



Szyfrowanie plików i folderów

Windows 7 - szybkie szyfrowanie

- Szyfrowanie plików i katalogów to jedna z metod zabezpieczania danych oferowana przez system. Gwarantuje ona, że nawet po kradzieży komputera czy dysku złodziej nie będzie mógł sprawdzić ich zawartości.



Windows 7 - szybkie szyfrowanie

- Gdy mowa o szyfrowaniu danych w systemach Windows, należy przede wszystkim zacząć od najpopularniejszego rozwiązania: **podsystemu EFS**. Jest to technika pozwalająca każdemu zalogowanemu użytkownikowi szyfrować swoje pliki i foldery.



Windows 7 - szybkie szyfrowanie

- **EFS dostępny** jest tylko w droższych edycjach Windows 7: Professional, Enterprise (dostępnej tylko na zasadach licencjonowania zbiorowego, przeznaczonego dla firm) oraz najdroższej Ultimate.



Windows 7 - szybkie szyfrowanie

- Szyfrowanie **EFS** ma sens wyłącznie w przypadku, gdy konto jest chronione silnym hasłem.
- W jaki sposób EFS szyfruje dane, skoro nie trzeba wprowadzać żadnego klucza? Nie będziemy tutaj szczegółowo przedstawiać całego procesu, skupimy się jedynie na **podstawowych etapach**.

Szyfrowanie EFS

- W momencie pierwszego żądania szyfrowania obiektu system tworzy dla zalogowanego użytkownika osobisty certyfikat zawierający parę kluczy **(publiczny/prywatny)**.

Szyfrowanie EFS

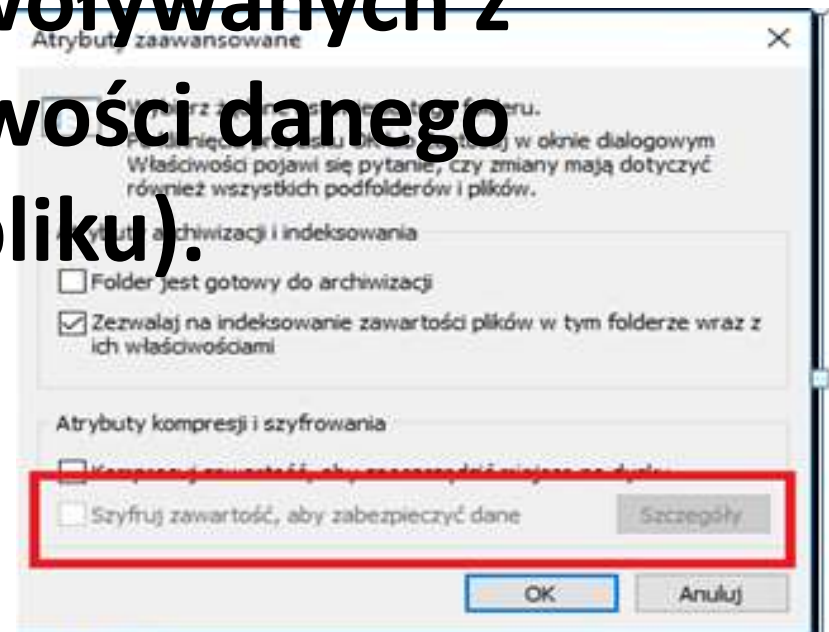
- W tym samym momencie generowany (losowo) jest klucz szyfrowania, tzw. File Encryption Key (**FEK**).
- Za jego pomocą Windows szyfruje wybrane pliki i foldery. Następnie system szyfruje FEK za pomocą klucza publicznego należącego do zalogowanej osoby.

Szyfrowanie EFS

- **Aby odszyfrować dane**, trzeba najpierw odszyfrować FEK – do tego celu wykorzystywany jest klucz prywatny przechowywany w certyfikacie użytkownika.

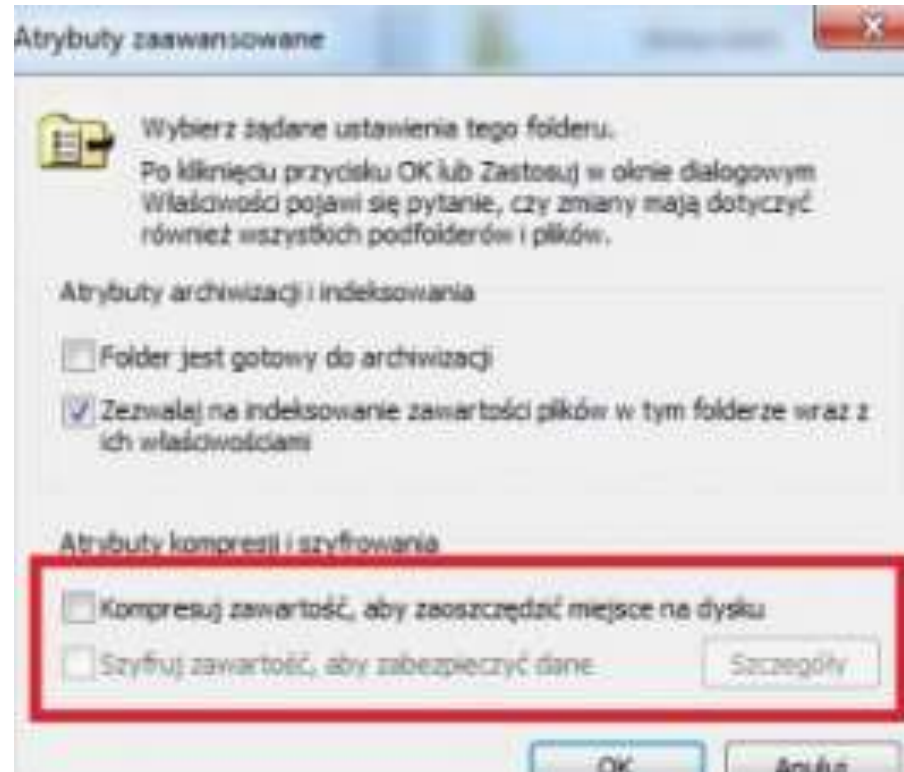
Szyfrowanie EFS

- Zabezpieczanie plików czy folderów za pomocą EFS jest proste. Polega na zaznaczeniu odpowiedniego pola wyboru w jednym z okien **wywoływanych z poziomu okna właściwości danego obiektu (folderu lub pliku)**.



kompresowanie

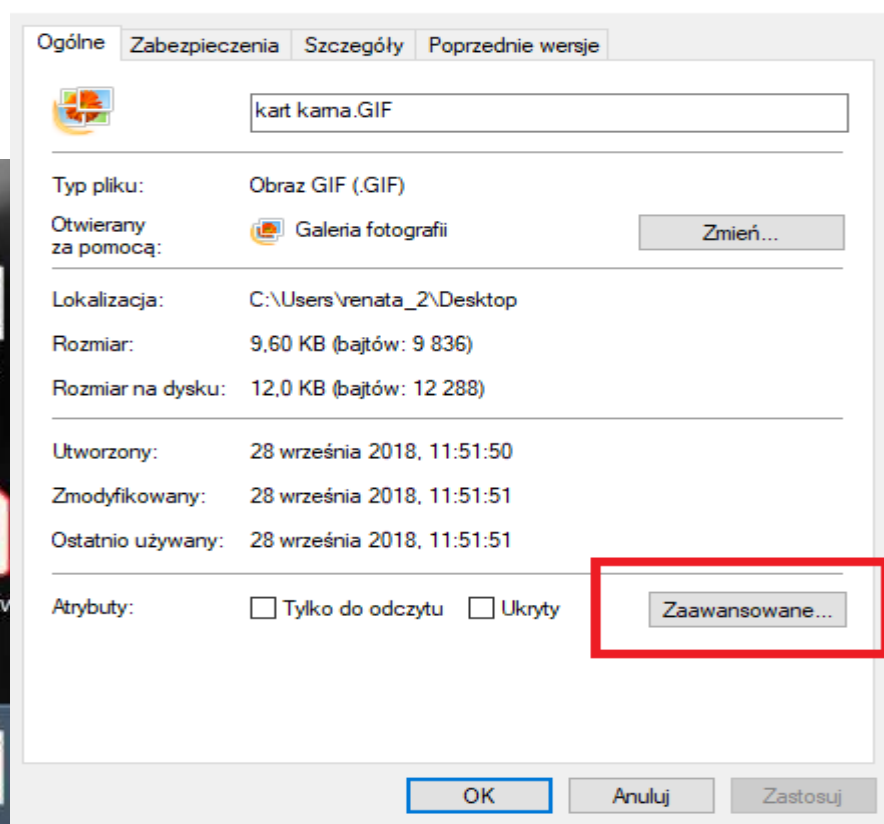
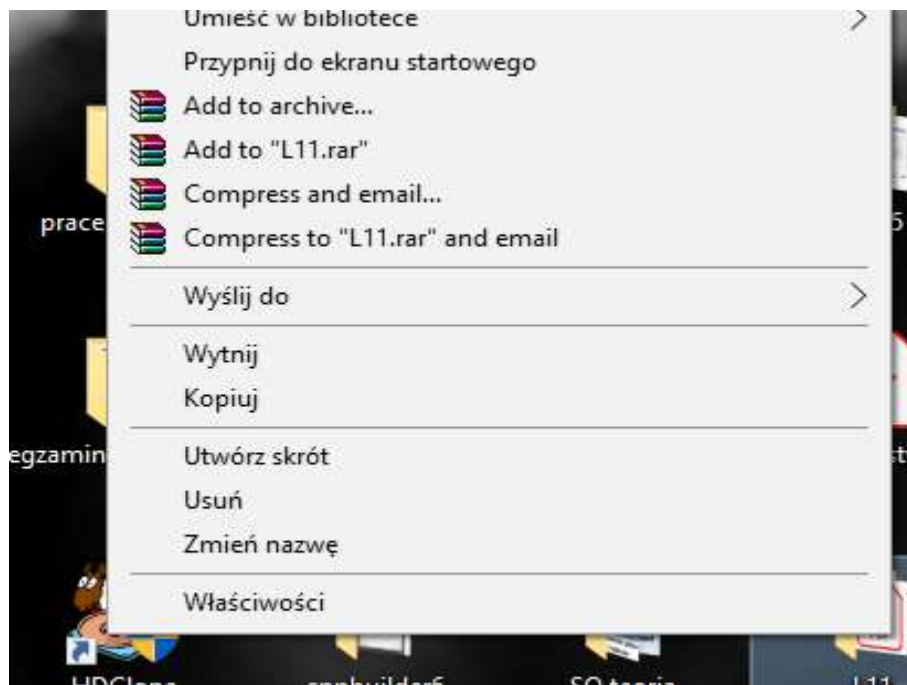
- W tym samym oknie można również włączyć kompresowanie danego pliku lub folderu, ale uniemożliwi to zaszyfrowanie takiego obiektu.



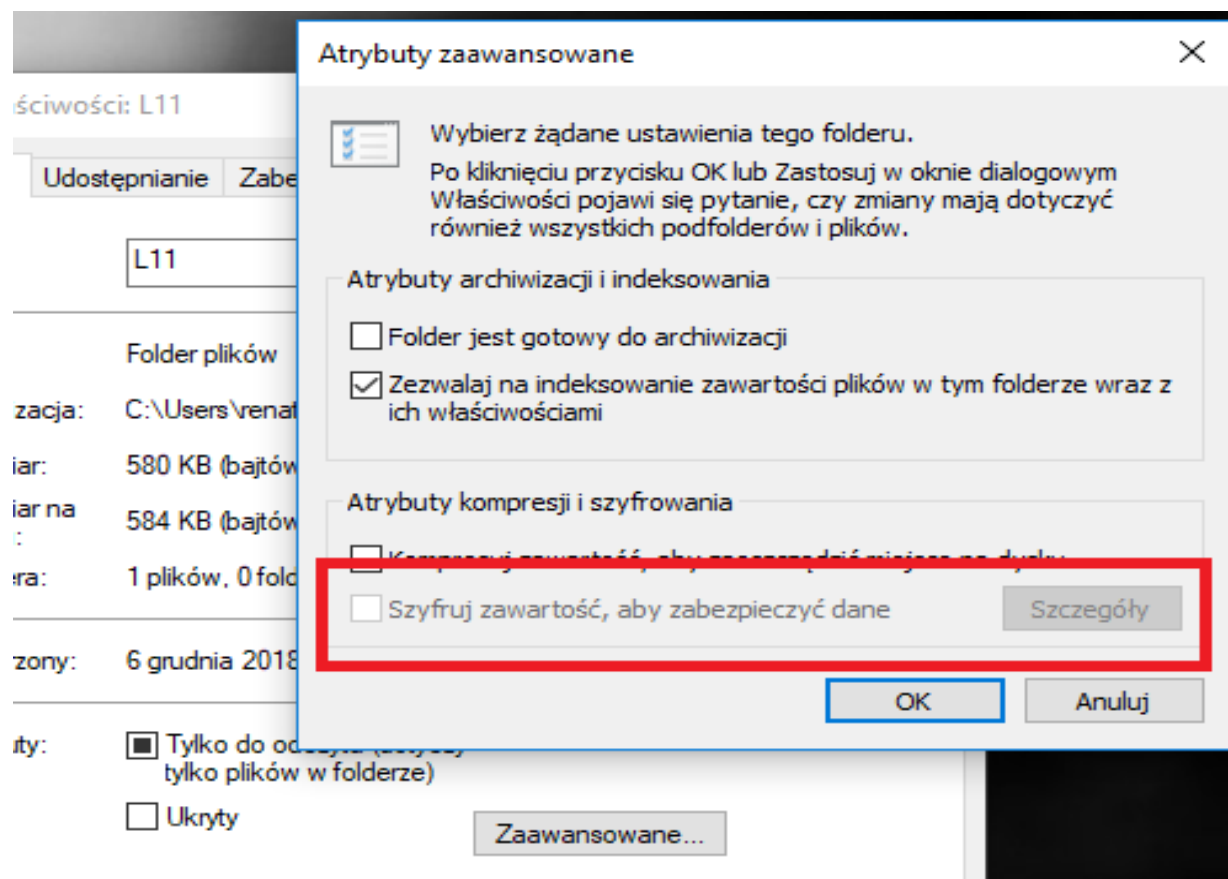
Kompresja i szyfrowanie to dwie wzajemnie wykluczające się funkcje systemu plików NTFS.

Windows 7 - szybkie szyfrowanie

- Aby zaszyfrować plik bądź katalog, kliknij go prawym przyciskiem myszy, wybierz polecenie Właściwości i przycisk Zaawansowane na karcie Ogólne.



- **Zaznacz Szyfruj zawartość, by zabezpieczyć pliki i zaakceptuj zmiany przyciskiem OK.**



Jak szyfrować dane (Windows 7)



Szyfrowanie plików i folderów korzystając z konsoli CMD

- Oprócz funkcji EFS wbudowanych w standardowy Eksplorator Windows do dyspozycji jest działające z wiersza poleceń narzędzie ***cipher.exe***.

Szyfrowanie plików i folderów korzystając z konsoli CMD

- Można za jego pomocą nie tylko szyfrować i deszyfrować obiekty systemu plików, ale również wykonywać inne działania, choćby wymazywać „skasowane” dane z dysku, tak aby nie dało się ich odzyskać.

Polecenie cipher

- Najlepiej korzystać z polecenia cipher, dysponując uprawnieniami administratora.
- **bez parametrów** wyświetla **stan szyfrowania bieżącego folderu i wszystkich znajdujących się w nim plików**.

```
MDOWS\system32>cipher C:\Users\renata_2\Desktop\L11
```

Polecenie cipher

- Wpisując :
- **cipher /e *.***
- zaszyfrujesz wszystkie pliki znajdujące się w bieżącym katalogu.

Polecenie cipher

- Wpisując :
- **cipher /d *.***
- odszyfrujesz wszystkie zasoby dyskowe.

Wyższość polecenia nad GUI

- Bez polecenia cipher nie obejdziesz się w żadnej z wersji Windows (XP, Vista i 7 ...),
- jeśli masz zamiar dokonać zmian na koncie użytkownika - np. zdefiniować nowe hasło dostępu lub usunąć konto jednego z użytkowników. Zaszyfrowane zasoby stałyby się niedostępne w wyniku takiej operacji,
- zatem wcześniej trzeba koniecznie odszyfrować wszystkie pliki.

Polecenie cipher

- Wprawdzie Eksplorator ułatwia odnalezienie zaszyfrowanych plików, zaznaczając je innym kolorem, jednak poszukiwanie zabezpieczonych zasobów we wspomniany sposób okazuje się nad wyraz mozolne i czasochłonne.



Program Files



Kierownik



Polecenie cipher

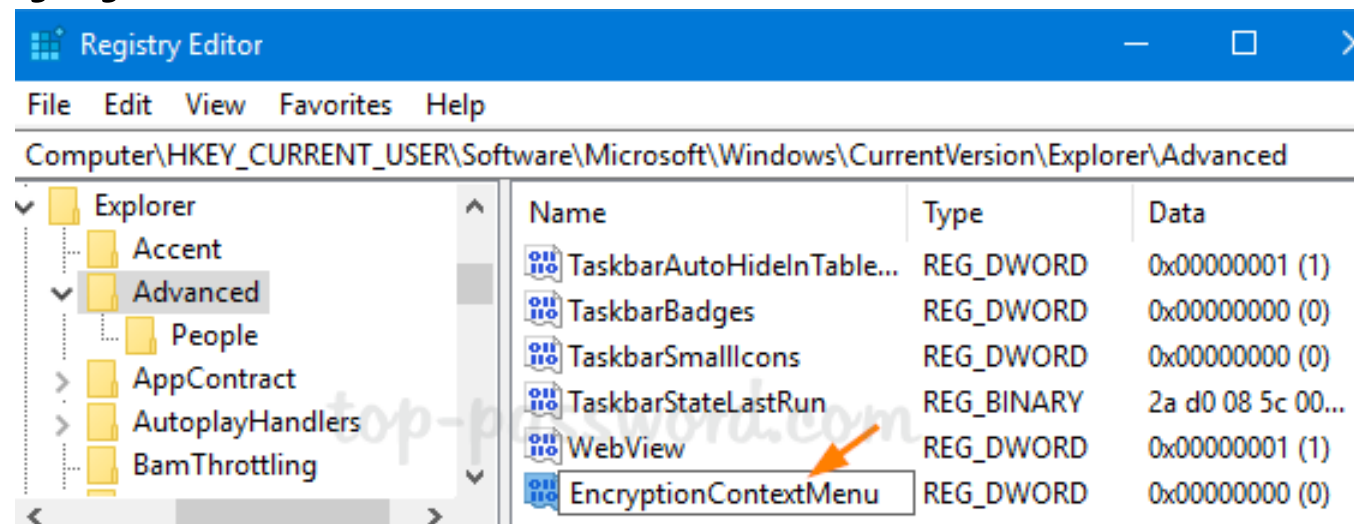
- Wpisując
- **`cipher /d /h /i /s:c:\`**
- odszyfrujesz wszystkie pliki partycji C:
z uwzględnieniem podkatalogów, a także
plików opatrzonych atrybutem "ukryty" lub
"systemowy".

Szyfrowanie plików i folderów korzystając z konsoli CMD

- Podczas codziennej pracy wygodniej jest, oczywiście, korzystać z funkcji szyfrowania za pośrednictwem Eksploratora Windows. Warto wiedzieć, że proces szyfrowania/odszyfrowywania można jeszcze bardziej uprościć, modyfikując nieco rejestr systemu Windows. Wystarczy w kluczu:

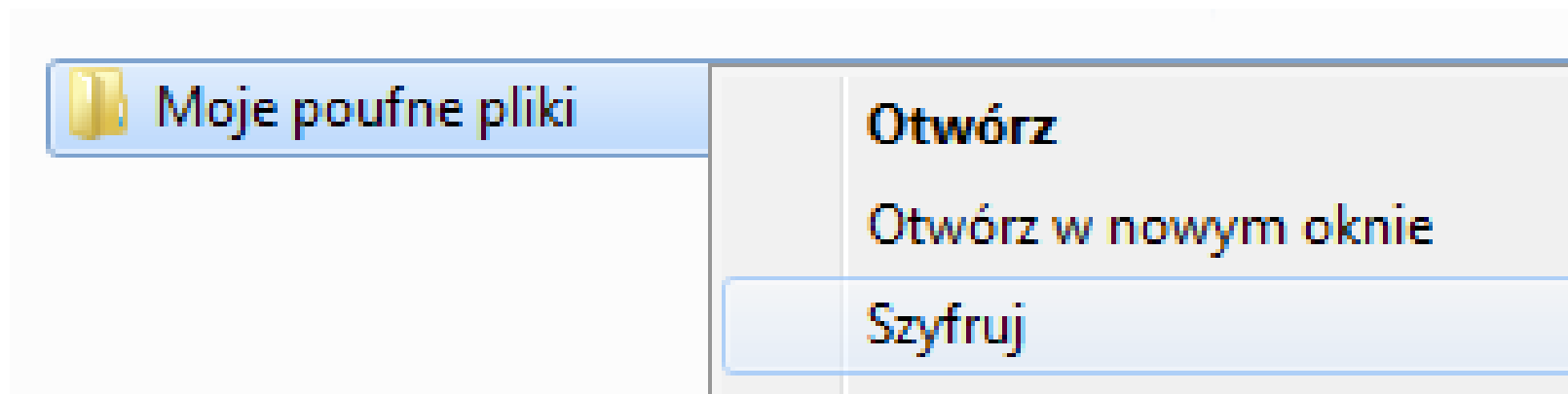
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

- Wystarczy w kluczu:
- *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced*
- utworzyć wartość typu **DWORD** o nazwie *EncryptionContextMenu* i przypisać jej



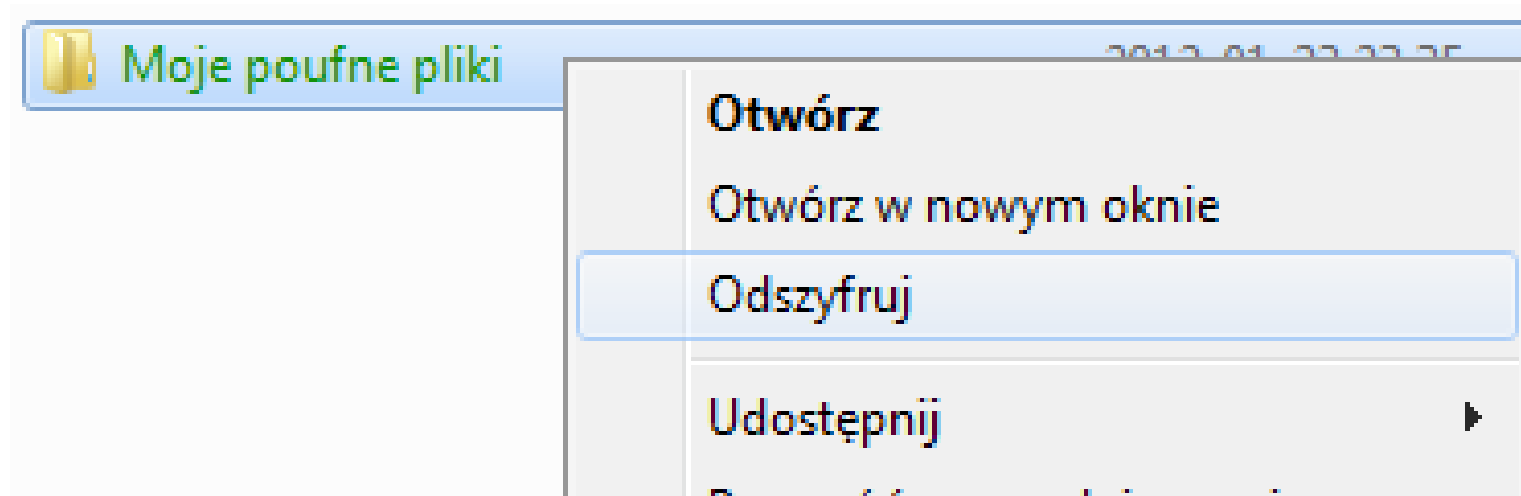
Szyfrowanie plików i folderów korzystając z konsoli CMD

- W przypadku kliknięcia danych niezaszyfrowanych pojawi się w menu kontekstowym Eksploratora nowe polecenie ułatwiające zaszyfrowanie zaznaczonego pliku lub folderu.



Szyfrowanie plików i folderów korzystając z konsoli CMD

- Analogicznie gdy menu kontekstowe wywoływane jest dla obiektu zaszyfrowanego, widoczne będzie polecenie pozwalające odszyfrować go.



Windows BitLocker

- Windows 10 zabezpiecza nośniki, wykorzystując funkcję BitLocker. Pozwala ona na szyfrowanie partycji sektor po sektorze,
- Możemy zaszyfrować partycję systemową, jak również i każdą inną. W przypadku systemowej partycji proces jest bardziej skomplikowany.

Windows BitLocker

Uwaga!

- Funkcja BitLocker jest wbudowana w Windows 7 Ultimate i Enterprise, Windows 8 Pro i Enterprise oraz Windows 10 Pro i Enterprise.

BitLocker – szyfrowanie pendrive'ów i partycji w Windows 10 Pro



Codziennność z szyframi

- W domowych komputerach działających pod kontrolą Windows 7 przeważa wersja Home Premium tego systemu. Jej użytkownicy są pozbawieni zarówno systemu EFS, jak i mechanizmów BitLocker

Codziennność z szyframi

Dlatego w sytuacji, kiedy celem jest ukrycie określonych treści, należy skorzystać z alternatywnych narzędzi do szyfrowania.

Jednym z najpopularniejszych jest udostępniany bezpłatnie **TrueCrypt**

TrueCrypta

Za pomocą **TrueCrypta** można szyfrować całe dyski twarde lub wybrane partycje, a także tworzyć wirtualne szyfrowane dyski na praktycznie dowolnych nośnikach.

TrueCrypta

Możliwe jest również szyfrowanie dysków przenośnych, SSD i flashdysków.

Nie można – jak w przypadku EFS – szyfrować pojedynczych plików lub folderów.

TrueCrypt

TrueCrypt - Testowanie szybkości algorytmów szyfrujących

Bufor: 50 MB Metoda sortowania: Średnia prędkość (malejąco)

Algorytm	Szyfrowanie	Deszyfrow...	Średnia
AES	1.9 GB/s	1.4 GB/s	1.6 GB/s
Twofish	303 MB/s	296 MB/s	299 MB/s
AES-Twofish	277 MB/s	270 MB/s	273 MB/s
Serpent	186 MB/s	176 MB/s	181 MB/s
Serpent-AES	148 MB/s	160 MB/s	154 MB/s
Twofish-Serpent	115 MB/s	114 MB/s	115 MB/s
Serpent-Twofish-AES	106 MB/s	102 MB/s	104 MB/s
AES-Twofish-Serpent	99 MB/s	101 MB/s	100 MB/s

Testuj

Zamknij

Szybkość jest zależna od wydajności procesora i charakterystyki urządzeń składających.

Testy są przeprowadzane w pamięci RAM.

7-Zip

- 7-Zip. Daje możliwość stworzenia samorozpakowalnego archiwum z zaszyfrowanymi plikami. Adresat wiadomości musi znać ustalone przez nas hasło.
- **7-Zip to program głównie do kompresji/dekompresji danych.**