Exercise 1

Question 1

Xét $M = C = K = \{0, 1, 2, \dots, 255\}$ and consider the following cipher defined over (K, M, C):

$$E(k, m) = m + k \pmod{256} \qquad ; \qquad D(k, c) = c - k \pmod{256}\ .$$

Does this cipher have perfect security?

Question 2

Suppose you are told that the one time pad encryption of the message `attack at dawn` is

```
6c73d5240a948c86981bc294814d
```

(the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one time pad encryption of the message `attack at dusk` under the same OTP key?