Mathematical Ciphers

Assignment 1

1 Shift Cipher

The shift cipher (also called Caesar cipher) works as follows. The English alphabet is represented by numbers from 0 to 25 i.e., $\{A, B, \ldots, Z\}$ are mapped to $\{0, 1, \ldots, 25\}$ in the same order.

Define $K = \{0, 1, 2, \ldots, 25\}$, $M = C = \{0, 1, 2, \ldots, 25\}$.
Gen(): $k \overset{U}{\leftarrow} \mathrm{K}$
Enc(k, $m = m_1 m_2 \ldots m_n$): Set $c_i \leftarrow (m_i + k) \mod 26$.
Ciphertext is given by $c = c_1 c_2 \ldots c_n$.
Dec(k, $c = c_1 c_2 \ldots c_n$): Recover message components as
$m_i \leftarrow (c_i - k) \mod 26$.

(a) Is this encryption perfectly secret?

(b) What change can we make to the key so that it becomes perfectly secret? (Hint: Can increasing length of key help if we modify encryption scheme in some way?)

2 Let's code

Seeing that you all might be quite familiar with shift cipher now, lets try to implement this. Assume we have a key ranging from 0 to 25 and a lowercase English message. (You can assume that space is not encrypted)

(a) Write a function **Enc(m, k)** that takes 2 parameters **m** and **k**, the message and key respectively, to encrypt the message using shift cipher. And so find the encrypted versions of the following messages -

(i) 'iitk is better than iitd and iitb' with k = 9
(ii) 'lets learn cryptography' with k = 25

(b) Given an encrypted message, write a function to list all possible original messages with a randomized key. Also given the original message was intelligible, find the most probable message from the list.

(i) 'bm ptl wtfg xtlr tztbg'
(ii) 'rc fjb mjvw njbh'