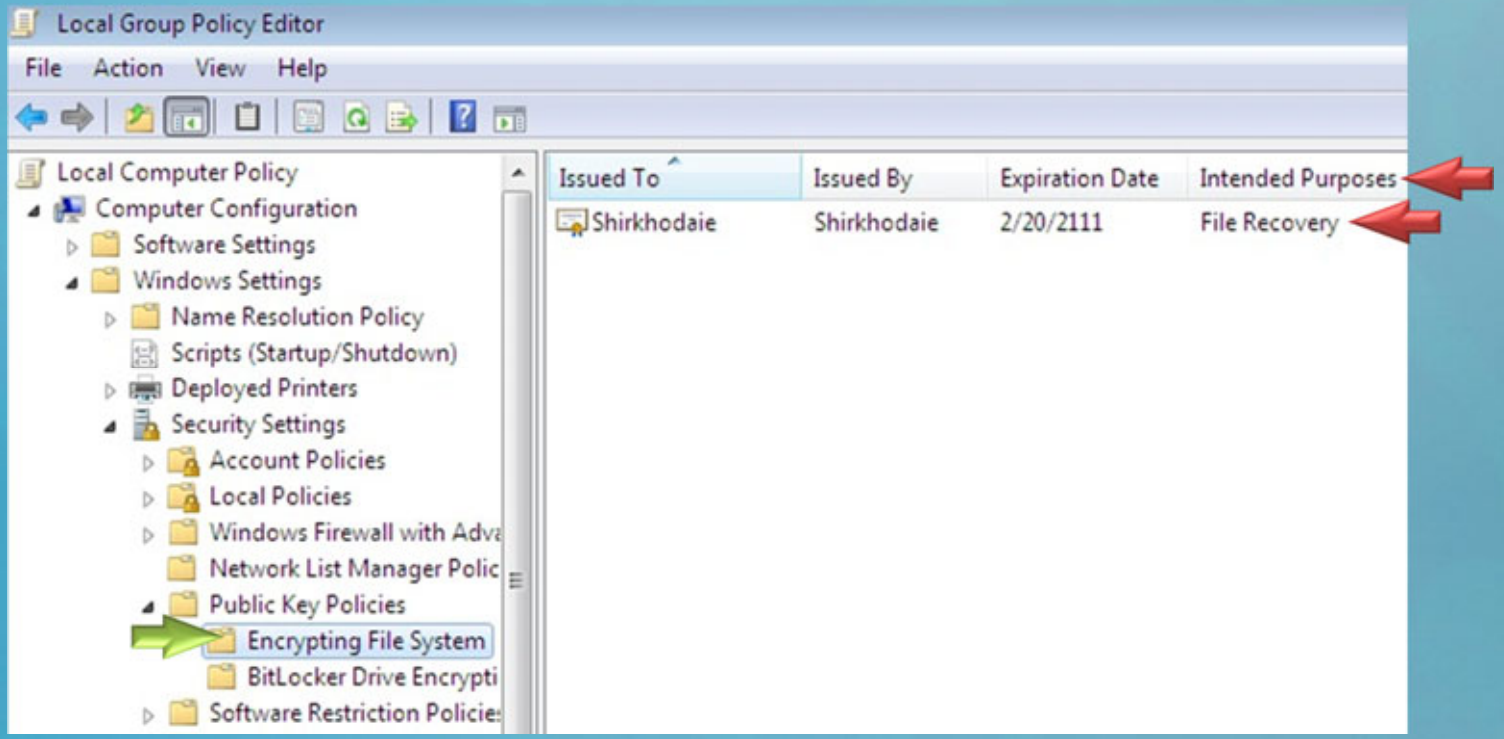


www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

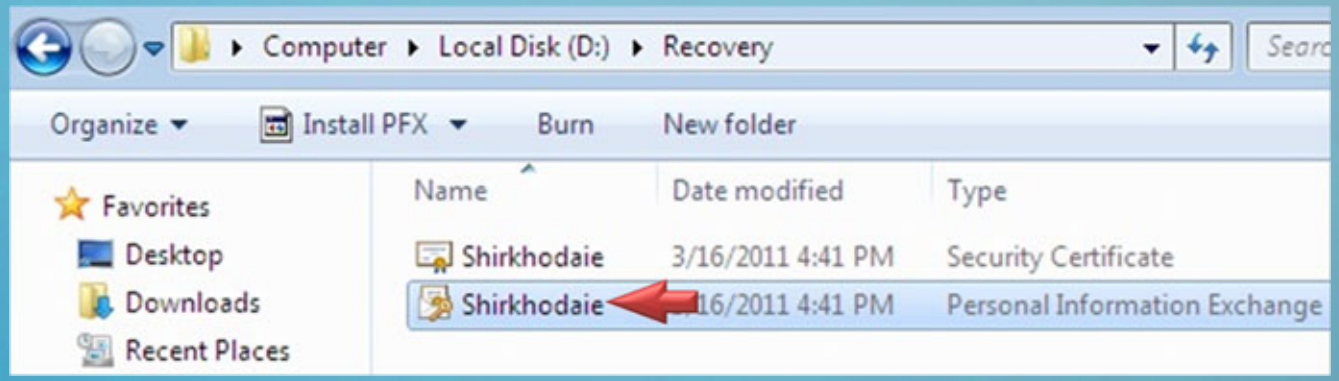
بعد از تکمیل پروسه می بایست نام کاربر مورد نظر در داخل Local Group Policy تعریف شده باشد، در قسمت Intended Purpose نیز حتماً می بایست عبارت File Recover را مشاهده نمایید:



www.ParsBook.org

چگونگی Encrypt نمودن اطلاعات

آخرین قدم باقی مانده مربوط می شود به وارد کردن (Import)، فایل مختص به Private Key که در صفحات قبل با دستور Cipher /r تهیه کرده بودید، برای این منظور فایل مختص به آن را اجرا کرده و مراحل Wizard را دنبال نمایید:



www.ParsBook.org

WWW.SOFTGOZAR.COM

چگونگی Encrypt نمودن اطلاعات

پس انجام مراحل فوق یک بار با تمام کاربران موجود بر روی کامپیوتر Login کرده و سپس Logoff نمایید، و در انتها با کاربری که بعنوان Recovery Agent آن را تعریف کرده Login نمایید و به این ترتیب امکان دسترسی به محتوای فایل های Encrypt شده سایر کاربران را به دست خواهید آورد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تمرین عملی

در تمرین عملی مربوط به مالتی مدیای آموزشی به بررسی مـوارد گفتـه شـده در طـول درس مختص به چگونگی Encrypt نمودن اطلاعات، تحت سیستم عامل Windows 7 و بررسی چگونگی تهیه کپی و Backup کلید Private Key را پیاده سازی خواهیم نمود و همچنـین چگونگی تعریف نمودن Data Recovery Agent خواهیم پرداخت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تمرین عملی

- استفاده از قابلیت Encryption در ویندوز 7
- استفاده از دستور Cipher برای رمزگذاری و رمزگشایی دیتا
- بررسی اعمال مختلف بر روی دیتا های رمزگذاری شده
- مشاهده و دسترسی به Private Key های کاربران

www.ParsBook.org

قسمت پنجم:

غیر فعال نمودن قابلیت EFS

در Domain & Workgroup

تحت Windows XP & 7

www.ParsBook.org

معرفی درس

در این درس قصد داریم در رابطه با کنترل و مدیریت EFS (Encrypting File System) در محیط های شبکه ایی Workgroup & Domain صحبت کرده، و به بررسی چگونگی غیر فعال نمودن قابلیت فوق بر روی کامپیوترهای Domain و یا کامپیوترهای Local (یعنی آنهایی که در Workgroup قرار دارند) پرداخته و شرایط مختلف در همین رابطه را مورد بررسی قرار دهیم.

www.ParsBook.org

WWW.SOFTGOZAR.COM

بررسی استفاده از EFS

یکی از مواردی که قالباً مدیران شبکه از آن شکایت دارند مختص است به استفاده بی مورد کلاینت ها از قابلیت EFS بر روی کامپیوترهای موجود در شبکه می باشد، با توجه به اینکه که در صورت عدم اطلاع مدیر دامین از وجود دیتاهای رمزگذاری شده بر روی کامپیوترهای شبکه، ممکن است با به وجود آمدن کوچک ترین مشکلی دیتاهای کاربران دچار مشکل شود. بنابراین مدیریت و استفاده از قابلیت فوق می بایست حتماً با نظارت مدیر شبکه صورت پذیرد، در غیر اینصورت ممکن است مشکلی هر چند کوچک منجر به از دست دادن همیشگی دیتا های Encrypted شده کاربران گردد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

بررسی استفاده از EFS

در لیست زیر نمونه هایی از مواردی را که ممکن است باعث از دست رفتن دائمی دیتاهای رمزگذاری شده گردد را مشاهده می نمایید:

- ریست شدن پسورد کاربر (Reset Password) در مدل شبکه ایی Workgroup البته شرایط فوق مختص به محیط دامین نمی باشد.
- پاک شدن User Account کاربر از Active Directory or SAM (در هر دو محیط Workgroup & Domain صادق می باشد.)

www.ParsBook.org

WWW.SOFTGOZAR.COM

بررسی استفاده از EFS

- نصب مجدد سیستم عامل (در هر دو محیط Workgroup & Domain صادق می باشد.)

ولی در تمامی موارد فوق گفته شده فوق می توانید با استفاده از کاربری که آن را در نقش مامور بازیابی به کامپیوتر معرفی می نمایید اقدام به Recovery نمودن دیتاهای رمزگذاری شده کاربران نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

بررسی استفاده از EFS

همچنین می توانید با Export گرفتن از Private Key هر کاربر و نگه داری آن در جایی امن در صورت به وجود آمدن هر مشکلی اقدام به Import مجدد بر روی کامپیوتر نمایید، بنابراین اگر مدیر شبکه از موضوع Encrypt شدن اطلاعات آگاهی داشته باشد می تواند با استفاده از راهکارهایی که گفته شد مانع از دست رفتن اطلاعات کاربر گردد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

اطلاع از فایل های Encrypt شده

اگر بخواهید یک کامپیوتر را از نظر داشتن دیتا های Encrypt شده مورد بررسی قرار دهید، در این حالت می بایست از راه حل زیر استفاده نمایید، فرض نمایید که می خواهید کامپیوتر یک کاربر را مورد بررسی قرار دهید که آیا بر روی آن کامپیوتر فایل هایی به صورت Encrypt شده وجود دارد و یا خیر؟

در این حالت بررسی تمامی فایل های کاربر امری محال به نظر می رسد، بنابراین از روش توضیح داده شده در صفحه بعد می بایست استفاده نمایید:

www.ParsBook.org

WWW.SOFTGOZAR.COM

اطلاع از فایل های Encrypt شده

برای بررسی و آگاهی از اینکه آیا یک کاربر بر روی کامپیوتر فایل های خود را به صورت Encrypt شده درآورده است و یا خیر، می بایست از ریجستری ویندوز استفاده نمایید.

برای این منظور وارد ریجستری ویندوز شده (استفاده از دستور Regedit) و سپس مسیر زیر را پیدا نمایید:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\EFS

www.ParsBook.org

WWW.SOFTGOZAR.COM

اطلاع از فایل های Encrypt شده

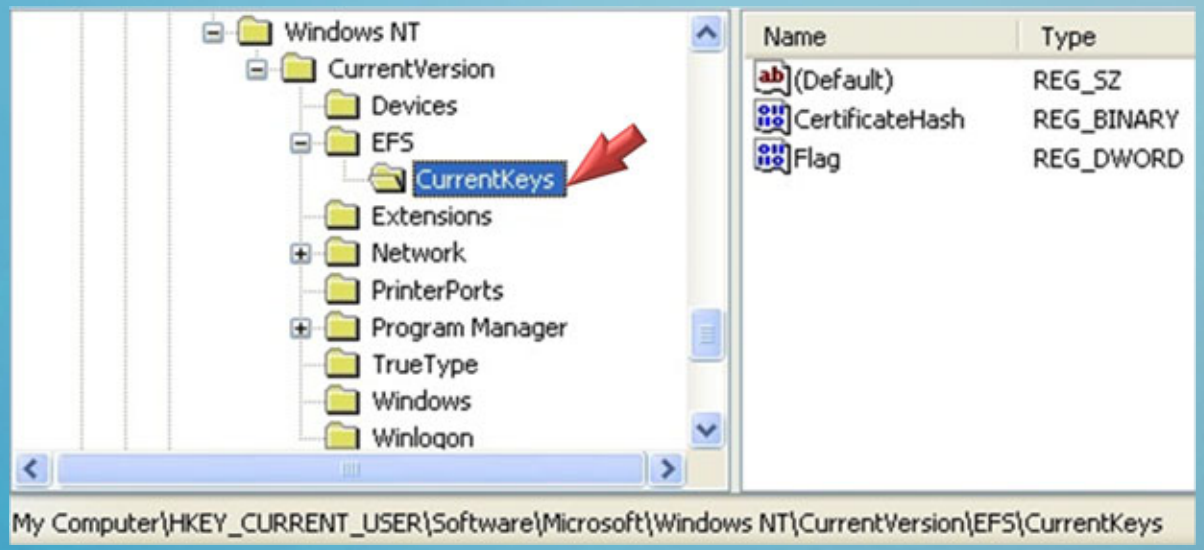
اگر کاربر بر روی کامپیوتر فایل های Encrypt شده نداشته باشد قسمت EFS را در قسمت CurrentVersion مشاهده نخواهید کرد:

www.ParsBook.org

WWW.SOFTGOZAR.COM

اطلاع از فایل های Encrypt شده

ولی در شکل فوق نمایی از EFS را به همراه دو کلیدی که وجود دارد را مشاهده می نمایید:



بنابراین کاربر بر روی کامپیوتر از فایل ها رمزگذاری شده استفاده می نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Disable کردن EFS

برای Disable نمودن استفاده از قابلیت EFS برای کامپیوترهای دامین می بایست در Group Policy وارد قسمت زیر شوید:

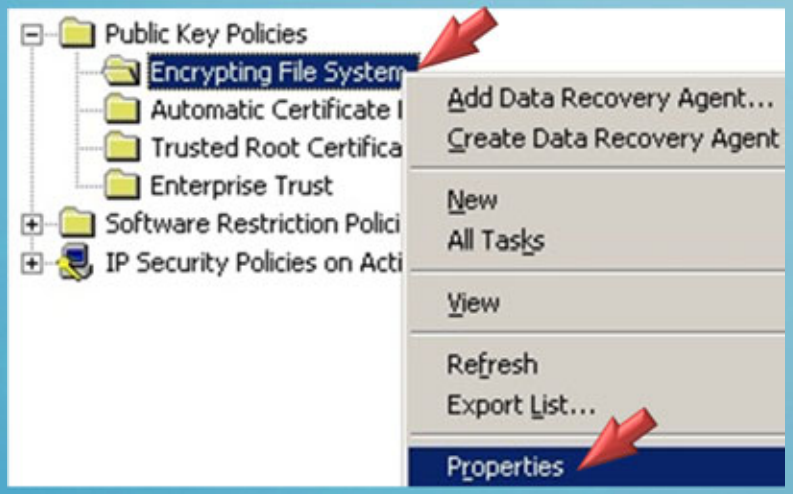
- Computer Configuration\ Windows Settings\ Security Settings\ Public Key Policies\ Encrypting File System

www.ParsBook.org

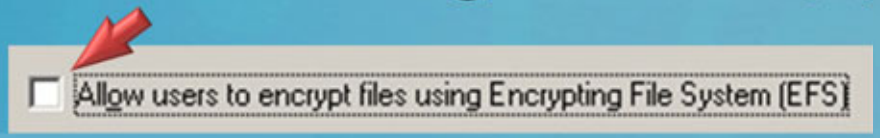
WWW.SOFTGOZAR.COM

Disable کردن EFS

سپس بر روی قسمت Encrypting File System راست کلیک کرده و سپس Properties را انتخاب نمایید:



در ادامه می بایست چک مارک گزینه زیر را از حالت انتخاب خارج نمایید:



www.ParsBook.org

WWW.SOFTGOZAR.COM

Disable کردن EFS

در ادامه دستور Gpupdate را اجرا و سپس کلاینت ها را restart نمایید تا تغییرات بر روی آنان اعمال گردد.

در صورتی که بخواهید بر روی یک Local Computer قابلیت EFS را Disable نمایید تا هیچ کاربری نتواند فایل های خود را Encrypt نمایید می بایست از ریجستری و مراحل مختص به آن استفاده نمایید.

این مراحل را در ادامه مورد بررسی قرار می دهیم.

www.ParsBook.org

WWW.SOFTGOZAR.COM

Disable کردن EFS

برای Disable نمودن استفاده از قابلیت EFS در کامپیوترهای (Workgroup) می بایست وارد مسیر زیر از ریجستری شوید:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EFS\

سپس می بایست یک New DWORD value بنام زیر ساخته و مقدار (0x01) را برای آن ست نمایید:

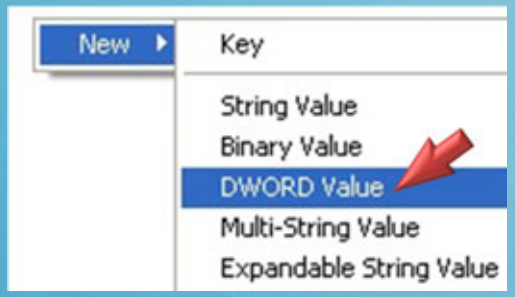
- EfsConfiguration

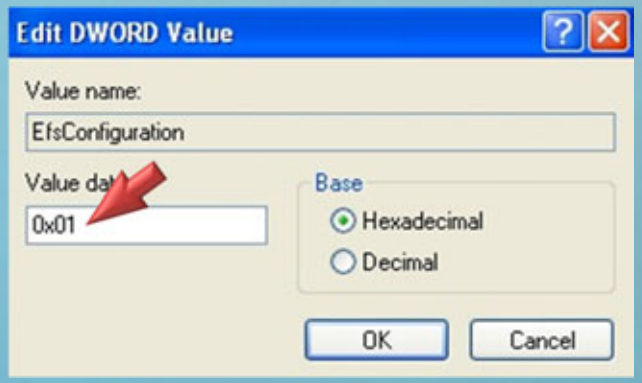
www.ParsBook.org

WWW.SOFTGOZAR.COM

Disable کردن EFS

در شکل های زیر نمایی از کلید موردنظر را که می بایست ایجاد نمایید و Value را که باید به آن تخصیص دهید را مشاهده می نمایید:





در شکل های فوق نوع Value و مقدار آن را مشاهده می نمایید. (بعد از ست کردن کلید فوق یک بار کامپیوتر را Restart نمایید)

www.ParsBook.org

WWW.SOFTGOZAR.COM

Disable کردن EFS

بعد از راه اندازی مجدد کامپیوتر در صورتی که (حتیAdministrator) بخواهد فایلی را Encrypt نمایید با پیغام خطای زیر مواجه می گردد:

در این پیغام به این نکته اشاره شده است که قابلیت Encryption برای کامپیوتر فوق غیر فعال می باشد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

نکته

فایل هایی که تا قبل از مشخص کردن کلید ریجستری به صورت Encrypt شده درآمده بودند به همان صورتقبلی (یعنی Encrypt شده کماکان باقی خواهند ماند)

ولی باید توجه داشته باشید:

که امکان دسترسی به آنان دیگر وجود نخواهد داشت!!!!

در صورتی که بخواهید مجدداً به فایل های Encrypt شده قبلی دسترسی داشته باشید، می بایست کلید ریجستری را که ایجاد شده است را Delete کرده و سپس یک بار کامپیوتر را Restart نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

نکته

همچنین می توانید برای سهولت از انجام عمل ایجاد کلید در ریجستری دستور زیر را وارد نمایید:

- **reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS" /v EfsConfiguration /t REG_DWORD /d 1 /f**

با اجرای دستور فوق کلید مختص به Disable شدن Encryption در ریجستری اضافه می گردد.

www.ParsBook.org

WWW.SOFTGOZAR.COM

نکته

در شکل زیر نمایی از اجرای دستور مختص به ایجاد کلید برای Disable نمودن قابلیت EFS را مشاهده می نمایید:

```
C:\>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS" /v EfsConfig
uration /t REG_DWORD /d  1 /f

The operation completed successfully
```

www.ParsBook.org

WWW.SOFTGOZAR.COM

غیر فعال کردن Encryption در Windows 7

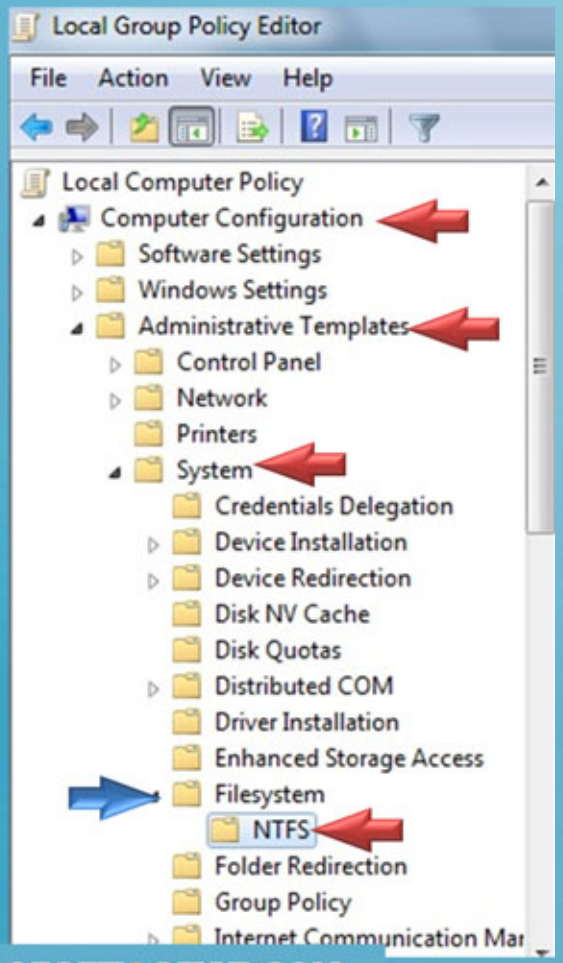
شرایطی که بیان شده مختص به غیر فعال نمودن قابلیت Encryption در Windows XP از طریق Registry می باشد، ولی در Windows 7 می توانید از طریق Group Policy اقدام به غیر فعال نمودن Encryption برای کاربران نمایید.

www.ParsBook.org

WWW.SOFTGOZAR.COM

غیر فعال کردن Encryption در Windows 7

برای این منظور وارد Group Policy شوید با استفاده از gpedit.msc و سپس وارد مسیر مشخص شده در عکس زیر شوید:



www.ParsBook.org

WWW.SOFTGOZAR.COM

غیر فعال کردن Encryption در Windows 7

Policy را که می بایست به صورت Enable ست نمایید در زیر مشخص شده است:

Setting	State
Do not allow compression on all NTFS volumes	Not configured
Do not allow encryption on all NTFS volumes	Not configured
Enable NTFS pagefile encryption	Not configured
Short name creation options	Not configured

Policy فوق را باز کرده و به صورت Enable ست نمایید، یک بار کامپیوتر را راه اندازی مجدد نمایید، تا امکان Encrypt نمودن فایل ها دیگر میسر نباشد!!!

www.ParsBook.org

WWW.SOFTGOZAR.COM

تمرین عملی

در تمرین عملی مختص به مالتی مدیای آموزشی به بررسی چگونگی غیر فعال نمودن قابلیت Encryption در محیط های شبکه ایی Workgroup & Domain تحت دو سیستم عامل Windows XP & 7 خواهیم پرداخت.

www.ParsBook.org

WWW.SOFTGOZAR.COM

تمرین عملی

- پیاده سازی غیرفعال نمودن Encryption برای تمامی کامپیوترهای دامین
- غیر فعال نمودن Encryption برای کامپیوترهای Local تحت Windows XP & 7
- بررسی شرایط فایل های رمزنگاری شده بعد از غیر فعال شدن Encryption

www.ParsBook.org

برای تهیه محصولات آموزشی

به صورت مالتی مدیا

(شامل کلیه دروس تئوری و عملی)

لطفا به سایت

www.modir-shabake.com

مراجعه فرمایید

www.PartsBook.org

برای تهیه کتاب الکترونیک از دوره های

(Net+,Windows XP,Windows Server 2003)

www.PartSBook.org

لطفا به سایت

www.modir-shabake.com

مراجعه فرمایید

مشخصات محصولات آموزشی مالتی مدیا تخصصی شبکه

- آموزش تئوری فارسی و انگلیسی مطالب (همراه با عکس)
- آموزش عملی کلیه مطالب تئوری (در قالب تمرین عملی)
- آموزش پیاده سازی مطالب در قالب سناریو های عملی و کاربردی
- آموزش نرم افزارهای جانبی (مرتبط با مفاهیم آموزشی)

www.ParsBook.org

محصولات آموزشی تخصصی مهندسی شبکه

- کتاب الکترونیک دوره های آموزشی Net+,Windows XP,Server 2003
- کتاب الکترونیک دوره آموزشی ارتقاء Windows Server 2003 to Windows Server 2008
- مالتی مدیا دوره آموزشی Windows XP
- مالتی مدیا دوره آموزشی Windows Server 2003
- مالتی مدیا دوره آموزشی ارتقاء Windows XP to Widows 7
- مالتی مدیا دوره آموزشی ارتقاء Windows Server 2003 to Windows Server 2008

www.ParsBook.org