Zaawansowane Metody Programowania - Dokumentacja

Bartosz Sabat
Jan Wąż-Ambrożewicz
Michał Milczarz

1 Wprowadzenie

Projekt polegał na stworzeniu aplikacji o interfejsie graficznym, która umożliwia generowanie kluczy za pomocą algorytmu RSA.

W aplikacji użytkownik ma możliwość wygenerowania nowych kluczy, które składają się z klucza publicznego, który może być udostępniany innym użytkownikom, oraz klucza prywatnego, który jest bezpiecznie przechowywany. Aplikacja umożliwia użytkownikowi wprowadzenie wiadomości, a następnie podpisanie jej przy użyciu klucza prywatnego i funkcji skrótu MD4.

Po podpisaniu wiadomości, użytkownik może również sprawdzić poprawność podpisu, korzystając z klucza publicznego. Jeśli podpis jest poprawny, oznacza to, że wiadomość nie została zmieniona po podpisaniu.

Aplikacja ma też możliwość zapisu kluczy do plików, co pozwala na ich przechowywanie i odtworzenie w przyszłości. Ponadto, użytkownik może odczytać klucze i wiadomości z wcześniej zapisanych plików, co zapewnia elastyczność i ułatwia zarządzanie kluczami i wiadomościami.

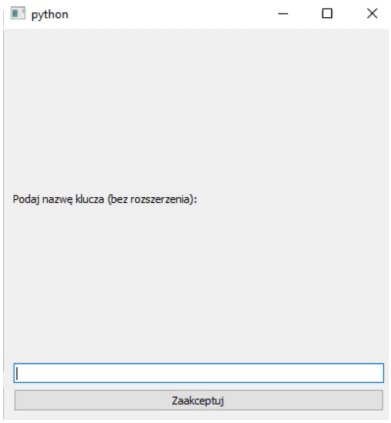
2 Instrukcja obsługi

Nasza aplikacja (jak widać na poniższym obrazku) posiada 6 funkcjonalności o których krótko opowiemy. Poniżej przedstawiamy krótkie opisy głównych funkcjonalności, które znajdziesz w aplikacji.

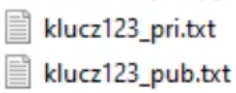
Rysunek 1:

2.1 Generuj klucze

Po kliknięciu tego przycisku na ekranie pojawi się nowe okno, w którym użytkownik zostanie poproszony o podanie nazwy klucza (bez rozszerzenia). Po zaakceptowaniu nazwy klucza, pojawi się komunikat "Wczytano klucze", a w folderze projektu pojawią się dwa nowe pliki: pri.txt i pub.txt. Plik pri.txt będzie zawierał klucz prywatny, a plik pub.txt klucz publiczny. Wartym dodania jest fakt, że można wielokrotnie generować nowe klucze bez potrzeby restartowania aplikacji.



Rysunek 2:



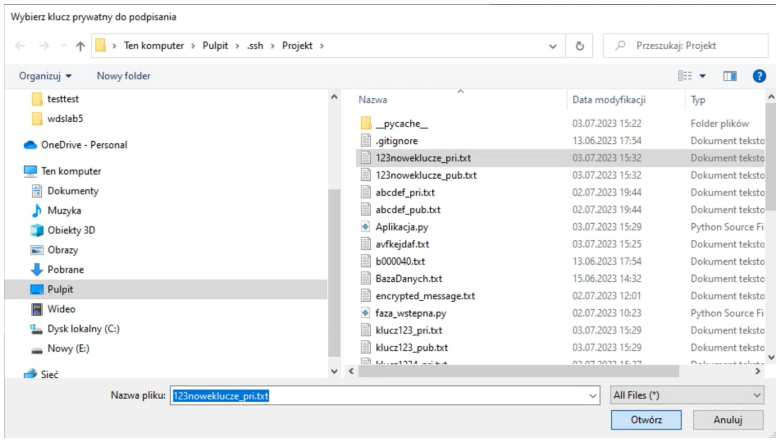
Rysunek 3:

2.2 Odczytaj zawartość pliku

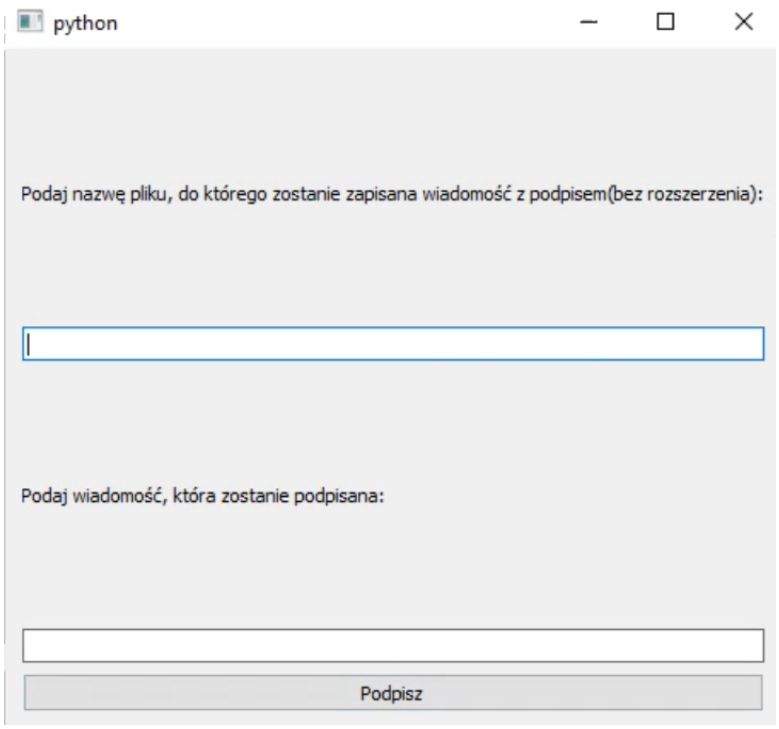
Po kliknięciu tego przycisku na ekranie pojawi się nowe okno, w którym użytkownik zostanie poproszony o wybór pliku do odczytu. Należy zauważyć, że ta funkcjonalność nie jest wymagana w ramach tej aplikacji.

2.3 Podpisz wiadomość

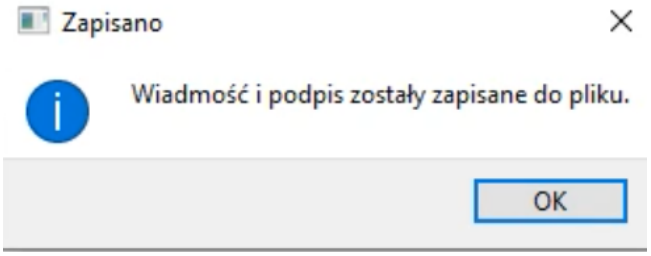
Po kliknięciu tego przycisku na ekranie pojawi się nowe okno, w którym użytkownik będzie poproszony o podanie klucza prywatnego (np. ten, który został wcześniej wygenerowany) w celu podpisania wiadomości. Następnie użytkownik zostanie poproszony o wprowadzenie wiadomości, którą chce zaszyfrować, oraz nazwy pliku, w którym zostanie zapisana zaszyfrowana wiadomość. Na zakończenie wyświetli się komunikat informujący o podpisaniu wiadomości.



Rysunek 4:



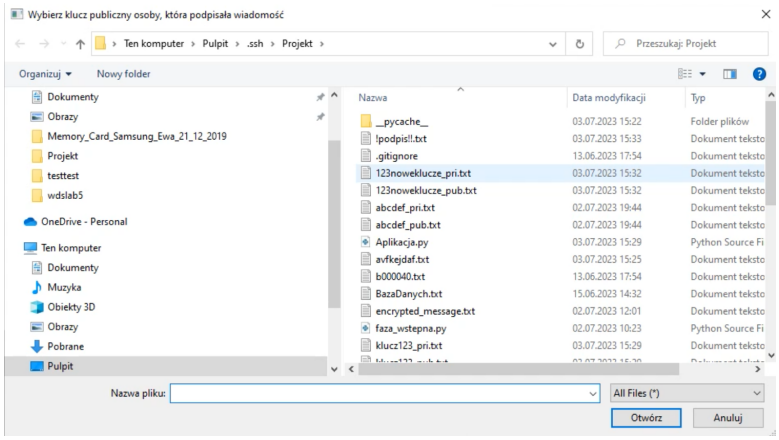
Rysunek 5:



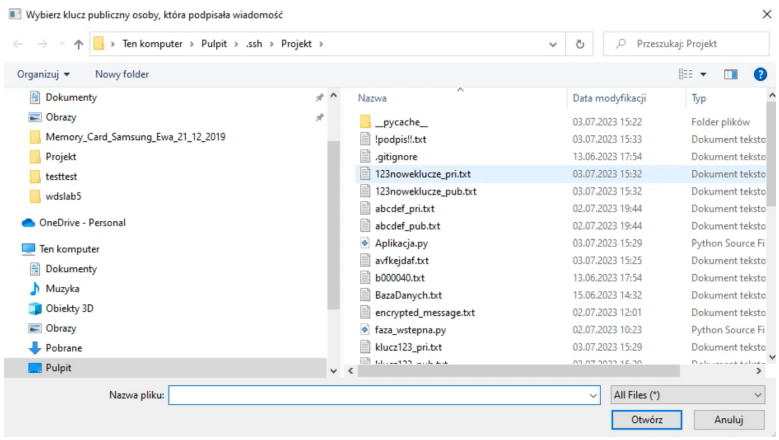
Rysunek 6:

2.4 Sprawdź podpis cyfrowy

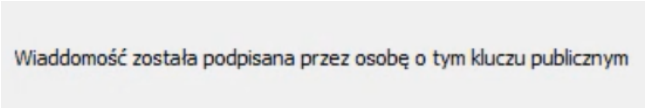
Po kliknięciu tego przycisku na ekranie pojawią się dwa nowe okna. W tych oknach będziemy musieli wybrać klucz publiczny osoby, która podpisała wiadomość, oraz plik zawierający zaszyfrowaną wiadomość. Jeśli wybierzemy odpowiednie pliki, zostanie wyświetlony komunikat potwierdzający, że wiadomość została faktycznie podpisana przez osobę posiadającą określony klucz publiczny.



Rysunek 7:



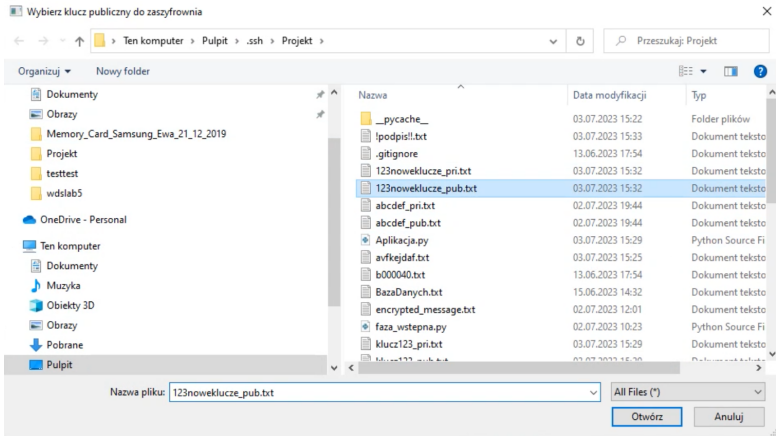
Rysunek 8:



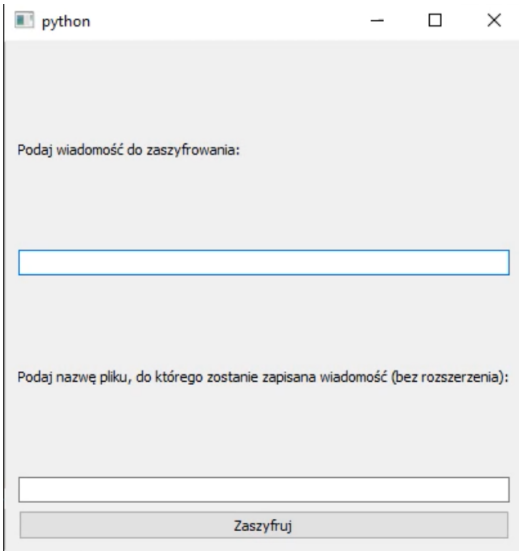
Rysunek 9:

2.5 Zaszyfruj wiadomość

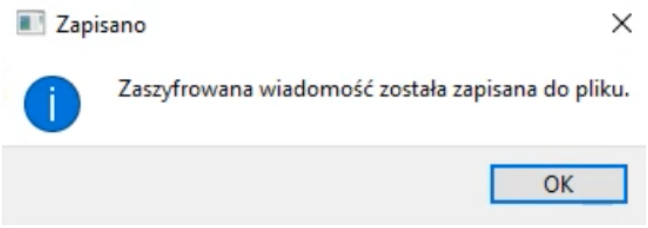
Po kliknięciu tego przycisku na ekranie pojawią się dwa okna. Użytkownik będzie poproszony o wybranie klucza publicznego do zaszyfrowania wiadomości. Następnie będzie mógł wpisać treść wiadomości oraz podać nazwę pliku, do którego ma być zapisana ta wiadomość.



Rysunek 10:



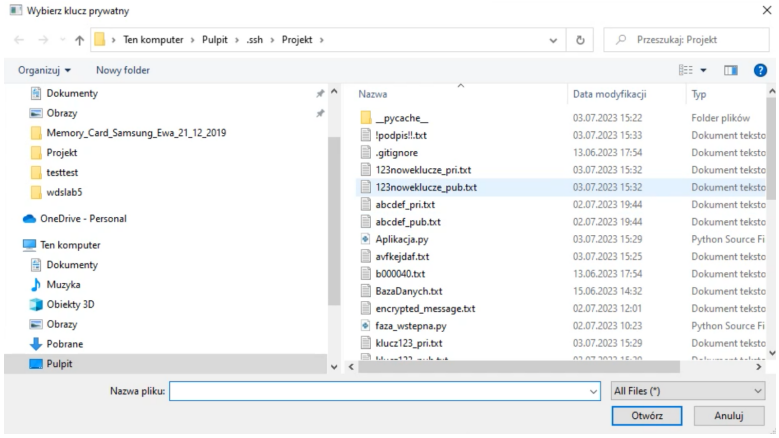
Rysunek 11:



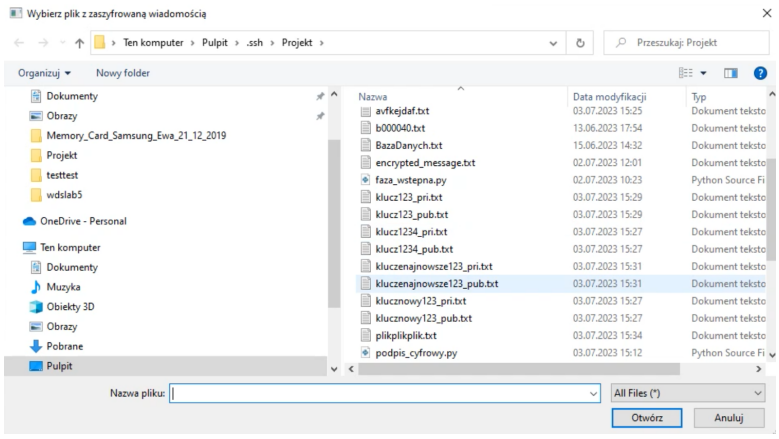
Rysunek 12:

2.6 Odszyfruj wiadomość

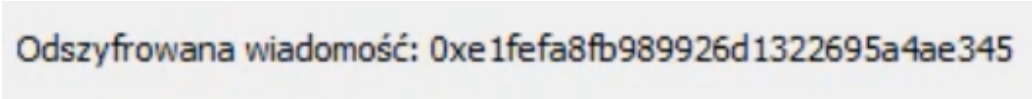
Po kliknięciu tego przycisku na ekranie pojawią się dwa okna. Użytkownik zostanie poproszony o wybranie klucza prywatnego, a następnie pliku z zaszyfrowaną wiadomością. Jeśli wybierzemy odpowiednią wiadomość i poprawny klucz prywatny, zostanie wyświetlony komunikat z rozszyfrowaną wiadomością.



Rysunek 13:



Rysunek 14:


Odszyfrowana wiadomość: 0xe1fefa8fb989926d1322695a4ae345

Rysunek 15: