Decryption in Windows: A Comprehensive Guide

In today's digital world, encryption plays a crucial role in protecting sensitive information from unauthorized access. However, there are situations where decryption becomes necessary, whether it's to recover forgotten passwords, access encrypted files, or investigate potential security breaches. This article aims to provide a comprehensive guide to decryption in the Windows environment, covering various scenarios and techniques applicable to Windows operating systems.

Examples:

1. Decrypting Encrypted Files:
    - Using Windows Explorer: In Windows, encrypted files can be decrypted by right-clicking on the file, selecting "Properties," and then clicking on the "Advanced" button under the "General" tab. From there, uncheck the "Encrypt contents to secure data" option and apply the changes.
    - Command Prompt: The "cipher" command in Command Prompt can be used to decrypt files and folders. For example, to decrypt a folder named "Documents," the command "cipher /d /s:C:\Path\to\Documents" can be executed.

2. Decrypting BitLocker-Protected Drives:
    - Using BitLocker Drive Encryption: BitLocker is a built-in encryption feature in Windows that allows users to encrypt entire drives. To decrypt a BitLocker-protected drive, open the BitLocker Drive Encryption control panel, select the drive, and click on the "Turn Off BitLocker" option. Follow the on-screen instructions to complete the decryption process.

3. Decrypting EFS-Encrypted Files:
    - Using Command Prompt: The "cipher" command can also be used to decrypt files encrypted with the Encrypting File System (EFS). For example, executing the command "cipher /d /a:C:\Path\to\File.txt" will decrypt the specified file.
    - Using PowerShell: In PowerShell, the "Unprotect-CmsMessage" cmdlet can be used to decrypt EFS-encrypted files. For instance, the command "Unprotect-CmsMessage -Path C:\Path\to\File.txt" will decrypt the file.