**CSCI 531 Quiz 1**

**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. [10] List and briefly define three security goals of cryptography as discussed in class.

* Confidentiality (secrecy, privacy): only the intended recipient can see the communication
* Authenticity (integrity): the communication is generated by the intended sender information is not altered or destroyed
* Non-repudiation: party in a dispute cannot repudiate, or refute the validity of a statement

1. [15] Briefly describe ciphertext only attack, known plaintext attack, chosen plaintext attack and chosen ciphertext attack. Which of these attacks is the most difficult to **defend** against?

Ciphertext only attack:

Analysis of the ciphertext itself, generally applying various statistical tests to it.

Known plaintext attack:

The analyst may be able to capture one or more plaintext messages as well as their encryptions. With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed.

Chosen plaintext attack:

Chosen plaintext: If the analyst is able to choose the message to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.

Chosen plaintext attack:

In a chosen-ciphertext attack, you get to choose both plaintext values and ciphertext values. For every plaintext that you choose, you get the corresponding ciphertext, and for any Ciphertext you choose, you get the corresponding plaintext. This is the hardest attack to defend against.

1. [15] Data compression is often used in data storage and transmission. Suppose you want to use data compression in conjunction with encryption. Which of the following options makes more sense? Briefly explain.
   1. The order does not matter - neither one will compress the data
   2. The order does not matter - either one is fine
   3. Encrypt then compress
   4. Compress then encrypt

Answer: 4

Ciphertext tends to look like random strings and therefore the only opportunity for compression is before encryption.

1. [15] Recall that the core principles of modern cryptography are:
2. Formal definitions
3. Assumptions
4. Proofs of security

Why do we need “proofs of security”? Briefly explain.

Proofs give us confidence in the security of particular schemes and more importantly, allow us to move away from the design-break-patch cycle that was used historically. That is, rather than propose a scheme and wait for someone to come along and break it, we can instead hope to propose a scheme along with a proof of security that ensures that no one can break it.

1. [15] Recall that Kerckhoff’s principle: the security of encryption scheme must depend only on the secret key and not on the secrecy of algorithm. Do you believe this makes sense? Explain why or why not.

Answer: yes, it does

The key can be selected randomly. The algorithm cannot.

The key can be changed easily; the algorithm cannot.

The key is short and can be more easily hidden.

Algorithm can be reverse engineered

1. [15] What is a substitution cipher? How would you break it?

Answer: The key is a bijection from the alphabet to itself: each letter is substituted by

another letter (same plaintext letter always becomes the same ciphertext letter).

Use frequency of English letters, e.g., digrams, trigrams

1. [15] Explain in plain English how a Randomized Algorithm differs from a Deterministic Algorithm.

output of a randomized algorithm changes every time you run iteven though the inputs to the randomized algorithm can be the same; output of deterministic algorithm is the same for the same input