Cryptosystems and Hash Functions

**Abstract**

Cryptosystems have a rich history of concealing trying messages with sensitive information. From the days of ancient Italy, under Julius Ceaser reign. The Allies in World War II trying to decipher the Axis communications. To modern day message relaying; our emails, bank account and social media. Cryptosystems surround every business aspect of the world wide web , that requires trust and company integrity.

However, cryptosystems make up a huge part of the eco-system of the web; they are based on theormes in mathematics. Different mathematical techniques are applied to make cryptosystems and to ensure security. This is known as a hash function. In the past, ciphers were to be written with paper and pen. This is no longer the case in the modern world were the power of computing is exponential and growing. Computers, are used in the research and development of new cryptostytems and hash functions.

Mathematica, is a programming language with many keywords that support the research and development of cryptosystems in research. Mathematica, will also give the opportunity to transform data in different formats to expose different ideas in cryptography. Mathematica, also has a repertoire of plotting formats that allows a person to contemplate the nature of numbers used in cryptography.

The conclusion being , to gain experience programming with Mathematica. As well to make the synthesis between the ideas in mathematics and computational sciences. Exploring exclusive programming paradigms available in Mathematica, such as procedural and functional to analyze and research a problem.

**History**

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 However, these are still pretty outdated compared to more secure forms of encryption.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.

**Introduction**

* EXPLAIN THE GOALS OF YOUR PROJECT
* Indicate why this topic is exciting and useful
* Introduce your project and outline importance
* Why is this topic useful/exciting

Goals in the project is to demonstrate the importance of numbers in the real world.

Example being how conglomerate enterprises rely heavly on the security of their products.

Consumers who purchase services from companies need to trust that their account information is secure. Companies built a reputation on the integrity and credibility of their services, making cryptography important to the eco-system of trading goods and services. Since, cryptography has become exclusive to the realm of digital systems by generating different formats of verifying information; to checksums, qr-codes, and identicons.

**Background**

* Background information required to understand
* Defining Scientific Terms

As all scientific topics, a plethora of vocabulary words must be known to be versitle in the science.

Cryptography has a rich history; from the humble origin of "shifting" ciphers of Julius Ceaser to

the modern AES algorithm.

Hashing is the transformation of a digital object into fixed value. A key that represent the original object. Hashing is used to index and retrieve information that may be sensitive in nature and requires validiation. Entropy is the randomness collected by an operating system or application for use in cryptography or other cases requiring random data. Checksums are used as a verification token when downloading applications from the internet. It it helps the consumer by verifiying the original application is untampered. A checksum is a hash of the whole application. Encryption is a form of computerized cryptography using a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Asymmetric encryption is a method of encryption known as a "third-party" system. Two encrypted objects are generated; a public and a private key. The propetary of the asymmetric lock will be the only one with access to the private key. The public key will be distributed across the web and to whomever it concerns. This with the purpose to offer a form of security for the user. The entity in posession of the private key will be able to verify the legitamitcy of the encrypted object by decrypting. Decrypting is allowed using the private if the original message was signed with the public key.

Define, Public Key \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Define, Private Key \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A QR-Code is a machine readable code consisting of an array of black and white squares, typically used for storing urls or other information. This can be accessed with a smartphone. An identicon is a visual representation of a hash value, usually of an IP address, that serves to identify a user of a computer system as a form of avatar. Is programming nomenclature for an object which is an array of bytes. Whatever the data-type of the elements wihtin the set -- yields the integer in binary represantion. It is an extremly powerful tool in programming. To be able to compress information and reduce the computer energy consumption. Number Theory, is the study of numbers and their properties.

**Main Section**

* What did you learn ?
* How does this have to do with your major ?
* Connect it to the real world or community ?
* Do you intend to present this project to an audience ?
* References ?
* REAL-LIFE EXAMPLES must be included

The Wolfram Language's extensive base of state-of-the-art algorithms and

efficient handling of very long integers make it uniquely suited for both research and

implementation of cryptographic number theory.

When reading complimentary material for the project based on the nature of the numbers it was intresting to visualize the ideas. As I learned Wolfram Language it became easy and clear to translate the ideas from paper and ink to the digital.

Research in the topic is crucial in today's society rotating around digital devices. Research in this field can be transfered to the benfit of the city by generating validation key for key cards. An large number of business in the El Paso rely on smart authentication cards.

Real life example of supercomputing, \_\_\_\_\_\_\_\_\_\_\_\_\_

Real life example of crytography, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Another real life example is crypto-currencies \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cryptography is important, it is used in all forms of electronic media. We use it in our emails, social media accounts and to verify our passwords. Cryptography also offers an extra layer of security in the Information Technology world. By using public keys on trusted devices and verifying them when they connect to the internet. Using the domain name of the network configured with a provate key to verify the electronic device is allowed to browse the web or communicate with other devices.

**Conclusion**

* What new knowledge was aquired.
* Why is your project excitig/useful
* Connections between what you learned so far …

Knowledge was aquired with respect to the property numbers in realtion to cryptography. Knowledge was aquired in respect with scientific computing....

The project is useful because it uses cloud -- an enterprise solution for resource disapition. Resources , in the context of reducing infrastructure costs and increasing profit.