

Politechnika Częstochowska
Wydział Inżynierii Mechanicznej i Informatyki



Laboratorium z przedmiotu
Bezpieczeństwo komunikacji elektronicznej

Sprawozdanie nr 10
Szyfrowanie i podpisywanie poczty elektronicznej

Damian Łukasik
nr. 112993
II stopień, 2 semestr , 1 rok

Częstochowa 28 grudnia 2015 r.

1. Cel ćwiczenia laboratoryjnego

Celem ćwiczenia laboratoryjnego jest zapoznanie się z mechanizmami szyfrowania i podpisywania poczty elektronicznej za pomocą jednego z popularniejszych algorytmów szyfrowania PGP. Z przeprowadzonego ćwiczenia zostały wyciągnięte wnioski. Do sprawozdania załączono zrzuty ekranu w postaci *printscreensów*.

2. Opis ćwiczenia

PGP (ang. *Pretty Good Privacy*) jest stosowany głównie przy komunikacji za pośrednictwem poczty elektronicznej, umożliwia także podpisywanie i szyfrowanie plików na dysku. Na potrzeby laboratorium została wykorzystana darmowa implementacja algorytmów PGP, GnuPG¹. W tym celu skorzystano z darmowego klienta poczty – *Thunderbird* oraz jeden z dodatków do niego pozwalający na łatwą konfigurację PGP – *Enigmail*

3. Przebieg ćwiczenia laboratoryjnego

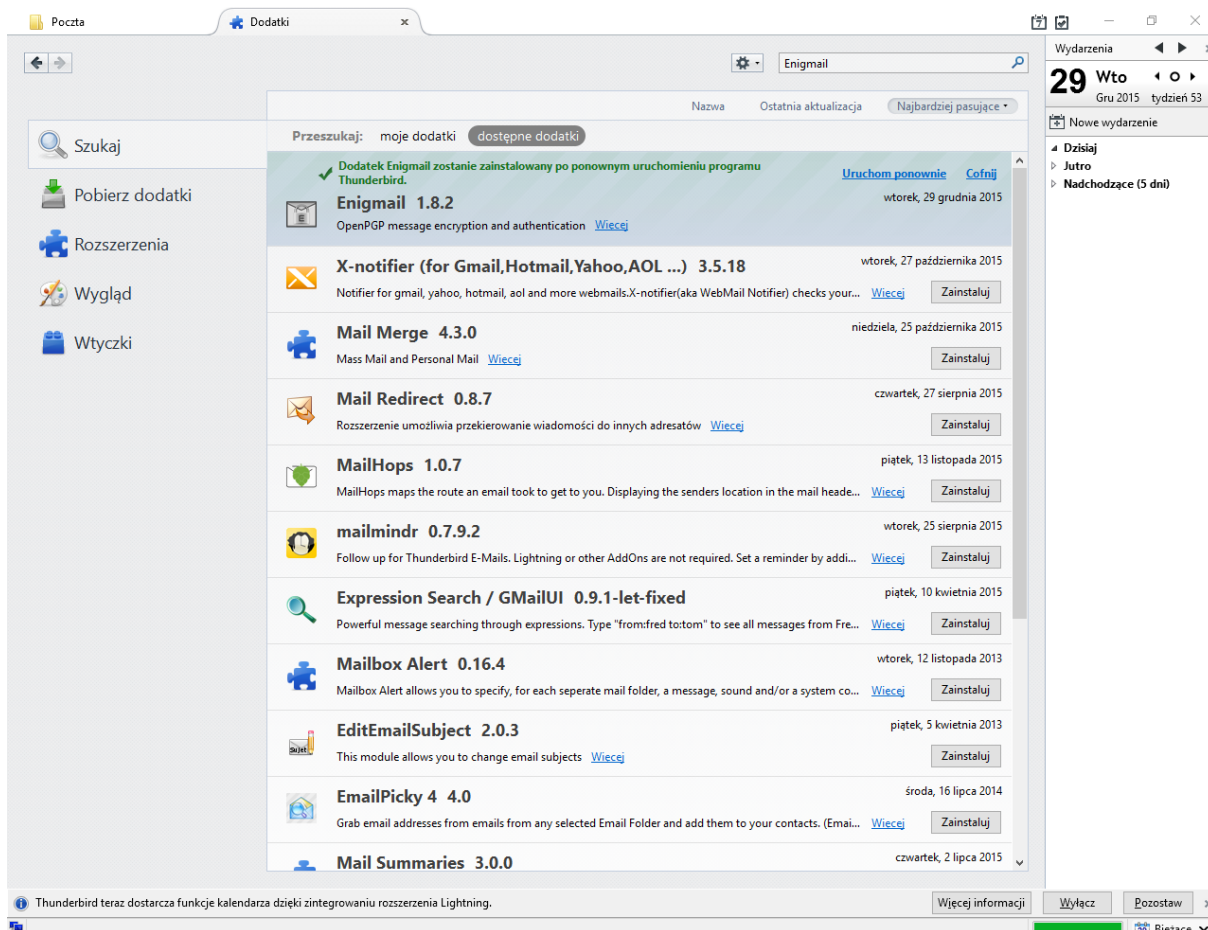
W pierwszej kolejności zainstalowano *Thunderbird* oraz *GnuPG*.

W drugiej kolejności skonfigurowano klienta poczty i dodatku *Enigmail*, który pozwoli w łatwy sposób zarządzać funkcjonalnościami GPG w *Thunderbirdzie*.

Rys1. Okno startowe *Thunderbird*.

Przy pierwszym uruchomieniu klienta poczty, otrzymujemy okno startowe w którym uzupełniamy dane naszego konta *e-mail*, bądź zakładamy nowe konto, z którego będziemy korzystać poprzez *Thunderbirda*.

¹ <http://www.gnupg.org/>



Rys2. Manager dodatków Thunderbird.

Po połączeniu klienta poczty z kontem, pobrano i zainstalowano dodatek *Enigmail* poprzez manager dodatków *Thunderbirda*.

W następnej kolejności skonfigurowano *OpenPGP* za pośrednictwem kreatora konfiguracji. Uruchamiany go po zainstalowaniu dodatku *Enigmail* poprzez uruchomienie z menu głównego *Thunderbirda* (*Enigmail* → *Asystent Konfiguracji*).

Welcome to the Enigmail Setup Wizard

It looks like you started Enigmail for the first time on this computer. In order to use Enigmail, you need to first set it up properly. This assistant can guide you through the setup process.

Do you want to set up Enigmail now, or do you wish to do this later?

- ☒ Start setup now
☐ Configure Enigmail later

< Wstecz

Dalej >

Anuluj

*Rys3. Konfiguracja Enigmail.***How would you like to Configure Enigmail?**

Would you like to setup Enigmail manually, or do you need assistance in the setup process?

- ☒ I prefer a standard configuration (recommended for beginners)
☐ I prefer an extended configuration (recommended for advanced users)
☐ I prefer a manual configuration (recommended for experts)

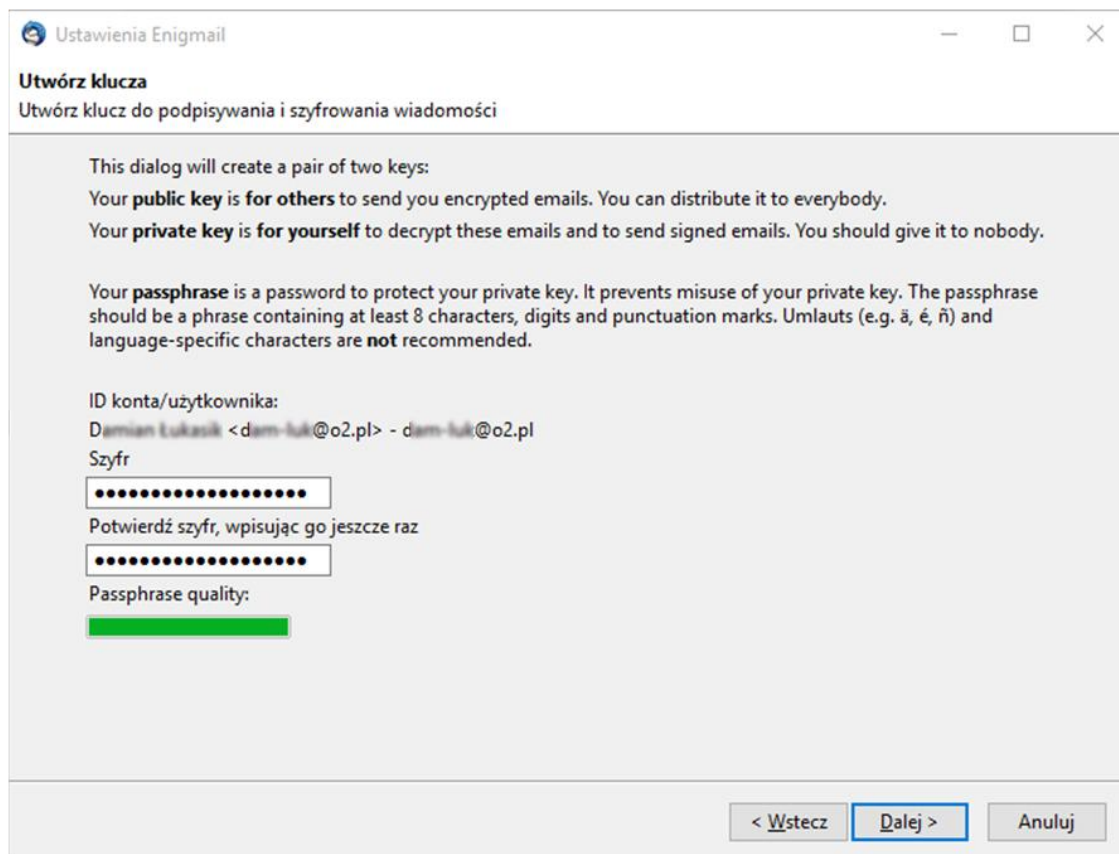
< Wstecz

Dalej >

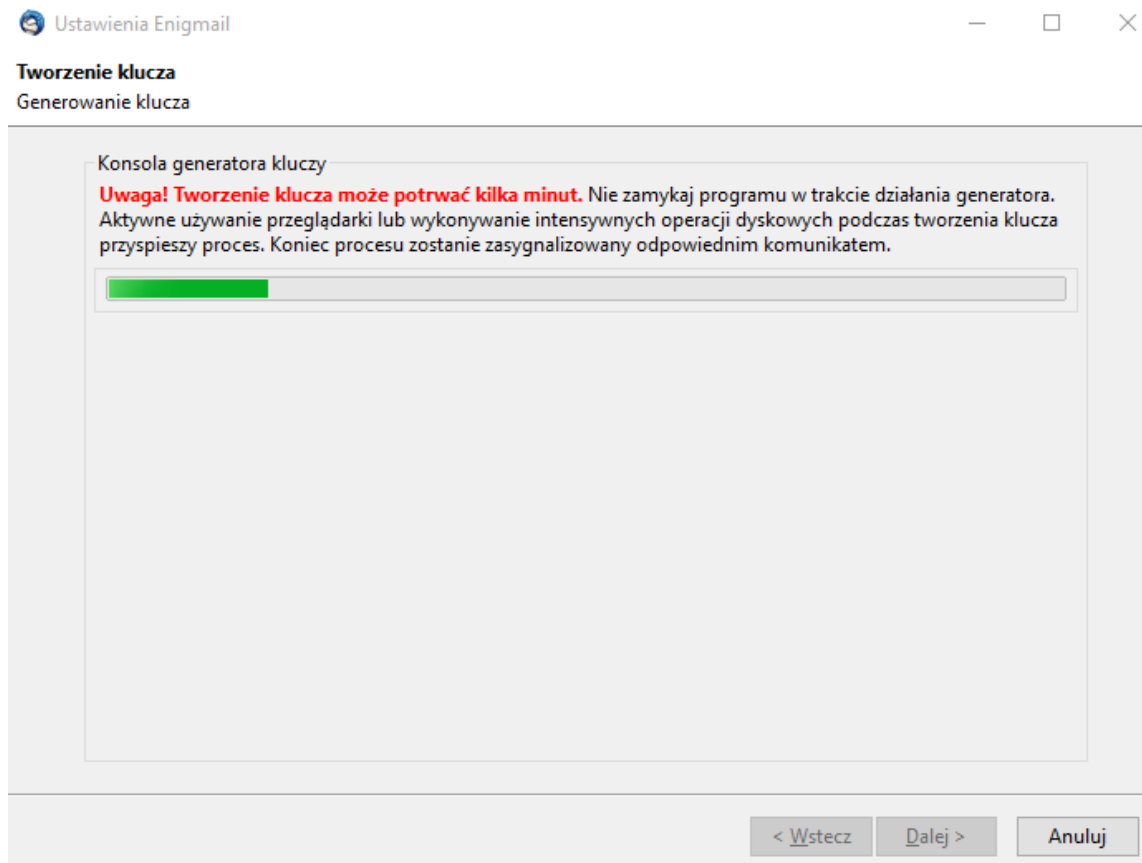
Anuluj

Rys4. Konfiguracja Enigmail.

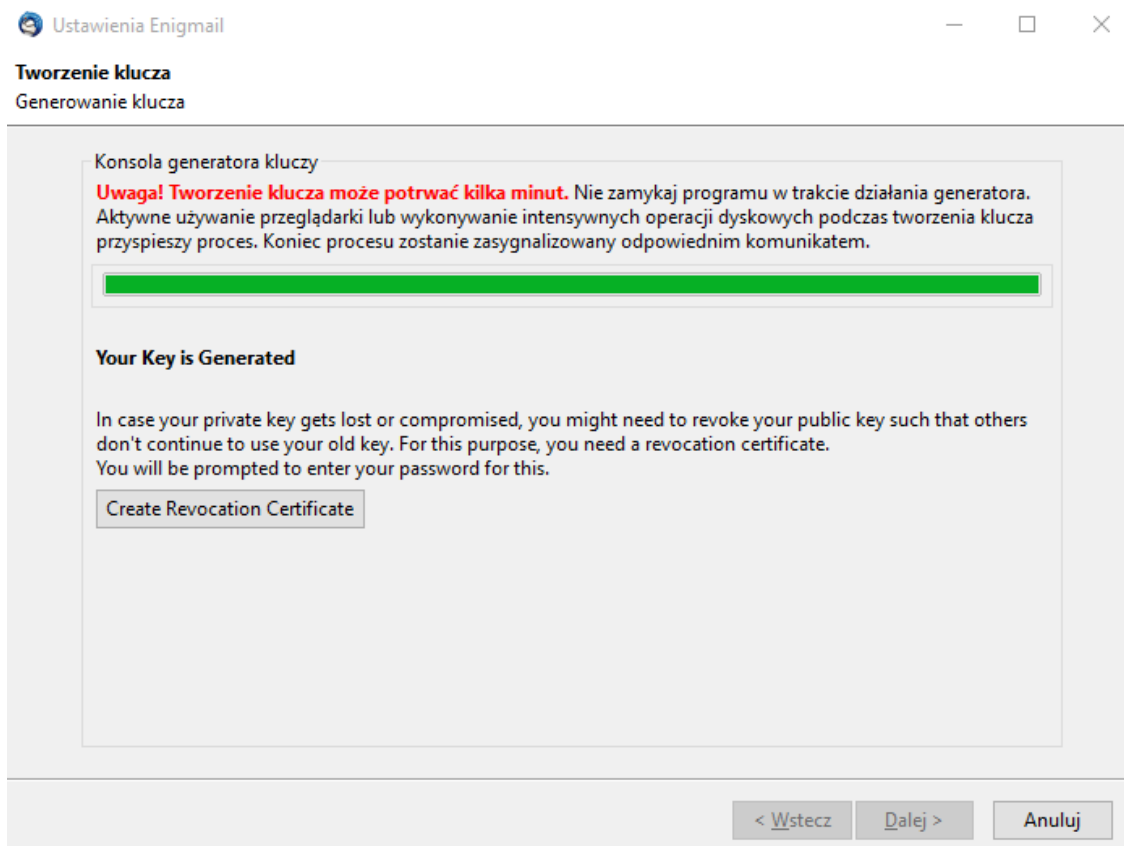
Następnie utworzono klucze do podpisywania wiadomości e-mail.



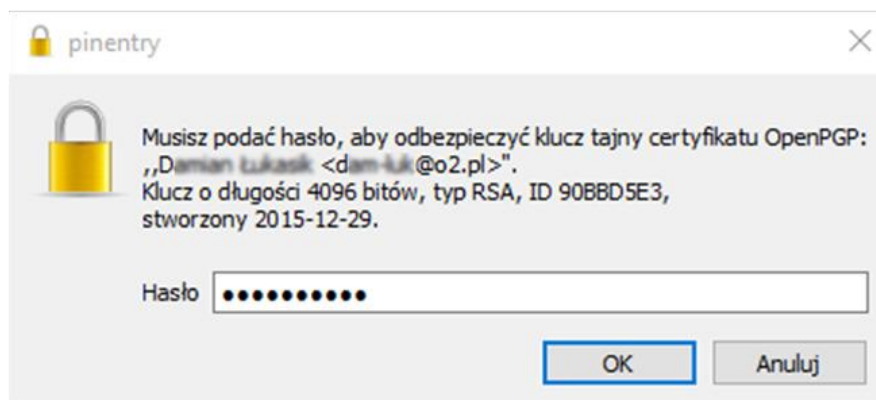
Rys5. Tworzenie kluczy szyfrujących.



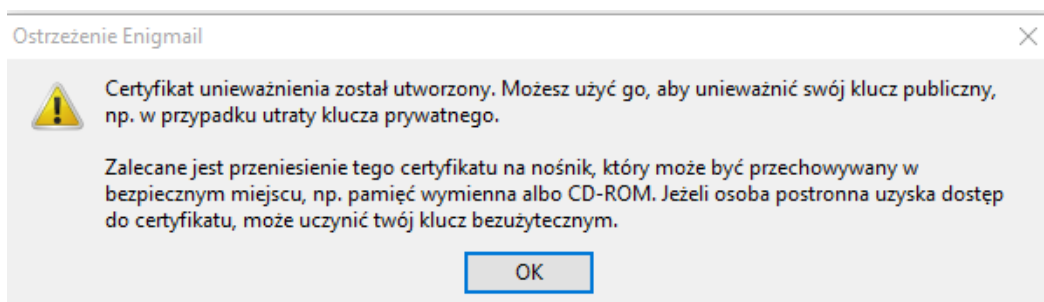
Rys6. Generowanie klucza.



Rys7. Tworzenie certyfikatu.

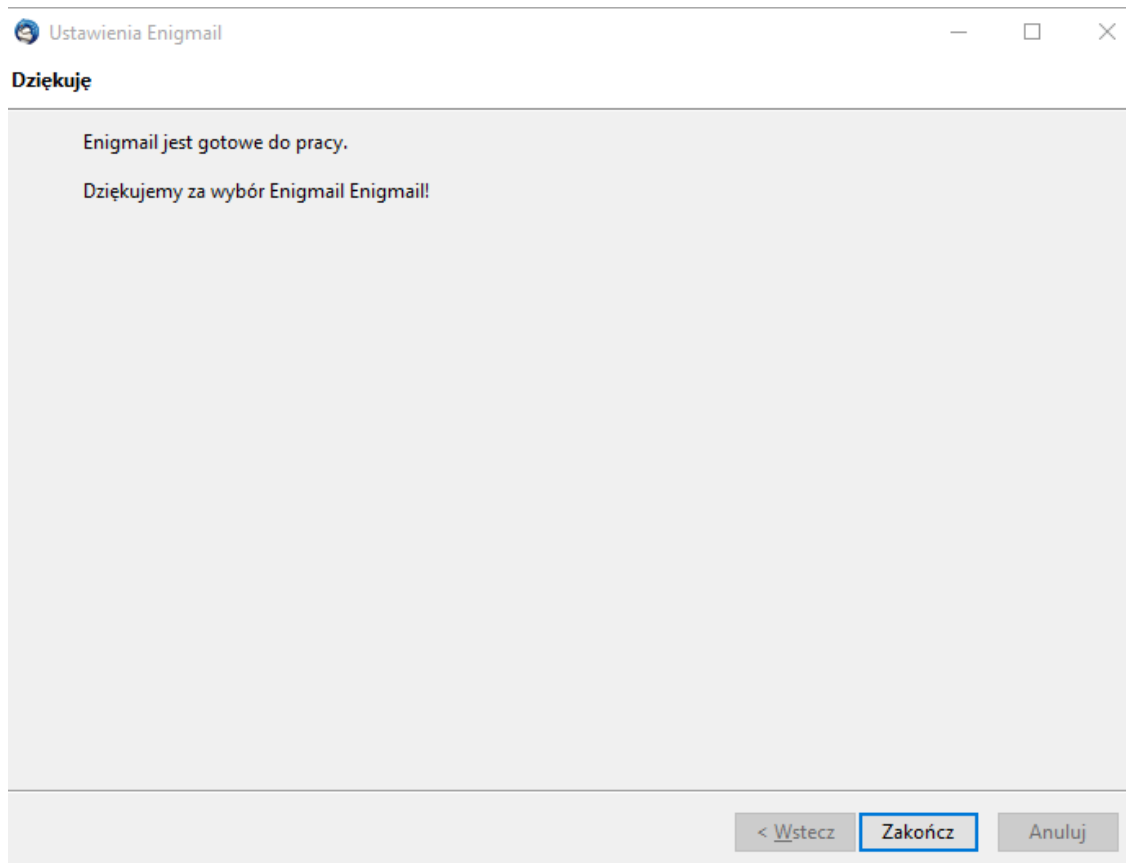


Rys8. Wprowadzanie hasła.

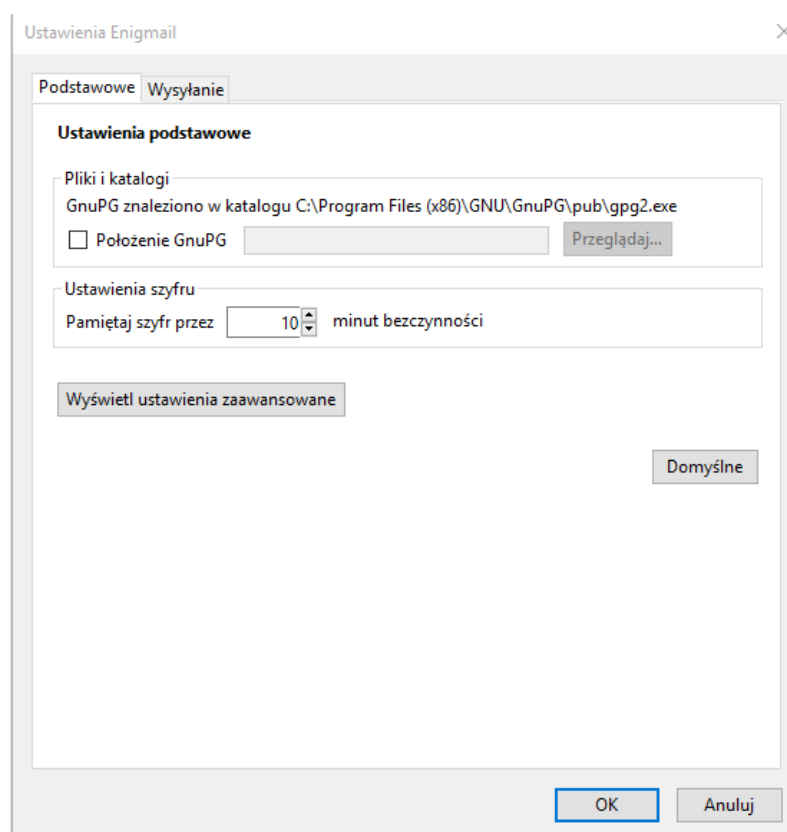


Rys9. Komunikat Enigmail.

Po wygenerowaniu pary kluczy prywatnego i publicznego, kreator oferuje również opcję wygenerowania klucza unieważniającego, którego możemy użyć w celu unieważnienia naszych kluczy w momencie np.: włamania na konto poczty.

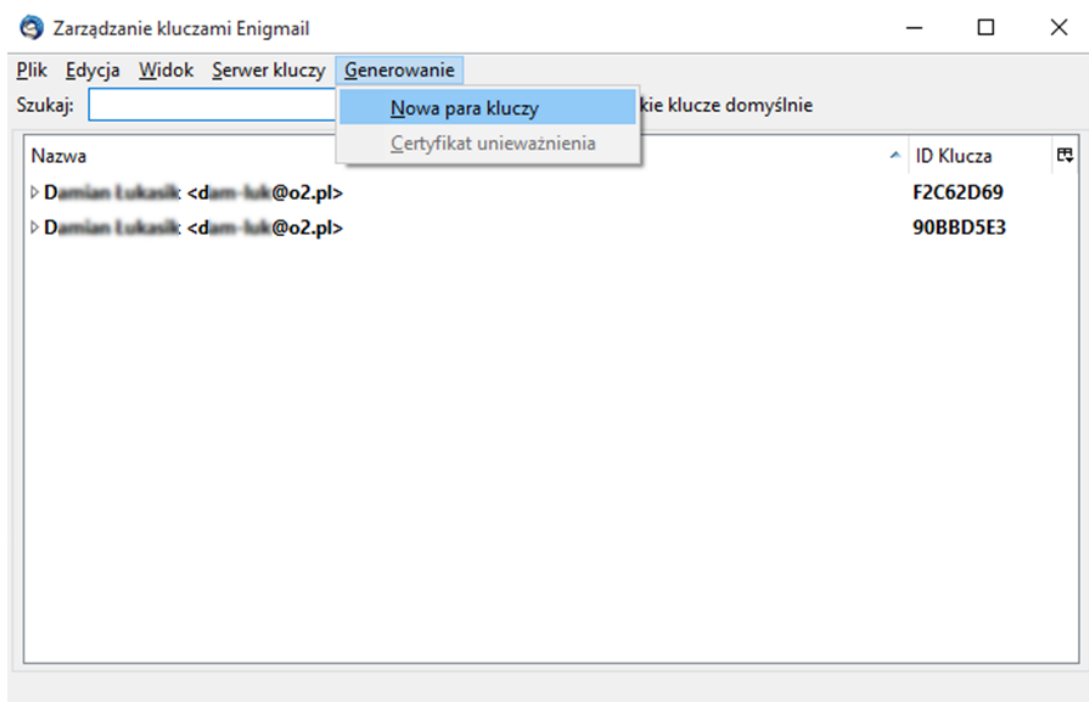


Rys10. Końcowe okno kreatora konfiguracji.

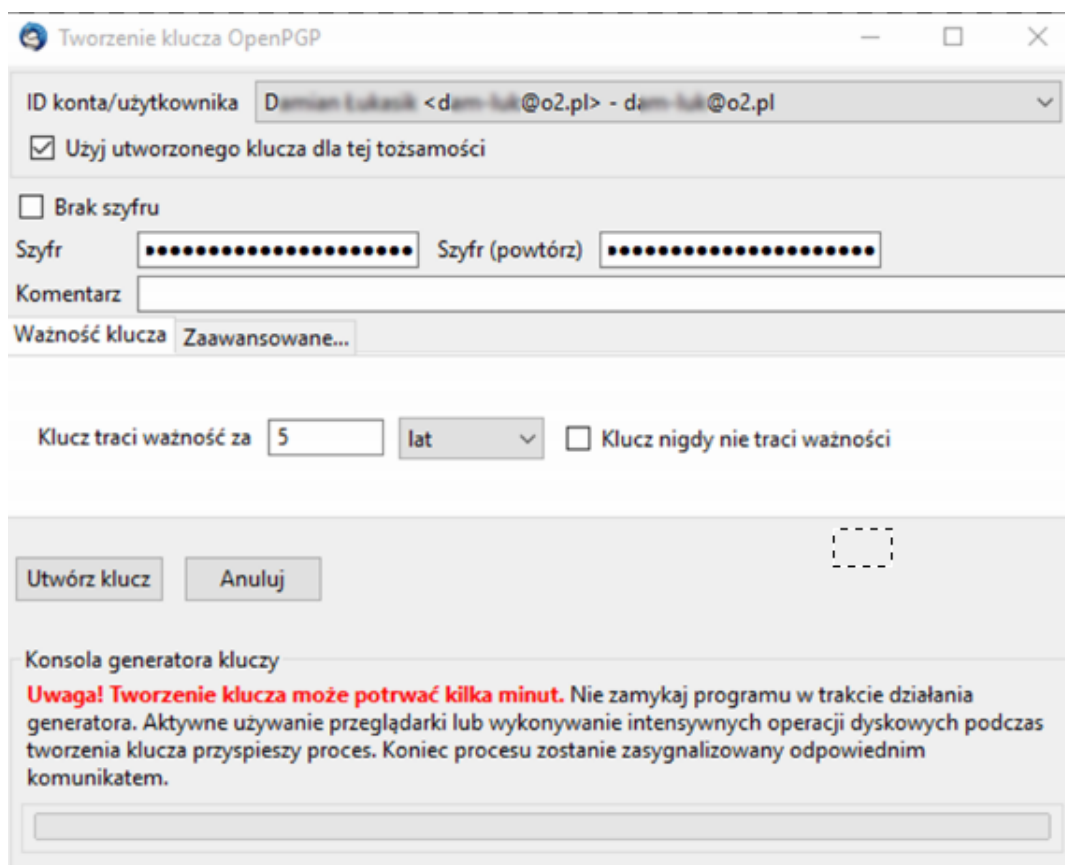


Rys11. Ręczna konfiguracja OpenPGP w Enigmail.

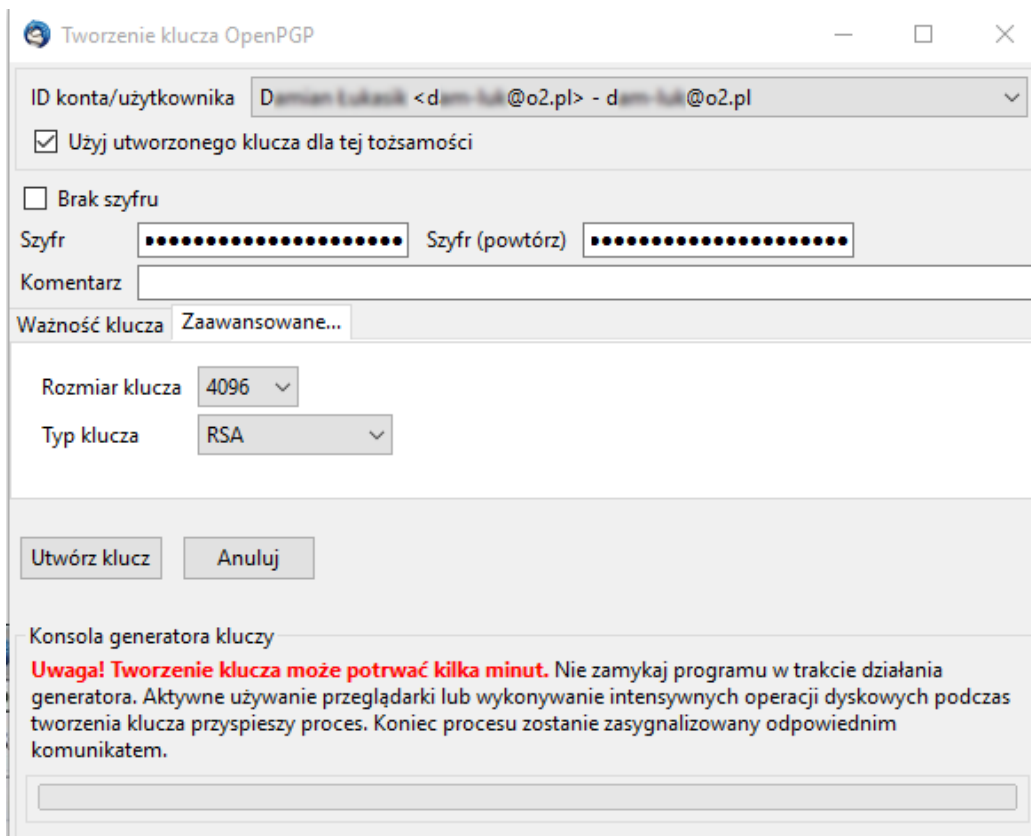
Konfigurację *OpenPGP* można przeprowadzić ręcznie (*OpenPGP* → *ustawienia*).



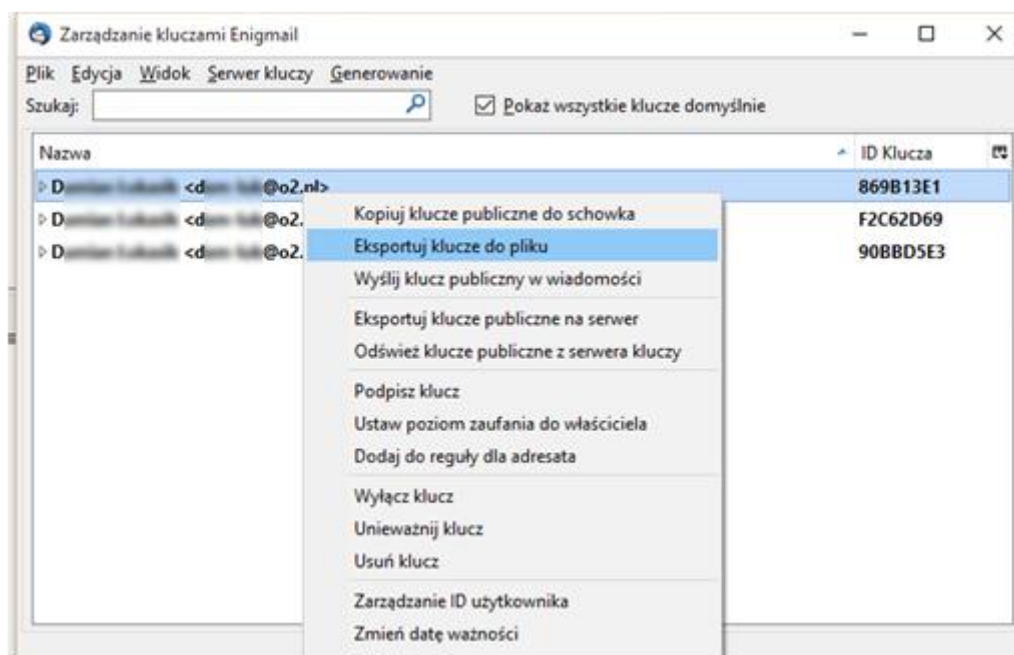
Rys12. Widok Zarządzania kluczami w Enigmail.



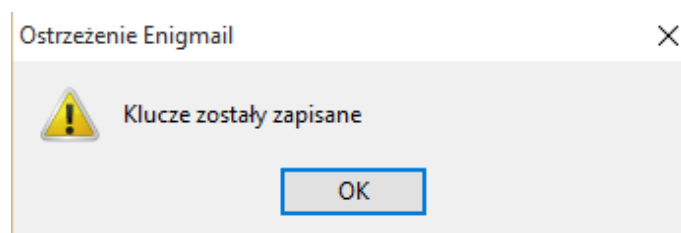
Rys13. Ręczne generowanie nowej pary kluczy.



Rys14. Ręczne generowanie nowej pary kluczy.

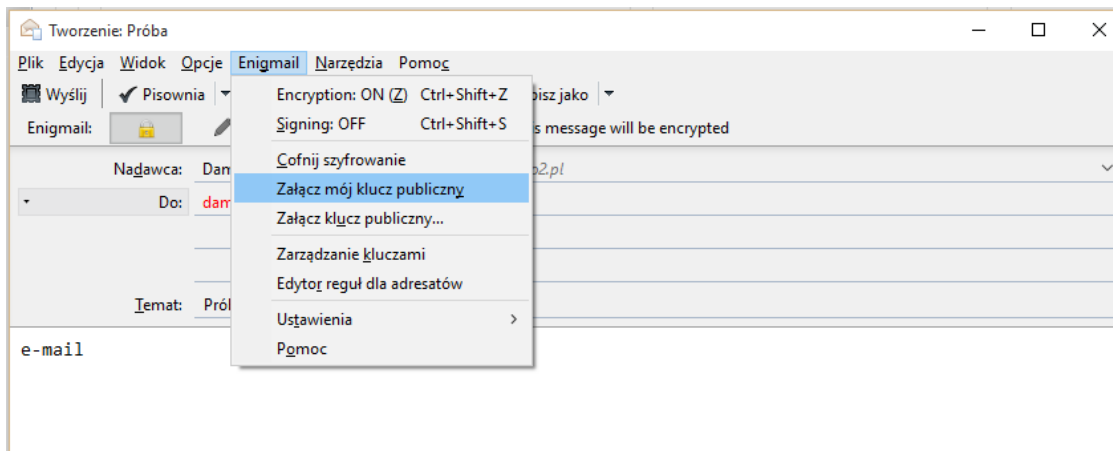


Rys15. Eksport klucza do pliku.

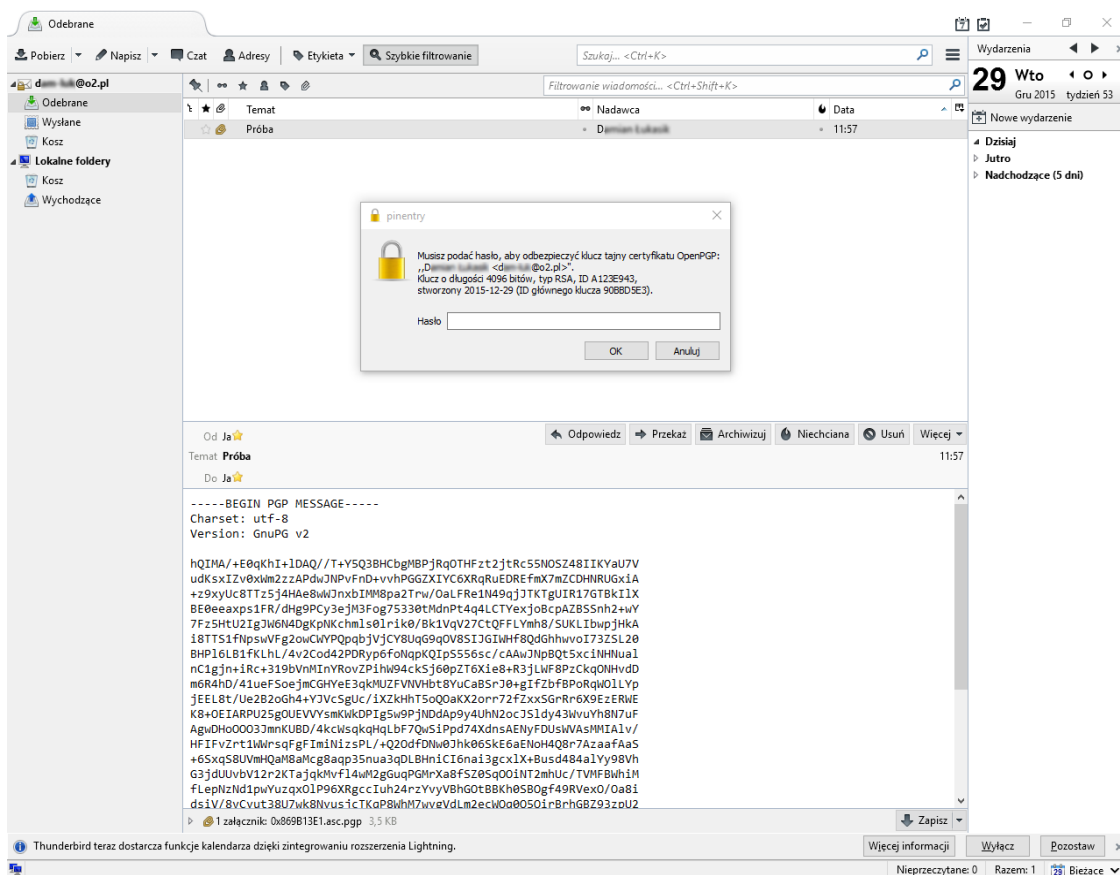


Rys16. Pomyślnie zakończony eksport klucza do pliku.

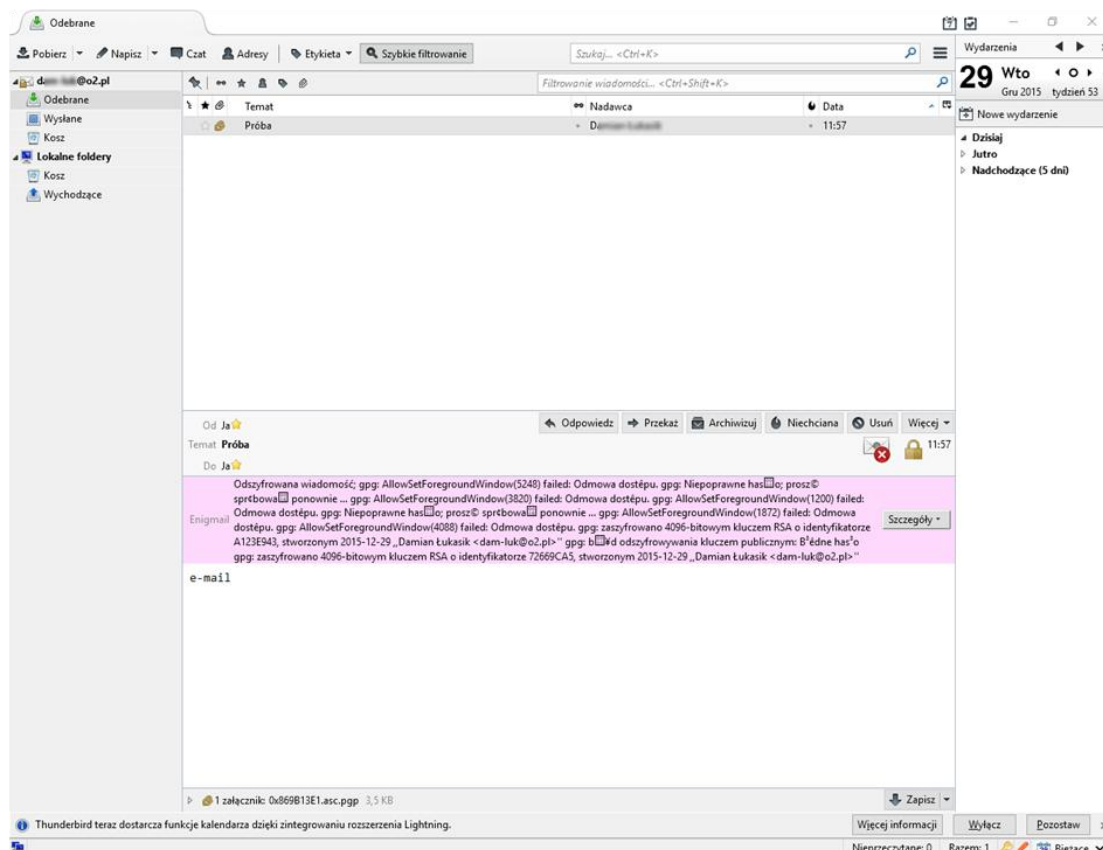
Po wygenerowaniu kluczy, przesłano klucz publiczny do osoby, z którą ma być przeprowadzona korespondencja zaszyfrowaną pocztą. W tym celu wystarczy załączyć klucz publiczny do przesyłanej wiadomości poprzez opcję *Załącz mój klucz publiczny* w menu *Enigmail*.



Rys17. Dołączanie klucza do szyfrowanej wiadomości.



Rys18. Odbiór zaszyfrowanej wiadomości.



Rys18. Odszyfrowana wiadomość.

4. Wnioski

Laboratorium zrealizowano zgodnie z instrukcją. Zapoznano się z bezpiecznym sposobem przesyłania poczty elektronicznej w oparciu o *OpenPGP*.

Wykorzystanie szyfrowania PGP w programie *Thunderbird* z dodatkiem *Enigmali* jest proste w obsłudze oraz w użytkowaniu, część opcji jest wykonywana automatycznie, a obsługa *OpenPGP* jest ograniczona do przeprowadzenia konfiguracji *Enigmali* przy pomocy kreatora konfiguracji. Dzięki zastosowaniu dodatku *Enigmali* przesyłane wiadomości były nie do odczytania bez posiadania odpowiedniego klucza.