College of Natural and Computational Science
Department of Mathematics

INTRODUCTION TO CRYPTOGRAPHY

Prepared by: Abdulhakim Jemal

Advisor: mr.Ayele Hailu

A Project Submitted to the Department of Mathematics, Wolkite University in Partial Fulfillment of the Requirements of the Bachelor of Science Degree in Mathematics

January, 2021

Contents

Wolkite University
Department of Mathematics

The undersigned hereby certify that they have read and recommend to the Department of Mathematics for acceptance of a project entitled **Introduction to Cryptography** by Student name in partial fulfillment of the requirements for the degree of Bachelor of Science.

Dated: January,2021

Advisor: _____
Advisor name

Examining committee: _____

_____

January, 2021

Acknowledgment

First and fore most I would like to thanks my creature ALLAH! who is most merciful and beneficiary. allowing me to be in these stages grate for respect to my family for their continues in all situation and able to thank all friend that contribute to this work.I pay a very big tribute to my advisor MR.Ayele Hailu for limitless effort in guiding supervising and making critical reading of my project.Finally,I would like to thank the department of mathematics,for all support that I have got during my study.

Abstract

The project contains two chapter,the first chapter is about preliminaries concepts and the second chapter is about Mathematics of cryptography.More general the first chapter contains specially definition of cryptography,history of cryptography and Goal and service of cryptography and the second chapter contain basic definition and Example of algebraic structure.Finally this paper contains conclusion and reference.

Introduction

Cryptography is stuff of novels and action comics.kids once saved up oval tine labels and sent away for contain mid nights secret decoder ring.Almost every one has seen a television show or movies involving a nondescript suit clad gentle-man with a brief case hand cuffed to his wrist.sales report to a coworker in away that no else can read it.you just want to be sure that your colleague was the actual and only recipient of the email and you want to him or her to know that you were unmistakably the sender.It's not national security at state,but if your company's competitor got hold of it,it could cost you.

Chapter 1

preliminaries

1.1 Definition of cryptography

Cryptography is the science of using mathematics to encrypt and de crypt data.cryptography enable you to store sensitive information or transmit it across in secure net work (like the internet)so that it cannot be read by any one except the intended recipient.While cryptography is the science of analyzing and breaking secure communication.classical cryptanalysis involves an interesting combination of analytical reasoning,application of mathematical tools,pattern finding,patience,determination and luck. Fundamental building block of security is Cryptography

A **cryptosystem** is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

The various components of a basic cryptosystem are as follows:

- **Plain text**:The original message,before being transformed.
- **Encryption Algorithm**:transforms the plain text into cipher.
- **cipher text**:After the message transformed.
- **Decryption**: Recovering plain text from the cipher text
- **secret Key**:Used to set some or all of the parameters/numbers used by the encryption algorithm.
- **Decryption algorithm**:trans forms the cipher text back into plain.

While **cryptography** is the science of securing data, **cryptanalysis** is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. **Cryptology** embraces both cryptography and cryptanalysis.

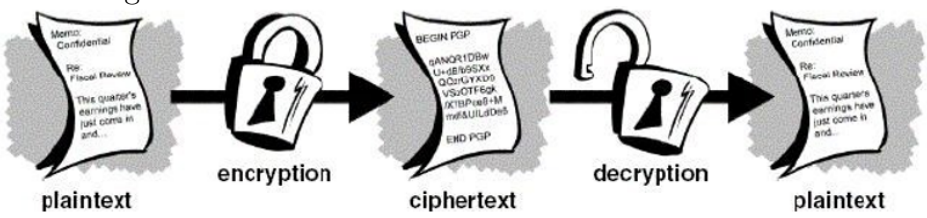
1.2 Encryption and Decryption

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**.

- **Encryption**:a process of encoding a message so that is meaning is not obvious.
- **decryption**:the reverse process
- **plain text**:the original form of a message
- **cipher text**:the encrypted form

A **cipher (or cypher)** is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure.

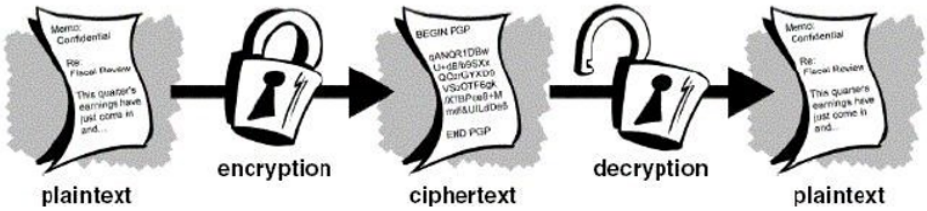
Example1:if we encode the word"**THE TIME IS LIFE**"using caeser key value of 2,we off set the alphabet so that second letter down (c) begins the alphabet.
so starting with



plain text:A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

cipher text: C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
where **A=C ,B=D, C=E**and so on.
using this scheme the plain text"**THE TIME IS LIFE**"encrypt as"**VJGVKOGKUNKHG**".To allow some one else to read the cipher text,you tell them that the key is 2

Example2:if we encode the word"**HELLO**"using caeser key value of 3,we off set the alphabet so that third letter down (D) begins the alphabet.
so starting with



plain text:A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

cipher text: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
where **A=D ,B=E, C=F**and so on.

using this scheme the plain text"**HELLO**"encrypt as"**EBIIL**".To allow some one else to read the cipher text,you tell them that the key is 3.

1.3 History of cryptography

As civilization evolved human being got organized in tribes,groups and kingdoms,This led to the emergence of ideas such a power,battles,supremacy and politics.These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured in the continuous evolution of cryptography as well.The root of cryptography are found in roman and Egyptian civilization.

Cryptography is one of the oldest fields of technical study we can find records of, going back at least 4,000 years. It is quite noteworthy that of all the cryptosystems developed in those 4,000 years of effort, only 3 systems in widespread serious use remain hard enough to break to be of real value. One of them takes too much space for most practical uses, another is too slow for most practical uses, and the third is widely believed to contain serious weaknesses.

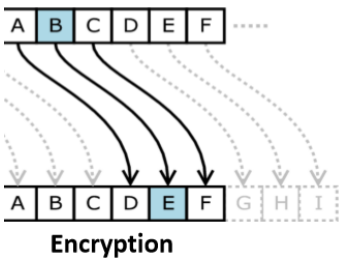
We begin with a classification scheme for ciphers given by Gary Knight [Knight78] in the first of a series of articles which posed ciphers to the reader, and after a given period of time demonstrated reader solutions along with explanations of how they solved the ciphers. Versions of the solutions attained by the author were also given along with many mathematical techniques for "attacking the unknown cipher".

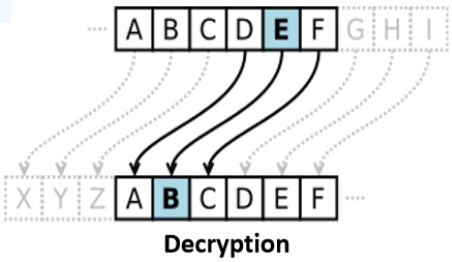
1.3.1 caesar shift cipher

caeser shift cipher the letter of a message by an agreed number (three was a common choice),the recipient of this message would then shift the letter back by the same number and obtain the original message The Caeser cipher named after Julius caeser,who used it with a shift of three to protect message of military significance.

Example:if we encode the word"**TREATY IMPOSSIBLE**"using caeser key value of 3,we off set the alphabet so that third letter down (D) begins the alphabet.

so starting with





plain text: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

cipher text: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
where **D=A ,E=B, F=C**and so on.

using this scheme the plain text"**TREATY IMPOSSIBLE**"encrypt as"**Wuhdwb lpsrvvleoh**".To allow some one else to read the cipher text,you tell them that the key is 3.

1.3.2 kamasutra cipher

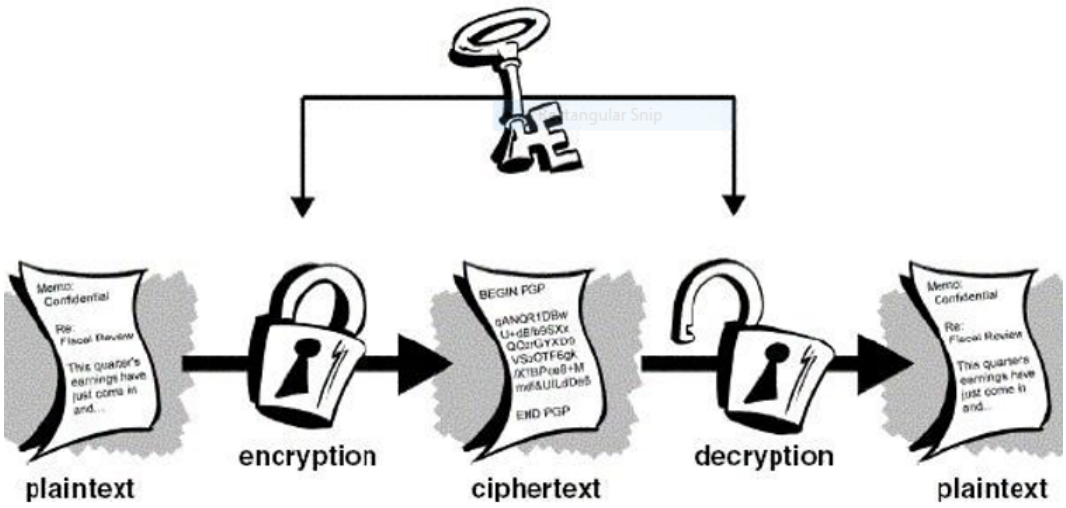
The Kamasutra cipher is one of the earliest known substitution method.It described in the kamasutra 400 BC.The purpose was to teach women how to hide secret message from prying eyes.The techniques involves randomly pairing letter of the alphabet and then substituting each letter in the original message with in partner.

1.4 Types of cryptography

1.4.1 symmetric key cryptography

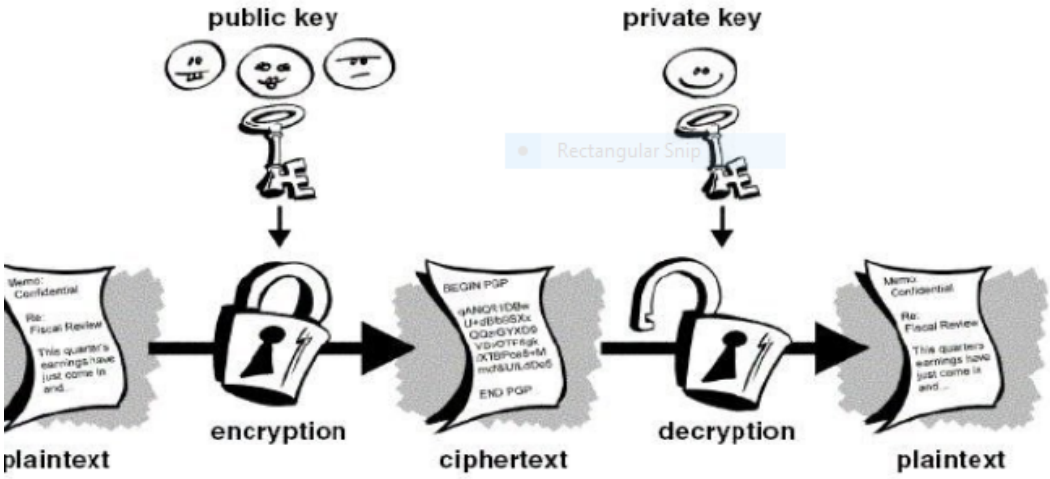
Also known as **Secret Key Cryptography or Conventional Cryptography, Symmetric Key Cryptography** is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. The Algorithm use is also known as a secret key algorithm or sometimes called a symmetric algorithm A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher.

The key for encrypting and decrypting the file had to be known to all the recipients. Else, the message could not be decrypted by conventional means.



1.4.2 Asymmetric key cryptography

Asymmetric cryptography , also known as**Public-key cryptography**, refers to a cryptographic algorithm which requires two separate keys, one of which is private and one of which is public. **The public key** is used to encrypt the message and the **private** one is used to de crypt the message.



1, Give your public key to the sender.

2, Sender uses your public key to encrypt the plain text.

3, Sender gives the cipher text to you.

4, Use your private key and pass phrase to de crypt the cipher text.

ElGamal

- **ElGamal** is a public key method that is used in both encryption and digital signing.
- **The encryption algorithm** is similar in nature to the Diffie-Hellman key agreement protocol
- It is used in many applications and uses discrete logarithms.
- **ElGamal encryption** is used in the free GNU Privacy Guard software

1.4.3 Hash function

A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest.

The ideal cryptographic hash function has four main properties:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash

1.5 Goal and service of cryptography

Goal: The primary goal of cryptography is to secure important data on the hard disk or as it passes through a medium that may not be secure itself. Usually, that medium is a computer network.

Services: Cryptography can provide the following services:

- **Confidentiality (secrecy)**
- **Integrity (anti-tampering)**
- **Authentication**
- **Non-repudiation**

Confidentiality (secrecy)

- Ensuring that no one can read the message except the intended receiver
- Data is kept secret from those without the proper credentials, even if that data travels through an insecure medium

Integrity (anti-tampering)

- Assuring the receiver that the received message has not been altered in any way from the original.

Authentication

- Cryptography can help establish identity for authentication purposes The process of proving one's identity.
- (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)

Non-repudiation

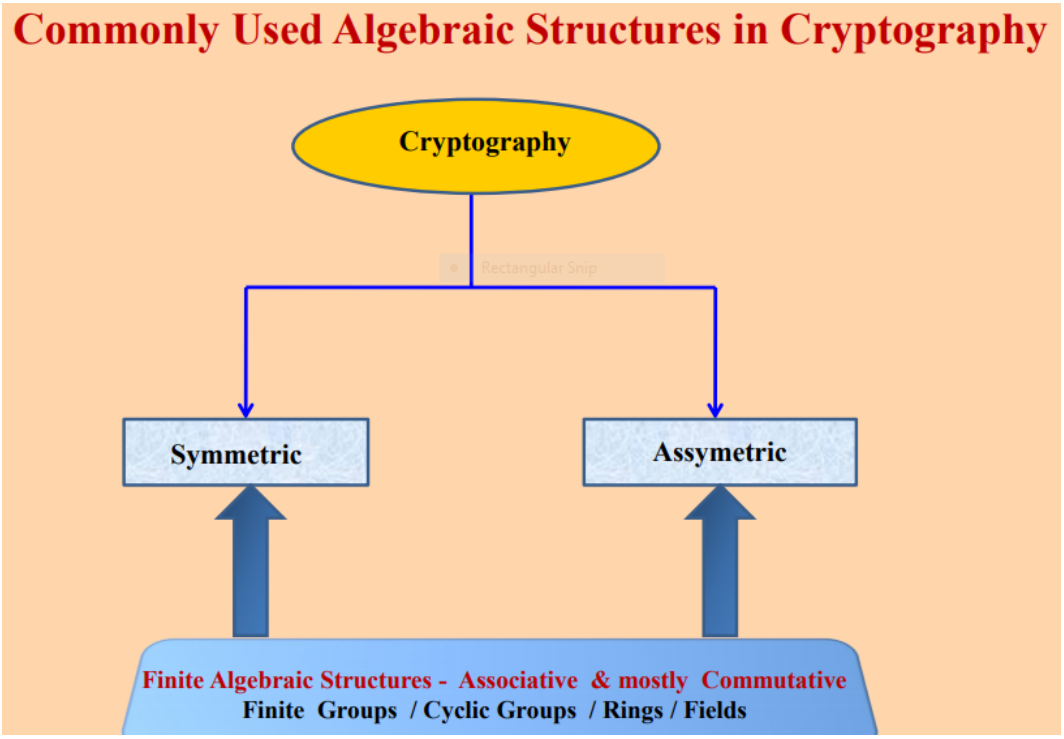
- A mechanism to prove that the sender really sent this message

Chapter 2

Mathematics of cryptography

2.1 Algebraic structure

Cryptography requires sets of integers and specific operation that are defined for those sets. The combination of the set and the operation that are applied to the elements of the set is called **An Algebraic structure**.



- Finite Fields , are used mainly in Symmetric Ciphers
- z_n and Z_n^* are another two important structures in cryptography
- In public key cryptography based on DLP mainly used prime order cyclic subgroup of z_p^*

- For secrecy generally use modulo large prime /GF(2^m) where m is quite large ECDLP also based on cyclic group
- Choice of the cyclic groups are important for the security.

All these structures are Associative and Commutative

In this chapter,we will define two common algebraic structure:**groups and ring.**

Common Algebraic structure

- Group
- Ring

2.1.1 Group

Definition:A group (G) is a set of element with a binary operation (.) that satisfied four properties or axiom . A commutative group satisfied an extra property,commutativity:

- **Closure**
- **Associativity**
- **Existence of identity**
- **Existence of inverse**

commutativity is needs to be satisfied only for a commutative group

Application
Although a group involves a single operation, the properties imposed on the operation allow the use of a pair of operation as long as they are inverses each other.

Example The set residues integer with the addition operator,$G =< Z_n, + >$, is a commutative group,we can perform addition and subs traction in the element of this set with out moving out of the set.

Example The set Z_{n^*} with multiplication operator,$G =< Z_{n^*}, * >$is also an Abelian group.

- $\forall$ a,b $\in z_n$, $a \bullet b \in z_n$
- $\forall$ a,b, c $\in z_n$,(ab)•c=a•(bc) $\in z_n$
- $\forall$ 1 $\in z_n$, $\exists$ 0 $\in z_n$ such that 0•1=0=1•0
- $\forall$ a $\in z_n$, $\exists$ $a^{-1} \in z_n$ such that a• a^{-1}=e=a^{-1} •a
- $\forall$ a,b $\in z_n$,ab=ba.

A very interesting group is the permutation group. The set is the set of all permutation and the operation is composition: app ling one permutation after another.

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \bullet \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

•	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	**[1 2 3]**	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	**[1 2 3]**	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
[2 1 3]	[2 1 3]	[3 1 2]	**[1 2 3]**	[3 2 1]	[1 3 2]	[2 3 1]
[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	**[1 2 3]**	[2 1 3]
[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	**[1 2 3]**	[2 3 1]	[1 3 2]
[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 3 1]	**[1 2 3]**

Cyclic group

Definition:If a sub group of a group can be generated using the power of an element, the sub group is called the **Cyclic sub group**

$a^n = a * a * ..... * a(ntimes)$

$a^n = a + a + ... + a(ifoperationaddition)$

Example

Four cyclic sub groups can be made from the group $G =< Z_6, \oplus >$ They are $H_1 =< (0), + >$,$H_2 =< (0, 2, 4), + >$,$H_3 =< (0, 3), + >$ and $H_4 = G$

- $0^0 mod 6 = 0$

- $1^0 mod 6 = 0$
- $1^1 mod 6 = 1$
- $1^2 mod 6 = (1 + 1) mod 6 = 2$
- $1^3 mod 6 = (1 + 1 + 1) mod 6 = 3$
- $1^4 mod 6 = (1 + 1 + 1 + 1) mod 6 = 4$
- $1^5 mod 6 = (1 + 1 + 1 + 1 + 1) mod 6 = 5$

- $2^0 mod 6 = 0$
- $2^1 mod 6 = 2$
- $2^2 mod 6 = (2 + 2) mod 6 = 4$

- $3^0 mod 6 = 0$
- $3^1 mod 6 = 3$

- $4^0 mod 6 = 0$
- $4^1 mod 6 = 4$
- $4^2 mod 6 = (4 + 4) mod 6 = 2$

- $5^0 mod 6 = 0$
- $5^1 mod 6 = 5$

- $5^2 mod 6 = 4$
- $5^3 mod 6 = 3$
- $5^4 mod 6 = 2$
- $5^5 mod 6 = 1$

A cyclic group is a group that is its own cyclic sub group.

$e, g, g^2, ...g^{n-1}.where g^n = e$

Example
The group $G =< Z_4, \oplus >$ is a cyclic group with two generates, g=1 and g=3

$1 \in Z_4 < 1 > = \{1^n / \text{n} \in Z\}$

$= \{0, 1, 2, 3\}$

$(z_4, \oplus 4)$ is cyclic group.

$3 \in Z_4 < 3 > = \{3^n / \text{n} \in Z\}$

$= \{0, 3, 2, 1\}$

$(z_4, \oplus 4)$ is cyclic group.

Lagrange's theorem
Assume that G is a group, and H is a sub group of G.If the order of G and H are $|G|$ and $|H|$,respectively ,then based on this theorem, $|H|$ divides $|G|$

Order of an element
The order of an element is the order of the cyclic group it generates

- If $a \in G$ is of finite order m then m is the smallest positive integer such that $a^m = e$

Example: In the group $G =< Z_4, \oplus >$,the order of the elements are:

- ord(0)=1 m=1

  ord(1)=4 because

- $1^1 = 1$
- $1^2 = 2$
- $1^3 = 3$
- $1^4 = 0 = e$ m=4

  ord(2)=2 because

- $2^1 = 2$
- $2^2 = 0 = e$ m=2

  ord(3)=4 because

- $3^1 = 3$
- $3^2 = 6$
- $3^3 = 9$
- $3^4 = 0 = e$ m=4

2.1.2 Ring

Definition:A ring $R =< +, \bullet, >$ is an algebraic structure with two operations.

$(R, +)$ **is an Abelian group.**

- **Closure**
- **Associativity**
- **Commutativity**
- **Existence of identity**
- **Existence of inverse**

(R, x) **multiplication**

- **Closure**
- **Associativity**
- **Commutativity**

Commutativity is only satisfied commutative ring.

Example
The set of integer with two binary operations, Addition and Multiplication is a commutative ring.we show it by $R =< Q, +, x >$.Addition satisfies all of the five properties;multiplication satisfies only 3 properties.

$(Q, +)$ **is an Abelian group.**

- $\forall$ a,b $\in$ Q,a+b $\in$ Q
- $\forall$ a,b c $\in$ Q,(a+b)+c=a+(b+c) $\in$ Q
- $\forall$ a $\in$ Q, $\exists$ 0 $\in$ Q such that 0+a=a=a+0
- $\forall$ a $\in$ Q, $\exists$ -a $\in$ Q such that a+(-a)=e=-a+a
- $\forall$ a,b $\in$ Q,a+b=b+a.

(R, x) **multiplication**

- $\forall$ a,b $\in$ Q,ab$\in$ Q
- $\forall$ a,b c $\in$ Q,(ab)c=a(bc).
- $\forall$ a,b $\in$ Q,ab=ba

Conclusion

In this project, We have presented on over view of the introduction to cryptography.This project provided the relevant and mathematics of cr cryptography.Generally,from this project understand the definition of cryptography,encryption,decryption,symmetric,asymmetric and mathematics of cryptography with example and also algebraic structure group and ring.

Bibliography

[1] Introduction to cryptography

[2] Cryptography and net work security

[3] http://www.xways.net/md5 collision.html