Spis treści

Szyfr AtBash

Funkcje

1. Różne kodowania znaków:
    a. zmiana ogonków na odpowiedniki – jeśli tekst szyfrowany będzie zawierał polskie znaki, program zamieni je na odpowiedniki, np. ó zamieni na o, ź na z itd.
    b. w oparciu o polski alfabet – szyfrowanie z użyciem 32 znaków, inne znaki pomijane

c. w oparciu o angielski alfabet – szyfrowanie z użyciem 26 znaków, inne znaki pomijane

2. Odczytywanie i zapisywanie szyfrogramu z pliku

Użycie

```
Usage: AtBash.exe [options] [args]

Atbash is a simple substitution cipher for the Hebrew alphabet.

Options:
  --version   show program's version number and exit
  -h, --help  show this help message and exit
  -d          tryb deszyfrowania
  -l LANG     ustawienie kodowania tekstu:
              0 - zamiana znakow diakrytycznych na ich odpowiedniki
              1 - kodowanie dla angielskiego alfabetu
              2 - kodowanie dla polskiego alfabetu
  -f FILE     wskaz plik z tekstem do (de)szyfrowania
```

Przykłady

- szyfrowanie z użyciem polskich liter, przełącznik `-l 2`

```
AtBash.exe -l 2

Szyfr AtBash

       Autor: Lukasz Banasiak <lukasz@banasiak.me>
   Kodowanie: dla polskiego alfabetu

 IN> gęślą jaźń
OUT> rśęnź ożąk
```

- w oparciu o angielski alfabet `-l 1`

```
 IN> gęślą jaźń
OUT> tęśoą qzźń
```

- zamiana znaków na odpowiedniki (domyślnie)

```
 IN> gęślą jaźń
OUT> tvhoz qzam

 IN> gesla jazn
OUT> tvhoz qzam
```

- odszyfrowanie, przełącznik `-d`

```
AtBash.exe -d

Szyfr AtBash

       Autor: Lukasz Banasiak <lukasz@banasiak.me>
   Kodowanie: zamiana znakow diakrytycznych na ich odpowiedniki

 IN> tvhoz qzam
OUT> gesla jaźń
```

- wczytanie pliku do odszyfrowania/zaszyfrowania, przełącznik `-f`

```
AtBash.exe -f pl.txt
```

```
Szyfr AtBash

       Autor: Lukasz Banasiak <lukasz@banasiak.me>
   Kodowanie: zamiana znakow diakrytycznych na ich odpowiedniki

 IN> pl.txt
OUT> _pl.txt
```

Szyfr Bacon'a

Funkcje

1. Zmiana polskich ogonków na odpowiedniki - jJeśli tekst szyfrowany będzie zawierał polskie znaki zamieni je na odpowiedniki, np. ó zamieni na o, ź na z itd.
2. Odczytywanie i zapisywanie szyfrogramu z pliku

Użycie

```
Usage: Bacon.exe [options] [args]

Method of steganography devised by Francis Bacon in 1605.

Options:
  --version   show program's version number and exit
  -h, --help  show this help message and exit
  -d          tryb deszyfrowania
  -f FILE     wskaz plik z tekstem do (de)szyfrowania
```

Przykłady

- zamiana znaków na odpowiedniki (domyślnie)

```
Bacon.exe

Szyfr Bacona

       Autor: Lukasz Banasiak <lukasz@banasiak.me>
        Tryb: Szyfrowanie

 IN> gęślą jaźń
OUT> AABBAAABAABAABAABABBAAAAAABAABAAAAABBAABABBAB

 IN> gesla jazn
OUT> AABBAAABAABAABAABABBAAAAAABAABAAAAABBAABABBAB
```

- deszyfrowanie

```
Bacon.exe -d

Szyfr Bacona

       Autor: Lukasz Banasiak <lukasz@banasiak.me>
        Tryb: Deszyfrowanie

 IN> AABBAAABAABAABAABABBAAAAAABAABAAAAABBAABABBAB
OUT> GESLAJAZN
```

- wczytanie pliku do odszyfrowania/zaszyfrowania, przełącznik `-f`

```
 IN> pl.txt
OUT> _pl.txt
```

Szyfr Delastelle'a

Funkcje

1. Zmiana polskich ogonków na odpowiedniki – jeśli tekst szyfrowany będzie zawierał polskie znaki zamieni je na odpowiedniki, np. ó zamieni na o, ź na z itd.
2. Możliwość ustawienia własnego klucza transformacji szachownicy
3. Możliwość włączenia trybu pokazujące stany pośrednie
4. Odczytywanie i zapisywanie szyfrogramu z pliku

Użycie

```
Usage: Bifid.exe [options] [args]

Bifid cipher is a cipher which combines the Polybius square with
transposition, and uses fractionation to achieve diffusion.

Options:
  --version   show program's version number and exit
  -h, --help  show this help message and exit
  -d          tryb deszyfrowania
  -k KEY      klucz transformacji szachownicy
  -V          pokazuje posrednie etapy
  -f FILE     wskaz plik z tekstem do (de)szyfrowania
```

Przykłady

- transformacja szachownicy o słowo KLUCZ, przełącznik `-k klucz`

```
Bifid.exe -k klucz

Szyfr Delastelle'a

       Autor: Lukasz Banasiak <lukasz@banasiak.me>
        Tryb: Szyfrowanie
Tryb verbose: Nie
 Szachownica:
      1   2   3   4   5
 1 [  K   L   U   C   Z  ]
 2 [  A   B   D   E   F  ]
 3 [  G   H   I   M   N  ]
 4 [  O   P   Q   R   S  ]
 5 [  T   V   W   X   Y  ]

 IN> gęślą jaźń
OUT> HOBUCVKY
```

- pokazanie pośrednich etapów, przełącznik `-V`

```
Bifid.exe -k klucz -V

Szyfr Delastelle'a

       Autor: Lukasz Banasiak <lukasz@banasiak.me>
        Tryb: Szyfrowanie
Tryb verbose: Tak
 Szachownica:
      1   2   3   4   5
 1 [  K   L   U   C   Z  ]
 2 [  A   B   D   E   F  ]
 3 [  G   H   I   M   N  ]
 4 [  O   P   Q   R   S  ]
 5 [  T   V   W   X   Y  ]
```

```
 IN> gęślą jaźń
  1: 31 24 45 12 21 21 15 35  # po wyznaczeniu wspolrzednych
  2: 32 11 22 41 41 55 13 25  # po transformacji poziomej
OUT> HOBUCVKY
```

- zamiana znaków na odpowiedniki (domyślnie)

```
 IN> gęślą jaźń
OUT> HOBUCVKY

 IN> gesla jazn
OUT> HOBUCVKY
```

- wczytanie pliku do odszyfrowania/zaszyfrowania, przełącznik `-f`

```
 IN> pl.txt
OUT> _pl.txt
```

Szyfr Cezara

Funkcje

1. Ustawianie przesunięcie
2. Różne kodowania znaków:
    a. zmiana ogonków na odpowiedniki – jeśli tekst szyfrowany będzie zawierał polskie znaki, program zamieni je na odpowiedniki, np. ó zamieni na o, ź na z itd.
    b. w oparciu o polski alfabet – szyfrowanie z użyciem 32 znaków, inne znaki pomijane
    c. w oparciu o angielski alfabet – szyfrowanie z użyciem 26 znaków, inne znaki pomijane
3. Odczytywanie i zapisywanie szyfrogramu z pliku

Użycie

```
Usage: Caesar.exe [options] [args]

In cryptography a Caesar cipher is one of the simplest and most widely known encryption
techniques.

Options:
  --version   show program's version number and exit
  -h, --help  show this help message and exit
  -d          tryb deszyfrowania
  -s SHIFT    liczba przesuniecia wzgledem pierwszej litery alfabetu
  -l LANG     ustawienie kodowania tekstu:
              0 - zamiana znakow diakrytycznych na ich odpowiedniki
              1 - kodowanie dla angielskiego alfabetu
              2 - kodowanie dla polskiego alfabetu
  -f FILE     wskaz plik z tekstem do (de)szyfrowania
```

Przykłady

Jeśli chcemy użyć kodowania ROT13 ustawiamy przesunięcie na 13 :

- z użyciem polskich liter uruchamiamy program ze zmiennymi `-s 13 -l 2`

```
Caesar.exe -s 13 -l 2

Szyfr Cezara
```

```
      Autor: Lukasz Banasiak <lukasz@banasiak.me>
   Kodowanie: dla polskiego alfabetu
Przesuniecie: 13
       Tryb: Szyfrowanie

 IN> gęślą jaźń
OUT> ródwl tkiż
```

- w oparciu o angielski alfabet `-s 13 -l 1`

```
 IN> gęślą jaźń
OUT> tęśyą wnźń
```

- zamiana znaków na odpowiedniki (domyślnie) `-s 13`

```
 IN> gęślą jaźń
OUT> trfyn wnma

 IN> gesla jazn
OUT> trfyn wnma
```

- wczytanie pliku do odszyfrowania/zaszyfrowania, przełącznik `-f`

```
 IN> pl.txt
OUT> _pl.txt
```

Szyfr Polibiusza

Funkcje

1. Zmiana polskich ogonków na odpowiedniki – jeśli tekst szyfrowany będzie zawierał polskie znaki zamieni je na odpowiedniki, np. ó zamieni na o, ź na z itd.
2. Możliwość ustawienia własnego klucza transformacji szachownicy
3. Reprezentacja szyfru nie ma wpływu na deszyfrację, np. `42aaaa 41 1233 512414 32 35` `331121ddddsss` jest równoważne `42 41 12 33 51 24 14 32 35 33 11 21`
4. Odczytywanie i zapisywanie szyfrogramu z pliku

Użycie

```
Usage: Polybius.exe [options] [args]

In cryptography the Polybius square is a device for fractionating plaintext
characters.

Options:
  --version   show program's version number and exit
  -h, --help  show this help message and exit
  -d          tryb deszyfrowania
  -k KEY      klucz transformacji szachownicy
  -f FILE     wskaz plik z tekstem do (de)szyfrowania
```

Przykłady

- transformacja szachownicy o słowo KLUCZ, przełącznik `-k klucz`

```
Polybius.exe -k klucz

Szachownica Polibiusza
```

```
       Autor: Lukasz Banasiak <lukasz@banasiak.me>
        Tryb: Szyfrowanie
 Szachownica:
      1   2   3   4   5
 1 [  K   L   U   C   Z  ]
 2 [  A   B   D   E   F  ]
 3 [  G   H   I   M   N  ]
 4 [  O   P   Q   R   S  ]
 5 [  T   V   W   X   Y  ]

 IN> gęślą jaźń
OUT> 31 24 45 12 21 21 15 35
```

- zamiana znaków na odpowiedniki (domyślnie)

```
 IN> gęślą jaźń
OUT> 31 24 45 12 21 21 15 35

 IN> gesla jazn
OUT> 31 24 45 12 21 21 15 35
```

- deszyfrowanie z użyciem klucza, przełącznik `-k klucz -d`

```
Polybius.exe -k klucz -d

Szachownica Polibiusza

       Autor: Lukasz Banasiak <lukasz@banasiak.me>
        Tryb: Deszyfrowanie
 Szachownica:
      1   2   3   4   5
 1 [  K   L   U   C   Z  ]
 2 [  A   B   D   E   F  ]
 3 [  G   H   I   M   N  ]
 4 [  O   P   Q   R   S  ]
 5 [  T   V   W   X   Y  ]

 IN> 31 24 45 12 21 21 15 35
OUT> GESLAAZN
```

- format szyfru nie ma wpływu na deszyfrację

```
IN> 42aaaa 41 1233 512414    32 35 331121ddddsss
OUT> POLITECHNIKA
```

- wczytanie pliku do odszyfrowania/zaszyfrowania, przełącznik `-f`

```
 IN> pl.txt
OUT> _pl.txt
```

Częstotliwość występowania znaków

Funkcje

1. Możliwość zliczania wszystkich znaków albo tylko liter
2. Interpretacja danych rozróżnianiem semantyki liter małych i wielkich.
3. Wyliczanie procentu dla danej liczby
4. Odczytywanie tekstu z pliku

Użycie

```
CharFreq.exe --help
Usage: CharFreq.exe [options] [args]

In cryptanalysis, frequency analysis is the study of the frequency of letters
or groups of letters in a ciphertext.

Options:
  --version   show program's version number and exit
  -h, --help  show this help message and exit
  -a          zliczaj wszystkie znaki
  -c          rozroznianie semantyki malych i wielkich liter
  -f FILE     wskaz plik z tekstem
```

Przykłady

- zliczenie tylko liter oraz nie rozróżnianie wielkości liter na przykładzie Pana Tadeusza, (domyślnie), przełącznik `-f`

```
CharFreq.exe -f pan_tadeusz.txt

Czestotliwosc wystepowania znakow

       Autor: Lukasz Banasiak <lukasz@banasiak.me>
        Tryb: Zliczanie tylko liter
 Case-sensi.: Nie

 IN> pan_tadeusz.txt
  A: 14589  (8.96%)
  I: 13997  (8.59%)
  E: 11062  (6.79%)
  O: 10995  (6.75%)
  Z: 10485  (6.44%)
  S: 8073  (4.96%)
  N: 7711  (4.73%)
  W: 7482  (4.59%)
  R: 7227  (4.44%)
  C: 6652  (4.08%)
  Y: 6215  (3.82%)
  K: 5933  (3.64%)
  D: 5598  (3.44%)
  T: 5313  (3.26%)
  M: 4908  (3.01%)
  Ł: 4773  (2.93%)
  P: 4232  (2.60%)
  U: 3733  (2.29%)
  L: 3288  (2.02%)
  J: 3154  (1.94%)
  B: 2833  (1.74%)
  Ę: 2410  (1.48%)
  G: 2365  (1.45%)
  Ą: 2143  (1.32%)
  H: 1966  (1.21%)
  Ż: 1533  (0.94%)
  Ó: 1420  (0.87%)
  Ś: 1245  (0.76%)
  Ć: 844  (0.52%)
  Ń: 283  (0.17%)
  Ź: 212  (0.13%)
  F: 175  (0.11%)
  V: 6  (0.00%)
  X: 6  (0.00%)
  +: 162861
```

- rozróżnianie wielkości liter na przykładzie Hamleta, przełącznik `-c`

```
CharFreq.exe -f hamlet.txt -c

Czestotliwosc wystepowania znakow

      Autor: Lukasz Banasiak <lukasz@banasiak.me>
       Tryb: Zliczanie tylko liter
 Case-sensi.: Tak

 IN> hamlet.txt
  e: 14657  (11.32%)
  t: 11034  (8.52%)
  o: 10790  (8.33%)
  a: 9274  (7.16%)
  s: 8085  (6.24%)
  n: 8079  (6.24%)
  h: 7828  (6.04%)
  i: 7618  (5.88%)
  r: 7580  (5.85%)
  l: 5569  (4.30%)
  d: 4876  (3.76%)
  u: 4288  (3.31%)
  m: 3987  (3.08%)
  y: 3070  (2.37%)
  w: 2642  (2.04%)
  f: 2483  (1.92%)
  c: 2413  (1.86%)
  g: 2161  (1.67%)
  p: 1775  (1.37%)
  b: 1564  (1.21%)
  v: 1187  (0.92%)
  k: 1088  (0.84%)
  H: 884  (0.68%)
  I: 853  (0.66%)
  T: 785  (0.61%)
  A: 625  (0.48%)
  W: 484  (0.37%)
  O: 370  (0.29%)
  B: 261  (0.20%)
  S: 250  (0.19%)
  M: 247  (0.19%)
  G: 245  (0.19%)
  L: 245  (0.19%)
  E: 230  (0.18%)
  P: 227  (0.18%)
  F: 196  (0.15%)
  x: 179  (0.14%)
  K: 178  (0.14%)
  N: 175  (0.14%)
  C: 170  (0.13%)
  R: 134  (0.10%)
  Y: 129  (0.10%)
  D: 126  (0.10%)
  Q: 111  (0.09%)
  q: 108  (0.08%)
  j: 101  (0.08%)
  z: 71  (0.05%)
  U: 36  (0.03%)
  V: 32  (0.02%)
  J: 9  (0.01%)
  +: 129509
```

- zliczanie wszystkich znaków, nie rozróżnianie wielkości liter na przykładzie Hamleta, przełącznik `-a`

```
CharFreq.exe -f hamlet.txt -a

Czestotliwosc wystepowania znakow

      Autor: Lukasz Banasiak <lukasz@banasiak.me>
       Tryb: Zliczanie wszystkich znakow
 Case-sensi.: Nie

 IN> hamlet.txt
   : 47747  (25.61%)
  E: 14887  (7.98%)
  T: 11819  (6.34%)
  O: 11160  (5.99%)
  A: 9899  (5.31%)
  H: 8712  (4.67%)
  I: 8471  (4.54%)
  S: 8335  (4.47%)
  N: 8254  (4.43%)
  R: 7714  (4.14%)
  L: 5814  (3.12%)
  D: 5002  (2.68%)
  U: 4324  (2.32%)
  M: 4234  (2.27%)
  Y: 3199  (1.72%)
  W: 3126  (1.68%)
  .: 3108  (1.67%)
  ,: 2972  (1.59%)
  F: 2679  (1.44%)
  C: 2583  (1.39%)
  G: 2406  (1.29%)
  P: 2002  (1.07%)
  B: 1825  (0.98%)
  K: 1266  (0.68%)
  V: 1219  (0.65%)
  ': 1201  (0.64%)
  ?: 452  (0.24%)
  ;: 442  (0.24%)
  !: 373  (0.20%)
  -: 298  (0.16%)
  Q: 219  (0.12%)
  X: 179  (0.10%)
  [: 116  (0.06%)
  ]: 112  (0.06%)
  J: 110  (0.06%)
  Z: 71  (0.04%)
  (: 44  (0.02%)
  ): 43  (0.02%)
  :: 32  (0.02%)
  1: 6  (0.00%)
  ": 1  (0.00%)
  &: 1  (0.00%)
  +: 186457
```