Manuel Aguilar

Cryptosystems and Hash Functions

Discrete Mathematics

December 5, 2018

Manuel Aguilar

Abstract

Cryptosystems have a rich history of concealing trying messages with sensitive information. From the days of ancient Italy, under Julius Caesar 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 ecosystem of the web; they are based on theorems 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 cryptosystems 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 However, these are still pretty outdated compared to more secure forms of encryption.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 today's standards. In the essay we will be discussing how these systems work, and why they are safe.

Introduction

   Goals in the project is to demonstrate the importance of numbers in the real world. Example being how conglomerate enterprises rely heavily 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 ecosystem of trading goods and services. Since, cryptography has become exclusive to the realm of digital systems by generating different formats of verifying information; to checksum, qr-codes, and identicons.

Background

   As all scientific topics, a plethora of vocabulary words must be known to be versatile in the science. Cryptography has a rich history; from the humble origin of "shifting" ciphers of Julius Caesar 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 validation. Entropy is the randomness collected by an operating system or application for use in cryptography or other cases requiring random data. Checksum are used as a verification token when downloading applications from the internet. It it helps the consumer by verifying 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 proprietary 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 possession of the private key will be able to verify the legitimacy of the encrypted object by decryption. Decryption is allowed using the private if the original message was signed with the public key.

A Public Key is a generated digital-signature made to be shared. The purpose it is shared is that it can be verified with the private key. By using the private key one can see the integrity of the object in

question. Whether it was tampered and altered for some reason. Also it can show where the package originally comes from. Private key, is a variable that is used within an algorithm to encrypt and decrypt code. Quality encryption follows a fundamental rule: "the algorithm doesn't need to be a secret, but the key does". Private keys play important roles in both symmetric and asymmetric cryptography.

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 within the set -- yields the integer in binary representation. It is an extremely 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

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 number theory in relation with cryptography.

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 transferred to the benefit 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 cryptography, one easy to explain encryption system that is not used today Vigenere Cipher. The reason it is not used to today is because it is easily breakable. The way the system work is by using a key length from 1-N up to the length of the length of the message. For example starting from the first letter key DICE, D is used to shift the first index of the message and then the 4th one the 8th one repeating. D shifts the message 4 places from the letter of the alphabet. For example Hhdiu LVXNEW uxh WKWVCEW, krg k wbbsqa si Mmwcjiqm they key for this is 4 and the key are The keys are 3 30 10 4. So that is the way the message will be decrypted. The original message Enter BRUTUS and CASSIUS, and a throng of Citizens. Notice the shift in the letter is how the message got decrypted. E got shifted 4 letters, n got shifted 30 letters and so on. The program works

for many languages since it counts the amount of words that are valid in 12 languages and selects the one with the most valid words that it counted in the dictionary.

Another real life example is crypto-currencies they work by using hash functions to validate the currency, and to transfer the currency. The currency uses public keys and private keys. Once they currency is transferred over to the new user the both users have a new hash function which represents the new total's. The reason this system is secure is because the hash functions are created in a unique way. First a certain amount of 0's are required to be part of the hash table. Lastly the new Hash tables get built on top of each other so each transaction creates a new hash table based on the previous hash table.

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 private key to verify the electronic device is allowed to browse the web or communicate with other devices.

Knowledge was acquired with respect to the property numbers in relation to cryptography. Knowledge was acquired in respect with scientific computing and the complications that arise when exhausting machines.

The project is useful because it uses cloud -- an enterprise solution for resource dissipation. Resources , in the context of reducing infrastructure costs and increasing profit. However, cloud is limited in it's performance depending on the payment plan set up. Usually, cloud providers have a pay-as-you-grow payment model or computing credits. The optimal solution for research is bare-metal machine that has extraordinary capabilities so they can be exploited. Exploited in the sense the computer can do hard-processing tasks like huge data-sets.

Bibliography

Hastings, Cliff, et al. Hands-on Start to Wolfram Mathematica: and Programming with the Wolfram Language. Wolfram Media, 2016.

Wolfram Language Documentation, reference.wolfram.com/language/guide/PrimeNumbers.html.

Wolfram Language Documentation, reference.wolfram.com/language/guide/Cryptography.html.

Wolfram Language Documentation, reference.wolfram.com/language/ref/ListPlot.html.

Wolfram Language Documentation, reference.wolfram.com/language/guide/DataVisualization.html.

Aumasson, Jean-Philippe. Serious Cryptography: a Practical Introduction to Modern Encryption. No Starch Press, 2018.

"Lecture Notes on Classical Cryptology." *Cryptology Lecture Notes 2*,

www.math.ucdenver.edu/~wcherowi/courses/m5410/m5410cc.html.

Wolframalpha Diagrams

✘ *Hash Functions*

| Hashing Algorithm	Checksum
Adler32	135 332 455
MD2	175 593 414 339 692 162 985 324 972 822 726 990 222
MD4	84 845 478 232 863 148 719 478 827 667 834 617 641
MD5	40 423 484 761 541 238 382 905 956 627 771 067 589
SHA	1 398 159 894 576 866 049 018 023 610 109 846 384 462 526 399 142
SHA256	57 080 914 990 382 652 018 975 454 686 244 920 197 179 840 614 193 418 ‹ 429 741 265 023 699 207 040 488
SHA256SHA256	75 282 984 869 686 547 033 353 926 851 434 342 486 641 504 584 554 712 ‹ 296 953 086 155 350 376 418 163
SHA384	13 562 084 471 007 220 712 854 655 934 427 672 120 557 912 358 406 699 ‹ 800 378 858 006 517 427 730 812 564 064 542 365 807 440 342 864 157 ‹ 242 321 578 188
SHA512	567 584 861 444 521 757 987 592 168 817 487 901 212 127 703 889 608 ‹ 468 131 708 958 906 297 413 514 299 784 497 037 912 425 878 949 436 ‹ 807 891 799 962 149 517 269 913 834 740 897 637 772 636 904 883 829
RIPEMD160	1 460 802 423 991 320 589 790 627 455 214 415 478 664 116 343 346
RIPEMD160SHA256	694 818 053 040 215 637 815 965 630 285 984 990 202 021 666 113

✘ *Visualize hash-function entropy (**Collisions**)*

Manuel Aguilar
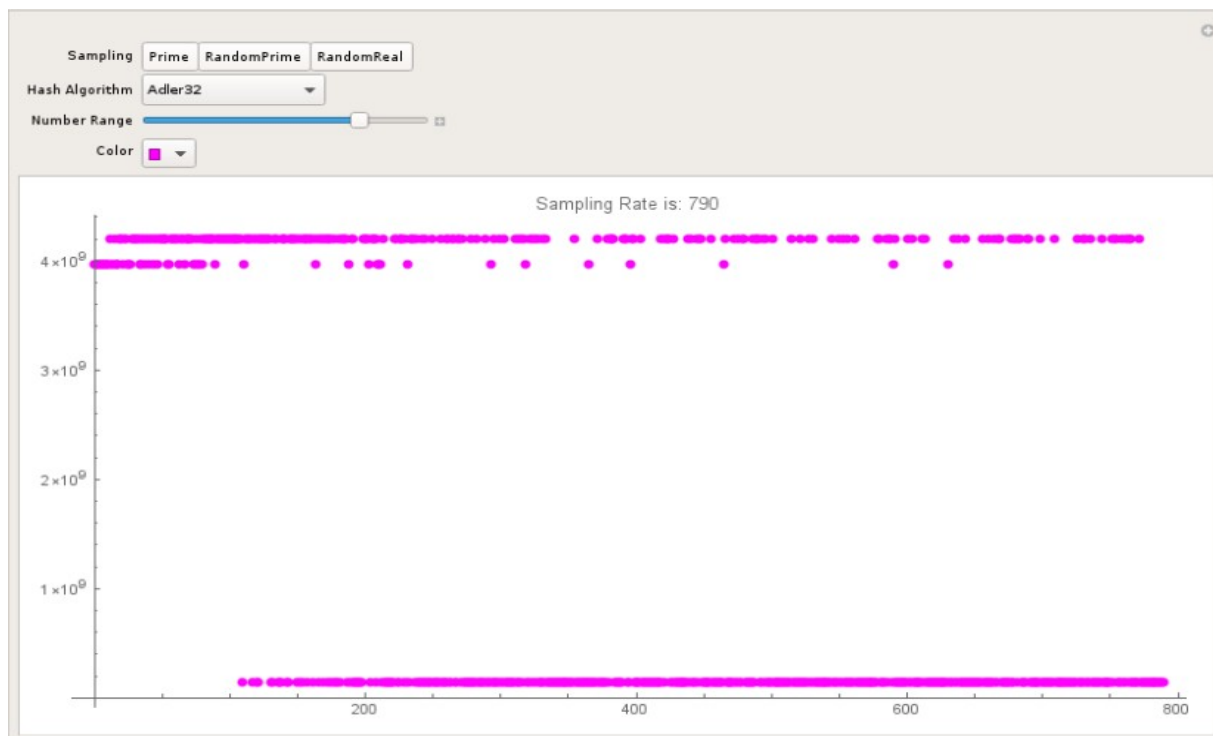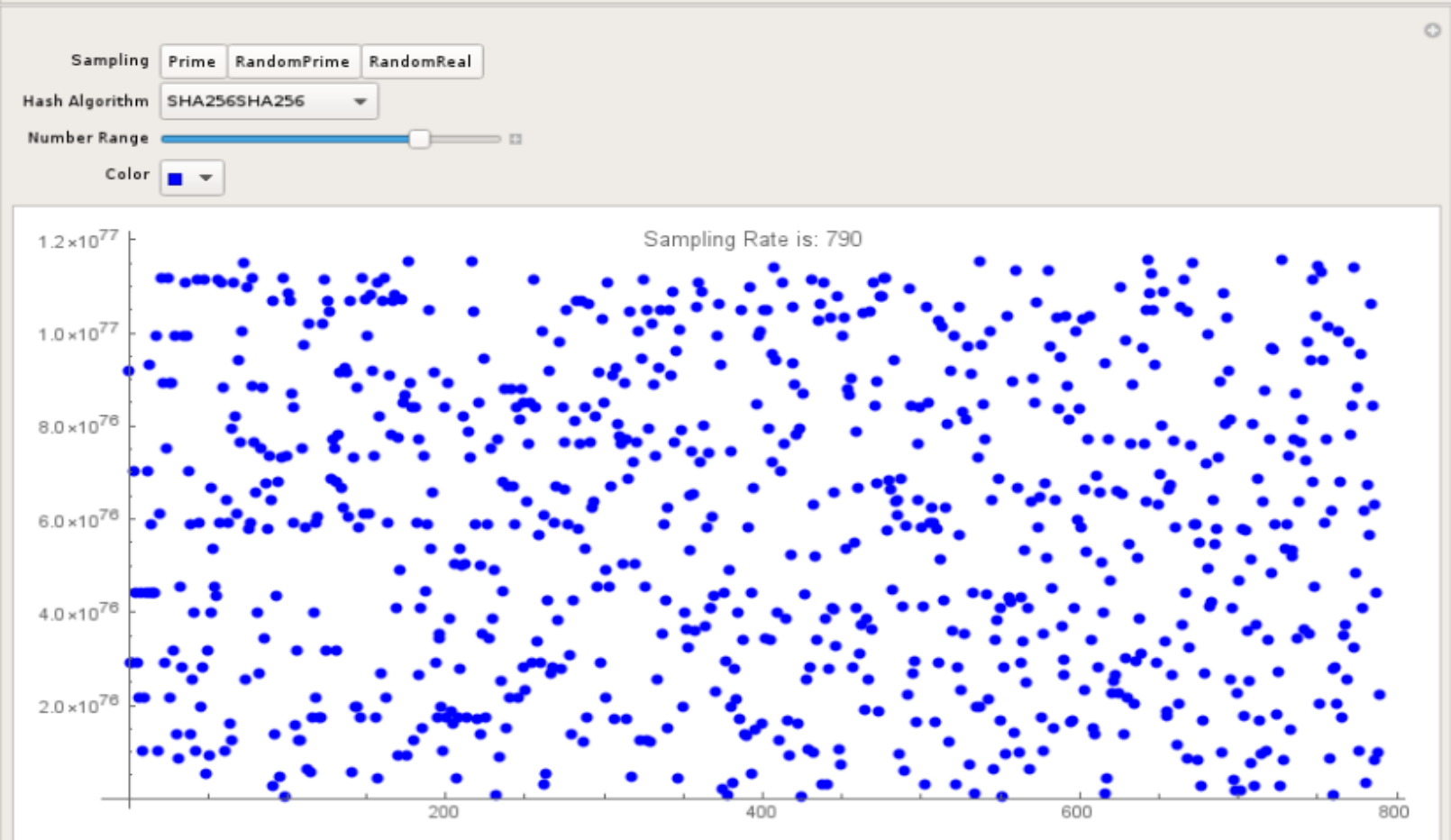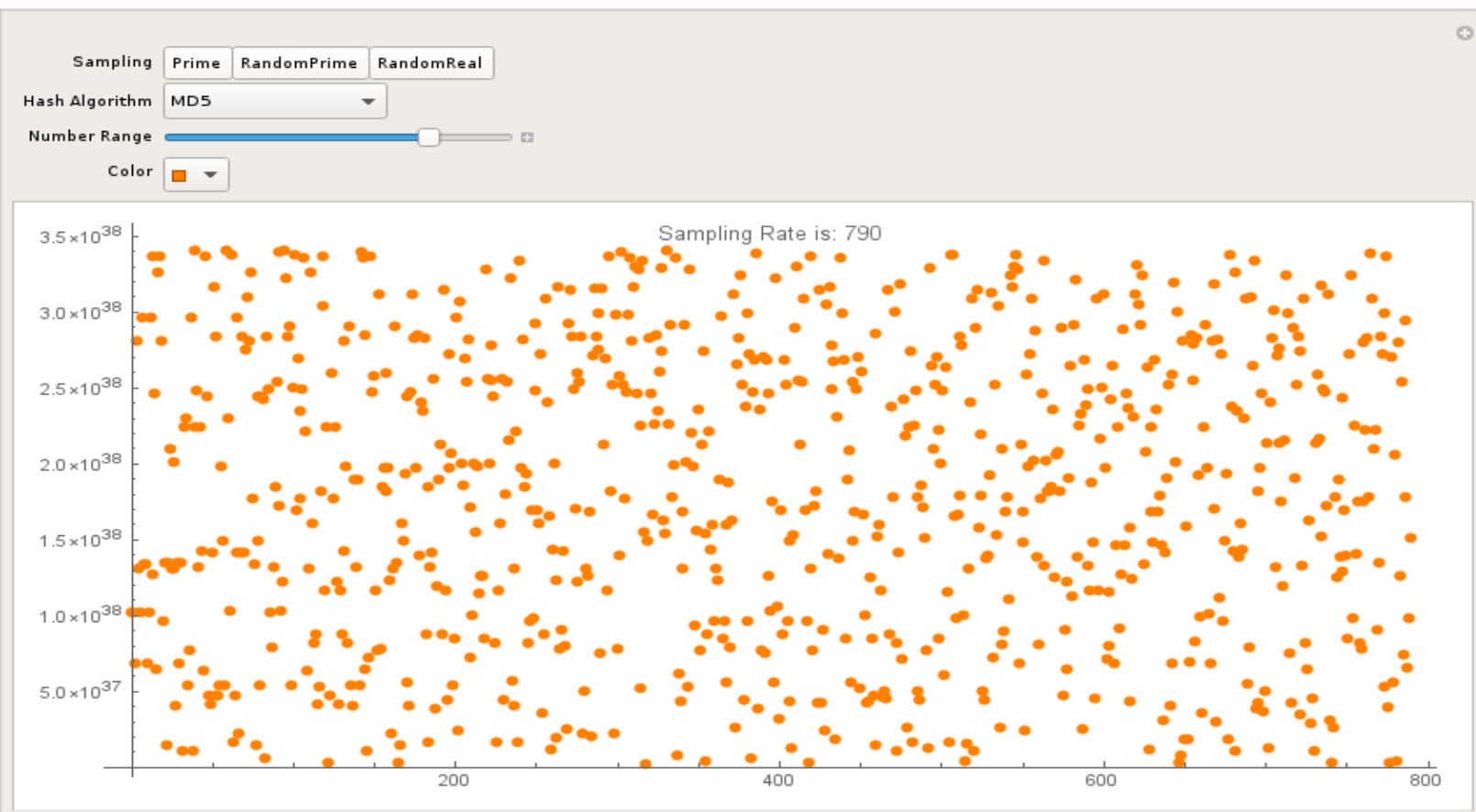
✘   *Symmetric Key Encryption*

SymmetricKey [cipher: AES256
block mode: CBC
key length: 256 bits]

Symmetric Key	Properties
Cipher	AES256
Key	ByteArray [32 bytes]
InitializationVector	None
BlockMode	CBC

✘   *Asymmetric Key Encryption*

⟨ | PrivateKey → PrivateKey [⊞ cipher: RSA
public modulus length: 2048 bits
private exponent length: 2044 bits] ,

PublicKey → PublicKey [⊞ cipher: RSA
public modulus length: 2048 bits] | ⟩

✘ *Binary Analysis (**Block Volatility**)*

Comparisons between ECB and CBC

ECB				
CBC				

ECB .vs. CBC