Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego

Laboratorium z przedmiotu:
Wprowadzenie do Kryptologii

Sprawozdanie z ćwiczenia laboratoryjnego nr 4:
Kryptografia asymetryczna

Prowadzący:
mgr inż. Marta Turowska

Wykonał: Radosław Relidzyński
Grupa: WCY20IY4S1
Data laboratoriów: 20.05.2021 r.

Spis treści

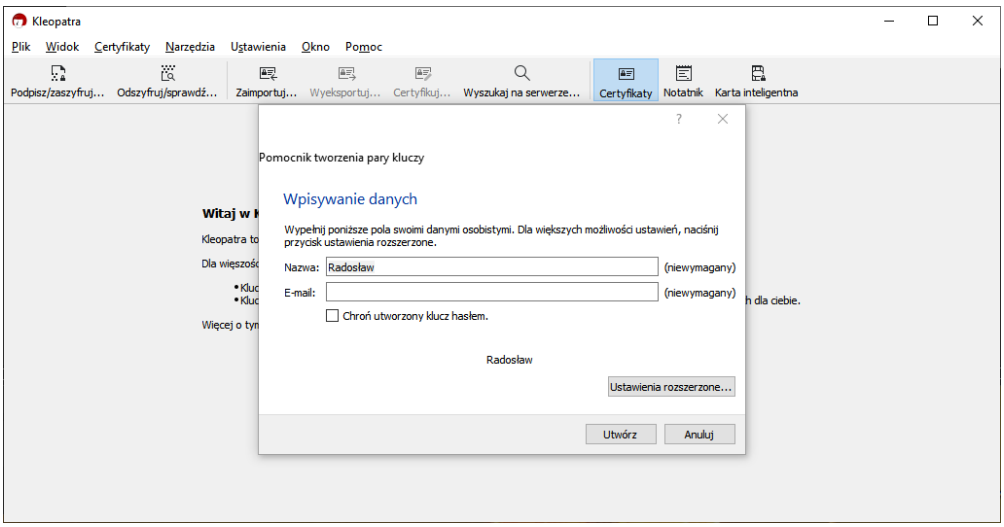
A. Treść zadania

Wygenerować parę kluczy publiczny i prywatny dla swojego adresu email, a następnie wygenerować podpis pliku i wyciągnąć wnioski z działania.

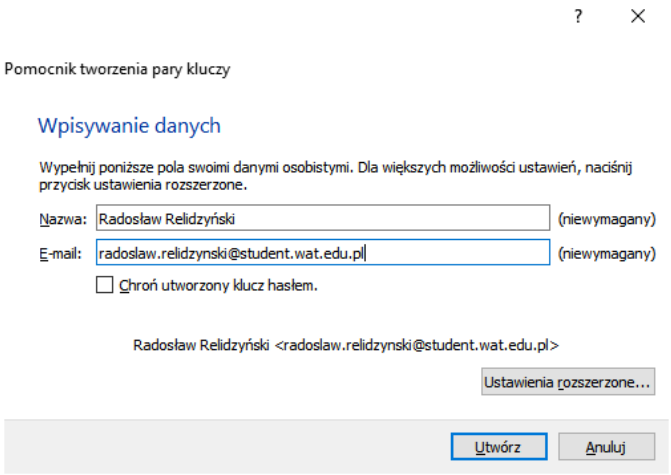
B. Kolejne działania

Generuję parę kluczy

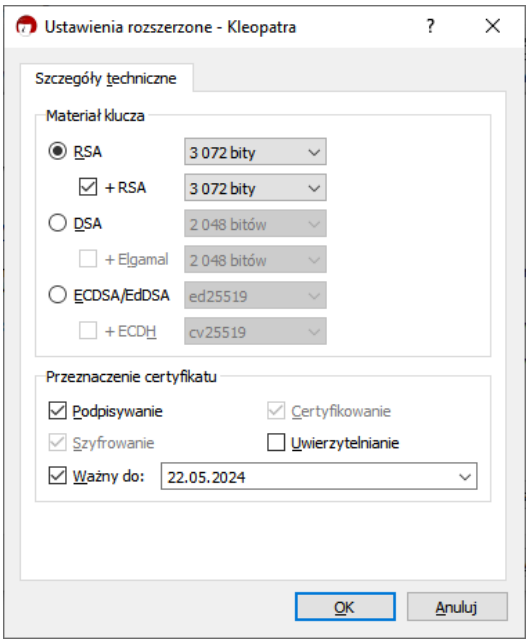
1. Klikam „Nowa para kluczy”.



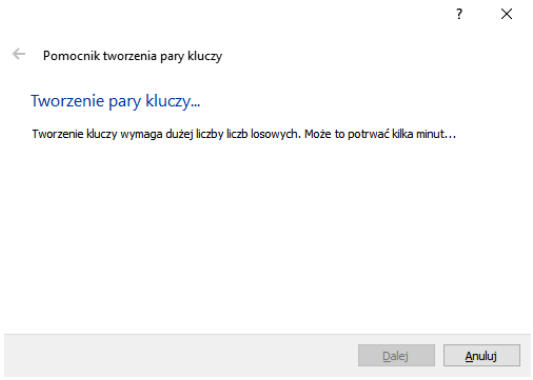
2. Uzupełniam dane.



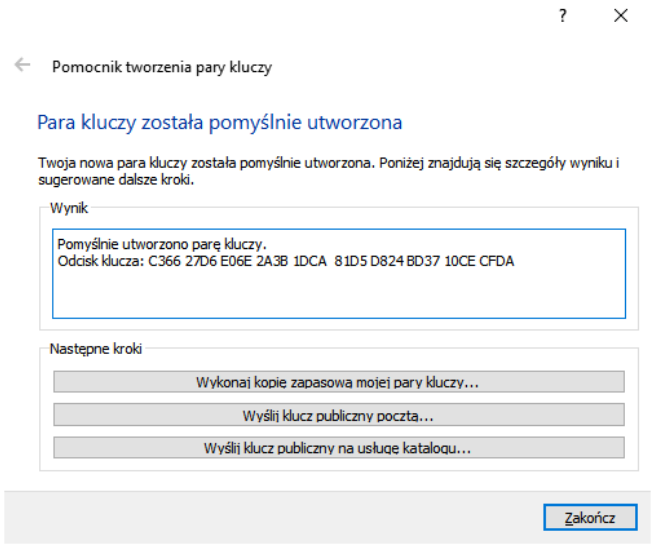
3. Wchodzę w „ustawienia rozszerzone…” i wybieram opcję materiału klucza „RSA”.



4. Klikam „OK”, a następnie „Utwórz”.

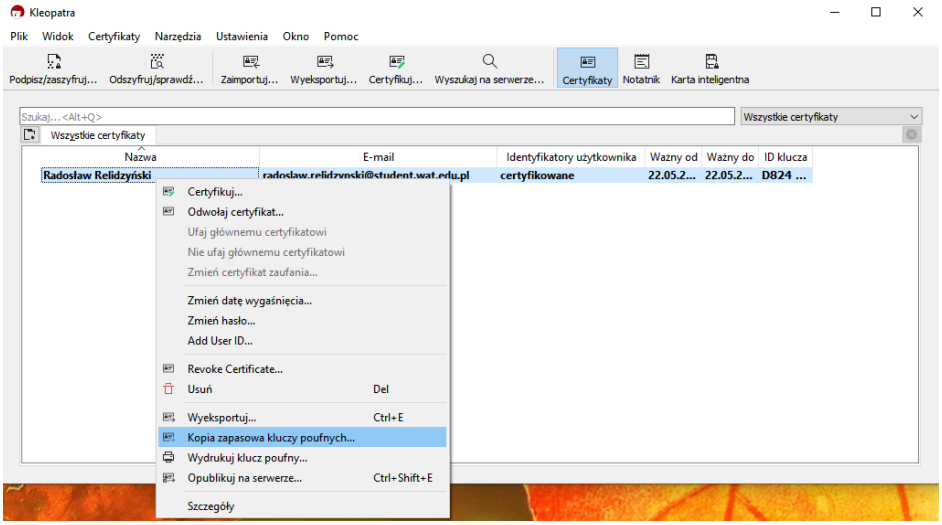


5. Otrzymuję komunikat o utworzeniu kluczy. (odcisk klucza: C366 27D6 E06E 2A3B 1DCA 81D5 D824 BD37 10CE CFDA)

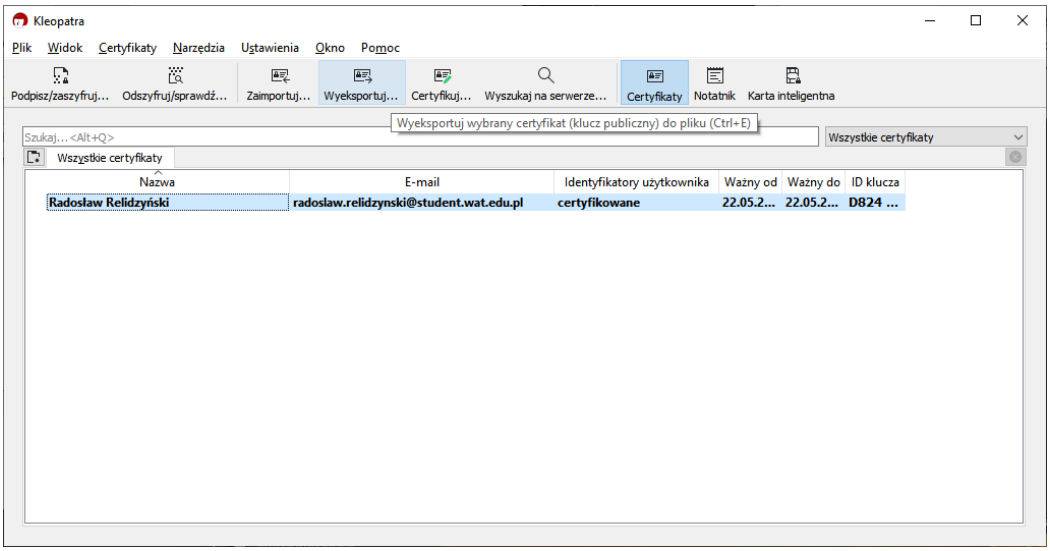


Tworzę kopię zapasową kluczy oraz eksportuję klucz publiczny

1. W głównym oknie programu klikam w utworzony certyfikat i wybieram opcję „Kopia zapasowa kluczy poufnych”. Następnie wybieram miejsce do jego zapisania i klikam „Zapisz”.

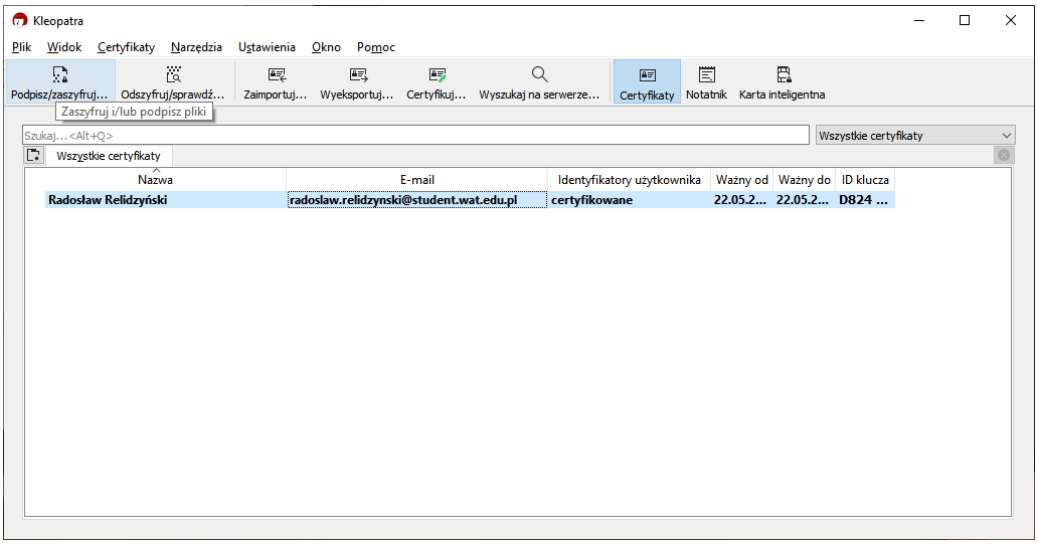


2. Po utworzeniu kopii zapasowej eksportuję klucz publiczny (opcja „Wyeksportuj…”). Następnie wybieram miejsce do jego zapisania i klikam „Zapisz”.

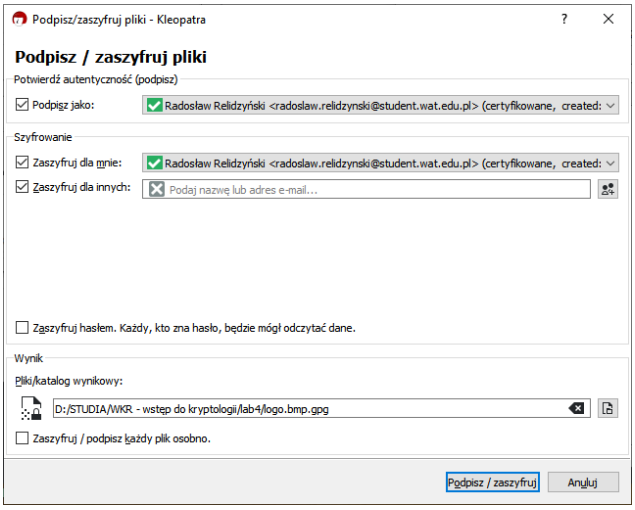


Szyfruję plik

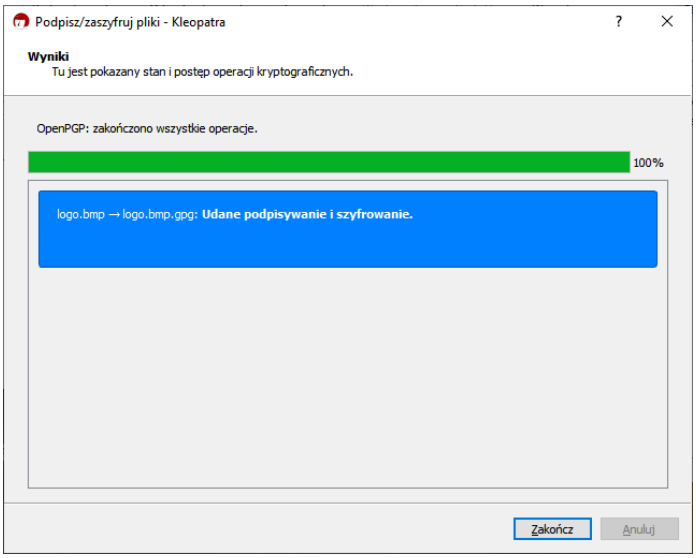
1. Wybieram opcję „Pospisz/zaszyfruj…” a następnie wybieram plik, który chcę zaszyfrować.



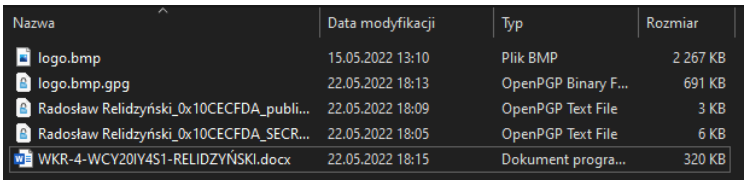
2. W dodatkowym oknie sprawdzam, czy wszystkie dane są poprawne i jeśli są to klikam „Podpisz/zaszyfruj”.



3. Otrzymuję komunikat o poprawnym podpisaniu i zaszyfrowaniu. Klikam „zakończ”.

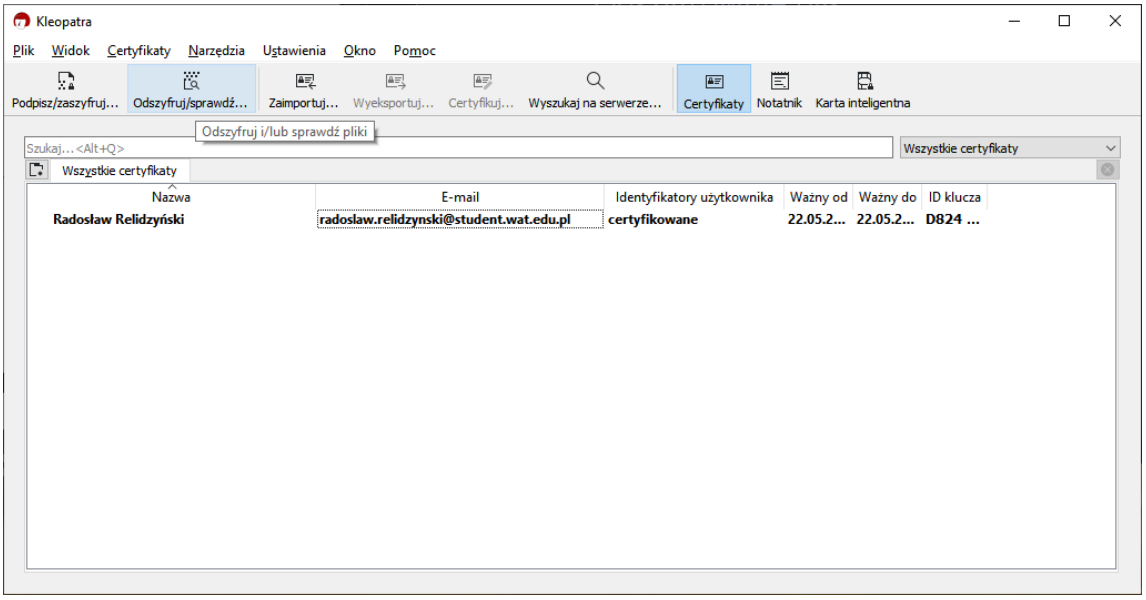


4. W tym momencie posiadam zaszyfrowany plik.

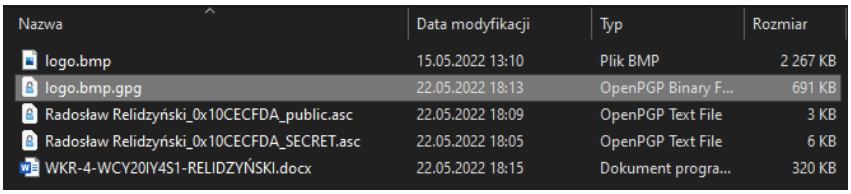


Odczytuję zaszyfrowany plik

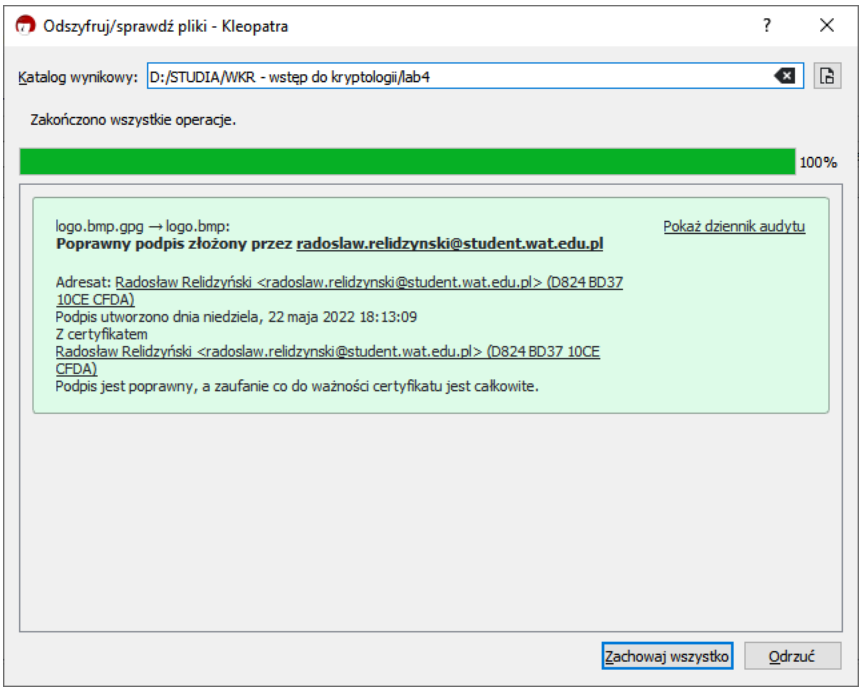
1. W głównym oknie programu wybieram opcję „Odszyfruj/sprawdź…”



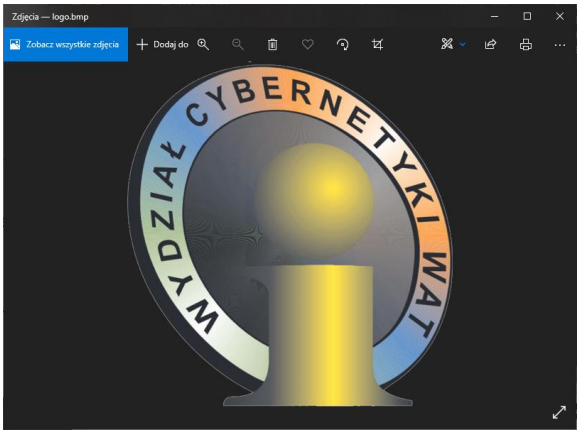
2. Wybieram zaszyfrowany plik i zatwierdzam „Otwórz”.



3. Otrzymuję informację o poprawnym podpisie i o zakończeniu operacji. Klikam opcję „Zachowaj wszystko”, a następnie w dodatkowym oknie „Zastąp”.

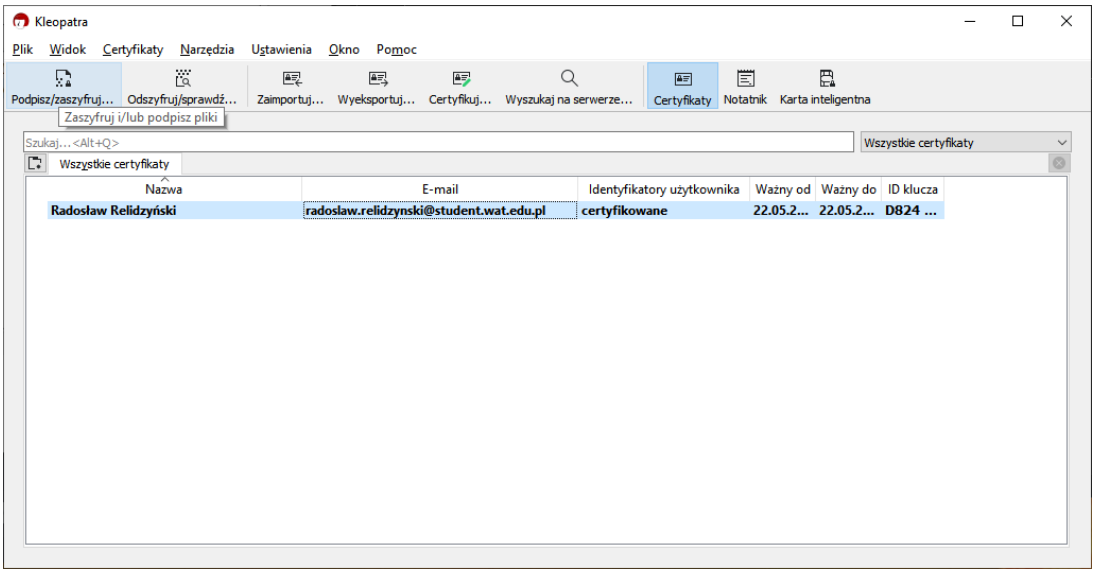


4. Logo po odczytaniu jest niezmienione.

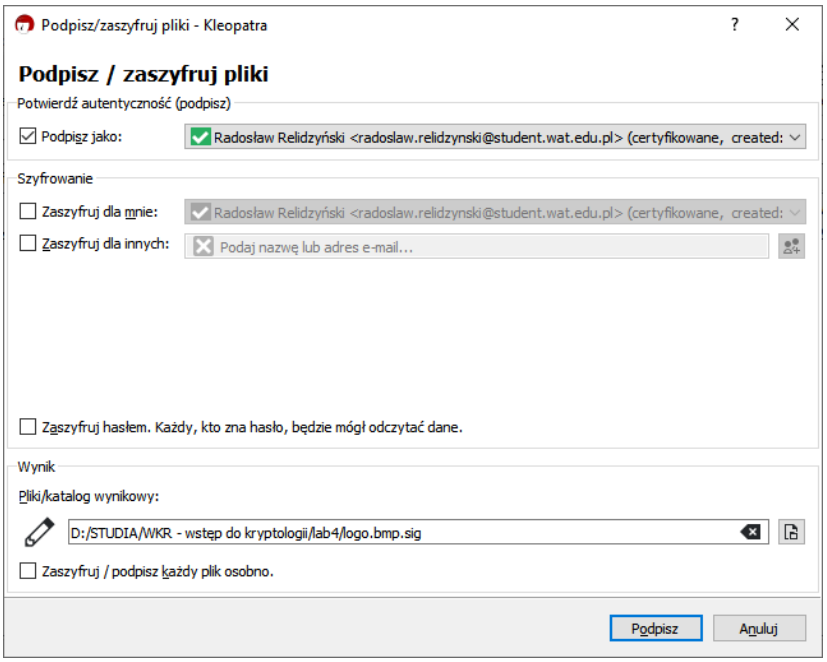


Wykonuję samo podpisanie pliku

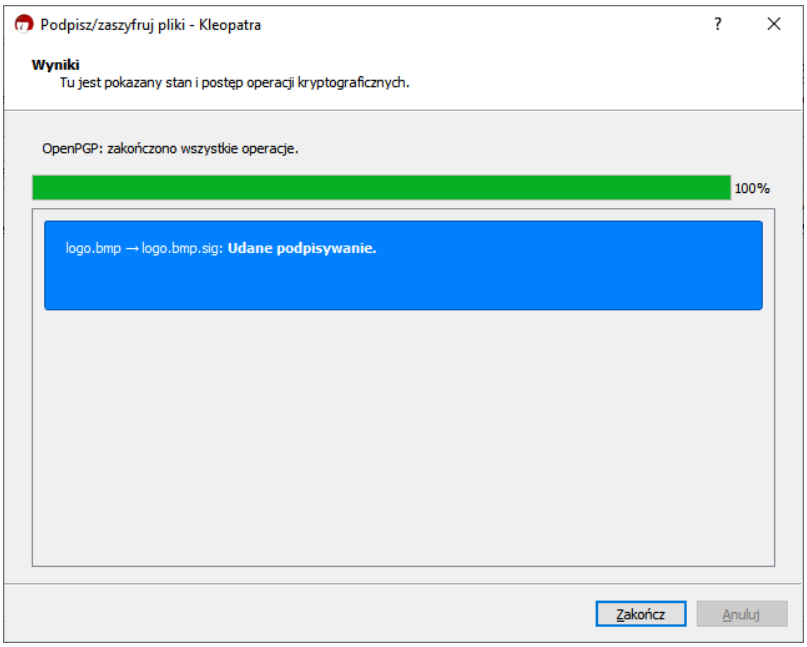
1. Ponownie wybieram opcję „Pospisz/zaszyfruj…” a następnie wybieram plik, który chcę zaszyfrować.



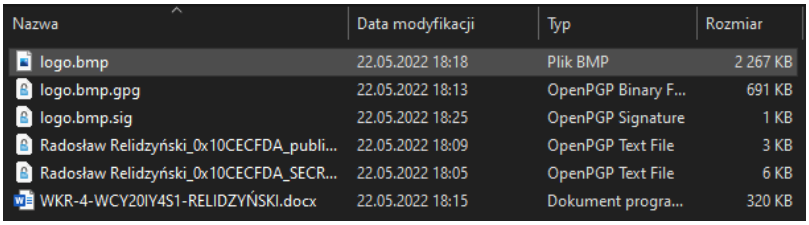
2. W dodatkowym oknie odznaczam opcje szyfrowania oraz sprawdzam, czy wszystkie dane są poprawne i jeśli są to klikam „Podpisz”.



3. Otrzymuję komunikat o poprawnym podpisaniu. Klikam „zakończ”.

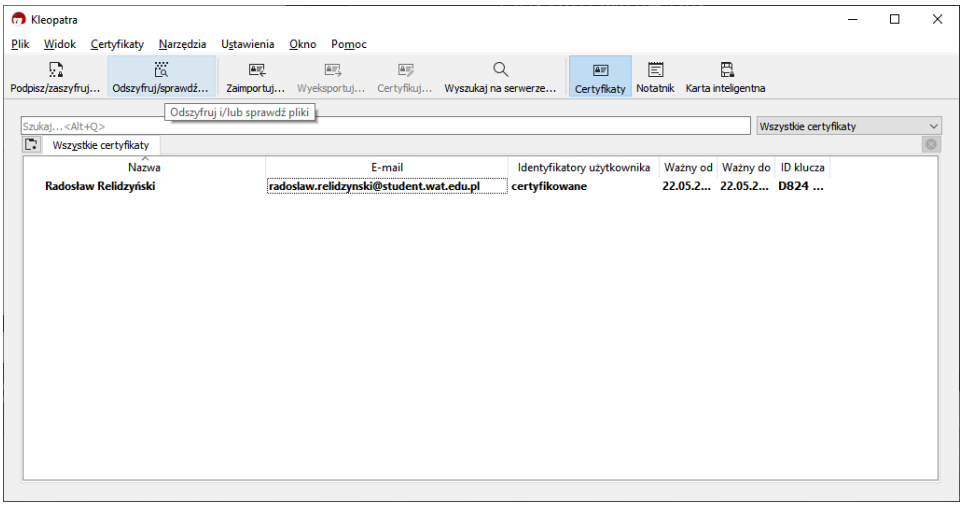


4. W tym momencie posiadam podpisany plik.

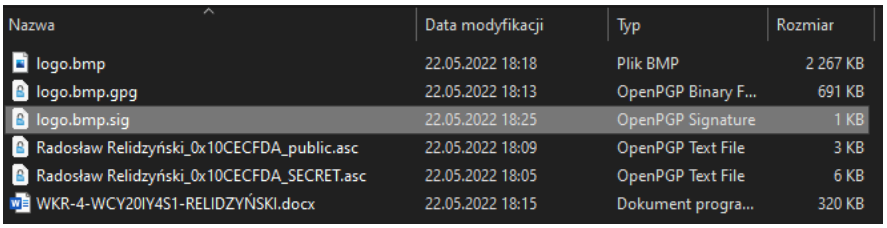


Odczytuję podpisany plik

1. W głównym oknie programu wybieram opcję „Odszyfruj/sprawdź…”

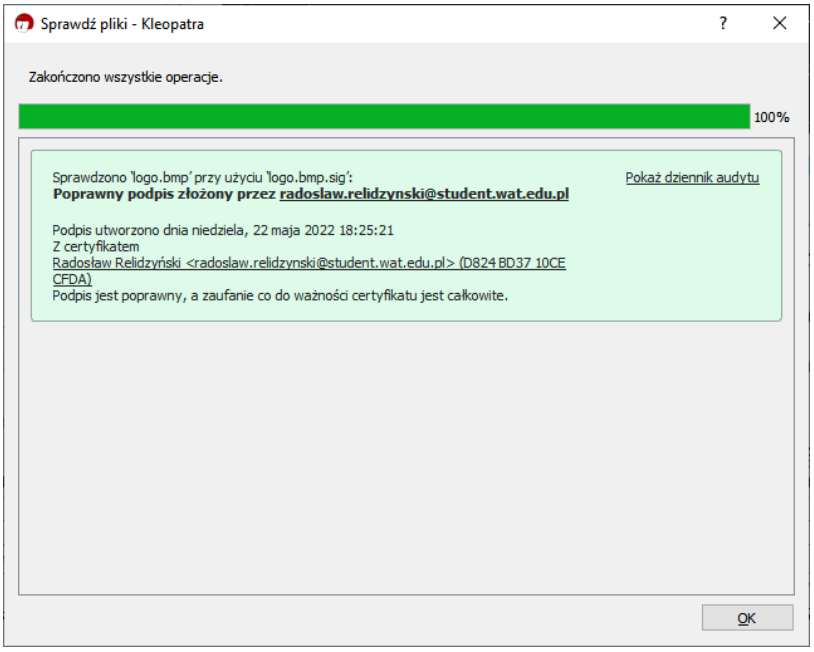


2. Wybieram podpisany plik i zatwierdzam „Otwórz”.



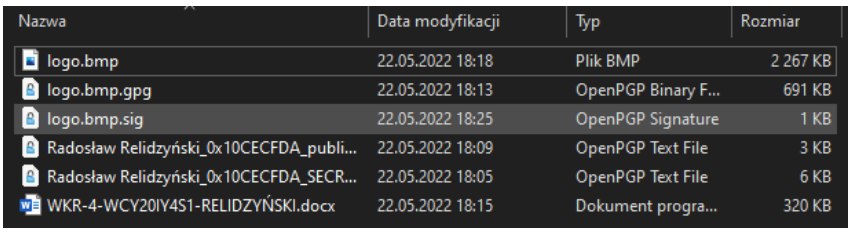
Nazwa	Data modyfikacji	Typ	Rozmiar
logo.bmp	22.05.2022 18:18	Plik BMP	2 267 KB
logo.bmp.gpg	22.05.2022 18:13	OpenPGP Binary F...	691 KB
logo.bmp.sig	22.05.2022 18:25	OpenPGP Signature	1 KB
Radosław Relidzyński_0x10CECFDA_public.asc	22.05.2022 18:09	OpenPGP Text File	3 KB
Radosław Relidzyński_0x10CECFDA_SECRET.asc	22.05.2022 18:05	OpenPGP Text File	6 KB
WKR-4-WCY20IY4S1-RELIDZYŃSKI.docx	22.05.2022 18:15	Dokument progra...	320 KB

3. Otrzymuję informację o poprawnym podpisie i o zakończeniu operacji. Klikam opcję „OK”.



Wnioski

Efekt końcowy ćwiczenia:



Nazwa	Data modyfikacji	Typ	Rozmiar
logo.bmp	22.05.2022 18:18	Plik BMP	2 267 KB
logo.bmp.gpg	22.05.2022 18:13	OpenPGP Binary F...	691 KB
logo.bmp.sig	22.05.2022 18:25	OpenPGP Signature	1 KB
Radosław Relidzyński_0x10CECFDA_publi...	22.05.2022 18:09	OpenPGP Text File	3 KB
Radosław Relidzyński_0x10CECFDA_SECR...	22.05.2022 18:05	OpenPGP Text File	6 KB
WKR-4-WCY20IY4S1-RELIDZYŃSKI.docx	22.05.2022 18:15	Dokument progra...	320 KB

Podpis pliku zawiera jedynie informację o nadawcy pliku, przez co waży zaledwie 1 KB. Pozwala on jedynie na sprawdzenie autentyczności pochodzenia pliku (w przeciwieństwie do szyfrowania pliku, który posiada również informacje o zawartości).

Podpisywanie pliku jest więc wydajną i skuteczną metodą na sprawdzanie autentyczności pochodzenia pliku na podstawie jego nadawcy. Przez swój niewielki rozmiar sprawdziłby się w sytuacji, kiedy takich podpisów potrzeba by było w znacznej ilości. Chcąc przechowywać zaszyfrowane informacje kosztowałoby to ogromną ilość pamięci. Potwierdza to wydajność korzystania z podpisów.