***Wojskowa Akademia Techniczna***

***im. Jarosława Dąbrowskiego***

Laboratorium z przedmiotu:

[Wprowadzenie](http://shaql.w.staszic.waw.pl/~shaql/wcy/viewforum.php?f=13) 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 2](#_Toc104137131)

[B. Kolejne działania 2](#_Toc104137132)

[Generuję parę kluczy 2](#_Toc104137133)

[Tworzę kopię zapasową kluczy oraz eksportuję klucz publiczny 4](#_Toc104137134)

[Szyfruję plik 4](#_Toc104137135)

[Odczytuję zaszyfrowany plik 6](#_Toc104137136)

[Wykonuję samo podpisanie pliku 7](#_Toc104137137)

[Odczytuję podpisany plik 9](#_Toc104137138)

[Wnioski 10](#_Toc104137139)

# Treść zadania

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

# Kolejne działania

### Generuję parę kluczy

1. Klikam „Nowa para kluczy”.

Obraz zawierający tekst

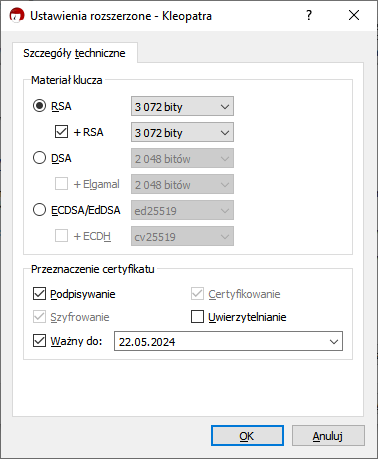
Opis wygenerowany automatycznie

1. Uzupełniam dane.

Obraz zawierający tekst

Opis wygenerowany automatycznie

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



1. Klikam „OK”, a następnie „Utwórz”.

Obraz zawierający tekst

Opis wygenerowany automatycznie

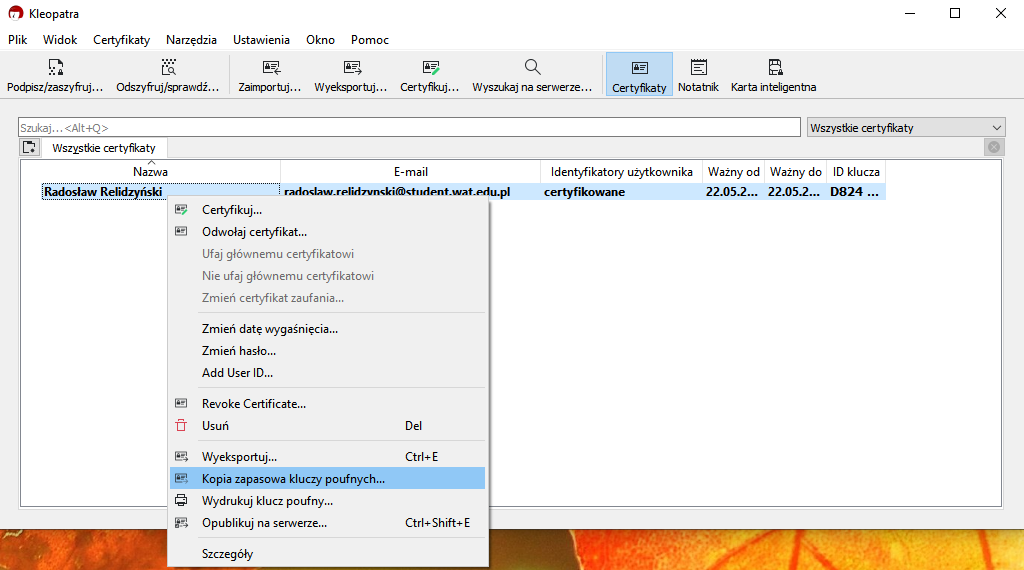
1. Otrzymuję komunikat o utworzeniu kluczy. (odcisk klucza: C366 27D6 E06E 2A3B 1DCA 81D5 D824 BD37 10CE CFDA)

Obraz zawierający tekst

Opis wygenerowany automatycznie

### 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”.



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

Obraz zawierający tekst

Opis wygenerowany automatycznie

### Szyfruję plik

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

Obraz zawierający tekst

Opis wygenerowany automatycznie

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

Obraz zawierający tekst

Opis wygenerowany automatycznie

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

Obraz zawierający tekst

Opis wygenerowany automatycznie

1. W tym momencie posiadam zaszyfrowany plik.

Obraz zawierający tekst

Opis wygenerowany automatycznie

### Odczytuję zaszyfrowany plik

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

Obraz zawierający tekst

Opis wygenerowany automatycznie

1. Wybieram zaszyfrowany plik i zatwierdzam „Otwórz”.

Obraz zawierający tekst

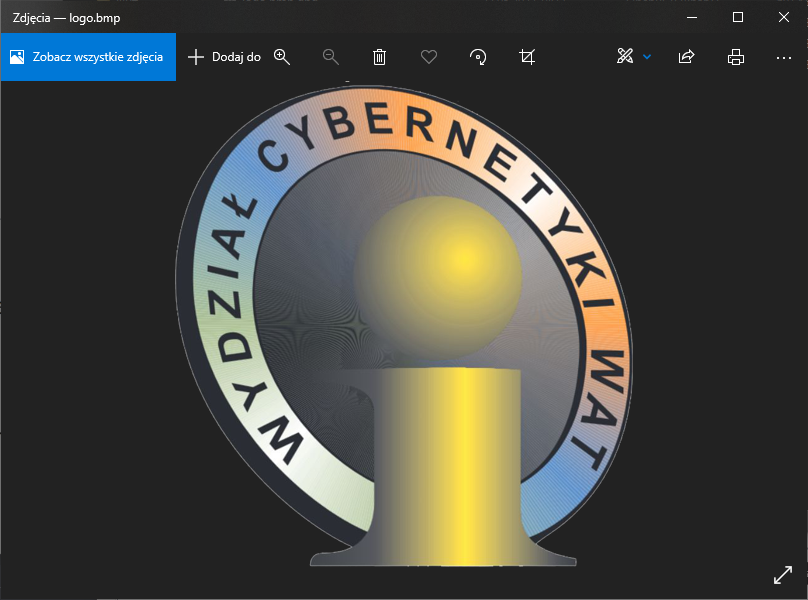
Opis wygenerowany automatycznie

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

Obraz zawierający tekst

Opis wygenerowany automatycznie

1. Logo po odczytaniu jest niezmienione.



### Wykonuję samo podpisanie pliku

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

Obraz zawierający tekst

Opis wygenerowany automatycznie

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

Obraz zawierający tekst

Opis wygenerowany automatycznie

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

Obraz zawierający tekst

Opis wygenerowany automatycznie

1. W tym momencie posiadam podpisany plik.

Obraz zawierający tekst

Opis wygenerowany automatycznie

### Odczytuję podpisany plik

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

Obraz zawierający tekst

Opis wygenerowany automatycznie

1. Wybieram podpisany plik i zatwierdzam „Otwórz”.

Obraz zawierający tekst

Opis wygenerowany automatycznie

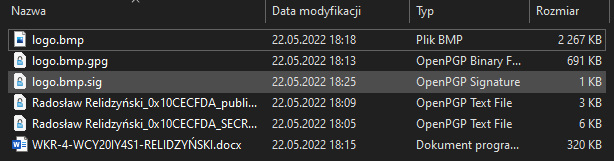
1. Otrzymuję informację o poprawnym podpisie i o zakończeniu operacji. Klikam opcję „OK”.

Obraz zawierający tekst

Opis wygenerowany automatycznie

### Wnioski

Efekt końcowy ćwiczenia:



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.