

# ◆ Kryptonøtt

*Skrevet av: Arve Seljebu*

*Oversatt av: Stein Olav Romslo*

*Kurs: Python*

*Tema: Tekstbasert*

*Fag: Programmering*

*Klassetrinn: 8.-10. klasse, Videregående skole*

## Introduksjon

Kryptering har vore i bruk i kommunikasjon lenge. Faktisk brukte dei det for nesten 4000 år sidan! I tillegg er det artig å sende hemmelege meldingar. Før du startar på denne oppgåva anbefalar me at du har gjort Hemmelege koder ([../hemmelige\\_koder/hemmelige\\_koder\\_nn.html](#)) fyrst.

Denne oppgåva er ei nøtt. Det vil seie at du skal finne ut av det meste sjølv. Står du heilt fast må du spørje nokon om hjelp.

## Kryptering med Vigenère-metoden

Vigenère er litt smartare enn krypteringa i Hemmelege koder ([../hemmelige\\_koder/hemmelige\\_koder\\_nn.html](#)), men den er ikkje så annleis. Det er viktig at du forstår koden frå den oppgåva, sidan du skal lage nesten lik kode sjølv.

### Python 2

Denne koden fungerer best med Python 3. Viss du har Python 2 må du leggje ein `u` framfor alle strengar, altså må strengen `'asdf'` skrivast slik som dette: `u'asdf'`.



### Lag kommentarar med forklaring



Les koden under.



## Hint

Du kan bruke kommandoen `help('funksjonsnamn')` i Python-terminalen for lese manualen. Prøv disse:

- ☐ `help('def')`
- ☐ `help('len')`
- ☐ `help('vigenere_encode')`

## Dekryptering

No skal me sjå på korleis me kan dekode meldingar. Etter kvart vil me til og med kunne lese hemmelege meldingar utan å kjenne den hemmelege nøkkelen på førehand.

### ☒ Lag `vigenere_decode`

Lag ein funksjon som gjer det motsette av den over (altså dekode). Koden skal sjå nesten lik ut som den over.

- ☐ Funksjonen skal ta inn to parametarar: ein koda tekst og ein nøkkel.
- ☐ Den skal dekode den koda teksten med nøkkelen.
- ☐ Og returnere den dekode teksten.
- ☐ Test at funksjonen fungerer og prøv med dine egne strenger og dekodingsnøkler.
- ☐ Kanskje du kan dele nøkkelen og sende den dekode teksten til ein ven?

### ☒ Cracking

- ☐ No skal du prøve å knekke ein koda streng. Det er vanskeleg, så du må leggje ei plan fyrst. Strengen er:

```
q00: ;AI"E47FRBQNBG4WNB8B4LQN8ERKC88U8GEN?T6LaNBG4G0""N6K086HB"08CRHW"+L
S790""N29QCLN5WNEBS8GENBG4F047a
```

## Hint

- ☐ Nøkkelen er seks små bokstavar.
- ☐ Språket i setninga er engelsk.
- ☐ Finn ein metode å sjekke om den dekrypterte strengen er korrekt. Til dømes kan du tenke på kor mange mellomrom den burde innehalde.
- ☐ For å generere moglege nøklar kan du bruke `itertools.product()`. Prøv til dømes å sjå kva du får om du loopar over `itertools.product('abcd', repeat=2)`.

## ✓ Bruk ei ordbok

Så lenge me brukar engelske ord som nøklar er det mykje raskare å knekke krypteringa med ei ordbok. Ei ordbok finst på alle Linux/Mac/Unix-maskiner under **/usr/share/dict**. Brukar du Windows kan du laste ned ei slik fil frå Internett. Søk til dømes på *large English vocabulary word lists*.

- ☐ Desse filene inneheldt alle ord som står i ei engelsk ordbok, separert med linjeskift. Finn ut korleis du kan laste inn orda frå fila (pass på at du fjernar linjeskifta) og bruk dei til å dekryptere ein ny streng:

```
t-J0:BK0aM, :CQ+ÆAGW?FJGB0KVCQM6SQN"GAIDL-PÅ7954E:7Jr, IÆoCF0M"CQd0VLHD5
3CÅ; IA2DMG50HD0VåL: JQ0439LRBBVEMTBÆ6CF0M"CQNAG8G1V6LÅ8FF4Z
```

- ☐ Bruk metodane du laga i oppgåva over for å sjekke om du har funne riktig nøkkel. Viss du køyrer skriptet ditt med kommandoen `time python3 vigenere.py` kan du sjå kor lang tid den brukar.

---

## Premie

Viss du klarar denne nøtta vil forfattaren av oppgåva gjerne spandere ein sjokolade på deg, føresett at du deler koden din. Send ein epost til [arve@seljebu.no](mailto:arve@seljebu.no) (<mailto:arve@seljebu.no>) :-)

Lisens: CC BY-SA 4.0 (<http://creativecommons.org/licenses/by-sa/4.0/deed>)