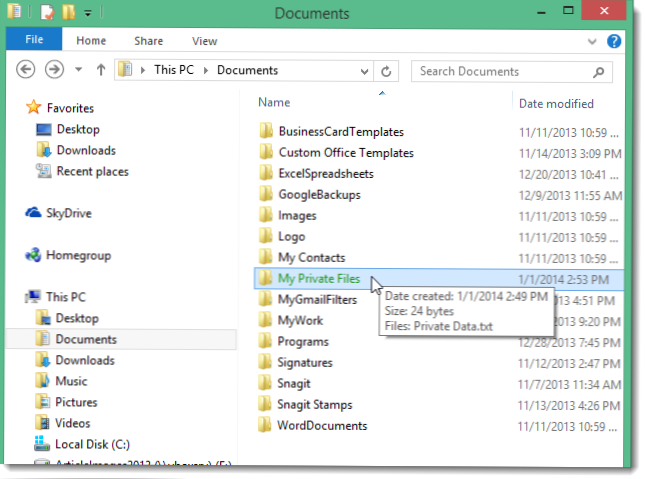
**EFS - system szyfrowania plików**

System szyfrowania plików (**EFS**) może szyfrować pliki na woluminie **NTFS**, których nie można używać chyba że użytkownik ma dostęp do **kluczy wymaganych** do odszyfrowania informacji. Domyślnie, kiedy zaszyfrujesz plik za pomocą **EFS**, plik lub folder zmieni kolor na **zielony**, aby pokazać, że plik jest **zaszyfrowany.**(rys.1) Po zaszyfrowaniu pliku nie trzeba wcześniej ręcznie odszyfrowywać zaszyfrowanego pliku, można go używać tak jakby nie był zaszyfrowany. Po otwarciu pliku zaszyfrowanego przy użyciu **EFS** plik jest **automatycznie odszyfrowywany** w razie potrzeby. Jeśli jednak inny użytkownik próbuje uzyskać dostęp do tego samego pliku, **nie może go otworzyć**, ponieważ nie ma odpowiedniego klucza, aby otworzyć plik. **EFS** używa **klucza szyfrowania** do szyfrowania danych, które są przechowywane w **certyfikacie cyfrowym.** Gdy użytkownik po raz pierwszy szyfruje plik lub folder, tworzony jest **certyfikat** i **klucz szyfrowania** powiązany z kontem użytkownika. Użytkownik, który utworzył plik, **jest jedyną osobą**, która może go odczytać. Podczas pracy użytkownika, **EFS** szyfruje pliki za pomocą klucza wygenerowanego z **klucza publicznego** użytkownika. Dane zaszyfrowane tym kluczem można odszyfrować tylko za pomocą **klucza prywatnego**.



Zaszyfrowany plik (rys.1)

**Podczas pracy z EFS pamiętaj o następujących kwestiach:**

• Możesz szyfrować lub kompresować pliki NTFS tylko wtedy, gdy używasz EFS; nie możesz zrobić obu. Jeśli użytkownik oznacza plik lub folder do zaszyfrowania, ten plik **lub** folder jest zdekompresowany.

• Jeśli zaszyfrujesz plik, zostanie on automatycznie odszyfrowany, jeśli skopiujesz lub przeniesiesz plik do wolumin, który nie jest wolumin, który nie jest woluminem NTFS.

• Przeniesienie niezaszyfrowanych plików do zaszyfrowanego folderu automatycznie powoduje takie pliki zaszyfrowane w nowym folderze.

• Przeniesienie zaszyfrowanego pliku z folderu zaszyfrowanego przez EFS nie powoduje automatycznego odszyfrowania. Zamiast tego musisz jawnie odszyfrować plik.

• Pliki oznaczone atrybutem System lub znajdujące się w katalogu znajdujące się w katalogu głównym nie mogą być zaszyfrowane.

• Pamiętaj, że zaszyfrowany folder lub plik nie chroni przed usunięciem pliku

**BitLocker**

Szyfrowanie dysków funkcją **BitLocker** **(BDE)** to funkcja, która może korzystać z zaufanego komputera. Platform Module (**TPM**), czyli mikroczip wbudowany w komputer. To jest używane do **przechowywania** informacji kryptograficznych, takich jak **klucze szyfrowania**. Informacje przechowywane w **Moduł** **TPM** może być bardziej zabezpieczony przed atakami z zewnątrz i kradzieżą fizyczną. Szyfrowanie dysków funkcją **BitLocker** przechowuje również pomiary podstawowych plików systemu operacyjnego w module **TPM**. Wymagania systemowe funkcji **BitLocker** to:

Posiadaj co najmniej dwie partycje: jedną systemową i drugą tą na której będą zaszyfrowane dane. Komputer musi mieć system BIOS zgodny z TPM i obsługujący USB urządzeń podczas uruchamiania komputera.

Gdy używasz funkcji **BitLocker** na stałych i wymiennych dyskach danych, które nie są woluminem systemu operacyjnego, możesz użyć jednego z następujących sposobów szyfrowania:

**• Hasło**

**• Karta inteligentna**

**• Automatyczne odblokowanie**

Panelu sterowania funkcji **BitLocker** umożliwia odzyskanie klucza szyfrowania i odzyskiwanie

hasło do woli. Po użyciu funkcji **BitLocker** do szyfrowania dostępne są następujące opcje

napęd:

• **Utwórz kopię zapasową klucza odzyskiwania**

**• Zmień hasło**

**• Dodaj kartę inteligentną**

**• Wyłącz BitLocker**