**CSCI 531 Quiz 2**

**Write your name here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**The number of points for each question or sub-question is indicated by the integer in brackets [n] before the question or sub-question. The total number of points is 100.**

1. [15] Explain in plain English: what property XOR has that makes it so useful in cryptography (hint: use the notion of random variable)?

if we take an arbitrarily distribution and XOR with independent uniform random variable we end up with is a uniform random variable

1. [15] Define what it means for a cipher to have *perfect secrecy* (or be *information-theoretic secure*) in general terms (plain English).

*Perfect Secrecy* (or *information-theoretic secure*) means that the ciphertext conveys no information about the content of the plaintext. In effect this means that, no matter how much ciphertext you have, it does not convey anything about what the plaintext and key were. It can be proved that any such scheme must use at least as much key material as there is plaintext to encrypt. In terms of probabilities, it means that the probability distribution of the possible plaintexts is independent of the ciphertext.

1. [10] Why one should not reuse a stream cipher key?

If two plaintexts are encrypted with the same key using a stream cipher then cryptanalysis is often quite simple. If the two cipher text streams are XOR together the result is the XOR of the original plaintexts. So it is not desirable to reuse a stream cipher key. Since the cleartext usually has lots of redundancy, one can use that to discover both messages.

These ciphers typically generate a stream of pseudo-random numbers depending on the input password which is XOR-ed with the plaintext to create the ciphertext. The property of the XOR operations is that two ciphertexts with the same keystream can be XORed to get the XOR of the plaintexts, from which you are an XOR or two away from the keystream and any plaintext.

1. [15] What does it mean for a cryptosystem be *semantically secure*? Explain in general terms (plain English).

No efficient adversary can distinguish the encryption of one message from the encryption of another one. Knowledge of the ciphertext (and length) of some unknown message does not reveal any additional information on the message that can be feasibly extracted

1. [15] What does it mean for the output of the pseudorandom generator to be indistinguishable from random (plain English)?

An adversary looks at the output of the generator and can't distinguish it from the output of the uniform distribution over the entire set

1. [15] Consider a pseudorandom generator G that outputs N bit strings and a statistical test on N bit strings. What does it mean for a statistical test to be able to break G (plain English)? Hint: we discussed the notion of advantage.

We want a statistical test to distinguish the output of the generator from random.

If the advantage is close to 0, the statistical test behaves pretty much the same on pseudo random inputs as it does on truly random inputs. And we cannot not distinguish the generator from random. If advantage is close to 1, then we can distinguish – break G.

1. [15] What is the difference between a block cipher and a stream cipher (plain English)?

Answer: A stream cipher is one that encrypts a digital data stream one bit or one byte at a

time. A block cipher is one in which a block of plaintext is treated as a whole and

used to produce a ciphertext block of equal length.