Hjemmeoppgave: Cæsars kode

Gratulerer! Du har gjort spesielt god figur og er videre fra førstegangsintervjuet! Nå gleder vi oss til andregangsintervjuet hvor du skal få vise frem alt det tekniske du kan.

Hvorfor gir vi hjemmeoppgaver?

Istedenfor å bare snakke om programmering, har vi lyst til å se på noe kode du har skrevet. Vi tror at tekniske samtaler blir bedre hvis vi tar utgangspunkt i noe konkret, i stedet for bare å snakke løst rundt ulike tekniske begreper. I tillegg tror vi ikke at folk nødvendigvis får vist frem det de kan "på sparket" foran en tavle på selve intervjuet. Derfor har vi lyst til at du lager en implementasjon av kryptering med Cæsars kode som et utgangspunkt til en teknisk samtale i andregangsintervjuet.

Kryptering med Cæsars kode

I denne oppgaven skal du lage et program som leser inn en tekstfil og krypterer innholdet med Cæsars kode (https://no.wikipedia.org/wiki/C%C3%A6sarchiffer).

Hvordan fungerer Cæsars kode?

Cæsars kode er en enkel substitusjonskode, hvor man bytter ut hver bokstav i teksten som skal krypteres med en bokstav et gitt antall plasser lengre bort i alfabetet.

Gitt at man koder ved å bruke bokstaver som er tre plasser lengre til høyre i alfabetet, vil ordet HALLO bli kodet som KDOOR. Under ser vi en illustrasjon av hvordan hver bokstav er flyttet tre plasser lengre til høyre i alfabetet under.

```
   ABCDEFGHIJKLMNOPQRSTUVWXYZÆØÅ
   |       |    |   |
ABCDEFGHIJKLMNOPQRSTUVWXYZÆØÅ
```

For å dekryptere teksten går man bare motsatt vei, og flytter hver bokstav tre plasser tilbake i alfabetet. På denne måten blir antallet plasser du må flytte hver bokstav nøkkelen du må vite for å dekryptere teksten.

Hva slags program skal jeg lage?

Dette er helt opp til deg, men programmet kan godt bare være en konsollapplikasjon som leser inn navnet på en fil med tekst, et tall som forteller hvor mange plasser man skal flytte hver bokstav og et flagg som forteller om innholdet skal krypteres eller dekrypteres. Resultatet kan godt skrives rett til terminalvinduet.

Det viktige er at programmet i det minste:

1. Kan lese inn innholdet av en tekstfil og kryptere eller dekryptere innholdet med Cæsars kode.
2. Kan ta inn et tall som bestemmer hvor mange plasser man skal flytte bokstavene i alfabetet.
3. Kan både kryptere og dekryptere tekst.

Eksempel på hvordan en løsning kan fungere

Gitt at du velger å implementere løsningen din som en konsollapplikasjon, er et mulig eksempel på hvordan programmet kan fungere vist under.

Kryptering:

```
$> caesar 7 plaintext.txt
lawlyplujlgpzgæolgælhjolygvmghssgæopunz
uvgvulgpzgzvgiyhålgæohægolgpzguvægkpzæøyilkgibgzvtlæopungøulawljælk
pgohkgyhæolygilgmpyzægpughgåpsshnlgæohugzljvukghægyvtl
tlugmyllsbgilsplålgæohæg opjogæolbgklzpyl
pgjhtlgpgzh gpgjvuxølylk
```

Dekryptering:

```
$> caesar 7 ciphertext-shift-7.txt -d
experience is the teacher of all things
no one is so brave that he is not disturbed by something unexpected
i had rather be first in a village than second at rome
men freely believe that which they desire
i came i saw i conquered
```

I eksempelet er “caesar” programmet, eller en måte å kjøre programmet på, og flagget “-d” brukes til å indikere at programmet skal dekryptere teksten.

Hva forventer vi?

Det er ikke meningen at du skal bruke år og dag på løsningen. Bruk tid på det du synes er gøy eller viktig å bruke tid på. Har du mye annet du skal gjøre? Lag en minimal løsning, så kan vi heller snakke om hva du ville ha gjort hvis du hadde bedre tid.

Lykke til! Vi gleder oss til å se hvordan du løser oppgaven!