COP 5615 DOSP
Fall 2022
Weekly Report

Jaswanth Reddy Kankanala
UFID : 22719671

Using cryptography, confidential information is converted into a code that cannot be deciphered by anybody who is not authorized to do so. This ensures that the information is not seen by any other individuals. A message that is written in plaintext, which is text that humans are able to read, is transformed into ciphertext during the process of cryptography. This transformation may be accomplished by the use of an algorithm or a series of mathematical operations. In the event that you are not familiar with cryptography in any way, the ciphertext will seem to be incomprehensible to you.

Messages that have been encrypted are typically converted into plaintext at some point during the processing of cryptographic systems. This enables the user to understand the message and choose how to put it to use.

Let's take a little break and discuss two of the most fundamental concepts in cryptography before moving on to the more complex subjects we'll be covering later on today. The premise that comes first is known as the Kerckhoffs' principle. The Dutch cryptographer Auguste Kerckhoffs, who had a lot of success in the 1800s, is the inspiration for the name of this algorithm. To briefly recap what has previously been covered, in order for a cryptographic system to function correctly, it is necessary to have both a key and an algorithm. Kerckhoffs believed that if the key to a cryptographic system was kept hidden, then the system should still be secure despite the fact that the key was hidden.

On the other hand, during this time period, practically all applications of cryptography were found in the military. Despite the fact that you may be tempted to keep your cryptography method a secret from your opponent, there is a 100% chance that they will discover it at some time in the not too distant future. Claude Shannon, a pioneer in information theory and a cryptographer for the United States government during World War II, is credited as saying, "The opponent knows the system." The argument that Kerckhoffs and Shannon are attempting to make here is that it is not the most effective method to conceal information by using an algorithm that is, by its very definition, a secret. On the other side, open source cryptography methods are viewed as a positive thing in today's society, rather than a necessary evil. This shift in perception occurred very recently. When compared to how things were in the past, this is a significant shift. You don't need to build your own private

encryption techniques since the conventional cryptographic algorithms have already been properly investigated and tested.

Your encryption key is something that you are always required to preserve a well guarded secret. In a minute, we'll go into the mathematics that behind that, but in the meanwhile, it's essential that you have a solid understanding of an additional cryptographic concept that underpins the existence of that mathematics. One-way functions, which are mathematical processes that are difficult to reverse, are used in order to accomplish this goal.

A well-known example of a one-way function is the product that is obtained by multiplying together two very big prime integers. It is not difficult to do the calculations; nevertheless, if you merely obtained the result, it would be exceedingly difficult, if not impossible, to determine which two prime integers were used in the computation. Even though many functions can't be done backwards due to the limits of modern computers, mathematicians continue to fight about whether or not any function can be fully one-way and whether or not any function can be truly one-sided.