# Assignment 1

## Answers

1. A)

No. The condition for perfect secrecy is

P[M=m | C=c] = P[M = m]

LHS = P[K = k] = P[K = (c-m) mod 26] != 1/26 sometimes

Like in the distribution P[M = 'one'] = ½, P[M = 'ten'] = 1/2

Take m = 'ten' and c = 'rqh’

Here LHS = 0.

Else if m = ‘ten’ and c = ‘ufo’ then LHS = 1/26 for k = 1

RHS = P[M = m] = sum(P[K = k] . P[M = (c-k) mod 26]) = 1/26 \* sum (P[M = c-k mod 26) = 1/26

LHS != RHS

Therefore, not perfectly secret.

B) As in the previous part, we see that the LHS becomes zero if key does not match with each letter in the message and cipher text.

If we choose different keys for different letters, we get –

RHS = 1/26 (in above part)

LHS = P[K = k] = P[K = (c-m) mod 26] = 1/26 iff each k is selected with a probability of 1/26.

Then we can achieve perfect secrecy.

1. A) def enc(m, k):

ans = ""

for onechar in m:

c = chr(((ord(onechar) - ord('a') + k) % 26) + ord('a'))

ans += c

return ans

1. rrct rb knccna cqjw rrcm jwm rrck
2. kdsr kdzqm bqxosnfqzogx

B)

def dec(c):

for k in range(26):

ans = ""

for onechar in c:

if onechar != ' ':

p = chr(((ord(onechar) - ord('a') + k) % 26) + ord('a'))

else:

p = onechar

ans += p

print(ans)

i) it was damn easy again

ii) it was damn easy