Quiz 9

Problem 1
Consider a Caesar-type shifted substitution cipher with key K, where the message M is any integer in the interval $[0, 10^6 - 1]$ and $0 \leq K \leq 9$. For example, if $K = 1$ and $M = 123456$, then the encryption of M under key K is the ciphertext $C = 234567$. Assume all messages, and all keys, are equally likely.

- Compute $H(M)$ and $H(K|C)$, where H denotes entropy.