Nazwa implementacji: Szyfrowanie

Autor:

Adam Jurkiewicz

Opis implementacji: Zaawansowane użytkowanie Linuksa, podstawowe informacje o bezpieczeństwie danych i szyfrowaniu.

- Na kartce rozpisz szyfrowanie w stylu ROT-13, np.:

A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	R	S	T	U

I w ten sposób zapisz zaszyfrowane zdanie: Linux jest super. Porównaj z pracami innych.

W katalogu domowym tworzymy plik tekstowy za pomocą menadżera Nautilus.

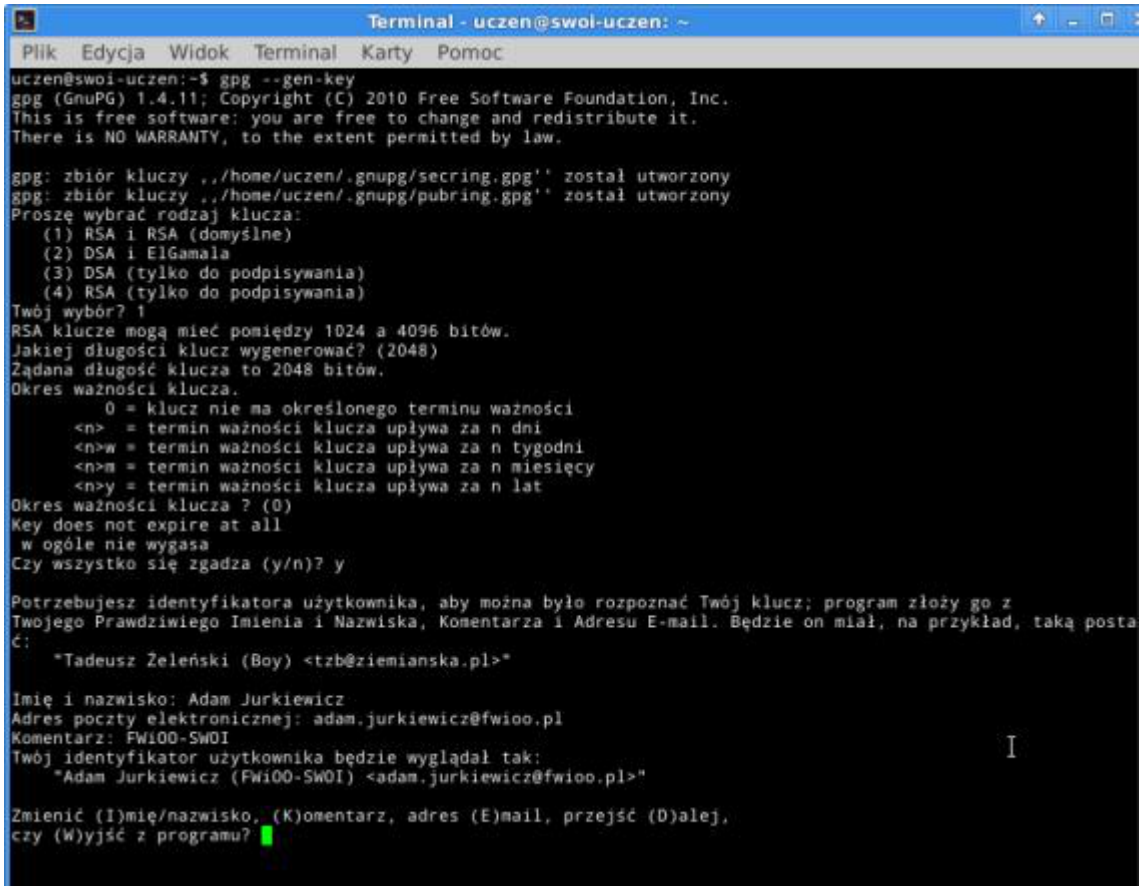
W terminalu sprawdzamy, czy plik istnieje (polecenie ls).

Wworzymy klucze dla siebie.

(gpg –-gen-key)

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
ORE
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

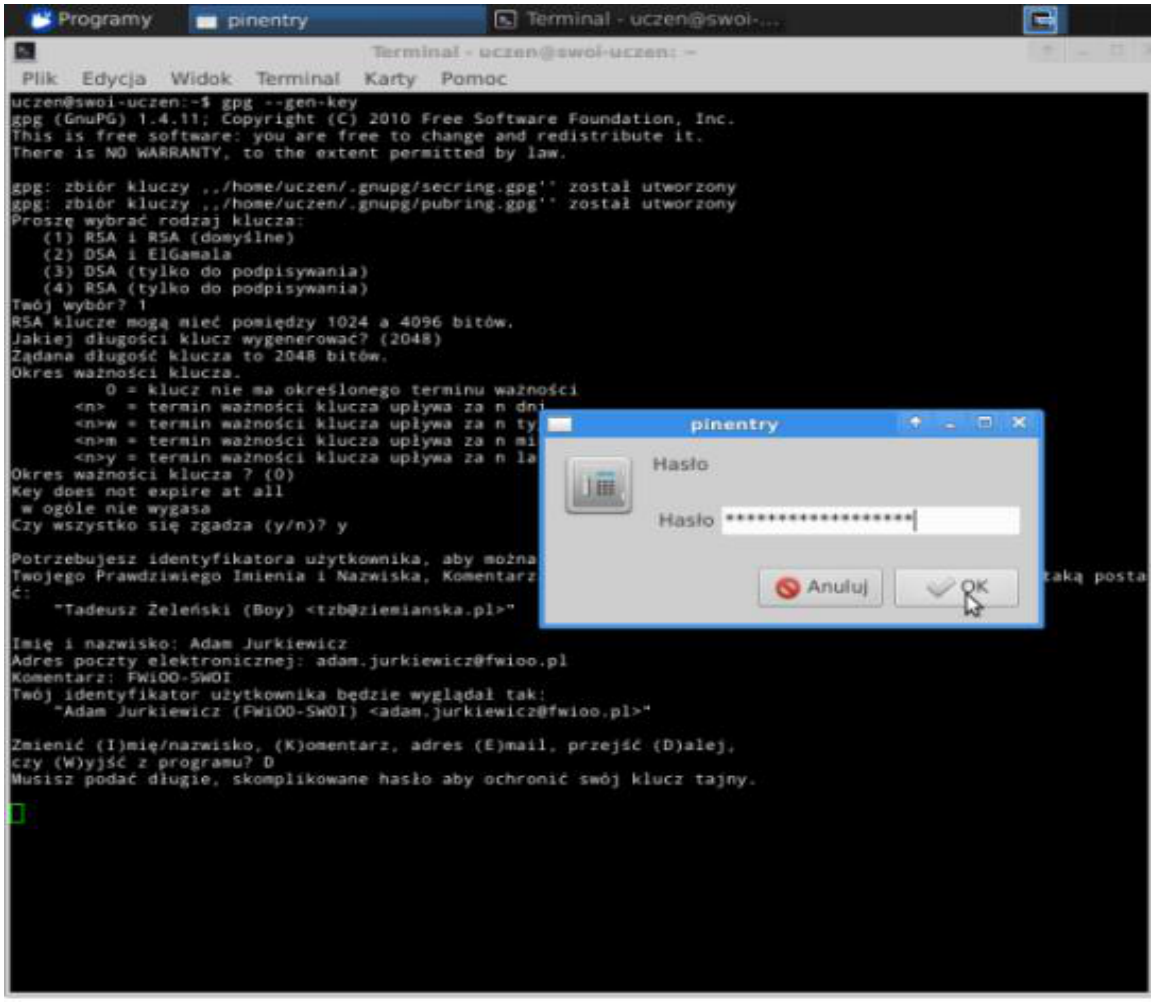
Projekt “Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych” współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.



Aby chronić nasz klucz w bazie kluczy systemu, konieczne będzie wymyślenie długiego i skomplikowanego hasła – nie wolno go zapomnieć!

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
ORE
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

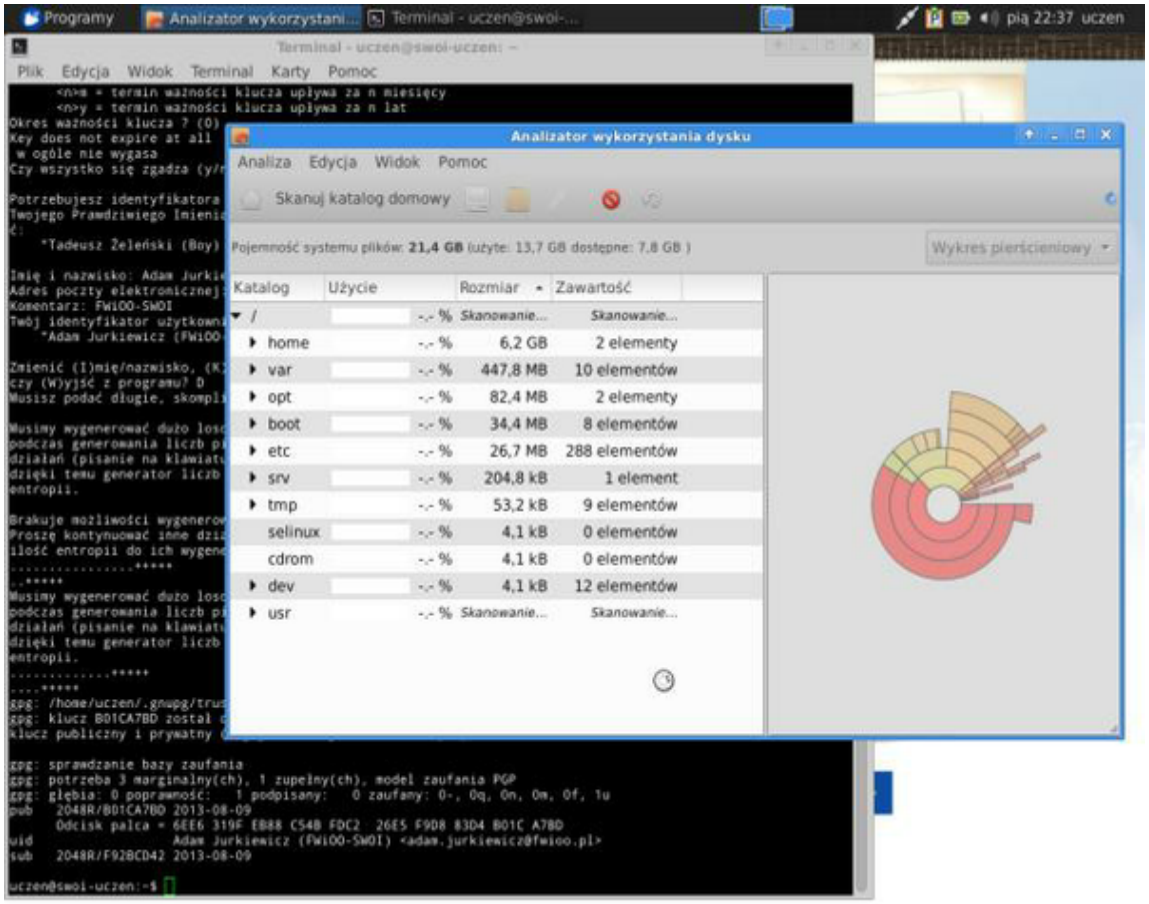
Projekt "Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych" współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.



- Należy również pamiętać, że dla dobrego klucza konieczne jest dużo danych losowych. Można to uzyskać, dając systemowi dużo operacji dyskowych do wykonania. Ja proponuję w tym momencie uruchomić program SYSTEM | Analizator wykorzystania Dysku – to pozwoli systemowi generować dużo danych.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
ORE
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

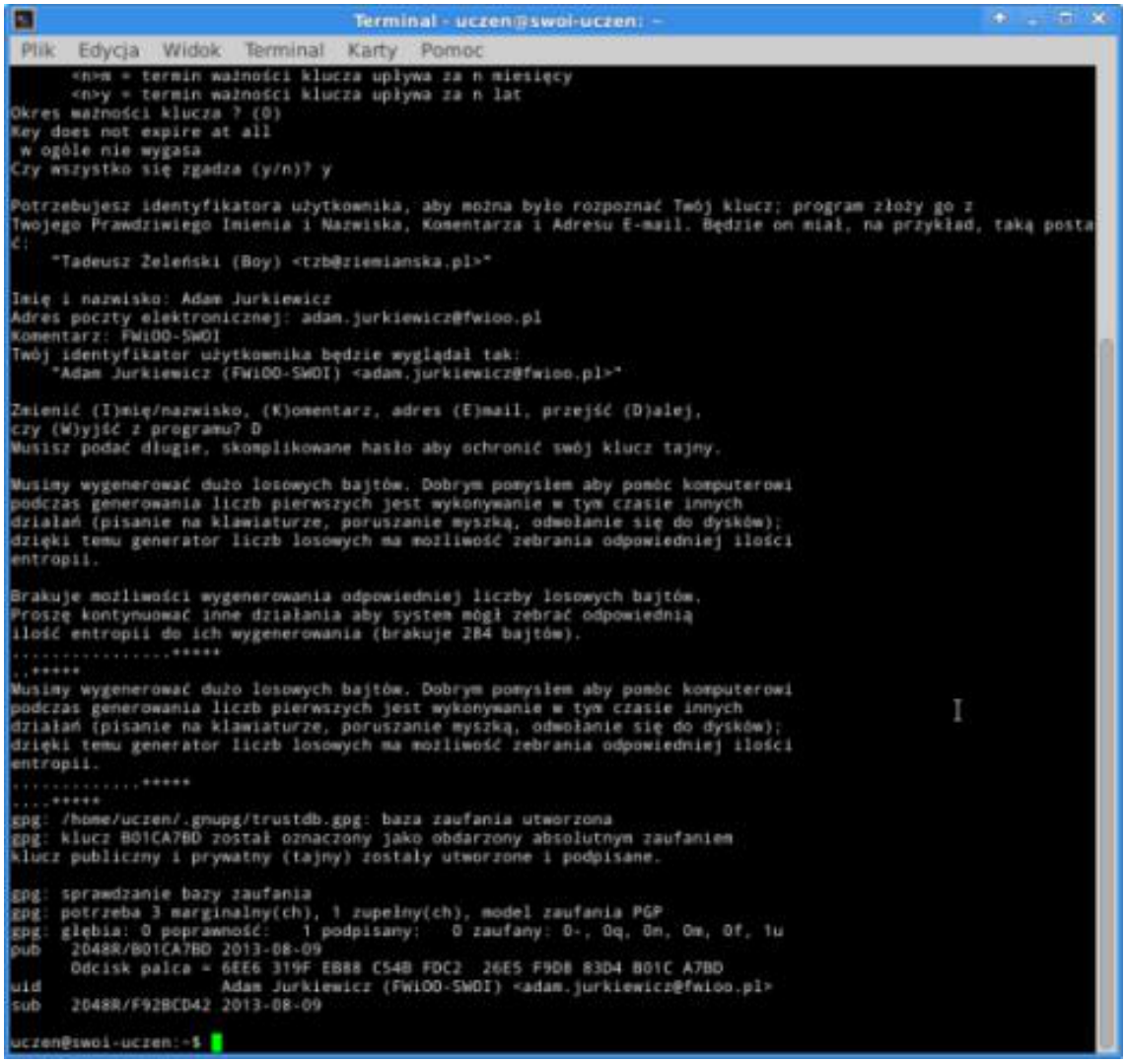
Projekt “Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych” współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.



- W tym momencie mamy już wygenerowany nasz klucz PGP:

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
ORE
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

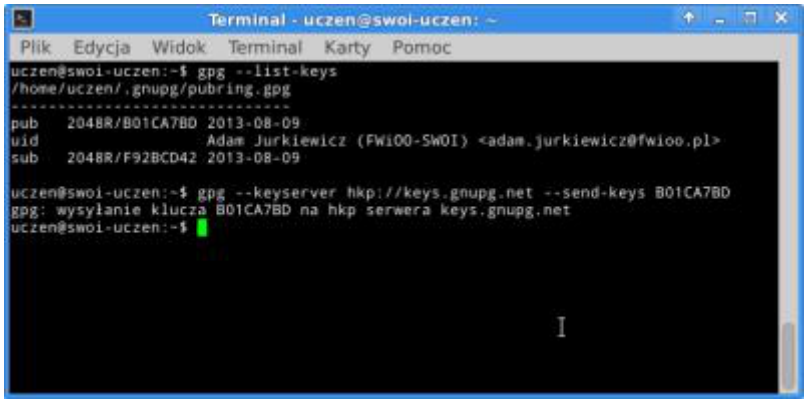
Projekt “Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych” współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.



Eksportujemy klucze na serwer kluczy.
(gpg –keyserver hkp://keys.gnupg.net –-send-keys key_ID)

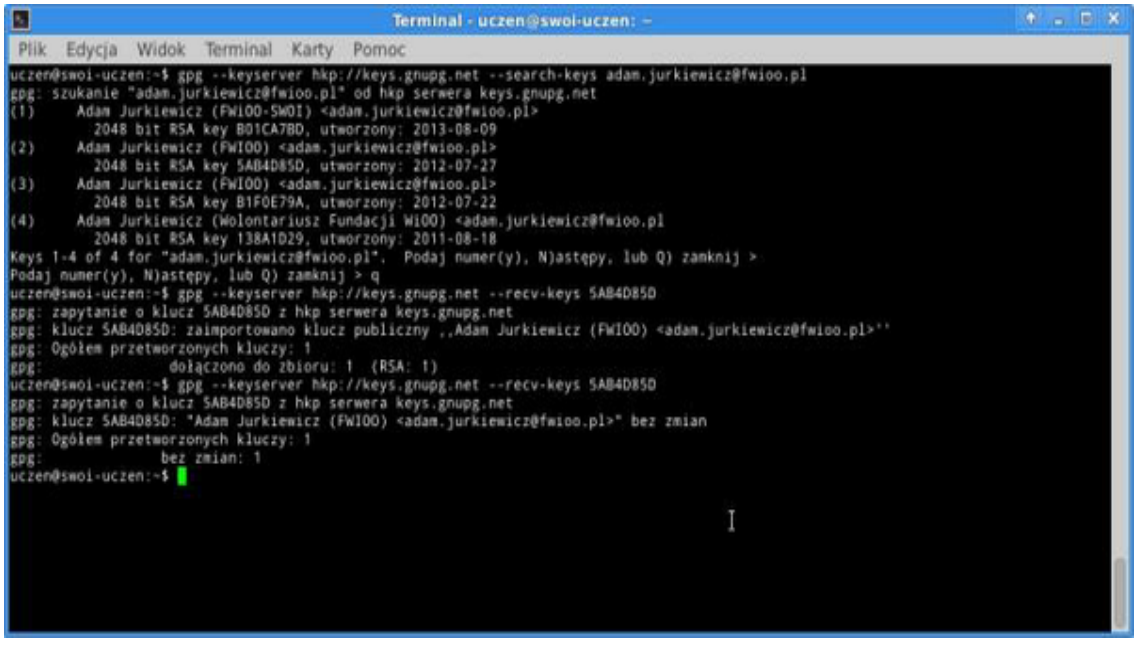
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
ORE
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt “Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych” współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.



Na serwerze kluczy wyszukujemy klucze innych osób.
(gpg –keyserver hkp://keys.gnupg.net –-search-keys key_ID)

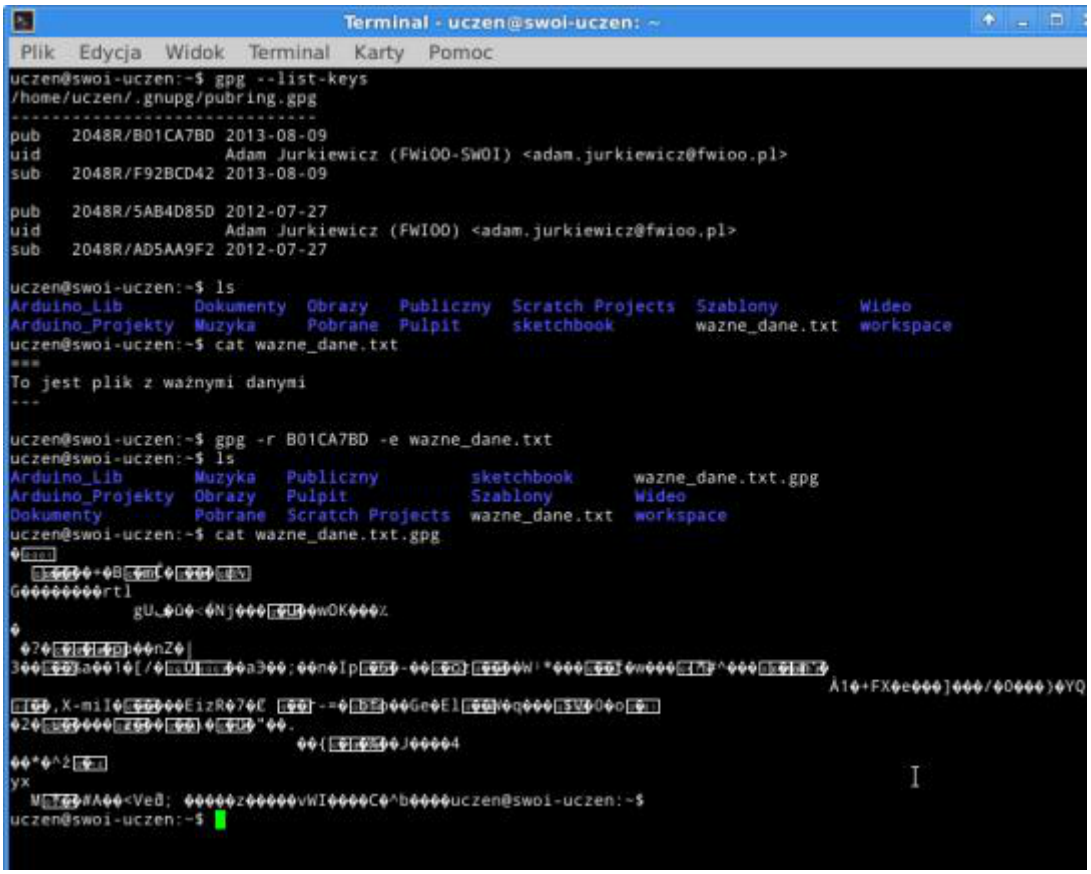
- Importujemy wybrany klucz innej osoby.
(gpg –keyserver hkp://keys.gnupg.net -–recv-keys key_ID)



- **Szyfrujemy własny plik własnym key_ID.**
(gpg –r key_ID –e nazwa_pliku)

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
ORE
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt “Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych” współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.



Zadanie 1 – ćwiczenie:

Zaszyfruj plik tekstowy, następnie skasuj go. Potem dzięki manualowi systemowemu sprawdź, jakie opcje trzeba dać dla polecenia gpg, aby odszyfrować zaszyfrowany plik. Sprawdź, czy ci się to udało poprawnie i czy widzisz tekst w pliku.

Zadanie 2 – ćwiczenie:

Zaszyfruj plik tekstowy, korzystając z key_ID innej osoby, zaimportowanego z keyserwera. Potem skopiuj plik do osoby, której klucz był użyty do szyfrowania. Sprawdź, czy ci się to udało poprawnie i czy druga widzi tekst po rozszyfrowaniu swoim **key_ID**.

key_ID

= w powyższych poleceniach key_ID należy zamienić odpowiednim ID klucza, które powstaje podczas generowania nowego klucza.

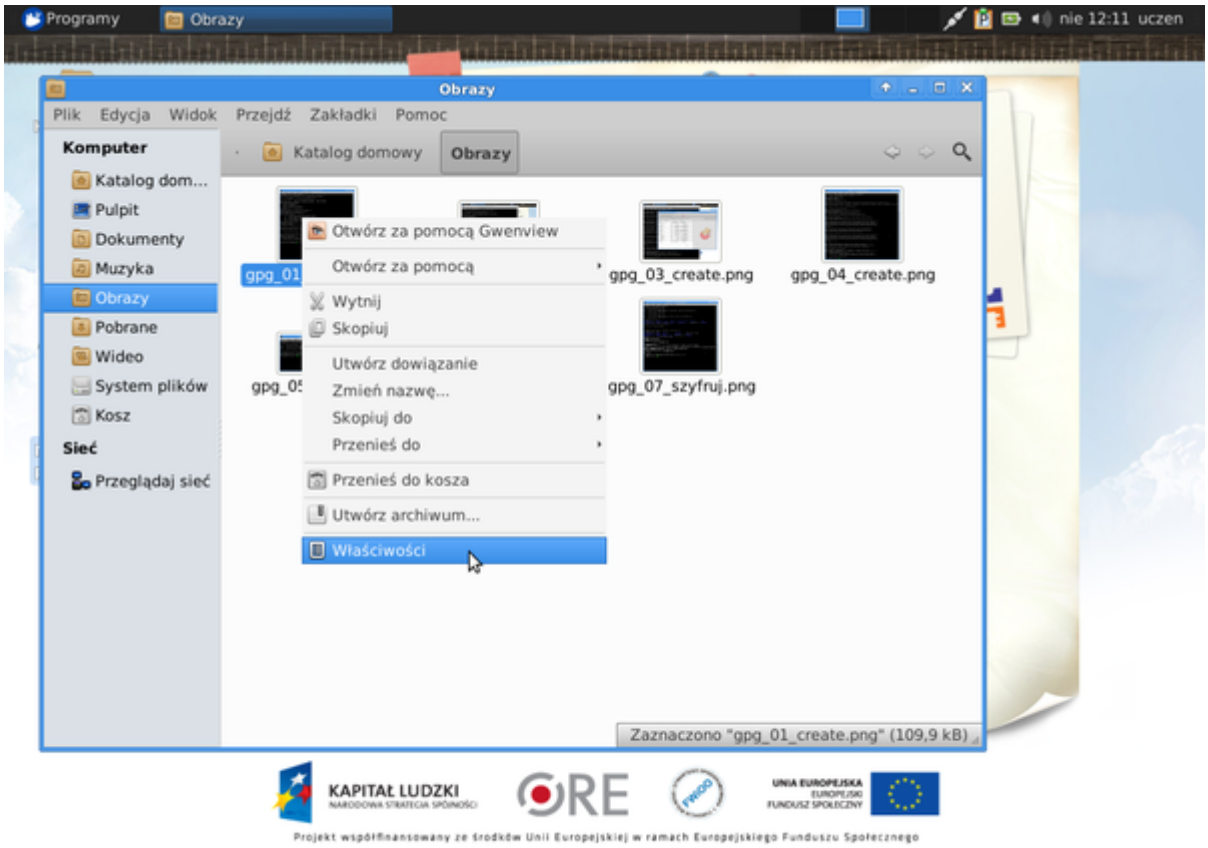
W tych przykładach key_id = B01CA7BD

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
ORE
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt “Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych” współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Dla weryfikacji poprawności danych przeprowadzamy ćwiczenie:

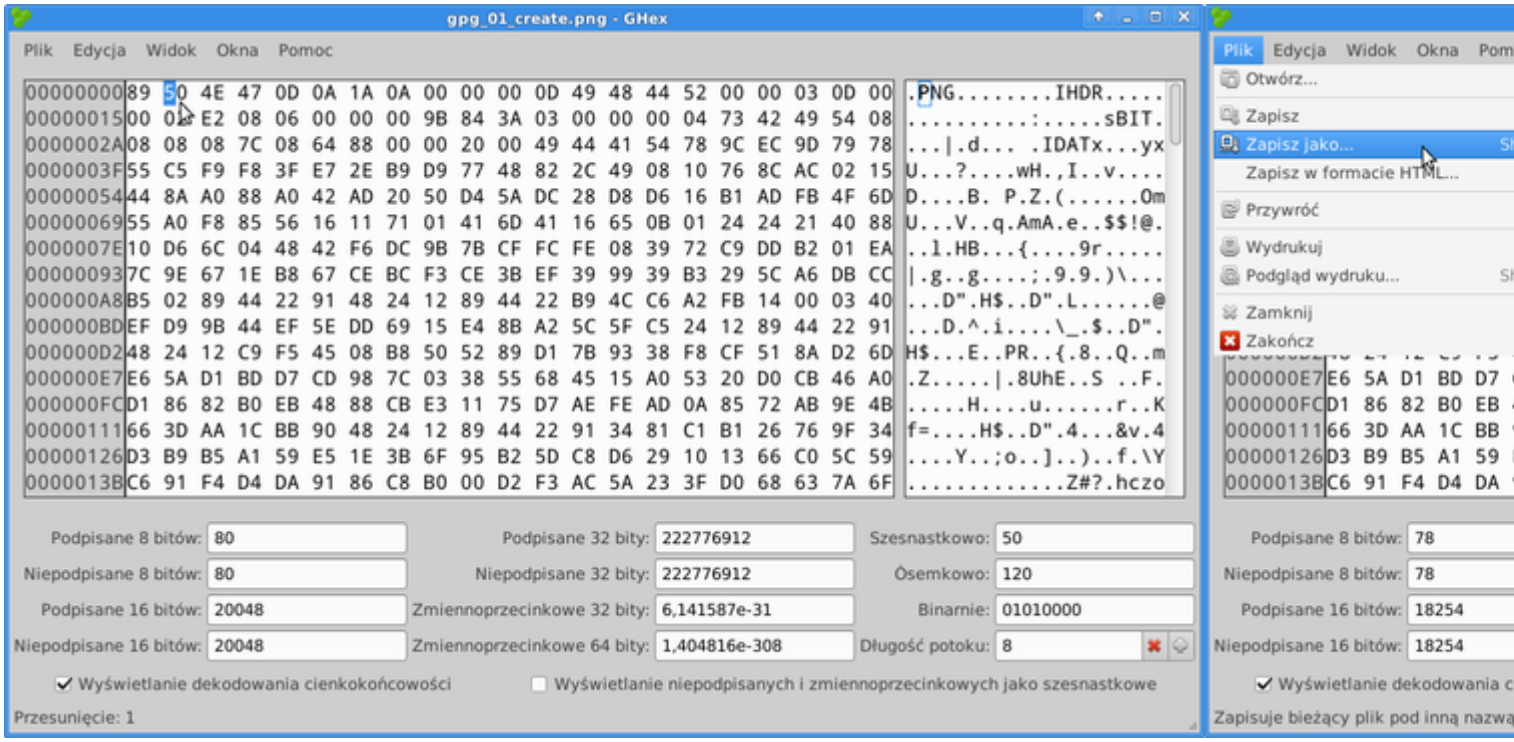
W menadżerze plików zrób kopię obrazu pobranego z internetu na pierwszych zajęciach, a następnie funkcją Prawy Przycisk Myszy - Właściwości | Sumy Kontrolne sprawdź sumy kontrolne MD5 obu plików i porównaj, czy są identyczne.



Następnie otwórz program PROGRAMY | Programowanie | Ghex i otwórz w nim plik kopii obrazka. Zmień 2gi bajt pliku na 00. Zapisz zmiany.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

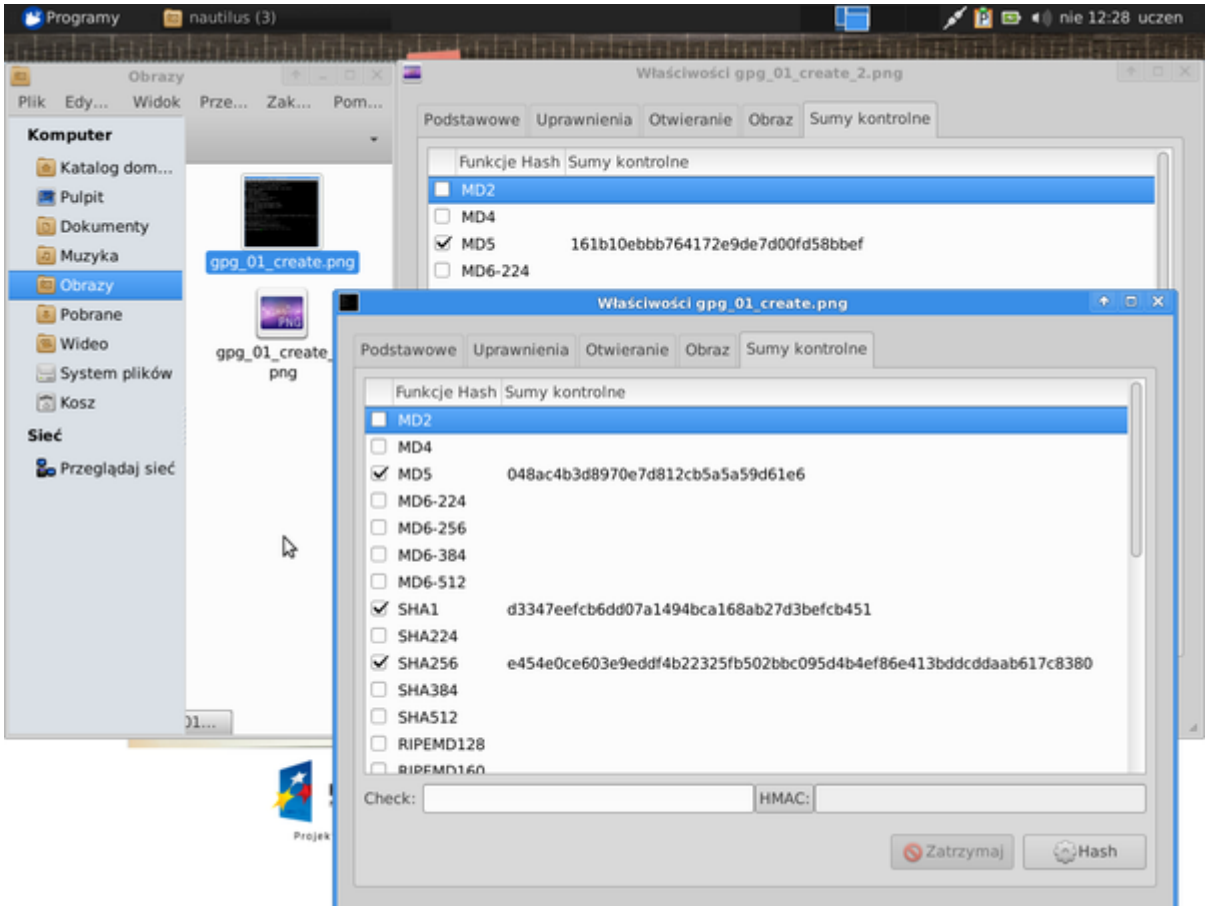
Projekt “Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych” współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.



Następnie sprawdź ponownie sumy kontrolne MD5 dla tych plików. Omów różnice.

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
ORE
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt “Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych” współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.



Zadanie dla dociekliwych:

Sprawdź w manualu systemowym opis polecenia md5sum i wykonaj analogiczne czynności sprawdzające, ale z wykorzystaniem tego polecenia (pamiętaj o przekierowaniu wyników polecenia do pliku poprzez potok systemowy „>”) oraz z wykorzystaniem funkcji sprawdzającej md5sum.

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
ORE
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt “Strategia Wolnych i Otwartych Implementacji jako innowacyjny model zainteresowania kierunkami informatyczno-technicznymi oraz wspierania uczniów i uczennic w kształtowaniu kompetencji kluczowych” współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.