

Kryptografia

Laboratorium nr 1

Stefan Sokołowski

Zadanie 1:

Proszę napisać programy szyfrujące i deszyfrujące wg prostych zasad omówionych w wykładzie 1 (iis.ans-elblag.pl/~stefan/Dydaktyka/Krypto/Slajdy/01a.pdf):

- (a) „szyfr dla dzieci” — [str. 2](#)
- (b) szyfr Cezara z dowolnym (podawanym przez użytkownika) kluczem — [str. 3](#)
- (c) przestawianie za pomocą kwadratowej tabelki (jej wielkość program szyfrujący i program deszyfrujący powinny wyliczać po wczytaniu tekstu) — [str. 4](#)
- (d) podstawienia z kluczem (podawanym przez użytkownika) — [str. 8](#)

Zadanie 2 (domowe na punkty):

Proszę napisać program szyfrujący i program deszyfrujący dla następującej metody szyfrowania:

Tekst jawny dzielimy na bloki po 16 liter; ew. ostatni blok dopełniamy spacjami do 16.

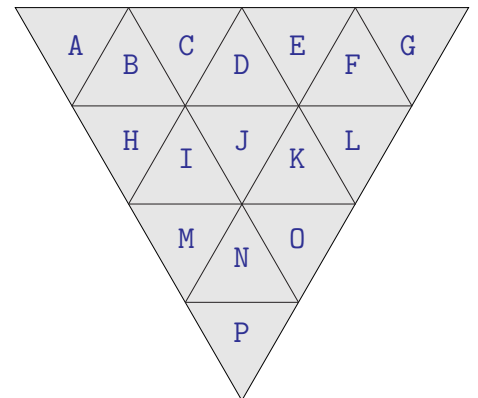
Potem każdy blok liter z osobna szyfrujemy przestawieniowo przy pomocy takiego „trójkąta z trójkącików” jak na rysunku obok. Mianowicie jego litery wpisujemy do trójkącików po jednej, **wiersz za wierszem**, zaczynając od górnego wiersza. Następnie duży trójkąt obracamy o 120° w kierunku ruchu wskazówek (przestarzałego) zegara. Potem z trójkącików w tym obróconym trójkącie wypisujemy litery wiersz za wierszem.

W przykładzie obok z wejściowego tekstu jawnego

ABCDEF GHI JKLMNOP

powstanie szyfrogram

PNMIHBAOKJDCLFEG



Uwaga:

Czas na przysłanie (na s.sokolowski@ans-elblag.pl): 2 tygodnie od zajęć 1 — potem już nie przyjmuję rozwiązań. Liczba punktów zależy od oryginalności i elegancji rozwiązania. W mailu proszę koniecznie podać swoje **nazwisko**, **numer zajęć** i **numer zadania**.
