OPIS WYBRANYCH ALGORYTMÓW, ZASADY DZIAŁANIA PROGRAMU ORAZ INSTRUKCJE, JAK NALEŻY KORZYSTAĆ Z PROGRAMU W CELU PRAWIDŁOWEGO SZYFROWANIA BĄDŹ DESZYFROWANIA TEKSTU Z DANEGO ZAIMPORTOWANEGO PLIKU

Niniejszy program / aplikacja została napisana w języku C# .NET oraz umożliwia szyfrowanie oraz deszyfrowanie tekstu z wczytanych plików .txt przy użyciu algorytmu AES bądź DES.

Program zawiera łącznie w sobie 7 metod, z czego jedna metoda obsługuje ewentualne błędy przy wybieraniu algorytmu szyfrującego oraz przy szyfrowaniu bądź deszyfrowaniu tekstu z pliku, jak i również w przypadku wykrycia braku wczytanego pliku z tekstem do szyfrowania / deszyfrowania.

Idąc dalej zostają już tylko 4 metody, gdzie metoda ‘static void Main(string[] args)’ jest punktem wejścia do aplikacji konsolowej. Jej zadaniem jest wywołanie metody ‘public static void InstrukcjaDzialaniaProgramu()’, która wyjaśnia dokładne działanie całego programu w rozpisanych krokach, zaczynając od punku 0, gdzie jest przygotowanie pliku z tekstem, idąc po wczytanie pliku, podanie lokalizacji do zapisania pliku z nowymi danymi, wybranie algorytmu szyfrującego AES lub DES, a na koniec zdecydowanie, czy chcemy szyfrować, czy jednak deszyfrować tekst z pliku. W skrócie niniejsza metoda wyświetla instrukcje dotyczące działania programu, po czym prosi o wciśnięcie dowolnego klawisza, aby przejść do kolejnej metody, czyli ‘public static (string, string) SzyfrowanieDeszyfrowanieTekstuPliku()’.

Instrukcje z metody ‘InstrukcjaDzialaniaProgramu()’ zostały przygotowane i zapisane w następujący sposób, czyli:

- Niniejszy program służy do szyfrowania oraz deszyfrowania tekstu plików, czyli:
  (0) przygotowanie pliku, na którym będziemy działać [np. do zaszyfrowania]
  (1) wczytanie pliku .txt, który zawiera tekst do zaszyfrowania lub odszyfrowania
  (1a) aby wczytać plik .txt należy podać dokładną ścieżkę do tego pliku
  (1b) przykładowa ścieżka to: C:/Users/luqasz/Desktop/tekst.txt
  (2) następnym krokiem jest podanie miejsca, gdzie ma być zapisany plik
  (2a) może to być ta sama lokalizacja i ten sam plik, lecz wtedy będzie plik nadpisany
  (2b) jeśli chcemy zapisać do innego pliku to też można, lecz także będzie on nadpisany
  (2c) jeśli chcemy zapisać wynik działania to wtedy można stworzyć nowy plik w nowym miejscu
  (2d) przykładowo, stworzenie nowego pliku w danym miejscu to: C:/Users/luqasz/Desktop/wynik.txt
  (3) wybranie algorytmu szyfrującego/deszyfrującego, czyli algorytm AES bądź algorytm DES
  (3a) algorytm AES jest bardziej bezpieczny i trudniejszy do złamania
  (3b) algorytm DES jest krótszy i też trochę prostszy do złamania
  (4) po wybraniu algorytmu trzeba wybrać, czy chcemy szyfrować, czy deszyfrować tekst w pliku
  (4a) po wybraniu szyfrowania będzie stworzony zaszyfrowany tekst w nowym lub istniejącym pliku
  (4b) po wybraniu deszyfrowania będzie stworzony odszyfrowany tekst w nowym lub istniejącym pliku

Kontynuując, kolejną metodą jest wspomniana wcześniej metoda ‘public static (string, string) SzyfrowanieDeszyfrowanieTekstuPliku()’, która prosi użytkownika o podanie ścieżki pliku z danymi do zaszyfrowania / odszyfrowania oraz ścieżki dla nowego pliku, gdzie będą zapisane dane po szyfrowaniu / odszyfrowaniu (istnieje możliwość nadpisania już istniejącego pliku, skąd zostały pobrane dane do szyfrowania). Po podaniu wyżej wspomnianych ścieżek program ponownie prosi o prosi o wciśnięcie dowolnego klawisza, aby przejść do kolejnej metody, czyli ‘public static void WyborAlgorytmuAESlubDES(string SciezkaPlikuDoWczytania, string SciezkaPlikuDoZapisania)’.

Po przejściu do metody ‘WyborAlgorytmuAESlubDES()’ program prosi użytkownika o wybranie algorytmu szyfrującego, a więc AES bądź DES. Po wybraniu konkretnego algorytmu szyfrowania plik zostaje zaszyfrowany bądź odszyfrowany w zależności od wybranej opcji.

Podsumowując, niniejsza aplikacja konsolowa umożliwia nie tylko szyfrowanie i deszyfrowanie, ale też pokazuje, jak ona działa oraz jak może ona zostać zaimplementowana. Mimo tego, iż zabrakło czasu na to, aby dobrze to zaimplementować jako aplikację konsolową to można w przyszłości jeszcze udoskonalić działanie całego programu.

Jednym z udoskonaleń, które udało się zaimplementować to sposób szyfrowania, a więc stworzenie bardziej złożonego, trudniejszego kodu do złamania (przy AES jest bardziej złożony niż na początku tworzenia projektu). Można to zaobserwować, chociażby, przy stworzeniu pliku tekstowego .txt, gdzie znajduje się tekst ‘ALA MA KOTA’. Można zaszyfrować dane kilka razy, ale musi być zawsze odszyfrowany tym samym algorytmem, którym był szyfrowany [chodzi o kolejność].

Opis działania programu, aplikacji konsolowej C# opisał Łukasz W. Tworzydło.

Dane studenta:
=> Imię i nazwisko: Łukasz Tworzydło
=> Numer albumu: gd29623
=> Nr. kierunku: INIS4_PR2.2
=> Przedmiot: Programowanie .NET