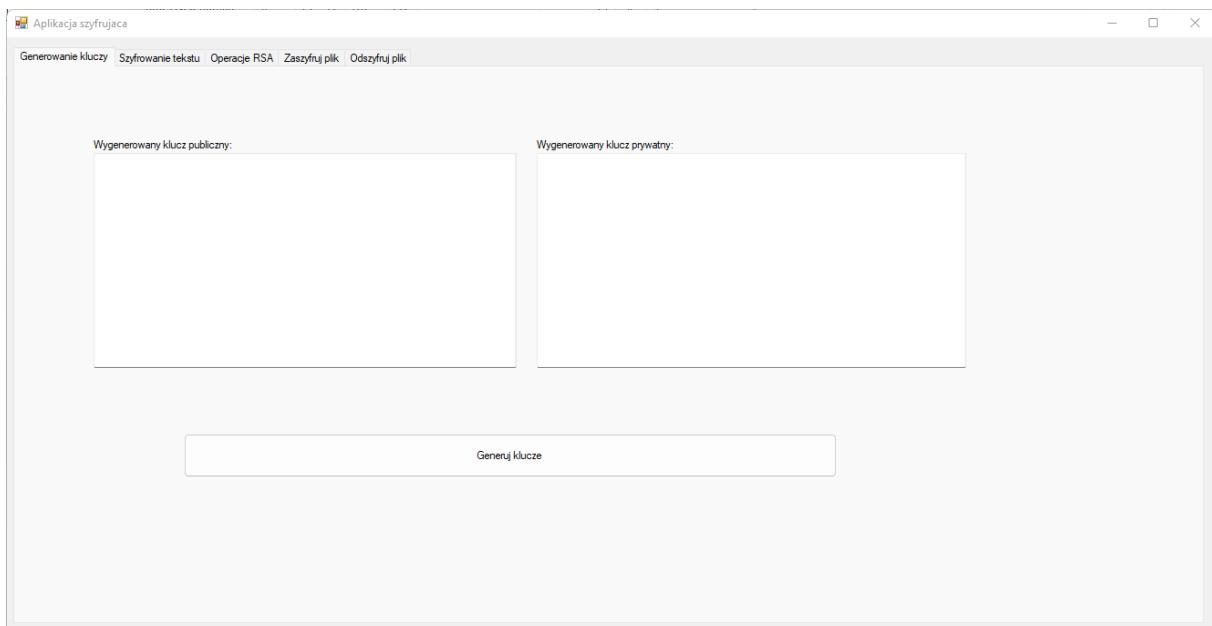


Akademia Nauk Stosowanych w Nowym Sączu
Wydział Nauk Inżynierijnych
czesawodność systemów informatycznych –2022/2023

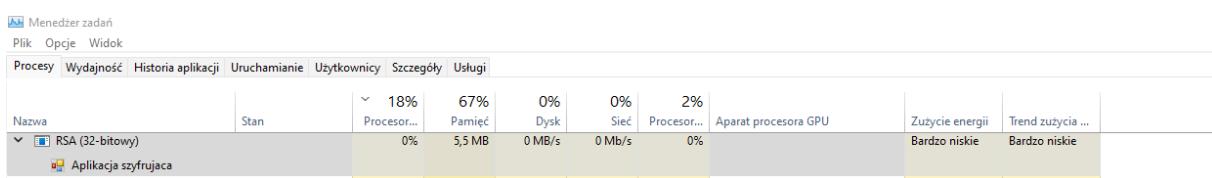
Imię i nazwisko: Filip Rzepiela **Data:** 06.12.2022
Grupa: P2

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

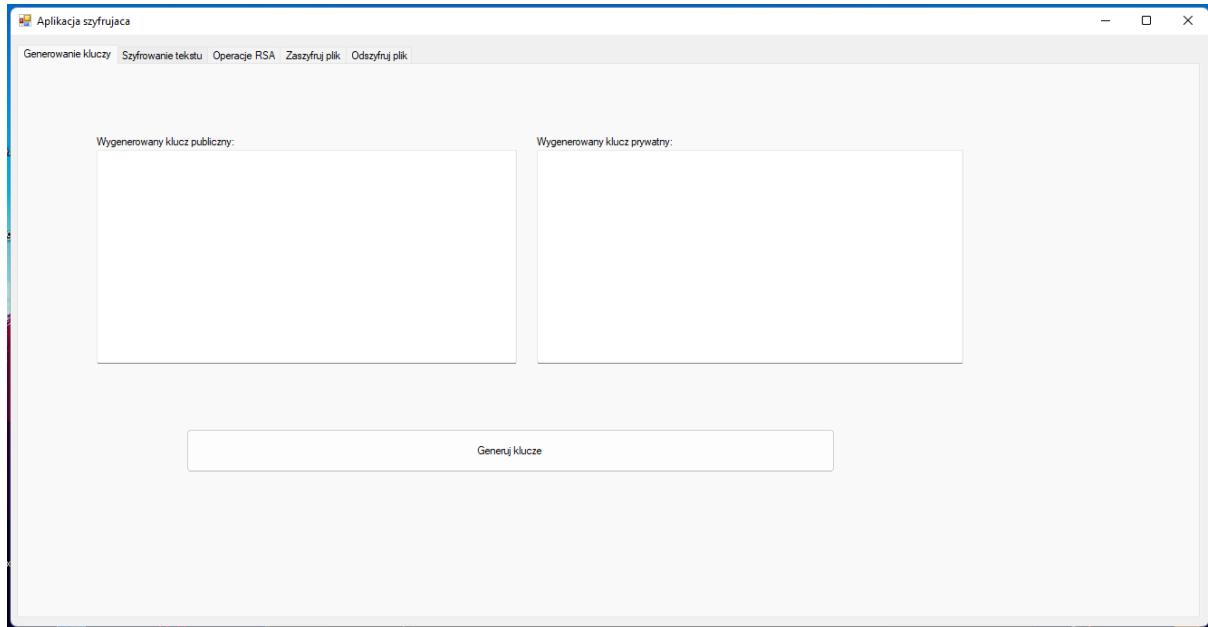
Zakładka pierwsza – generowanie kluczy publicznych



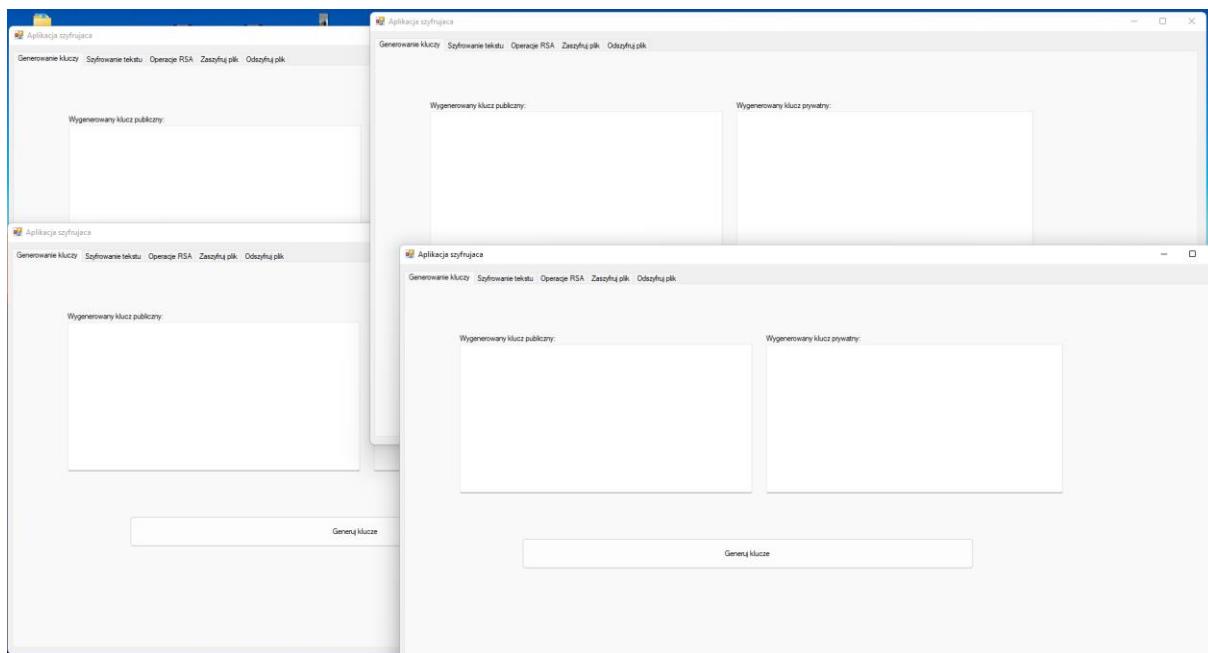
Zużycie zasobów w czasie bezczynności



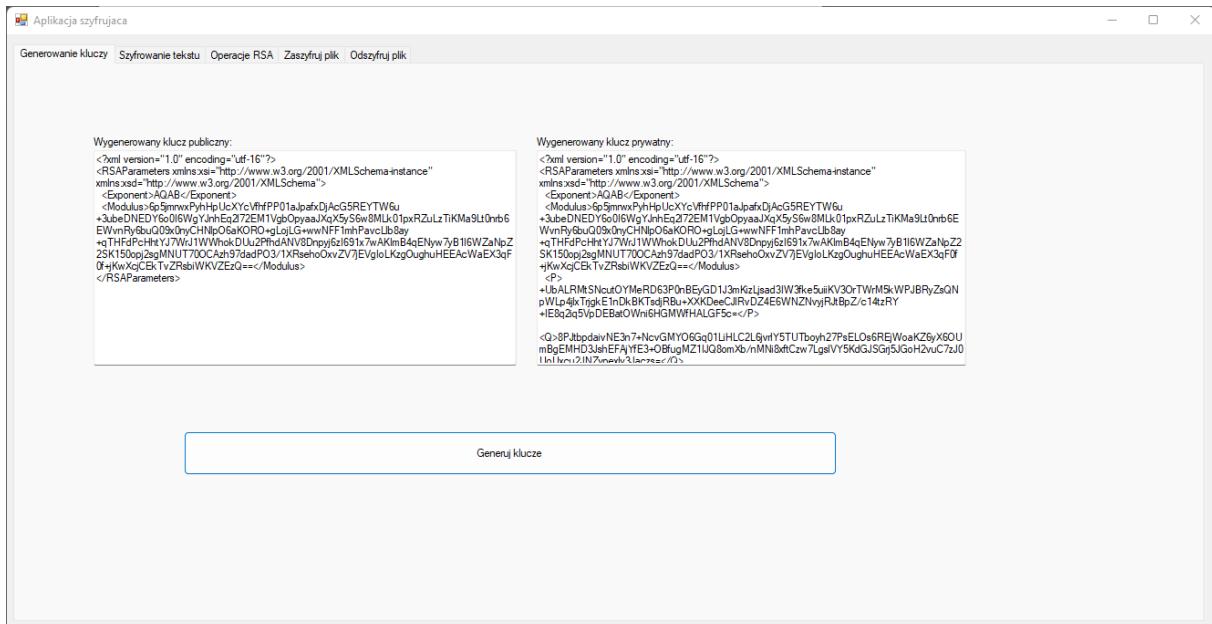
Po najechaniu na dowolną kartę, karta nabiera szarawy kolor



Możliwe jest uruchomienie kilku instancji programu



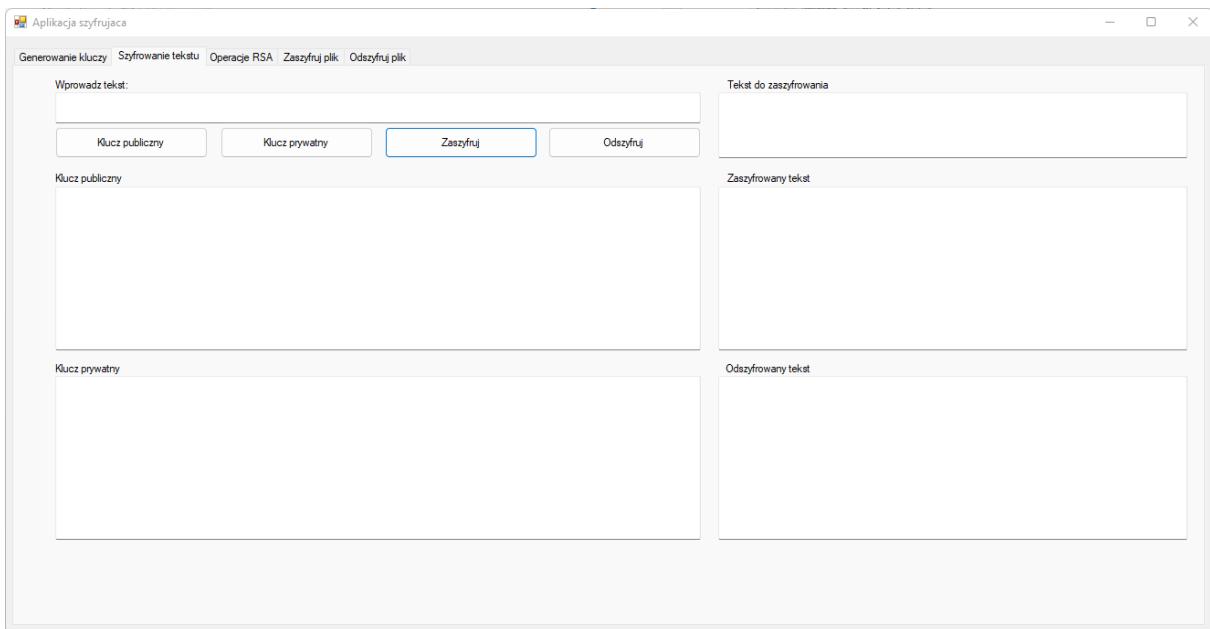
Test generowania kluczy



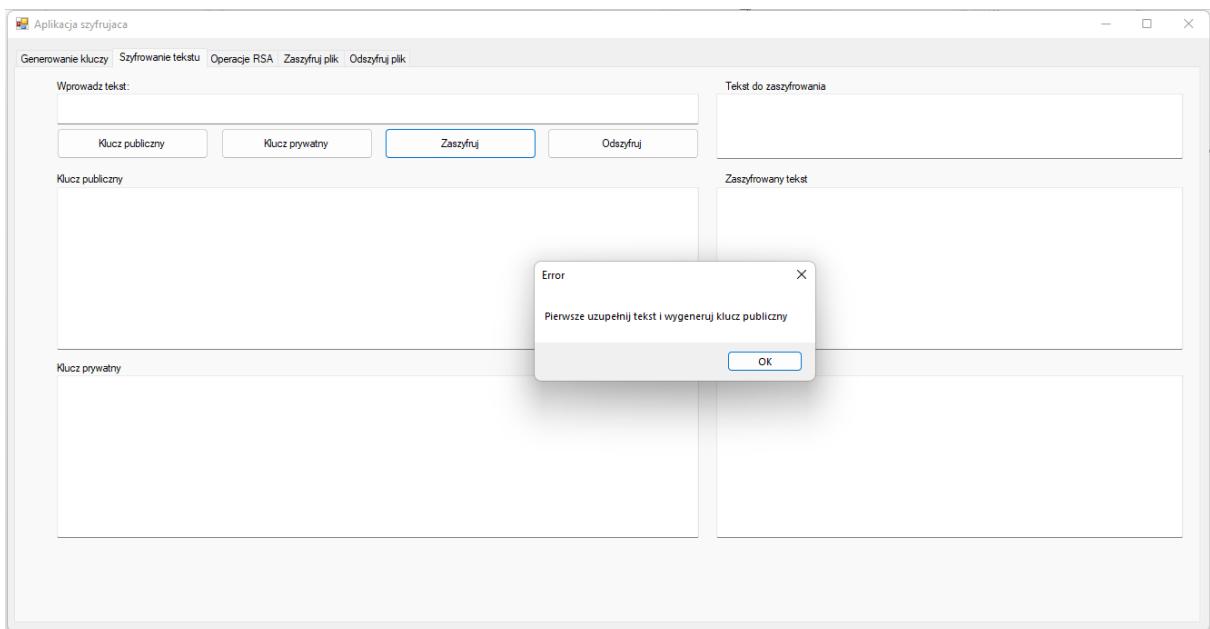
Jak możemy zauważyć, po wcisnięciu generuj klucze otrzymujemy wygenerowany klucz prywatny oraz publiczny.

Test szyfrowania tekstu

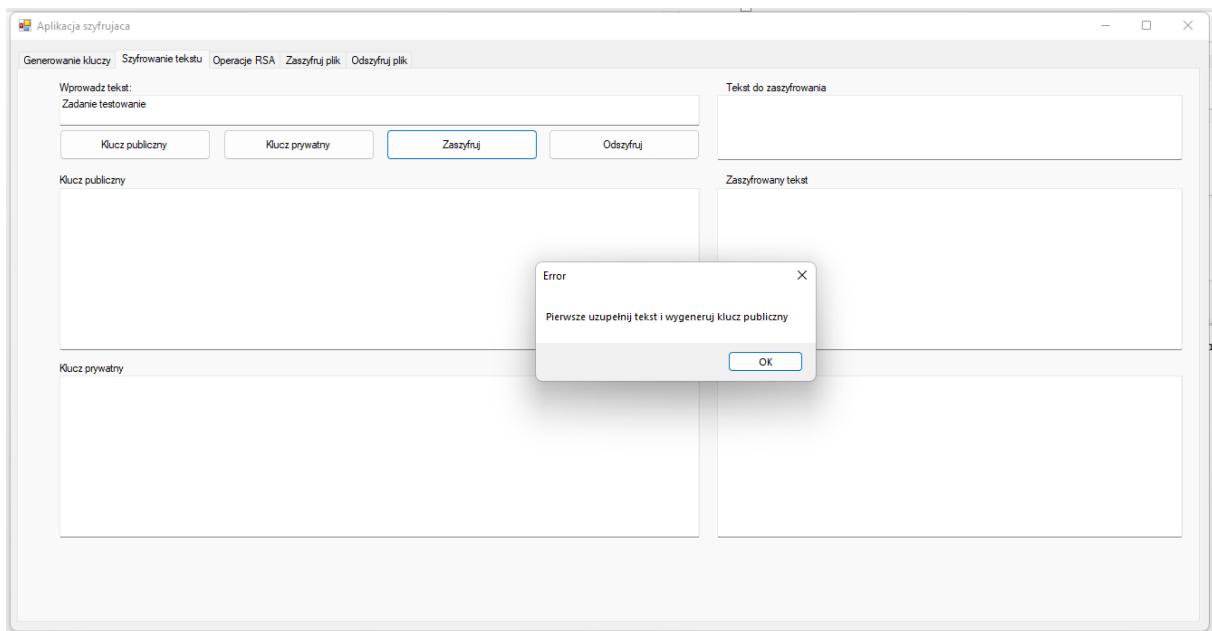
Okno szyfrowania tekstu



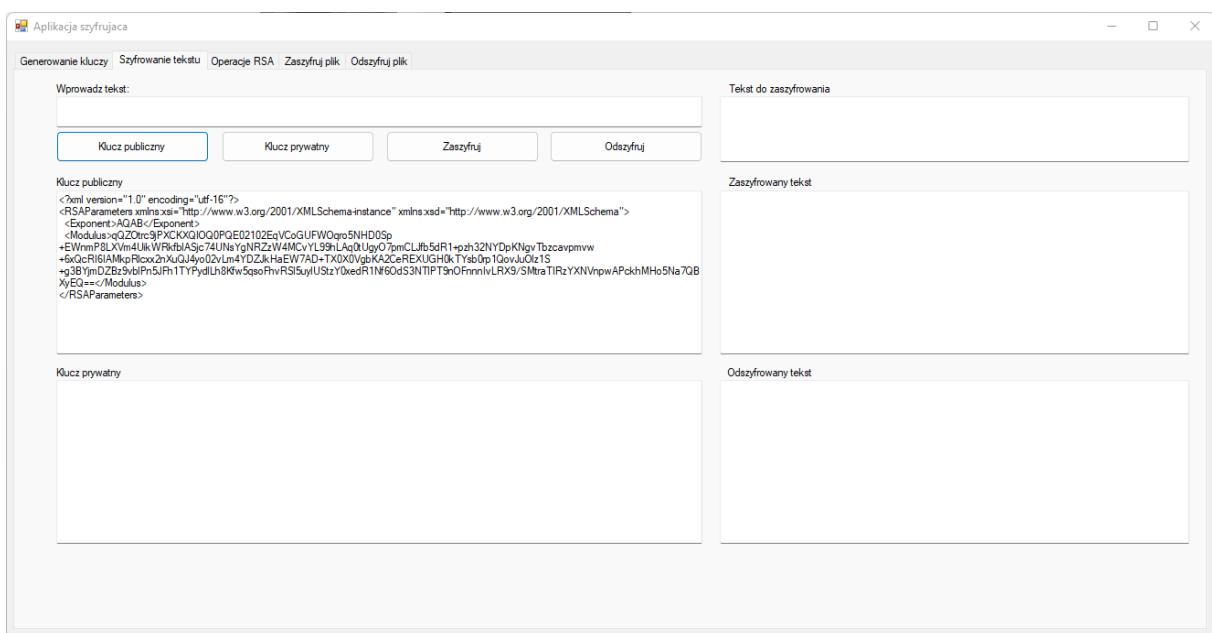
Próba zaszyfrowania przy pustych polach:



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

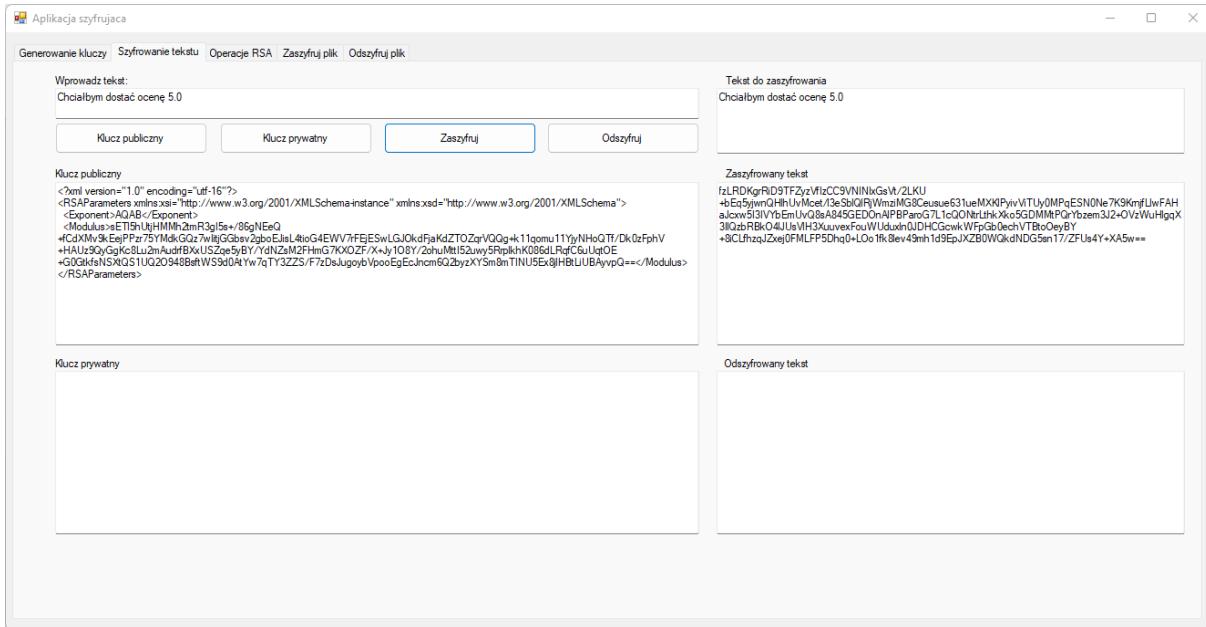


Test generowania klucza publicznego.



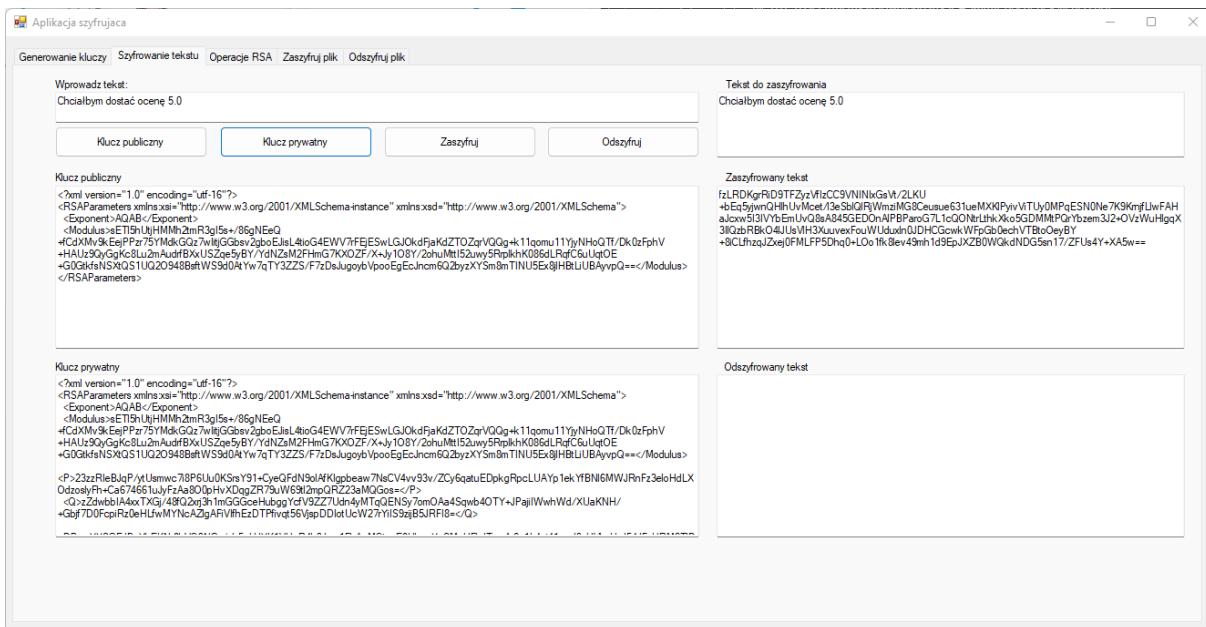
Po wcięnięciu przycisku klucz publiczny wygenerowany zostanie żądany przez nas klucz

Test szyfrowania krótkiego tekstu.



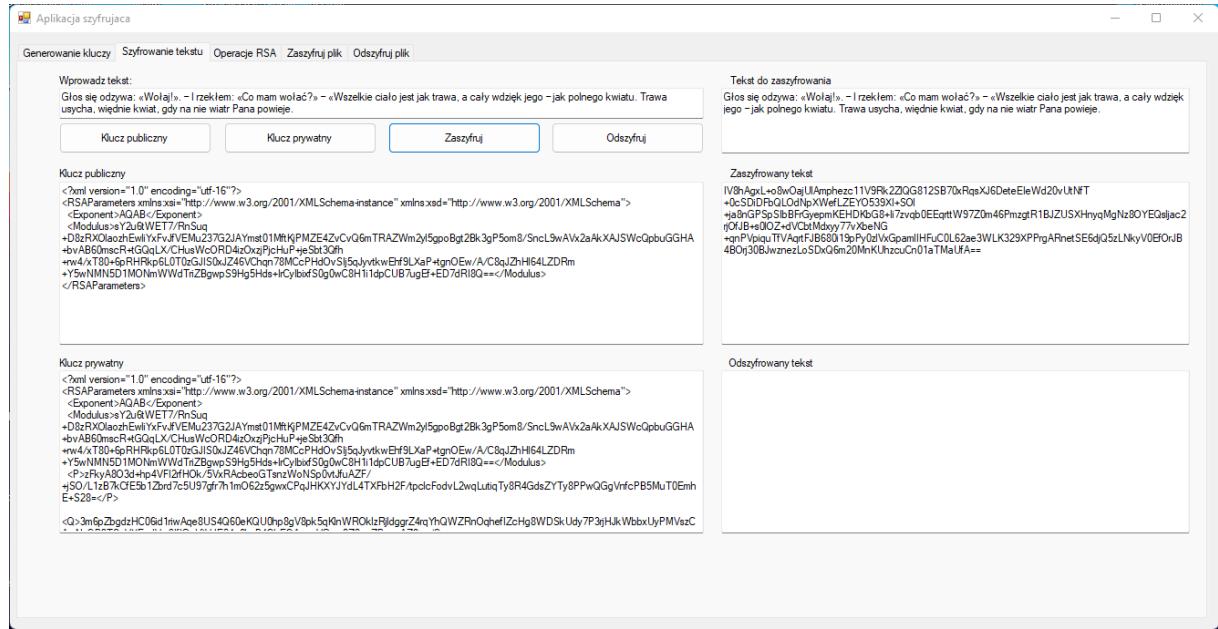
Tekst został zaszyfrowany i pojawił się w polu zaszyfrowany tekst

Test generowania klucza prywatnego.



Klucz został wygenerowany i pojawił się w polu klucz prywatny

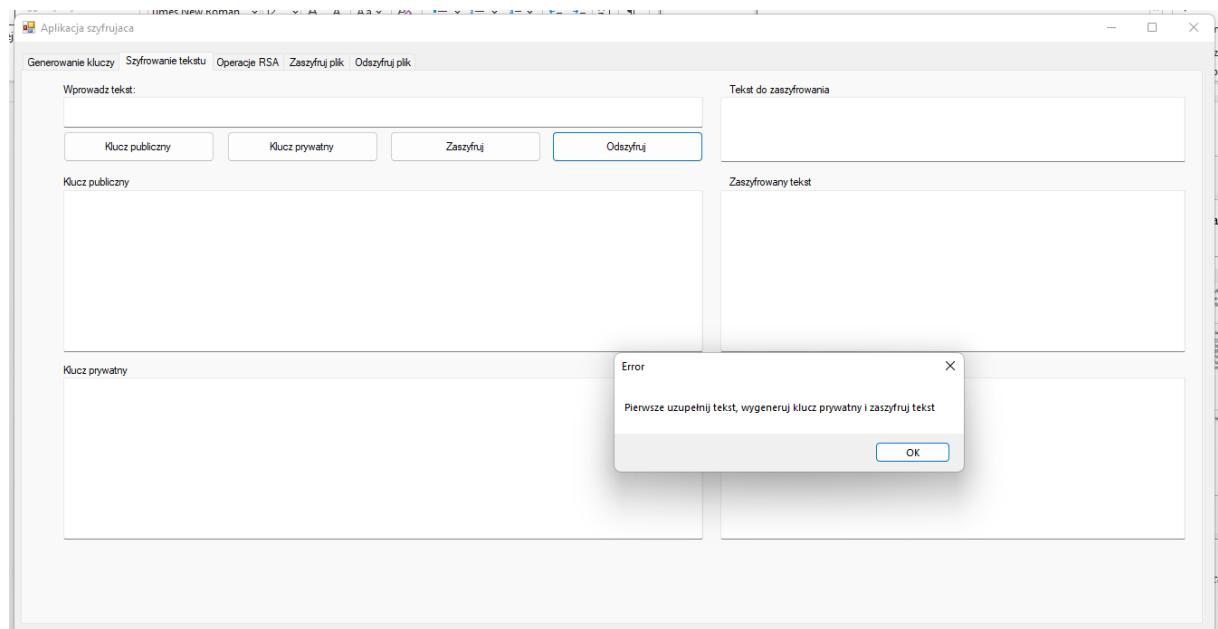
Test szyfrowania dłuższego fragmentu tekstu.



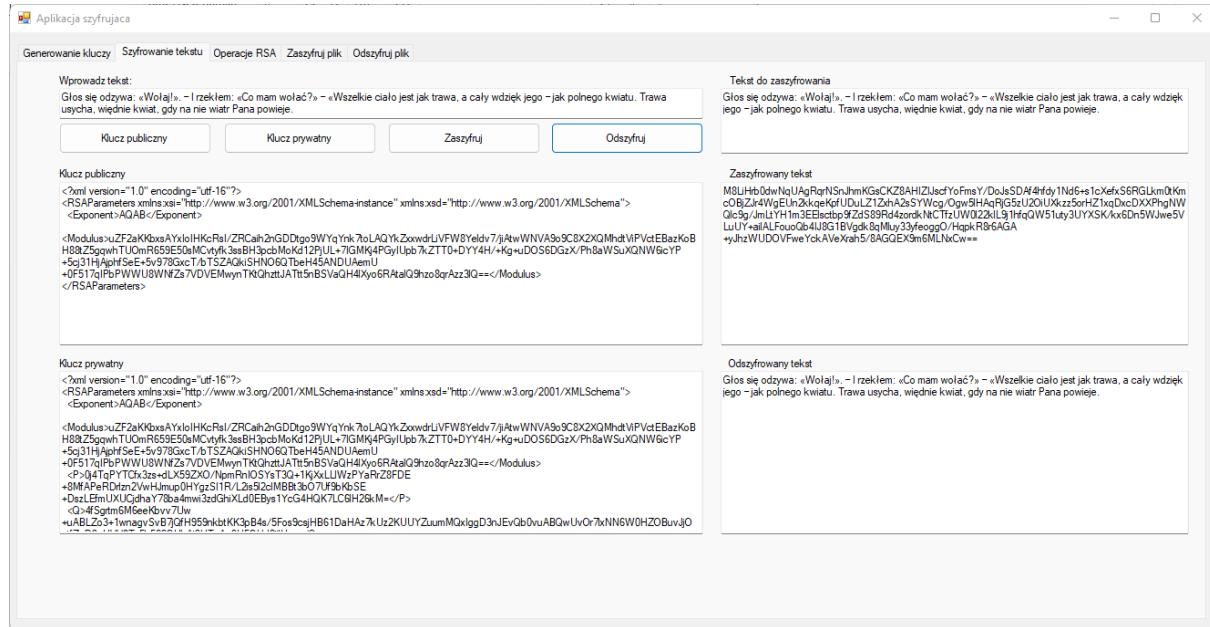
Aplikacja ogranicza maksymalną ilość znaków możliwą do wpisania w polu Tekst do zaszyfrowania do 214 znaków. Szyfrowanie odbywa się poprawnie.

Test deszyfracji tekstu

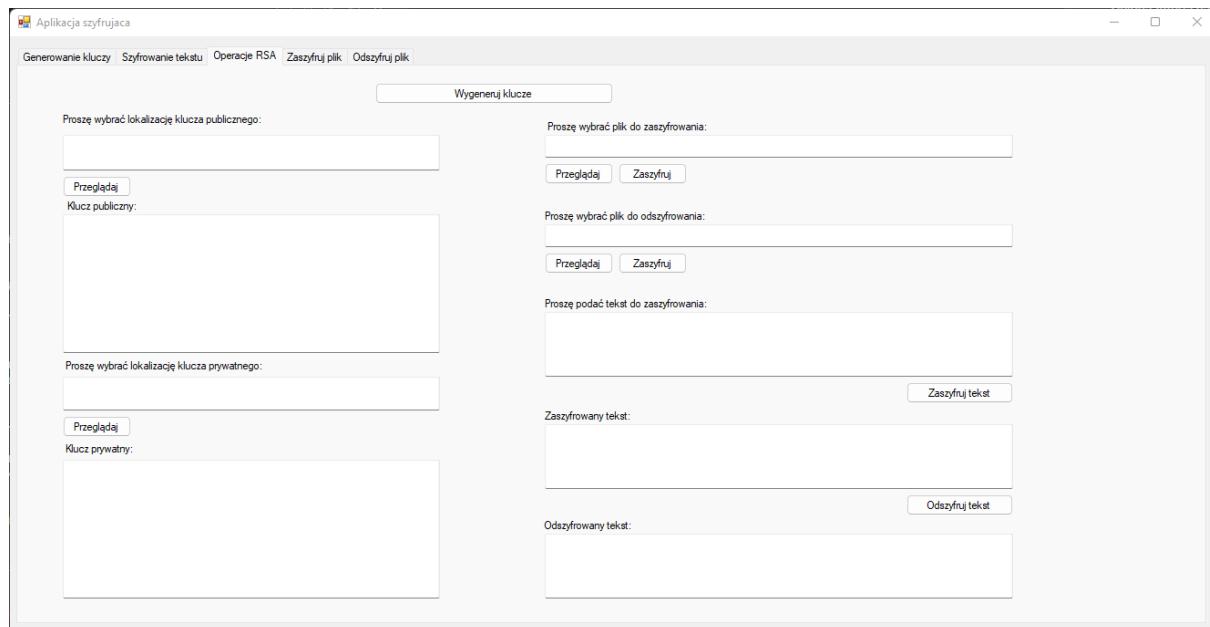
Test deszyfracji przy pustych polach.



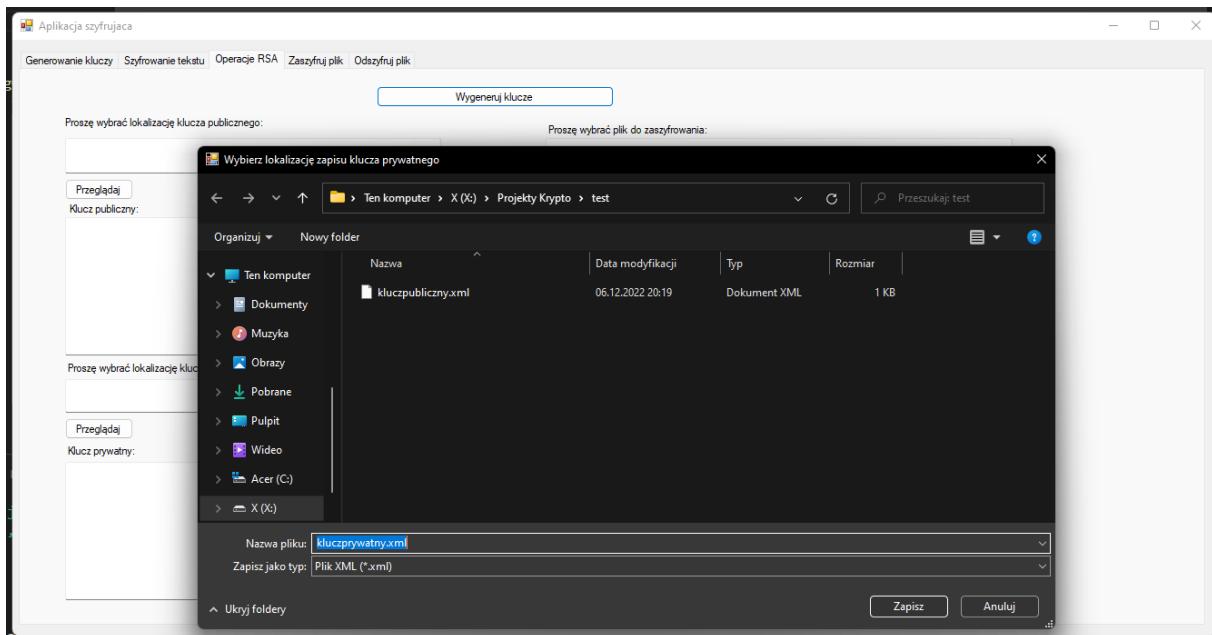
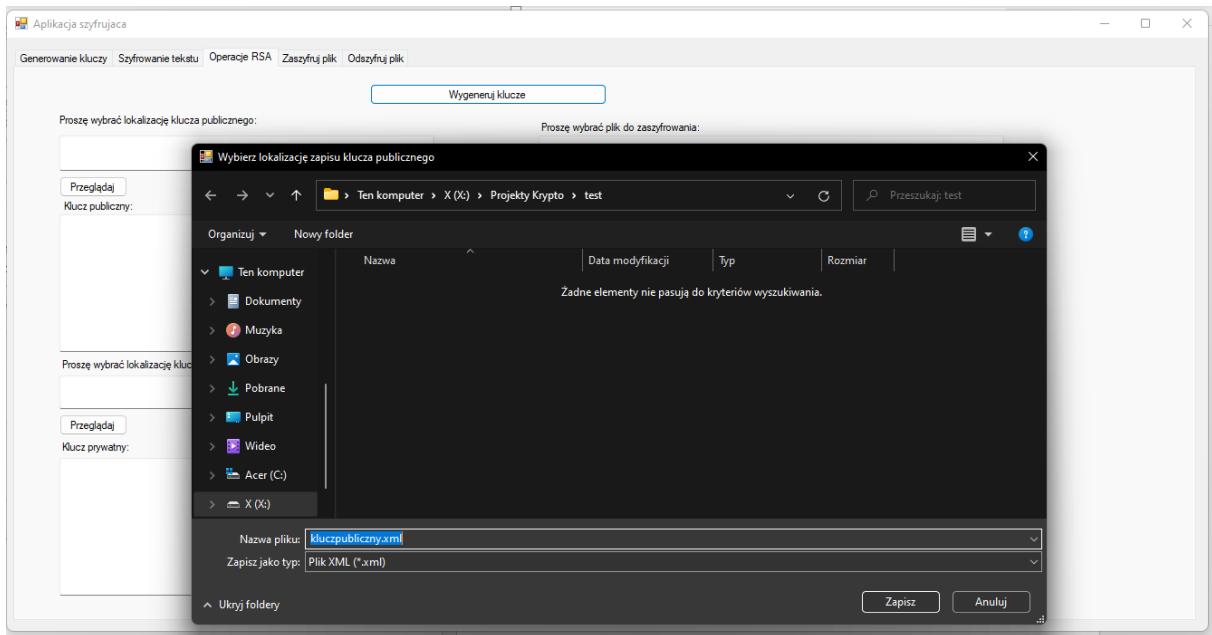
Test deszyfracji tekstu



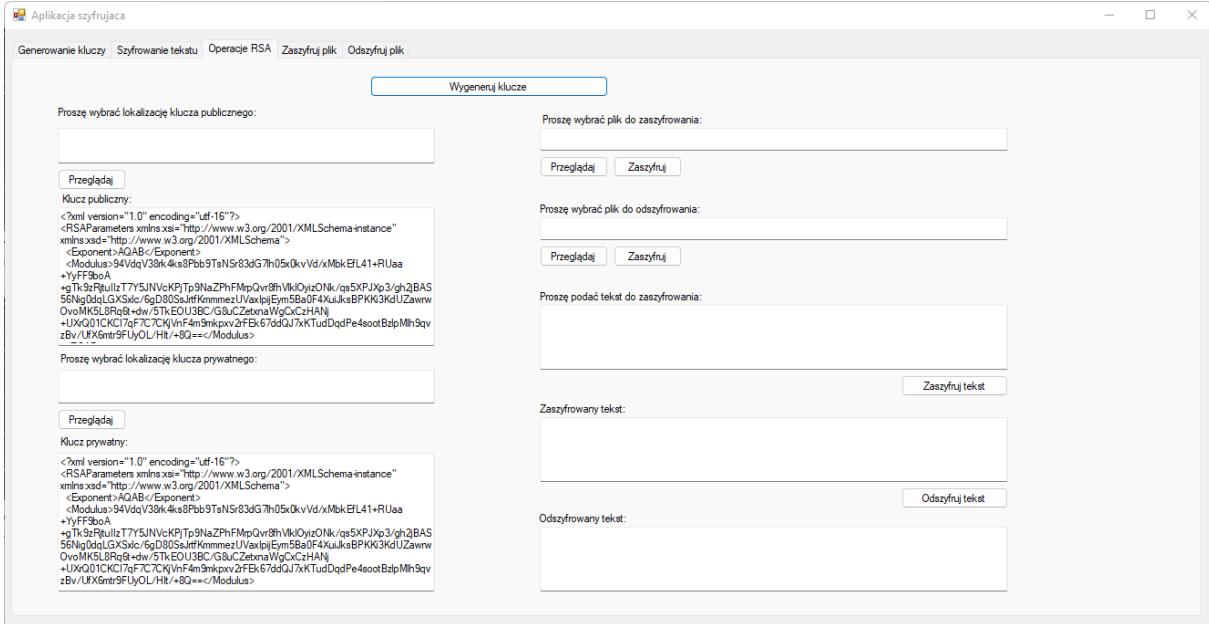
Zakładka trzecia to OPERACJE RSA.



Test generacji kluczy

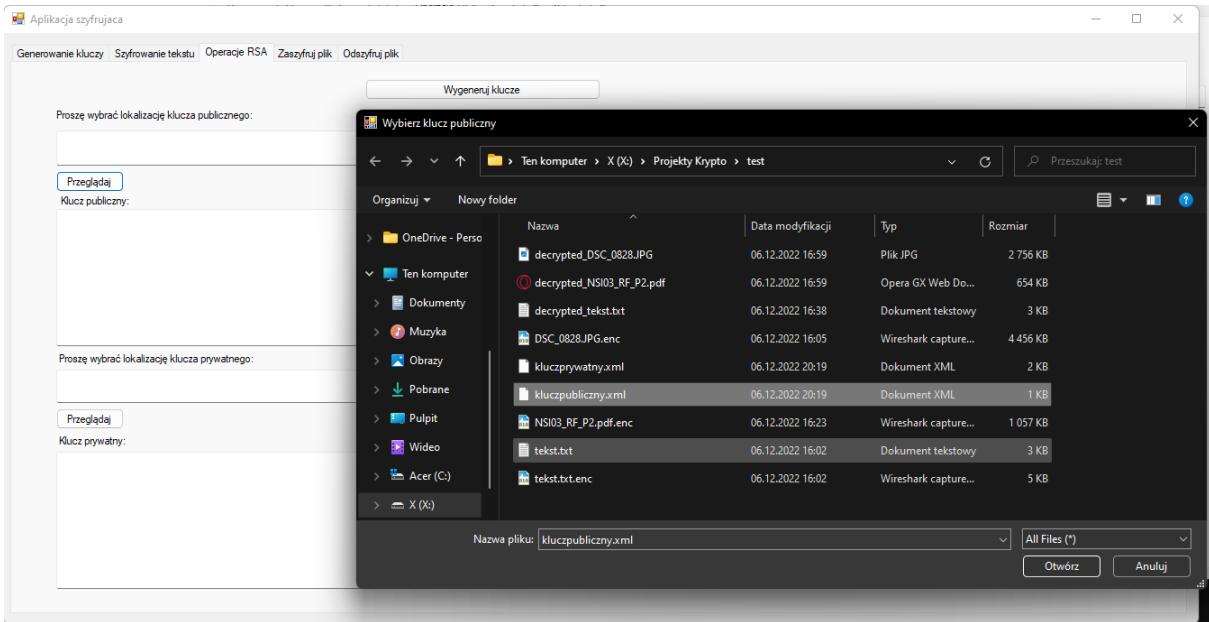


Kliknięcie przycisku wygeneruj klucze powoduje otworzenie okna, w którym wskazujemy lokalizację do zapisu wygenerowanych kluczy w formacie .xml

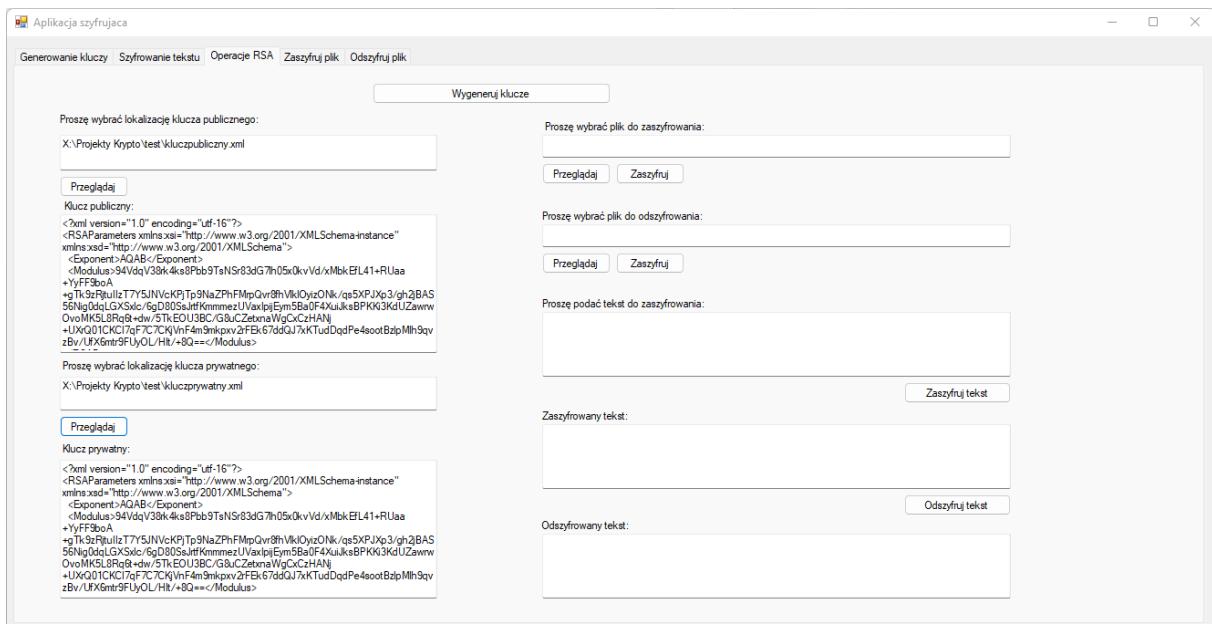


Wygenerowane klucze automatycznie uzupełniają pola klucz publiczny oraz klucz prywatny.

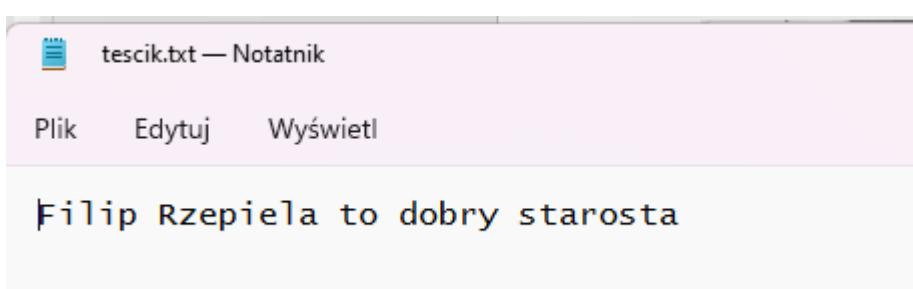
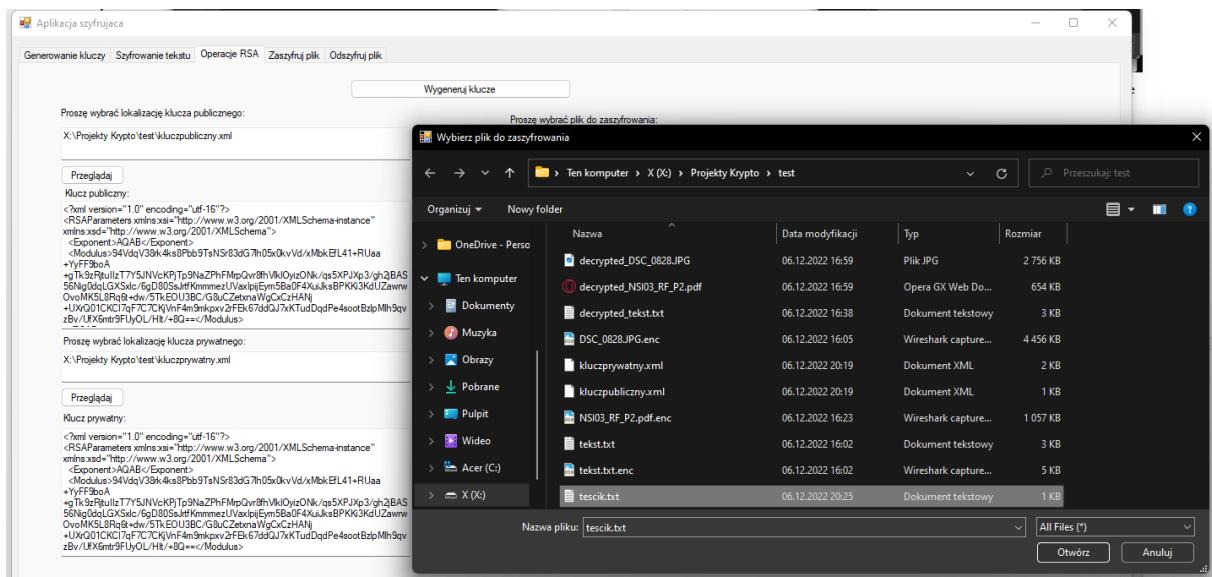
Test pobrania kluczy z pliku.



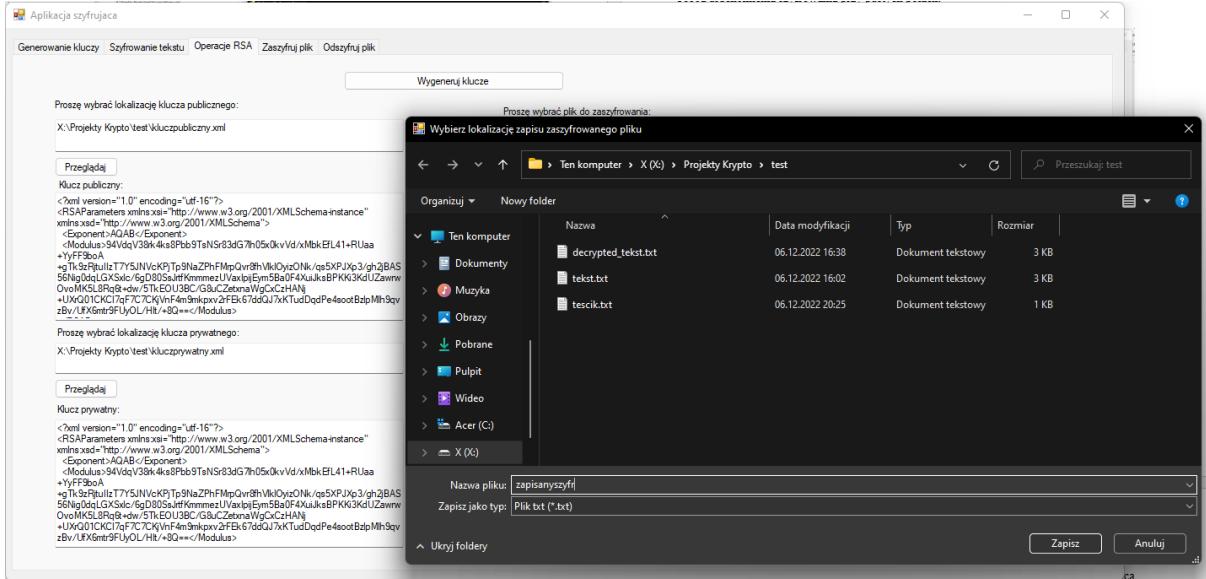
Wybieramy plik klucza publicznego, który pojawia się w polu klucza publicznego. Podobnie w przypadku klucza prywatnego.



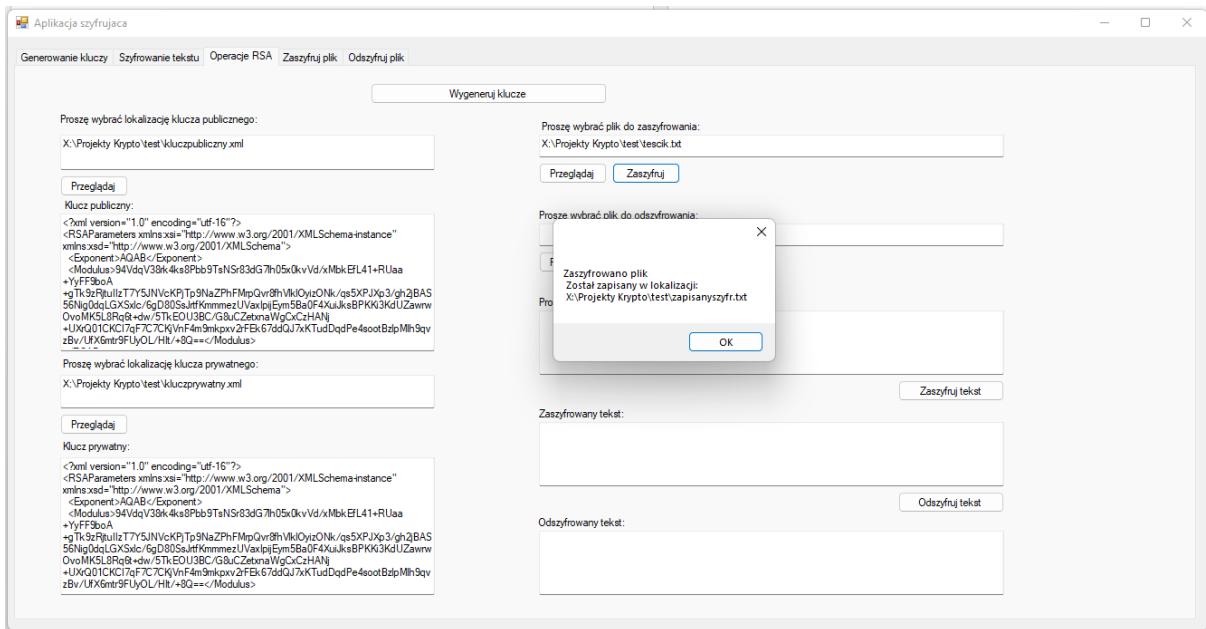
Test zaszyfrowania tekstu z pliku



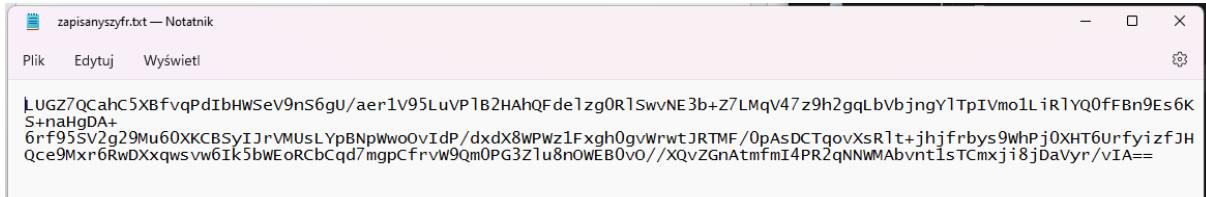
Wybieramy plik i klikamy zaszyfruj.



Po wciśnięciu zaszyfruj otwiera nam się okno w którym zapisujemy zaszyfrowany plik.

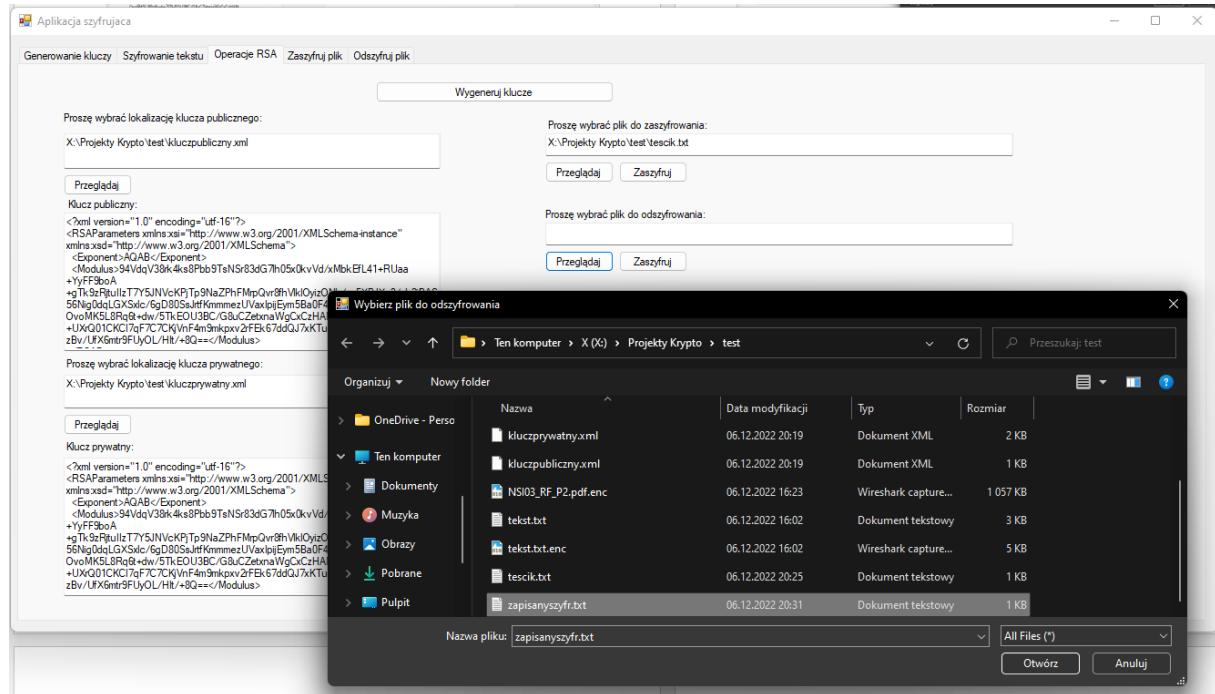


Program zwraca powiadomienie o zapisanym pliku i jego lokalizacji

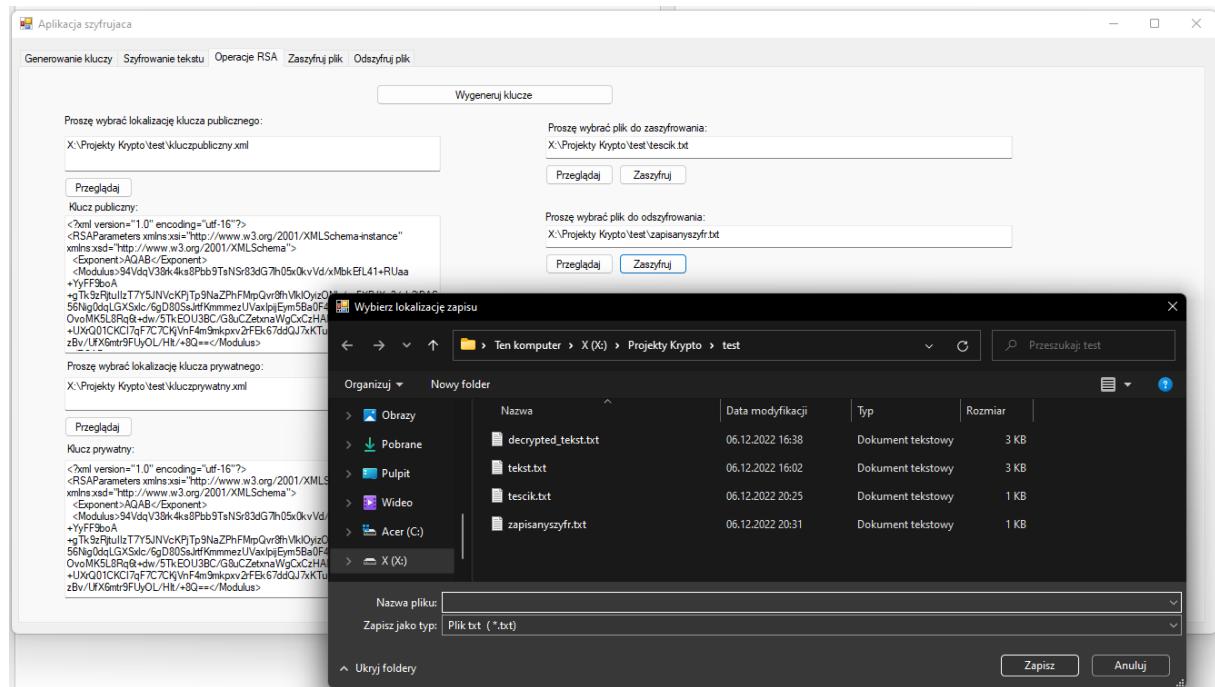


Test odszyfrowywania pliku

Klikamy przeglądaj w celu wskazania pliku do odszyfrowania

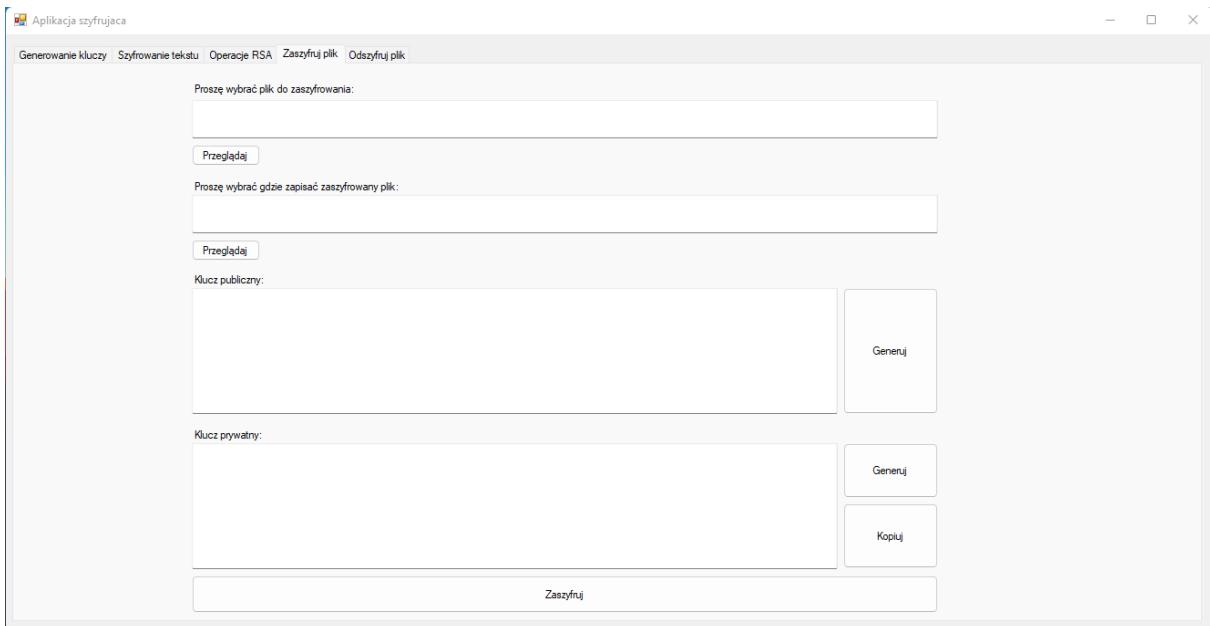


Klikamy odszyfruj (przycisk zaszyfruj zapomniałem poprawić) i wskazujemy lokalizację

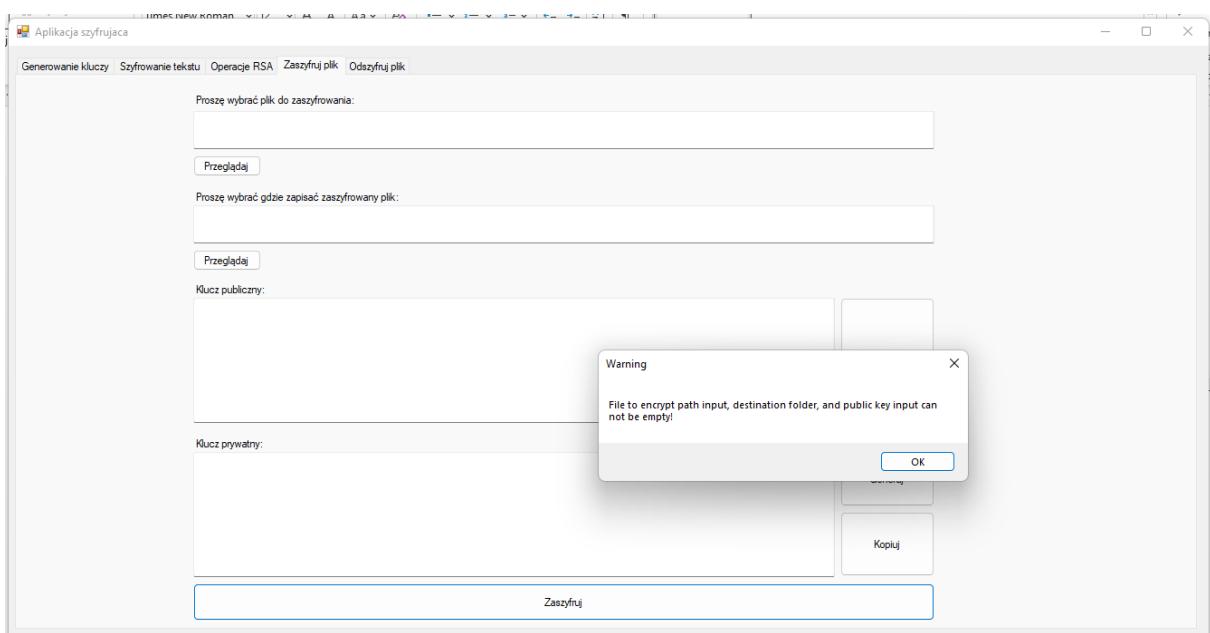


Test szyfrowania plików

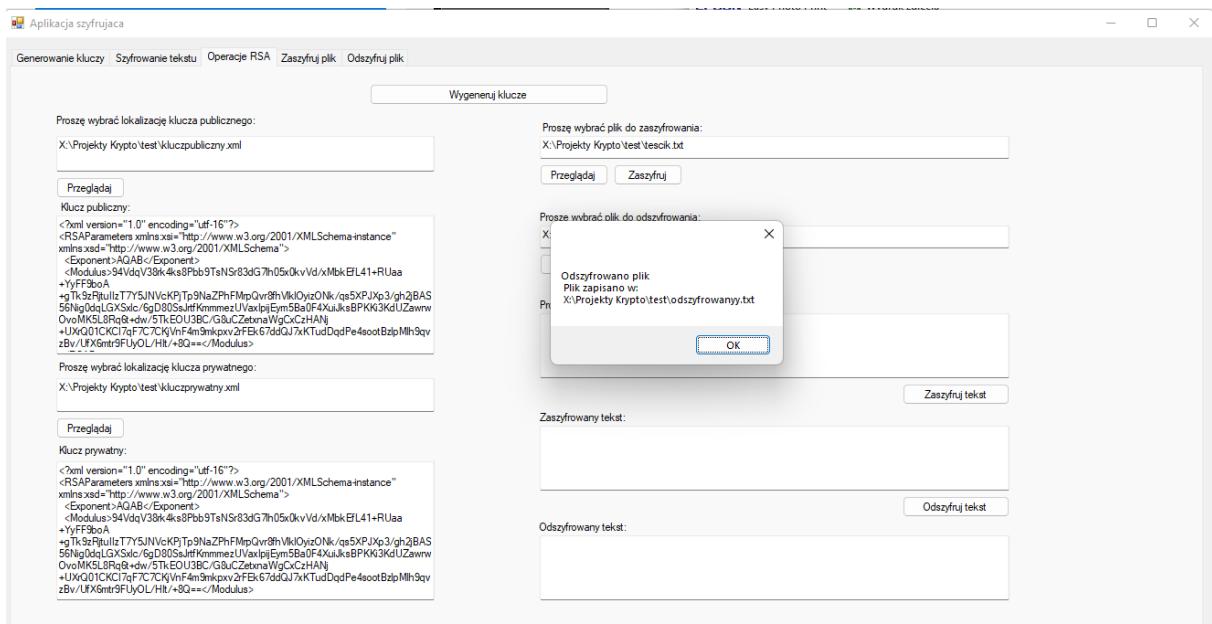
Widok okna szyfrowania plików.



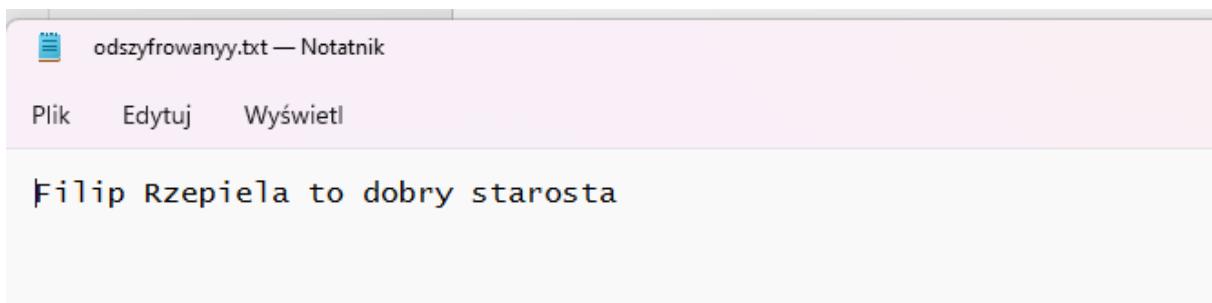
Próba uruchomienia szyfrowania przy pustych polach.



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.

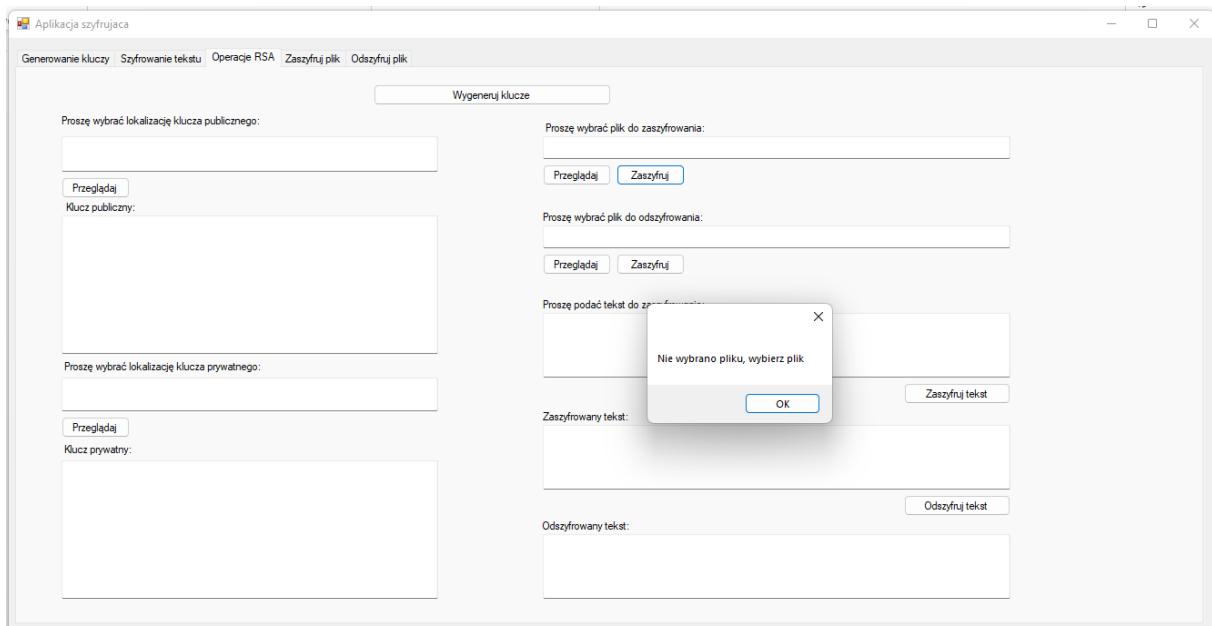


Program informuje nas o odszyfrowaniu oraz lokalizacji

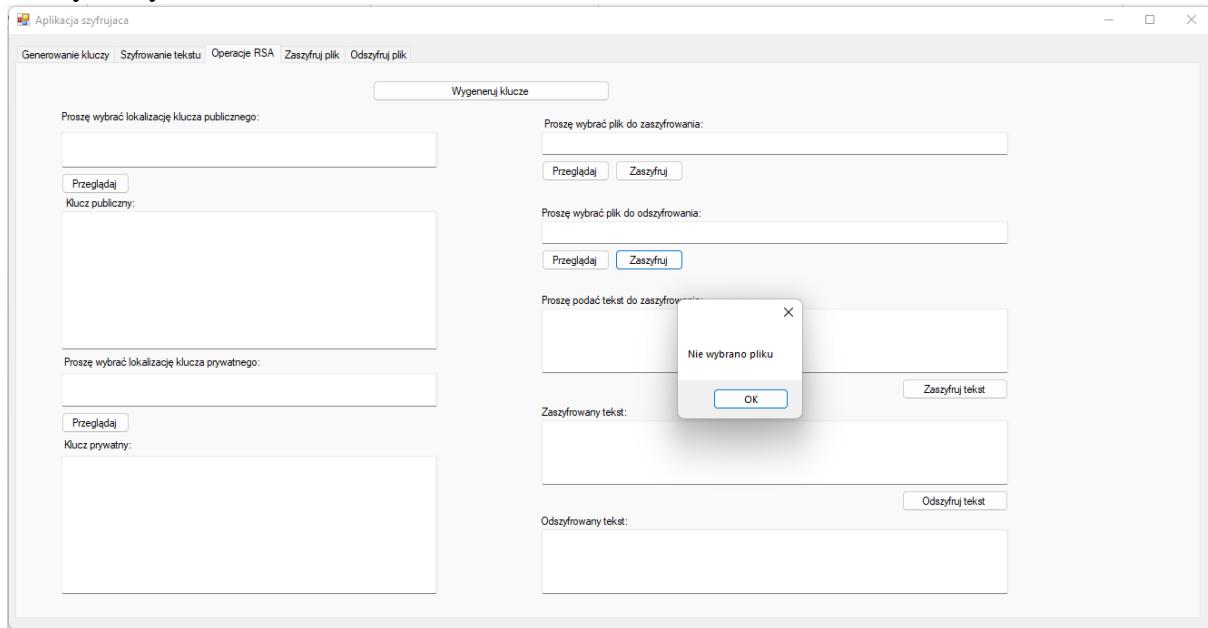


W przypadku niewprowadzenia bądź wygenerowania kluczy zwrócony zostanie komunikat

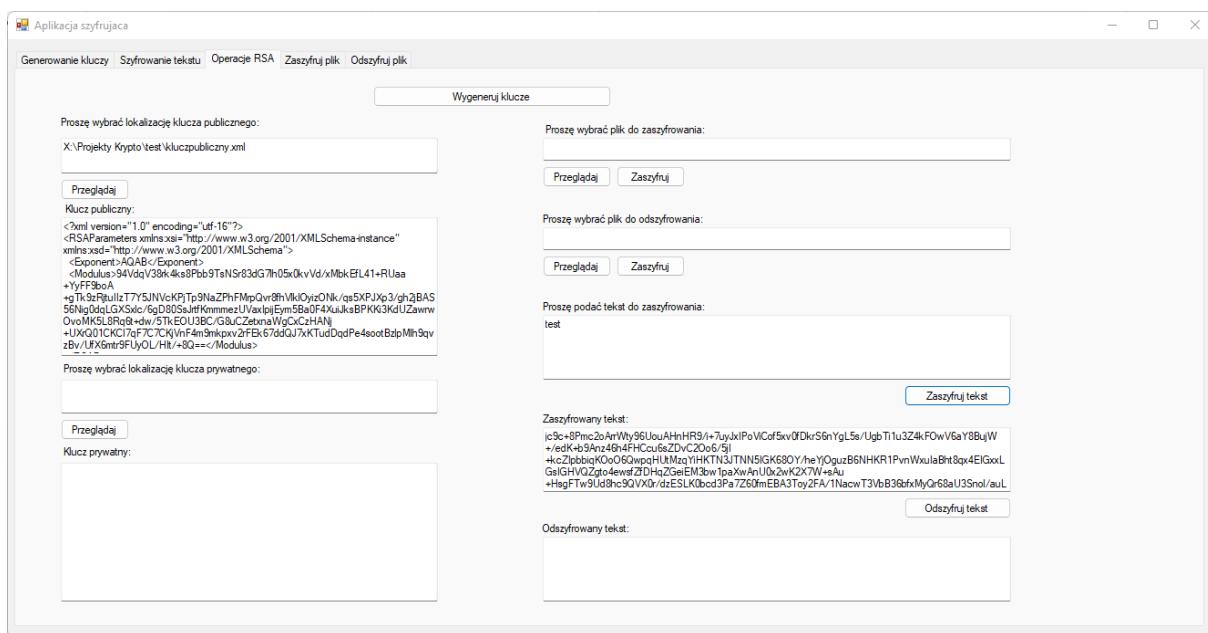
Szyfrowanie:



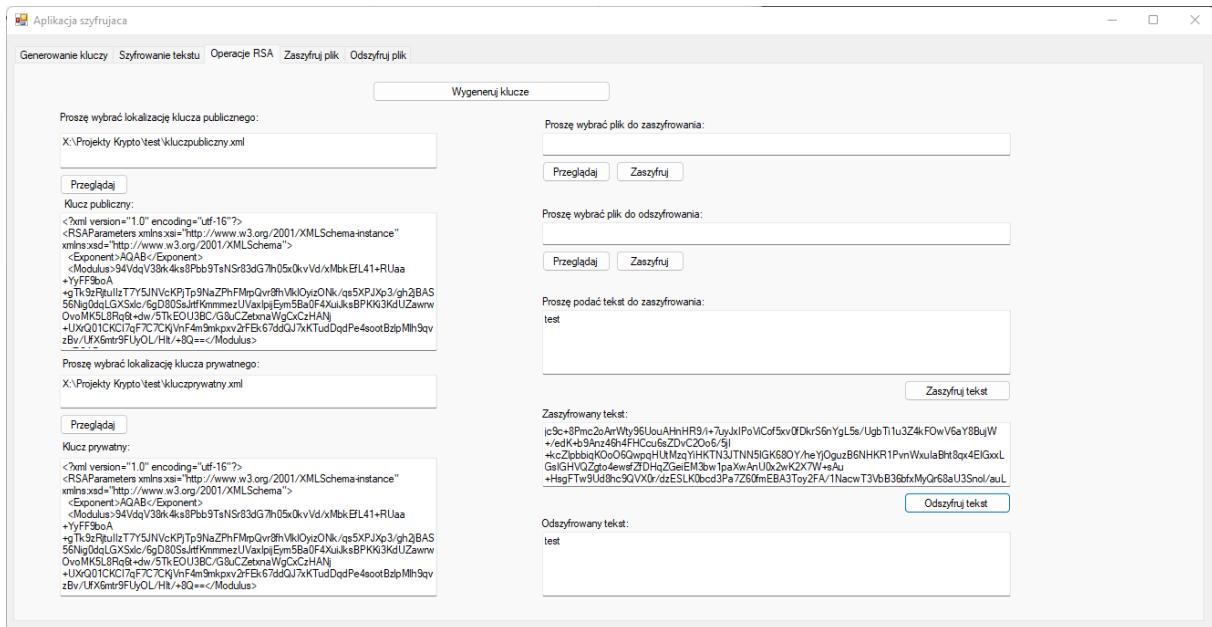
Odszyfrowywanie:



Test szyfrowania pliku

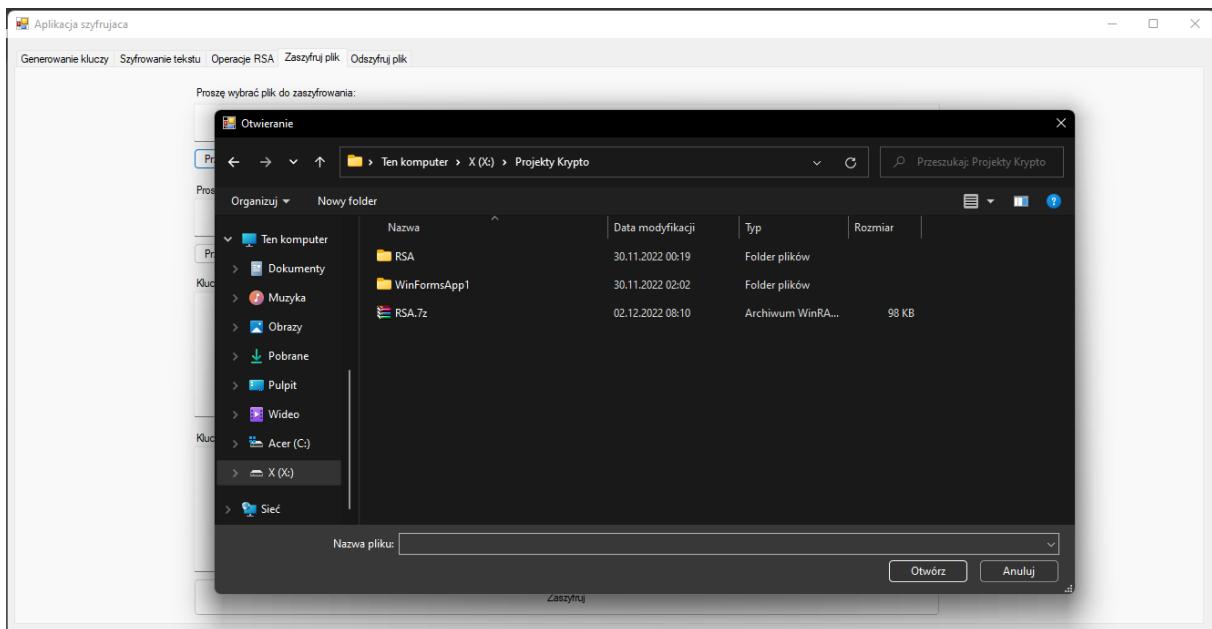


Aby zaszyfrować plik musimy mieć klucz publiczny.

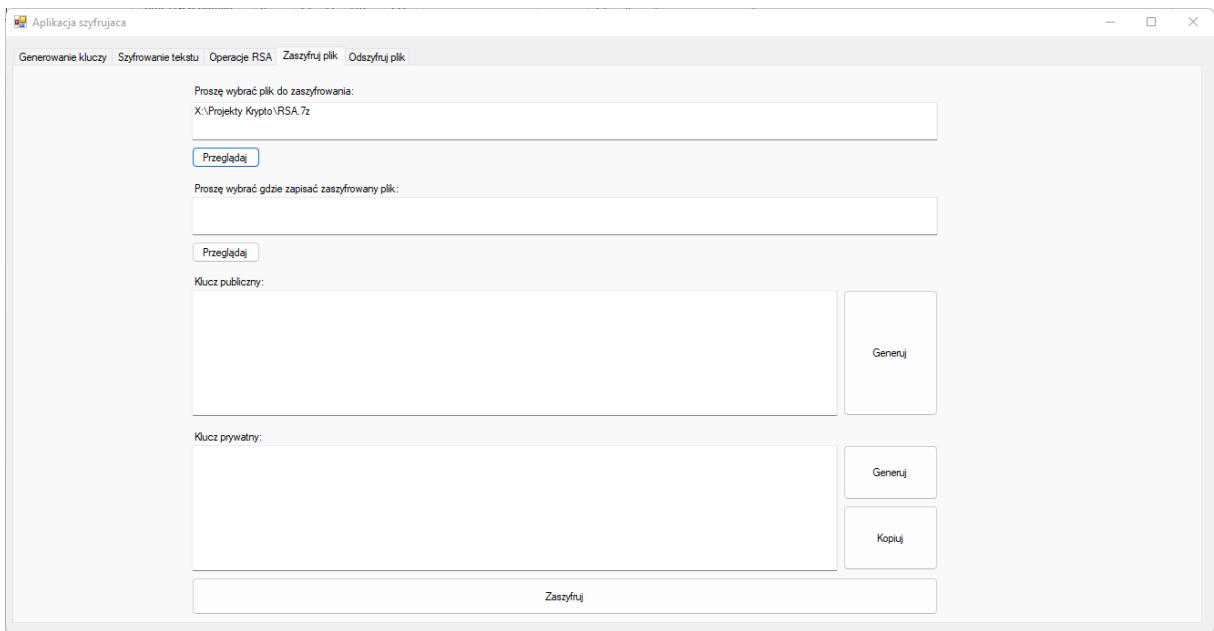


W przypadku odszyfrowania potrzebujemy również klucza prywatnego

Test pola wskazania pliku do zaszyfrowania

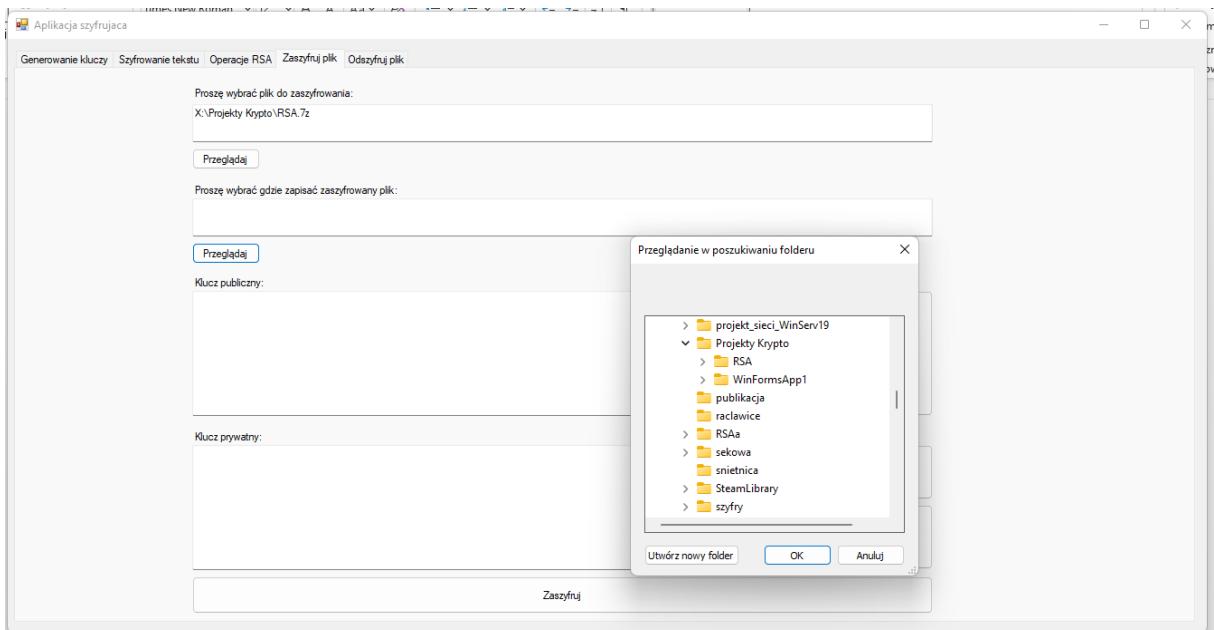


Po wybraniu pliku do zaszyfrowania jego ścieżka pojawia się w polu

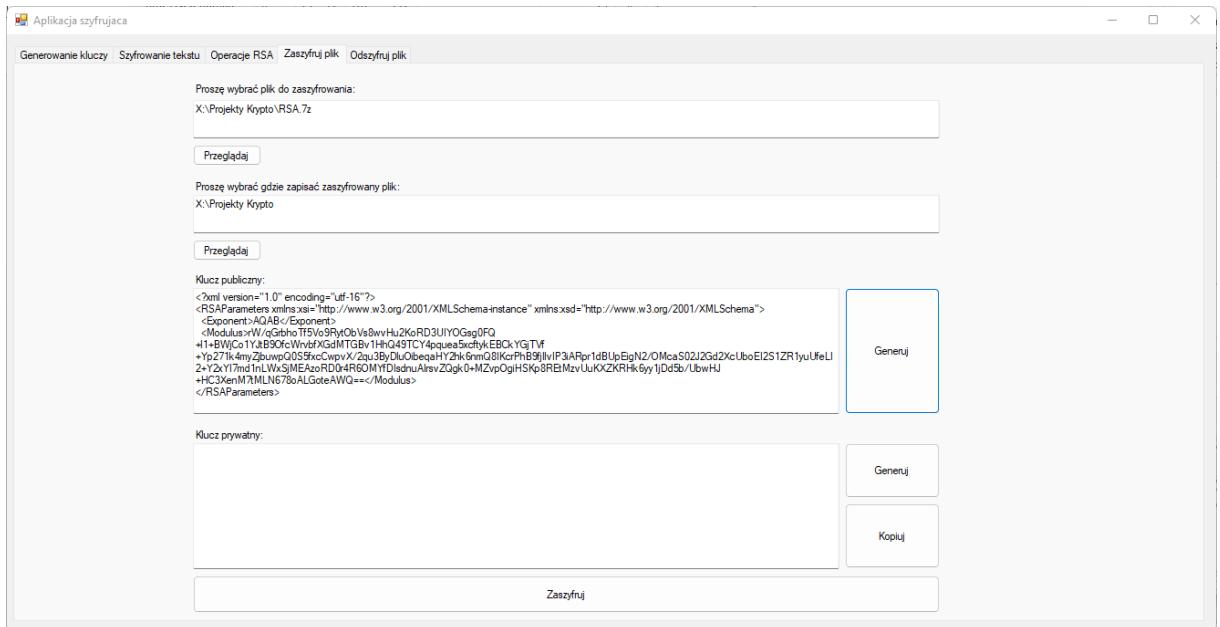


Test wybrania lokalizacji dla zaszyfrowanego pliku

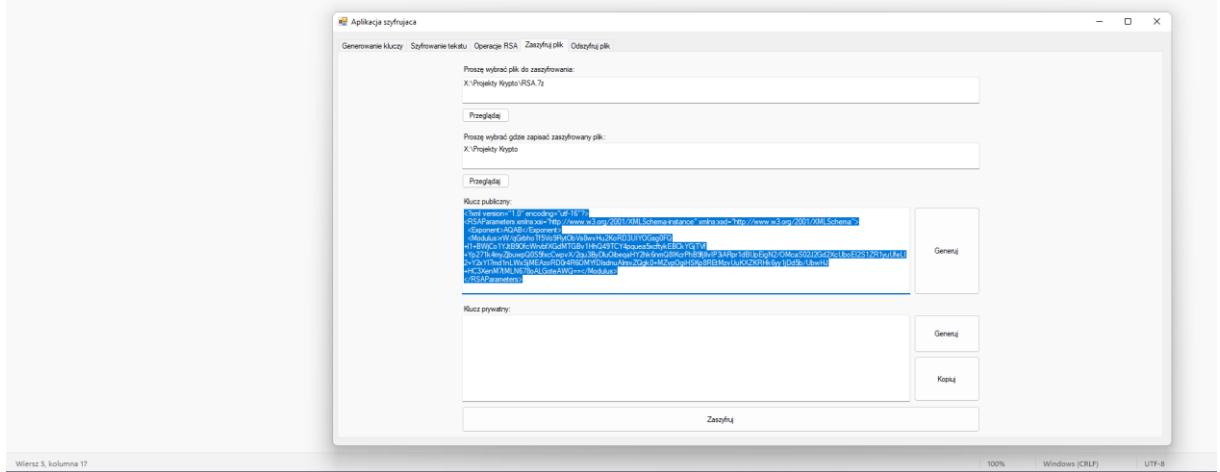
Sytuacja jest podobna jak w przypadku pola wskazującego plik do zaszyfrowania. Za pomocą przycisku znajdującego się obok pola uruchamiane jest okno wyboru folderu.



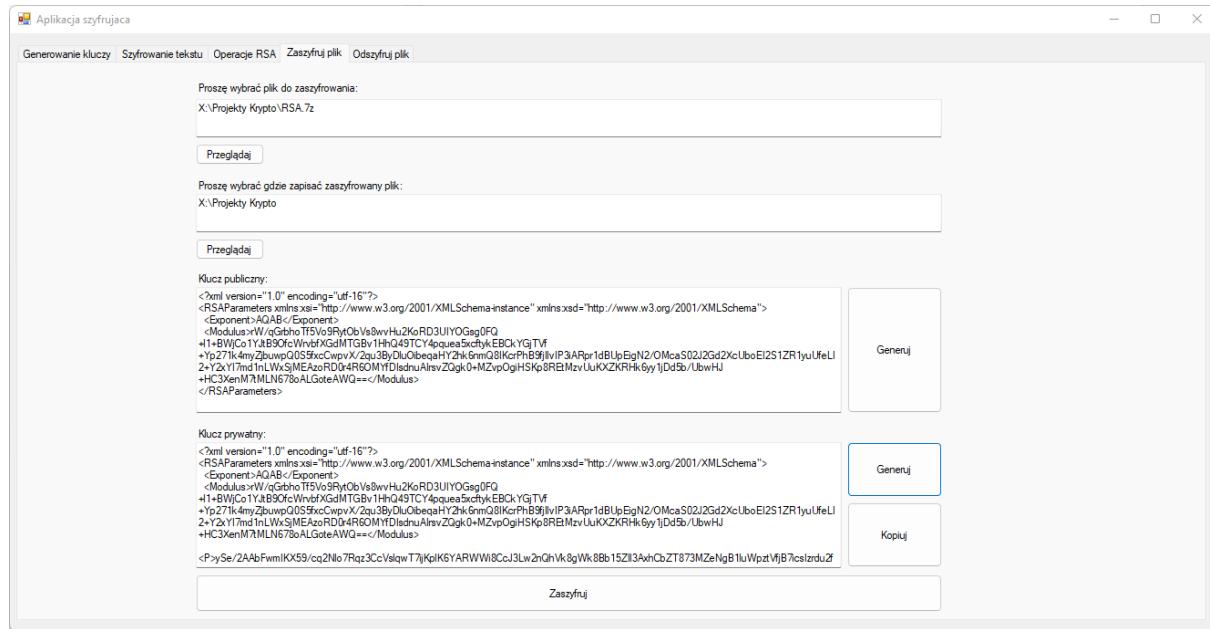
Test generowania klucza publicznego



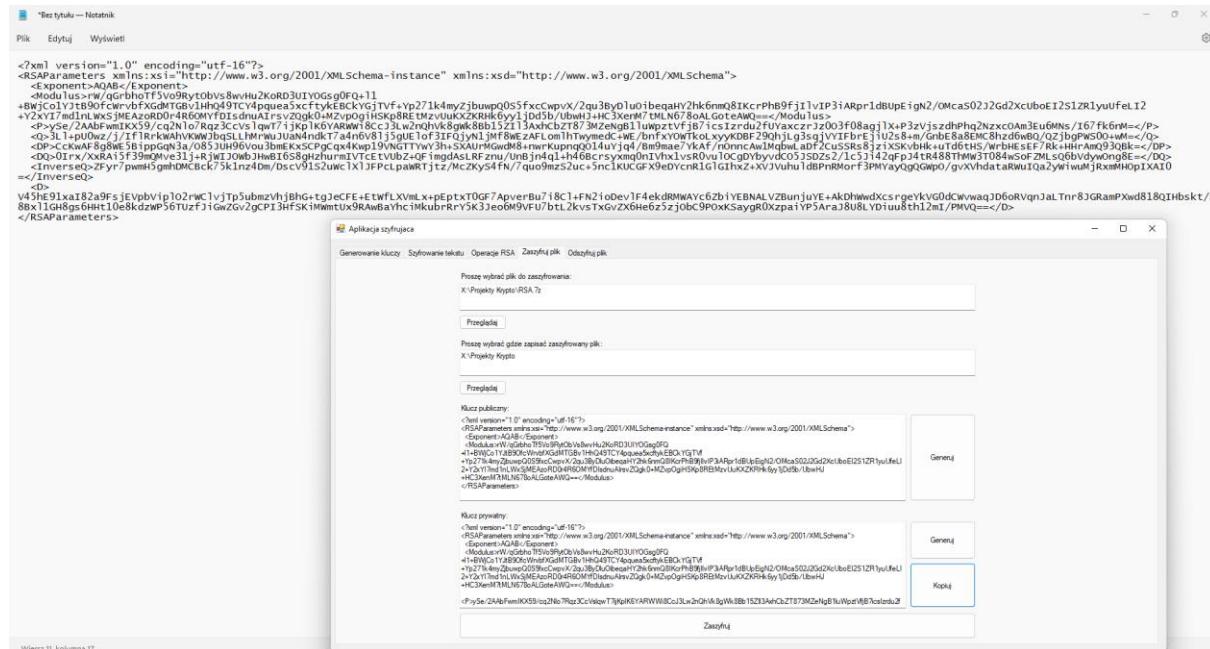
Oczywiście wygenerowany klucz, możemy zaznaczyć w całości za pomocą ctrl+a, skopiować i wkleić do np. notatnika



Test generowania klucza prywatnego.

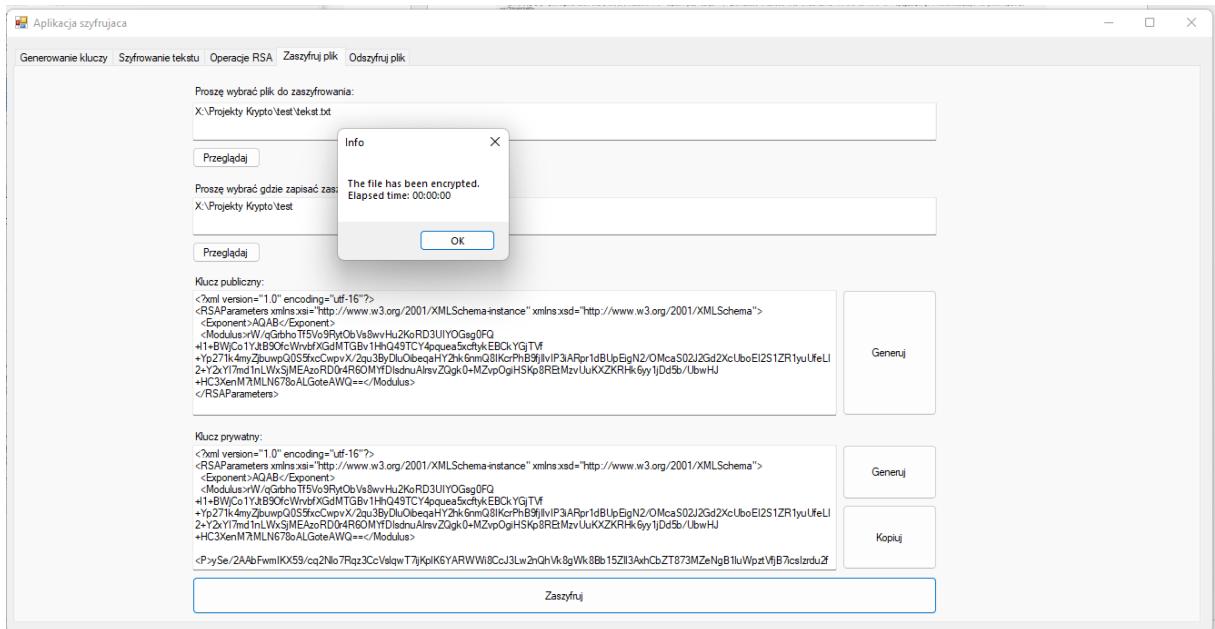


Możemy go skopiować za pomocą przycisku kopij bądź jak wyżej 😊

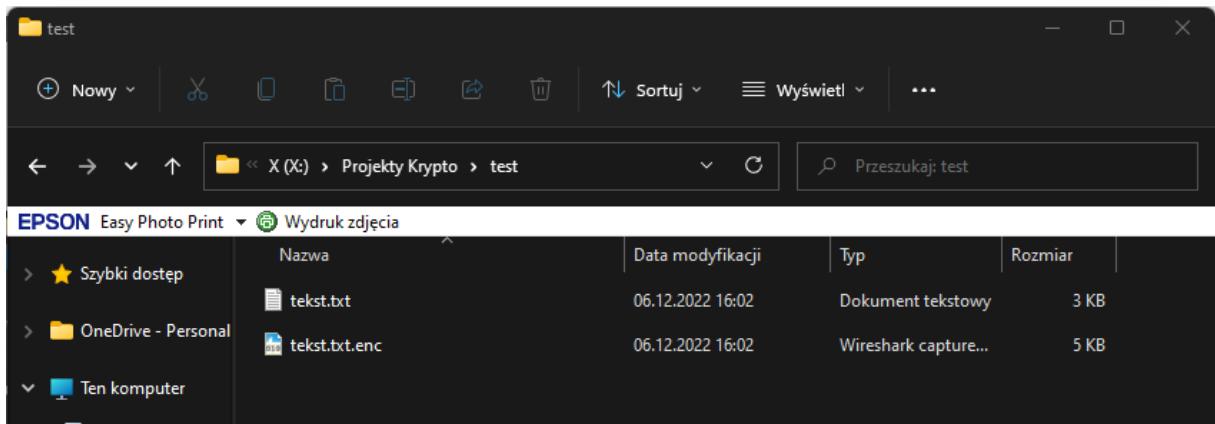


Wiersz 11, kolumna 17

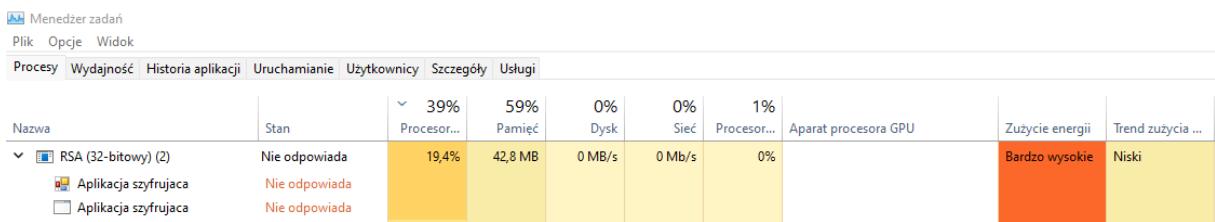
Test szyfrowania pliku tekstowego

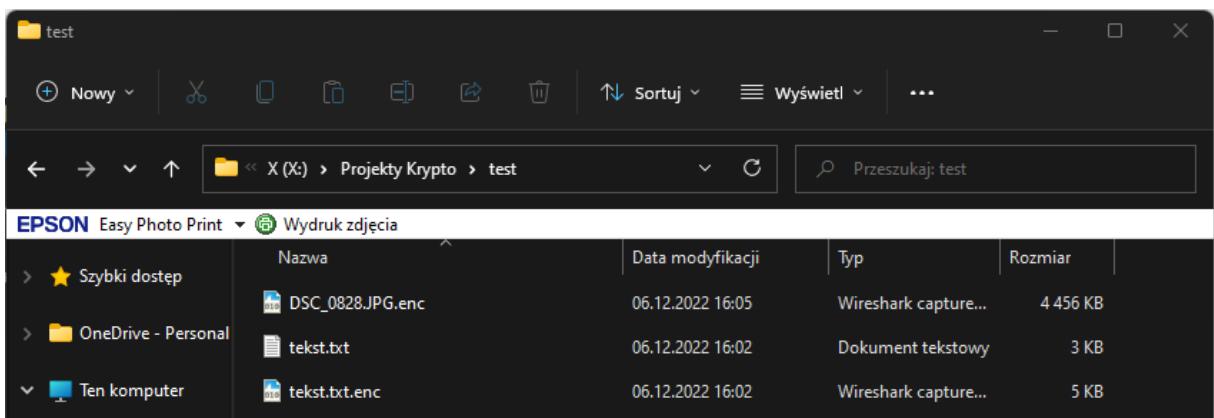
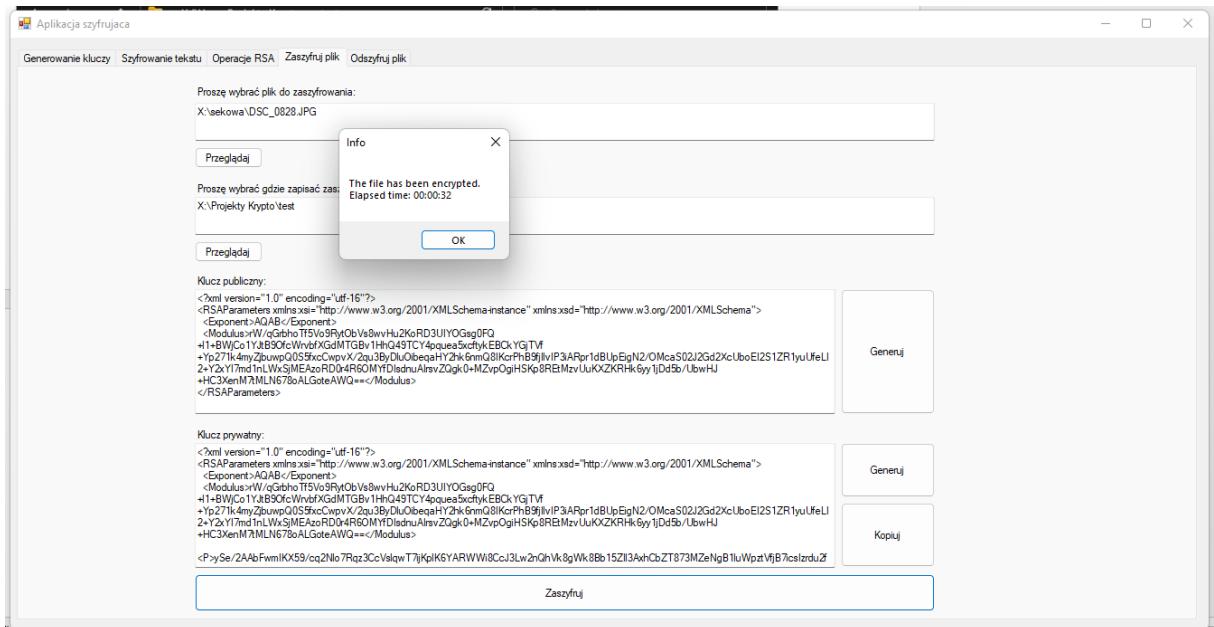


W folderze pojawił się zaszyfrowany plik

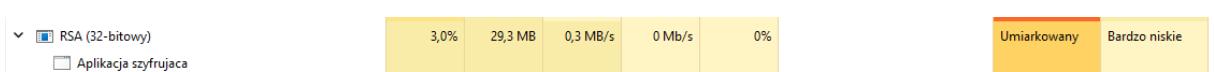
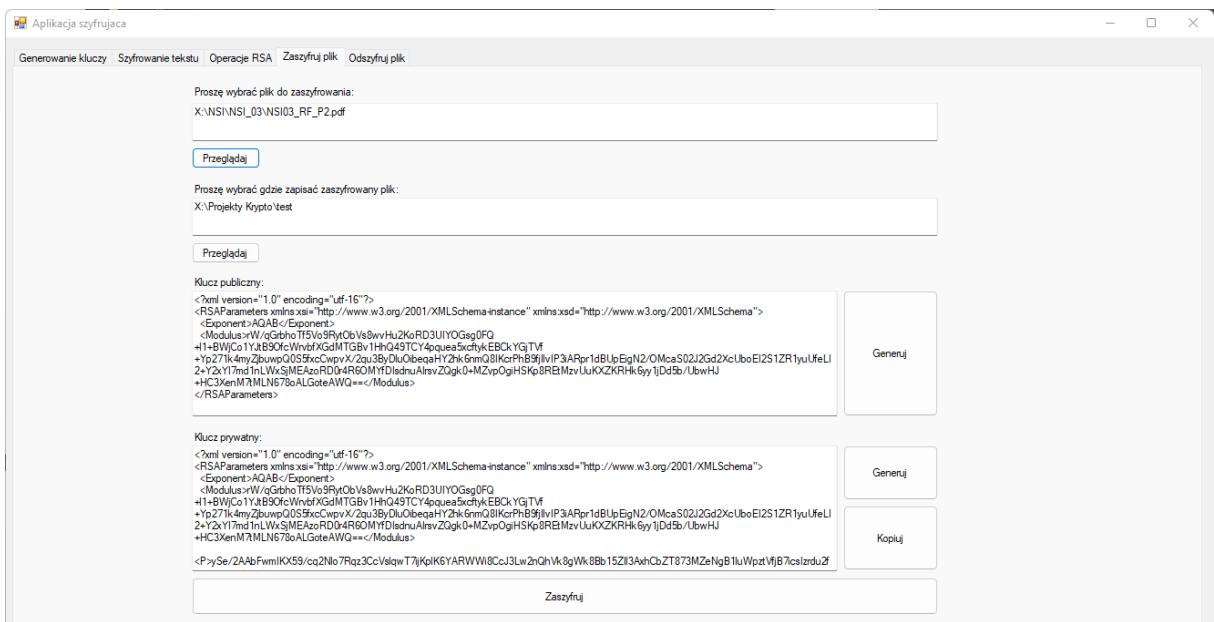


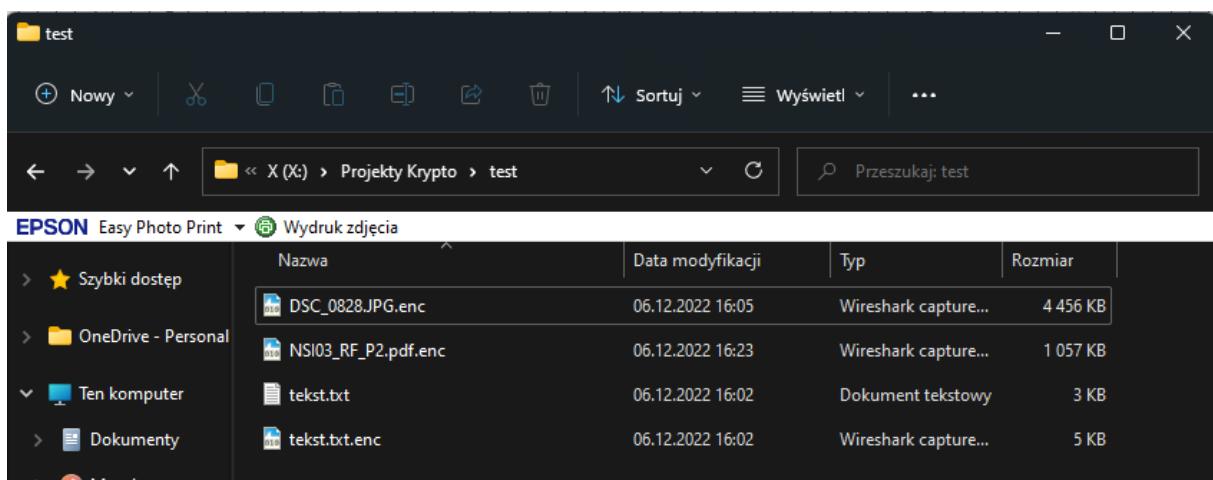
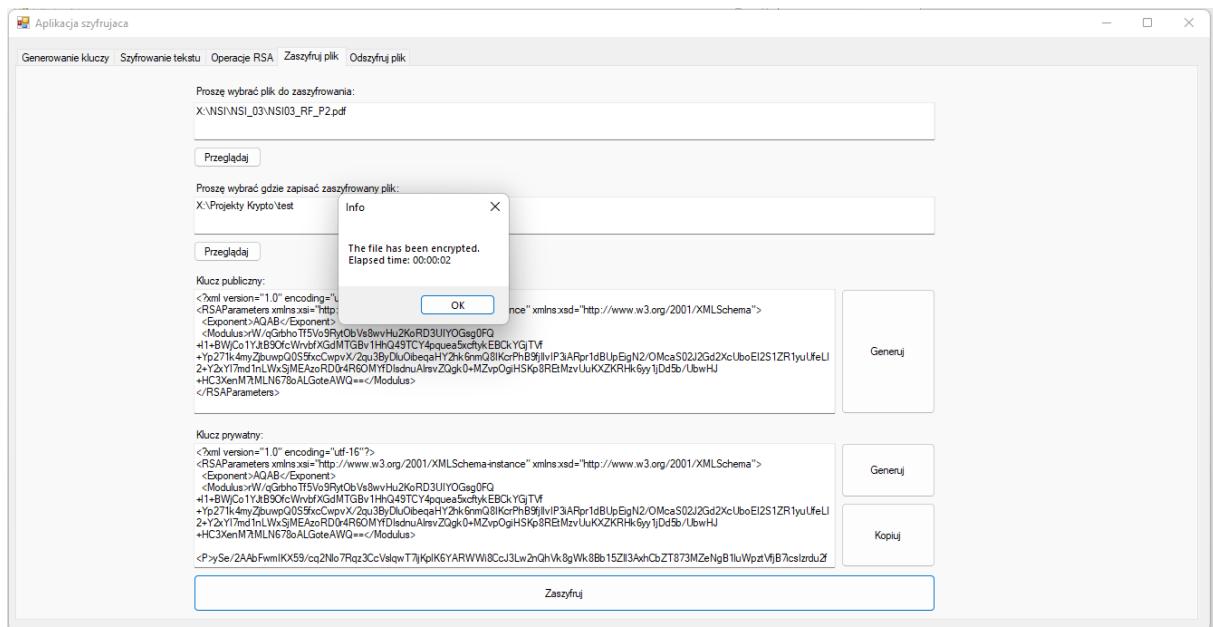
Test szyfrowania pliku .jpg



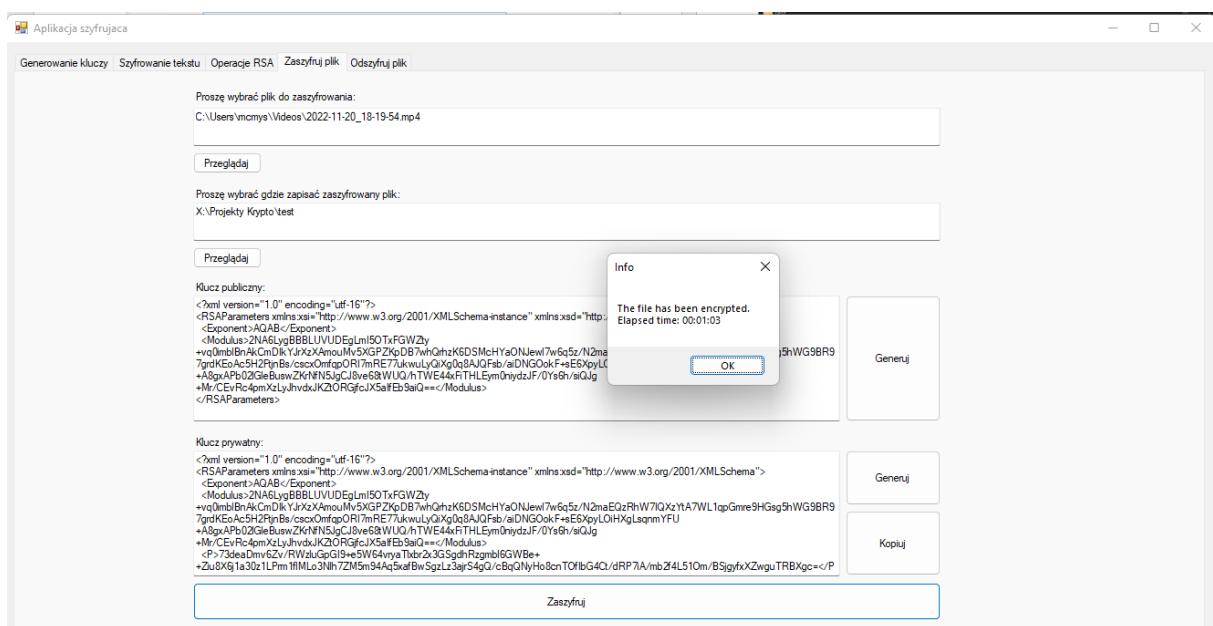


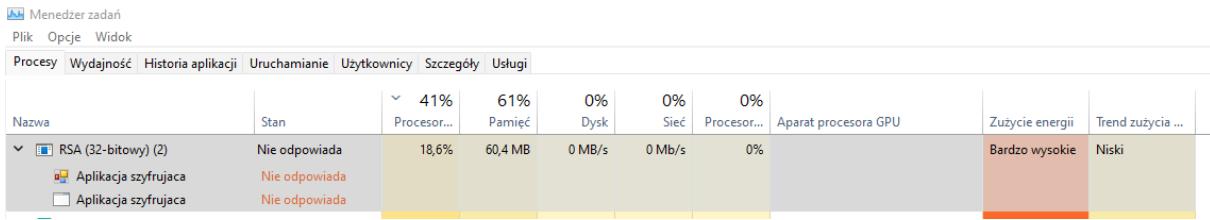
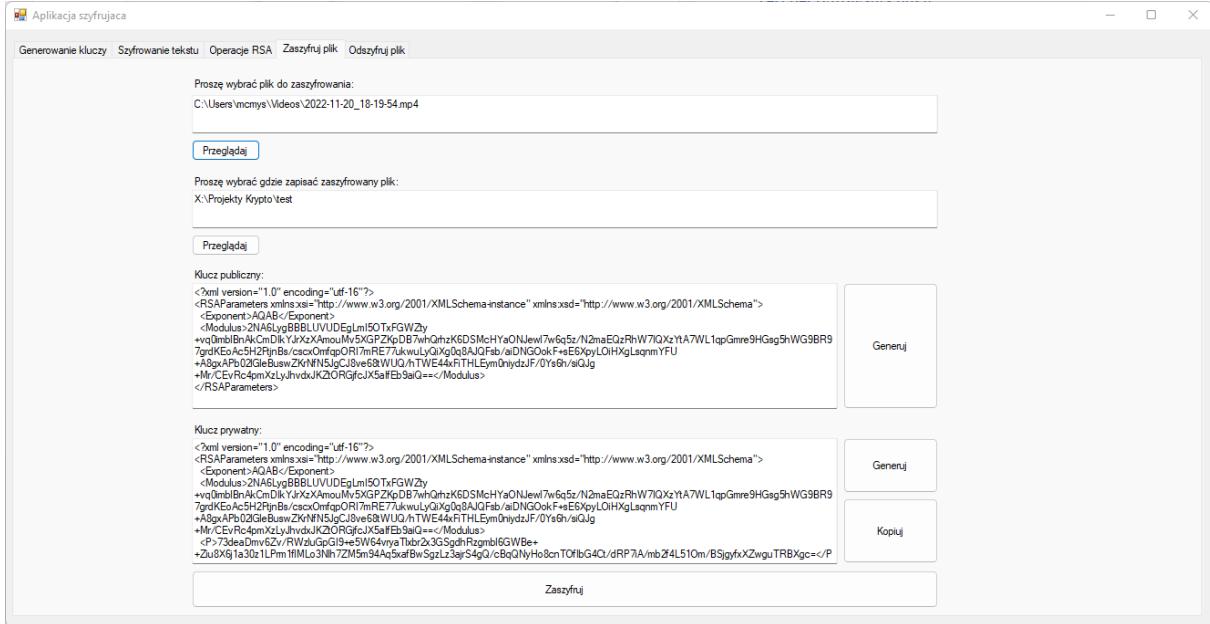
Test szyfrowania pliku .pdf





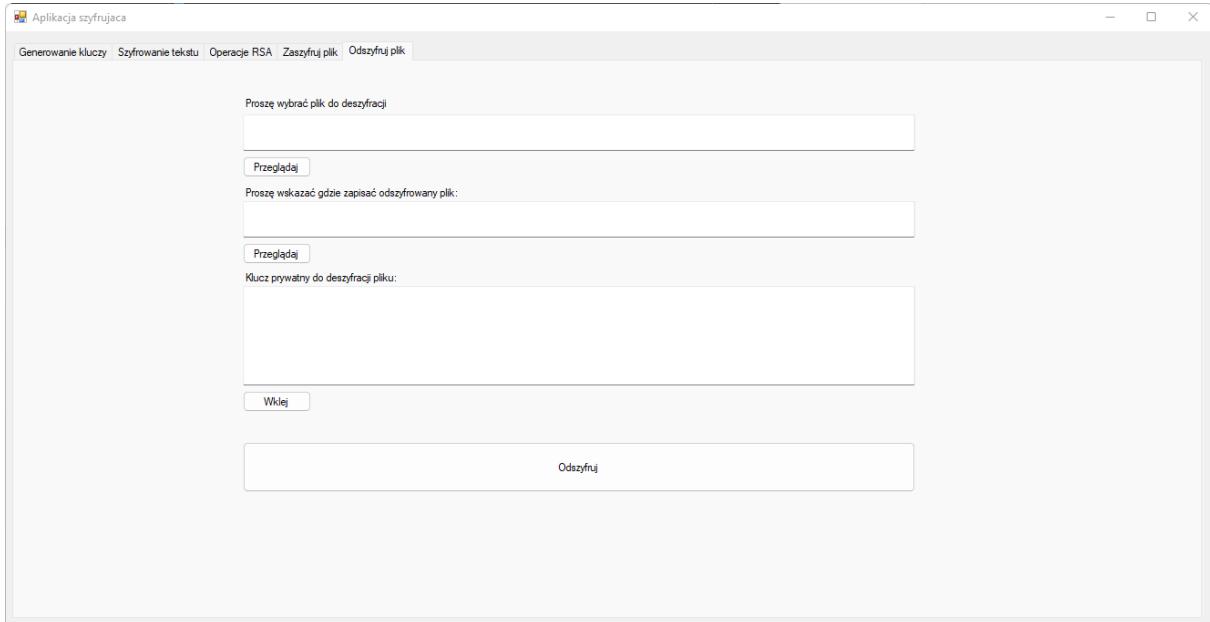
Test zaszyfrowania pliku wideo



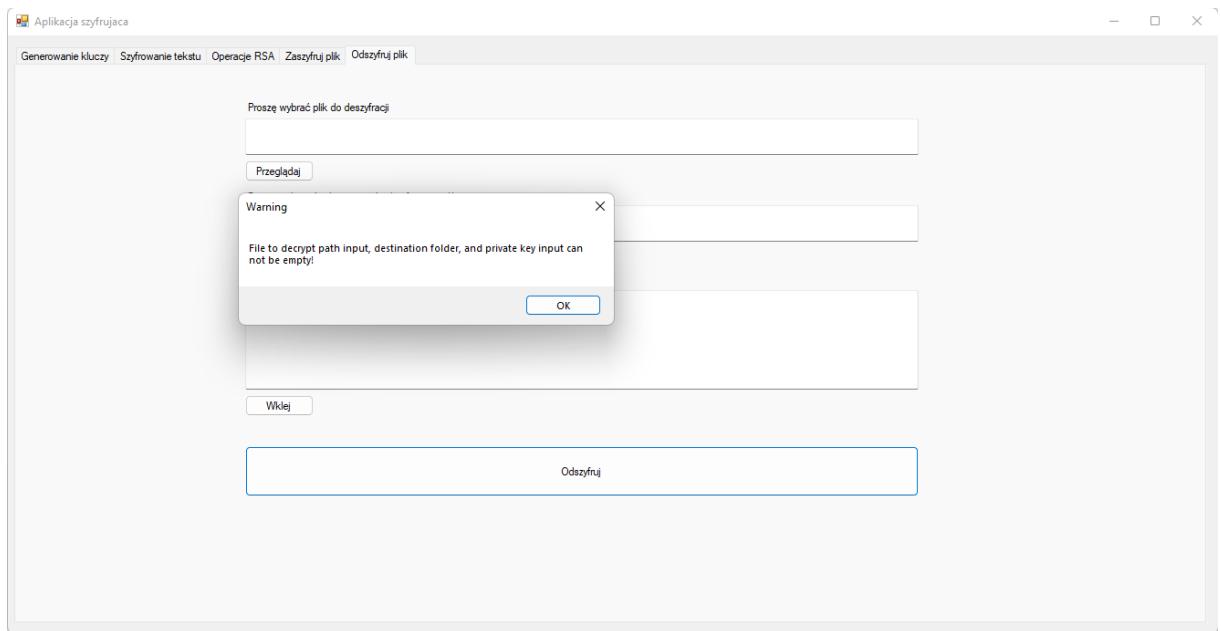


Test deszyfrowania pliku

Widok okna deszyfrowania pliku

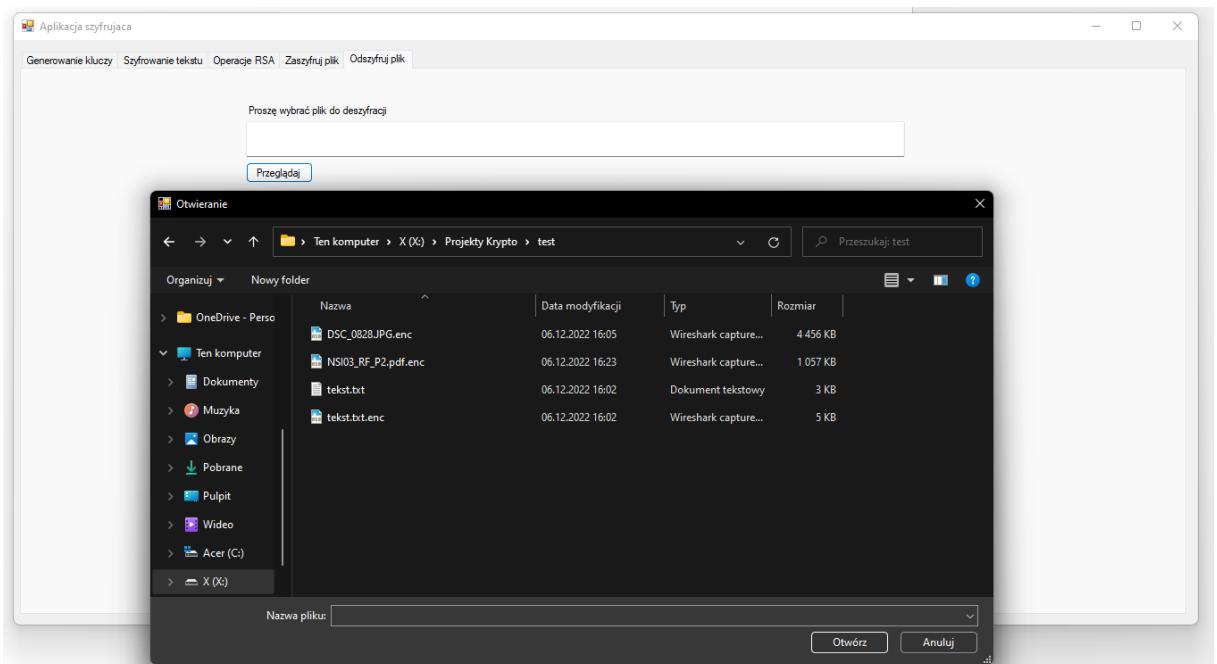


Test uruchomienia deszyfrowania przy pustych polach

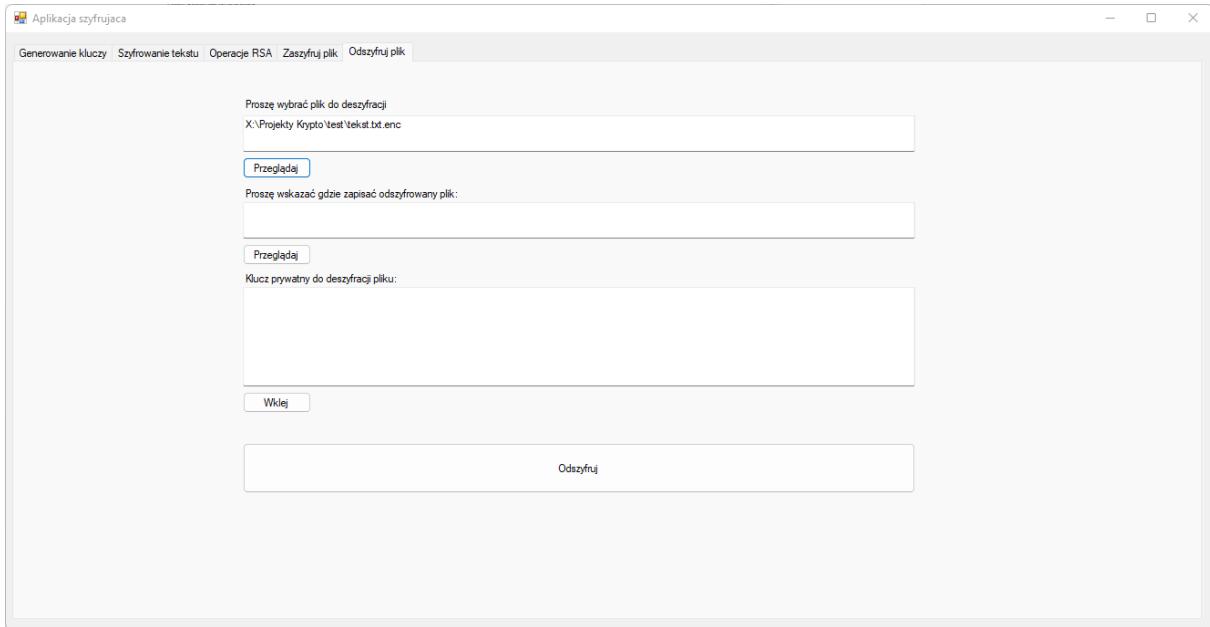


Aplikacja wyświetla komunikat, że pola nie mogą być puste. Komunikat wyświetlany jest zarówno, gdy jedno lub więcej z pól jest puste.

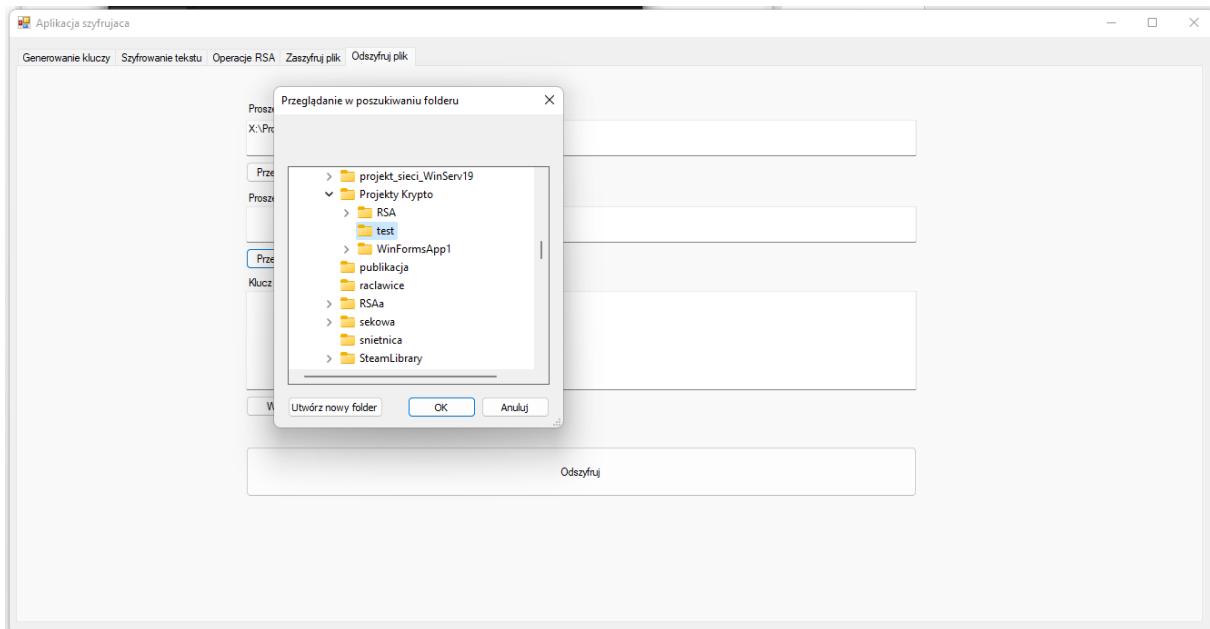
Test pola wskazania pliku do deszyfracji



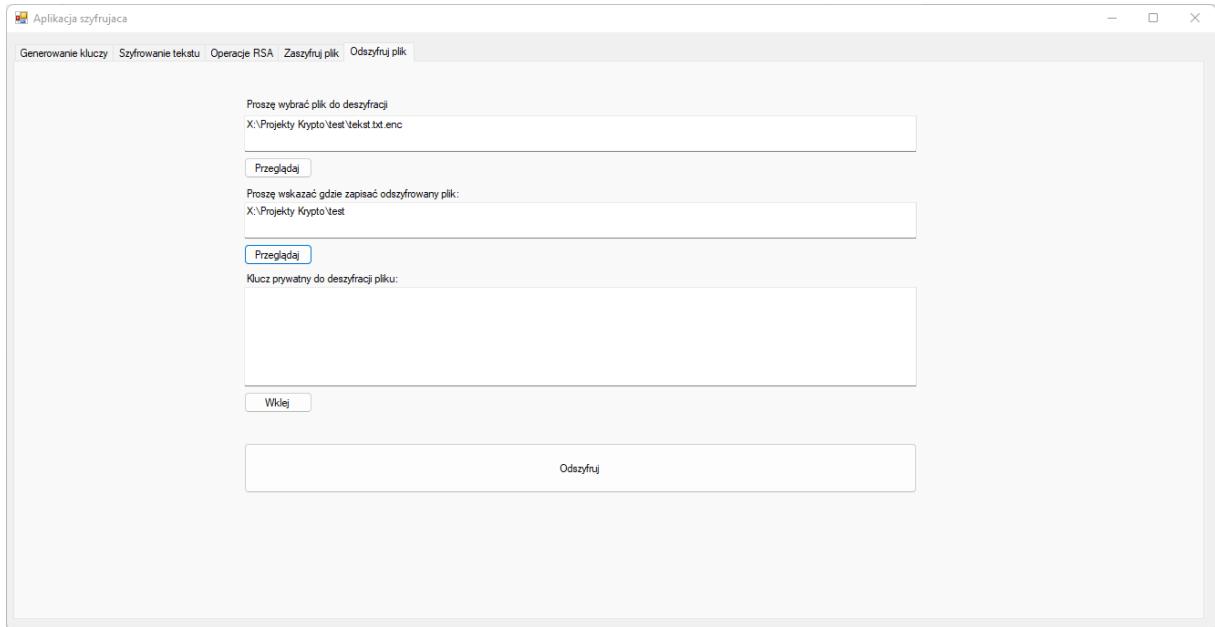
Po wybraniu pliku ścieżka pojawia nam się w polu.



Test pola wskazania, gdzie zapisać odszyfrowany plik

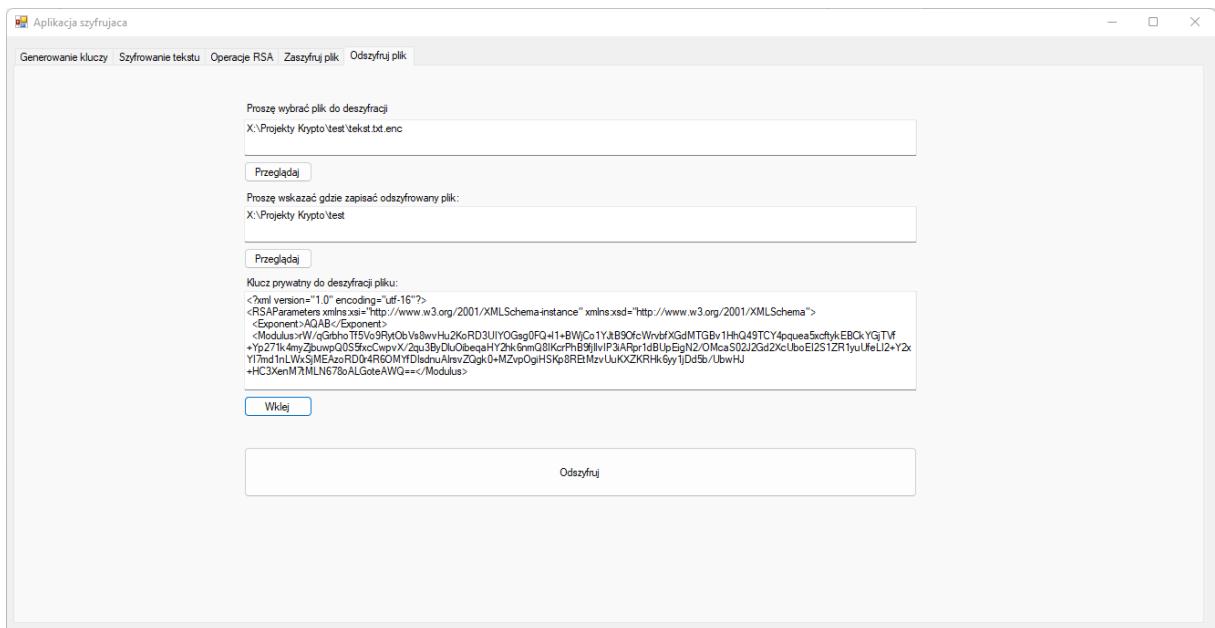


Po wskazaniu ścieżka pokazuje nam się w polu

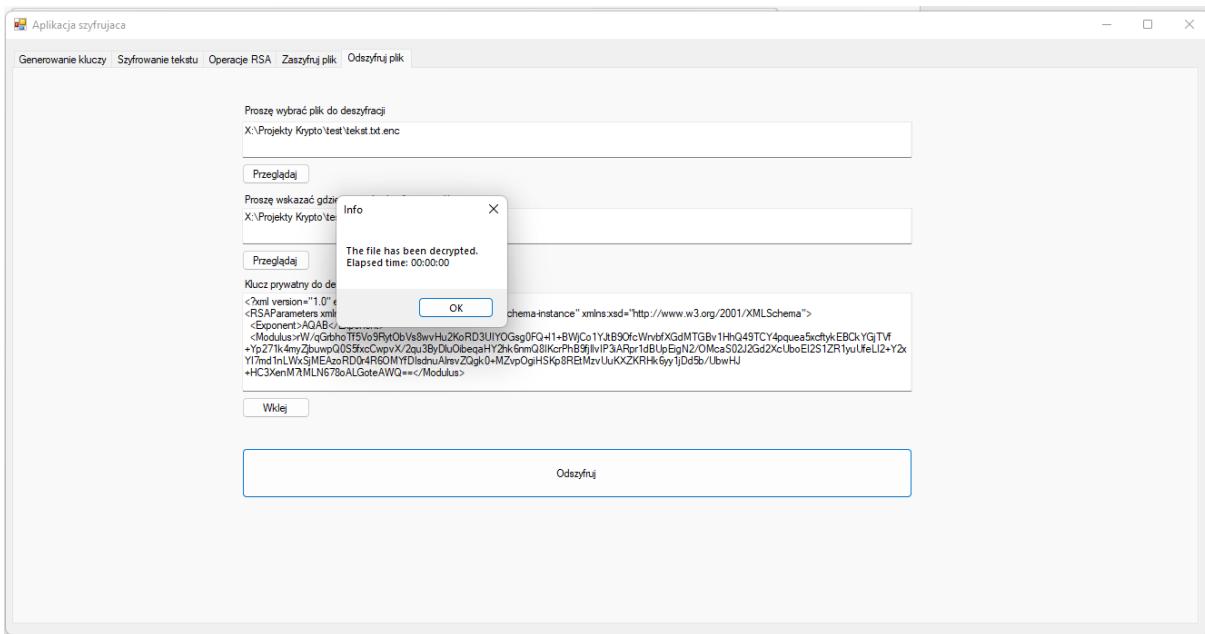


Test generowania klucza prywatnego (skopiowanego z zakładki szyfrowanie)

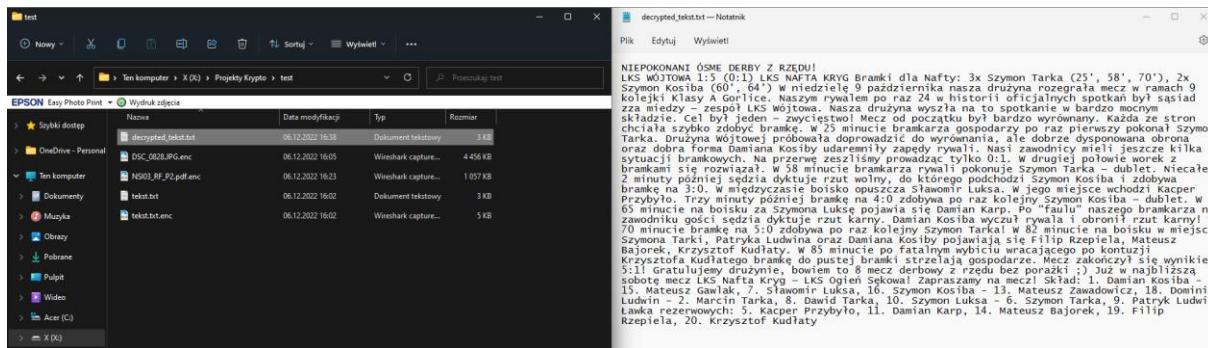
Za pomocą przycisku wklej dodajemy wcześniej skopiowany przez nas klucz prywatny



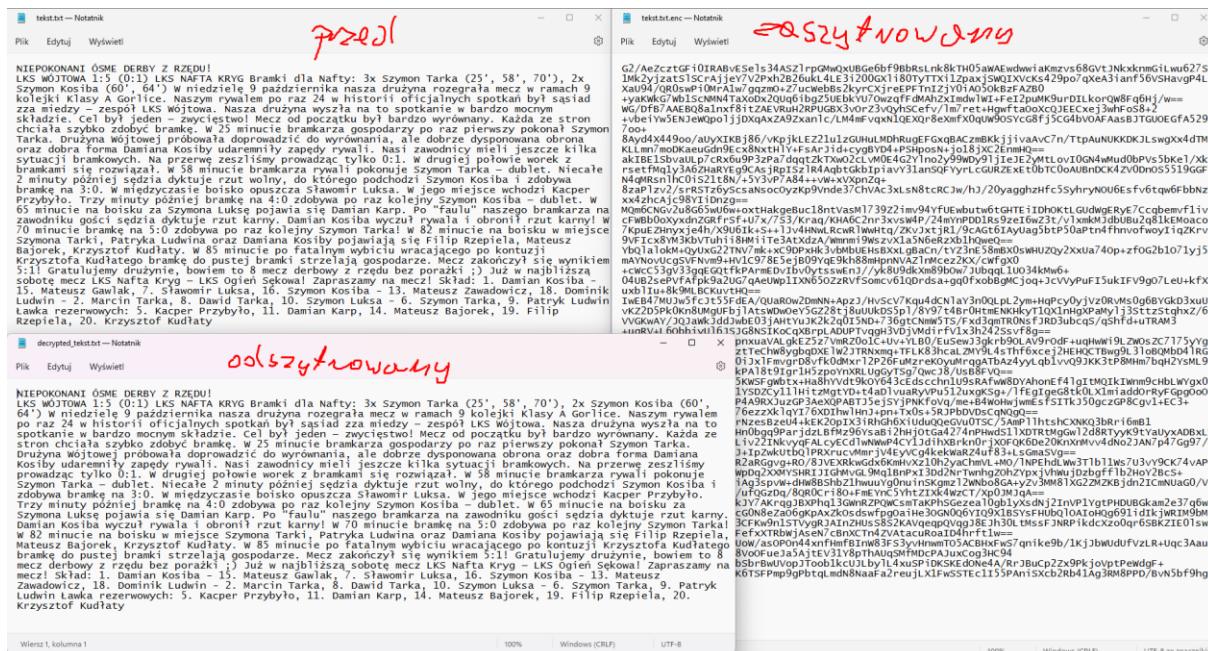
W celu rozszyfrowania pliku wciskamy przycisk Odszyfruj. Plik zostaje odszyfrowany



W folderze pojawia się plik decrypted_NAZWA.txt

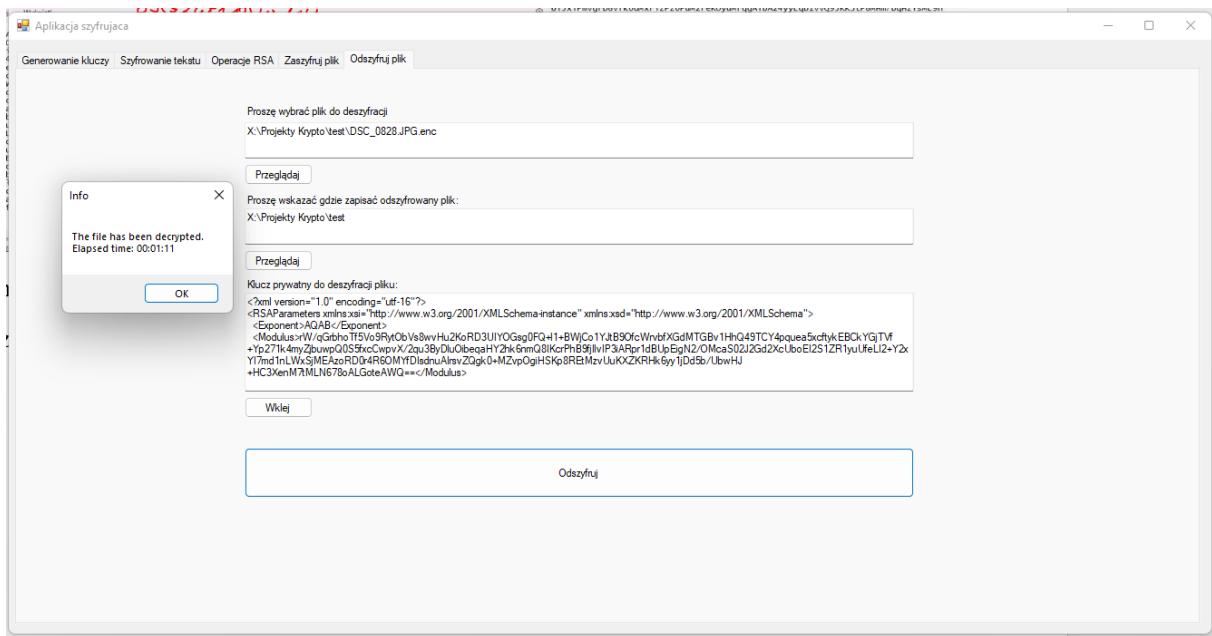


Porównanie zawartości plików. Przed szyfrowaniem. Po zaszyfrowaniu. Po rozszyfrowaniu

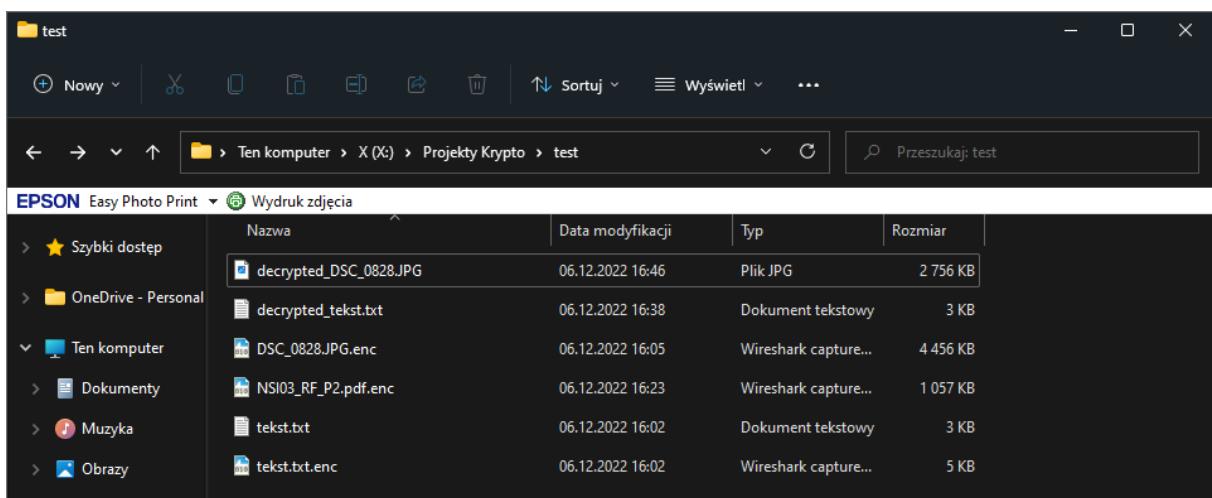


Jak można zauważyć plik został poprawnie odszyfrowany.

Odszyfrowanie pliku .jpg

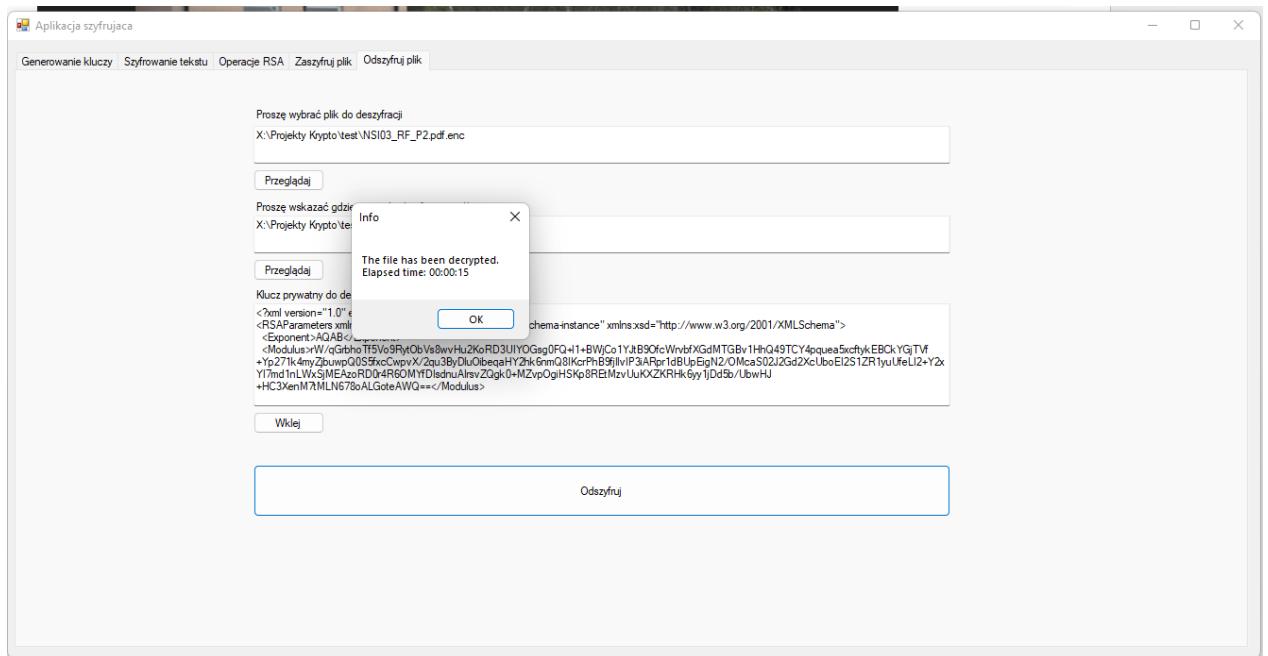


W folderze pojawia się plik decrypted_NAZWA.jpg

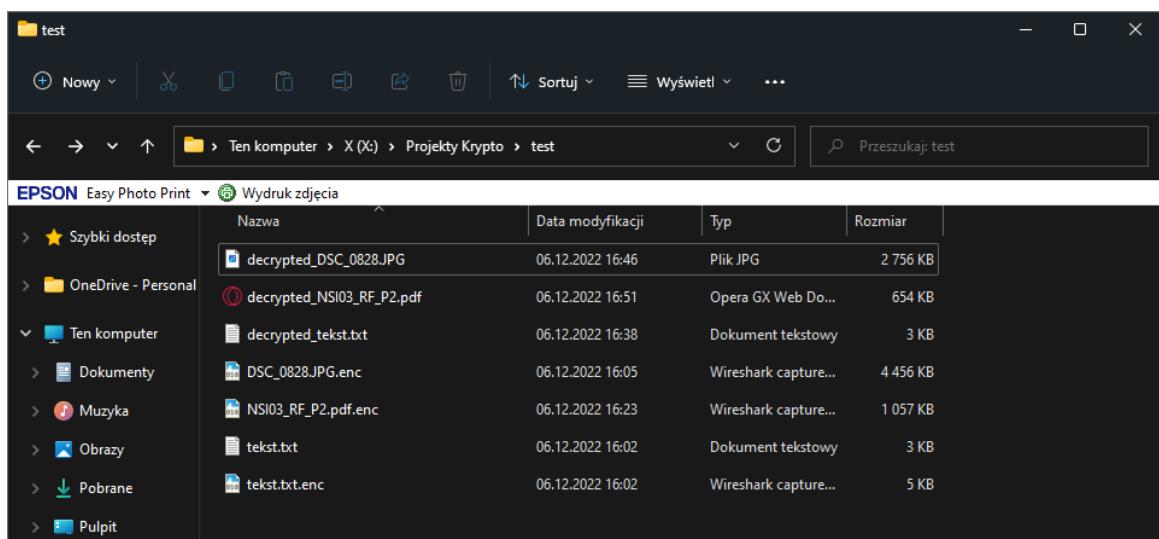


Przed odszyfrowaniem:

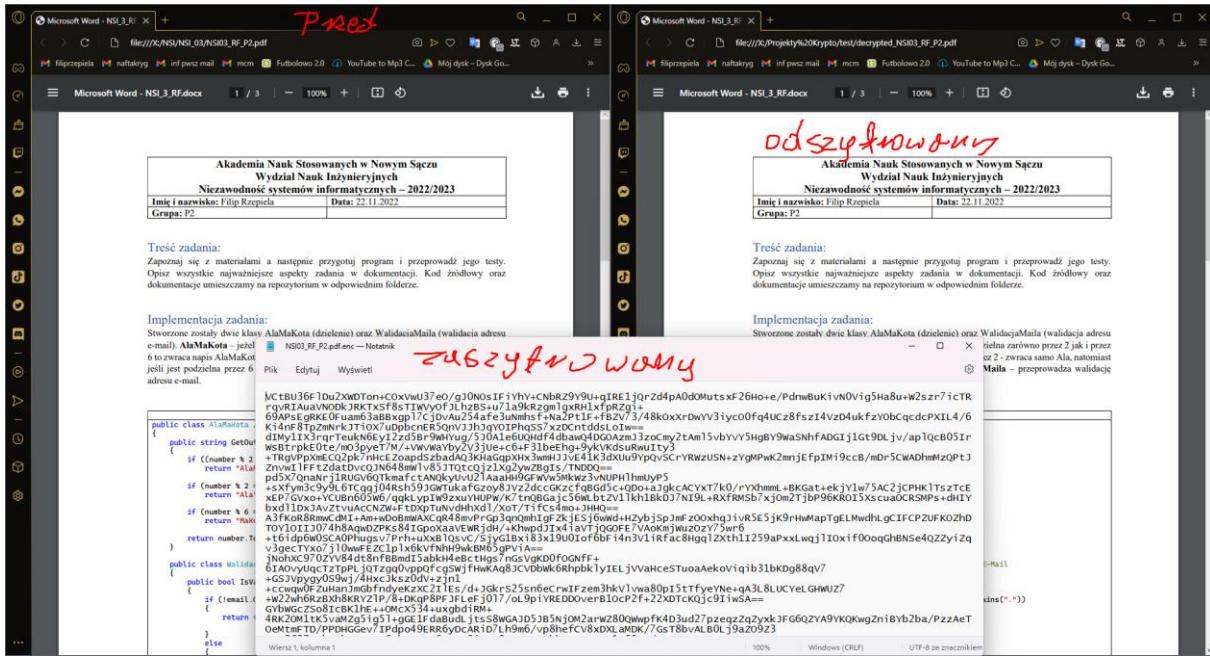




W folderze pojawia się plik decrypted_NAZWA.pdf



Porównanie przed zaszyfrowaniem, zaszyfrowany i odszyfrowany



Zużycie zasobów podczas odszyfrowywania

Deszyfracja wideo

Proszę wybrać plik do deszyfrowania

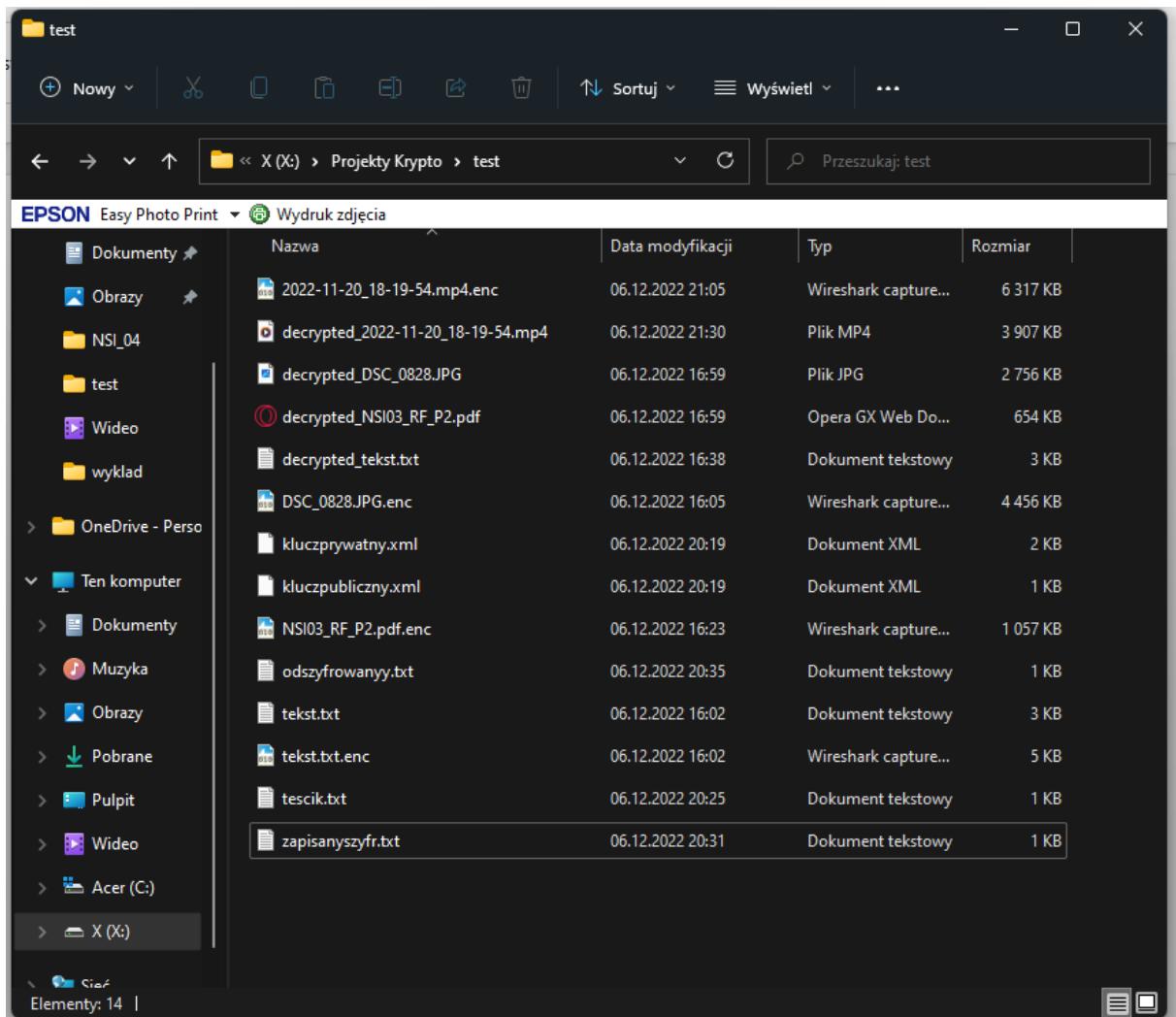
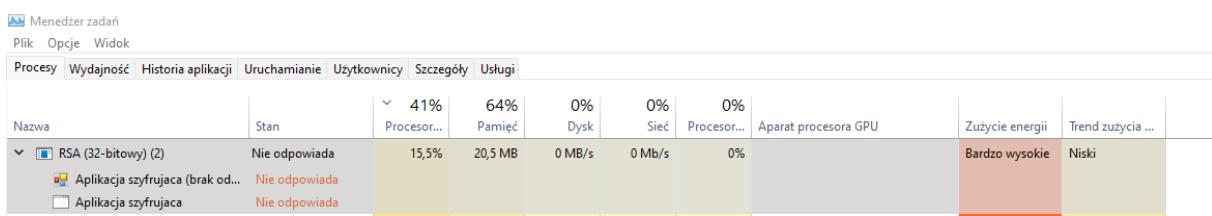
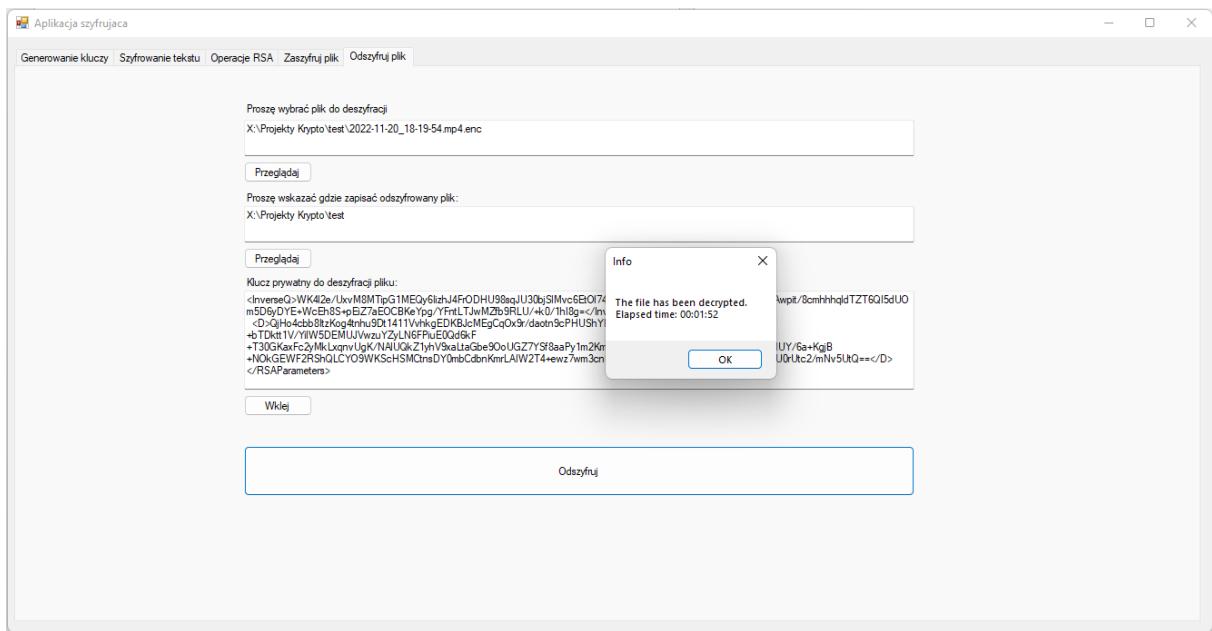
X:\Projekty Krypt\test\2022-11-20_18-19-54.mp4.enc

Proszę wskazać gdzie zapisać odszyfrowany plik:

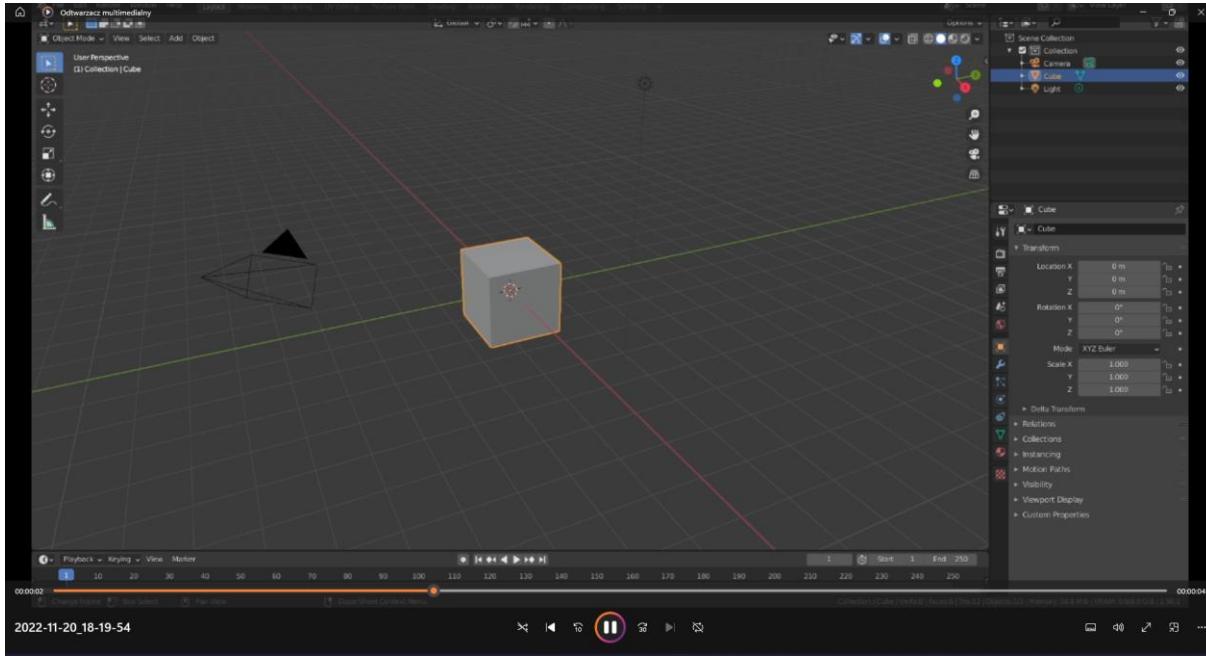
X:\Projekty Krypt\test

Klucz powtarzajacy do deszyfrowania pliku:

```
<inverseQ>-W</><2x>UxxMMMTcG1ME0y6ib-<4P>ODHU88sqJU30bSMv65E0t74MKBF5FL0yhbtEmM5Hb17fJfIf3Jn7KAwpit/8cmHhgldTZT6Ql5dUO
m5D6y6DYE-W</>W</>5h-5h</>E73EOC8Kk</>1pY</>Fr1-TwJmZtb5RLU-+k0/1h8g=</inverseQ>
<D>QH4-acba0tkaZopJhrnzu9D1411VvhkgEDKbJcMEgCqOx9r</>dadt9cPHUSHyHTXs-g4XatzPoVp6dVjX3fbuPDkjh
+htDkr</>Y/W5DEMUVwzuYZylNMFPuENQz6f
+T30GKavFc2yMkLxqnvUgK/N4U0kZ1yhV9aLia'be90oUGZ7YSf8aaPy1m2kmawXjO&jyIR6fp5CnLwQvnNMgyL+akldIUY/6a+KgIB
+NokGEWF2RS9hQLCY09WSchSMQnsDY0mbCdbnKmrLAIW2T4+ewz7wm3cnlPmWjMA23kb14hboubwecNs4ofvdRUD0Uc2/mhv5UtQ==</D>
</RSAParameters>
```



Przed zaszyfrowaniem

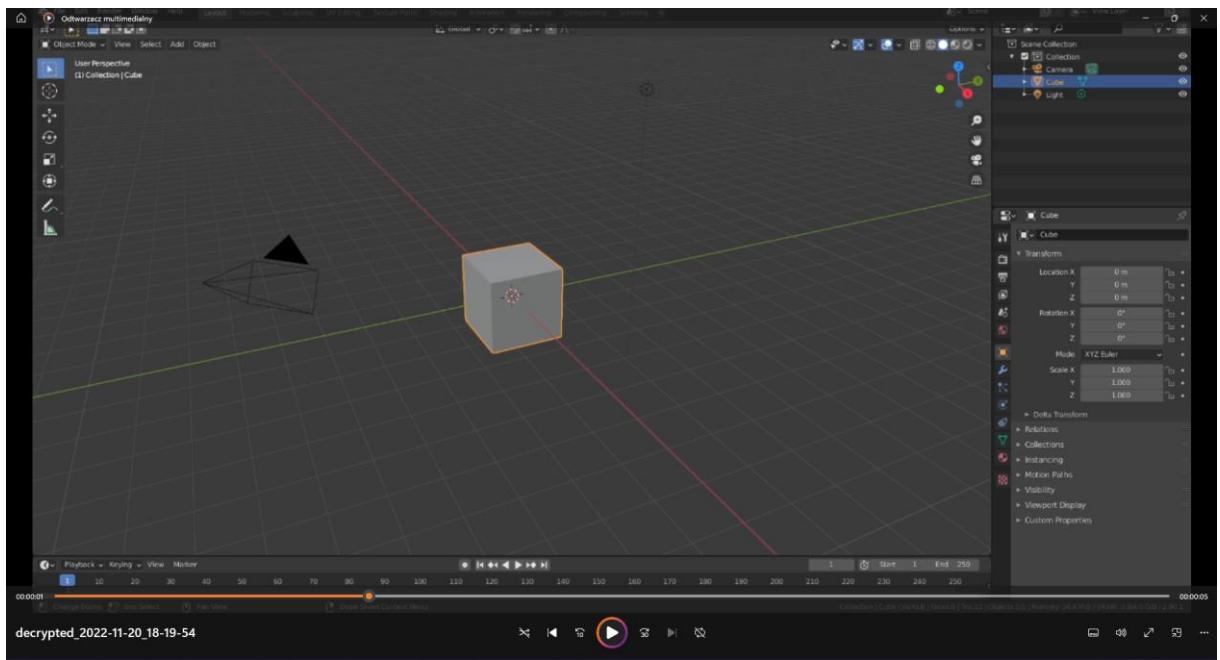


Po zaszyfrowaniu

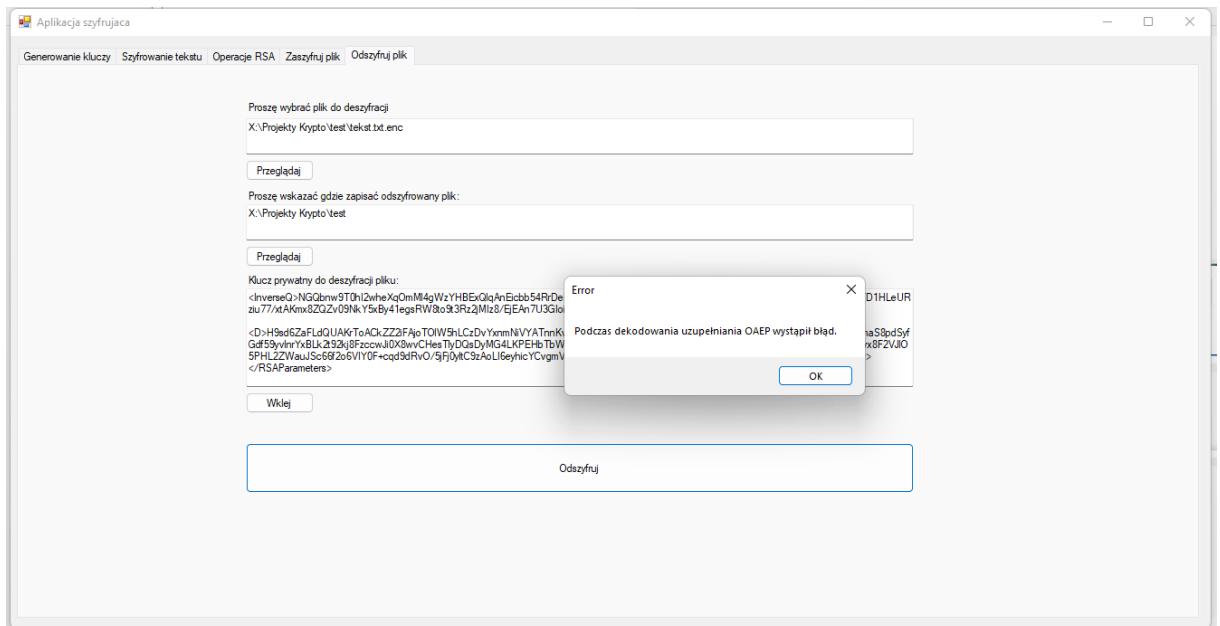
```
2022-11-20_18-19-54.mp4.ENC — Notatnik
Plik Edytuj Wyświetl

1HC3Uu1AasEcyzBFGDZX+gqWacNip4qXAZZIwGR3iON8yKYt2xbmNALU1fZKAYQQGmkXR+Fdqr2yxx+dXBjg1Fsm4zHJ1DzDg3wVrJVCEwCCWhFRZUVxH/lwHAXFWzeOLnQrIF3kJ/YutvkkJ606rPCTw320m4tEPxtvu8U+7+N6Av+UCppNz9zoPMWUoju/dqKsrgbtrS6+f7VLugA83i6ule54sVj3HVkj511UhzKInP7nbj9tJfrQXntu8Y013sacbNLajRGfV1r8809xfqfmu1d4Dk/k4u3ADfgnr78M3/57GxkpzMucyKOVp7PX781bqIgN3dqKEB5Zk8A==NUwi0JKwysUnjw1/i2anychNfseZdXTyyRDeI/odP/X/r9LIMFds0CNmjnSv9y7gXKYK94yu50/isywXcT+jEGURltrKN480Qqp71ownbQWEwKgWnOPbsd2PLr5hpAIjTS/afv9j9ivOnkOp58Qyhk97ZZHfHY5wsSfb/gzzFLpiNd/Uqq0L6vhaz9BCavx1Zxcqvc1DELOJ/agfo+wRUCB1lg105mCaucCMIZ+QyhyUmzIZ0gepjfQavD17HJ2x0iHFRi1b3M43GQWM8mxHX7rhg7Y52MD4K3nIRjJW1Hdsdp/wMcUjfpr9nZhSxSP0Iho3ci83brc78whuYsDeg==Q0behIkbgSNJvvLWXROCwEb/P1soIAnea/p9pKv47swOFbDcolaZglejn5KU/4GhK4upyA7libUKw2baem9cGiDpWie003V/p3pEaqh0qK8VvuIZmhs tEu9XVYxCpd0QmNmBmvmAUr4EiV3wqmItgfHad6zLocjzUTos5EevTmTxxi7Dcpbn0Cq8L1ntIr4fSRqybi6FGwZxywAcaW0f7DSqwqsRmN91giA7h01S61nRdwLm4URxKIYKjvp2b+vEqC/3CMzOPmm59Su4fz0zs3wTp3cfXP62bs1v675Tp+XD3F8UMMewtcGyc6obzHWhv5L84R8z1tlyLSKxs+w==bSOAMjwT5Q8obCFKPwh5hu1vGA4g2Cx2j6s0Ef14Pb7DrZqQofRwpLyxFsQF6xyP6I+xwADPiTwUkgve12UDcu31yMA8djco8sarzxh4CdfDBKjCzfZI3LGuzJT23j5niVmz7TrNaKjD5IDoEnuAkq2E6fxM2vVzI2WX/fr0ZzuJgrftDhMpCYR/nNVfoTQvxk2LJptN9501f0jih8GIGb9VqHzJxA02ZXKdogaTSE02ist8x7zuuw1qvcgyJU1IM1kf8kc95uu+VF+hsmJzHeNczEmd625f+KndQcfvso4I8gg90A2Idm5L9Ln4YCKdbVvPQ67nwMk1FOeMqa==1h7PZipNgTRAnEHUPKT0jfNv+LcdcQZLrzENcIyk2bSARLFmvyr99Cu2r36t20h/37c06FJXXy/AjvCAYD5VMHiJySmnznLNAs1Ubwxh+MjT/3hp8rjf/M12VIT1lU1ssSjgQ/MaCUA+xduc21xw+hcNCTPmrV+5o1b4oc89crWryUloGCVnI1c6fwu4k9GZh2qj9orikTLYcE94C7rkCPWLdnsApJ/aJo7b0bDBe/CsdmiATVRTmKvhaV8H1DD4f5CoiaafrwixCYjLBt2jMt1ce7Z2xAd/V18DK1LSCcJoxRSFpwzmqVOLR1Q6jymZoM8TRdSYQ25y+BiG==j5y3GwveZTMYR6Lvx48RJMOT525BM2muQ19x4ud4J6HJ0kBeodwB1WNGra0yY5D0xIkxf10E+dp19ktwdsJnuFE8k+9Y1z4VGnPZg88rvG/ubg+AuGsspMbowF5qa05ylObw2uHrgcU7uu3pT1dRyKgY0c60g1gwzbP2UzKbuQfxxyG7h9ZT/ffp4pFsdaC5Q+HMLDTHXhonQ1qgPba6fvSzU7Yxw/Ck-j11EcmX8uU6nRxHSceAPbwk+WxzMoZt27091wb4CmldkMj8sjRCKdQ7UwOvx8B01zzbs2DzrxQzI7yyjf3jGWL79Xm0Lwu12Is8+rsl1yLJvulvDw==
```

Po odszyfrowaniu



Test bezpieczeństwa – niepoprawny klucz prywatny



W przypadku wprowadzenia niepoprawnego klucza prywatnego program zwróci błąd

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.

Pod względem użyteczności – aplikacja posiada pięć zakładek, z której każda odpowiedzialna jest za inny, bądź podobny proces.

Pod względem pielęgnowalności aplikacja mogłaby zostać opracowana w lepszy sposób. Jej głównym problemem jest zbyt duża ilość kodu, z którego ostatecznie zrezygnowano (za komentowany) oraz część niewykorzystanych funkcjonalności. Część zmiennych posiada podobne nazwy co jest często powodem pomyłek podczas próby naprawy błędów. Kod jest zbyt długi, powinien być skrócony i zoptymalizowany. Natomiast nazwy pól tekstowych oraz guzików Windows Forms mają przyjęte stałe nazewnictwo i w łatwy sposób można się do nich odnosić.

Pod względem jakości aplikacja spełnia założenia oraz działa w sposób szybki. Zastosowanie base64 mogłoby skrócić znaczco czas szyfrowania większych plików. Program stworzony metodą prób i błędów o czym też świadczy ilość zakładek. Nie zawiera ulepszeń wyglądowych – ma działać a nie wyglądać 😊

W przypadku błędów zwraca komunikaty – jest to aspekt bezpieczeństwa.

Podczas testowania aplikacji pod kątem przeciążalności zaszyfrowane zostało zdjęcie oraz sześciosekundowy

Pod względem niezawodności aplikacja posiada instrukcje warunkowe sprawdzające czy konieczne w jakimś celu pola zostały uzupełnione. W przypadku, gdy któreś pole jest puste, a nie powinno informuje o tym i umożliwia poprawę, a nie kończy się awarią aplikacji.

Jeśli chodzi o efektywność – wszystkie procesy aplikacji działają poprawnie, co zostało udokumentowane zrzutami ekranu.

Kwestie wydajności zostały przedstawione zrzutami ekranu z menadżera zadań.