IRIS

Journal for Young Scientists

ISSN 2278 – 618X **(Print)**

ISSN 2278 – 6384 **(Online)**

© Patna Women's College, Patna, India

http://www.patnawomenscollege.in/journal

Use of Number Theory in Cryptography and Network Security

- **Priya Raj** • **Shreya Kumari** • **Swati Kumari**
- **Alka Kumari**

Received : July, 2022

Accepted : August, 2022

Corresponding Author : **Alka Kumari**

Abstract: *We are living in an information society. As information and communication technologies are developing, the threats related to leakage of confidential information, the theft of identities and the unauthorized modification of data is also increasing day by day. This shows a need for trustworthy information system which can be implemented by network security technologies, and an essential building blocks for such system is cryptography. The aim of cryptography is to send messages over any communication medium so that only the intended recipient of the message can read it. The privacy of data is a big concern for everybody. It is an emerging technology which is very important to give security to the network. This paper focuses on how various techniques of cryptography can enhance security of the network, so that any confidential messages can be exchanged by two parties without any worry of adversary.*

Keywords: *Encryption, Decryption, Public key cryptosystem, Network security, Number theory, RSA cryptosystem, One-time pad.*

Priya Raj
B.Sc. III year, Mathematics (Hons.), Session: 2019-2022,
Patna Women's College (Autonomous),
Patna University, Patna, Bihar, India

Shreya Kumari
B.Sc. III year, Mathematics (Hons.), Session: 2019-2022,
Patna Women's College (Autonomous),
Patna University, Patna, Bihar, India

Swati Kumari
B.Sc. III year, Mathematics (Hons.), Session: 2019-2022,
Patna Women's College (Autonomous),
Patna University, Patna, Bihar, India

Alka Kumari
Head, Department of Mathematics
Patna Women's College (Autonomous),
Bailey Road, Patna–800 001, Bihar, India
E-mail : alka.math@patnawomenscollege.in

Introduction:

Cryptography is science of mathematics for securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus, preventing modification of data by attacker/hacker. In early stages, messages were converted into unreadable group of figures. The word cryptography, derived from Greek word "*kryptos*" means "hidden" and the suffix "*graphein*" means "writing" (Burton, 2007).

The whole world revolves around mathematics. In cryptography, the techniques which are used to protect information are obtained from mathematical concepts, specially number theory and some rule for calculations that make it hard to decode is known as algorithms to convert message in the hidden form. The set up, $P \xrightarrow{f} C \xrightarrow{f^{-1}} P$ is called Cryptosystem, where P denotes Plaintext, C denotes cipher text, f is the enciphering function and f^{1} is deciphering function (Kishan, 2021). Cryptography provides many methods for network security purposes.

There are many applications of number theory, like in computer science, numerical analysis and one of the most important is cryptography. It is one of the oldest and most natural parts of mathematics (Silverman, 2009). Carl Friedrich Gauss quoted beautifully, "Mathematics is the queen of the sciences and number theory is the queen of mathematics" (Burton, 2007).

Secret Key Cryptosystem: Secret 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 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.

Public Key Cryptography: The public key cryptosystem was introduced 1970's by Diffie and Hellman. So as the name suggests, a public key would be used to encrypt the plain text and the private key would enable the cipher text to be decrypted. Public key can be known to everyone but the private key is only known to the recipient of the encrypted message.

Security: Different cryptosystem have different level of securities. The attack model specifies that what information the adversary or attacker have. The adversarial goal specifies the requirements to break the cryptosystem. The security level means to quantify the effort required to break the cryptosystem (Kahate, 2006).

In this paper, it was studied about what part of number theory that can be used in cryptography to make the network safe and secure for the transmission of messages and data. First it was reviewed how data was transmitted in ancient period by the concept of classical cryptography, and for today's era, why the classical methods are not strong enough to protect our data. Also, how to get the best use of number theory for network security purposes.

Materials and Methods:

Number theory is a vast field of mathematics that plays an important role in encryption algorithm. Cryptography is the method of hiding information and converting secret information to not relatable texts. There are many concepts of number theory like primes, congruencies, Euler's phi function, modular arithmetic and many more which are used in cryptography.

Prime number: A central concern of number theory is the study of prime numbers.

An integer p >1 is a prime number, if and only if its only divisors are 1 or p.

RSA cryptosystem totally depend on the fact that prime factorization of large numbers takes a long time (Washington, 2018).

Public key consisting of a product of two large primes used to encrypt message and a secret key consisting of those two primes numbers used to decrypt the message.

Fundamental theorem of arithmetic: Every positive integer n>1 can be expressed as the product of prime factors uniquely.

Affine function: Function of the form e(x) ≡ (ax+b) mod26 where a,b $\in$ Z_{26} is called affine function and it is injective. This function is used in the Affine cipher.

Arithmetic modulo m ($\mathbb{Z}_m$) $\mathbb{Z}_m$ is the set {0,1,……..,m-1}, equipped with two operations, +(addition) and · (multiplication). This set is used to denote the set of private and primary keys.

Euler's Phi Function: The Euler's phi function, written as φ (η) for positive integers n, is the number of non-negative integers less than n which are relatively prime to n (Kishan,2021).

Euclidean Algorithm: The Euclidean algorithm is basically a continual repetition of the division. The number is to repeatedly divide the divisor by the remainder until the remainder is 0. The gcd is the last non-zero remainder in the algorithm.

The Extended Euclidean Algorithm: Extended Euclidean algorithms are widely used in cryptography. It is very helpful to compute modular inverses.

Fermat's Little Theorem: Fermat's little theorem helps to compute powers of integers modulo prime numbers.

Modular Arithmetic: It is an arithmetic that reduces all numbers to one of a fixed set [0,1,……..,n-1] for some number n. Any integer outside this range is reduced to one of this range by taking the remainder after division by n.

We can create groups, rings and fields which are the basics of most of the modern public key cryptosystems by using Modular arithmetic.

Congruence: Two integers a and b are said to be congruent modulo n, if difference of the two numbers (i.e., a-b) is divisible by n.

It is denoted as: a≡ b (mod n).

Chinese Remainder Theorem: In cryptography, Chinese remainder theorem speeds up the calculation process.

Primitive root: If an integer 'a' has order φ (n) modulo *n* where *n* is a positive integer and (a,n) = 1, then 'a' is called primitive root of *n*

It is used in the Diffie-Hellman key exchange.

Now, it will be described what steps and method of cryptography should be followed for a network to be secure with the help of number theory.

I. The concepts of number theory was studied to use it in the algorithm of cryptography and tried to find suitable examples for every topic to discuss in our project.

II. This paper is based on the theoretical research of cryptography for network security. Now, It has been seen that in ancient times, how the classical cryptography helps to make the network secure and how with the change of generation cryptosystem has become more important and reliable for encrypting the data.

The concepts of various types of classical cryptography was studied one by one. RSA cryptosystem and One time pad cipher has been used with examples.

Classical Cryptography

The main goal of the cryptography is to enable two parties say, Amy and Andy to communicate through a not so secure medium(as, telephone line or internet), such that the eavesdropper Sam couldn't understand transmitted message (Stallings, 2011).

1. In **Shift Cipher,** the domain is Z_{26}, since there are 26 letters in the English alphabet.

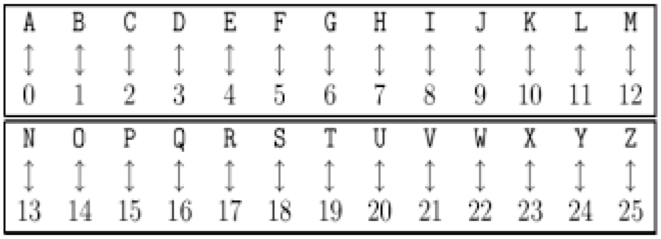
The encryption and decryption key for this cryptosystem are:

$e_k(x) \equiv (x+K) \bmod 26$, $d_k(y) \equiv (y-K) \bmod 26$,

where $x, y \in Z_{26}$, $0 < K < 26$

For particular K=3, the shift cipher referred to as *Caesar cipher.*

We consider the given conversion table for the English alphabet.



A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

for eg.:

(i) Using the above table, letters of message "cookie" can be represented as their corresponding numbers: 2 14 14 10 8 4.

(ii) Now we add 3 (the encryption key) to each number, we get: 5 17 17 13 11 7

(iii) Now we use the table to replace these numbers with their corresponding letters, we get: FRRNLH.

So, the cipher text corresponding to the plaintext "cookie" is "FRRNLH".

2. In **Substitution Cipher,** key will be permutation of the 26 alphabetic characters.

Encryption key of a letter by a shift n can be described mathematically as:

$$e_n(x) \equiv (x+n) \bmod 26$$

and, decryption key as:

$$d_n(X) = (X-n) \bmod 26$$

for eg.: plain text: i am studying data

encryption key: 4

Cipher text: MEQWXYHCMRKHEXE

3. **Affine cipher,** shift ciphers is one of the type of affine cipher.

for eg.:

Encrypt the message "*danger*" using an affine cipher with key K (5,2).

Encryption function for the given key is,

$$e_k(x) \equiv 5x + 2 \pmod{26}$$

& decryption function will be,

$$d_k(y) \equiv 5^{-1}(y-2) \pmod{26}$$
$$\equiv 21\,(y-2) \pmod{26}$$

(i) 1st convert the letters of message "danger", using shift cipher table with their corresponding numbers, we get : 3 0 13 6 4 17

(ii) Now, we encrypt these numbers using $e_k(x) = 5x + 2 \pmod{26}$, we get : 17 2 15 6 22 9

(iii) After replacing these numbers by corresponding letters using the table, we get: RCPGWJ, which is the required cipher text.

The classical cryptography methods does not provide that much of security to the network. So, public-key cryptosystem is more often used for network security purposes.

RSA Cryptosystem:

The RSA cryptosystem is an example of a "public-key" cryptosystem. In 1977, Rivest, Shamir, and Adleman invented the RSA Cryptosystem (Stallings, 2011). In RSA Cryptosystem, the security is based on the difficulty of factoring large integers.

for eg.: Let Shreya wants to send a message to Swati in an encrypted form. She then represent her message as 'm' and splitted m into 2 block of message m_1& $m_2$each of which is less than the RSA modulus N(=pq). Now, she take two distinct prime numbers say, p =19 and q = 23 and so, N =19.23 = 437, φ (N) = (p -1) (q -1) =18.22 =396. Then Sheya will produce the cipher text using the encryption key: $c = m^e$ (mod N). And Swati on receiving 'c' can decrypt the cipher text to get message 'm' by decryption key : $m = c^d$(mod N).

Let Shreya has public key e =29, as gcd(29,396) = 1. Then using the extended Euclidean algorithm, she obtain d= 41 since, 29.41 = 1188 = 1(mod396). Let the message that Shreya wants to send is 'NO' given by, digital equivalence m=1415, she splits m into 2 block of digits m_1 & m_2. Then to encrypt m, m_1 will be encrypted as c_1 $=14^{29}$(mod 437)=203(mod 437) & m_2 will be encrypted as, $c_2 = 15^{29}$(mod 437)=402(mod 437). So , the cipher text for m = 1415 will be c = 203402. Now, to decrypt the cipher text c, Swati will compute $m_1 = (203)^{41}$(mod 437) and $m_2 = (402)^{41}$(mod 437).

One-time pad: An improvement to the Vernam cipher was given by Mauborgne which provides very strong security to the network. One-time pad cipher is unbreakable. In one-time pad cipher, the key is chosen randomly of the same length of the message without repetition of the key. One key can be used only once for the encryption or decryption. Assume that the attacker has find two keys to decrypt, then two plaintexts are produced corresponding to the single cipher text. But actually the key was chosen randomly, so the attacker can't say that which plaintext is correct and which one is not.

Thus, one-time pad cryptosystem shows *perfect secrecy* (Stinson and Paterson, 2019).

Results and Discussions:

As a result, we discussed various techniques of cryptography that can be implemented to a network to make it secure. For current time, the classical cryptosystem are not preferred as the hackers are also very much aware of correct decryption of these techniques. And these classical cryptography techniques are easily breakable by the attacker/hacker.

So, for the current scenario, Public- key cryptosystem (such as, RSA cryptosystem) or One-time pad, are much preferred.

There are so many other cryptosystem which provides a strong network security (such as, AES, Triple DES, Two fish). Zoom meeting app uses AES cryptosystem.

Earlier, we saw the step-by-step procedure of key generation in different algorithms.

Some constraints must be followed while creating keys to ensure the security, which are :

For RSA cryptosystem, the two prime numbers which are chosen of which the RSA modulus is their product must be a large prime because this system is completely based on fact that factorization of large prime is not so easy.

For One-time pad, the key chosen must be as long as the message length and it should be unrepeated.

Conclusion:

From this research paper, it is concluded that number theory plays vital role in cryptography and cryptography is much needed for communication to take place through a secure network. The cryptanalysis of different type of cryptography was also described. In ancient times also, the classical methods were used to keep secrets and or military purposes.

Encrypt message with strongly secure key which is known only by sender and recipient end is main thing for security in cloud. Problems like forgery of data, unauthorized modification in data and many other related problem can be overcome on implementing cryptography techniques to the network. Cryptography is used in many apps such as, WhatsApp, Telegram, PhonePe, Paytm, etc., which we commonly use in our daily life. These apps are also end-to-end encrypted, which means no third party can eavesdrop on our activities. The new feature of WhatsApp is another example of cryptography that gives advancement to the network security, which gives the facility to the sender to restrict the recipient to view the message only once, so that the forwarding of confidential messages and secrets cannot take place.

With more mathematical tools and cryptography methods we can make the communication network system more and more secure.

References:

Burton David M. (2007). Elementary Number Theory, 6th Ed., Tata McGraw-Hill, New Delhi, pp. 13-17; 197-207.

Kahate Atul (2006). Cryptography and Network Security, 8th Ed., Tata McGraw-Hill, New Delhi, pp. 190-199.

Kishan Hari (2021). Number theory, 14th Ed., Krishna Prakashan, Meerut, pp. 142-145.

Silverman Joseph H. (2009). A friendly introduction to Number Theory, 3rd Ed., Pearson, Noida, Uttar Pradesh, pp. 127-128; 228-231.

Stallings William (2011). Cryptography and Network Security principles and practice, 5th Ed., Pearson, Noida, pp.140, 239, 340, 298.

Stinson Douglas R. and Paterson Maura B. (2019). Cryptography theory and practice, 4th Ed., CRC press, USA, pp. 238-246.

Washington Lawrence C. (2018). An introduction to Number theory with Cryptography, 2nd Ed., CRC press, USA, pp. 400-410.