Reading Report: Cryptography

A Security Pillar of Privacy, Integrity, and Authenticity of Data Communication

Vaishnavi Deshpande

May 2, 2021

Abstract

The number of cyberattacks have seen a monumental increase over the last few years, with 2020 registering almost 155.8 million records[1] being compromised because of the lack of appropriate information security. Therefore, there is a pressing need to understand cryptography so that we can effectively relay digital material in a secure manner. In this report I provide a comprehensive report on the paper, “Cryptography - A security pillar of privacy, integrity and authenticity of data communication”[2]. In this paper, the authors have highlighted mathematical concepts such as modular arithmetic and the extended Euclidean algorithm to outline the implementations of advanced encryption ciphers. I have analyzed the paper and presented an explanation of the concepts using proofs and diagrams to support my work.

1 Introduction

Although companies, and individuals are aware of the detrimental effects of cyberattacks, not enough has been done in order to secure private information. According to research conducted by Varonis, only 5% of folders are adequately protected[3]. Furthermore, the development in machine learning algorithms have only increased the potential of threats because of their heightened ability to crack codes and recognize patterns. Therefore, with the rapid advancements in these high potential technologies, it has become necessary for companies and individuals to enhance their awareness about methods and strategies to keep their data safe from malicious attackers. The authors in the chosen paper stress the importance of cryptography in tackling these pressing issues. They highlight the necessary mathematics (modular arithmetic, linear congruence, and the extended Euclidean algorithm) needed for readers to understand complex topics in cryptography such as types of ciphers, encryption standards (Data Encryption Standard and Advanced Encryption Standard), and other topics (chosen-cipher attack, Diffie-Helman algorithm, RSA digital signature scheme, and others) that support these concepts. The chosen paper covers a wide range of complexities, ranging from the simple Euclidean Algorithm to an advanced implementation of AES. A comprehensive analysis using proofs and diagrams is provided.

2 Prerequisite Mathematics

2.1 The Euclidean Algorithm

This algorithm is a method to efficiently calculate the greatest common divisor (GCD) of two natural numbers. I present the recursive steps to find the where a and b are both natural numbers.

1. If then (base case)
2. If then (base case)
3. is written in a form that satisfies the following conditions.
4. Now, needs to be calculated (recursive step)

The authors provide an example and can be solved using the provided steps:

2.2 The Extended Euclidean Algorithm

This algorithm provides us a way to express as a linear combination of the numbers a and b:

Here

2.2.1 Finite Field or Galois Field

First, I define a field: A field is a set on which basic operations such as addition, subtraction, multiplication, and division are defined. These operations must have the same effect on each of the elements as they do on real numbers. Further, such a set of fields which have only a finite number of elements are called Galois fields[4].

Using this high-level understanding of fields, an idea of the operations performed on fields can be formed. The authors use the Extended Euclidean Algorithm to find the multiplicative inverse in a Galois field. This step offered a level of complexity that can be resolved through a deeper understanding of Galois Fields. However, a fair comprehension of the authors’ example was achieved.

2.3 Modular Arithmetic

2.3.1 Definition and Notation

For two given integers, the modulo operator is defined as the remainder obtained when dividing the two values such that the quotient obtained is an integer as well.

The complete set of residues is a set consisting of possible remainders for a given number. This is not a unique set for a number.

For example:

The complete set of residues modulo 100 can be written as .

However, another such set is .

2.3.2 Congruence

Consider

The above is equivalent to saying that n divides the difference of p and q.

Residue classes are described to be a set of integers where values from two different residue classes can never result in a congruency as defined above

If , then we see that:

and

If two numbers are picked from two distinct sets, the difference of their values can never yield a multiple of 100.

The authors also introduce theorems of congruence:

*Theorem 1.* suppose

Then,

1.

2.

I have presented a proof for the above:

It is given that . This implies that:

Similarly, as well

For part 2, we see that:

*Theorem 2.* suppose

Then,

We have,

If d is given to be we know that are both integers

Therefore, dividing both sides with d, we get

Here the entire RHS is a product of three integers.

3 Ciphers

Ciphers are a combination of computations or algorithms that perform an encryption and further also provide the steps for decryption. The authors introduce important types of ciphers. Here, I discuss the combinatorics that can be applied.

3.1 Substitution Ciphers

In a simple substitution, each letter of the alphabet is mapped onto a letter from the alphabet. In a more general case, it is possible for a particular letter to map onto itself.

Here I consider all possible cases of substitution ciphers,

Let A be the set:

So, we have:

Therefore, if we are to find all the possible mapping for each letter in A, we just need to permute them and match them with each letter in the respective positions.

Therefore, the total number of possible ciphers is

If we were to make sure that no letter maps to itself, we can apply the concept of derangement. A derangement of is a permutation such that:

Let the possible number of such permutations be

3.2 Caesar Cipher

This cipher is very common and is also known as the shift cipher. The possible mapping to the alphabet is actually a much smaller subset than the general substitution cipher. This leads to the fact that decryption is very easy for this type. However, it easy to understand as noted by the authors as well.

Here each letter is mapped onto a letter in the alphabet that is a fixed number of indices away from it.

For example, let the fixed number be

For

In the above example, A maps to B and B maps to C and so on. We see that in the Caesar Cipher, there are only 25 possible fixed numbers to shift. At the 26th shift, we are back to alphabetical order. Since the possible keys are so few, such a cipher is incredibly easy to crack.

3.2 Transposition Ciphers

This method of encryption differs from substitution ciphers. Here, the resulting ciphertext is a permutation of the text that is to be encrypted, that is, there is no type of disguise applied on the letters. The positions of the characters are shifted according to some bijective function and by definition, its inverse is used to decrypt.

The number of possible transposition ciphers are dependent on the number of characters in the original message. The number of possible keys is way too many to compete with substitution ciphers.

If there are  characters in the plaintext, the possible number of permutations will be . If the message is large, it is a tremendous task to crack the code.

A simple example would be the Rail Fence Cipher where the characters is arranged on diagonal position in horizontal rails. For example, if we were to encrypt the message- “U RAH RAH WISCONSIN”

We would write it out this way.

U . . . R . . . I . . . N . . .

. R . H . A . W . S . O . S . N

. . A . . . H . . . C . . . I .

3.3 Symmetric Ciphers

The authors introduce the important concept to set up an implementation of the Advanced Encryption Ciphers. The technique of splitting up data into chunks of blocks helps us get started with the concept of block ciphers.