Løsningsforslag til tilleggsoppgave Del 1

Gjett på tall ved hjelp av halveringsmetoden!

```
# Forslag til løsning på et program for å gjette på et tall mellom 0
# og det tallet du setter som topp

import random

print("Dette er et program som lagrer et tall mellom 0 og det tallet du velger.")
print("Så skal du gjette på hvilket tall programmet har lagret(random/tilfeldig)!")
print("Programmet vil fortelle om tallet er for høyt, for lavt eller riktig.")

topp = int(input("Skriv inn øvre grense for hvilket tall programmet skal tenke på."))

print("Da gjetter programmet på et tall mellom 0 og", topp, ".")

rett = False
tall = random.randint(0, topp)
gjettinger = 0

while rett == False:
  gjett=int(input("Skriv inn hvilket tall du tror programmet tenker på."))
  gjettinger = gjettinger + 1
  if gjett < tall:
    print("Tallet du skrev inn, er for lavt.")
  elif gjett > tall:
    print("Tallet du skrev inn, er for høyt.")
  else:
    print("Du gjettet helt rett!")
    rett = True

print(f"Du brukte {gjettinger} gjettinger på å komme fram til rett svar.")
```

Løsningsforslag til tilleggsoppgave Del 1

Passord, 3 muligheter, x sec. ventetid

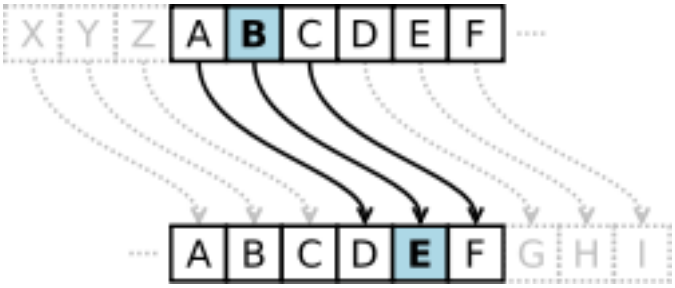
```
import time
Navn ="Gunnar Knutsen"
Adresse ="Kongetoppen"
Mail ="post@fellesfag.no"
Mobil ="93679342"

key = "namnam"
ant = 3

while ant >0:
    inn = str(input("Tast inn passord: "))
    if inn == key:
        print(f"Kult, du traff:\n  {Navn}\n  {Adresse}\n  {Mail}\n  {Mobil}\n\n")
    else:
        ant = ant - 1
        if ant > 0:
            print("Feil passord. Du har",ant, "forsøk igjen!")
        else:
            print("Du må vente i 10 sekunder før du kan forsøke igjen")
            time.sleep(10)
            ant =3
```

Denne øvelsen er gøy å bruke i forbindelse med krypteringsøvelser, slik som krypteringsmetoden Cæsar chiffer.

Løsningsforslag til tilleggsoppgave Del 1

Cæsar chiffer

Fra Wikipedia, den frie encyklopedi



Illustrasjon av Cæsar chiffer, her med en klassisk forskyvning på tre plasser i alfabetet.

Innen kryptografi er **Cæsar chiffer**, også kjent som **Caesars chiffer**, **skiftchiffer**, **Cæsars kode** og **Cæsar skift**, en av de enkleste og mest kjente krypteringsteknikker. Det er en type substitusjonschiffer der hver bokstav i klarteksten erstattes med en annen bokstav et gitt antall steg lenger ut i alfabetet. Med et skift på tre steg erstattes D med A, E med B, F med C og så videre. Metoden har navn etter Julius Cæsar som benyttet denne koden til å kommunisere med sine generaler.

Selv om Cæsar chiffer er meget enkelt, så inngår det likevel ofte i mer komplekse krypteringsstrukturer som vigenèrechifferet. En finner det også igjen i moderne anvendelser som ROT13. Cæsar chiffer i seg selv, som et monoalfabetisk substiusjonschiffer, er i dag et meget enkelt system å bryte og gir ingen kommunikasjonssikkerhet. Det egner seg imidlertid til en første introduksjon til kryptering.

Python Cæsar chiffer,

```
# Program for å kryptere tekst ved å forskyve plasser i alfabetet
# Vi benytter dette alfabetet
alfabet =
"abcdefghijklmnopqrstuvwxyzæøåABCDEFGHIJKLMNOPQRSTUVWXYZÆØÅ?!.,:-)(; "
# 68 TEGN
melding = "Andreas er ikke så hyggelig som alle tror!" # Melding som skal krypteres
key = 19 # Krypteringsnøkkel: antall plasser som forskyves
krypt_mld = "" # Variabel som skal inneholde den krypterte meldingen

for i in melding: # Starter en løkke som tar bokstav for bokstav i meldingen
    pos = alfabet.find(i) # Finner posisjon i alfabet
    pos = pos + key # Finner ny posisjon i alfabet
    if pos > 67: # Dersom posisjon blir for stor, så starter den å telle på nytt
        pos = pos - 68
    krypt_mld = krypt_mld + alfabet[pos] # Legger kryptert bokstav til den krypterte
meldingen

print(krypt_mld) # Skriver ut den krypterte meldingen
```

Løsningsforslag til tilleggsoppgave Del 1

Januar 2023 G. Knutsen