

Encryption :

(Can be used for all letters having ASCII between 32 and 125)

Assume key is "hello" and message to be encrypted is "welcome to coep"

1. Compute n - the sum of ASCII decimal codes of the encryption key

Here n is

$$h + e + l + l + o = 104 + 101 + 154 + 154 + 111 = 624$$

2. Split the message into chunks of length key.size

The message is split into - [welco, me to, coep]

3. For each chunk:

a. Reverse each chunk

So, the chunks would be [oclew, ot em, peoc]

b. Shift each character upwards by 'n' characters. If the selected character code exceeds the possible ASCII length, reassign from the start.

(Circular shift each character by n characters)

For e.g for oclew, the output would be

$$\text{o i.e. } 111 + 642 \Rightarrow 735 \Rightarrow 77 \bmod 94 \Rightarrow 77 \Rightarrow M$$

Similarly we can do this for all letters in all chunks.

c. Reverse each chunk again

This will give you the final output.

Decryption:

1. Compute n - the sum of ASCII decimal codes of the decryption key

2. Split the message into chunks of length key.size

3. For each chunk:

a. Reverse each chunk

b. Circular Shift each character downwards by 'n' characters.

c. Reverse each chunk again

