

Quiz 2

Name:

1. In your own words, what does it mean for an encryption scheme to be perfectly secret?

2. The *shift cipher* is a historical cipher used to encrypt English text. It works by representing the letters of the English alphabet by numbers in $\{0, \dots, 25\}$.
Key generation chooses key k uniformly at random from 0 to 25 (i.e., $k \leftarrow \{0, \dots, 25\}$)
Given an l -letter message m ,
Encrypt by computing $Enc_k(m_1, \dots, m_l) = c_1, \dots, c_l$, where $c_i = [(m_i + k) \bmod 26]$
Decrypt by computing $Dec_k(c_1, \dots, c_l) = m_1, \dots, m_l$, where $m_i = [(c_i - k) \bmod 26]$.
 - (a) Is the shift cipher perfectly secret when only one letter is encrypted? Why or why not?

 - (b) What if two letters are encrypted? Why or why not?

3. Let E be an event that occurs with *negligible* probability when we run an experiment. If we repeat the experiment polynomially many times, the probability that we observe the event E is
 - a) undetermined
 - b) negligible
 - c) non-negligible