Kryptografi: Skördetröskan

FRA har jobbat hårt och länge på ett topphemligt projekt vid namn Skördetröskan. Som ni säkert hört så har visselblåsaren Edvin Snöigloo nu till slut läckt lite information om detta topphemliga projekt. Det visar sig att Skördetröskan är ett krypteringssystem. Dock så lyckades Edvin bara läcka krypteringsdelen av koden och några hemliga meddelanden. Så nu sitter han där med sina meddelanden och kan inte dekryptera dem. :(

Det är där du kommer in! Skriv en dekrypteringsfunktion baserat på krypteringsfunktionen och ta reda på vad det hemliga meddelandet säger.

Här är krypteringsfunktionen Edvin läckte:

```
#!/bin/env python3
def encrypt(message, key):
    alphabet = "abcdefghijklmnopqrstuvwxyz"
    rot = [[0,1,2],[0,2,1],[1,0,2],[1,2,0],[2,0,1],[2,1,0]]
    ciphertext = ""
    for i in range(0, len(message), 3):
        for j in range(3):
            position = i + rot[key[0]][j]
            if position >= len(message):
                continue
            letter = message[position]
            if letter not in alphabet:
                ciphertext += letter
                continue
            num = alphabet.index(letter)
            num += key[1]
            if num >= len(alphabet):
                num -= len(alphabet)
            ciphertext += alphabet[num]
    return ciphertext
```

Edvin läckte även dessa meddelanden, deras krypterade form och nycklarna som använts:

Meddelande	**Nyckel**	**Krypterat meddelande**
"godis ar gott"	[4, 20]	"xai cm ulnain"
"skordetroskan ar det basta kryptosystemet"	[5, 7]	"vrzlkyvyahrzh uk y alzhi hafyrvawzfztlaal"

Edvin läckte även ett hemligt meddelande och nyckeln som användes för att kryptera det. Det är det här meddelandet som han vill att du ska dekryptera genom att skriva en dekrypteringsfunktion.

Krypterat meddelande	**Nyckel**
"ace yjb btdu uxcybw qcjeufibjqidu baeasq djuh qf kzbvqjde"	[1, 16]

Tips:

- Börja med att testa att kryptera lite olika meddelanden för att se att det funkar.
- Testa att kryptera samma meddelande med lite olika nycklar för att försöka förstå vad algoritmen gör.
- Det kan vara bra att testa att kryptera med nycklarna [0, N] och [N, 0] där N är lite olika tal.
- Vad påverkar det första talet i nyckeln? Vad påverkar det andra talet i nyckeln?
- Vilka delar av koden motsvarar det?
- På vilken sätt behöver du ändra dom delarna av koden så att den avkrypterar istället för att kryptera?
- När du väl har skrivit en dekrypteringsfunktion, verifiera att den funkar korrekt genom att först kryptera ett meddelande, sedan dekryptera meddelandet och se om det är samma som du började med.
- Nu kan du dekryptera det hemliga meddelandet! Tjoho!

Bonusuppgift:

Krypterat meddelande: 'dwhaidhkhdzacp gp pkaxsv icrxt'

Skapad av Mattias Grenfeldt