In a system where the message space consists of 128 ASCII characters and the key space ranges from 0 to 127, with the key randomly generated from this space, the encryption function ( text{Enc}\_k(m) ) is defined as ( (m + k) mod 128 ), and the decryption function ( text{Dec}\_k(y) ) is defined as ( (y - k)mod 128 ). The correctness property holds true if ( text{Dec}\_k(text{Enc}\_k(m)) = m ).

When analyzing the security of such a system:

Cipher Text Only Attack (CTO): Since the key space contains only 128 possible values, an attacker could simply try all possible keys by shifting the message 128 times. The decrypted message with a meaningful interpretation in ASCII 128 characters would likely be the correct one. This attack is straightforward due to the limited key space.

Index of Coincidence (IOC) Analysis: If the standard frequencies of each letter in the ASCII 128 set are known, one can calculate the IOC of the ciphertext by multiplying the probabilities of each letter with their standard probabilities and summing all the products. If the calculated IOC matches or closely resembles the standard IOC, it indicates a successful decryption of the ciphertext. This method relies on statistical analysis and knowledge of letter frequencies.

These methods illustrate how the limited key space in this system affects its security. While brute forcing through all possible keys is feasible due to the small key space, statistical analysis can also aid in decrypting messages, especially if the expected frequencies of characters are known.