def Enc(m, k):

encrypted\_message = ''

for char in m:

if char.isalpha():

shifted\_char = chr(((ord(char) - 97 + k) % 26) + 97) if char.islower() else chr(((ord(char) - 65 + k) % 26) + 65)

encrypted\_message += shifted\_char

else:

encrypted\_message += char

return encrypted\_message

# Test cases

message1 = 'iitk is better than iitd and iitb'

key1 = 9

encrypted\_message1 = Enc(message1, key1)

print("Encrypted message 1:", encrypted\_message1)

message2 = 'lets learn cryptography'

key2 = 25

encrypted\_message2 = Enc(message2, key2)

print("Encrypted message 2:", encrypted\_message2)

Encrypted message 1: rrct rb kjyylc aolw rrmmq jas jkks

Encrypted message 2: kdsr kfbso dsqsbujnpdqb

def Dec(encrypted\_message, k):

decrypted\_message = ''

for char in encrypted\_message:

if char.isalpha():

shifted\_char = chr(((ord(char) - 97 - k) % 26) + 97) if char.islower() else chr(((ord(char) - 65 - k) % 26) + 65)

decrypted\_message += shifted\_char

else:

decrypted\_message += char

return decrypted\_message

def possible\_original\_messages(encrypted\_message):

possible\_messages = []

for key in range(26):

possible\_messages.append(Dec(encrypted\_message, key))

return possible\_messages

# Example usage

encrypted\_message1 = 'bm ptl wtfg xtlr tztbg'

encrypted\_message2 = 'rc fjb mjvw njbh'

# Dummy language model score function, replace with your own

def dummy\_language\_model\_score(message):

# Example: simply counting the number of spaces

return message.count(' ')

probable\_message1 = most\_probable\_message(encrypted\_message1, dummy\_language\_model\_score)

probable\_message2 = most\_probable\_message(encrypted\_message2, dummy\_language\_model\_score)

No, the Caesar cipher is not perfectly secret. Perfect secrecy, as defined by Shannon, means that the ciphertext provides no information about the plaintext, regardless of the computational resources available to the attacker. However, in the Caesar cipher, each letter in the plaintext is shifted by a fixed amount, which means patterns in the plaintext can still be discerned in the ciphertext. Additionally, since there are only 25 possible keys in the Caesar cipher, a brute-force attack is feasible.