**Formal Definition.**

Message Space: ***M = {128 ASCII characters}\****Key Space: ***K = {0,1,2,3,4,5…,125,126,127}***k 🡸 Gen, where k € {0,1,2,3…..127}  
key is randomly generated.

Enck(m) = (m + k) mod 128

Deck(y) = (y-k) mod 128

**Correctness :** Deck(Enck(m)) = m

**Modifications in Shift Cipher Attack if we use ASCII 128 letters**By using **cryptanalysis**:  
Since the key space only contains 128 letters.  
The Cryptanalysis could easily try for all the values by shifting the message 128 times, and which ever may seem to be having a meaningful message in ASCII 128 alphabets , that would be our decrypted message , which is fairly easy to break since we have to shift only 128 times. This is the Cipher Text Only Attack.

By using **Index of Coincidence** but only if we have the standard frequency for ASCII 128 letters :

If we know the standard frequency for each letter of ASCII 128 , we can compare with the standard IOC, which is meant for the ASCII 128, by calculating IOC by multiplying probabilities of each letter with their standard probability and summing all the products.  
If our standard IOC and calculated IOC comes equal or nearly same, we could have successfully decoded the cipher text.