Dokumentacja programu „Kryptografia”

Wersja 1.0

Mateusz Goniprowski,
Kamil Niesłuchowski,
Paweł Załuska
2015

Spis treści

1. Wprowadzenie

Program „Kryptografia” powstał na potrzeby zaliczenia przedmiotu „Zaawansowane metody ochrony informacji” na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. Skład zespołu, który odpowiada za jego stworzenie to Mateusz Goniprowski, Kamil Niesłuchowski oraz Paweł Załuska.

1.1 Sposób działania

Głównymi funkcjami programu są szyfrowanie oraz deszyfrowanie tekstów wczytanych od użytkownika. Tekst może być wczytywany automatycznie (z pliku) oraz ręcznie (wpisany za pomocą klawiatury). Dodatkami ułatwiającymi życie kryptologom korzystającym z oprogramowania są m.in. automatyczne wyznaczanie charakterystyki szyfrogramu, generowanie statystyki wzorcowej czy też kryptoanaliza metodą prób i błędów. Szerszy opis interfejsu opisany został w rozdziale 3.

1.2 Konfiguracja programu

Program nie wymaga konfiguracji. Po uruchomieniu gotowy jest do pracy.

1.3 Wymagania sprzętowe

Do prawidłowej pracy niezbędny jest komputer klasy PC, który spełnia następujące wymagania:

- 512 MB RAM
- PROCESOR PENTIUM 4 2,4 GHZ
- ok. 1 MB wolnego miejsca na dysku twardym
- Monitor SVGA (1024 x 768)

1.4 Wymagane oprogramowanie

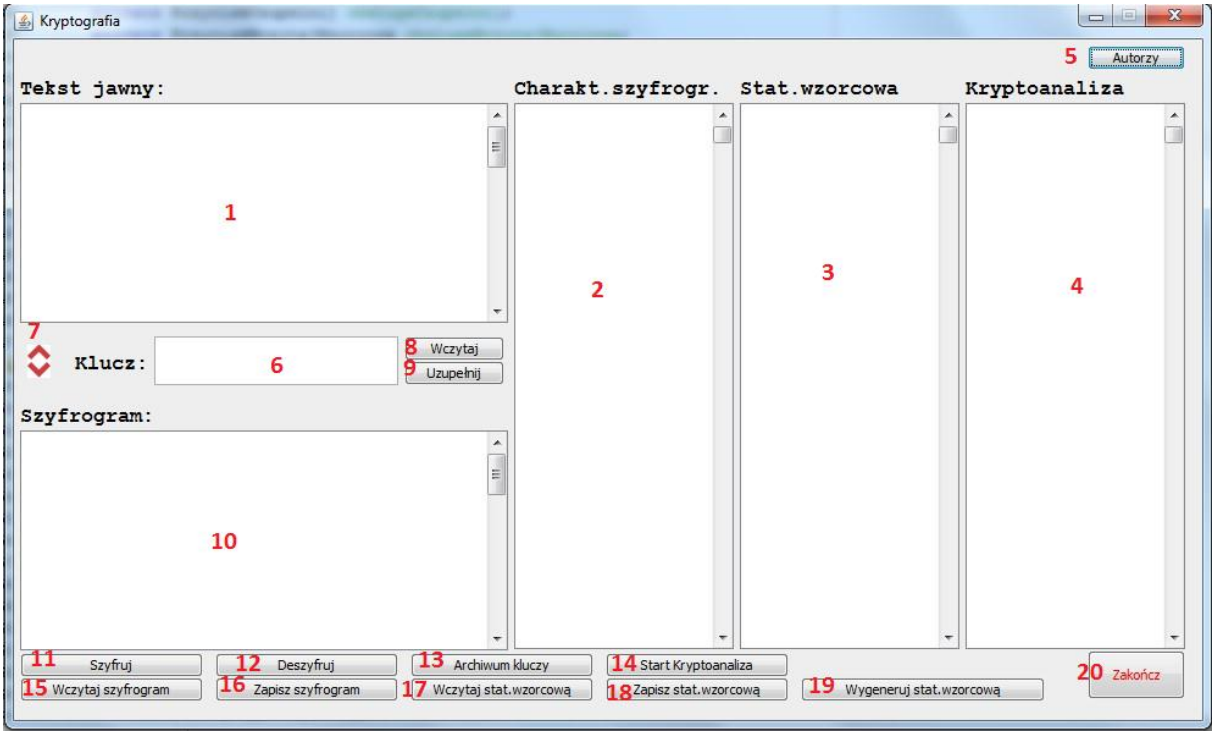
Poza wymaganiami wymienionymi w punkcie 1.3., niezbędne do działania programu jest oprogramowanie wymienione poniżej:

- Dowolny system operacyjny z zainstalowaną maszyną wirtualną Javy w wersji JRE 7+

2. Instalacja programu

Aby zacząć używać programu wystarczy uruchomić plik o nazwie „kryptografia.jar”. W celu korzystania z archiwum kluczy należy dodatkowo stworzyć plik tekstowy (jeżeli nie istnieje w folderze programu) o nazwie „klucze” z rozszerzeniem *.txt . Przykładowe pliki do wczytywania tj. tekst jawny oraz charakterystyka wzorcowa znajdują się w folderze „pliki”.

3. Wygląd oraz opis interfejsu



Rys. 1 – Wygląd interfejsu programu

Opis interfejsu:

1) **Pole tekstu jawnego**

   Pole do wprowadzania tekstu na dwa sposoby – ręczny za pomocą klawiatury oraz automatyczny za pomocą przycisku „Wczytaj szyfrogram” i wyborze interesującego nas pliku.

2) **Pole charakterystyki szyfrogramu**

   Pole, które wyświetla aktualna charakterystykę szyfrogramu posortowaną od najczęściej do najrzadziej występujących liter.

3) **Pole statystyki wzorcowej**

   Pole, które wyświetla statystykę wzorcową stosowaną przy kryptoanalizie. Wygenerować ją można na 2 sposoby:

   a) Używając przycisku „Wczytaj statystykę wzorcową”

      Pobieranie wcześniej zapisanej statystyki z pliku

   b) Używając przycisku „Wygeneruj statystykę wzorcową”

      Generowanie statystyki na podstawie wczytanego pliku tekstowego

4) **Pole kryptoanalizy**

   Pole, w którym wyświetlane są litery alfabetu z literami, na które chcemy zamienić nasz tekst jawny. Format zapisu – „A => B” co oznacza, że litera A zostanie zastąpiona literą B w tekście.

5) **Przycisk „Autorzy”**

   Wyświetlenie komunikatu z listą autorów programu.

6) **Pole klucza**

   Pole do którego wpisujemy klucz do szyfrowania i deszyfrowania tekstu.

7) **Przycisk zamiany stron tekstu jawnego z szyfrogramem**

   Zamienia miejscami tekst jawny z szyfrogramem.

8) **Przycisk „Wczytaj”**

   Wczytywanie ostatniego użytego klucza.

9) **Przycisk „Uzupełnij”**

   Uzupełnianie klucza losowymi literami alfabetu bez powtórzeń, np. jeżeli użytkownik wpisze klucz „QWERTY”, funkcja może wygenerować następujący klucz „QWERTYABCDZG…” o łącznym rozmiarze 26 znaków. W przypadku pustego klucza zostanie wygenerowany losowy ciąg znaków bez powtórzeń.

10) **Pole szyfrogramu**

    Pole, w którym wyświetlana jest treść szyfrogramu.

11) **Przycisk „Szyfruj”**

    Szyfrowanie tekstu jawnego przy pomocy zadeklarowanego algorytmu szyfrowania.

12) **Przycisk „Deszyfruj”**

    Deszyfrowanie szyfrogramu przy pomocy zadeklarowanego algorytmu deszyfrowania.

13) **Przycisk „Archiwum kluczy”**

    Wyświetlenie dodatkowego okna z listą zarchiwizowanych kluczy. Archiwizacja przeprowadzana jest automatycznie w momencie szyfrowania tekstu jawnego. Aby wybrać dany klucz należy dwukrotnie kliknąć na nim lewym przyciskiem myszy.

14) **Przycisk „Start Kryptoanaliza”**

    Uruchomienie funkcjonalności kryptoanalizy. Pierwsze użycie przycisku wygeneruje szablon kryptoanalizy, kolejne spowodują zmiany w szyfrogramie i wyróżnienie małymi literami (pod warunkiem że zostały wprowadzone w szablonie kryptoanalizy).

15) **Przycisk „Wczytaj szyfrogram”**

    Wczytywanie szyfrogramu z pliku i umieszczenie go w polu tekstu jawnego.

16) **Przycisk „Zapisz szyfrogram”**

    Zapisywanie wcześniej wygenerowanego szyfrogramu do pliku.

17) **Przycisk „Wczytaj statystykę wzorcową”**

    Wczytywanie statystyki wzorcowej z pliku (bez generowania, samo wczytywanie).

18) **Przycisk „Zapisz statystykę wzorcową”**

    Zapisywanie wcześniej wygenerowanej statystyki wzorcowej do pliku.

19) **Przycisk „Wygeneruj statystykę wzorcową”**

Generowanie statystyki wzorcowej na podstawie wczytanego tekstu z pliku. Zliczane są wystąpienia liter i sortowane w kolejności od największej do najmniejszej ich ilości.

20) **Przycisk „Zakończ”**

Kończenie pracy programu.

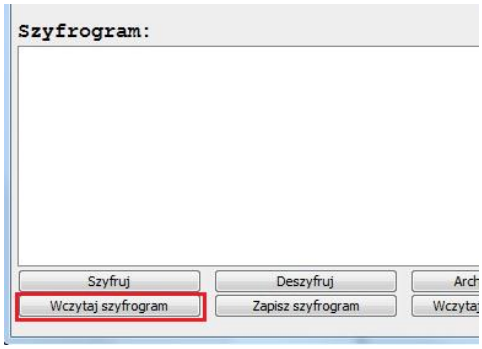
4. Przykładowe użycie

4.1 Szyfrowanie i deszyfrowanie

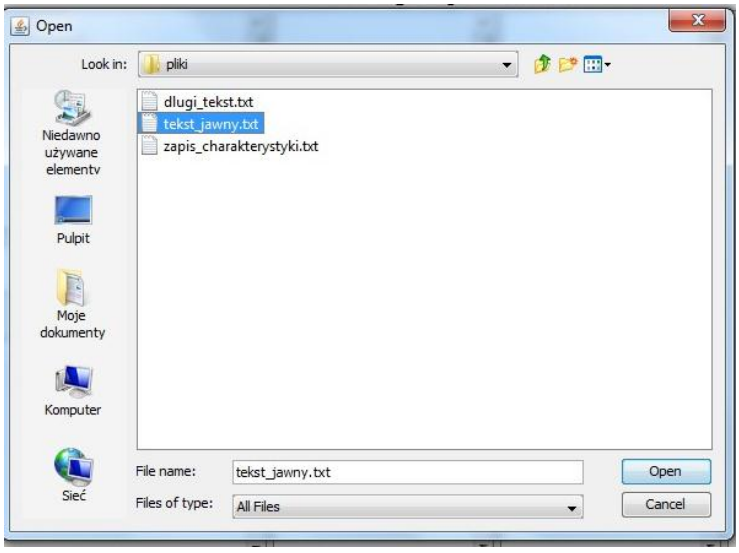
a) Szyfrowanie

Pierwszym krokiem w szyfrowaniu jest uzupełnienie pola „Tekst jawny” tekstem, który chcemy zaszyfrować. Można to zrobić na dwa sposoby:

- **Automatycznie** – wczytanie tekstu z pliku
  KROK 1: Używamy przycisku „Wczytaj szyfrogram”

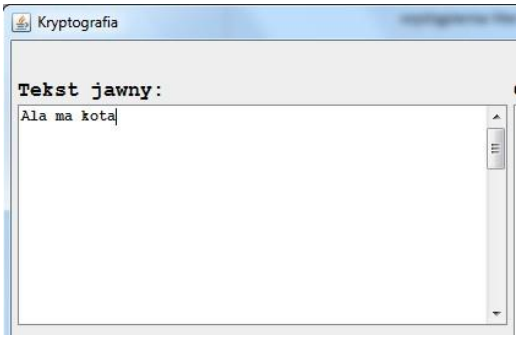


KROK 2: Po otwarciu dodatkowego okna wybieramy nasz plik z tekstem do



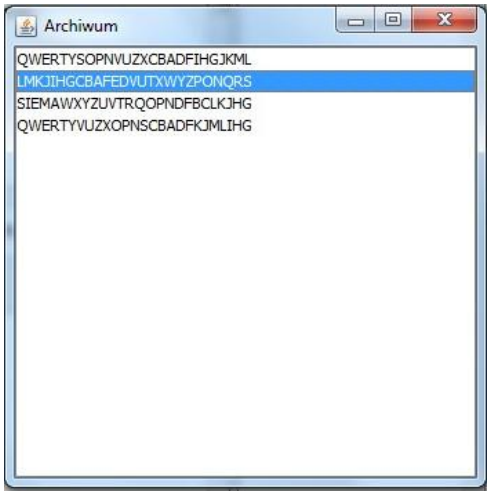
szyfrowania i klikamy przycisk „Open”

- **Ręcznie** – wpisanie tekstu za pomocą klawiatury

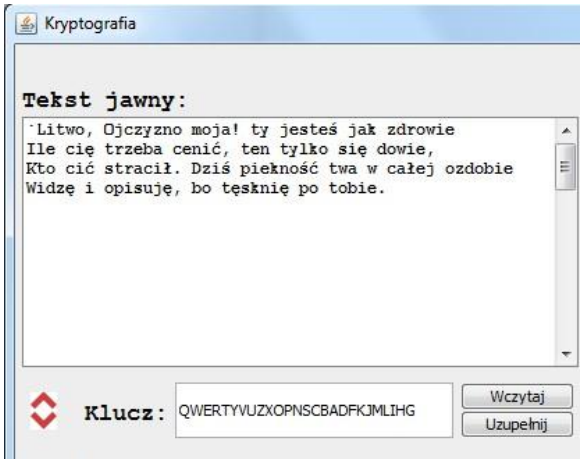


Po poprawnym uzupełnieniu tekstem pola „Tekst jawny” należy dodać klucz. Można to zrobić na 4 sposoby:

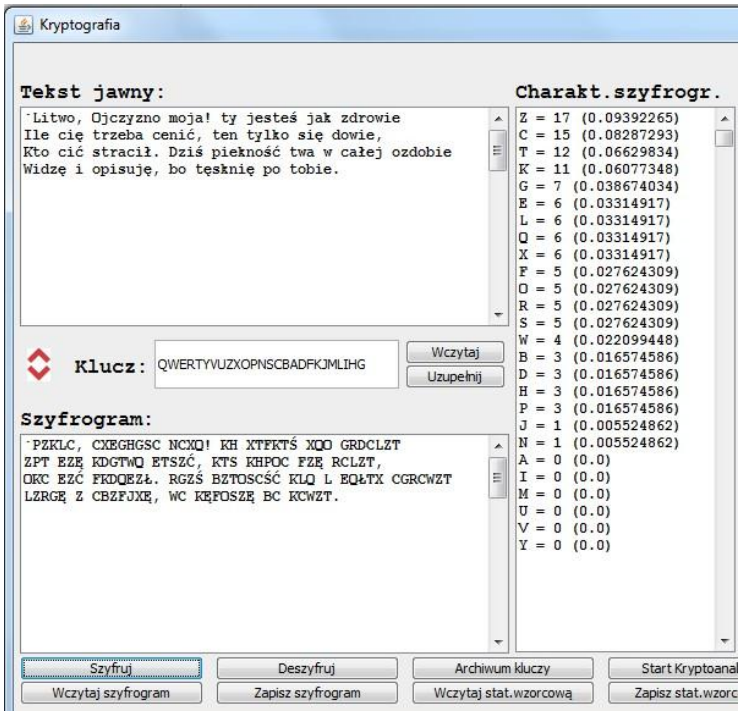
- **Ręcznie** – wpisanie tekstu za pomocą klawiatury. Należy pamiętać aby klucz miał 26 znaków bez powtórzeń.
- Używając przycisku **„Wczytaj”**, który wczytuje z archiwum ostatnio użyty klucz.
- Używając przycisku **„Uzupełnij”**, który generuje pseudolosowy ciąg znaków bez powtórzeń.
- Używając przycisku **„Archiwum kluczy”**, który powoduje wyświetlenie nowego okna do wyboru klucza spośród wcześniej używanych (zapisanych w archiwum).



Wszystkie metody powodują następujący efekt:



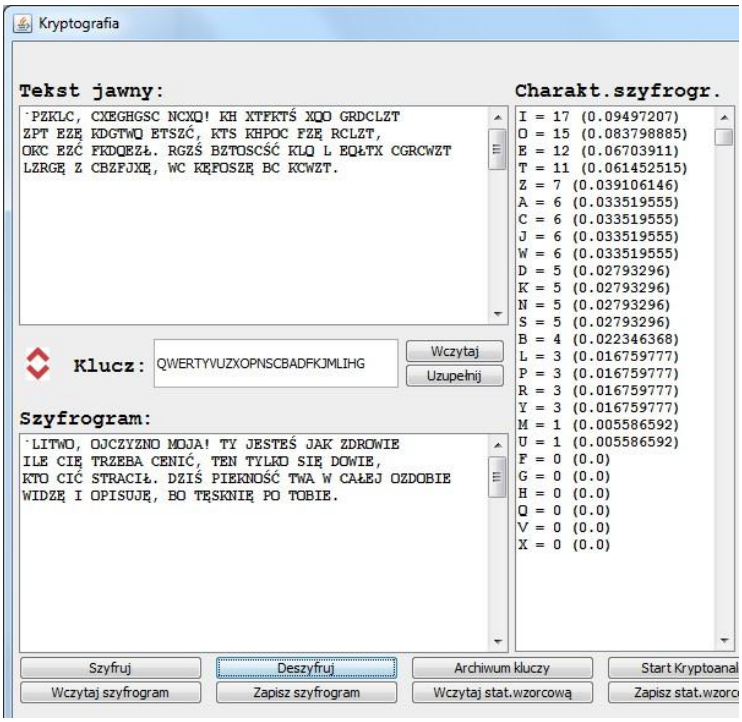
Zatem mamy już tekst jawny oraz klucz więc nie pozostaje nic innego jak szyfrowanie naszej wiadomości. Używamy zatem przycisku „Szyfruj” po czym w polu „Szyfrogram” pojawi się nasza zaszyfrowana wiadomość oraz jej charakterystyka. Efekt powinien wyglądać następująco:



Jesteśmy w stanie zapisać nasz szyfrogram do pliku używając przycisku „Zapisz szyfrogram”. Po pojawieniu się dodatkowego okna wybieramy miejsce zapisu oraz nazwę pliku wraz z rozszerzeniem tekstowym, np. „szyfrogram.txt” i na koniec klikamy „Save”.

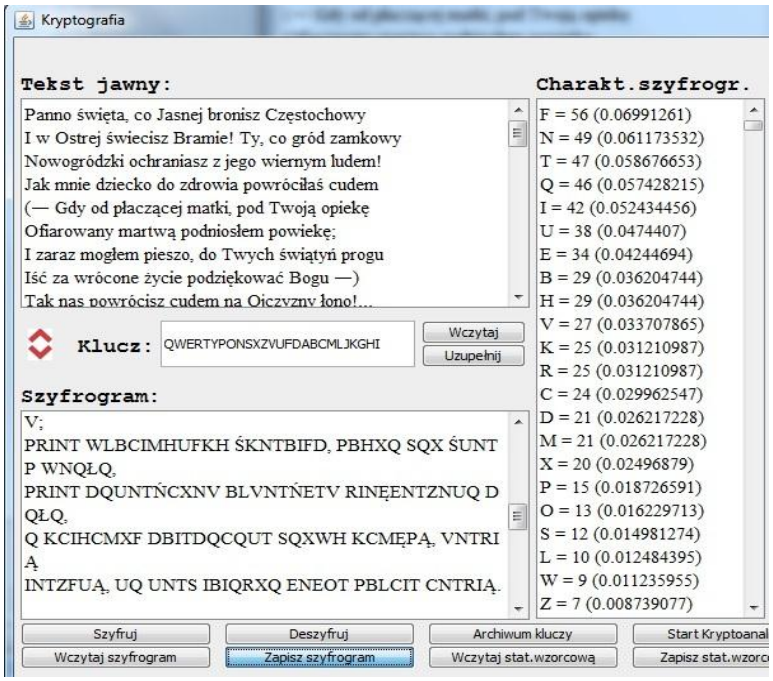
b) Deszyfrowanie

Deszyfrowanie wiadomości przebiega prawie identycznie jak jej szyfrowanie. W polu tekst jawny umieszczamy nasz tekst do deszyfrowania. Następnie ustawiamy prawidłowy klucz i używamy przycisku „Deszyfruj”, który powoduje deszyfrowanie naszej wiadomości i wpisanie wyniku w pole „Szyfrogram”. Rezultat powinien wyglądać następująco:

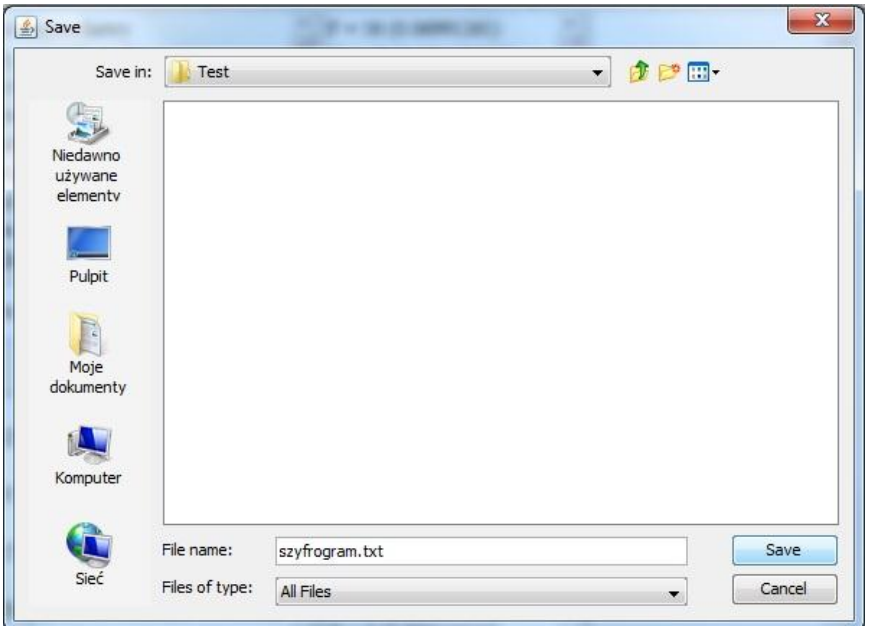


4.2 Zapis do pliku

Zapis szyfrogramu do pliku następuje po użyciu przycisku „Zapisz szyfrogram”.

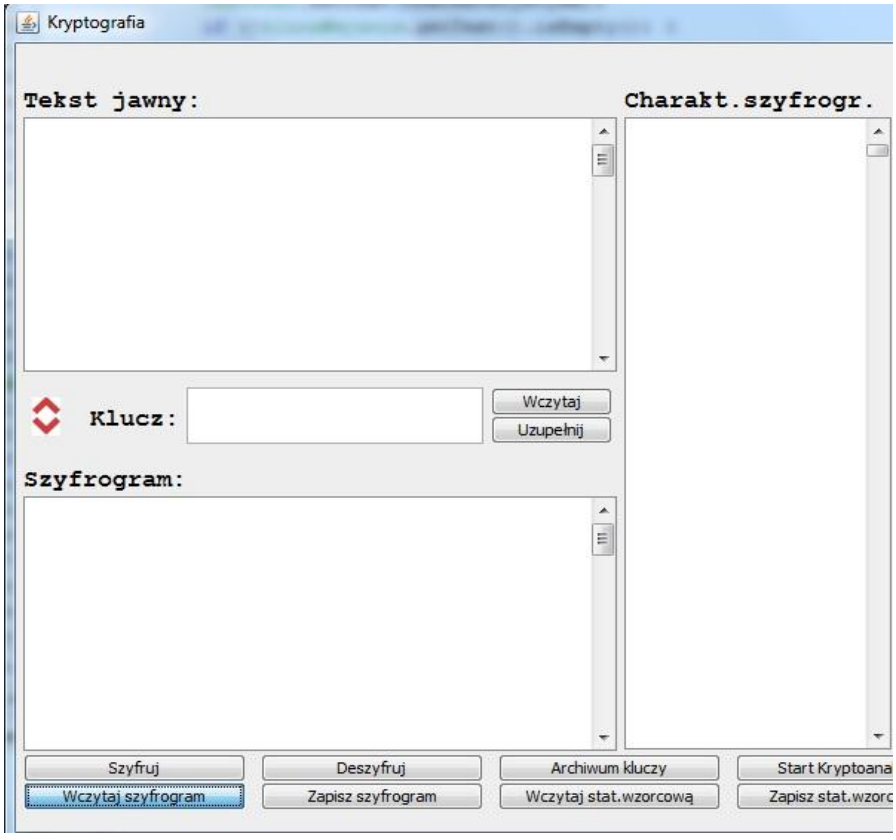


Po pojawieniu się dodatkowego okna wybieramy miejsce zapisu oraz nazwę pliku wraz z rozszerzeniem tekstowym, np. „szyfrogram.txt” i na koniec klikamy „Save”.

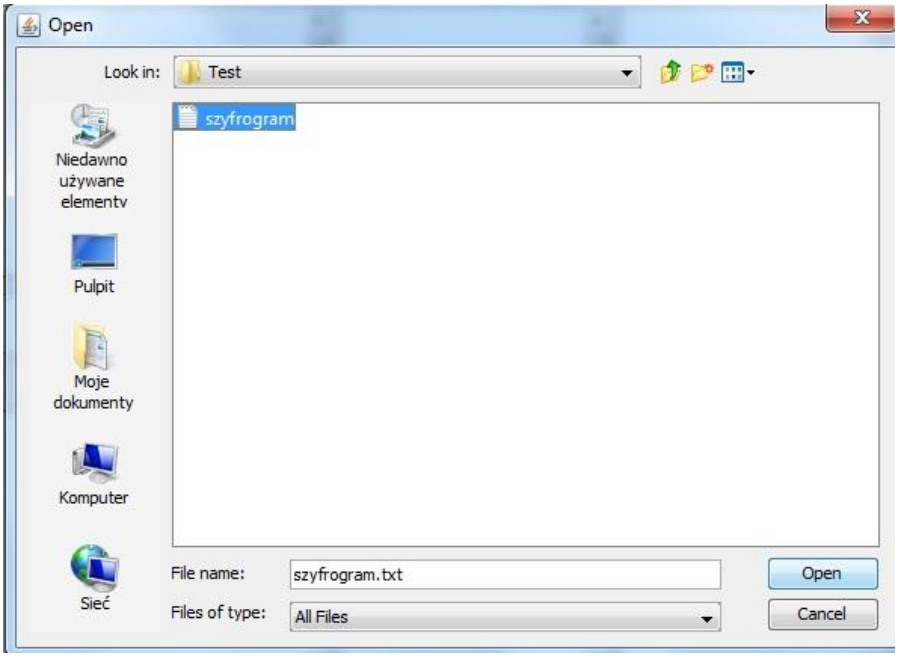


4.3 Wczytywanie z pliku

Wczytanie szyfrogramu z pliku następuje po użyciu przycisku „Wczytaj szyfrogram”.

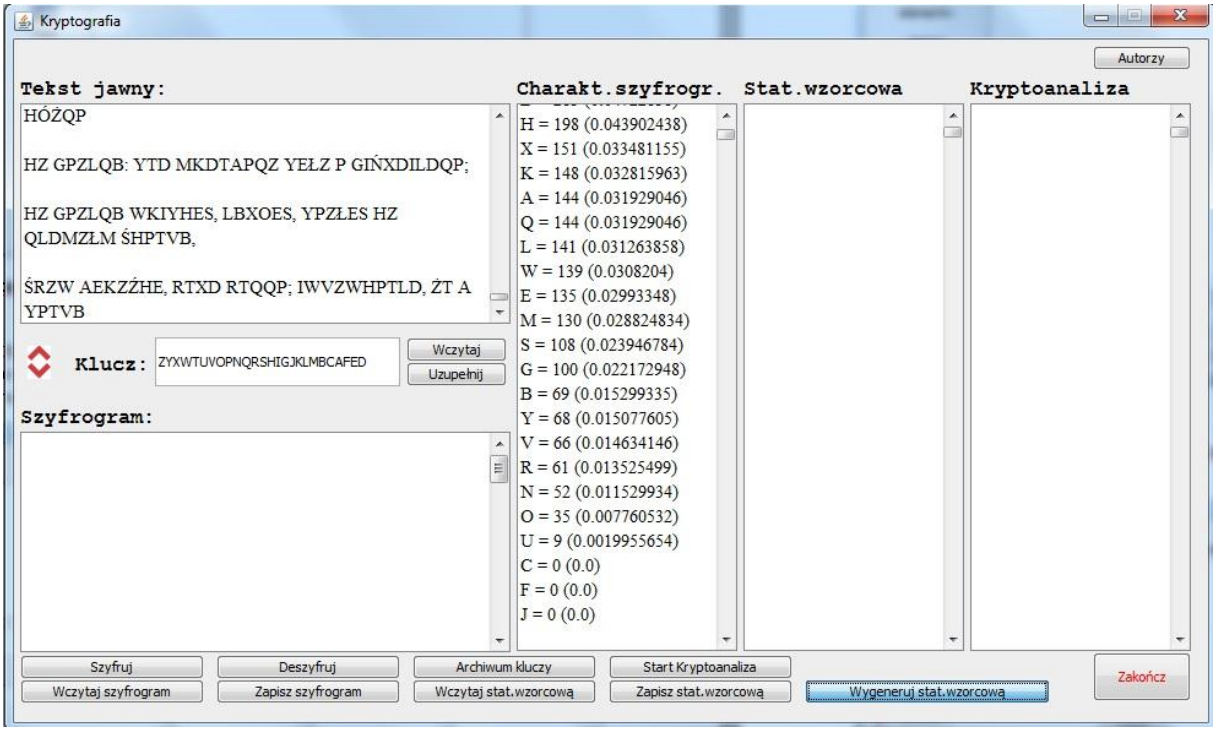


Po pojawieniu się dodatkowego okna wybieramy plik który chcemy otworzyć i następnie klikamy „Open”.

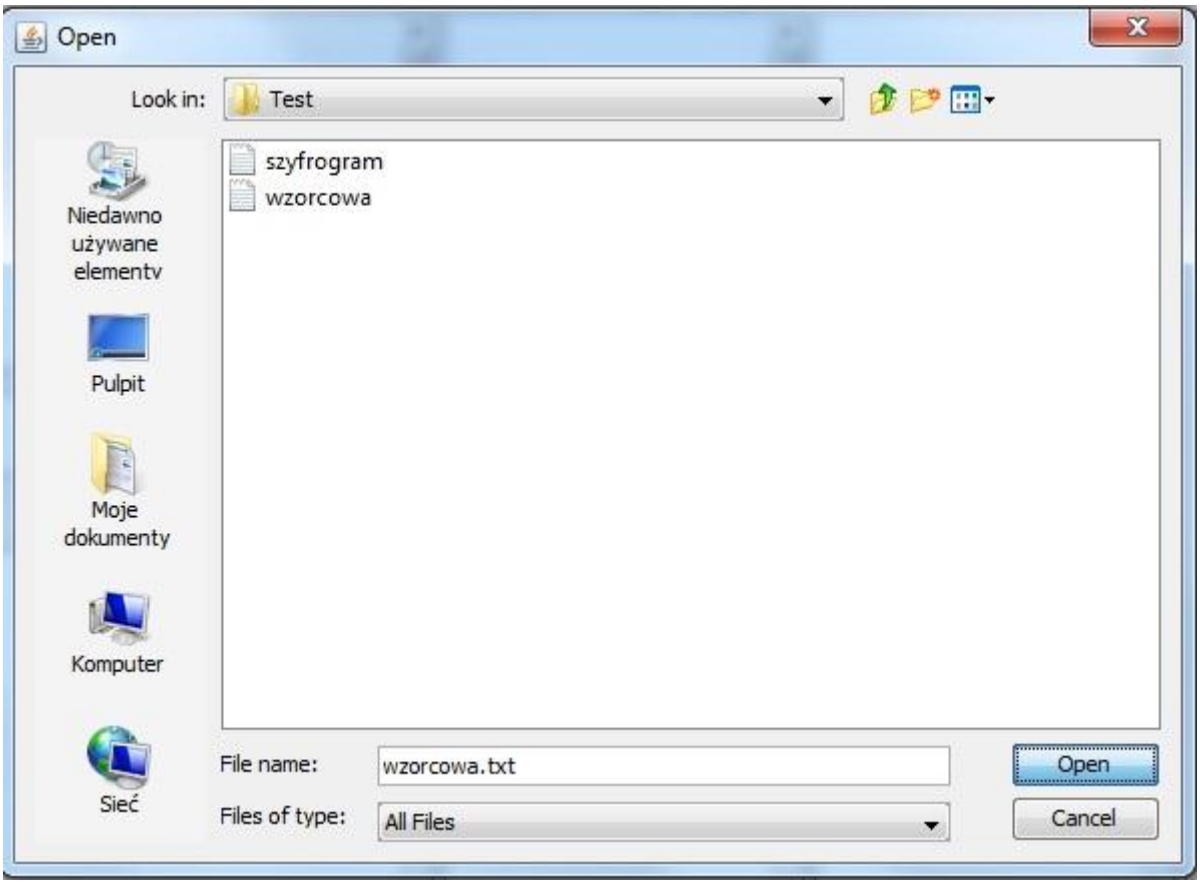


4.4 Kryptoanaliza

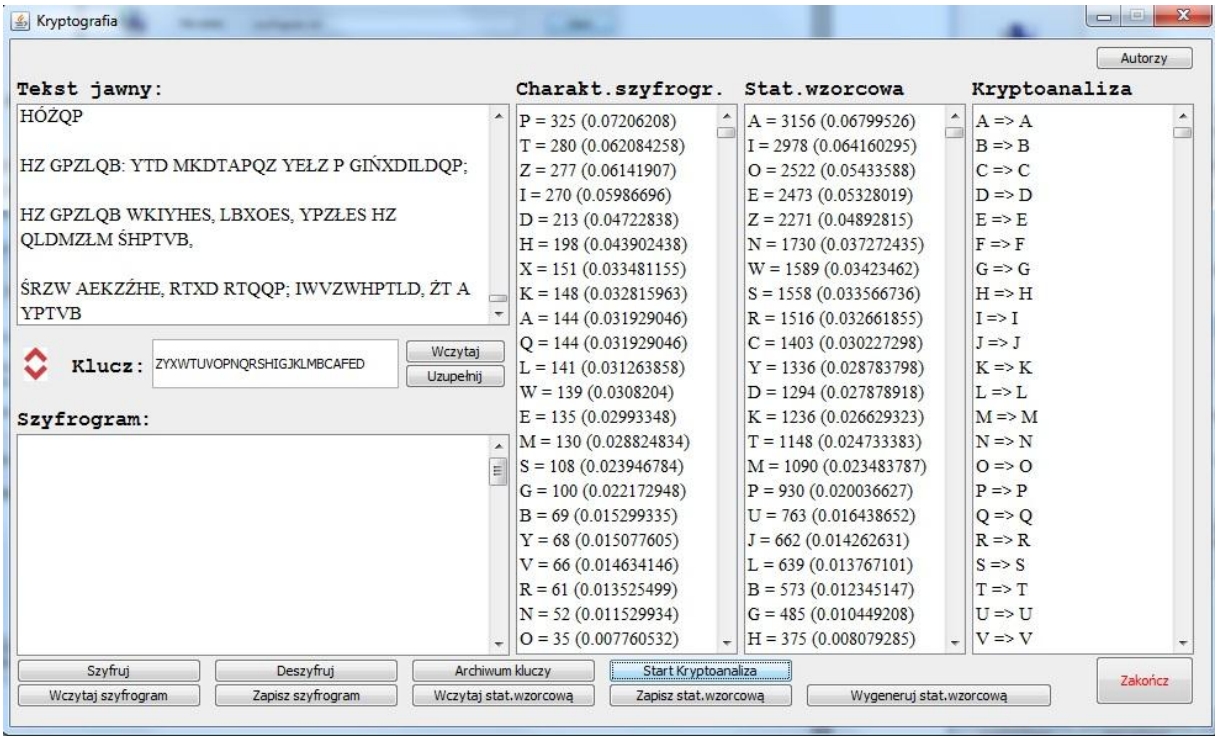
Aby rozpocząć kryptoanalizę jest nam potrzebna statystyka wzorcowa. Statystyka wzorcowa powinna być wygenerowana z odpowiednio długiego tekstu zapisanego najlepiej w tym samym języku. Za pomocą przycisku „wygeneruj stat. wzorcową” generujemy statystykę wzorcową z pliku.



Następnie wybieramy plik, z którego chcemy wygenerować statystykę.



Następnie używamy przycisku „start kryptoanaliza”, który generuje nam szablon kryptoanalizy.



Teraz należy podstawić odpowiednie litery w oknie kryptoanaliza, ponowne użycie przycisku „start kryptoanaliza” spowoduje zmiany w szyfrogramie i wyróżnienie ich czerwonym kolorem (pod warunkiem, że zostały wprowadzone w szablonie kryptoanalizy).