Cryptography: The Science of Secret Codes

– Discrete Mathematics: Assignment 3 –

submitted by

Ronit Singh and Ahsen Saaim

November 15, 2020

Ronit Singh and Ahsen Saaim
rs7358@nyu.edu and as13805@nyu.edu
Student ID: N14913479 and N10998807

Supervisor

1st: Moumena Chaqfeh
2nd: Dena Ahmed

Abstract

This report aims to provide a broad review of network security and cryptography. It introduces you to Cryptography Techniques that are done with the help of Discrete Mathematics. Cryptography is "The science of protecting data" and Network Security "keeping information private and secure from unauthorized users". The Cryptographic Process explaining through a generalized function is discussed through which encryption and decryption is done by the various algorithms like RSA algorithm, Hash functions and many cryptographic algorithms.

With the internet having reached a level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone connected to the web. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various algorithms and methods have been developed. Cryptography exactly deals with these techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender.

1 Introduction

Cryptography is the science of information security. The word is derived from the Greek "kryptos" meaning hidden, and "graphein" meaning To Write.

Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptology prior to the modern age was almost synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The sender retained the ability to decrypt the information and therefore avoid unwanted persons being able to read it. Since WWI and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

The main users of cryptographic system are the military, the diplomatic, banks, commercial, and government services. The increase of computers and communications systems in the mid of 1960s, brought with it a demand from the private sector, for means to protect information in digital form and to provide security services.

TYPES OF CRYPTOGRAPHY:

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Functions

2 Problem/Application Description

A message is plaintext (sometimes called cleartext). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption.

Mentioned below are some ciphers or methods that are used in cryptography with the help of discrete mathematics:

2.1 The Shift Cipher

Shift Cipher is one of the earliest and the simplest cryptosystems. A given plaintext is encrypted into a ciphertext by shifting each letter of the given plaintext by n positions. The 26 letters of the alphabet are assigned numbers as below:

$A \rightarrow 0, B \rightarrow 1, C \rightarrow 2, ..., Z \rightarrow 25$

The recipient of this message would then shift the letters back by the same number and obtain the original message.

2.2 The Caesar Cipher

The Caesar cipher is one of a family of ciphers called Shift ciphers.

The Caesar cipher is named after Julius Caesar , who used it to protect messages of military significance. Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet, sending the last three letters to the first three letters (by assigning 0, 1, 2, ..., 25 to each letter).

$A \rightarrow 0, B \rightarrow 1, C \rightarrow 2, ..., Z \rightarrow 25$

For example, the letter B is replaced by E and the letter X is replaced by A. This process of making a message secret is called encryption.

The recipient of this message would then shift the letters back by the same number and obtain the original message.

2.3 The Affine Cipher

Affine cipher is a monoalphabetical symmetrical substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. The whole process relies on working modulo m (the length of the alphabet used).

Affine cipher eliminates the biggest drawback of the Caesar cipher i.e. very easy cryptanalysis stemming from the low number of possible transformations.

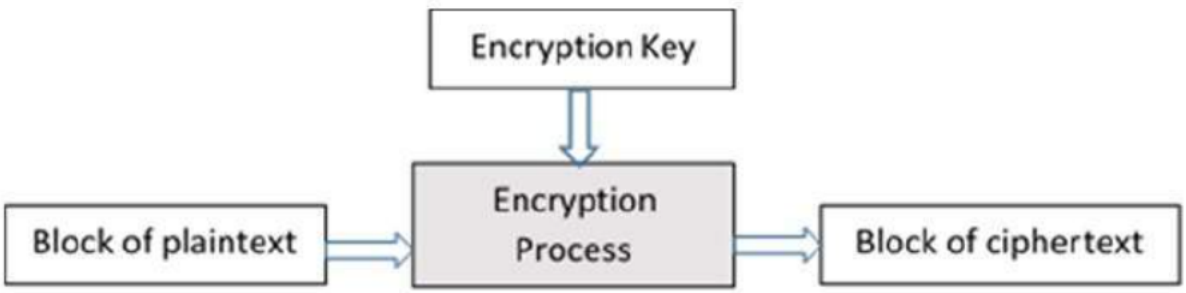
Because there are many possible combinations of input parameters of the Affine cipher, the brute force attack is inefficient, but still feasible. The weak point of the cipher is the frequency analysis.

2.4 The Block Cipher

Block cipher is an encryption method which divides the plain text into blocks of fixed size. Each block has an equal number of bits. At a time, block cipher operates only on one block of plain text and applies key on it to produce the corresponding block of ciphertext.

While decryption also only one block of ciphertext is operated to produce its corresponding plain text. Data Encryption Standard (DES) is the best example of it.

The basic scheme of a block cipher is depicted as follows



- A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size.
- The size of block is fixed in the given scheme.
- The choice of block size does not directly affect to the strength of encryption scheme.
- The strength of cipher depends up on the key length.

Though any size of block is acceptable, following aspects are borne in mind while selecting a size of a block.

- Avoid very small block size.
- Do not have very large block size.
- Blocks should be multiples of 8 bit.

2.5 The RSA (Rivest–Shamir–Adleman) System

RSA (Rivest–Shamir–Adleman) algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name RSA algorithm.

It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone.

The RSA algorithm holds the following features

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

Under RSA encryption, messages are encrypted with a code called a public key, which can be shared openly. Due to some distinct mathematical properties of the RSA algorithm, once a message has been encrypted with the public key, it can only be decrypted by another key, known as the private key. As the name suggests, the private key must be kept secret.

Without being able to access the private key, the original file can't be decrypted. This method can be used to keep messages and files secure, without taking too long or consuming too many computational resources.

Public key encryption schemes differ from symmetric-key encryption, where both the encryption and decryption process use the same private key. These differences make public key encryption like RSA useful for communicating in situations where there has been no opportunity to safely distribute keys beforehand.

2.6 The Cryptographic Hash Function

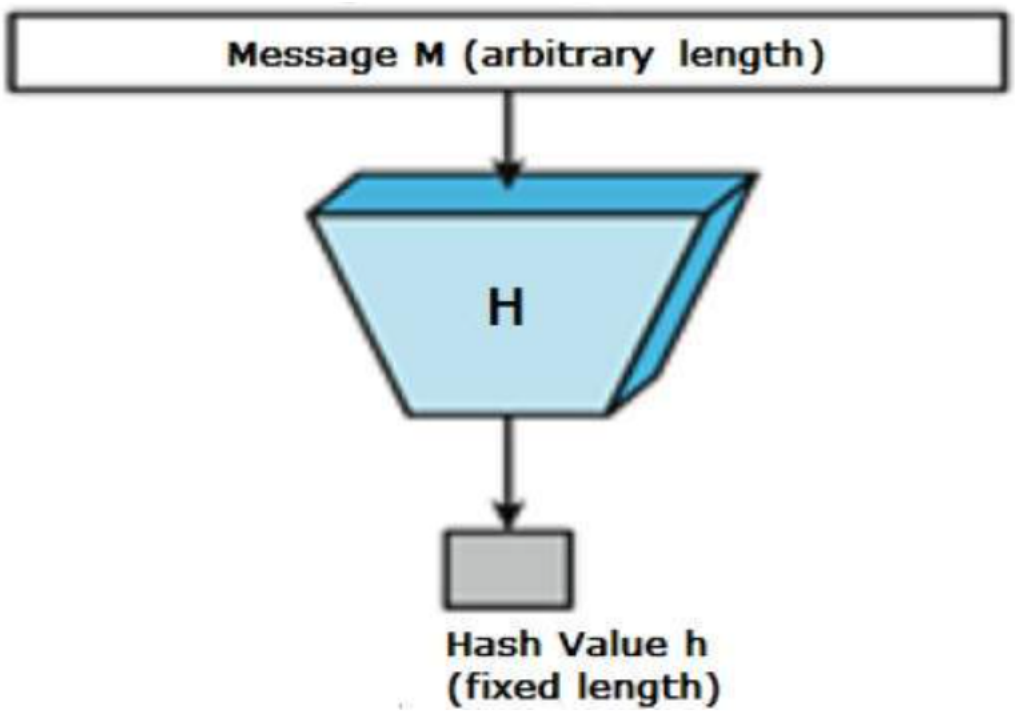
A cryptographic hash function is an algorithm that takes an arbitrary amount of data input—a credential—and produces a fixed-size output of enciphered text called a hash value, or just "hash." That enciphered text can then be stored instead of the password itself, and later used to verify the user.

Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called message digest or simply hash values.

The following picture illustrates hash function:



3 How this problem/application is related to Discrete Mathematics

Ciphers and codes use many tools from abstract algebra, number theory. and linear algebra including: congruences, quadratic residue theory, field theory, matrices, non-commutative groups, various mathematical algorithms, hash functions, and quantum algorithms. For instance, Number Theory and Modular arithmetic play a very large part in Cryptography.

All of these tools are part of Discrete Mathematics.

3.1 The Shift Cipher

Once we have coded the letters A, ..., Z, a general shift cipher with shift k can be described by:

$$f(p) \rightarrow (p + k) \bmod 26$$

MATH IS COOL becomes 12001907 08 18 02141411 if we just encode the letters. If we shift by 15, we get:

Letter	M	A	T	H	I	S	C	O	O	L
Coded	12	00	19	07	08	18	02	14	14	11
Shifted	1	15	8	22	23	7	17	3	3	00
Decoded	A	P	I	W	X	H	R	D	D	A

If we receive the message “APIWXHRDDA” and know that the shift key is 15, We just reverse the procedure above to decrypt our message, code the letters, shift by 15 which is the same as +11 mod 26, decode the result.

Cipher Letter	A	P	I	W	X	H	R	D	D	A
Coded	1	15	8	22	23	7	17	3	3	00
Shifted	12	00	19	07	08	18	02	14	14	11
Letter	M	A	T	H	I	S	C	O	O	L

3.2 The Caesar Cipher

The Caesar cipher is one of a family of ciphers called shift ciphers. Letters can be shifted by an integer k, with 3 being just one possibility. The encryption function is:

$$f(p) = (p + 3) \bmod 26$$

and the decryption function is:

$$f(p) = (p - 3) \bmod 26$$

Example: Encrypt the message "CAESAR" using the Caesar cipher.

Solution: Replacing characters with values,

02 01 04 18 01 17

Now replace each of these numbers p by $f(p) = (p + 3) \bmod 26$.

05 04 07 21 04 20

Translating the numbers back to letters produces the encrypted message:

"FEHVEU"

Decryption of the same can be done similarly by using $f(p) = (p - 3) \bmod 2$ instead.

3.3 The Affine Cipher

Encryption Process

It uses modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that correspond to a ciphertext letter. The encryption function for a single letter is:

$$E(x) = (ax + b) \bmod m$$

modulus m: size of the alphabet.

a and b: key of the cipher.

a must be chosen such that a and m are co-prime.

Decryption Process

In deciphering the ciphertext, we must perform the opposite (or inverse) functions on the ciphertext to retrieve the plaintext. Once again, the first step is to convert each of the ciphertext letters into their integer values. The decryption function is:

$$D\ (x) = a^{-1}\ (x - b) \bmod m$$

a^{-1} : modular multiplicative inverse of a modulo m.

3.4 The Block Cipher

Block ciphers replace blocks of letters with other blocks of letters.

The key is a permutation σ of the set $\{1, 2, \ldots, m\}$, where m is an integer, that is a one-to-one function from $\{1, 2, \ldots, m\}$ to itself.

To encrypt a message, split the letters into blocks of size m, adding additional letters to fill out the final block.

Example: using the transposition cipher based on the permutation σ of the set {1, 2, 3, 4} with $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 2$.

a) Encrypt the plaintext "DISCRETE MATH".

Solution:

Split the plaintext into four blocks "DISC RETE MATH"

Apply the permutation giving "ICDS EERT AHMT"

b) Decrypt "ICDS EERT AHMT", encrypted with the same cipher.

$\sigma^{-1}(1) = 2$, $\sigma^{-1}(2) = 4$, $\sigma^{-1}(3) = 1$, $\sigma^{-1}(4) = 3$

Apply the permutation σ^{-1} giving "DISC RETE MATH"

Split into words to obtain "DISC RETE MATH"

So, the decrypted message is DISCRETE MATH.

3.5 The RSA System

The implementation of RSA makes heavy use of modular arithmetic, Euler's theorem, and Euler's quotient function.

It is based on the principle that it is easy to multiply large numbers, but factoring large numbers is very difficult. For example, it is easy to check that 31 and 37 multiply to 1147, but trying to find the factors of 1147 is a much longer process.

Encryption Process

Sender A does the following:-

- Obtains the recipient B's public key (n,e).
- Represents the plaintext message as a positive integer m with $1 < m < n$.
- Computes the ciphertext C = M^e mod n.
- Sends the ciphertext c to B.

Now let's take a simple example i.e. we want to encrypt the message m = 7.

Public key = (n, e) = (33, 3)

Private key = (n, d) = (33, 7)

So, C = M^e mod n = 73 mod 33 = 343 mod 33 = 13

Hence the cipher-text c = 13.

Decryption Process

Recipient B does the following:-

- Uses his private key (n,d) to compute M' = C^d mod n.
- Extracts the plain-text from the message representative m.

To check decryption in the above example, we compute:

M = C^d mod n = 137 mod 33 = 7

4 Conclusion

In this report, we have explored how the various concepts taught in Discrete Mathematics are extremely useful in Cryptography, providing functionality for the encryption and decryption of data and authentication of other users.

Security structures and passwords for computers and other electronic systems, is based entirely on Discrete Mathematics. This is partly because computers send information in discrete – or separate and distinct – bits.

5 References

- RSA encryption https://brilliant.org/wiki/rsa-encryption/rsaencrypt, title=RSA Encryption, author=Alexander Katz, Aloysius Ng, Patrick Bourg, publisher=Brilliant
- https://www.researchgate.net/profile/Anupama_Mishra5/publication/276321131_ENHANCING_SECURITY_OF_CAESAR_CIPHER_USING_DIFFERENT_METHODS/links/565c83be08ae1ef92981e66d.pdf@articlemishra2013enhancing, title=Enhancing security of caesar cipher using different methods, author=Mishra, Anupama, journal=International Journal of Research in Engineering and Technology, volume=2, number=09, pages=327–332, year=2013
- http://www.programming-algorithms.net/article/40729/Affine-cipher
- https://www.comparitech.com/blog/information-security/rsa-encryption/lake2018 title=What is RSA encryption and how does it work?, author=Lake, Josh, year=2018, publisher=December
- https://www.tutorialspoint.com/cryptography/block_cipher.htm@article title=Learn cryptography Block cipher, publisher=tutorialspoint,
- https://sciencing.com/applications-discrete-math-8368995.html title=What Are the Applications of Discrete Math?, author=Damon Verial, year=2018