Szyfry podstawieniowe polialfabetyczne

Z1. Napisać program szyfrujący i deszyfrujący przy użyciu wybranych szyfrów podstawieniowych polialfabetycznych.

WYMAGANIA PODSTAWOWE

1. otwieranie tekstu i klucza z plików, zapisywanie wyników do pliku.
2. możliwość wyboru szyfrowania lub deszyfrowania.
3. szyfrowanie alfabetu 26-znakowego, pozostałe znaki są usuwane,
4. wybranie jednego z szyfrów polialfabetycznych,

WYMAGANIA DODATKOWE

5. kontrola błędów,
6. wybranie co najmniej dwóch szyfrów polialfabetycznych,
7. możliwość szyfrowania więcej niż 26-znaków np. z cyframi, spacjami itd.

Z2. Dokonać próby ataku na szyfr Vigenère'a.

WYMAGANIA PODSTAWOWE

1. pobrać pliki vigenere_szyfrogram.txt
2. wyszukać odpowiednie metody i spróbować znaleźć klucz bez znajomości tekstu jawnego,
3. opisać wszystkie próby w sprawozdaniu,

WYMAGANIA DODATKOWE

4. znaleźć klucz znając tekst jawny,
5. odszyfrować szyfrogram znając klucz.

Z3. Dokonać próby ataku na szyfr Hilla.

WYMAGANIA PODSTAWOWE

1. pobrać pliki hill_szyfrogram.txt
2. wyszukać odpowiednie metody i spróbować znaleźć klucz bez znajomości tekstu jawnego (macierz $2x2$),

3. opisać wszystkie próby w sprawozdaniu,

WYMAGANIA DODATKOWE

4. znaleźć klucz znając tekst jawny,
5. odszyfrować szyfrogram znając klucz.