Problem 1.

Part 1.





Part 2.

The one-time pad is not commonly used in practice due the limitation that the key length must be greater than or equal to the message length and the ciphertext length.

Problem 2.

The modified one-time pad encryption scheme is not perfectly secret. Let a random variable have a uniform distribution over . For all ,  , however since  . The scheme is not perfectly secret.

However, the scheme does have statistically -indistinguishable encryptions. Let  be a subset of the ciphertext space. For every key the probability of it being chosen is . So for every ,



The difference  is maximized when exactly one of , where it takes the value of . Thus the encryption is statistically secure for .

One should note that the one-time pad encryption scheme is preferable even though the message could be seen openly, even after encryption. The probability an n-bit string consisting of all 0’s is highly unlikely.

Problem 3

Part 1.

Perfect Secrecy – FALSE

Statistical Security – FALSE

Computational Security – TRUE

Part 2.

Perfect Secrecy – TRUE

Statistical Secrecy – TRUE

Computational Security - TRUE

Part 3.

Perfect Secrecy – FALSE

Statistical Secrecy – FALSE

Computational Security – TRUE

Part 4.

Perfect Secrecy – TRUE

Statistical Secrecy – TRUE

Computational Security – TRUE