Zaprogramować szyfrowanie i odszyfrowywanie wiadomości przy użyciu szyfru Cezara i szyfru afinicznego.

Program o nazwie cezar powinien umożliwiać wywołanie z linijki rozkazowej z następującymi opcjami:

-c (szyfr Cezara),
-a (szyfr afiniczny),
-e (szyfrowanie),
-d (odszyfrowywanie),
-j (kryptoanaliza z tekstem jawnym),
-k (kryptoanaliza wyłącznie w oparciu o kryptogram)

Program będzie czytał dane z pewnych plików i zapisywał na inne, nazwy tych plików są z góry ustalone:

plain.txt: plik z tekstem jawnym,
crypto.txt: plik z tekstem zaszyfrowanym,
decrypt.txt: plik z tekstem odszyfrowanym,
key.txt: plik zawierający klucz,
extra.txt: plik zawierający pomocniczy tekst jawny w przypadku kryptoanalizy z tekstem jawnym i zaszyfrowanym,
key-found.txt: plik zawierający znaleziony klucz w przypadku kryptoanalizy z tekstem jawnym i zaszyfrowanym.

- Program szyfrujący czyta tekst jawny i klucz i zapisuje tekst zaszyfrowany. Jeśli klucz jest nieprawidłowy, zgłasza jedynie błąd.
- Program odszyfrowujący czyta tekst zaszyfrowany i klucz i zapisuje tekst jawny. Jeśli klucz jest nieprawidłowy, zgłasza błąd. Dla szyfru afinicznego częścią zadania jest znalezienie odwrotności dla liczby *a* podanej jako część klucza – nie można zakładać, że program odszyfrowujący otrzymuje tę odwrotność.
- Program łamiący szyfr z pomocą tekstu jawnego czyta tekst zaszyfrowany, tekst pomocniczy i zapisuje obliczony klucz i odszyfrowany tekst. Jeśli niemożliwe jest obliczenie klucza, zgłasza sygnał błędu.
- Program łamiący szyfr bez pomocy tekstu jawnego czyta jedynie tekst zaszyfrowany i zapisuje jako tekst jawny wszystkie możliwe kandydatury (25 dla szyfru Cezara, 312 dla szyfru afinicznego).
- Program w żadnym wypadku nie ma prawa żądać istnienia plików niewymaganych dla danej opcji. Pliki, do których zapisujemy powinny być utworzone gdyby nie istniały.

Technologia:

Program może być napisany w dowolnym języku programowania (C, C++, C#, Java, python, ruby, golang, racket, Haskell, rust, awk, bash, tcl, php, perl, pascal, ...) pod warunkiem spełnienia powyższych warunków. (Mogę ustąpić, jeśli zajdzie wyższa konieczność, np. przygotowanie odpowiedniego arkusza Excela.)

Rozwiązanie powinno obejmować źródła programu, ew. wersja skompilowana jest opcjonalna (choć pożądana, gdy np. przygotowano program w Javie w środowisku Windows), oraz

przykładowy tekst jawny, zaszyfrowany i poprawny klucz dla szyfru afinicznego. Przesyłać należy pakiet tar lub zip.