Problem 1

1. State the definition of the one-time pad encryption scheme for n-bit messages. Your specification should include: the message space, the ciphertext space, the key space, and functions Gen, Enc, and Dec.



2. Why is the one-time pad not commonly used in practice?

Solution: The one-time pad is not commonly used in practice due to its limitation of the message length. It is not practical in practice to have a key length the size of the message space.

Problem 2.

Suppose the encryption key length (n) was equal to 1. The probability that the encryption key would be 1 is 1. Now suppose the encryption key where n is equal to 2, the probability that the key equals {1,0} is 1/3, {0,1} is 1/3, {1,1} is 1/3, and {0,0} is 0/3. Right away we know that this scheme does not satisfy perfect secrecy due to the fact that the key space is smaller than the message. The smallest  for which this scheme has  indistinguishable encryptions is as follows:

<scheme> <is / isn’t> <definition>.

<Consider uniform distribution / Let>

<random variable> <set operation> <probability space>.

<Then for any / For all / each> <element><set operation><probability space>, Pr[<random variable>=<element>] = <negligible function>

<However / Such that / So >

Pr[<random variable> = <element> given <function> = <element> ] = 0

Thus, <scheme> <is / isn’t> <definition>.

<scheme> <is / isn’t> <definition>

<Let / Consider Uniform Distribution><Random variables> be <set operations> of the <probability space>

<Then for any / For all / each> <element><set operation><probability space>,

<probability of an Event>>

s.t. <for all elements / for an element><probability, function(element)><set operation><random variable>.

<proves / disproves> satisfies definition <given a certain condition>

Thus <scheme> <is / isn’t> <definition> for <condition>

Yes or No

Proposition.

Setup variables.

Probability of Event

Probability of Event with Condition

Answer Questions (Optional)

Restate Thesis

Probability Space

Random Variable

Expectation

Markov’s Inequality

Chernoff Bound

Conditioning

Encryption Scheme

Perfect Indistinguishability

Perfect Secrecy

Perfect Adversarial Indistinguishability

Statistical Security

Computational Security

Concrete Computational Indistinguishability

Asymptotic Computational Indistinguishability

Partial Semantic Security

Pseudo Random Generator

Efficiently Computed

Expansion

Negligibly Indistinguishable