Klasyczne szyfry podstawieniowe

Z1. Zaimplementować algorytm kryptograficzny z wybranym szyfrem monoalfabetycznym.

WYMAGANIA PODSTAWOWE
Napisać funkcję, która:

1. usuwa znaki białe i interpunkcyjne,
2. zamienia litery na małe / na wielkie,
3. usuwa z liter symbole diakrytyczne (zamiana ą na a itd.),
4. usuwa cyfry,
5. formatu tekst w 7 kolumn po 5 znaków oddzielonych spacjami,
6. tekst wczytuje z/do plików wskazanych przez użytkownika (w pliku demo lub pobiera z konsoli),
7. otwiera wskazany przez użytkownika plik,
8. szyfruje tekst (wielkie litery) wybranymi algorytmami i zapisuje do pliku,
9. deszyfruje (małe litery) i zapisuje do pliku.

WYMAGANIA DODATKOWE

10. kontrola błędów,
11. ulepszenie usuwania znaków diakrytycznych (inne języki),
12. zaimplementowanie większej ilości wybranych szyfrów monoalfabetycznych.

Z2. Szyfr Bifid.

WYMAGANIA PODSTAWOWE

1. usuń zbędne znaki,
2. zaimplementuj szyfrowanie i odszyfrowanie tekstu zaszyfrowanego szyfrem Bifid, korzystając z macierzy Polibiusza,
3. wyświetl wynik na ekranie.

WYMAGANIA DODATKOWE

4. zoptymalizuj szyfrowanie tak, aby obsługiwało dłuższe wiadomości tekstowe,
5. pobieraj tekst z pliku,
6. wynik zapisuj do pliku,
7. dodaj kontrolę błędów.

Z3. Porównaj dwa wybrane, proste szyfry monoalfabetyczne.

WYMAGANIA PODSTAWOWE

1. usuń zbędne znaki,
2. zaimplementuj dwa wybrane szyfry,
3. porównaj ich złożoność czasową,
4. wyjaśnij różnice w efektywności tych szyfrów na przykładzie zaszyfrowania 1000-znakowego tekstu.

WYMAGANIA DODATKOWE

5. zaproponuj optymalizacje algorytmów, które mogłyby poprawić ich działanie dla bardzo dużych danych,
6. wypisz, jakie słabości mają te szyfry.

Z4. Szyfrowanie tekstu w różnych językach.

WYMAGANIA PODSTAWOWE

1. usuń zbędne znaki,
2. zaimplementuj szyfr Cezara (dla n liter, w zależności od wybranego alfabetu),
3. zbadaj, jak różne języki (np. polski, angielski, francuski) wpływają na efektywność szyfru Cezara (ze względu na różne częstotliwości liter).

WYMAGANIA DODATKOWE

4. zaproponuj, jak można dostosować szyfr Cezara do języków, które nie używają alfabetu łacińskiego.