Manuel Aguilar

Alejandro Sanchez

Cryptosystems and Hash Functions

Cryptosystems and hash functions, will be evaluations can be provided by using Mathematica. Mathematica, is a computer algebra system based on the Wolfram’s Language computational database. Scientific computation will be performed through Wolfram’s extensive collection of algorithms and handle of long prime integers. This property will be coupled with concepts pertaining to Discrete Mathematics. The computational approach will be for visualization purposes and symbolic manipulation of variables.

The goal to become an experience programmer with Mathematica. As well as make the synthesis between mathematics and computational sciences. Exploring different paradigms in programming , such as procedural and functional used to analyze a problem.

The programming aspect is to convert mathematical concepts to a virtual environment. This can extend the properties of a function aswell as the work able to be performed. Data can be manipulated in a variety of ways. From initial entry it can be seen as a vector. The common array or list in programming languages can be repesented as a vector. A vector – a one dimensional represnetation of elements in a set. A vector can be extended to a two-dimensional shape; a matrix. Matrices extend the properties of the numbers and increments the number of operatins available to perform. Certain things to be aware of a matrices is the order of operations. For example, the product of multiplication on two matrices will be different depending in which order computed. Matrix multiplication is not \_\_\_\_. From matrices we can visualize them to graphs, and brought back to the original form.

* Discuss the history of cryptography

One of the first methods of cryptography was the Caesar cipher. This was used to deliver messages safety back in the day. The way the Caesar Cipher worked is by shifting the letters of the alphabet to create a new word, or sentence. The key was used to shift the alphabet back to the original message. These methods are obsolete for example this would be easily cracked by shifting the alphabet yourself to see which one is in English, or figuring out that E is the most commonly used letter to shift the alphabet.

Today these methods are not used today, but was used to create the Vigenere Cipher which is based off the Caesar Cipher. The Vigenere Cipher is a more sophisticated method and the ROT13 system uses the cipher. However, these are still pretty outdated compared to more secure forms of encryption. Today we have many different forms of encryption such as SSL, 128 bit. encryption which are considered today uncrackable by todays standards. In the essay we will be discussing how these systems work, and why they are safe.

* Discuss the current methods of today cryptography

Today’s best forms of encryption are AES Advanced Encryption Standard, 3DES, and others which are nearly uncrackable today.

* Show an example of today’s cryptography