SQL Server 2005 Integration Services (SSIS) provides six package-protection options that pull together the concepts of sensitive-data protection and encryption.

***Encrypt all data with password.*** This option tells SSIS to encrypt the entire package with a password that you provide. The password, which is the encryption key, isn't stored in the package. No user can open the package without the password, and you can't recover a password-encrypted package without the password. This option is useful when you have intellectual property in a package or when you're sending packages across unencrypted channels such as email. The receiving party must know the password, which you can provide in a separate message or through a different medium. Encrypting an entire package hides more data than encrypting only the sensitive data, so a fully encrypted package is safer than a partially encrypted one.

***Encrypt sensitive data with password.*** This option tells SSIS to encrypt only those properties that are marked as sensitive, as I described in the main article. This option is useful if you're interested in protecting only the sensitive data in the package and not any of the other data or package logic.

***Encrypt all data with user key.*** This option is essentially the same as *Encrypt all data with password*, except that the user key is the encryption key. Only the person who saved the package with this option can open it and only on the same machine. This option is the default because it's the most transparent for developing packages, but you should choose the user-key encryption option only when you want to prevent anyone besides yourself from opening the package. Once the package is complete and ready to be deployed, you should consider switching to a different encryption option. If you create a package with this encryption mode, then attempt to share the package with others, they won't be able to open it on their machines.

***Encrypt sensitive data with user key.*** This option is similar to the *Encrypt all data with user key* option, except the user key encrypts only sensitive properties. Users other than the person who saved the package can open packages encrypted at this level, but they'll need to overwrite all sensitive data in the package.

***Do not save sensitive data.*** This option, which eliminates all sensitive data from the package, is useful when you want to purge all passwords from a package. For example, if you write a sample package to share with others or you want to post a package to a support forum to have someone troubleshoot it for you, you can use this option to ensure that you won't share any passwords.

***Rely on server storage for encryption.*** If you use this option, SSIS won't strip out or encrypt any part of the package; you're essentially saying that you want to use SQL Server security to protect your sensitive data. Because SSIS always communicates with SQL Server through an encrypted channel, SSIS won't transmit your sensitive data to SQL Server in clear text. This option is available only when you're saving the package to SQL Server.