2.2.1 Adversary Models

When it comes to steganography, an adversary can either be passive or active.

Passive

A passive adversary, Eve, will intercept messages sent between Alice and Bob. They will be able to read all messages, but will not make any changes to the messages and will send them on intact to the receiver. They will run analysis on the message to try and discover hidden data. In the scenario of the prisoners problem, this will be the warden only reading the messages.

Active

An active adversary, Mallory, will again intercept the messages sent between Alice and Bob, but this time will tamper with the message in order to remove any possible hidden data. For example, if the message was an image or some audio, they could run compression or noise reduction algorithms to damage the hidden data. If a structural method of text steganography is used, they could remove any extra white space or make the line spacing uniform. They could perform synonym substitution. which will affect the data if a semantic method was used as different synonyms usually mean different data. In the case of the prisoners problem, this will be any case when the warden makes any change to the message.

2.2.2 Methods

There are a number of methods of steganalysis available to attackers. The primary and most common method is to use statistical analysis [12]. This can be of many forms. To perform this analysis requires the steganalyst to perform one of the six kinds of attacks.
The six main types of attack available to steganalysts [29]:

Stego-only Attack

The attacker only has access to the stego-object. The attacker would need to perform statistical analysis on the object. For example, structural text steganography can be easily detected simply by searching for extra spaces, unusual line spacing and so on [1]. For semantic methods, this could involve using analysis of corpora to analyse the occurrences of words within text and then examining the suspicious message to see if there are any words which do not appear frequently in the corpus with the surrounding words. This may indicate that a word has been replaced with a less commonly used synonym. This method could also involve the construction of large context free grammars which will easily be able to identify unusual elements in text.