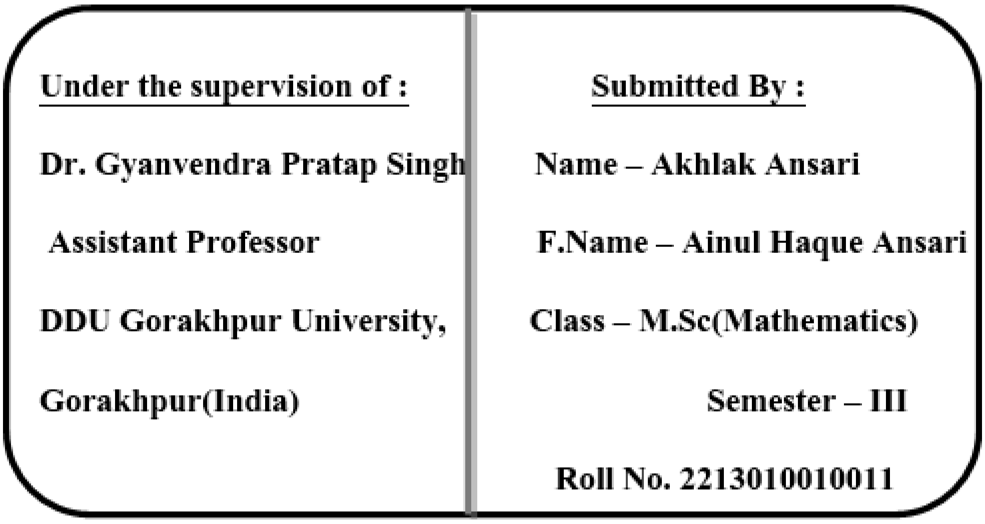
PROJECT: NUMBER THEORY

Akhlak Ansari

December 7, 2022

Department of Mathematics and Statistics



Under the supervision of :	Submitted By :
Dr. Gyanvendra Pratap Singh	Name – Akhlak Ansari
Assistant Professor	F.Name – Ainul Haque Ansari
DDU Gorakhpur University,	Class – M.Sc(Mathematics)
Gorakhpur(India)	Semester – III
	Roll No. 2213010010011

Fall' 2022-23

ROLE OF NUMBER THEORY IN CRYPTOGRAPHY

Number theory has an important role in Cryptographic foundation.To produce secret messages and send securely and secretly to the recepient in this technological era through internet, we must have knowledge of behaviour of numbers, which is summurize in the branch of mathematics called **Number Theory**.i.e what a number means and what kind of manipulation allows to do with numbers and all other kind of stuffs to encrypt the messages and make their secrecy. So In order to make an intuitive idea of **Cryptography**, we must have a deep knowledge of **Number Theory**.

Pre-Requisites:

1. Integers
2. Divisor
3. Division Algorithm
4. Greatest Common Divisor / gcd(a,b)
5. Least Common Multiple / lcm(a,b)
6. Euler totient function / Euler ϕ - function
7. Congruence
8. Encryption
9. Decryption

At this instance let's briefly discuss above mentioned pre-requisites.

1. Integers:

The integers is the set of positive and negative counting numbers including zero. It is represented by $\mathbb{Z}$.i.e

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

2. Divisor:

If an integer n can be eritten as a product $k \cdot d = n$ of two integers k and d , then we say that d divides n, or that n is divisible by d, or that d is a **divisor** of n. i.e

$$n = k.d \implies d|n. \; ; \; \forall \; n, k, d \in \mathbb{Z}$$

eg. 2|8, 6|24, 3|27 etc.

We occassionaly choose the term **proper divisor** to denote a positive divisor n which is not n. When $n = 8$, we see the that $1, 2, 4$ are all proper divisors.

3. Division Algorithm:

For $a, b \in \mathbb{Z}$ and $b > 0$, we can always write $a = q \cdot b + r$ with $0 \leq r < b$ and q an integer. Moreover, given a, b there is only one pair q, r which satisfies these constraints.We call the first element q the quotient and the second one r the remainder.

eg. $35 = 6 \cdot 5 + 5$.

4. Greatest Common Divisor:

If we consider the various divisors of two numbers a and b , we say that d is a **common divisor** of a and b if $d|a$ and $d|b$. If d is the bigger such common divisor, it is called the **greatest common divisor**, or gcd of a and b and written as,

$$d = gcd(a, b)$$

eg. $gcd(3, 10) = 1$.

5. Least Common Multiple:

Let a and b any two integers not both zero,then an integer $m \geq 1$ is called a **least common multiple** of a and b, if the following properties holds,

- $a|m$ and $b|m$
- For any integer n, if $a|n$ and $b|n$ then $m|n$.

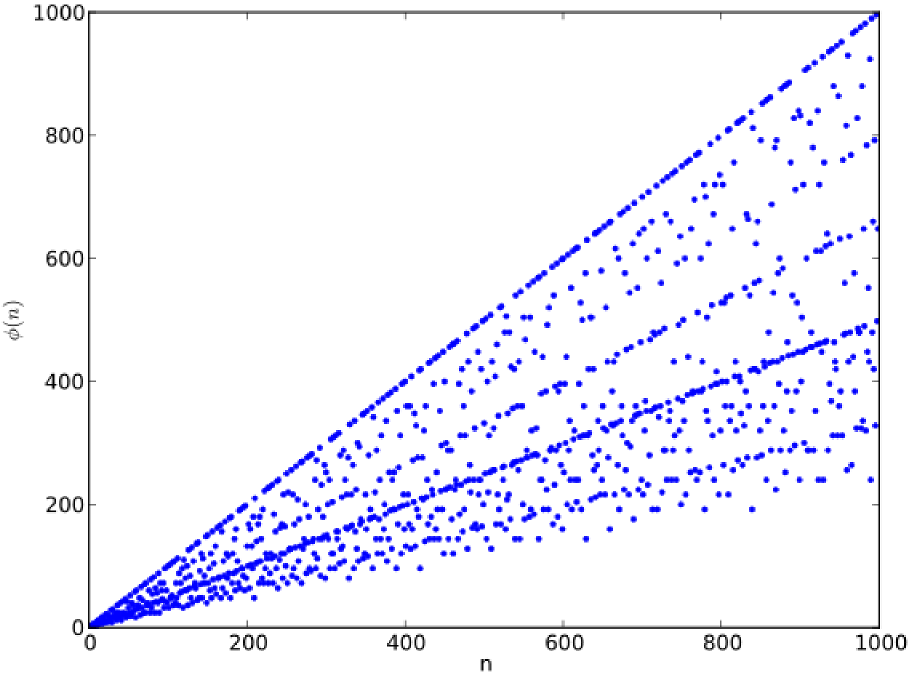
eg. $lcm(168, 490) = 5880$..

6. Euler totient function:

In number theory, Euler's totient function counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter ϕ as $\phi(n)$ and may also be called Euler's phi function. In other words, it is the number of integers k in the range $1 \leq k \leq n$ for which the greatest common divisor $gcd(n, k)$ is equal to 1. The integers k of this form are sometimes referred to as totatives of n.

$$\phi(n) = \{1 \leq k \leq n;\ gcd(n, k) = 1;\ \forall k, n \in \mathbb{Z}\}$$

On the next page we plot the data of first thousand $\phi(n)$ against first thousand primes n.(Courtesy: Wikipedia)



7. Congruence:

We say that a number a is congruent to b(another number) modulo n, or

$$a \equiv b \mod n$$

precisely if $n|(b-a)$. We call n, normally a positive integer greater than one,the modulus. The noun form of the relationship is called congruence.

8. Encryption:

Encryption is the method by which information is converted into secret code that hides the information's true meaning.

9. Decryption:

Decryption is a way to change electronic information or signals that were stored, written, or sent in the form of a secret code (= a system of letters, numbers, or symbols) back into a form that you can understand and use normally.

NOTE

The science of encrypting and decrypting information is called cryptography. In computing, unencrypted data is also known as plaintext, and encrypted data is called ciphertext.

Introduction:

Cryptography is a study of methods to communicate securely over an insecure line of communication. The main idea is to "encipher" the message into a form that only the intended recipient can understand.

Crypt, the root of the word,cryptography, comes from the Greek word "kryptos", meaning hidden or secret.It has played an important role throughout history. In ancient time, people used some simple forms of cryptography to protect their messages and knowledge. Some of Chinese silk traders studied how to protect the secret of manufacturing silk,and the Germans wanted to protect their military secrets by applying their famous Enigma machine. In recent times, cryptography is being widely used in computer industries, such as storing the user's information securely online, and protecting governmental secrets and so on.Before getting to know the actual cryptosystems, we will start with some basic number theory that will be helpful to understand the cryptographic algorithms.There are roughly two categories of cryptography. One is symmetric, and the other is asymmetric.

Symmetric cryptography is that people use the same key to communicate the message while asymmetric cryptography uses different keys for both sender and receiver. Each of them has its advantages and disadvantages. Symmetric cryptography requires both parties to find a way to a priori share some secure knowledge, which could be achieved by meeting physically, while asymmetric cryptography does not. However, asymmetric cryptography typically takes much longer to actually communicate messages than symmetric cryptography. We will introduce examples of both types of cryptosystems in the following sections, namely RSA(asymmetric cryptography) and Diffie-Hellman (symmetric cryptography). Last but not least, we will study the discrete logarithm to understand a possible attack on both RSA and Diffie-Hellman.

Number theory is a classical discipline in mathematics and has been studied already in ancient times. It is the study of relations among the integers. The study of elliptic curves by algebraists, algebraicgeometers and number theorists dates back to the middle of the nineteenth century. Cryptography is the art of secretly transmitting information and is as such as old as people trying to hide their secrets. In recent years cryptography has changed a lot-away from a science that was mostly related to military and secret service to a nominee present enabler of online banking, ecommerce, and secure email to mention just a few. The secret key cryptography and public key cryptography are the two main types of cryptography RSA is the most prominent algorithm used in public key cryptography techniques for encryption and digital signatures. Over the years, the key lengths for RSA have been increasing. This puts considerable burden on RSA. Another public key cryptography technique is gaining popularity in the last few years. It is called as Elliptic Curve Cryptography (ECC). The integers modulo a prime p form the simplest case of a finite field. Finite fields are an important building block of cryptography, in particular of public key cryptography. We consider general finite fields and study their use in elliptic curve cryptography.

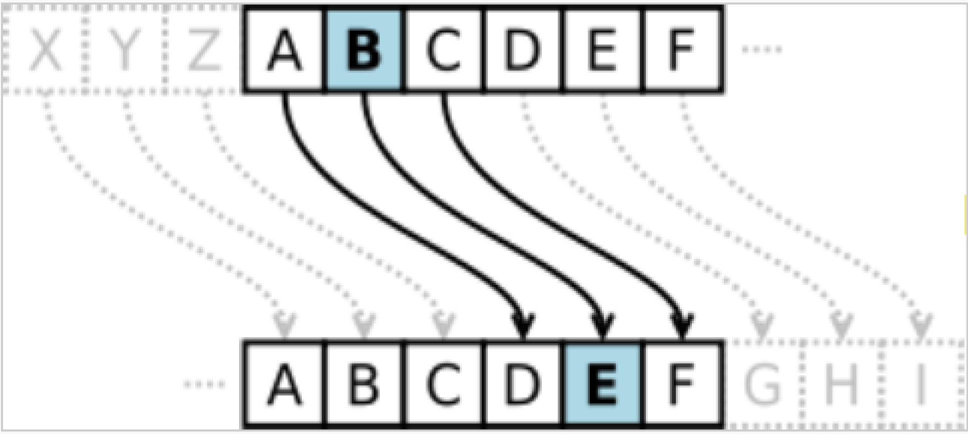
Methodology(How it works ?):

Let's discuss some methods of encryption and decryption of messages,

Caesar cipher:

In cryptography, a Caesar cipher, also known as a Caesar's cipher, the shift cipher, Caesar's Code or Caesar Shift, is one of the simplest and most widely-known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions further down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals.

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with all single alphabet substitution ciphers, the Caesar cipher is easily broken and in practice offers essentially no communication security.



The action of a Caesar cipher is to replace each plaintext letter with one a fixed number of places down the alphabet. This example is with a shift of three, so that a B in the plaintext becomes E in the ciphertext.

Example:

The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a right rotation of three places (the shift parameter, here 3, is used as the key):

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

To encipher a message, simply look up each letter of the message in the "plain" line and write down the corresponding letter in the "cipher" line. To decipher, do the reverse.

Plaintext: the quick brown fox jumps over the lazy dog
Ciphertext: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter x by a shift n can be described mathematically as,

$$E_n(x) = (x + n) \mod 26.$$

Decryption is performed similarly,

$$D_n(x) = (x - n) \mod 26.$$

The replacement remains the same throughout the message, so the cipher is classed as a type of monoalphabetic substitution, as opposed to polyalphabetic substitution.

Hill cipher:

Hill Cipher, in the pretext of classical cryptography, follows a polygraphic substitution cipher, which means there is uniform substitution across multiple levels of blocks. This polygraphic substitution cipher makes it possible for Hill Cipher to work seamlessly with digraphs (two-letter blocks), trigraphs (three-letter blocks), or any multiple-sized blocks for the purpose of building a uniform cipher.

Hill Cipher is based on linear algebra, the sophisticated use of matrices in general (matrix multiplication and matrix inverses), as well as rules for modulo arithmetic. Evidently, it is a more mathematical cipher compared to others.

The Hill Cipher is also a block cipher. A block cipher is an encryption method that implements a deterministic algorithm with a symmetric key to encrypt a block of text. It doesn't need to encrypt one bit at a time like in stream ciphers. Hill Cipher being a block cipher theoretically, means that it can work on arbitrary-sized blocks.

While Hill Cipher is digraphic in nature, it is capable of expanding to multiply any size of letters to add more complexity and reliability for better use. Since most of the problems and solutions for Hill Ciphers are mathematical in nature, it becomes easy to conceal letters with precision.

We will cover both Hill Cipher encryption and decryption procedures solving 2×2 matrices. However, it is possible to use Hill Cipher for higher matrices $(3 \times 3, 4 \times 4, 5 \times 5,$ or $6 \times 6)$ with a higher and advanced level of mathematics and complexity. Here, we will demonstrate simple examples that will provide more understanding of the Hill Cipher.

In Hill cipher, key K must be a square matrix and non-singular. and
$gcd(|K|, 26) = 1$ i.e co-prime.

Hill cipher Algorithm:

$$\text{Encryption: } C \equiv (K \cdot P)(\text{mod } 26)$$
$$\text{Decryption: } P \equiv (K^{-1} \cdot C)(\text{mod } 26)$$

.

Example:-

Encrypt and Decrypt the message `hello` with key $\begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$.

Solution:-

Here, Plaintext , $P = \begin{bmatrix} h & l & o \\ e & l & a \end{bmatrix} = \begin{bmatrix} 7 & 11 & 14 \\ 4 & 11 & 0 \end{bmatrix}$

and $K = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix} \implies |K| = (5 \times 2 - 3 \times 3) = 1 \neq 0.$

$$\text{so, } gcd(|K|, 26) = gcd(1, 26) = 1 \text{ i.e. co-prime}$$

.

Cipher text, $C \equiv (K \cdot P)(\text{mod } 26) = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 7 & 11 & 14 \\ 4 & 11 & 0 \end{bmatrix} (\text{mod } 26)$

$$= \begin{bmatrix} 47 & 88 & 70 \\ 29 & 55 & 42 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 21 & 10 & 18 \\ 3 & 3 & 16 \end{bmatrix}$$

$$= \begin{bmatrix} V & K & S \\ D & D & Q \end{bmatrix}$$

Cipher text is $= V\ D\ K\ D\ S\ Q$

Now, $K^{-1} = \frac{\text{adj. } K}{|K|} = \begin{bmatrix} 2 & -3 \\ -3 & 5 \end{bmatrix}^T = \begin{bmatrix} 2 & -3 \\ -3 & 5 \end{bmatrix}$

Plain text, $P \equiv (K^{-1} \cdot C)(\text{mod } 26) = \begin{bmatrix} 2 & -3 \\ -3 & 5 \end{bmatrix} \cdot \begin{bmatrix} 21 & 10 & 18 \\ 3 & 3 & 16 \end{bmatrix} (\text{mod } 26)$

$$\equiv \begin{bmatrix} 33 & 11 & -12 \\ -48 & -15 & 26 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 7 & 11 & 14 \\ 4 & 11 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} h & l & o \\ e & l & a \end{bmatrix}$$

So, our Plain text is $= h\ e\ l\ l\ o\ a\ \equiv$ `hello`.

There are a lot of other methods to encrypt and decrypt messages but here we discussed some famous and easy to understand methods.

Applications:

Secure communications:

The most obvious use of cryptography, and the one that all of us use frequently, is encrypting communications between us and another system. This is most commonly used for communicating between a client program and a server. Examples are a web browser and web server, or email client and email server. When the internet was developed it was a small academic and government community, and misuse was rare. Most systems communicated in the clear (without encryption), so anyone who intercepted network traffic could capture communications and passwords. Modern switched networks make interception harder, but some cases - for example, public wifi - still allow it. To make the internet more secure, most communication protocols have adopted encryption. Many older protocols have been dropped in favour of newer, encrypted replacements.

The best example is web encryption, since here you can choose between a clear or encrypted version of a website by switching between HTTP and HTTPS in the URL. Most large companies now use the encrypted form by default, and you'll see that any visit to Google, Facebook, Microsoft Office 365 or other sites will be to the HTTPS version of the site. This is accompanied in recent browsers by extra information, including a padlock to show that it is HTTPS. Something you can try is to click the padlock on an encrypted page, and your browser will tell you more about the page security. It will also tell you the especially relevant fact of the actual site name you're visiting. Therefore, if you're entering a password in a page, please do check that it is HTTPS.

End-to-end Encryption:

Email is one area where encryption is not widely in use. When email moves from server to server, and from server to you, it is encrypted. On the mail server and on your system, however, an administrator can read it. There are options to implement "end-to-end" encryption for email (I use PGP) but email systems are complex and these options are complex. Truly secure messaging systems - where only the sender and receiver can read the message - are those where encryption has been built in from the start.**Whatsapp** is good; Signal is better.

Digital Signatures/Authentication:

Authentication is any method by which such evidence is confirmed and checked. One will wish to check the origin of a document, the sender's identification, the time, dates and signatures of a document, the device or user's identity etc. A digital signature is an encryption tool that allows all of these to be verified. A document's digital signature is a detail dependent on the document and the private key of the signer. It is generally generated using a Hash function and a private signing feature (algorithms that create encypyted characters containing specific information about a document and its private keys).

Electronic Money:

The definition of electronic money (also called electronic cash or digital cash) is a term that is still evolving. It includes transactions carried out electronically with a net transfer of funds from one party to another, which may be either debit or credit and can be either anonymous or identified. There are both hardware and software implementations.

Anonymous applications do not reveal the identity of the customer and are based on blind signature schemes. Identified spending schemes reveal the identity of the customer and are based on more general forms of signature schemes. Anonymous schemes are the electronic analog of cash, while identified schemes are the electronic analog of a debit or credit card. There are also some hybrid approaches where payments can be anonymous with respect to the merchant but not the bank ;or anonymous to everyone, but traceable (a sequence of purchases can be related, but not linked directly to the spender's identity).

Encryption is used in electronic money schemes to protect conventional transaction data like account numbers and transaction amounts, digital signatures can replace handwritten signatures or a credit-card authorizations, and public-key encryption can provide confidentiality. There are several systems that cover this range of applications, from transactions mimicking conventional paper transactions with values of several dollars and up, to various micropayment schemes that batch extremely low cost transactions into amounts that will bear the overhead of encryption and clearing the bank.

Protection from Anonymous Remailers:

A remailer is a free service that strips off the header information from an electronic message and passes along only the content. It's important to note that the remailer may retain your identity, and rather than trusting the operator, many users may relay their message through several anonymous remailers before sending it to its intended recipient. That way only the first remailer has your identity, and from the end point, it's nearly impossible to retrace.

Here's a typical scenario - the sender intends to post a message to a news group via three remailers (remailer 1, remailer 2, remailer 3). He encrypts the message with the last remailer's (remailer 3's) public key. He sends the encrypted message to remailer 1, which strips away his identity, then forwards it to remailer 2, which forwards it to remailer 3. Remailer 3 decrypts the message and then posts it to the intended newsgroup.

References

- An Introduction to Number Theory with Cryptography:James S. Kraft , Lawrence C. Washington
- https://netleon.com/blog/real-world-application-of-cryptography
- https://blogs.ucl.ac.uk/infosec/2017/03/12/applications-of-cryptography/
- For Raw material, please visit: https://github.com/akhlak919