

Instrukcja obsługi szyfrowania dysków

Metoda Szyfrowania oprogramowaniem VeraCrypt oferuje wysoki poziom bezpieczeństwa dla zaszyfrowanych danych i partycji systemowej, a także chroni przed atakami m.in. typu brute-force.

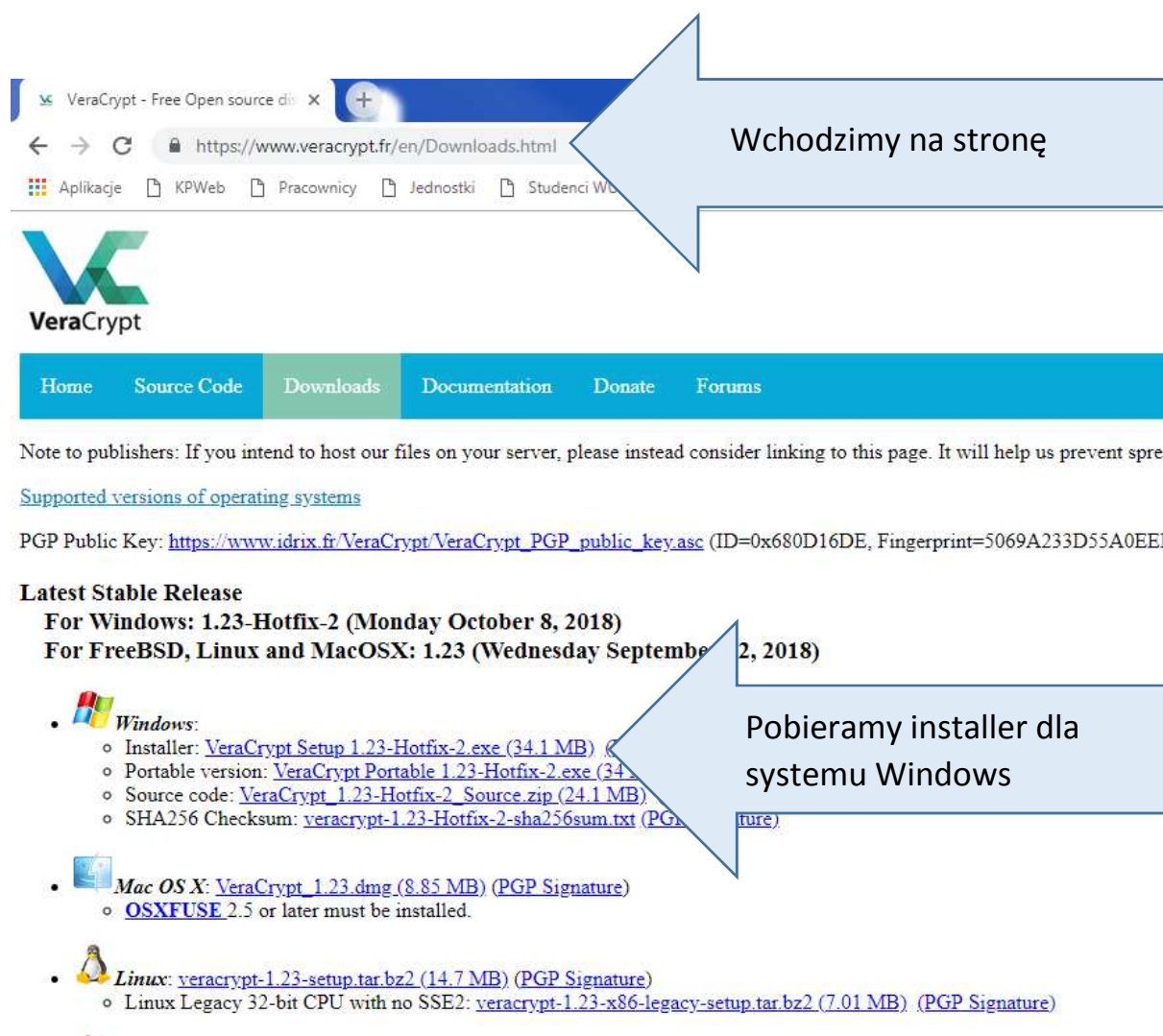
Poniżej opisana funkcja zabezpieczająca opóźnia jedynie otwieranie zaszyfrowanych partycji. **Natomiast nie zmniejsza wydajności pracy podczas użytkowania aplikacji.**

Proces szyfrowanie, może potrwać nawet kilka godzin zależnie od pojemności dysku oraz ilości danych, dlatego zalecane jest uruchomienie w godzinach wieczornych

Przed instalacją proszę przygotować:

- Ładowarkę,
- Płytę CD/DVD,

Do poprawnej instalacji wymagany jest napęd optyczny CD (wewnętrzny lub zewnętrzny), przypadku braku napędu prosimy o kontakt z Centrum Informatyki (ati-inf@wum.edu.pl)



Wchodzimy na stronę

Pobieramy installer dla systemu Windows

VeraCrypt - Free Open source disk encryption software

https://www.veracrypt.fr/en/Downloads.html

Applikacje KPWeb Pracownicy Jednostki Studenci W

VeraCrypt

Home Source Code Downloads Documentation Donate Forums




Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spread of our software.

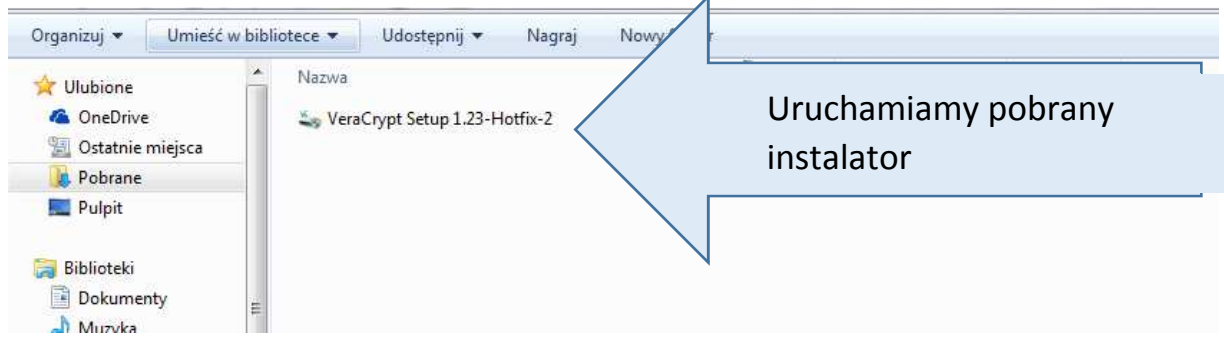
[Supported versions of operating systems](#)

PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x680D16DE, Fingerprint=5069A233D55A0EEB)

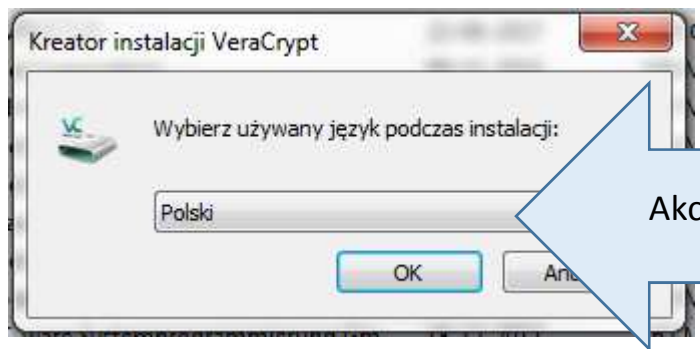
Latest Stable Release

For Windows: 1.23-Hotfix-2 (Monday October 8, 2018)
For FreeBSD, Linux and MacOSX: 1.23 (Wednesday September 27, 2018)

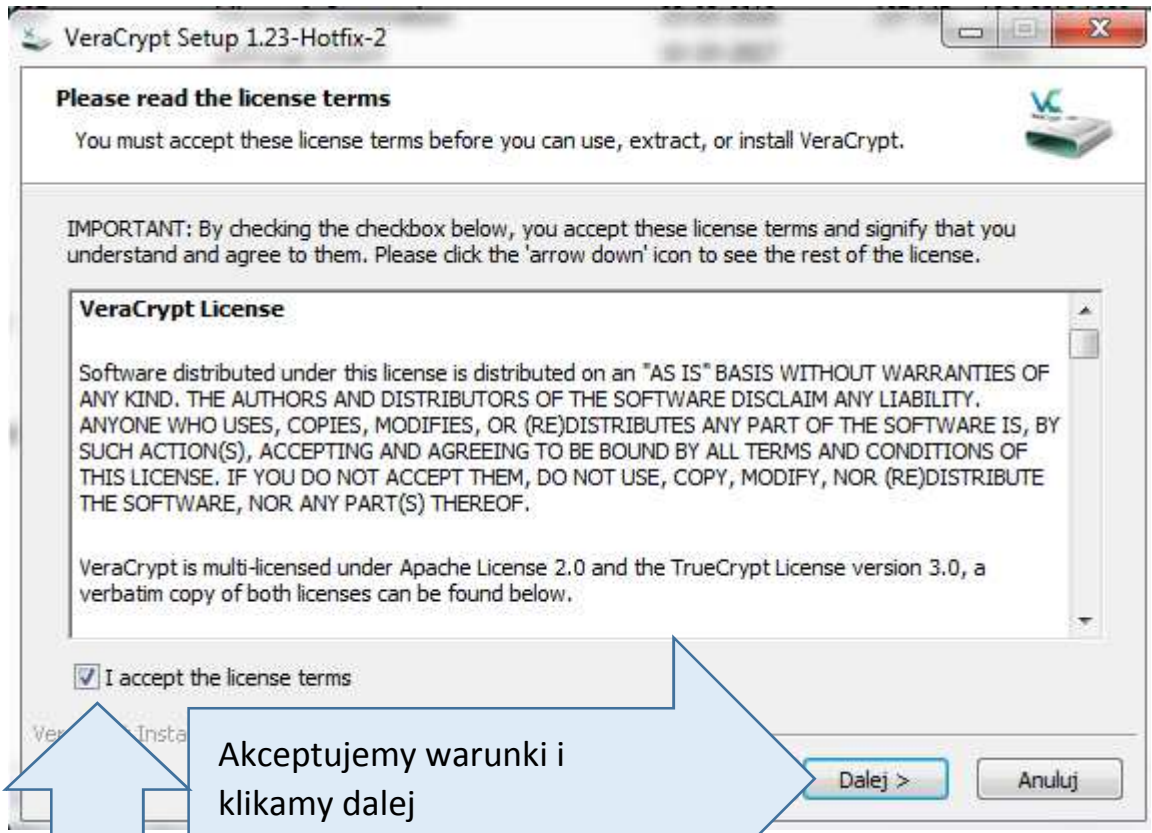
-  **Windows:**
 - Installer: [VeraCrypt Setup 1.23-Hotfix-2.exe \(34.1 MB\)](#) (PGP Signature)
 - Portable version: [VeraCrypt Portable 1.23-Hotfix-2.exe \(34.1 MB\)](#) (PGP Signature)
 - Source code: [VeraCrypt 1.23-Hotfix-2 Source.zip \(24.1 MB\)](#) (PGP Signature)
 - SHA256 Checksum: [veracrypt-1.23-Hotfix-2-sha256sum.txt \(PGP Signature\)](#)
-  **Mac OS X:** [VeraCrypt 1.23.dmg \(8.85 MB\)](#) (PGP Signature)
 - [OSXFUSE 2.5](#) or later must be installed.
-  **Linux:** [veracrypt-1.23-setup.tar.bz2 \(14.7 MB\)](#) (PGP Signature)
 - Linux Legacy 32-bit CPU with no SSE2: [veracrypt-1.23-x86-legacy-setup.tar.bz2 \(7.01 MB\)](#) (PGP Signature)



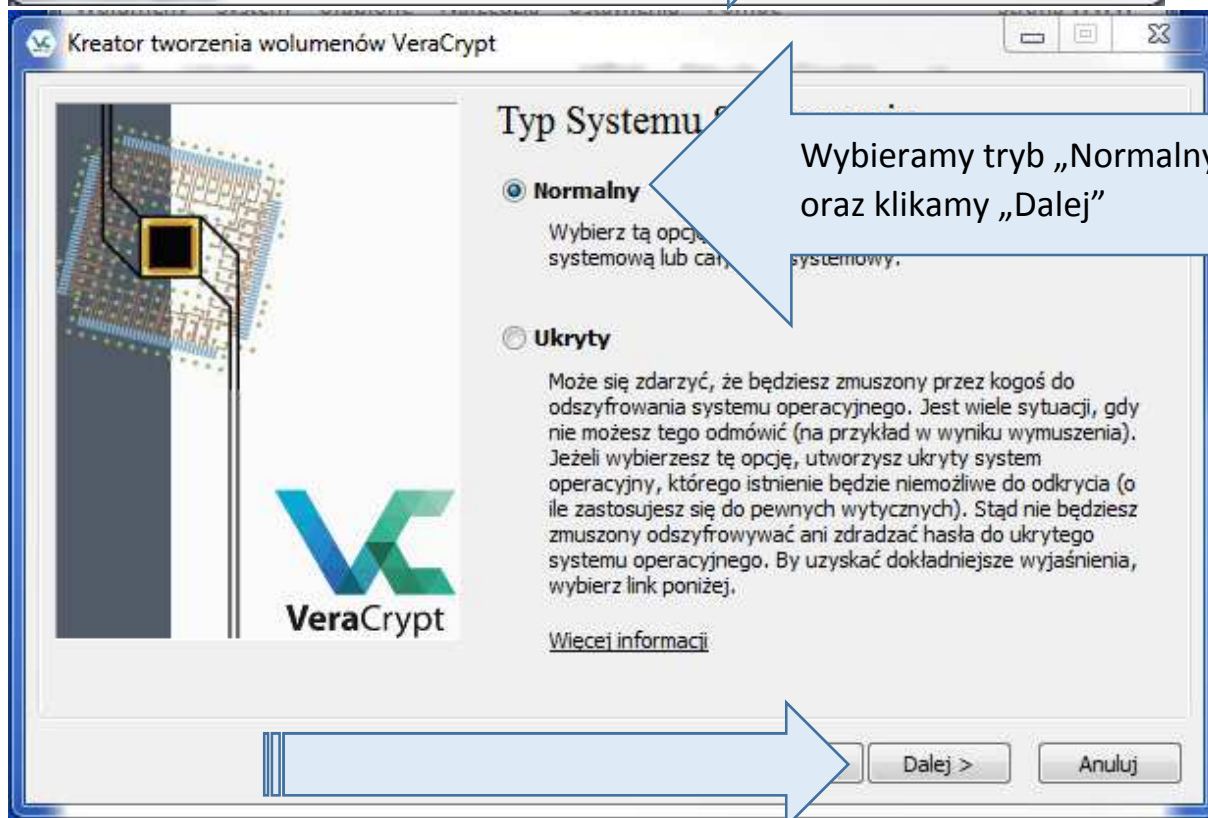
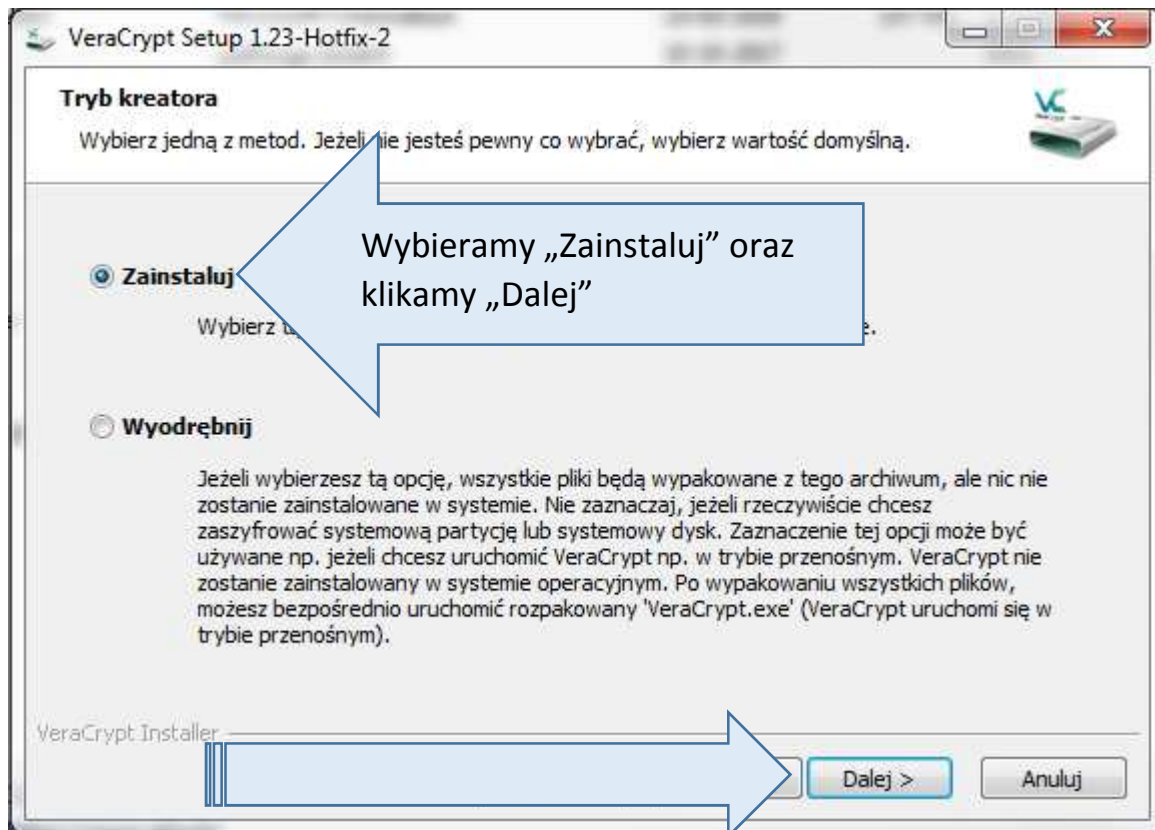
Uruchamiamy pobrany instalator

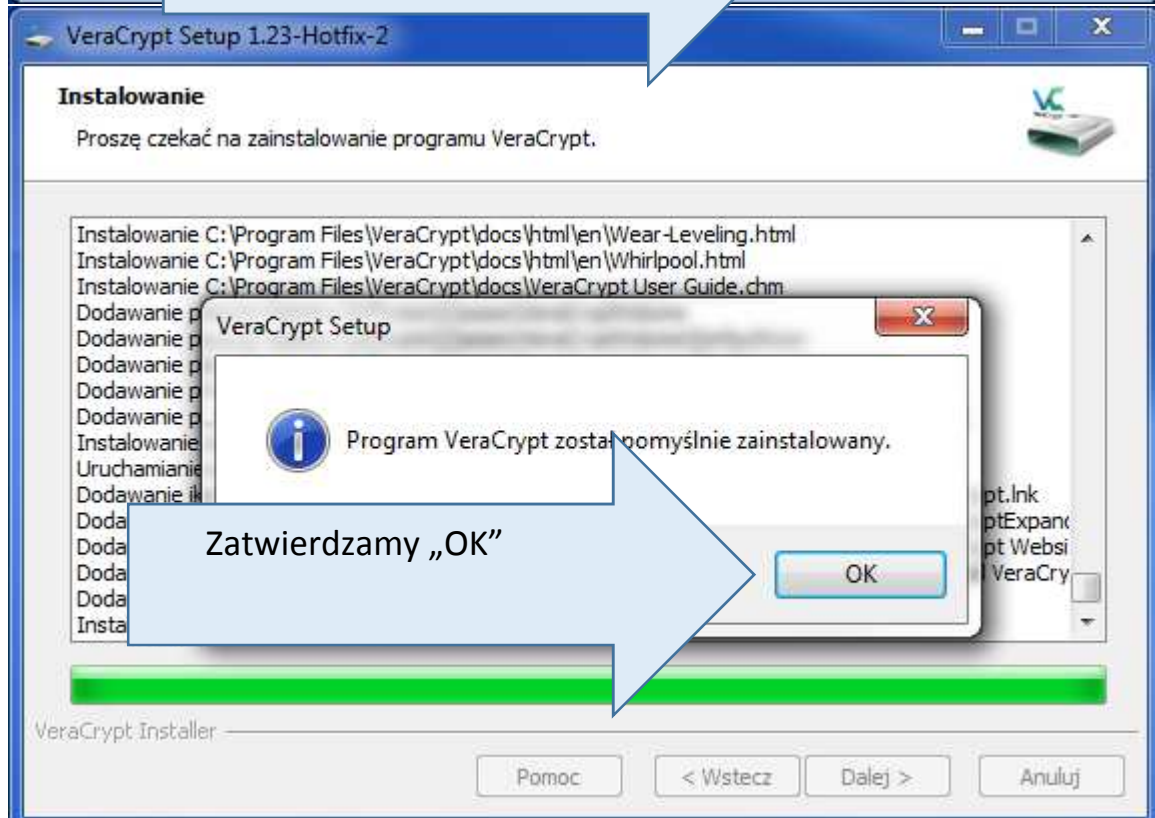
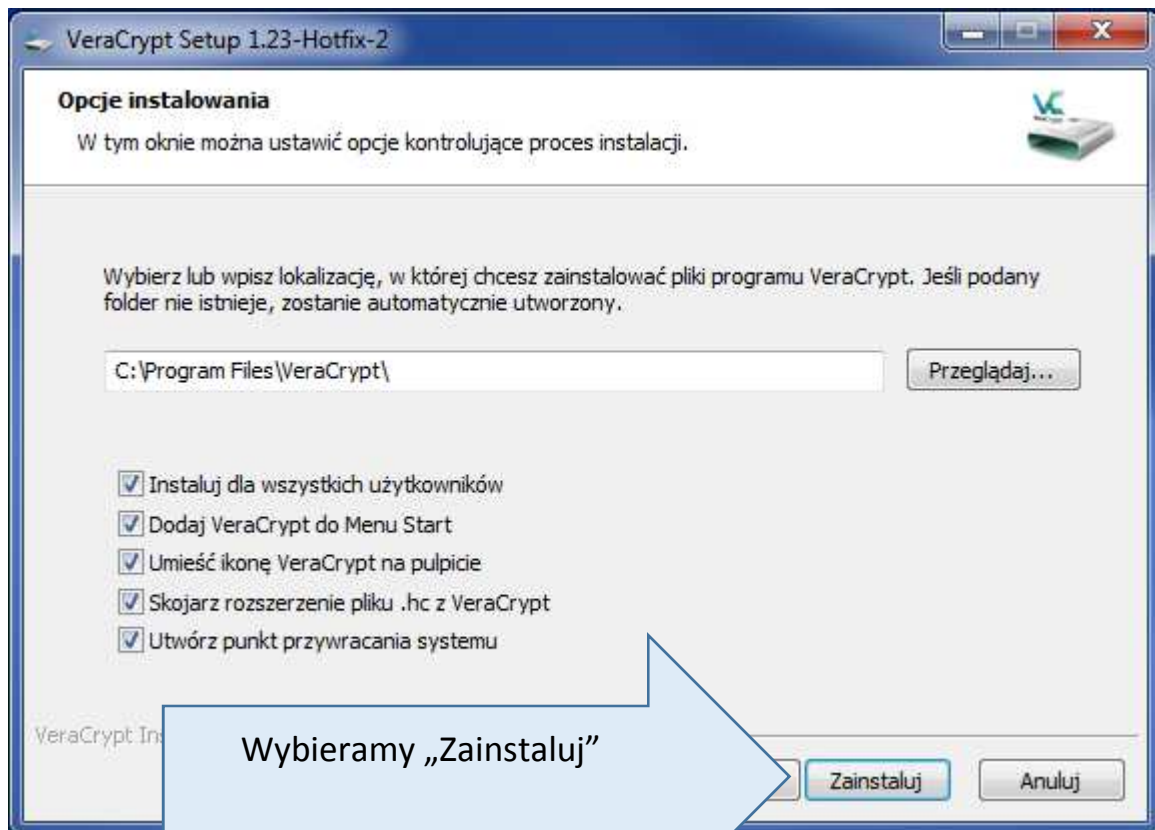


Akceptujemy język instalacji



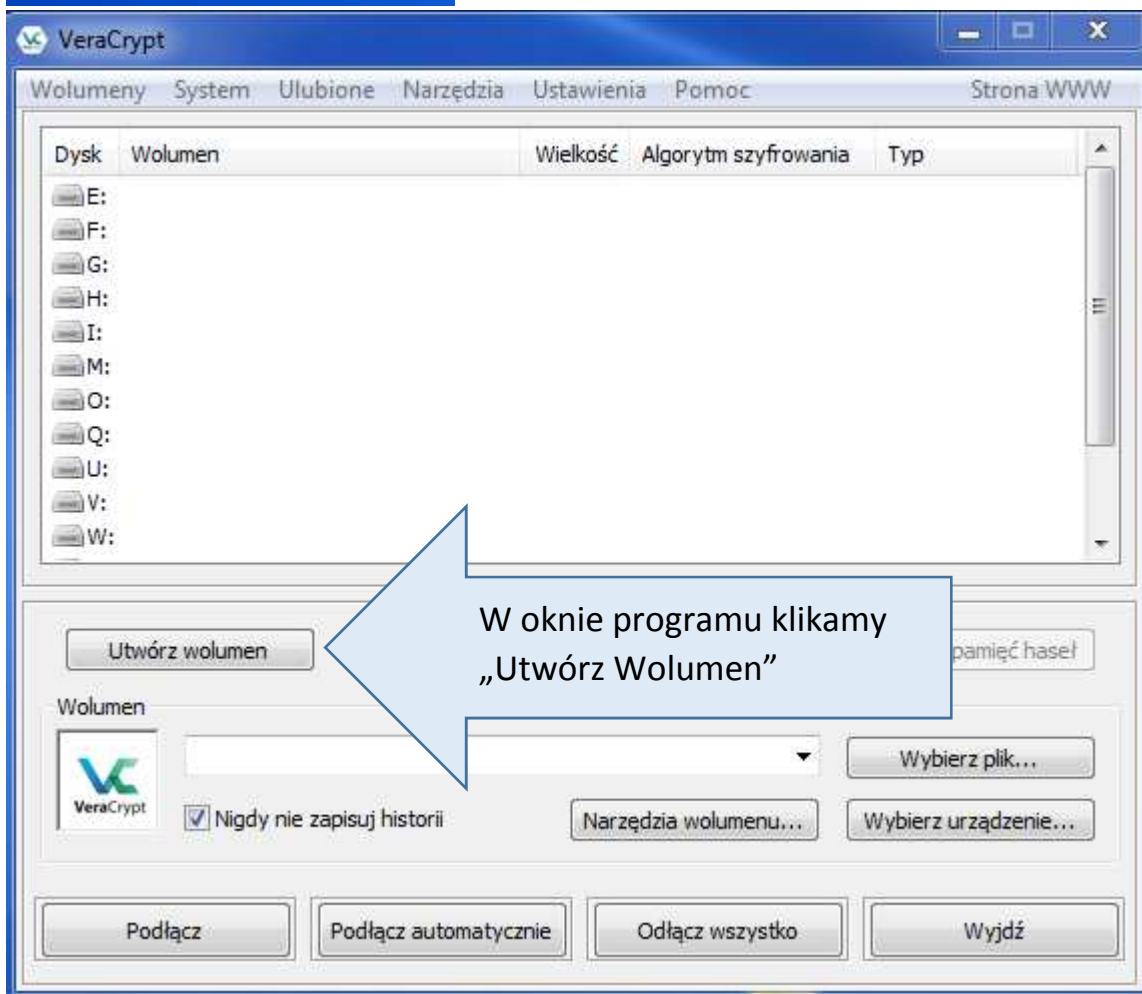
Akceptujemy warunki i klikamy dalej



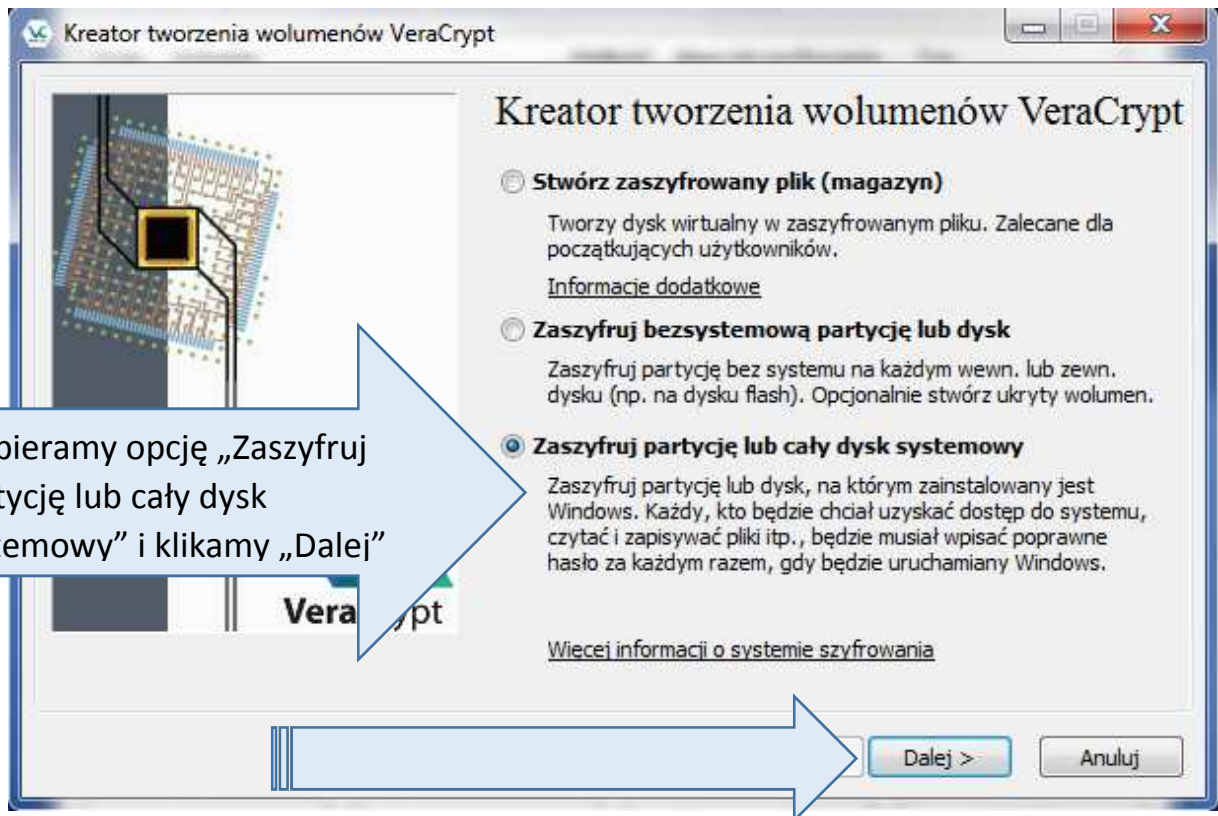




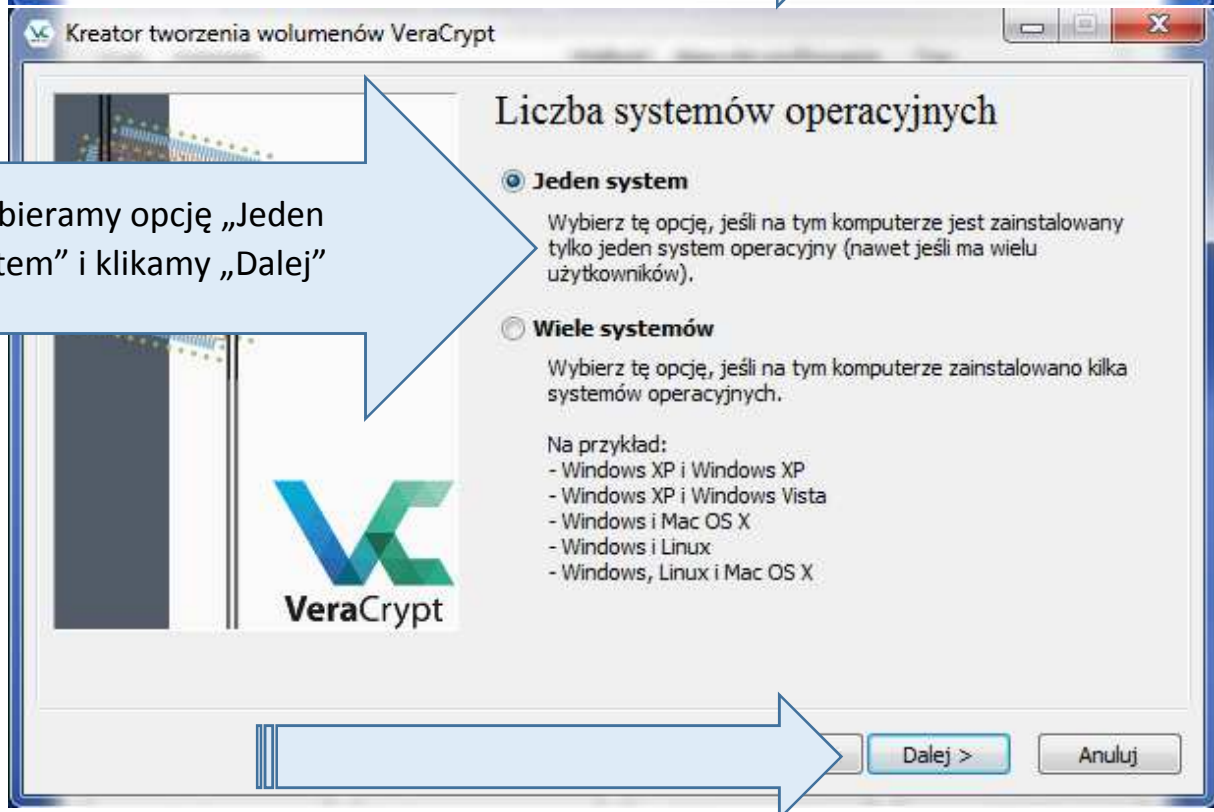
Uruchamiamy program VeraCrypt z pulpitu

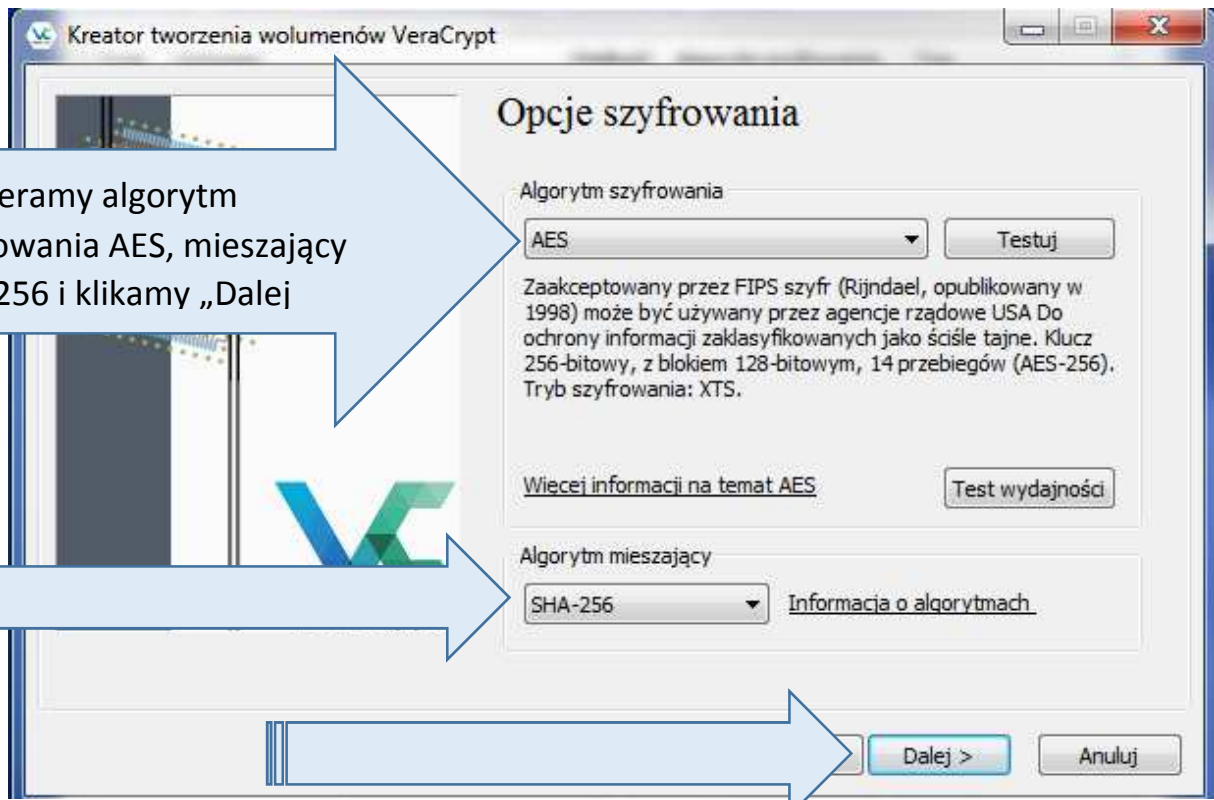


W oknie programu klikamy „Utwórz Wolumen”



Wybieramy opcję „Zaszyfruj partycję lub cały dysk systemowy” i klikamy „Dalej”





Wybieramy algorytm szyfrowania AES, mieszający SHA-256 i klikamy „Dalej”

Opcje szyfrowania

Algorytm szyfrowania

AES

Testuj

Zaakceptowany przez FIPS szyfr (Rijndael, opublikowany w 1998) może być używany przez agencje rządowe USA Do ochrony informacji zaklasyfikowanych jako ściśle tajne. Klucz 256-bitowy, z blokiem 128-bitowym, 14 przebiegów (AES-256). Tryb szyfrowania: XTS.

[Więcej informacji na temat AES](#)

Test wydajności

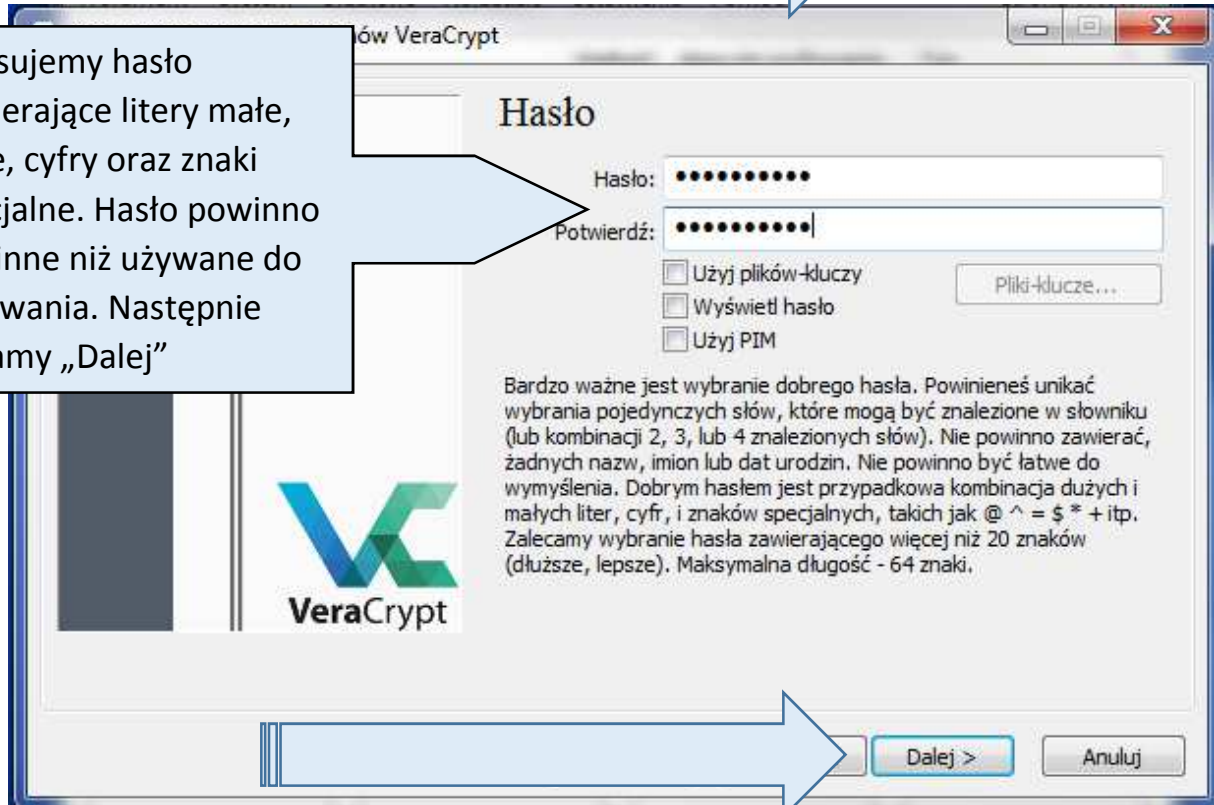
Algorytm mieszający

SHA-256

[Informacja o algorytmach](#)

Dalej >

Anuluj



Wpisujemy hasło zawierające litery małe, duże, cyfry oraz znaki specjalne. Hasło powinno być inne niż używane do logowania. Następnie klikamy „Dalej”

Hasło

Hasło:

Potwierdź:

Użyj plików-kłuczy

Wyświetl hasło

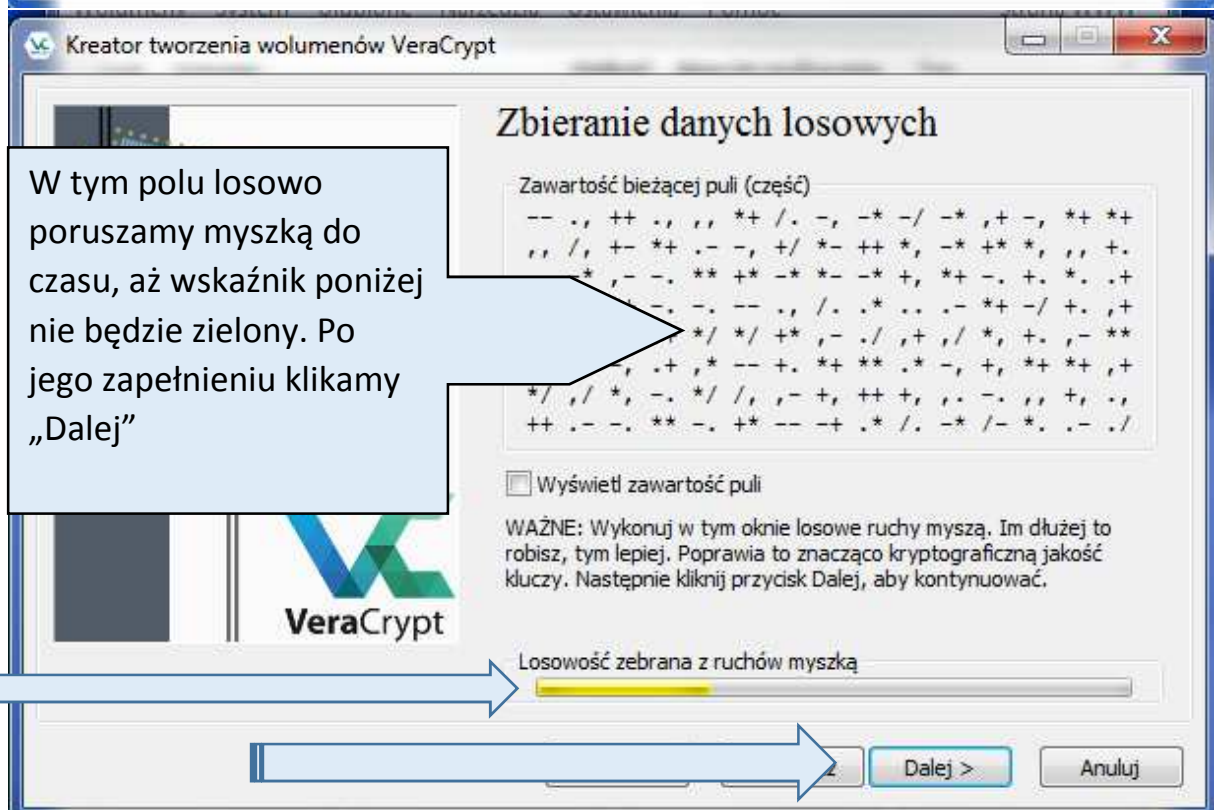
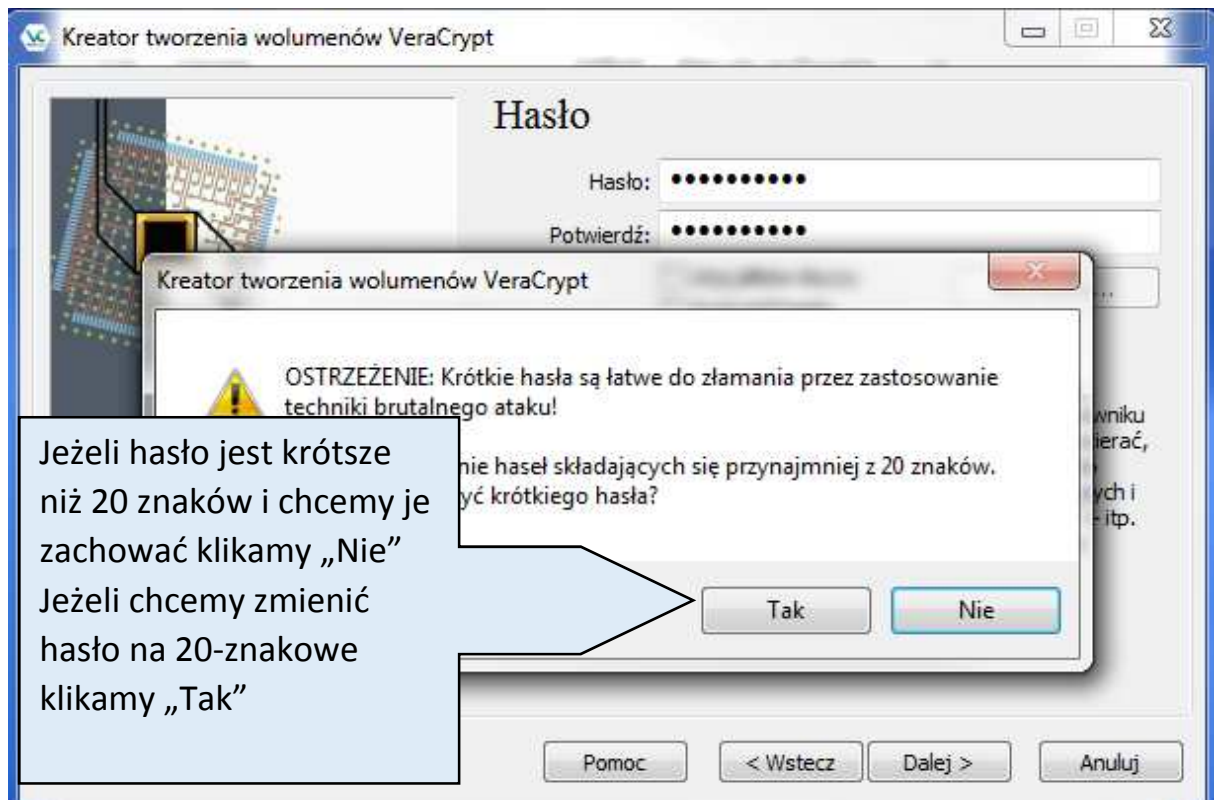
Użyj PIM

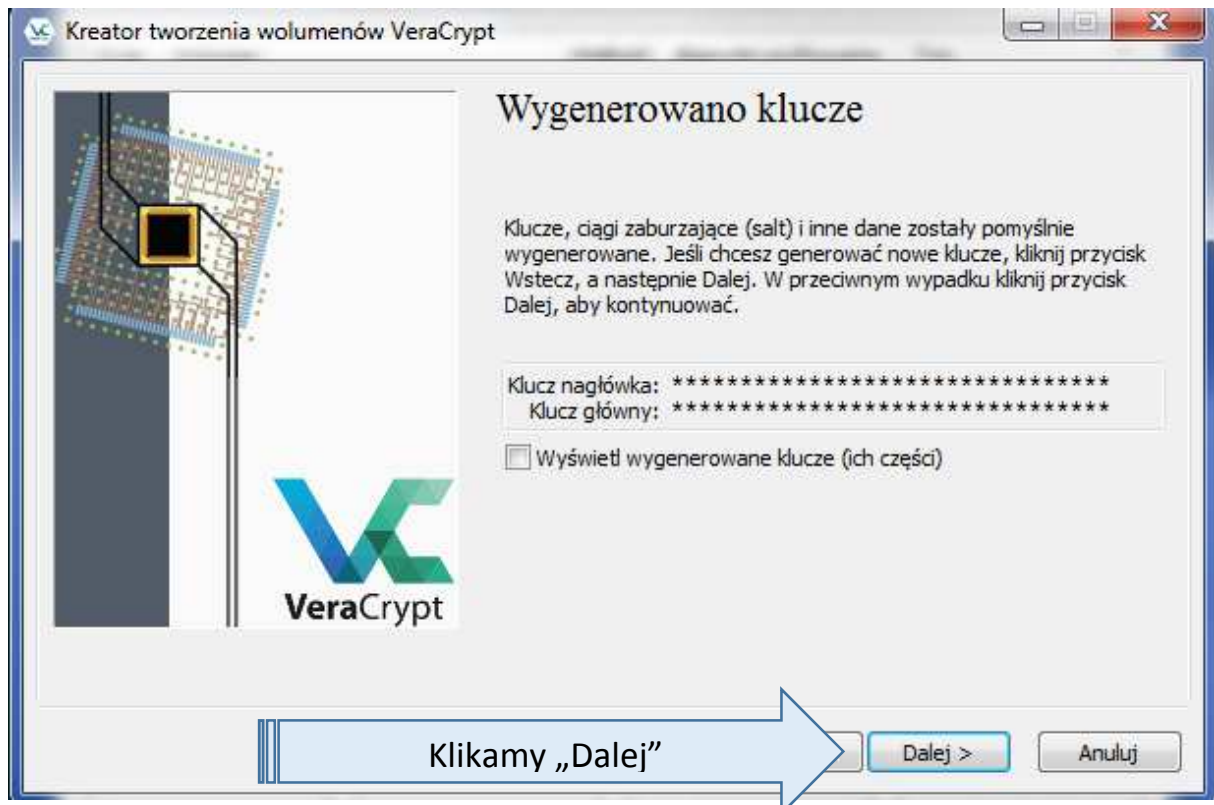
Pliki-kłucze...

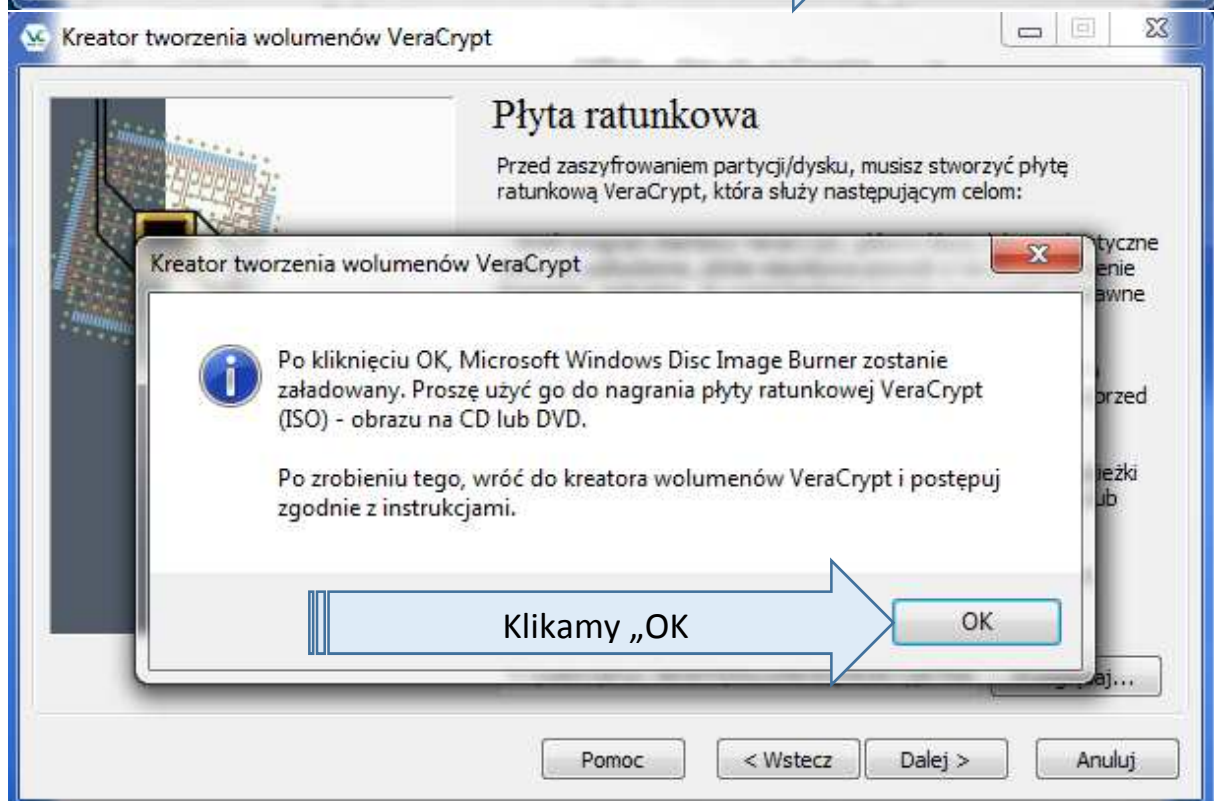
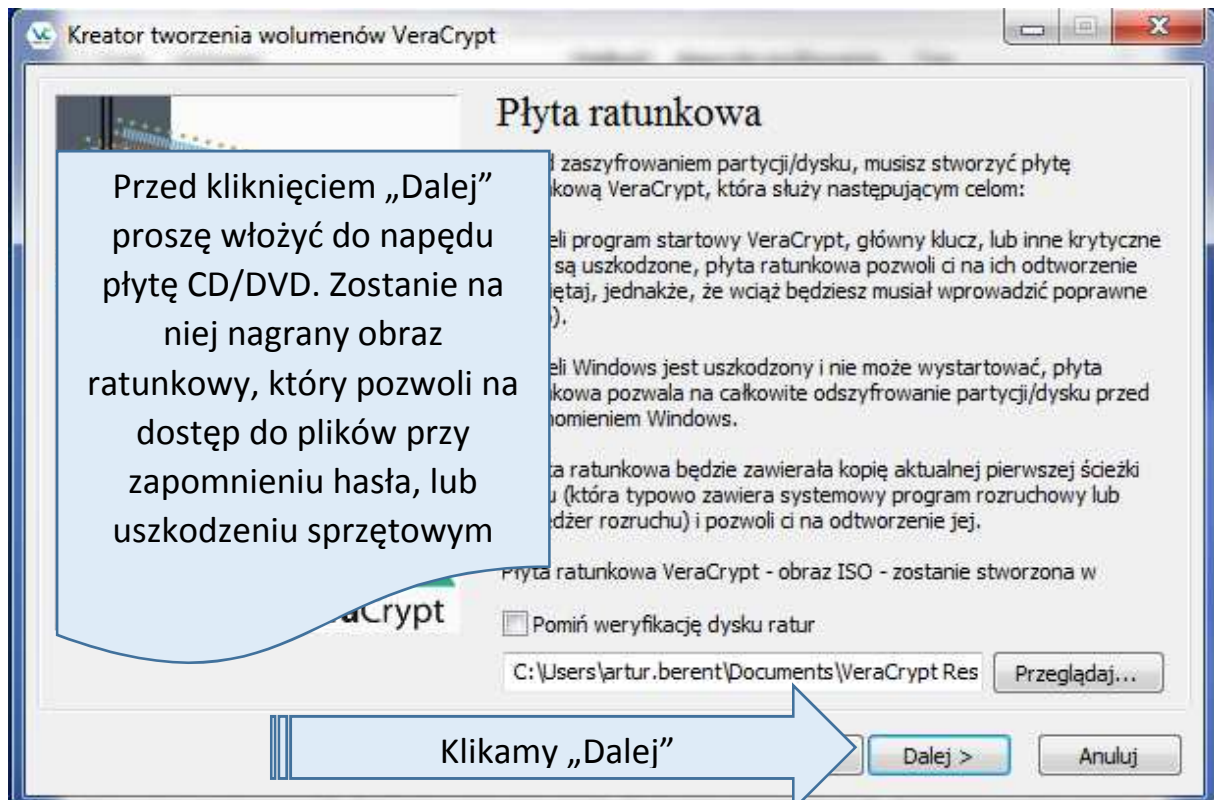
Bardzo ważne jest wybranie dobrego hasła. Powinieneś unikać wybrania pojedynczych słów, które mogą być znalezione w słowniku (lub kombinacji 2, 3, lub 4 znalezionych słów). Nie powinno zawierać żadnych nazw, imion lub dat urodzin. Nie powinno być łatwe do wymyślenia. Dobrym hasłem jest przypadkowa kombinacja dużych i małych liter, cyfr, i znaków specjalnych, takich jak @ ^ = \$ * + itp. Zalecamy wybranie hasła zawierającego więcej niż 20 znaków (dłuższe, lepsze). Maksymalna długość - 64 znaki.

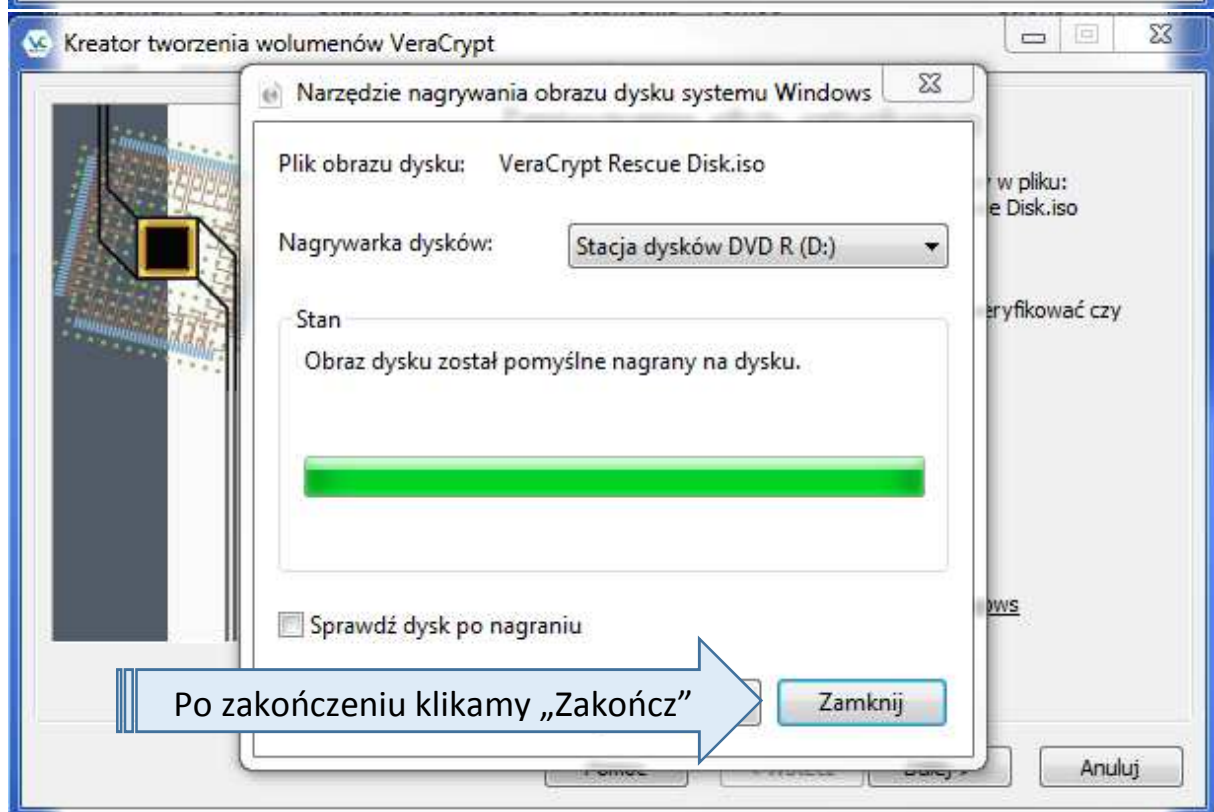
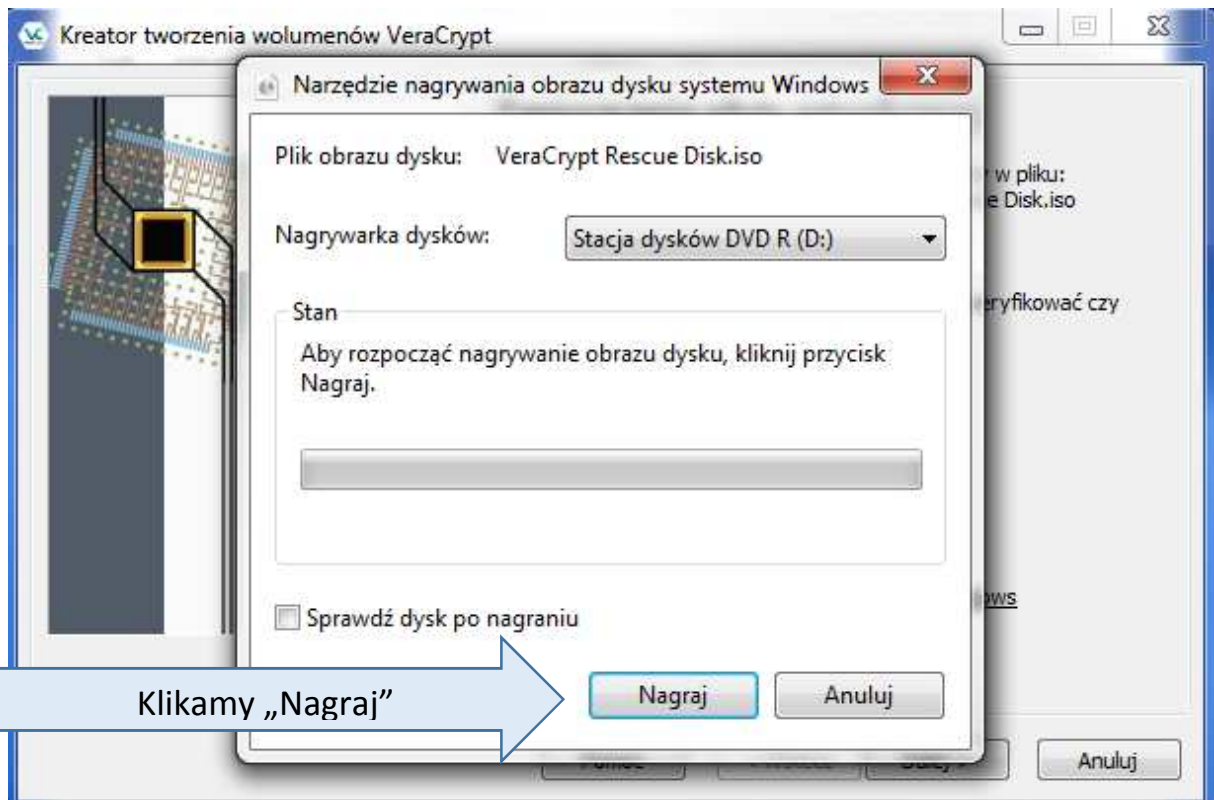
Dalej >

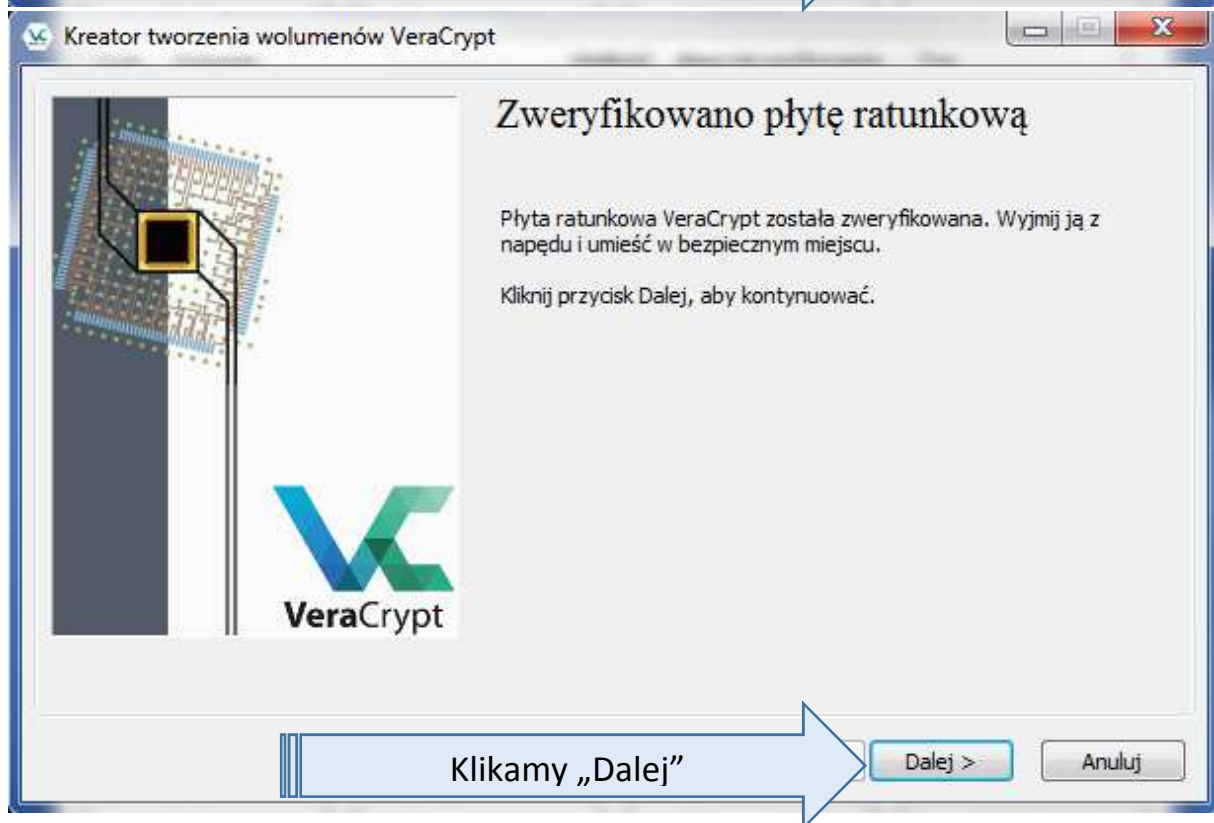
Anuluj

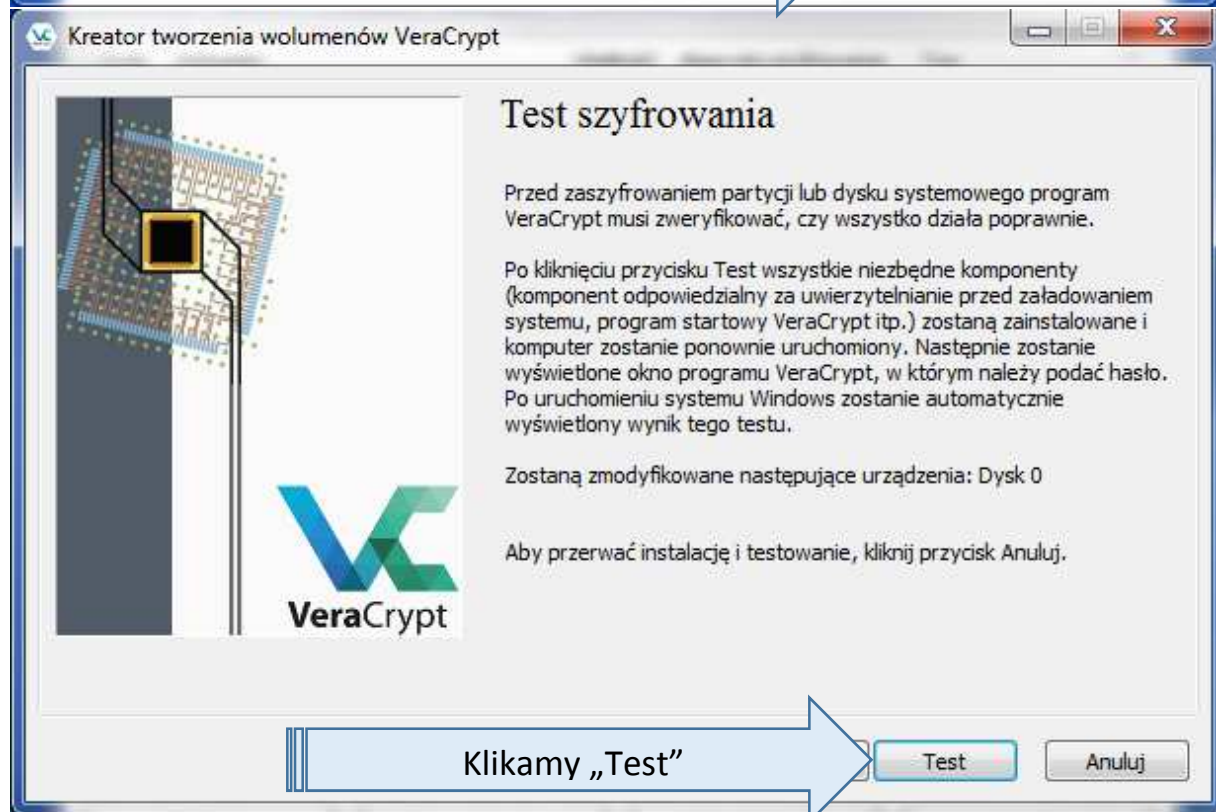
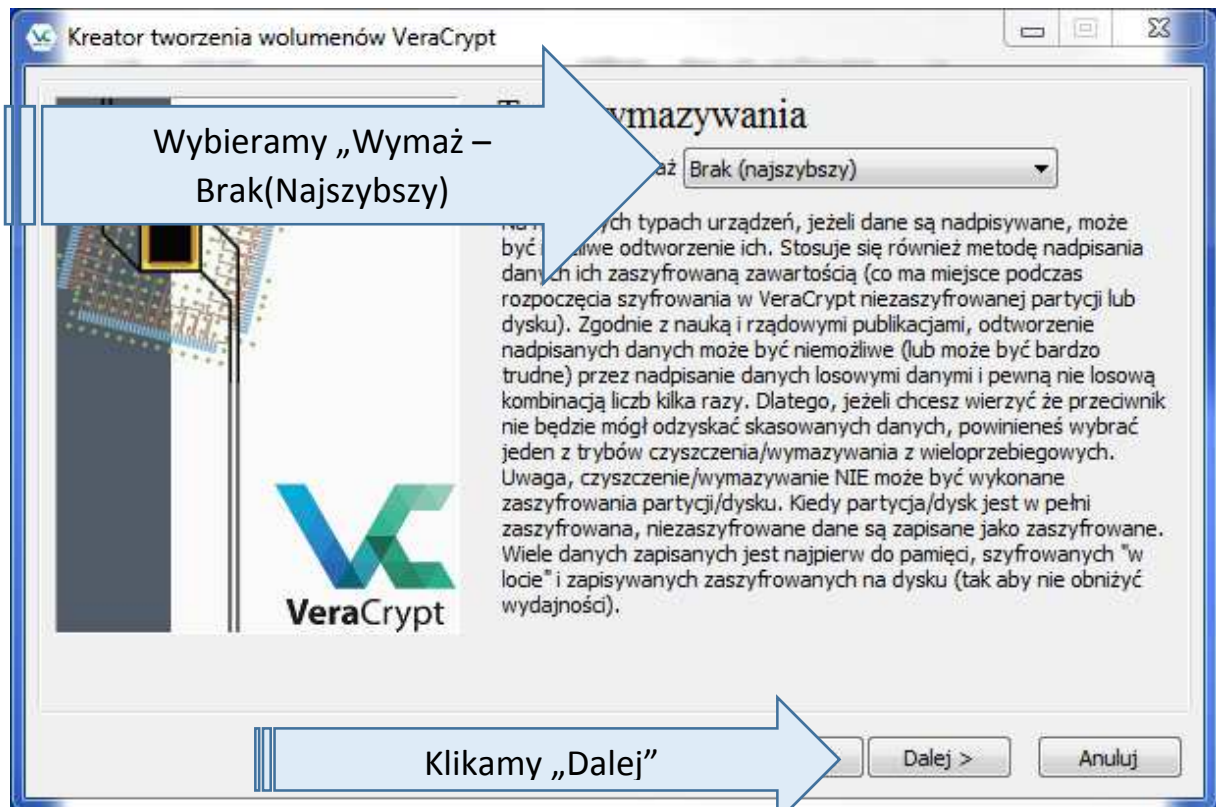


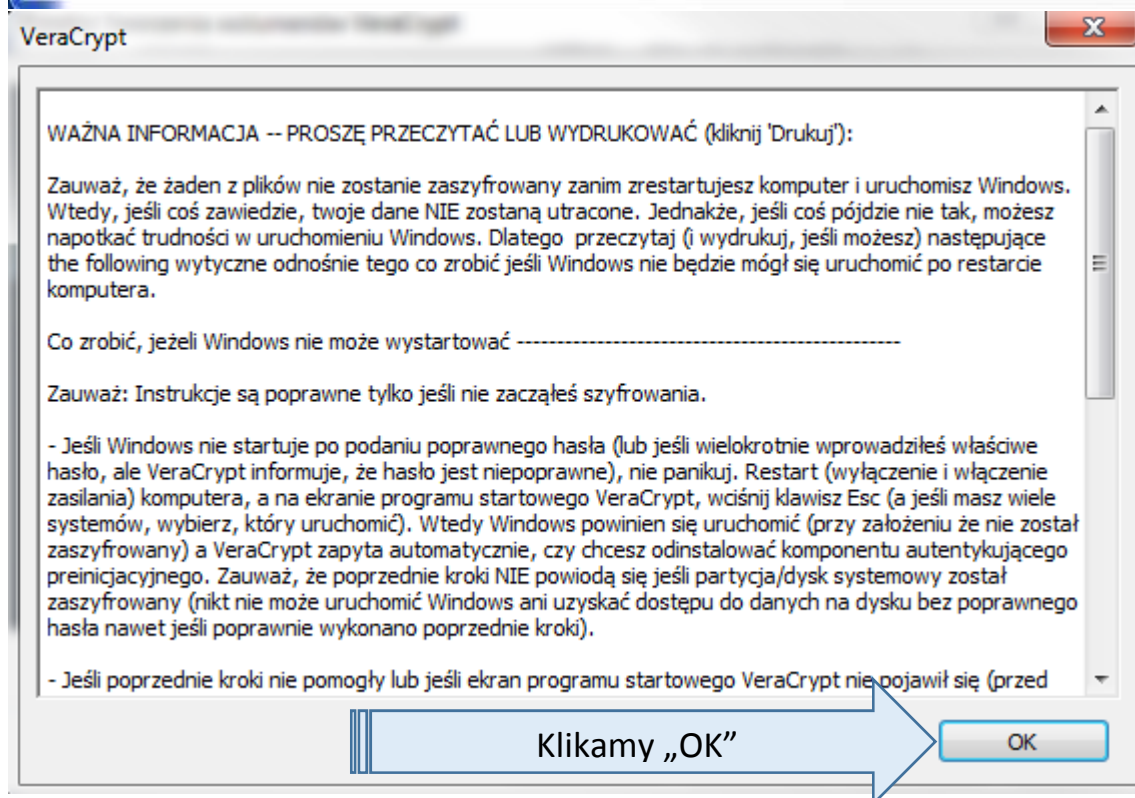
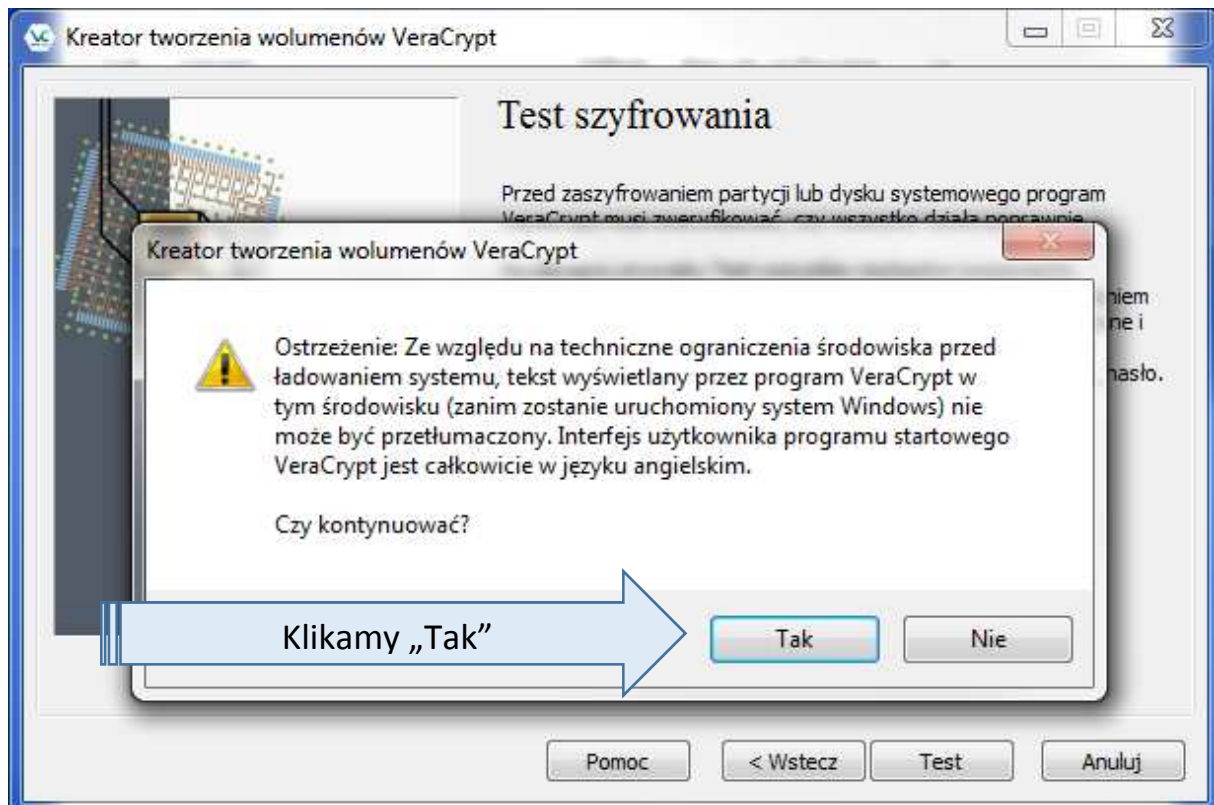


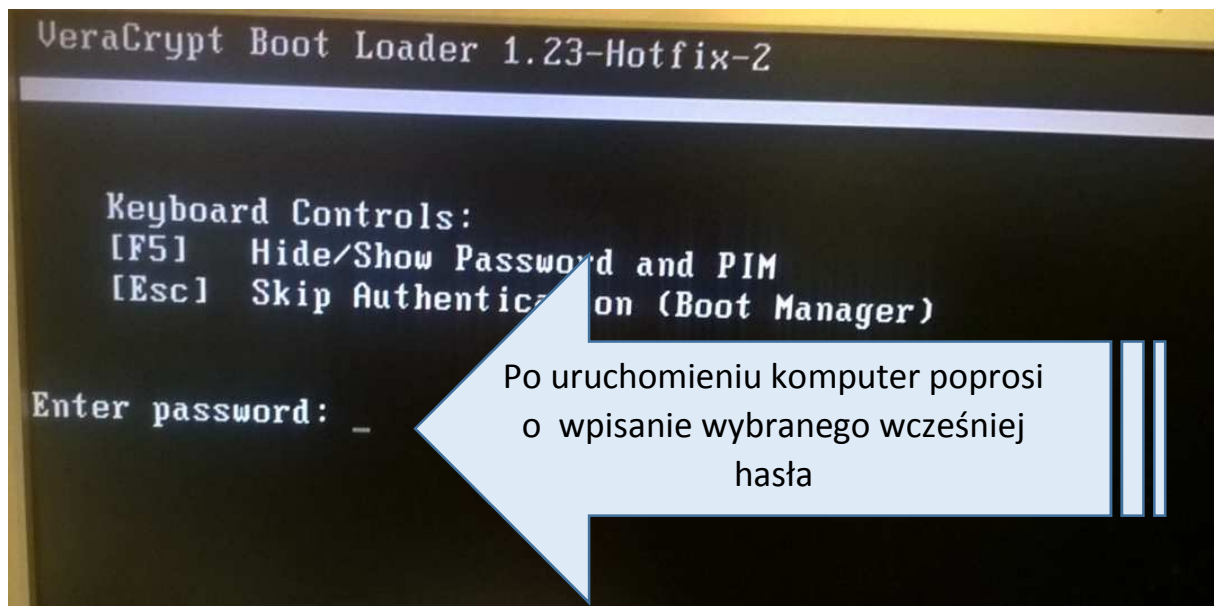
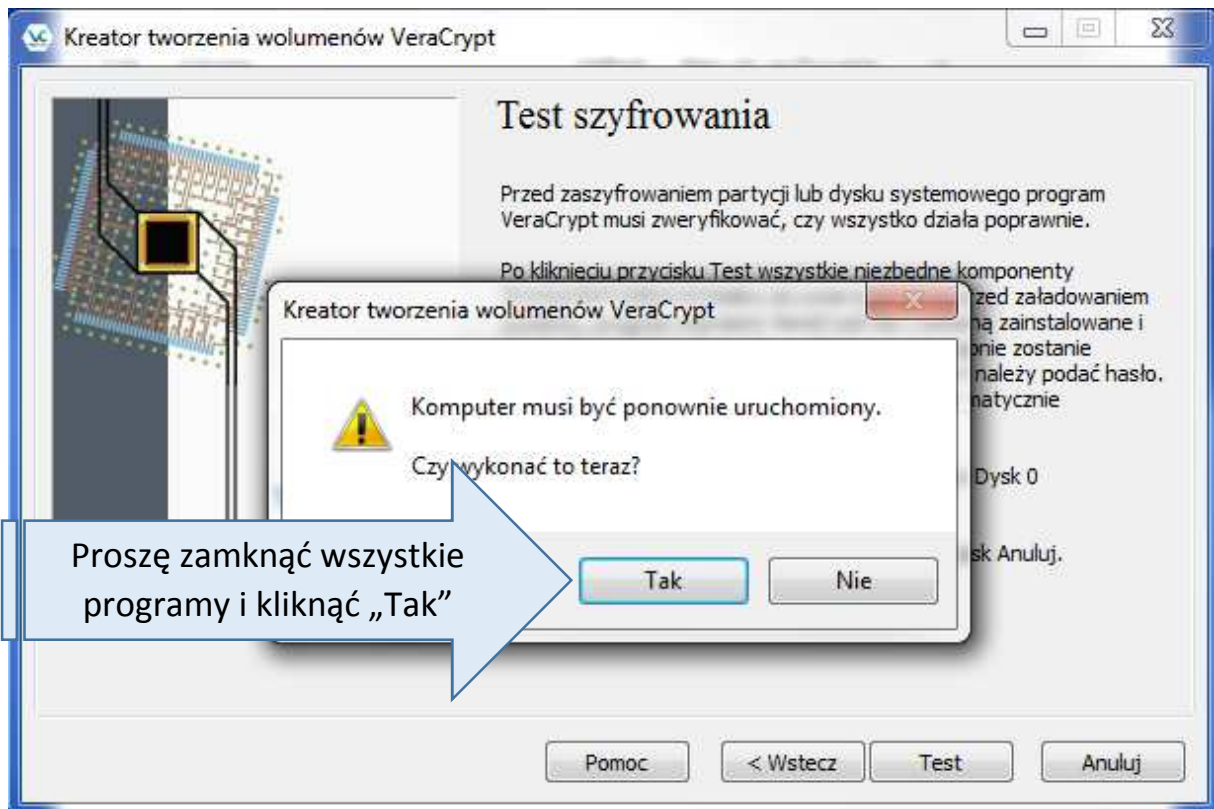


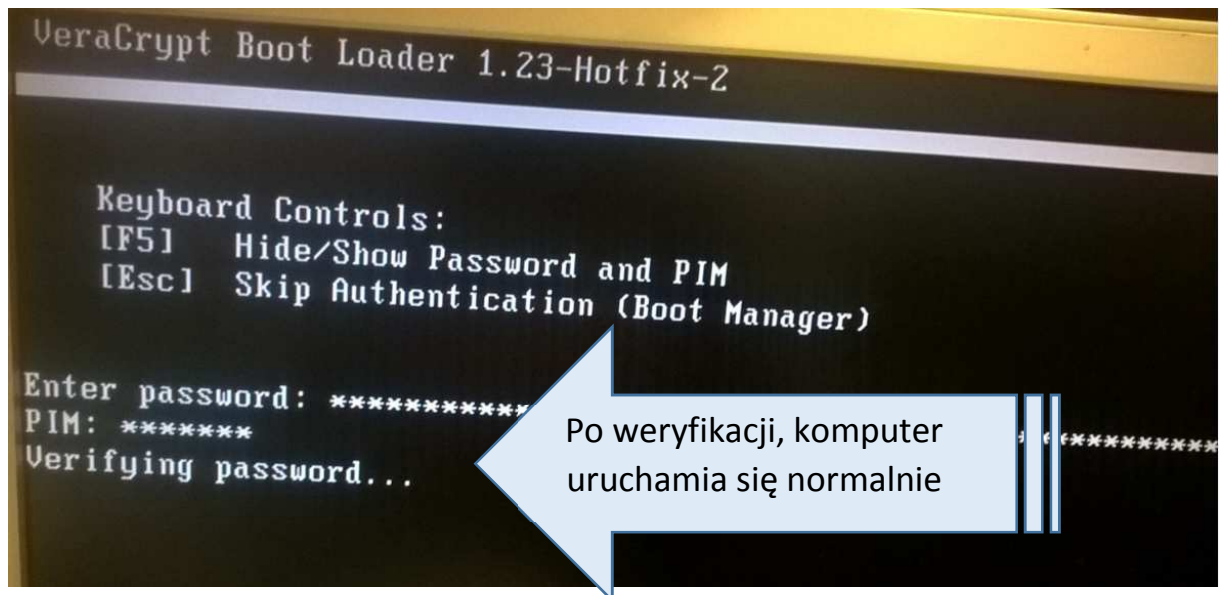
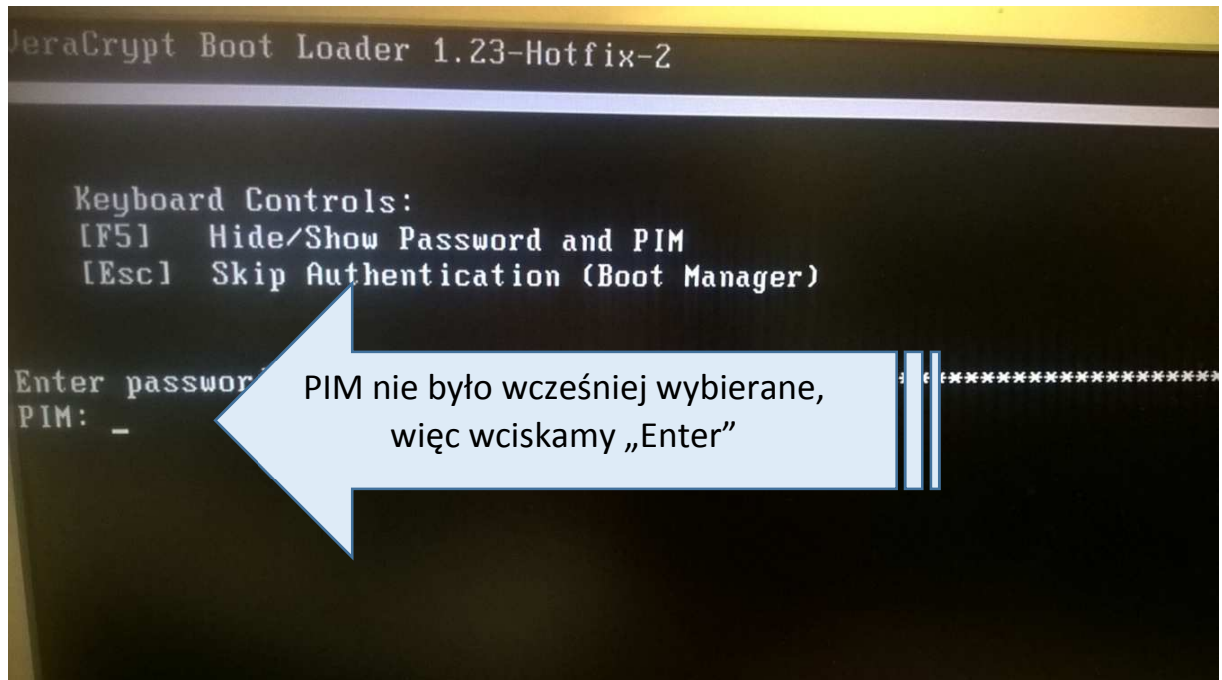








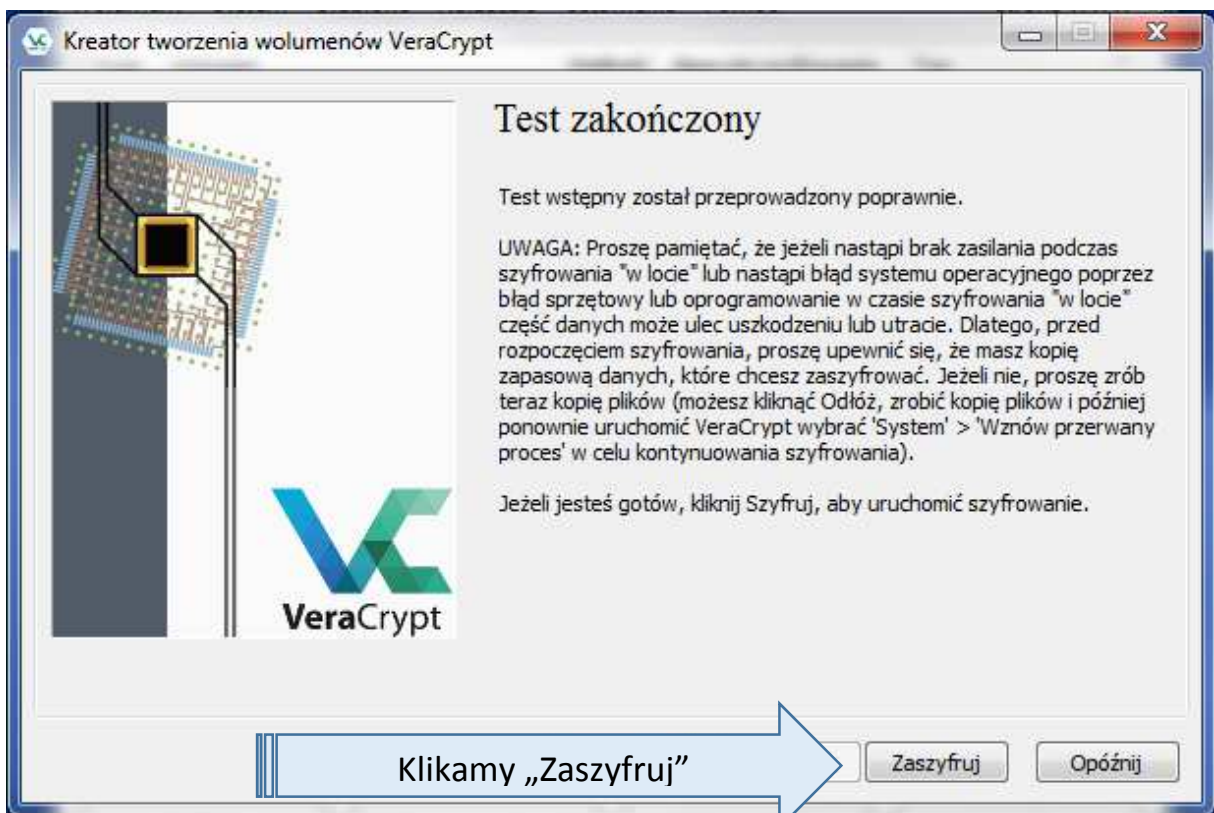




Logujemy się do komputera



Uruchamiamy ponownie program z pulpitu



Klikamy „Zaszyfruj”

Zaszyfruj

Opóźnij

