Kryptonøtt

Introduksjon

Kryptering har lenge vært i bruk i kommunikasjon. Faktisk brukte de d
sende hemmelige meldinger :-) Før du begynner på denne oppgaven,

Denne oppgaven er en nøtt. Det vil si at du skal finne ut av det meste
CodeMaster.

Kryptering med vigenere-n

Vigenere er litt smartere enn krypteringen i Hemmelige koder, men d
å forstå vigenere-koden. Det er viktig at du forstår denne koden, etter

Python 2

Denne koden fungerer best med python 3. Dersom du har python 2
`'asdf'` må skrives slik som dette: `u'asdf'`.

Lag kommentarer med forklar

- [ ] Les koden under.
- [ ] Hva er forskjellig fra Hemmelige koder?

- [ ] Hva gjør `alphabet.find`?
- [ ] Hva betyr det at `alphabet.find` gir `-1` som svar?
- [ ] Legg til kommentarer med `#` over/bak hver linjene med din forl

```
"""Vigenere encoding, by Arve Seljebu(arve@seljebu.no), MIT L

alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZÆØÅabcdefghijklmnopqrst

def vigenere_encode(msg, key):
    """Function that encodes a string with Vigenere cipher. T
       string is returned.
    """
    secret = ''
    key_length = len(key)
    alphabet_length = len(alphabet)

    for i, char in enumerate(msg):
        msgInt = alphabet.find(char)
        encInt = alphabet.find(key[i % key_length])

        if msgInt == -1 or encInt == -1:
            return ''

        encoded = (msgInt + encInt) % alphabet_length
        secret += alphabet[encoded]

    return secret

message = 'My first computer program was a song called Popcor
 I made was a bot made for IRC.'
keyword = 'source'

encrypted = vigenere_encode(message, keyword)
print(encrypted)
```

Hint

Du kan bruke kommandoen `help('funksjonsnavn')` i python-term

- [ ] `help('def')`
- [ ] `help('len')`
- [ ] `help('vigenere_encode')`

Dekryptering

Vi skal nå se på hvordan vi kan dekryptere meldinger. Etterhvert vil vi kjenne den hemmelige nøkkelen på forhånd.

Lag vigenere_decode

Lag en funksjon som gjør det motsatte av den over (altså dekrypterer

- [ ] Funksjonen skal ta inn to parametre: en kodet tekst og en nøkke
- [ ] Den skal dekryptere den kodede teksten med nøkkelen.
- [ ] Og returnere den dekrypterte teksten.
- [ ] Test at funksjonen fungerer og prøv med dine egne strenger og
- [ ] Kanskje du kan dele nøkkelen og sende den krypterte teksten ti

Cracking

Du skal nå prøve å knekke en kodet streng. Dette er vanskelig, så du

```
q0Ø:;AI"E47FRBQNBG4WNB8B4LQN8ERKC88U8GEN?T6LaNBG4GØ""N6K086HB"
```

Hint

- [ ] Nøkkelen er seks små bokstaver.
- [ ] Språket i setningen er engelsk.
- [ ] Finn en metode å sjekke om den dekrypterte strengen er kor mellomrom den burde inneholde?
- [ ] For å generere mulige nøkler kan du bruke `itertools.produ` looper over `itertools.product('abcd', repeat=2)`.

Bruk en ordbok

Sålenge vi har brukt engelske ord som nøkler er det mye raskere å kn på alle Linux/Mac/Unix-maskiner under **/usr/share/dict**. Bruker du Wi *large english vocabulary word lists*.

Disse filene inneholder alle ord som finnes i en engelsk ordbok, separ ordene fra filen (pass på at du fjerner linjeskiftene) og bruk dem til å

```
t-JO:BK0aM,:CQ+ÆAGW?FJGB0KVCGMQ6SQN"GAIDL-
PÅ7954E:7Jr,IÆoCF0M"CQdØVlHD53CÅ;IA2DMG5ØHDØVåL:JQØ439LRBBVEMT
```

Bruk metodene du laget i oppgaven over for å detektere om vi har fu kommandoen `time python3 vigenere.py` kan du se hvor lang tid der

Premie

Dersom du klarer denne nøtten, spanderer jeg gjerne en sjokolade på arve@seljebu.no :-)