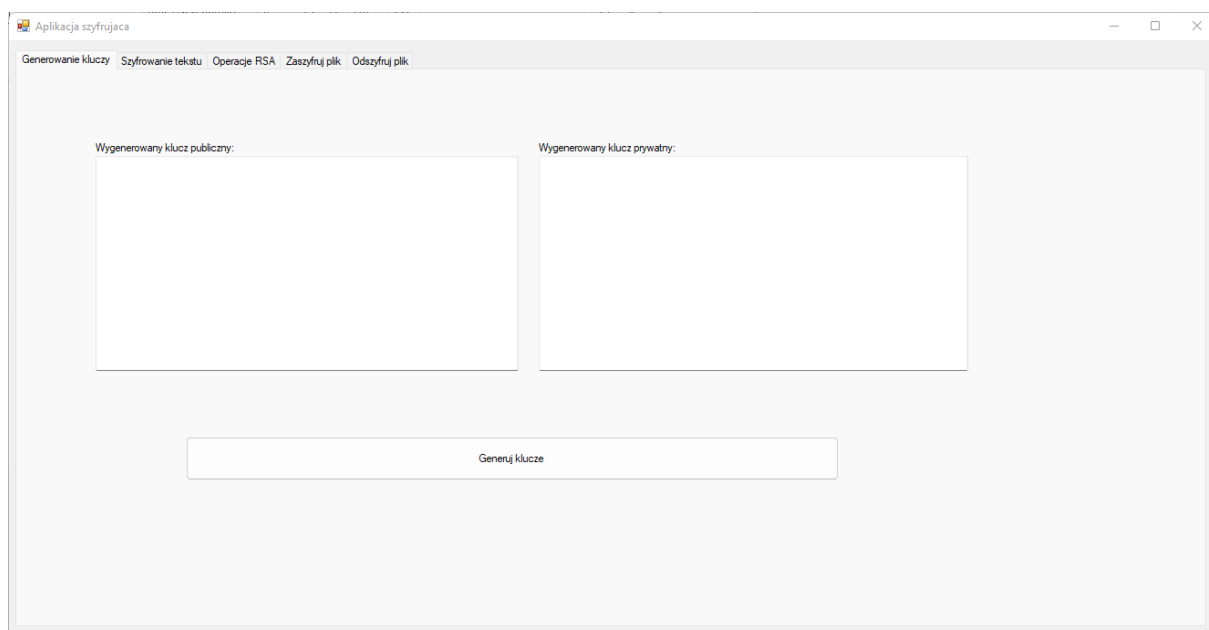


| | |
|--|------------------|
| Akademia Nauk Stosowanych w Nowym Sączu | |
| Wydział Nauk Inżynieryjnych | |
| Niezawodność systemów informatycznych –2022/2023 | |
| Imię i nazwisko: Filip Rzepiela | Data: 06.12.2022 |
| Grupa: P2 | |

Data: 06.12.2022

Testy manualne aplikacji do szyfrowania oraz deszyfrowania tekstu oraz plików za pomocą algorytmu RSA (aplikacja opracowana na potrzeby zaliczenia przedmiotu Kryptografia i teoria kodów

Okno główne:



Zużycie zasobów w czasie bezczynności

Menedżer zadań

Plik

Opcje

Widok

Procesy

Wydajność

Historia aplikacji

Uruchamianie

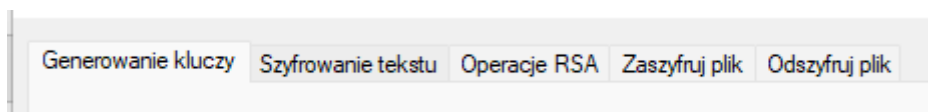
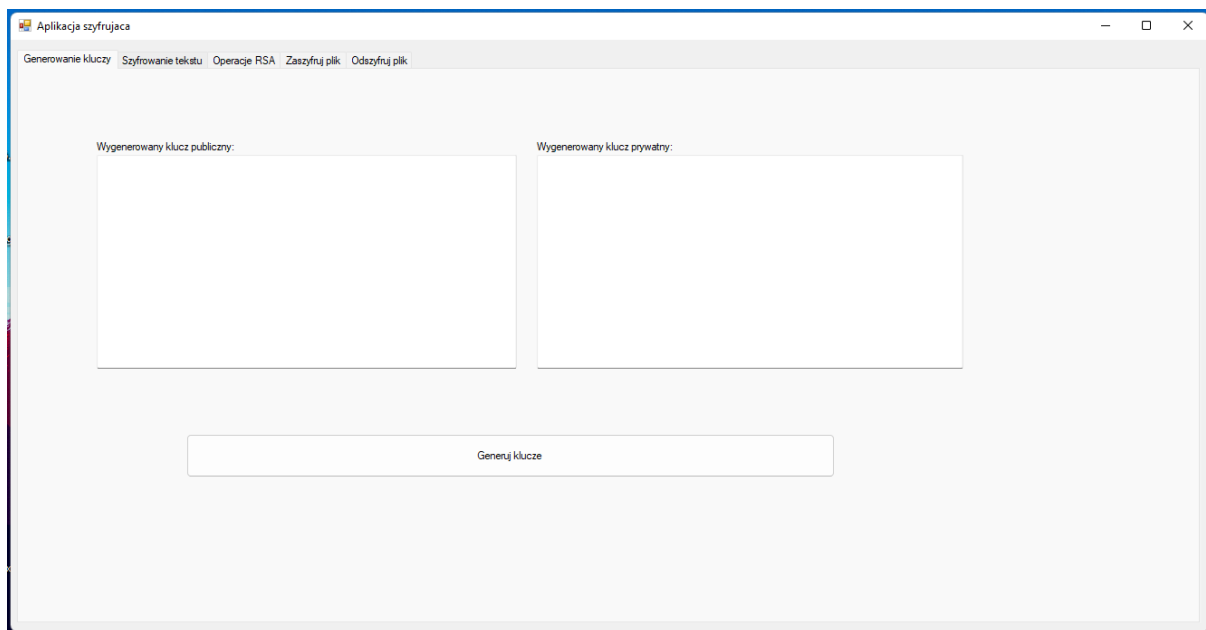
Użytkownicy

Szczegóły

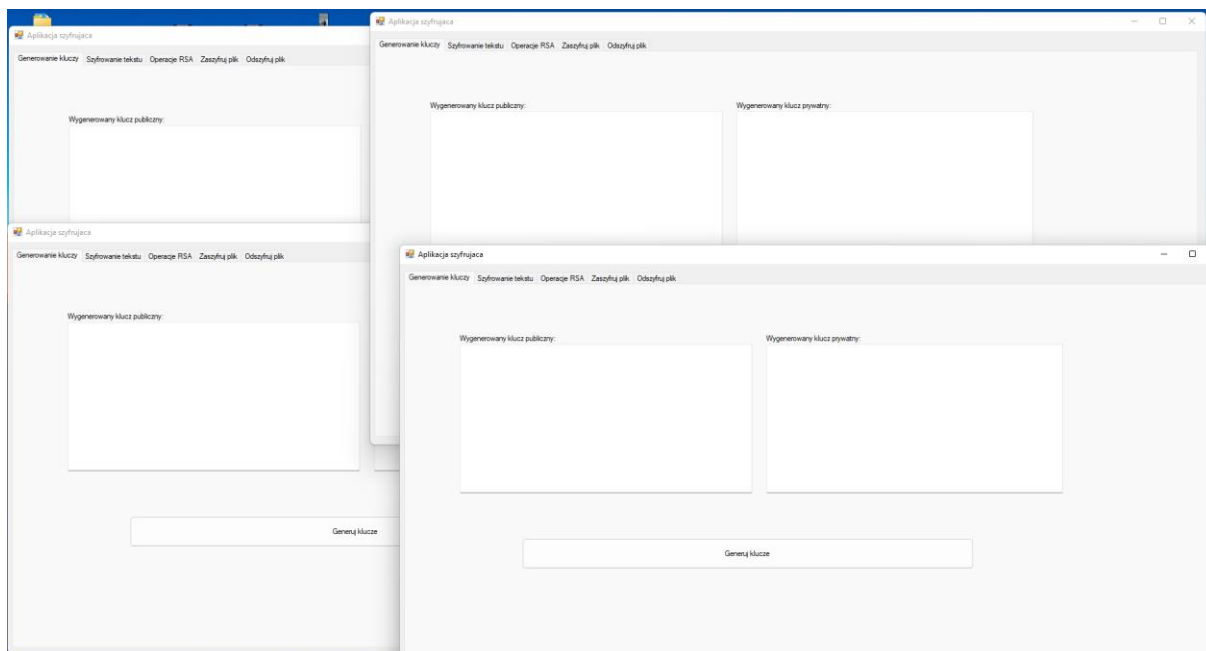
Usługi

| | | | | | | | | | |
|--|------|-------------|--------|--------|--------|-------------|----------------------|-----------------|-------------------|
| | | 18% | 67% | 0% | 0% | 2% | | | |
| Nazwa | Stan | Procesor... | Pamięć | Dysk | Sieć | Procesor... | Aparat procesora GPU | Zużycie energii | Trend zużycia ... |
| <div><div><div></div><div>RSA (32-bitowy)</div></div></div> | | 0% | 5,5 MB | 0 MB/s | 0 Mb/s | 0% | | Bardzo niskie | Bardzo niskie |
| <div><div><div></div><div>Aplikacja szyfrująca</div></div></div> | | | | | | | | | |

Po najechnaniu na dowolną kartę, karta nabiera szarawy kolor



Możliwe jest uruchomienie kilku instancji programu



Test szyfrowania tekstu

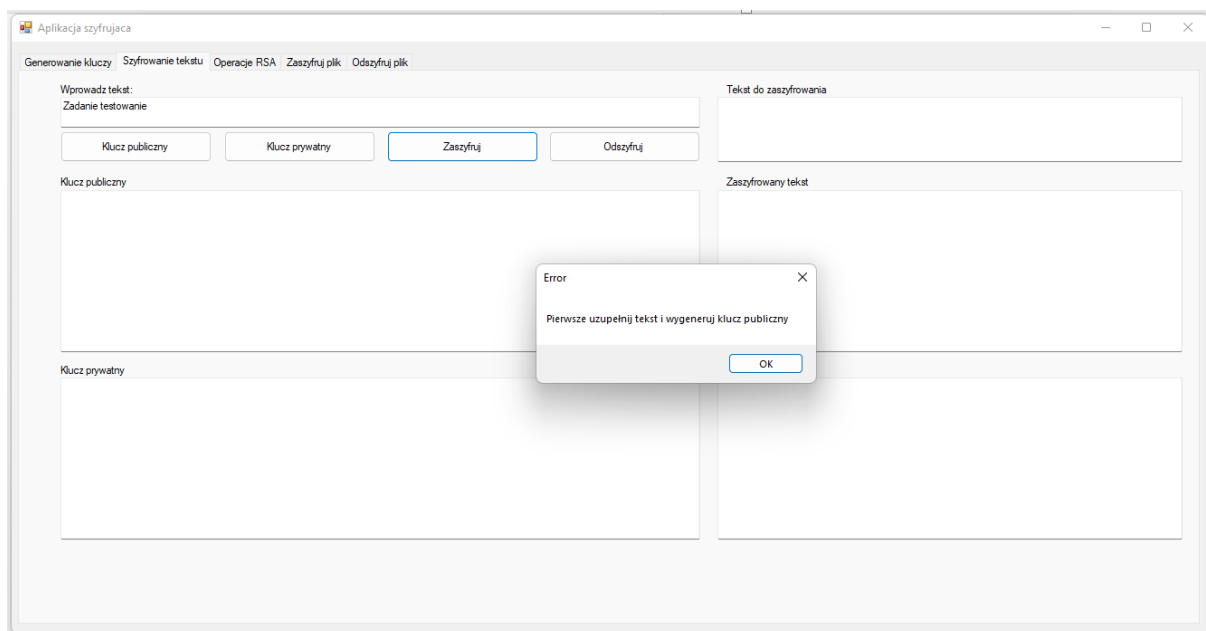
Okno szyfrowania tekstu

The screenshot shows a window titled 'Aplikacja szyfrująca' with a menu bar containing 'Generowanie kluczy', 'Szyfrowanie tekstu', 'Operacje RSA', 'Zaszyfruj plik', and 'Odszyfruj plik'. The 'Szyfrowanie tekstu' tab is active. The interface is divided into two main columns. The left column contains a 'Wprowadz tekst:' input field, four buttons ('Klucz publiczny', 'Klucz prywatny', 'Zaszyfruj', 'Odszyfruj'), and three large text areas labeled 'Klucz publiczny', 'Klucz prywatny', and 'Odszyfrowany tekst'. The right column contains two large text areas labeled 'Tekst do zaszyfrowania' and 'Zaszyfrowany tekst'. The 'Zaszyfruj' button is highlighted with a blue border.

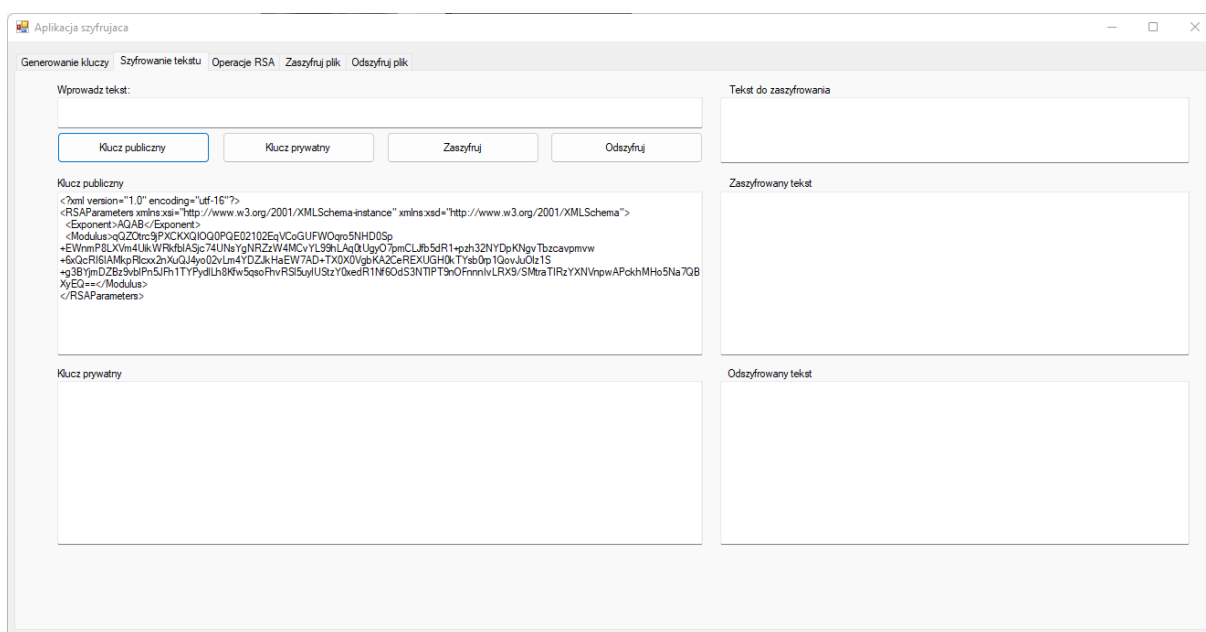
Próba zaszyfrowania przy pustych polach:

This screenshot shows the same application window as before, but with an error dialog box in the center. The dialog box is titled 'Error' and contains the message 'Pierwsze uzupełnij tekst i wygeneruj klucz publiczny' with an 'OK' button. The 'Zaszyfruj' button in the background is still highlighted.

Aplikacja wyświetla powiadomienie, że pole tekstowe oraz klucz publiczny nie mogą być puste. Dodatkowo, gdy jedno z pól zostanie niewypełnione również wyświetla się ten sam komunikat



Test generowania klucza publicznego.



Po wciśnięciu przycisku klucz publiczny wygenerowany zostanie żądany przez nas klucz

Test szyfrowania krótkiego tekstu.

Wprowadz tekst:
Chciałbym dostać ocenę 5.0

Klucz publiczny

Klucz prywatny

Zaszyfruj

Odszyfruj

Klucz publiczny

<?xml version="1.0" encoding="utf-16"?>
<RSAPublicKey xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Exponent>AQAB</Exponent>
<Modulus>eETI5hUjHMMh2mR3qI5e+/86gNEeQ
+CcdXMy9kEePPr75YmKGoZ7wllGGBevZgboEJsl4toG4EWW7fEJESwLGJOkdFjaKdZTOZqrVOQg+k11qomu11YyNHoQTF/Dk0zFphV
+HAUz9QyGgKc8Lu2mAudfBxUSZqe5yBY7YdNZaMZFhmG7KXOZF/X+jy108Y/2ohuMtlS2uwy5RplkhK086dLRqC6uUqtOE
+G0GkfsfNSXQ51UQ20948BstWS3d0R4Yw7qTY3ZZS/F7zDsJugoybVpooEgEcJncm6Q2byzXY5m8mTINU5Ex8jHBLUBAypQ==</Modulus>
</RSAPublicKey>

Klucz prywatny

Tekst do zaszyfrowania
Chciałbym dostać ocenę 5.0

Zaszyfrowany tekst

IzLRDKgrRD9TFZyzVfzCC9VNNINwGw/ZLKU
+bEq5ywnQhHvUvMceT/3eSblQIRjWmzIMG8Ceusue631ueMXkPpivVITUy0MPqESN0Ne7K9KmfLwFAH
aJcww5I3IVYbEmUvQ8aA84SGED0nAPBPParoG7L1cQ0NtrLtkXko5GDDMMpQrYbzem3J2+OvZwUhgqX
3lQzbRBkO4JUsVH3KuuvFouWUduXn0JDHCgwkWfPgGbOechVTBtoOeyBY
+8CLfhzqJZweJ0FMLFP5Dhqt+Loo1fk8ev49mh1d9EpJXZB0WqkdNDG5m17/ZFUs4Y+XA5w==

Odszyfrowany tekst

Tekst został zaszyfrowany i pojawił się w polu zaszyfrowany tekst

Test generowania klucza prywatnego.

Wprowadz tekst:
Chciałbym dostać ocenę 5.0

Klucz publiczny

Klucz prywatny

Zaszyfruj

Odszyfruj

Klucz publiczny

<?xml version="1.0" encoding="utf-16"?>
<RSAPublicKey xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Exponent>AQAB</Exponent>
<Modulus>eETI5hUjHMMh2mR3qI5e+/86gNEeQ
+CcdXMy9kEePPr75YmKGoZ7wllGGBevZgboEJsl4toG4EWW7fEJESwLGJOkdFjaKdZTOZqrVOQg+k11qomu11YyNHoQTF/Dk0zFphV
+HAUz9QyGgKc8Lu2mAudfBxUSZqe5yBY7YdNZaMZFhmG7KXOZF/X+jy108Y/2ohuMtlS2uwy5RplkhK086dLRqC6uUqtOE
+G0GkfsfNSXQ51UQ20948BstWS3d0R4Yw7qTY3ZZS/F7zDsJugoybVpooEgEcJncm6Q2byzXY5m8mTINU5Ex8jHBLUBAypQ==</Modulus>
</RSAPublicKey>

Klucz prywatny

<?xml version="1.0" encoding="utf-16"?>
<RSAPrivateKey xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Exponent>AQAB</Exponent>
<Modulus>eETI5hUjHMMh2mR3qI5e+/86gNEeQ
+CcdXMy9kEePPr75YmKGoZ7wllGGBevZgboEJsl4toG4EWW7fEJESwLGJOkdFjaKdZTOZqrVOQg+k11qomu11YyNHoQTF/Dk0zFphV
+HAUz9QyGgKc8Lu2mAudfBxUSZqe5yBY7YdNZaMZFhmG7KXOZF/X+jy108Y/2ohuMtlS2uwy5RplkhK086dLRqC6uUqtOE
+G0GkfsfNSXQ51UQ20948BstWS3d0R4Yw7qTY3ZZS/F7zDsJugoybVpooEgEcJncm6Q2byzXY5m8mTINU5Ex8jHBLUBAypQ==</Modulus>
<PrivateExponent>Pz23zRfIEJqPjYUjmw78P6Lu0KSnY91-Cye0fN3olAKkgbeaw7NsCV4v93v/ZCy6qatuEDpkgrPocLUAYp1ekYfBNi6MWJrnfF2eloHdLX
Odstwoy7H+Ca674651uYFAs00lpHvX0gZ7F7uW68ImQqZ23aMQGos=</PrivateExponent>
<QzZawbkiA4xTXG/48Q2g3h1mGGGceHJuggYcfV9Z27Udn4yMTQdEN5Y7omOA44Sqwb40TY+JPajlWwhWd/XUaKNH/
+Gbf7D0fcpRz0eHfWmYNoAZgARVfHeZDTPrvtq56VjapDDlatUcWZ7YiIS9qB5JRfI8=</QzZawbkiA4xTXG/48Q2g3h1mGGGceHJuggYcfV9Z27Udn4yMTQdEN5Y7omOA44Sqwb40TY+JPajlWwhWd/XUaKNH/>
</RSAPrivateKey>

Tekst do zaszyfrowania
Chciałbym dostać ocenę 5.0

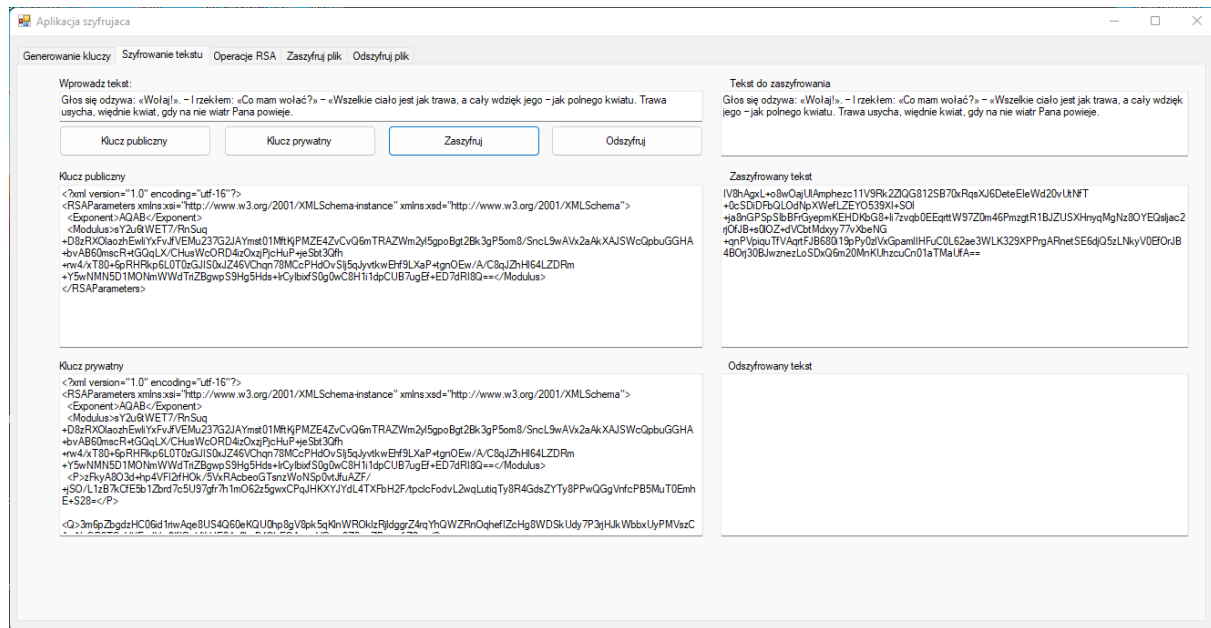
Zaszyfrowany tekst

IzLRDKgrRD9TFZyzVfzCC9VNNINwGw/ZLKU
+bEq5ywnQhHvUvMceT/3eSblQIRjWmzIMG8Ceusue631ueMXkPpivVITUy0MPqESN0Ne7K9KmfLwFAH
aJcww5I3IVYbEmUvQ8aA84SGED0nAPBPParoG7L1cQ0NtrLtkXko5GDDMMpQrYbzem3J2+OvZwUhgqX
3lQzbRBkO4JUsVH3KuuvFouWUduXn0JDHCgwkWfPgGbOechVTBtoOeyBY
+8CLfhzqJZweJ0FMLFP5Dhqt+Loo1fk8ev49mh1d9EpJXZB0WqkdNDG5m17/ZFUs4Y+XA5w==

Odszyfrowany tekst

Klucz został wygenerowany i pojawił się w polu klucz prywatny

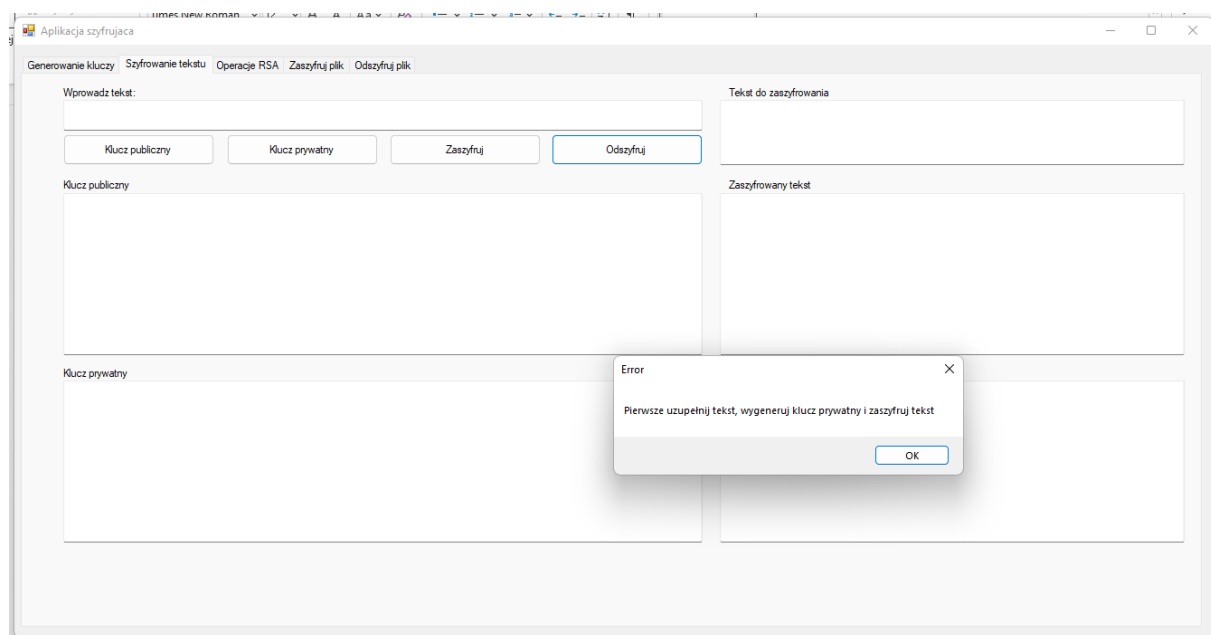
Test szyfrowania dłuższego fragmentu tekstu.



Aplikacja ogranicza maksymalną ilość znaków możliwą do wpisania w polu Tekst do zaszyfrowania do 214 znaków. Szyfrowanie odbywa się poprawnie.

Test deszyfracji tekstu

Test deszyfracji przy pustych polach.



Aplikacja szyfrująca

Generowanie kluczy Szyfrowanie tekstu Operacje RSA Zaszifruj plik Odzyskaj plik

Wprowadź tekst:

Głos się odzywa: «Woja!», – I rzekłem: «Co mam wolać?» – «Wszystkie ciało jest jak trawa, a cały wdzięk jego – jak pełnego kwiatu. Trawa usycha, więdną kwiat, gdy na nie wieje Pana powiewie.

Klucz publiczny Klucz prywatny Zaszifruj Odzyskaj

<?xml version="1.0" encoding="utf-16"?>
<RSAParameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <Exponent>AQAB</Exponent>

 <Modulus>zF2afKXbaAYxIoHkcRai/ZRCzh2nGDdGgoSWYqYnk7kLAQYhZooxdiLVFWB9yeldv7/jAfwWNVA9o3C8X2QMhdVPVctEBazKoB
H89Z5gqwTUOmR659E50aMCvykf3seBH3pcMoKd12PUL+7GiGMk4PyUlpb7kZTTO-DYY4H/+Kg-uDOS6DGx/P3BaSuXQGNW6cYP
+Scj3IHAphtSe+E+sv979GcT/bTSZAQkiSHN06QtoeH4SANDUAemU
+Of51ToIPbVFWUWIFNZs7V/DVEWynTKOhztJA1tts5BSVaQH4Yo6RAtaQGhzozgrAZz3Q==</Modulus>
</RSAParameters>

Klucz prywatny

<?xml version="1.0" encoding="utf-16"?>
<RSAParameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <Exponent>AQAB</Exponent>

 <Modulus>zF2afKXbaAYxIoHkcRai/ZRCzh2nGDdGgoSWYqYnk7kLAQYhZooxdiLVFWB9yeldv7/jAfwWNVA9o3C8X2QMhdVPVctEBazKoB
H89Z5gqwTUOmR659E50aMCvykf3seBH3pcMoKd12PUL+7GiGMk4PyUlpb7kZTTO-DYY4H/+Kg-uDOS6DGx/P3BaSuXQGNW6cYP
+Scj3IHAphtSe+E+sv979GcT/bTSZAQkiSHN06QtoeH4SANDUAemU
+Of51ToIPbVFWUWIFNZs7V/DVEWynTKOhztJA1tts5BSVaQH4Yo6RAtaQGhzozgrAZz3Q==</Modulus>

 <DP>qATqPTCh3zs+dLSXZKO/NpmRNIO5Y13Q+1KqXLUWzPYaRvZ8FDE
BMfAPeRDtmZvwHJmupOHYgz5I1R/L2e5dzMB83ko7U793bk6SE
DxtLzEnUUCghaY7Bsa4mw3zdGhndLEDBsY1CG4HQKL7GHZMk= </P>

 <Q>sqatmSMeeebw7Uw
+uABLZo3+1wnagvSV87QHf959tkKK3pAs4ZFos9cbJH1DaHz7kU2KUUYuzumMcqlggD3nzEvQb0vuAbQovUr7kNNH6NDZobuBJO

Tekst do zaszyfrowania

Głos się odzywa: «Woja!», – I rzekłem: «Co mam wolać?» – «Wszystkie ciało jest jak trawa, a cały wdzięk jego – jak pełnego kwiatu. Trawa usycha, więdną kwiat, gdy na nie wieje Pana powiewie.

Zaszyfrowany tekst

M8UjHBd0wNojUAgRnSnRhmkGsCK28AHIZuclYofmaY/DoJsDA84fy1Na6+s1ceXfeS6RGUkmOkm
coBZiaWqElzn2kaefRUduLz1Zh2aSwYmgOpv5ha4eRg5zLZOUIuxaeZwdncDXpphNW
Olcs9/AmLYHIm3EEactbp9Zds8SRPAzordkNCrTZUWQZ2Kh9IflrgQW51uty3UYXSX/kcdnSDswJweSV
LuLy+salALFour0u4UG81Bvgdk8Muuy33feegO/HapK8r6AGA
+yhjWUDOFWeYckAvexraH5/8AGQEX3m6MLkCx==

Odszyfrowany tekst

Głos się odzywa: «Woja!», – I rzekłem: «Co mam wolać?» – «Wszystkie ciało jest jak trawa, a cały wdzięk jego – jak pełnego kwiatu. Trawa usycha, więdną kwiat, gdy na nie wieje Pana powiewie.

Test szyfrowania plików

Widok okna szyfrowania plików.

The screenshot shows the 'Aplikacja szyfrująca' window with the 'Zaszyfruj plik' tab selected. The interface contains the following elements:

- Tab bar: Generowanie kluczy, Szyfrowanie tekstu, Operacje RSA, **Zaszyfruj plik**, Odszyfruj plik
- File selection: 'Proszę wybrać plik do zaszyfrowania:' with a text input field and a 'Przełączaj' button.
- Destination folder: 'Proszę wybrać gdzie zapisać zaszyfrowany plik:' with a text input field and a 'Przełączaj' button.
- Public key: 'Klucz publiczny:' with a large text input field, a 'Generuj' button, and a 'Kopiuż' button.
- Private key: 'Klucz prywatny:' with a large text input field, a 'Generuj' button, and a 'Kopiuż' button.
- Action: A large 'Zaszyfruj' button at the bottom.

Próba uruchomienia szyfrowania przy pustych polach.

The screenshot shows the same 'Aplikacja szyfrująca' window, but with a 'Warning' dialog box overlaid. The dialog box contains the following text:

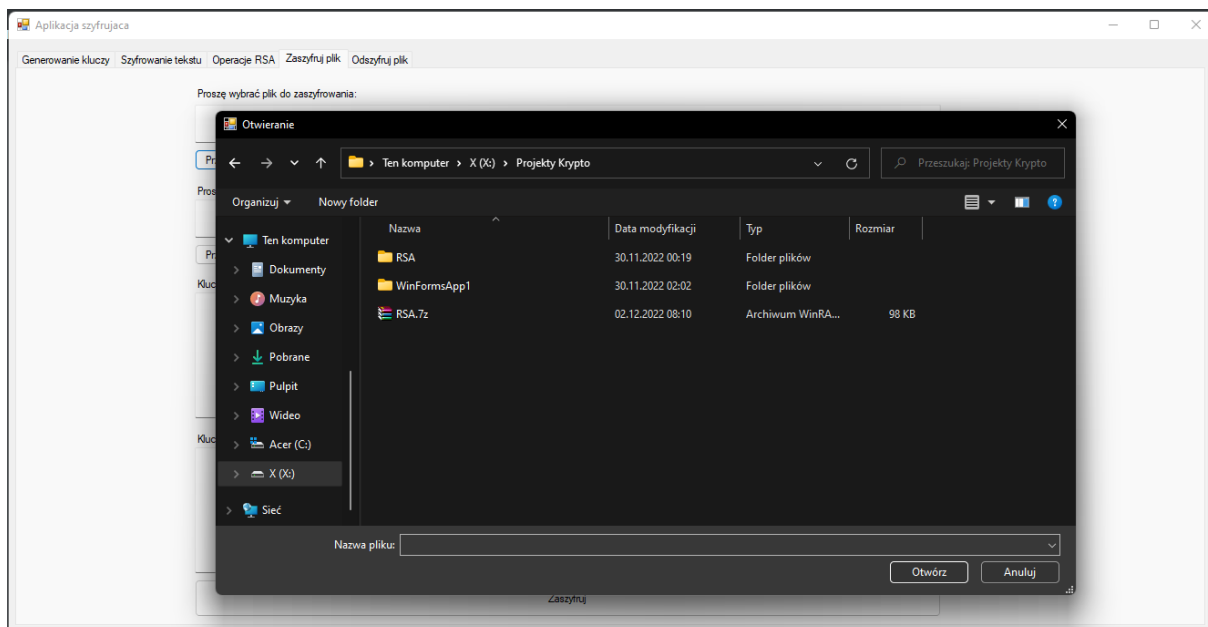
Warning

File to encrypt path input, destination folder, and public key input can not be empty!

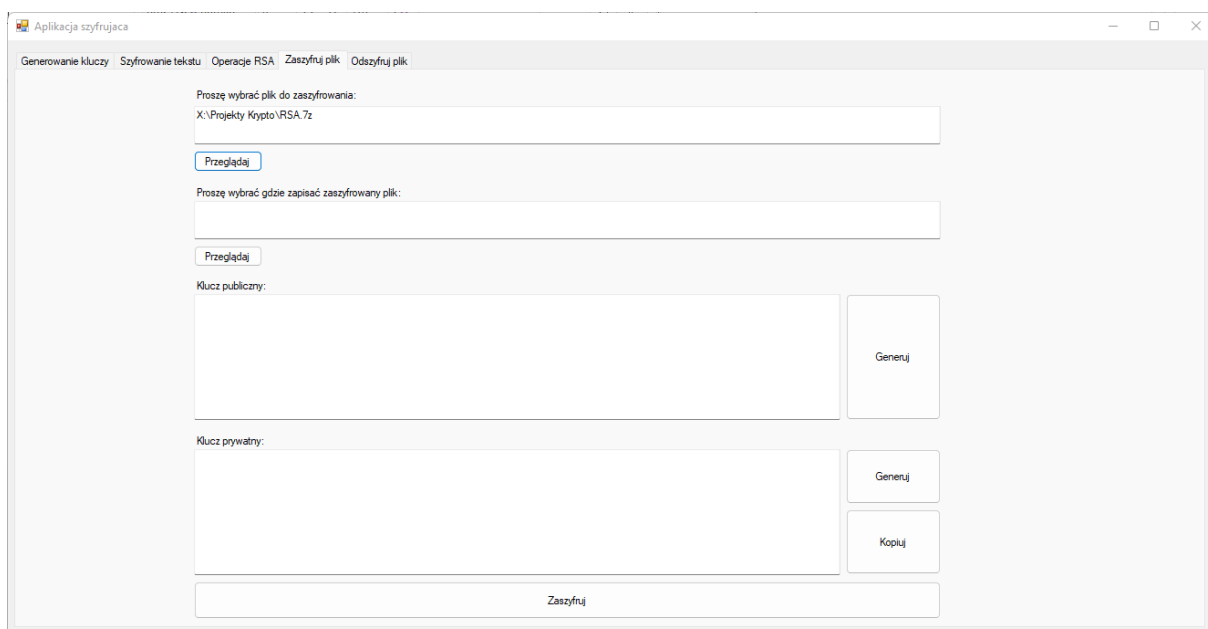
OK

Wyświetla się komunikat, że pola nie mogą być puste. Aplikacja wyświetla wyżej pokazany komunikat zarówno jeśli wszystkie pola są puste i jeśli jedno z wymaganych pól jest puste.

Test pola wskazania pliku do zaszyfrowania

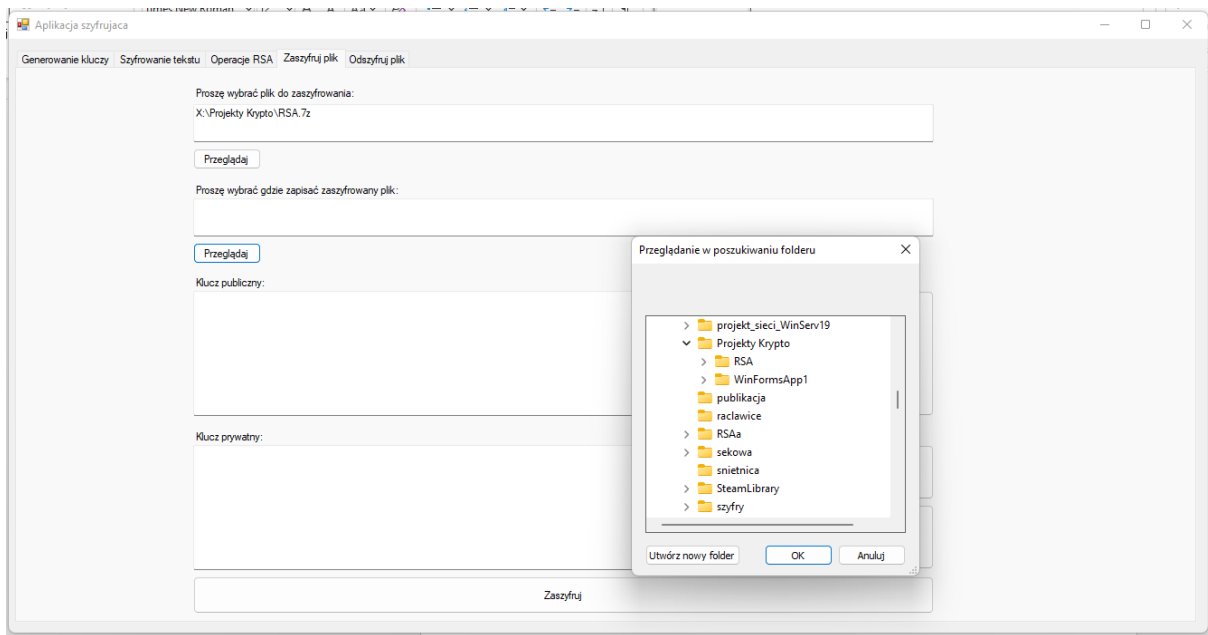


Po wybraniu pliku do zaszyfrowania jego ścieżka pojawia się w polu

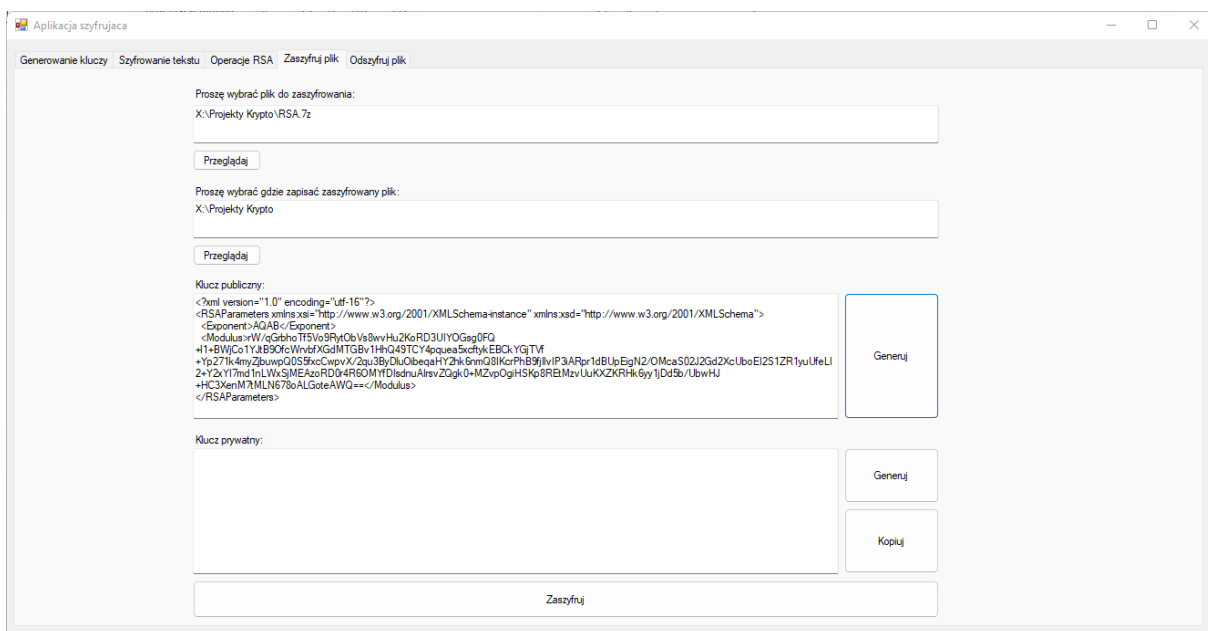


Test wybrania lokalizacji dla zaszyfrowanego pliku

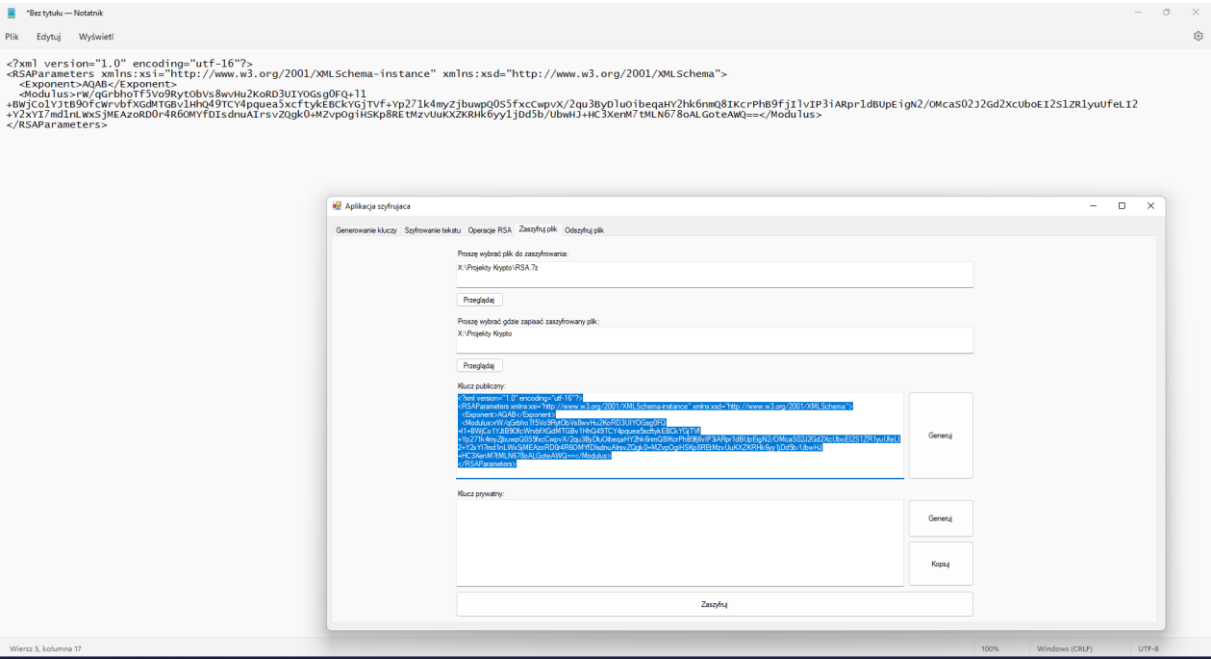
Sytuacja jest podobna jak w przypadku pola wskazującego plik do zaszyfrowania. Za pomocą przycisku znajdującego się obok pola uruchamiane jest okno wyboru folderu.



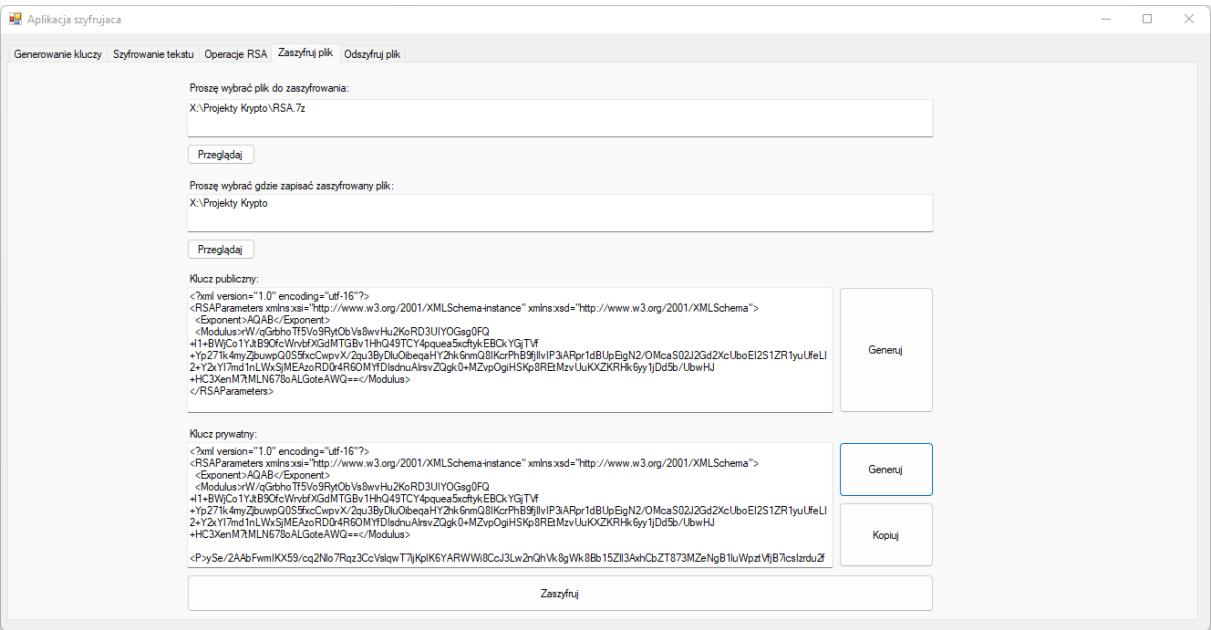
Test generowania klucza publicznego



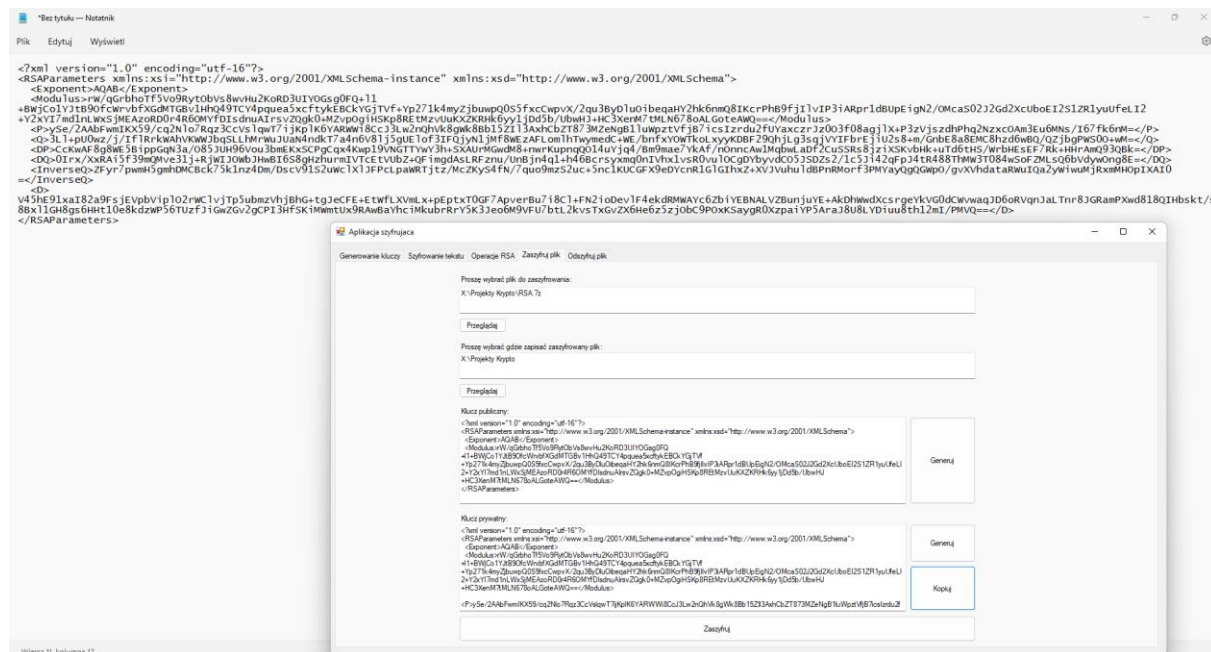
Oczywiście wygenerowany klucz, możemy zaznaczyć w całości za pomocą ctrl+a, skopiować i wkleić do np. notatnika



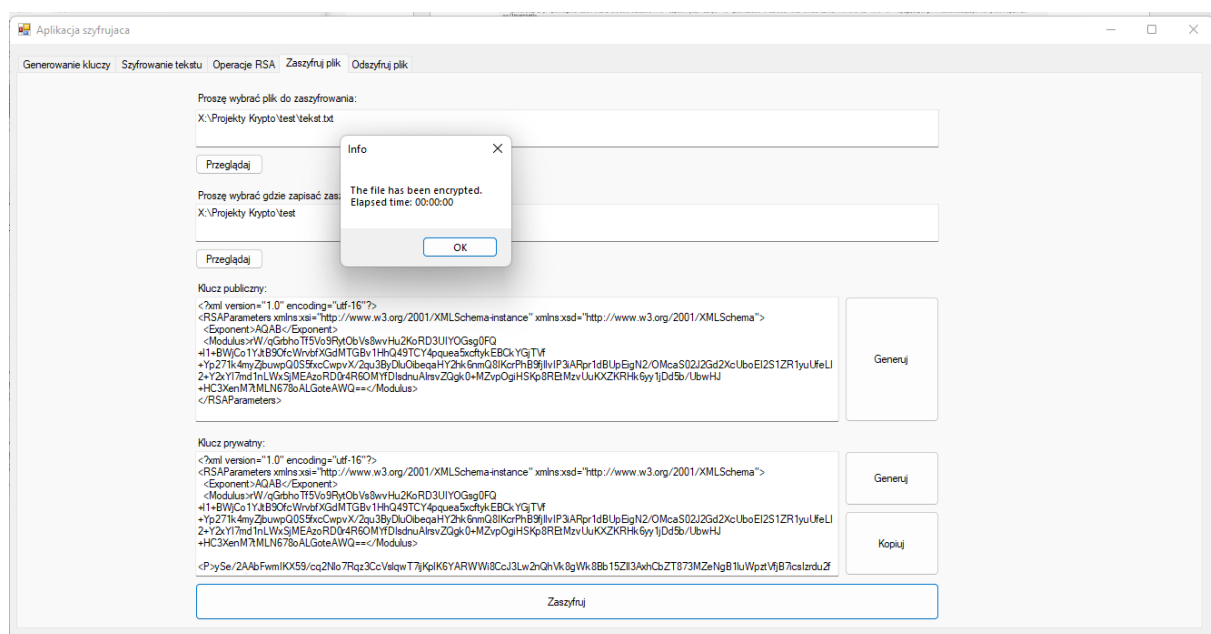
Test generowania klucza prywatnego.



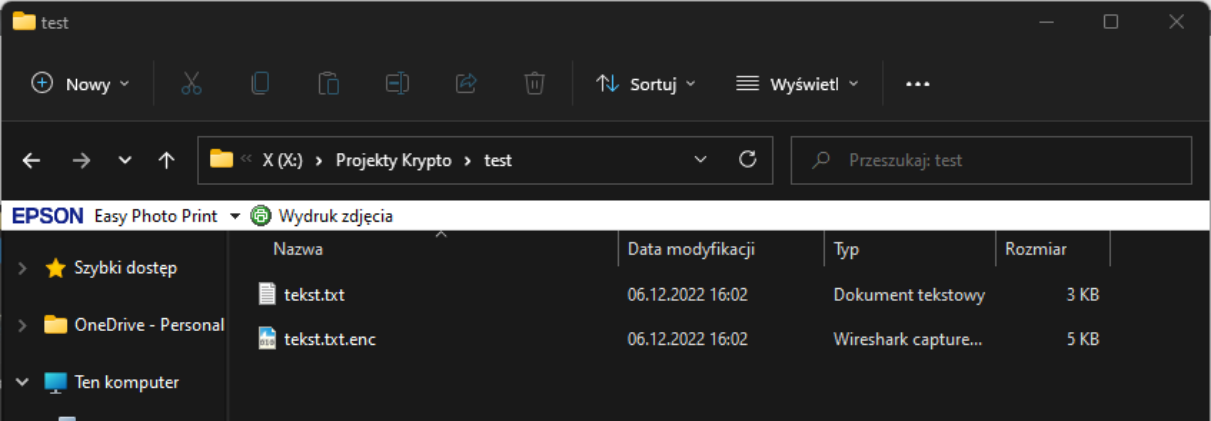
Możemy go skopiować za pomocą przycisku kopiuje bądź jak wyżej 😊



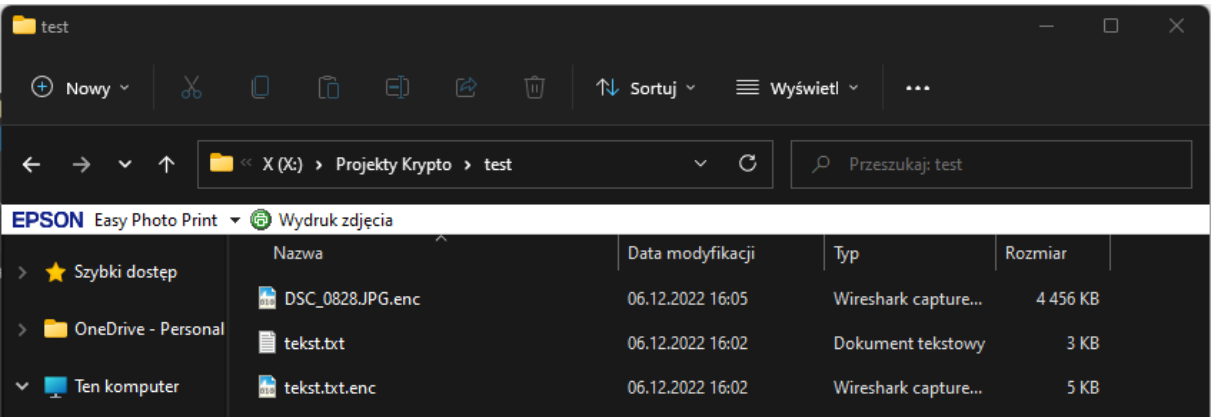
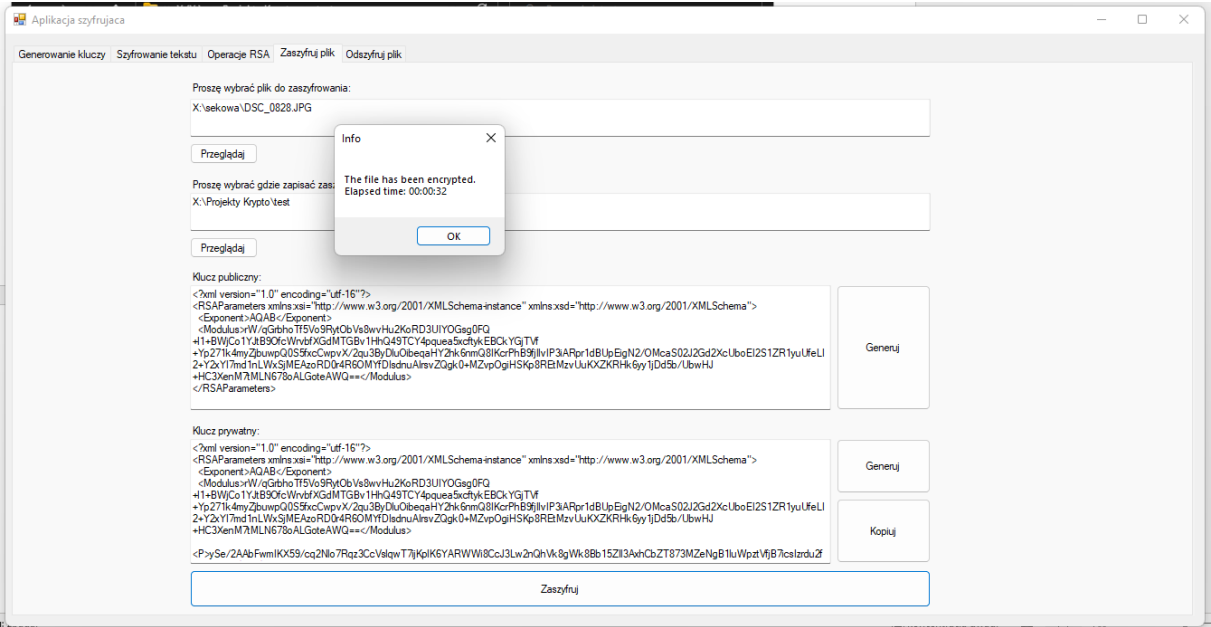
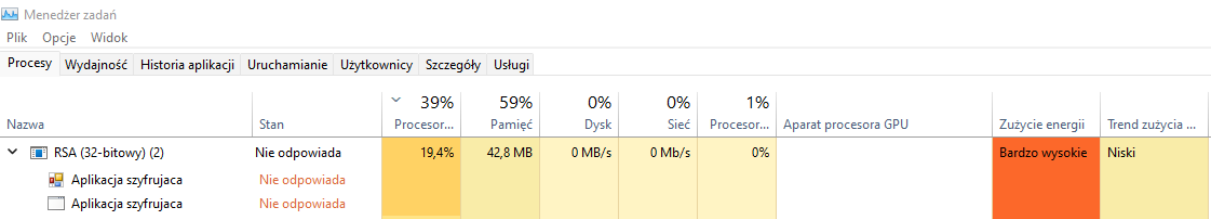
Test szyfrowania pliku tekstowego



W folderze pojawił się zaszyfrowany plik



Test szyfrowania pliku .jpg



Test szyfrowania pliku .pdf

Aplikacja szyfrująca

Generowanie kluczy

Szyfrowanie tekstu

Operacje RSA

Zaszyfruj plik

Odszyfruj plik

Proszę wybrać plik do zaszyfrowania:

X:\NSI\NSI_03\NSI03_RF_P2.pdf

Przeglądaj

Proszę wybrać gdzie zapisać zaszyfrowany plik:

X:\Projekty Krypto\test

Przeglądaj

Klucz publiczny:

<?xml version="1.0" encoding="utf-16"?>
<RSAParameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Exponent>AQAB</Exponent>
<Modulus>W/qGtbhoTf5Vo9RytObVa8wvHu2KoRD3UIYOGag0FQ
+1+BWjCo1Yt8B9CfWvbfXGdMTGBv1HhQ49TCY4puea5xchykEBCKYgTf
+Yp27Ik4myZbuwpQ055xkcCwpvX/2au3ByDuObegaHY2hk6mmQ8IKrPhB9JlVP3ARpr1dBUpEgN2/OmcaS02J2Gd2XcUboEI2S1ZR1yuUeLI
2+Y2xY17md1nLWxSMEazoRD04R60MYDIdnuAlrevZ0gk0+MZvpOgH5Kp8REBMzvUuKXZKRhk6yy1JdD5b/UbwHJ
+HC3XenM7MLN678oALGoteAWQ==</Modulus>
</RSAParameters>

Generuj

Klucz prywatny:

<?xml version="1.0" encoding="utf-16"?>
<RSAParameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Exponent>AQAB</Exponent>
<Modulus>W/qGtbhoTf5Vo9RytObVa8wvHu2KoRD3UIYOGag0FQ
+1+BWjCo1Yt8B9CfWvbfXGdMTGBv1HhQ49TCY4puea5xchykEBCKYgTf
+Yp27Ik4myZbuwpQ055xkcCwpvX/2au3ByDuObegaHY2hk6mmQ8IKrPhB9JlVP3ARpr1dBUpEgN2/OmcaS02J2Gd2XcUboEI2S1ZR1yuUeLI
2+Y2xY17md1nLWxSMEazoRD04R60MYDIdnuAlrevZ0gk0+MZvpOgH5Kp8REBMzvUuKXZKRhk6yy1JdD5b/UbwHJ
+HC3XenM7MLN678oALGoteAWQ==</Modulus>
<P>YSe/2AAbFwmlKX59/cq2N8o7Rqz3CcVslqwT7k/KpK6YARWWi8CcJ3Lw2nQhVh8gWk8Bb15Zl3AxBzT873MZeNgB1luWpztVjB7cslzduZf

Generuj

Kopij

Zaszyfruj

▼ RSA (32-bitowy)

3,0%

29,3 MB

0,3 MB/s

0 Mb/s

0%

Umiarkowany

Bardzo niskie

Aplikacja szyfrująca

Aplikacja szyfrująca

Generowanie kluczy

Szyfrowanie tekstu

Operacje RSA

Zaszyfruj plik

Odszyfruj plik

Proszę wybrać plik do zaszyfrowania:

X:\NSI\NSI_03\NSI03_RF_P2.pdf

Przeglądaj

Proszę wybrać gdzie zapisać zaszyfrowany plik:

X:\Projekty Krypto\test

Przeglądaj

Klucz publiczny:

<?xml version="1.0" encoding="utf-16"?>
<RSAParameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Exponent>AQAB</Exponent>
<Modulus>W/qGtbhoTf5Vo9RytObVa8wvHu2KoRD3UIYOGag0FQ
+1+BWjCo1Yt8B9CfWvbfXGdMTGBv1HhQ49TCY4puea5xchykEBCKYgTf
+Yp27Ik4myZbuwpQ055xkcCwpvX/2au3ByDuObegaHY2hk6mmQ8IKrPhB9JlVP3ARpr1dBUpEgN2/OmcaS02J2Gd2XcUboEI2S1ZR1yuUeLI
2+Y2xY17md1nLWxSMEazoRD04R60MYDIdnuAlrevZ0gk0+MZvpOgH5Kp8REBMzvUuKXZKRhk6yy1JdD5b/UbwHJ
+HC3XenM7MLN678oALGoteAWQ==</Modulus>
</RSAParameters>

Generuj

Klucz prywatny:

<?xml version="1.0" encoding="utf-16"?>
<RSAParameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Exponent>AQAB</Exponent>
<Modulus>W/qGtbhoTf5Vo9RytObVa8wvHu2KoRD3UIYOGag0FQ
+1+BWjCo1Yt8B9CfWvbfXGdMTGBv1HhQ49TCY4puea5xchykEBCKYgTf
+Yp27Ik4myZbuwpQ055xkcCwpvX/2au3ByDuObegaHY2hk6mmQ8IKrPhB9JlVP3ARpr1dBUpEgN2/OmcaS02J2Gd2XcUboEI2S1ZR1yuUeLI
2+Y2xY17md1nLWxSMEazoRD04R60MYDIdnuAlrevZ0gk0+MZvpOgH5Kp8REBMzvUuKXZKRhk6yy1JdD5b/UbwHJ
+HC3XenM7MLN678oALGoteAWQ==</Modulus>
<P>YSe/2AAbFwmlKX59/cq2N8o7Rqz3CcVslqwT7k/KpK6YARWWi8CcJ3Lw2nQhVh8gWk8Bb15Zl3AxBzT873MZeNgB1luWpztVjB7cslzduZf

Generuj

Kopij

Zaszyfruj

Info

The file has been encrypted.
Elapsed time: 00:00:02

OK

test

Nowy

Sortuj

Wyświetl

<> X (X%) > Projekty Krypto > test

Przeszukaj: test

EPSON Easy Photo Print

Wydruk zdjęcia

| | Nazwa | Data modyfikacji | Typ | Rozmiar |
|-----------------------|---------------------|------------------|----------------------|----------|
| > ★ Szybki dostęp | DSC_0828.JPG.enc | 06.12.2022 16:05 | Wireshark capture... | 4 456 KB |
| > OneDrive - Personal | NSI03_RF_P2.pdf.enc | 06.12.2022 16:23 | Wireshark capture... | 1 057 KB |
| > Ten komputer | tekst.txt | 06.12.2022 16:02 | Dokument tekstowy | 3 KB |
| > Dokumenty | tekst.txt.enc | 06.12.2022 16:02 | Wireshark capture... | 5 KB |

Test deszyfrowania pliku

Widok okna deszyfrowania pliku

Aplikacja szyfrująca

Generowanie kluczy Szyfrowanie tekstu Operacje RSA Zaszifruj plik Odszyfnuj plik

Proszę wybrać plik do deszyfracji

Przeglądaj

Proszę wskazać gdzie zapisać odszyfrowany plik:

Przeglądaj

Klucz prywatny do deszyfracji pliku:

Wklej

Odszyfnuj

Test uruchomienia deszyfrowania przy pustych polach

Aplikacja szyfrująca

Generowanie kluczy Szyfrowanie tekstu Operacje RSA Zaszifruj plik Odszyfnuj plik

Proszę wybrać plik do deszyfracji

Przeglądaj

Warning

File to decrypt path input, destination folder, and private key input can not be empty!

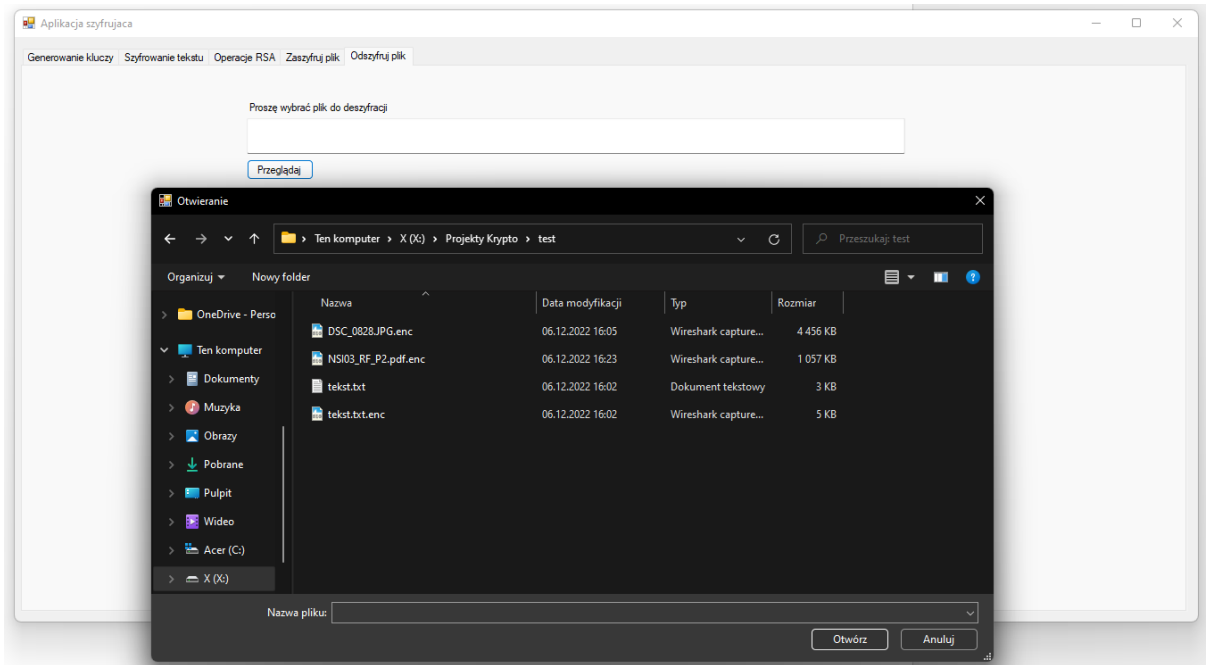
OK

Wklej

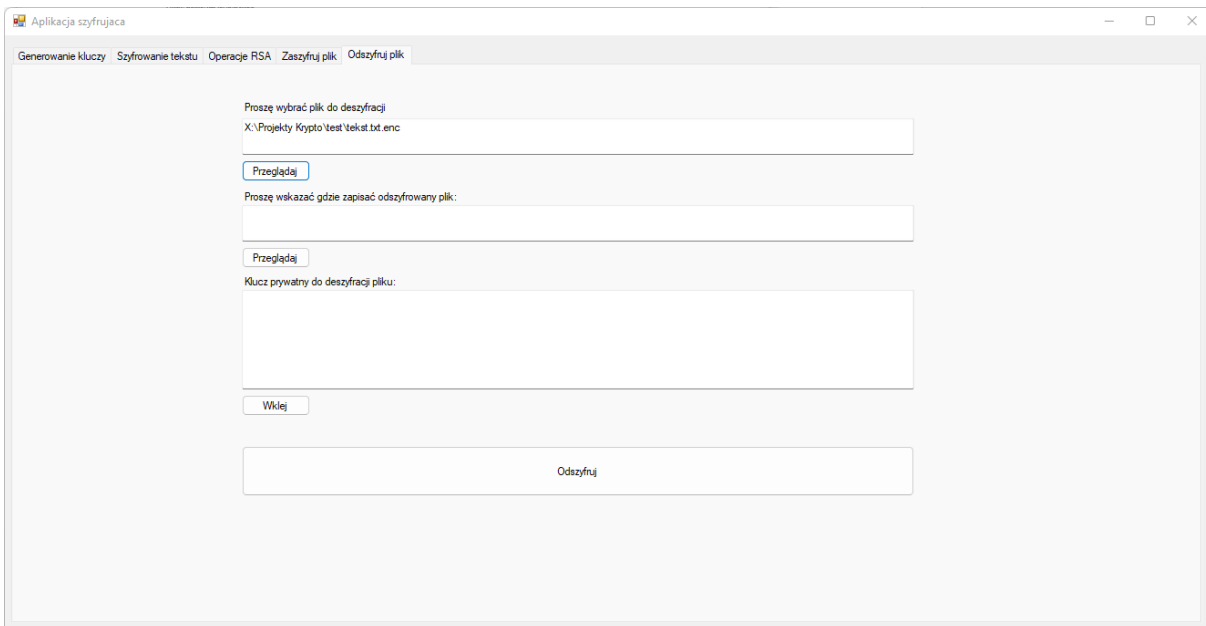
Odszyfnuj

Aplikacja wyświetla komunikat, że pola nie mogą być puste. Komunikat wyświetlany jest zarówno, gdy jedno lub więcej z pól jest puste.

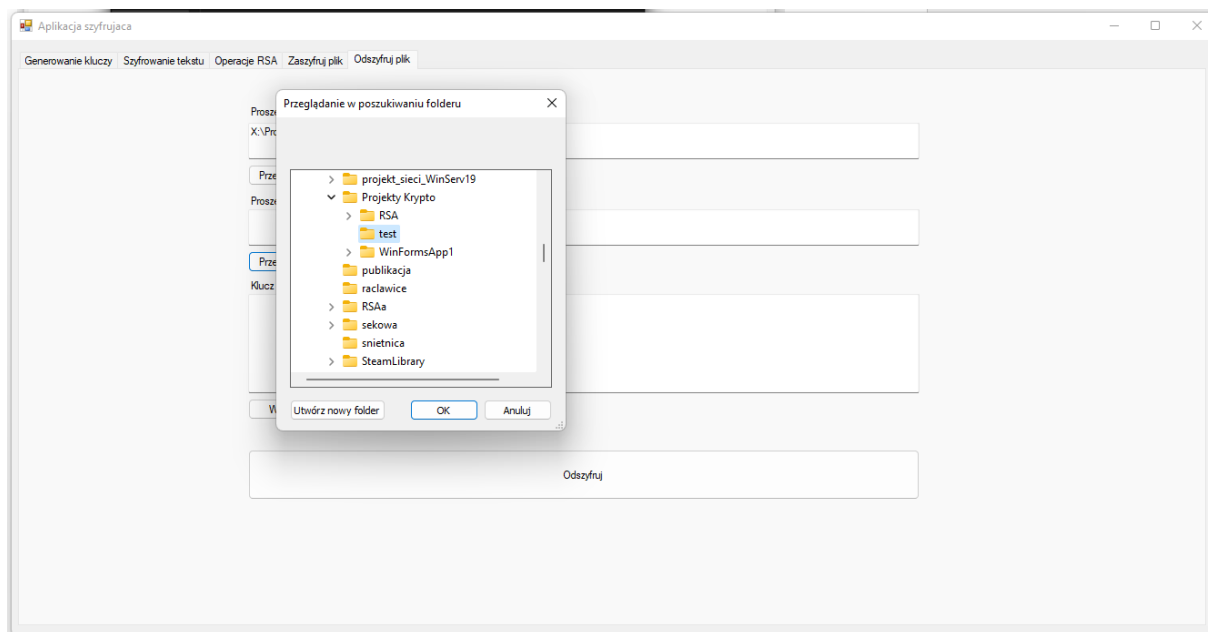
Test pola wskazania pliku do deszyfracji



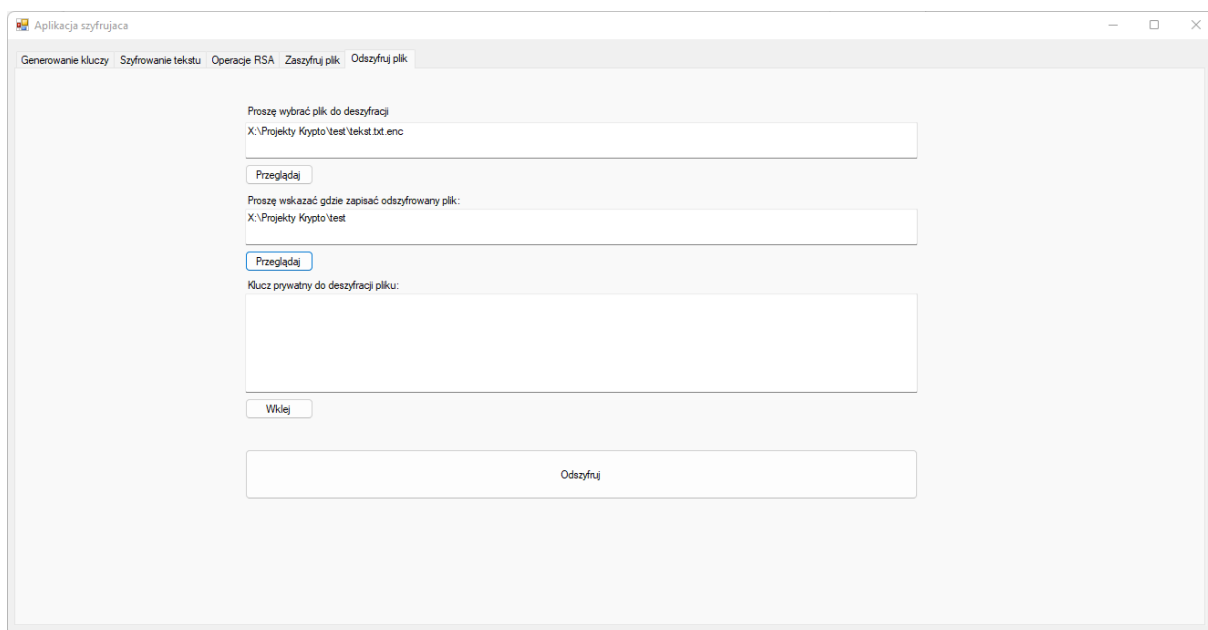
Po wybraniu pliku ścieżka pojawia nam się w polu.



Test pola wskazania, gdzie zapisać odszyfrowany plik



Po wskazaniu ścieżka pokazuje nam się w polu



Test generowania klucza prywatnego (skopiowanego z zakładki szyfrowanie)

Za pomocą przycisku wklej dodajemy wcześniej skopiowany przez nas klucz prywatny

Aplikacja szyfrująca

Generowanie kluczy Szyfrowanie tekstu Operacje RSA Zaszyfruj plik Odszyfruj plik

Proszę wybrać plik do deszyfracji:
X:\Projekty Krypto\test\tekst.bt.enc

Przeglądaj

Proszę wskazać gdzie zapisać odszyfrowany plik:
X:\Projekty Krypto\test

Przeglądaj

Klucz prywatny do deszyfracji pliku:
<?xml version="1.0" encoding="utf-16"?>
<RSAPrivateKey xmlns="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Exponent>AQAB</Exponent>
<Modulus>W/qGbh0Tf5Vo9RyObVs8wvHu2K6RD3UIYOgag0FQ+1+BWJCo1Yj8B90cWnbfXGdMTGBv1HhQ49TCY4paea5cftykEBCKYGTfVf
+Yp27k4myZbuwpQ0S5fxcCwvX/Zqu3ByDUObegaHY2k5nmQ8IKcPhB9jlvIP3ARp1d8UpEgN2/OmcaS02J2Gd2KcUboEi2S1ZRtyuLfeLJ2+Y2x
Y7md1nLWwSJMEazoRDQ4R6OMYDladrnAlravZ0gk0-MZvpOgH5Kp8REImzvUuKXZKRk4gy1jDd5b/UbwHJ
+HC3XenM7MLN678oALGoteAWQ==</Modulus>

Wklej

Odszyfruj

W celu rozszyfrowania pliku wciskamy przycisk Odszyfruj. Plik zostaje odszyfrowany

Aplikacja szyfrująca

Generowanie kluczy Szyfrowanie tekstu Operacje RSA Zaszyfruj plik Odszyfruj plik

Proszę wybrać plik do deszyfracji:
X:\Projekty Krypto\test\tekst.bt.enc

Przeglądaj

Proszę wskazać gdzie zapisać odszyfrowany plik:
X:\Projekty Krypto\test

Przeglądaj

Klucz prywatny do deszyfracji pliku:
<?xml version="1.0" encoding="utf-16"?>
<RSAPrivateKey xmlns="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<Exponent>AQAB</Exponent>
<Modulus>W/qGbh0Tf5Vo9RyObVs8wvHu2K6RD3UIYOgag0FQ+1+BWJCo1Yj8B90cWnbfXGdMTGBv1HhQ49TCY4paea5cftykEBCKYGTfVf
+Yp27k4myZbuwpQ0S5fxcCwvX/Zqu3ByDUObegaHY2k5nmQ8IKcPhB9jlvIP3ARp1d8UpEgN2/OmcaS02J2Gd2KcUboEi2S1ZRtyuLfeLJ2+Y2x
Y7md1nLWwSJMEazoRDQ4R6OMYDladrnAlravZ0gk0-MZvpOgH5Kp8REImzvUuKXZKRk4gy1jDd5b/UbwHJ
+HC3XenM7MLN678oALGoteAWQ==</Modulus>

Wklej

Odszyfruj

Info

The file has been decrypted.
Elapsed time: 00:00:00

OK

W folderze pojawia się plik decrypted_NAZWA.txt

test

Nowy Szukaj

Wybierz folder

Test komputer > X (D:) > Projekty Krypto > test

Przełączaj test

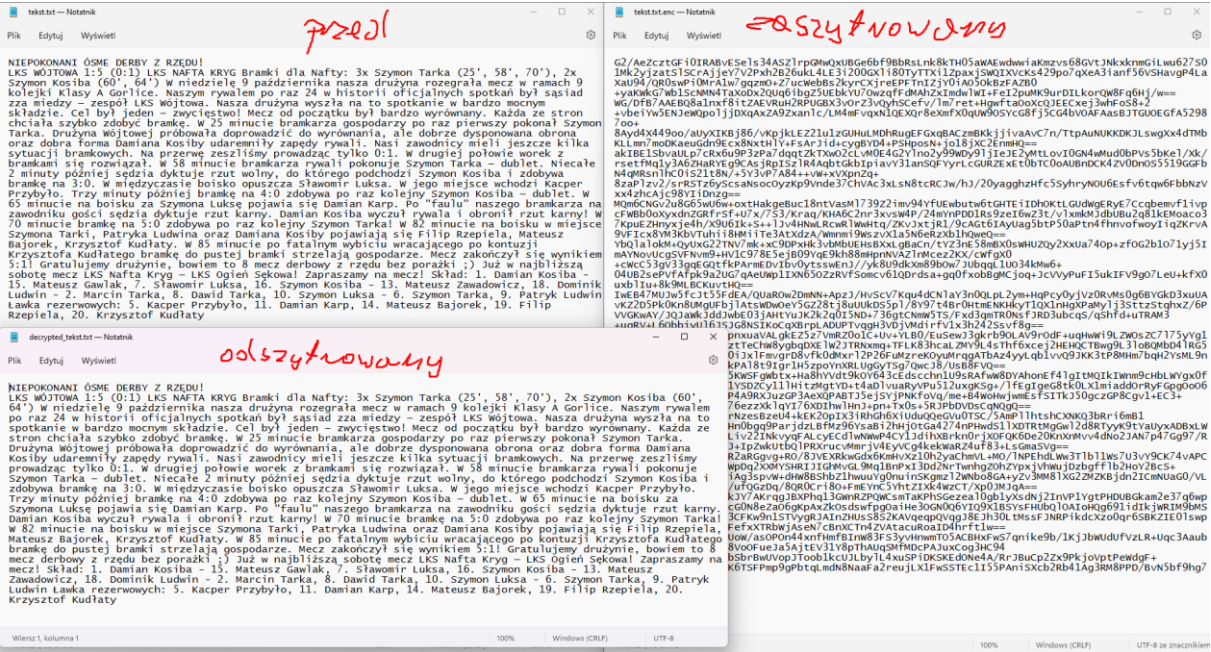
| Nazwa | Data modyfikacji | Typ | Rozmiar |
|--------------------|------------------|----------------------|----------|
| decrypted_idk.txt | 06.12.2022 16:36 | Dokument tekstowy | 3 KB |
| DSC_0028.JPG.enc | 06.12.2022 16:05 | Winetrack capture... | 4 456 KB |
| N903_RF_P2.pdf.enc | 06.12.2022 16:23 | Winetrack capture... | 1 057 KB |
| idk.txt | 06.12.2022 16:02 | Dokument tekstowy | 3 KB |
| idk.txt.enc | 06.12.2022 16:02 | Winetrack capture... | 5 KB |

decrypted_idk.txt - Notepad

Plik Edytuj Wyświetl

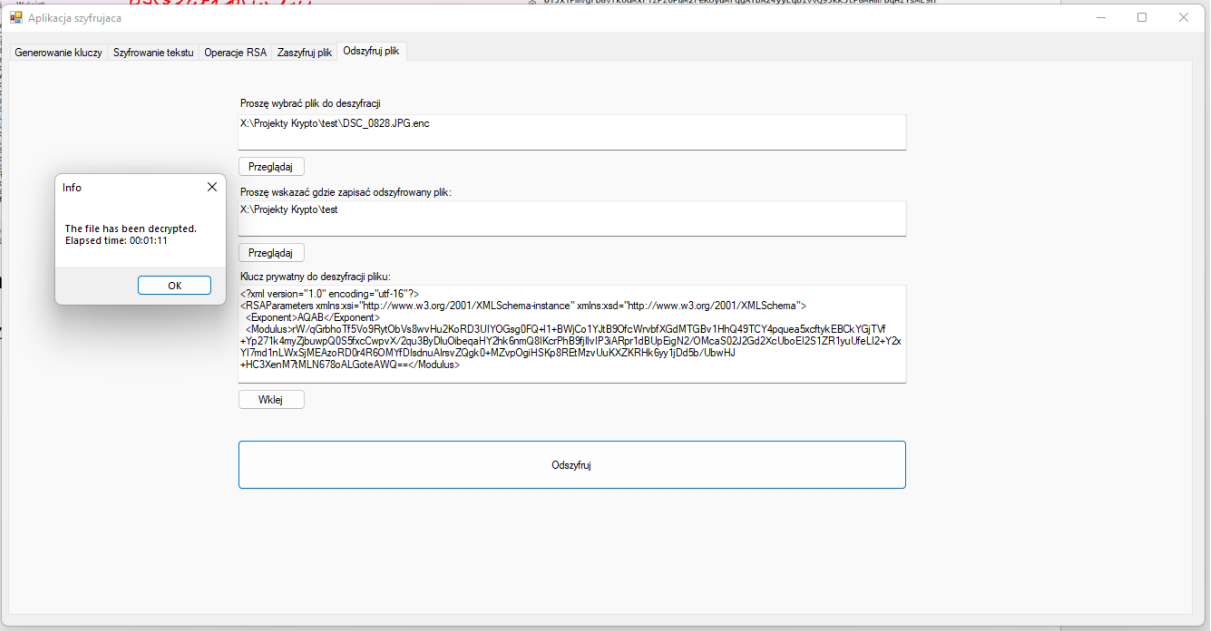
NIEPOKONANI ÓSMIE DERBY Z RZĘDU!
LKS WÓJTOWA 1:5 (0:1) LKS NAFTA KRYG Bramki dla Nafty: 3x Szymon Tarka (25', 58', 70'), 2x Szymon Kosiba (60', 64') W niedzielę 9 października nasza drużyna rozegrała mecz w ramach 9 kolejki Klasy A gorlice. Naszym rywalem po raz 24 w historii oficjalnych spotkań był sąsiad zza miedzy – zespół LKS Wójtowa. Nasza drużyna wyszła na to spotkanie w bardzo mocnym składzie. Cel był jeden – zwycięstwo! Mecz od początku był bardzo wyrównany. Każda ze stron chciała szybko zdobyć bramkę. W 25 minucie bramkarza gospodarzy po raz pierwszy pokonał Szymon Tarka. Drużyna wójtowej próbowała doprowadzić do wyrównania, ale dobrze dysponowana obrona oraz dobra forma Damiana Kosiby udaremniły zapędy rywali. Nasi zawodnicy mieli jeszcze kilka sytuacji bramkowych. Na przerwę zesłaliśmy prowadząc tylko 0:1. W drugiej połowie work z bramkami się rozwiązał. W 58 minucie bramkarza rywali pokonuje Szymon Tarka – dublet. Niecałe 2 minuty później sędzia dyktuje rzut wolny, do którego podchodzi Szymon Kosiba i zdobywa bramkę na 3:0. W międzyczasie boisko opuszcza Sławomir Luksa. W jego miejsce wchodzi Kacper Przybyło. Trzy minuty później bramkę na 4:0 zdobywa po raz kolejny Szymon Kosiba – dublet. W 65 minucie na boisku za Szymona Lukę pojawia się Damian Karp. Po "faulu" naszego bramkarza na zawodniku gości sędzia dyktuje rzut karny. Damian Kosiba wyczuł rywala i obronił rzut karny! W 70 minucie bramkę na 5:0 zdobywa po raz kolejny Szymon Tarka! W 82 minucie na boisku w miejsce Szymona Tarki, Patryka Ludwina oraz Damiana Kosiby pojawiają się Filip Rzepliela, Mateusz Bajorek, Krzysztof Kudłaty. W 85 minucie po fatalnym wybieciu wracającego po kontuzji Krzysztofa Kudłatego bramkę do pustej bramki strzelają gospodarze. Mecz zakończył się wynikiem 5:1! Gratulujemy drużynie, bowiem to 8 mecz derbowy z rzędu bez porażki ;) Już w najbliższą sobotę mecz LKS Nafta Kryg – LKS Opień Sękowal Zapraszamy na mecz! Skład: 1. Damian Kosiba - 15. Mateusz Gwiałak, 7. Sławomir Luksa, 16. Szymon Kosiba - 13. Mateusz Zawadowicz, 18. Dominik Ludwin - 2. Marcin Tarka, 8. Dawid Tarka, 10. Szymon Luksa - 6. Szymon Tarka, 9. Patryk Ludwin Ławka rezerwowych: 3. Kacper Przybyło, 11. Damian Karp, 14. Mateusz Bajorek, 19. Filip Rzepliela, 20. Krzysztof Kudłaty

Porównanie zawartości plików. Przed szyfrowaniem. Po zaszyfrowaniu. Po rozszyfrowaniu



Jak można zauważyć plik został poprawnie odszyfrowany.

Odszyfrowanie pliku .jpg



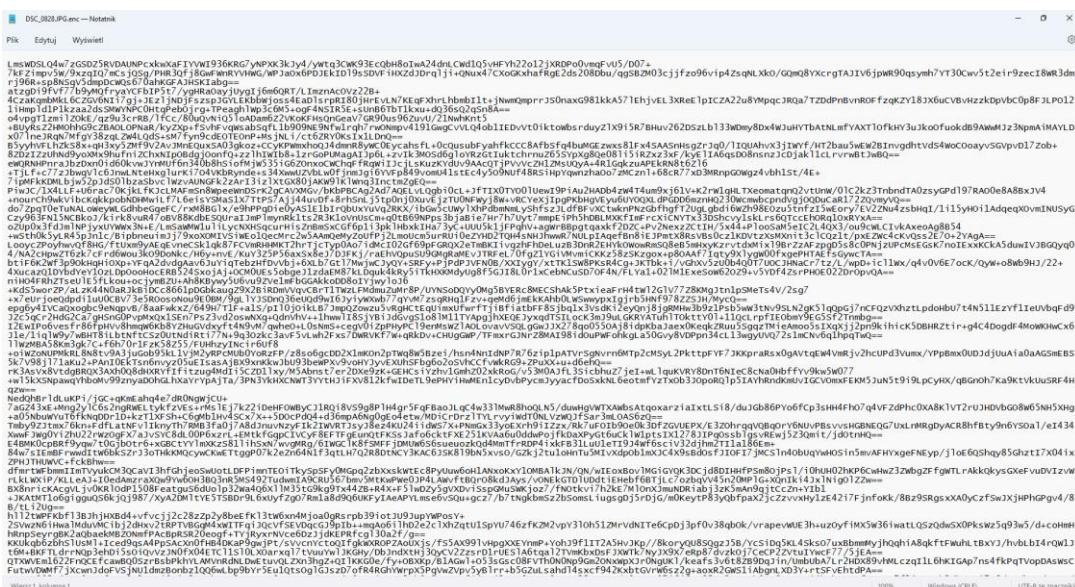
W folderze pojawia się plik decrypted_NAZWA.jpg

| | | | | |
|--|--|--|--|--|
| test | | | | |
| Nowy | | | | |
| Sortuj Wyświetl | | | | |
| ← → ↑ ↓ Ten komputer > X (C:) > Projekty Krypto > test | | | | |
| Przeszukaj: test | | | | |
| EPSON Easy Photo Print Wydruk zdjęcia | | | | |
| Nazwa Data modyfikacji Typ Rozmiar | | | | |
| Szybki dostęp | | | | |
| OneDrive - Personal | | | | |
| Ten komputer | | | | |
| Dokumenty | | | | |
| Muzyka | | | | |
| Obrazy | | | | |
| decrypted_DSC_0828.JPG | | | | |
| decrypted tekst.txt | | | | |
| DSC_0828.JPG.enc | | | | |
| NSIO3_RF_P2.pdf.enc | | | | |
| tekst.txt | | | | |
| tekst.txt.enc | | | | |

Przed odszyfrowaniem:



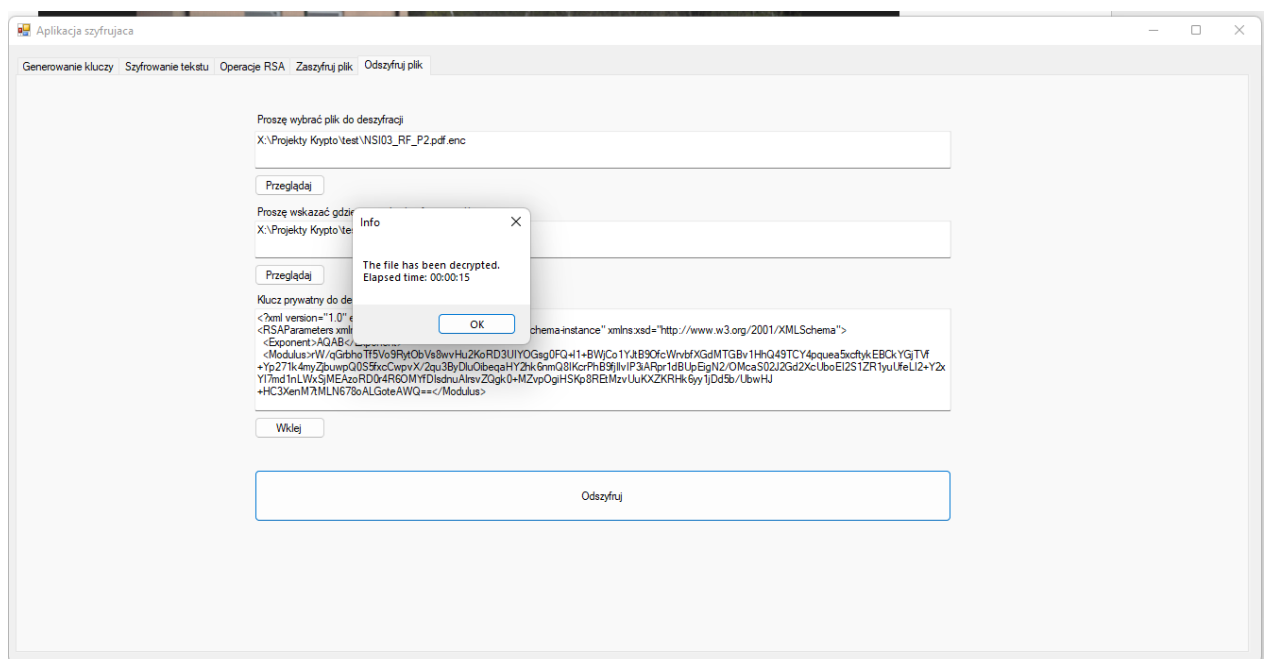
Po zaszyfrowaniu:



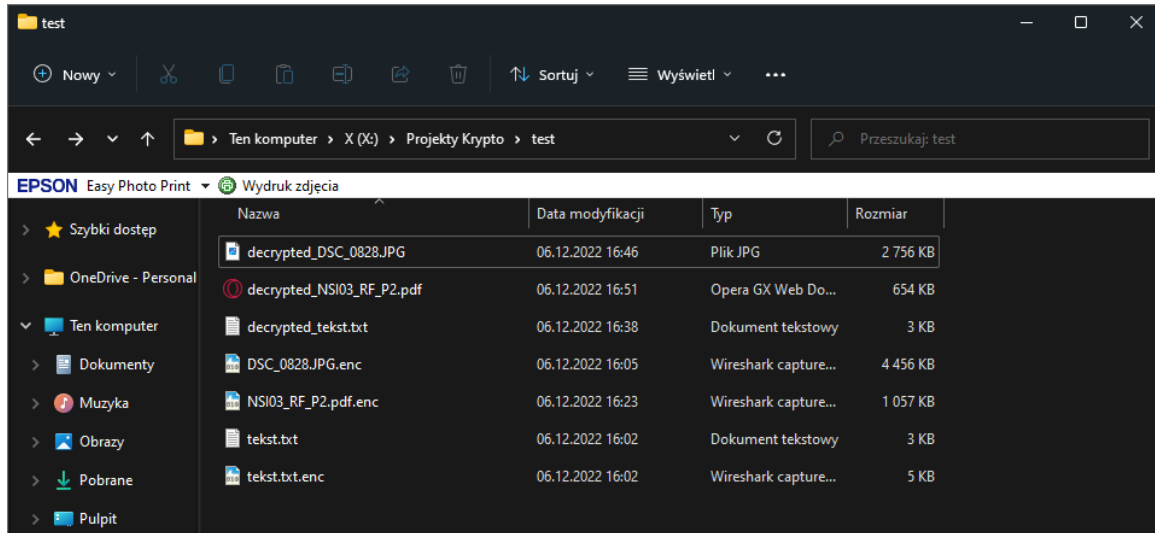
Po odszyfrowaniu:



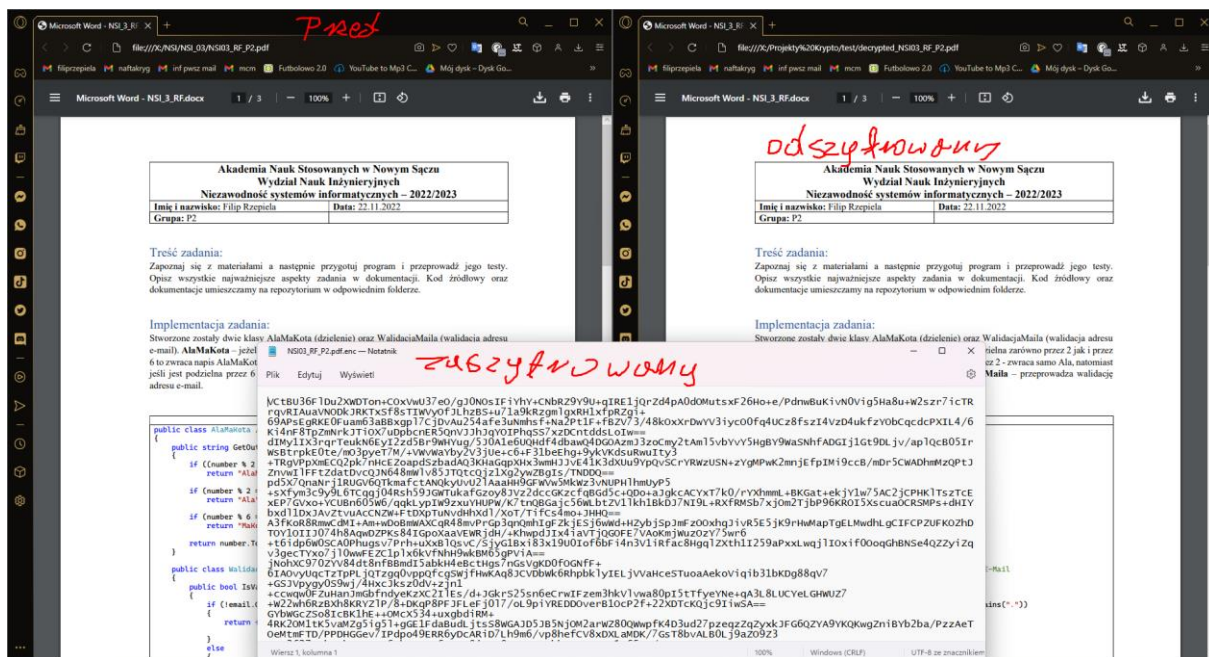
Rozszyfrowanie pliku .pdf



W folderze pojawia się plik decrypted_NAZWA.pdf



Porównanie przed zaszyfrowaniem, zaszyfrowany i odszyfrowany



Zużycie zasobów podczas odszyfrowywania

| | | | | | | | | | | |
|--|--|------|--------------------|---------------|------------|------------|-------------------|----------------------|-----------------|-------------------|
| Menedżer zadań | | | | | | | | | | |
| Plik Opcje Widok | | | | | | | | | | |
| Procesy Wydajność Historia aplikacji Uruchamianie Użytkownicy Szczegóły Usługi | | | | | | | | | | |
| Nazwa | | Stan | 53% Procesor... | 67% Pamięć | 0% Dysk | 0% Sieć | 3% Procesor... | Aparat procesora GPU | Zużycie energii | Trend zużycia ... |
| ▼ RSA (32-bitowy) | | | 14,9% | 21,6 MB | 0 MB/s | 0 Mb/s | 0% | | Bardzo wysokie | Niski |
| <input type="checkbox"/> Aplikacja szyfrująca | | | | | | | | | | |

Wnioski

- Interfejs graficzny jest łatwy oraz przyjemny w obsłudze.
- Aplikacja została zabezpieczona przed uruchomieniem, jeżeli pola są puste.
- Program działa relatywnie szybko.
- Aplikacja RSA w sposób poprawny dokonuje zaszyfrowania oraz odszyfrowania zarówno tekstu jak i plików. Atutem jest fakt, że nie powoduje uszkodzenia plików.
- Podczas przeprowadzanych testów Aplikacja RSA nie przestawała działać, nie wyrządzała błędów w systemie oraz nie wyłączała się.
- Mamy możliwość uruchomienia kilku okien aplikacji.