Problem 1: Understanding One-Time Pad

A one-time pad refers to a cryptographic system where a secret key is generated from a fully, or uniformly, random set of values and used only once to both encrypt and decrypt a single message. If the following conditions are met, then use of a one-time pad enables "perfect secrecy", which indicates that given the ciphertext of the message, an adversary gains no additional information about the underlying plaintext message, even if the adversary has theoretically infinite computing power:

- The Secret Key is only used once
- The values used to generate the key must be truly random
- The secret key is securely shared between the sending and receiving parties
- The secret key must be at least as long as the plaintext being encrypted

This last requirement is based on a theorem by Claude Shannon, which is stated formally as:

Any cipher achieving perfect secrecy requires that $|K| \geq |M|$, where K is the key space and M is the plaintext message space. Like other encryption systems, one-time pads also adhere to Kerchoff's Principle, which states: [The method of encryption] *must not be required to be secret, and it must be able to fall into the enemy's hands without causing inconvenience.* This principle implies that even if an adversary has knowledge of the encryption technique they will be unable to decrypt without the secret key.

However, the requirement of a key being at least as long as the plaintext message limits its practical use in many modern applications, including anything related to digital media.

Sources:

https://www.techtarget.com/searchsecurity/definition/one-time-pad

https://courses.grainger.illinois.edu/CS407/fa2023/Scribe%202.pdf