怪招迭出Vista系统下用cipher命令加密 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/246/2021_2022__E6_80_AA_E6_8B_9B_E8_BF_AD_E5_c100_246628.htm CIPHER [/E | /D | /C] [/S:directory] [/B] [/H] [pathname [……]] CIPHER /K CIPHER /R:filename [/SMARTCARD] CIPHER /U [/N] CIPHER /W:directory CIPHER /X[:efsfile] [filename] CIPHER /Y CIPHER /ADDUSER [/CERTHASH:hash | /CERTFILE:filename] [/S:directory] [/B] [/H] [pathname [……]] CIPHER /REMOVEUSER /CERTHASH:hash [/S:directory] [/B] [/H] [pathname [……]] CIPHER /REKEY [pathname [……]] /B 如果遇到错误则中止。 在默认方式下，即使遇到错误，CIPHER 也会继续执行。 /C 显示关于加密文件的信息。 /D 解密指定的文件或目录。 /E 加密指定的文件或目录。会标记目录，这样随后添加的文件就会被加密。如果父目录没有被加密，则当修改加密的文件时该文件将被解密。建议您给此文件和父目录加密。 /H 用隐藏或系统属性显示文件。在默认方式下，会忽略这些文件。 /K 创建新的证书和密钥以便使用 EFS。如果选择了此选项，会忽略所有其他选项。 /N 此选项只能与 /U 使用。这将阻止更新密钥。此选项用于查找本地磁盘上所有加密文件。 /R 生成一个 EFS 恢复代理密钥和证书，然后将它们写入一个 .PFX 文件(包含证书和私钥)和一个 .CER 文件(只包含证书)。管理员可以向 EFS恢复策略添加 .CER 内容，为用户创建恢复代理并导入.PFX 来恢复单独文件。 如果指定 SMARTCARD，然后将恢复密钥和证书写入智能卡生成 CER 文件（只包含证书）未生成PFX文件。 /S 在给定目录和所有

子目录执行指定的操作。 /U 尝试包括本地磁盘上所有加密的文件。如果用户文件加密密钥或恢复代理的密钥改变，这会将其更新为当前的密钥。除了 /N 外，此选项不能与其他选项一起使用。 /W 从整个卷上所有没有使用的磁盘空间删除数据。如果选择了此选项，会忽略其他选项。指定的目录可以位于本地卷上的任意位置。如果它是装入点或指向另一个卷上的目录，此卷上的数据将被删除。 /X 将 EFS 证书和密钥备份成文件的文件名。如果提供了 EFS 文件，将会备份当前用户的、用于加密此文件的证书。否则，将会备份用户当前的EFS 证书和密钥。 /Y 在本地 PC 上显示当前的 EFS 证书缩略图。 /ADDUSER 向指定的加密文件中添加用户。 如果提供了CERTHASH，密码将搜索带有此SHA1 哈希的证书。 如果提供了 CERTFILE，密码将从文件中提取证书。 /REKEY 更新指定的加密文件以使用配置的 EFS 当前密钥。 /REMOVEUSER 从指定文件中删除用户。 CERTHASH必须是要删除的证书的SHA1 哈希。 directory 目录路径。 filename 没有扩展名的文件名。 pathname 指定一个模式、文件或目录。 efsfile 加密的文件路径。 不用参数时，CIPHER 显示当前目录和它包含文件的加密状态。您可以使用几个目录名和通配符。多个参数之间必须有空格。