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

Availability: Makes sure that authorized users have timely and reliable access to information and resources when needed

Integrity: Makes sure information is accurate and unchanged, preventing unauthorized modification, insertion, or deletion of data.

Confidentiality: Makes sure that information is not disclosed to unauthorized individuals or systems. Protects sensitive data from being accessed or read by those without permission.

a. For maintaining the security of the patient information/data system at OU-HSC, confidentiality is more important than the others. Patient data involves sensitive personal health information that must be protected from unauthorized access to comply with privacy laws and prevent breaches.

b. For managing Norman's emergency alert system, integrity is more important than the others. The 2018 Hawaii false missile alert incident involved a human error where a false ballistic missile warning was sent, causing widespread panic for 38 minutes until corrected. This compromised integrity by sending inaccurate information, losing public trust. This is similar to what could happen if Norman's emergency alert system fails to protect its integrity. That incident really shows how false or altered messages can have severe consequences.

2. Explain DDoS Attacks and their impact on the Internet. What are the possible countermeasures against such attacks?

Distributed Denial-of-Service attacks are a type of DoS attack where multiple compromised machines (often botnets) from different locations flood a target system, network, or service with excessive traffic, making it unavailable to legitimate users. They target availability by overwhelming the target's capacity, such as data centers that drop connections when overloaded. Impacts on the internet include service disruptions (e.g., websites or online services becoming unreachable), financial losses, loss of user trust, etc. Possible countermeasures include rate limiting (e.g. limiting how frequently a user can make requests such as accepting only one web request per second from a user to prevent rapid flooding instead of allowing requests every millisecond). Additionally, we could perform attack identification and elimination which involves detecting malicious traffic patterns and blocking or filtering them out.

3. Does the frequency analysis attack also work on Vigenere cipher? Why?

No, frequency analysis attacks do not work effectively on the Vigenere cipher. Frequency analysis relies on mapping ciphertext letters to plaintext based on natural language frequencies, which works on monoalphabetic ciphers like Caesar because each letter is substituted consistently. In contrast, the Vigenere cipher is polyalphabetic, using a repeating key to apply multiple shift amounts. This reduces the letter frequencies across different alphabets, flattening the distribution and making it hard to identify patterns without knowing the key length.

4. If a system is perfectly secure, can we say the system cannot be cracked in any way? Why?

Yes, if a system is perfectly secure, it cannot be cracked in any way. Perfect security means the ciphertext reveals no information about the plaintext's likelihood and the plaintext reveals no information about likely ciphertexts. This is information-theoretic security, where even unlimited computational power provides no advantage to an attacker, as no probabilistic inference about the message is possible from the ciphertext.

5. Prove one-time pad is perfectly secure.

The one-time pad (OTP) is perfectly secure, as proven by showing that P(M|C) = P(M) for any message M and ciphertext C, meaning the ciphertext provides no information about the message.

OTP: C = M $\oplus$ K, where K is a random key of the same length as M, uniformly distributed (P(K = k) = 2^{-n} for n-bit length).

P(C = c | M = m) = P(m $\oplus$ K = c) = P(K = c $\oplus$ m) = 2^{-n}.

By Bayes' rule: P(M = m | C = c) = [P(C = c | M = m) * P(M = m)] / P(C = c).

P(C = c) = Σ P(C = c | M = m_n) * P(M = m_n) = Σ 2^{-n} * P(M = m_n) = 2^{-n} * Σ P(M = m_n) = 2^{-n} (since sum of probabilities over all possible messages is 1).

Thus, P(M = m | C = c) = (2^{-n} * P(M = m)) / 2^{-n} = P(M = m).

(For any fixed C, every possible M is equally likely, as each corresponds to a unique K.)

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.)

Alice's design is not good (not perfectly secure), as P(M|C) $\neq$ P(M) in general.

Assume bitwise multiplication on bits (equivalent to logical AND).

C = M * K, where K is uniform random.

Consider a 1-bit case for simplicity (extends to multi-bit).

Possible M, K, C (each 0 or 1, P(M=0)=P(M=1)=1/2 assume uniform: P(K=0)=P(K=1)=1/2.

If M=0, K=0 $\rightarrow$ C=0; M=0, K=1 $\rightarrow$ C=0; P(C=0|M=0)=1, P(C=1|M=0)=0.

If M=1, K=0 $\rightarrow$ C=0; M=1, K=1 $\rightarrow$ C=1; P(C=0|M=1)=1/2, P(C=1|M=1)=1/2.

P(C=0) = P(C=0|M=0)P(M=0) + P(C=0|M=1)P(M=1) = (1)(1/2) + (1/2)(1/2) = 1/2 + 1/4 = 3/4.

P(C=1) = 1/4.

Now, P(M=0|C=0) = [P(C=0|M=0)P(M=0)] / P(C=0) = (1 * 1/2) / (3/4) = (1/2)/(3/4) = 2/3 ≠ P(M=0)=1/2.

P(M=1|C=0) = (1/2 * 1/2) / (3/4) = (1/4)/(3/4) = 1/3 ≠ 1/2.

P(M=0|C=1) = 0 (since C=1 only if M=1 and K=1), P(M=1|C=1)=1 ≠ 1/2.

Thus, observing C reveals information about M (e.g., C=1 implies M=1), violating perfect security.

In the example (plaintext 001101, key 101110, ciphertext 001100), positions with C=0 could have M=0 or 1 (if K=0), but C=1 requires M=1 and K=1, leaking info.

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.)

No, using the same key twice in one-time pad is not secure, as it reduces to C = M ⊕ K ⊕ K = M ⊕ 0 = M, so C = M. Thus, P(M|C) = 1 if M=C, 0 otherwise ≠ P(M).

Mathematically:

- Standard OTP: C = M ⊕ K, secure if K used once.
- Here: C = M ⊕ K ⊕ K = M (since K ⊕ K = 0, M ⊕ 0 = M).
- Decryption: C ⊕ K ⊕ K = M.

Since C = M directly, an attacker sees the plaintext as ciphertext without needing K.

Even if interpreted as two encryptions, reusing K breaks security: If two messages M1, M2 with same K, C1 = M1 ⊕ K, C2 = M2 ⊕ K, then C1 ⊕ C2 = M1 ⊕ M2, allowing crib-dragging or frequency attacks on M1 ⊕ M2.

P(M|C): Since C=M, it fully reveals M, so P(M=m|C=c) = 1 if m=c, 0 else ≠ P(M).