Question 1

Decrypt the ciphertext "qbhsovsnowak og goy mg n zsec waxseiggmbt ebq jia gznwg".

Question 2

Is a longer or shorter key more effective at encrypting messages in the Vigenere cipher? Explain why. Assume the adversary does not know the key length in advance.

Question 3

Why do we choose to modify the last (rightmost) bit of an RGB value in image steganography in particular? What happens if we modify the first (leftmost) bit instead?

Question 4

Argue why it is possible to decrypt the entirety of a Caesar ciphertext if you know the plaintext value of exactly one letter.

Contributors:
- Ryan Cottone