|  |  |
| --- | --- |
| Akademia Nauk Stosowanych w Nowym Sączu | |
| Przedmiot: Teoretyczne i technologiczne podstawy multimediów. | |
| Imię i nazwisko: Jakub Kozub | Kierunek: Informatyka stosowana 3 (s) |
| Data: 04.10.2022 | Grupa: L2 |
| Temat: Napisz własny program szyfrujący z zastosowaniem algorytmu szyfrującego. | |

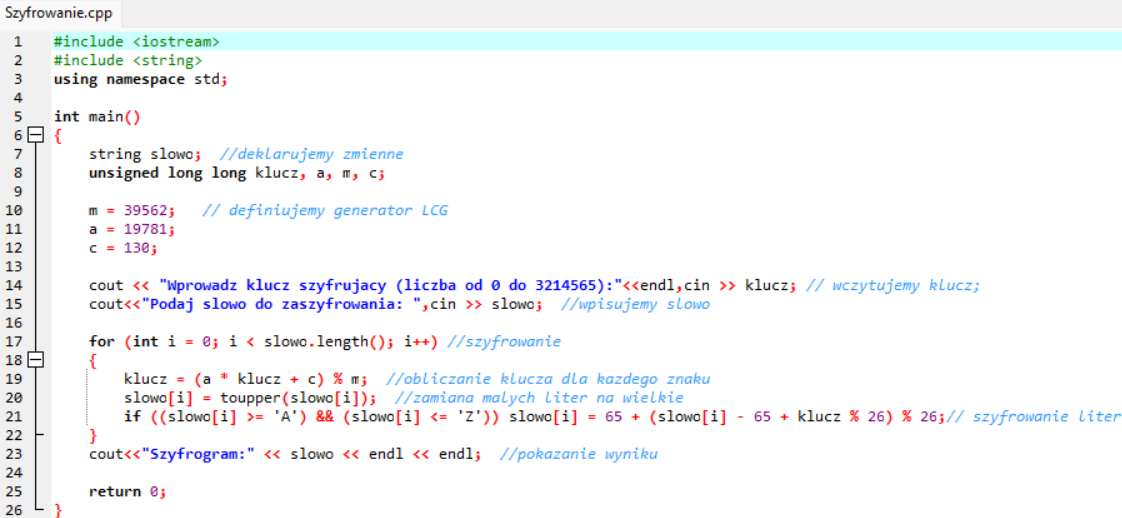
1. Algorytm szyfrujący.  
 Algorytm wykorzystujący funkcje matematyczne w celu szyfrowania i deszyfrowania jawnego tekstu. Zaszyfrowany tekst jest nazywany szyfrogramem. Algorytmy dzielą się na dwie główne grupy:  
 -Algorytm ograniczony - nie ma wysokiego poziomu bezpieczeństwa i jest skuteczny tylko wtedy, gdy nie jest znana jego postać.

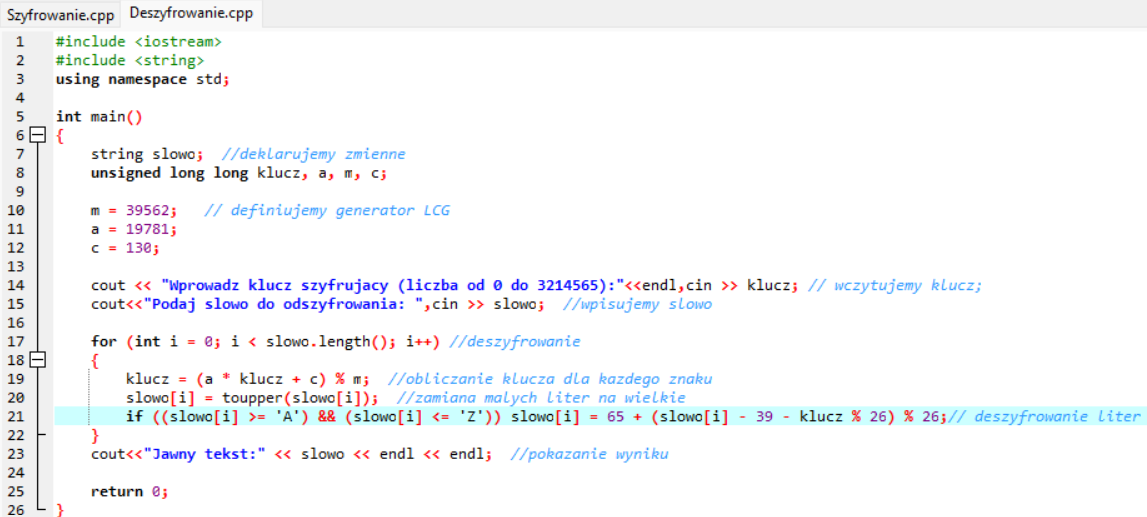
- Algorytmy z kluczem - wykorzystuje klucz, na którym oparte jest bezpieczeństwo i bez którego nie ma możliwości zaszyfrowania i odszyfrowania wiadomości.   
Algorytmy szyfrujące są wykorzystywane w celu ochrony informacji przed odczytem osób lub instytucji nieodpowiednich, uwierzytelniania dokumentów oraz zapewnienia wysokiego poziomu prywatności.

2. Algorytm szyfrujący i deszyfrujący z pseudolosowym odstępem wybranym przez użytkownika to algorytm wykorzystujący do szyfrowania znaków generator liczb pseudolosowych LCG. Po wybraniu przez użytkownika tzw. klucza szyfrującego, którym jest liczba od 0 do 3956279999, generator LCG tworzy ciąg liczb pseudolosowych służących do szyfrowania danego słowa przez wyliczenie ich ze wzoru wykorzystującego wprowadzony klucz jak i również wcześniej zadeklarowane w programie dane: klucz = (a \* klucz + c) % m; gdzie a to mnożnik, c to przyrost, m – moduł. Im dane wartości są większe, tym bardziej skomplikowany i bezpieczny jest klucz szyfrujący. Użytkownik, wpisuje tylko jedną wartość szyfrującą, a pozostałem muszą się zgadzać, żeby obliczane wartości dotyczące znaków były takie same.

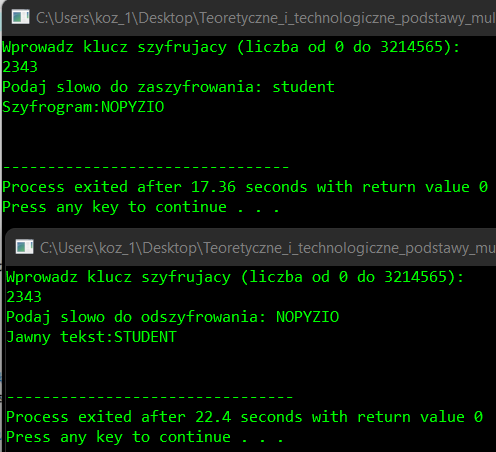
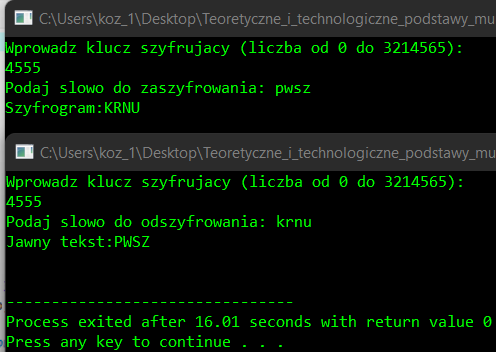
Każdy znak w słowie, które chcemy zaszyfrować musi być wielką literą, więc program zawiera warunek sprawdzający daną zależność. Po tym, obliczamy dla każdego znaku jego kod w pętli trwającej tyle, ile wynosi długość słowa i przypisywany jest on jako element szyfrogramu.

3. Kod programu szyfrującego i deszyfrującego z opisanymi funkcjami:





4. Rezultaty działania programu.

5. Wnioski.  
 Algorytm szyfrujący i deszyfrujący z pseudolosowym odstępem jest małym udogodnieniem popularnego algorytmu Cezara, gdyż przesunięcie jest wyliczane z kilku zmiennych i trudniej jest je odkryć, a także nie jest takie samo dla wszystkich znaków, co zwiększa bezpieczeństwo szyfrogramu. Sam kod algorytmu nie jest skomplikowany, a czytelny i intuicyjny, zwłaszcza po poznaniu wzorów na tworzenie kluczy szyfrujących. Samo pojęcie szyfrowania danych jest ciekawe i możliwe na wiele sposobów z różnym stopniem bezpieczeństwa.