Homework 1 (100 pts)

Rule: Finish all of the following on your own. Submit your solution in PDF format.

1. Explain the three major security objectives: availability, integrity and confidentiality. Which one is more important than the others in the following scenarios?
    a. Suppose your job is to maintain the security of the patient information/data system for the OU-HSC.
    b. What if you are managing Norman's emergency alert system?
        - Reading: https://en.wikipedia.org/wiki/2018_Hawaii_false_missile_alert

2. Explain DDoS Attacks and their impact on the Internet. What are the possible countermeasures against such attacks?
3. Does the frequency analysis attack also work on Vigenere cipher? Why?
4. If a system is perfectly secure, can we say the system cannot be cracked in any way? Why?
5. Prove one-time pad is perfectly secure.
6. Suppose Alice designs a one-time pad variant: the plaintext is to no longer XOR, but bite-wise multiply the one-time key that is generated uniformly at random. For example:

plaintext:	001101
key:	101110
ciphertext:	001100

Is Alice's design good? (hint: you should explain if P(M|C) ?= P(M) by using mathematical proof. Only textual explanation without the inclusion of mathematical formulas will result in an incomplete analysis and, therefore, may lead to a deduction in grading.)

7. Is using the same key twice in one-time pad secure (i.e., Encryption: $M \oplus K \oplus K = C$; Decryption: $C \oplus K \oplus K = M$)? Why? Please explain in detail. (hint: you should explain if P(M|C) ?= P(M) by using mathematical proof. Only textual explanation without the inclusion of mathematical formulas will result in an incomplete analysis and, therefore, may lead to a deduction in grading.)