Pojęcia

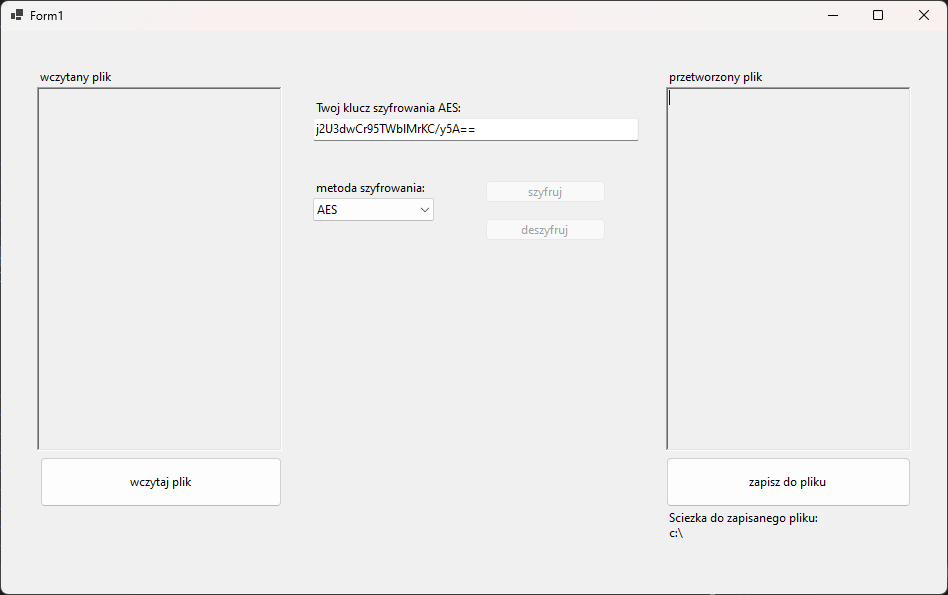
**Szyfrowanie RSA** jest jednym z najpopularniejszych algorytmów kryptograficznych używanych do szyfrowania i deszyfrowania danych. Algorytm wykorzystuje klucz publiczny i prywatny do szyfrowania i deszyfrowania wiadomości. W szyfrowaniu RSA wiadomość jest kodowana za pomocą klucza publicznego i może zostać odszyfrowana tylko przez posiadacza klucza prywatnego.   
\*UWAGA**:** Limit długości wiadomości do szyfrowania RSA zależy od długości klucza używanego do szyfrowania.

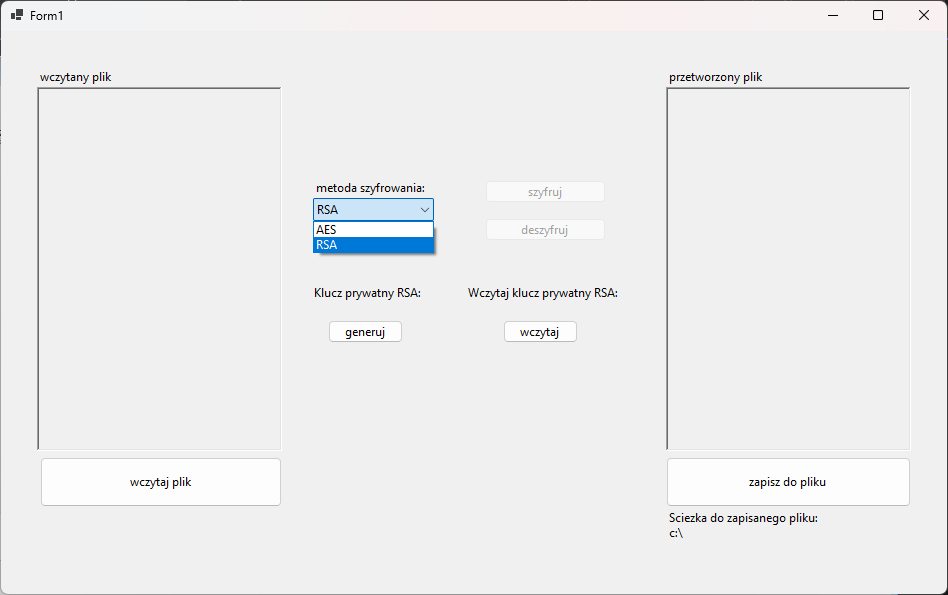
**Szyfrowanie AES** (Advanced Encryption Standard) jest jednym z najbardziej popularnych i bezpiecznych algorytmów kryptograficznych, wykorzystywanym do szyfrowania i deszyfrowania danych. Algorytm AES wykorzystuje symetryczne szyfrowanie, co oznacza, że ta sama klucz jest używana do szyfrowania i deszyfrowania wiadomości.   
**\***UWAGA: Vector (IV) w AES to losowo wygenerowany ciąg danych o stałej długości, który jest używany jako część procesu szyfrowania wiadomości. IV jest dodawany do wiadomości przed szyfrowaniem, a następnie jest odszyfrowywany razem z wiadomością. Jego głównym zadaniem jest zapobieganie atakom związanym z identycznością wiadomości.

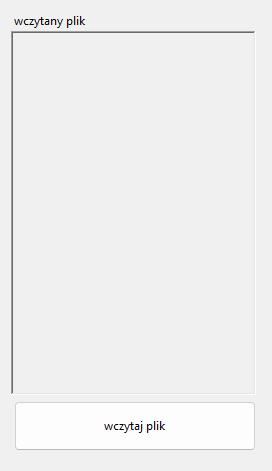
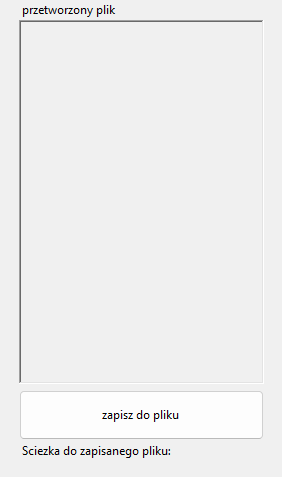
Zastosowanie Programu

Program służy do szyfrowania i deszyfrowania plików za pomocą metody szyfrowania RSA oraz AES.

Wygląd Programu

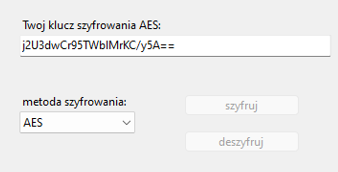
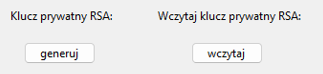
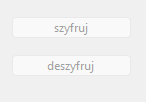




Wygląd Programu

**AES:**



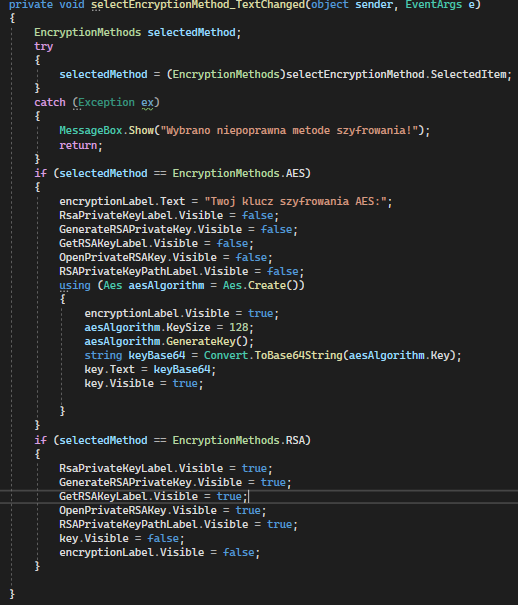
1. Okna tekstowe – TextBox:
   * + - * 2 pola tekstowe, do lewego TextBoxa wczytywany jest plik, w prawym wyświetlany zaszyfrowany plik.
         * Pola posiadają właściwość   
           multiline:True - wieloliniowość  
           ReadOnly:True – tylko do odczytu
       1. TextBox „Twój klucz szyfrowania AES”, w którym wyświetlany jest automatycznie wygenerowany klucz AES, lub użytkownik może podać swój własny.
          - Widoczny gdy wybrana jest metoda szyfrowania *AES*
       2.  **Kontrolka „ComboBox” z ustawioną właściwością „DropDownStyle” na *DropDownList.* Zawiera w sobie elementy *AES* i *RSA*.**
          - **Po wybraniu elementu z listy rozwijanej pokazują i chowają nam się odpowiednie kontrolki w programie. (zmieniana jest właściwość Visible:True/False odpowiednich kontrolek)**
       3.  W przypadku wybrania z listy *RSA* mamy dostępne przyciski (Button) „generuj” oraz „wczytaj”.
          - Przycisk generuj – generuje do pliku klucz prywatny RSA.
          - Przycisk wczytaj – wczytuje z pliku klucz prywatny RSA, potrzebny do odszyfrowania wczytanego pliku.
       4. Przyciski „szyfruj” i „deszyfruj” – zachowują się analogicznie do nazw.
          - Zmienia im się właściwośc Enabled na true, gdy wczytamy plik, do zaszyfrowania/odszyfrowania.

Opis Programu

Aby program działał prawidłowo wymagane jest zaimportowanie poniższych bibliotek.



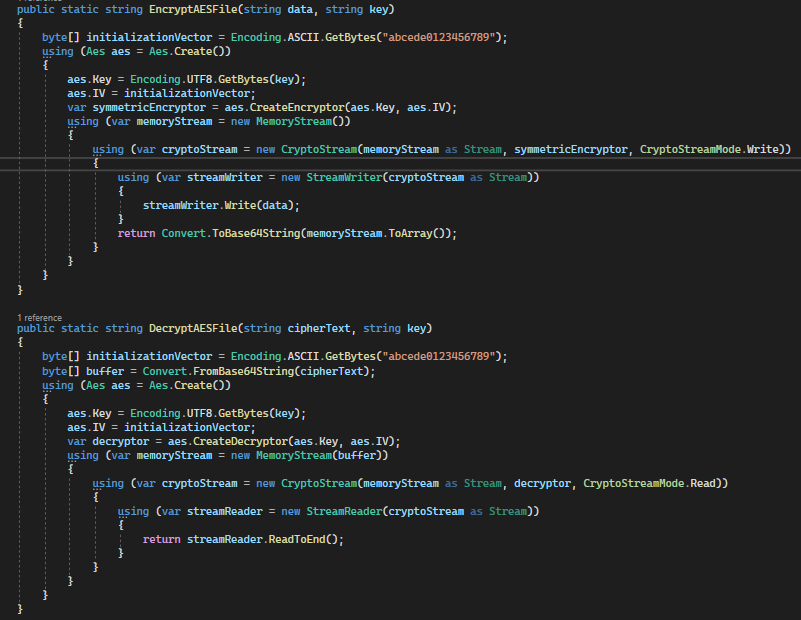
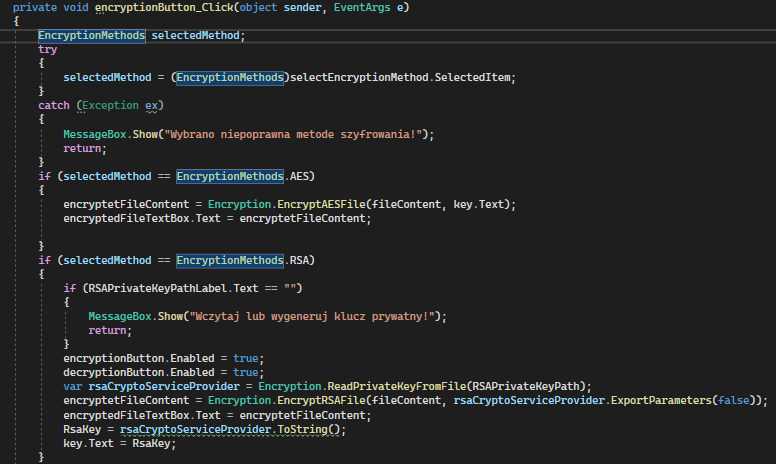
Program składa się z klasy Form1.cs, w której zaprogramowana jest obsługa kontrolek i wczytywanie plików, oraz klasy Encryption, w której zaprogramowane są metody do szyfrowania i deszyfrowania plików. Dodatkowo w programie jest enum, zawierający dostępne metody szyfrowania w programie, które są wyświetlane w liscie rozwijanej(ComboBox).



**Wybór metody szyfrowania z listy rozwijanej:**

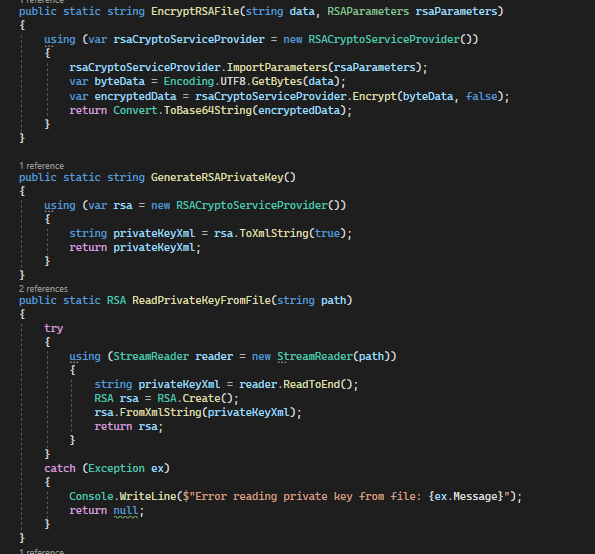
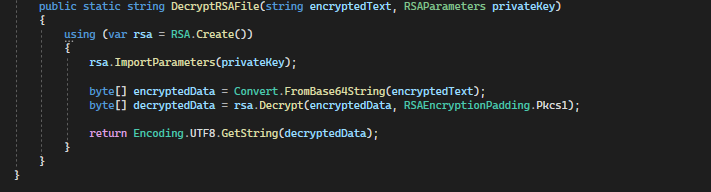
Ten kod odpowiada za wybór metody szyfrowania w programie, na podstawie wartości wybranej w ComboBoxie "selectEncryptionMethod". Jeśli wybrana metoda to AES, generowany jest losowy klucz szyfrowania AES o rozmiarze 128 bitów, który jest wyświetlany użytkownikowi w formie kodu string Base64. Jeśli wybrana metoda to RSA, interfejs programu zostaje uzupełniony o pola związane z generowaniem kluczy RSA i wyborem pliku klucza prywatnego lub możliwością jego wygenerowania, a odpowiednie pola dotyczące AES zostają ukryte.

**Wybór metody szyfrowania z listy rozwijanej:**

**Obsługa przycisku szyfruj:**  
\*Analogicznie działa deszyfruj  
  
Ten kod odpowiada za obsługę przycisku "Szyfruj". Najpierw jest pobierana wybrana metoda szyfrowania, a następnie w zależności od wybranej metody szyfrowania jest wykonywana odpowiednia akcja. Jeśli wybrano szyfrowanie AES, to zawartość pliku jest szyfrowana przy użyciu klucza AES zdefiniowanego w polu tekstowym "key". Natomiast jeśli wybrano szyfrowanie RSA, to najpierw jest sprawdzane, czy klucz prywatny RSA został wczytany lub wygenerowany. Następnie plik jest szyfrowany przy użyciu klucza publicznego RSA i wyświetlany w polu tekstowym "encryptedFileTextBox.

**Szyfrowanie i deszyfrowanie AES:**

W obu metodach tworzony jest obiekt klasy Aes, który służy do ustawienia klucza i wektora inicjalizacji, a następnie tworzony jest obiekt kryptograficzny symmetricEncryptor lub decryptor. Następnie dane są zapisywane lub odczytywane z pliku z użyciem strumieni kryptograficznych, a na końcu wynik jest kodowany do postaci Base64 i zwracany.

**Szyforwanie RSA:**

Funkcja EncryptRSAFile szyfruje dane za pomocą klucza RSA i zwraca zaszyfrowane dane jako ciąg znaków.  
Funkcja GenerateRSAPrivateKey generuje nowy klucz prywatny RSA i zwraca go jako ciąg znaków. Funkcja ReadPrivateKeyFromFile odczytuje klucz prywatny RSA z pliku i zwraca obiekt RSA.  
Funkcja DecryptRSAFile deszyfruje dane za pomocą klucza prywatnego RSA i zwraca je jako ciąg znaków.