Scholars Journal of Physics, Mathematics and Statistics
OPEN ACCESS
Abbreviated Key Title: Sch J Phys Math Stat
ISSN 2393-8056 (Print) | ISSN 2393-8064 (Online)
Journal homepage: http://saspjournals.com/sjpms

Comparative Study of Classical Ciphers with the Use of Congruence modulo Relation

Nikzad Jamali*

Institute of Science, Department of Mathematics, Chandigarh University Punjab, India

***Corresponding author:** Nikzad Jamali | **Received:** 15.03.2019 | **Accepted:** 28.03.2019 | **Published:** 30.03.2019
DOI: 10.21276/sjpms.2019.6.3.5

Abstract

Original Research Article

This paper is a brief introduction of Congruence Modulo Relation, its property and application in Encryption and Decryption. As we know Congruence modulo relation is a part of Number Theory, so this paper is a study of relation between number theory and network security. Also, in this paper will discuss about weakness, maintenance and comparison methods of Cryptography, which used congruence modulo relation.

Keywords: Congruence, Cryptography, Encryption, Decryption.

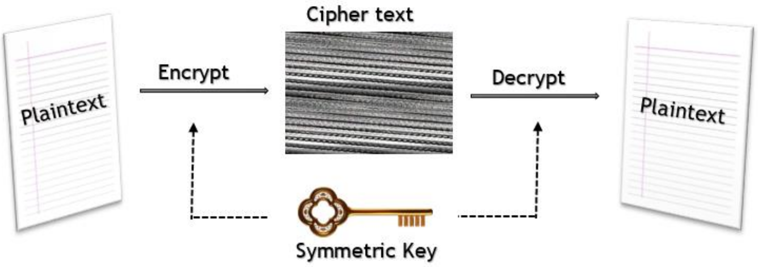
Introduction

As we know, cryptography is science of encryption and decryption of message, so with equivalent relation between letters and numbers we obtain a linearly process between encryption and decryption.

Let A wants to send a message (M) to B, he encrypts the message by using shift transformation and symmetric key (K), such that K is only known to sender A and the receiver B. mathematically this process shows like:

$$\text{A: M} \xrightarrow{K} \text{C} \longrightarrow \text{B}$$

When B has been obtained the cipher text, he can decrypt it by using symmetric key. Graphically this process shows like below:



To understand this paper firstly, we must know some basic concepts:

Definition 1.1: The method of changing cipher text back into plaintext using a key is called decryption.

Definition 1.2: The course of action of switching plaintext into cipher text with the help of a cipher plus a key is called encryption.

Definition 1.3: key is some personal information used by the cryptograph, known only to the sender & receiver.

Definition 1.4: The original intelligible message is called plaintext.

Definition 1.5: The transformed message is called Cipher text.

Many researchers have been working in the field of cryptography to modify security of Hill cipher and Ceaser cipher. Toorani *et al*. [5], has introduced symmetric cryptosystem which is a secure variant of Affine Hill cipher by using ciphering core. Each block of produced data is enciphered by considering unique random number, using chained hash function. Rushdi *et al*. [9] dropped the need of secure channel and overcome the problem of key distribution in symmetric encryption. They further observed that there will be no constraint on failure of key selection matrix and make it tough for the attacker to crack the key. Here the no of unknown are more than the available equations which leads to no mathematical solution. Benni Purnama *et al*. [1] has produced improved Ceaser cipher cryptography method in which they concluded that, this method has the key which lies on the line rotate root that could be used by user as it is required. The method is easily solvedby using monoalphabetic substitution, where user cipher text outcome making it undoubtful of certain parties.

Congruence modulo Relation

Carl Friedrich Gauss in (1777-1855) introduced the Congruence's theory, where he had defined the above conversion by using modulo relation as below: [4].

Definition2.1: Let l be a positive integer. Two integers **x**and **y**are said to be congruent modulo l,signifiedwith: $x \equiv y(\bmod l)$ If l divides(x-y); that is, provided that $x - y = kl$ for some k integer. [2].

Theorem 2.1: Let x, y,c, d, denote integers. Then:[4]

1. $x \equiv y(\bmod l)$, $y \equiv x(\bmod l)$ *and* $x - y \equiv 0(\bmod l)$ *are equivalent statements.*
2. $x \equiv y(\bmod l)$ *and* $y \equiv c(\bmod l)$, *then* $x \equiv y(\bmod l)$.
3. $x \equiv y(\bmod l)$ *and* $c \equiv d(\bmod l)$ *then* $x + c \equiv y + c(\bmod l)$.
4. $x \equiv y(\bmod l)$ *and* $c \equiv d(\bmod l)$ *then* $xc \equiv yd(\bmod l)$.
5. $x \equiv y(\bmod l)$ *and* d/l, $d > 0$, *then* $x \equiv y(\bmod d)$.
6. $x \equiv y(\bmod l)$ *then* $xc \equiv yc(\bmod l)$ *for* $c > 0$.

Theorem 2.2: In modular arithmetic, if a and b are any integers and m is a positive integer, then the congruence $ax \equiv b(\bmod m)$ has a solution for x iffthe g.c.d. of a and m is a factor of b. [7]

Solution of Linear Congruences

Linear congruences in the form $ax \equiv b(\bmod m)$ can be expressed to a linear equation in the form $x \equiv b + mq$ Where b is a residue, m is the modulus and q is any integer. The basic idea of the method is to express the given linear congruence to equation and solve it algebraically. The algorithm for solving linear congruences is presented below [7].

Step 1. Check the solvability of the given linear congruence.

Step2. Convert the given linear congruence into linear equation in terms of the unknown variable.

Step 3. Find the smallest positive integer solutions to the linear equation that will make the unknown variable a whole number.

Step 4. Evaluate the linear equation using the integer solution. The result will be the smallest positive integer that is a solution to the given linear congruence.

The general solution is given by the congruence $x \equiv b(\bmod m)$ where b is the smallest positive integer solution and m is the given modulus.

For example, solve $10x \equiv 22(\bmod 28)$.

Step 1. Check the solvability of the given linear congruence.

Since the greatest common divisor of 10 and 28 is 2 which is a factor of 22, the linear congruence has solutions.

Step 2. Convert the given linear congruence into linear equation in terms of the unknown variable.

$$10x \equiv 22(\bmod 28) \Rightarrow 10x = 22 + 28q \Rightarrow x = \frac{22+28q}{10} \Rightarrow x = \frac{11+14q}{5}$$

Step 3. Find the smallest positive integer solutions to the linear equation that will make the unknown variable a whole number.

Given $x = \frac{11+14q}{5}$, the smallest positive integer value of q that will make x a whole number is 1.

Step 4. Evaluate the linear equation using the integer solution. The result will be the smallest positive integer that is a solution to the given linear congruence. The general solution is given by the congruence $x \equiv b(\bmod m)$ where b is the smallest positive integer solution and m is the given modulus.

If q = 1, then evaluating $x = \frac{11+14q}{5}$ will be:

$$x = \frac{11+14(1)}{5}$$

$$x = \frac{11+14}{5} = 5$$

Thus, the solution to linear congruence $10x \equiv 22(\bmod 28)$ is $5(\bmod 28)$.

Substitution Techniques of Encryption and Decryption

A substitution technique is one where the letters of plaintext are replaced by other alphabets or by digits or by symbols [8]. We are now set to define Ciphers by transforming each letter of the plaintext into a different letter to produce cipher text. Such cipher is called character substitution cipher, since each letter is shifted individually to another letter by a substitution [3]. The following table shows numerical equivalents of an ordered English capital letters.

Table-1: positive integer's equivalents of English capital Letter

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

Ceaser Cipher

To communicate with his officers Julius Caesar used an additive ciphers ,which is the reason that additive ciphers sometimes are referred as Caesar Ciphers .For his communication Caesar used a shift key in 3. In the field of Cryptography Caesar Cipher is well known for Encryption- Decryption Algorithm [1].

The replacement of every single character of the text message is being changed by a character which is down by 3 positions to the existing position of the alphabet [8].

The relation of this cipher is:

$$\mathrm{C}_k = \mathrm{E}_n\ (3, \mathrm{p}_k) = (\mathrm{p}_k + 3) \bmod 26$$

$$\mathrm{P}_k = \mathrm{D}_n\ (3, \mathrm{C}_k) = (\mathrm{C}_k - 3) \bmod 26$$

A widely used version of this cipher would be expressed by [6]:

$$\mathrm{C}_k = \mathrm{E}_n\ (\mathrm{X}, \mathrm{p}) = (\mathrm{p}_k + \mathrm{X}) \bmod 26$$

$$\mathrm{P}_k = \mathrm{D}_n\ (\mathrm{X}, \mathrm{C}) = (\mathrm{C}_k - \mathrm{X})\bmod 26$$

In above formulas, 'X' is the secret key, 'P_k' plaintext 'C_k' shows the cipher text, and E_n ,D_n symbols of encryption and decryption respectively.

For example, let plaintext is "ACT" for changing this plaintext to cipher text, assume shift key is

$K = 5$.

Now, change every letter of "ACT "to equivalent integers, so $A = 0$, $C = 2$, $T = 19$.

For changing $"A"$ of plaintext to cipher text:

$$C_1 = (P_1 + K) \bmod 26 = (0+5) \bmod 26 = 5 \bmod 26 = 5 = F$$

For changing $"C"$ of plaintext to cipher text:

$$C_2 = (P_2 + K) \bmod 26 = (2+5) \bmod 26 = 7 \bmod 26 = 7 = H$$

For changing $"T"$ of plaintext to cipher text:

$$C_3 = (P_3 + K) \bmod 26 = (19+5) \bmod 26 = 24 \bmod 26 = 24 = Y$$

Hill cipher

Hill requires inverse of the key matrix while decryption. Actually,not every matrix have the existence inverse and thus they will not become key matrices in Hill Cipher scheme [9].The encryption key which used:

$$\text{H}=\begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \\ h_{31} & h_{32} & h_{33} \end{bmatrix}$$

Here the transformation of three letters from plaintext at a time can be done,these letters being represented as p1, p2, and p3, into three cipher text letters c1, c2, and c3 in their mathematical representation by [6].

$$\text{C}_1 = (h_{11}P_1 + h_{12}P_2 + h_{13}P_3) \bmod 26$$
$$\text{C}_2 = (h_{21}P_1 + h_{22}P_2 + h_{23}P_3) \bmod 26$$
$$\text{C}_3 = (h_{31}P_1 + h_{32}P_2 + h_{33}P_3) \bmod 26$$

The above system equations can be expressed in the following vector-matrix notation:

$$C = [H]P \bmod 26 \qquad \textit{Encryption formula}$$
$$P = [H^{-1}]C \bmod 26 \qquad \textit{Decryption formula}$$

For example, let plaintext is (ACT), first we change this word to equivalent integer: $\begin{bmatrix} A \\ C \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$

so, by using $\text{K}=\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$ we have:

$$C = [K]P \bmod 26$$

$$C = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} = \begin{bmatrix} P \\ O \\ H \end{bmatrix} = POH$$

Now for changing cipher text to plaintext we must find K^{-1}. By using basic math, we will obtain:

$\text{K}^{-1}=\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$. Using this matrix,the plaintext is:

$$P = [K^{-1}]C \bmod 26$$

$$P = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \bmod 26 = \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ C \\ T \end{bmatrix} = ACT$$

Conclusion

After detail studies of both the methods, i.e. Hill cipher and Caesar cipher it can be concluded that although the procedure of Caesar cipher is not quite laborious, and one can decrypt the text by entering the shift key from 1 to 25 reasoned poor security of cipher text, this means cipher text could be easily decrypted by giving trial of differ entered shift key. On contrary to Caesar cipher, in Hill Cipher the encryption key, which is a matrix, is very complex to decrypt as one must find the inverse of the matrix, so it is more secure and reliable procedure to encrypt a message. But the scheming of the method is relatively lengthy and time consuming.

Acknowledgement

I would like to express my gratitude to my supervisor; Dr. Jatinder Kaur Who helped, supported and gave me the golden opportunity to do this paper.

References

1. Benni Purnama and Hetty Rohayani AH. A New Modified Ceaser Cipher Cryptography Method with Legible Ciphertext from a Message to be encrypted, International conference on computer science and computational Intelligence.2015; 59: 195-204.
2. David M. Burton, Elementary Number Theory, McGraw Hill, Education (India) Private Limited, Seventh Edition. 2007.
3. Isa Sani and Abdulaziz, Cryptography using congruence modulo relation, American Journal of Engineering Research. 2017; 6(3): 56-160.
4. Ivan Niven and. An introduction to The Theory of Numbers, Wiley India (p.) Ltd, Fifth Edition. 1991.
5. Mohesen Toorani and abolfazlFalahati, a secure variant of the Hill Cipher, proceeding of the 14th IEEE Symposium on Computers and Communications (ISCC'09). 313-316.
6. Kumar M, Mishra R, Pandey RK, Singh P. Comparing Classical Encryption With Modern Techniques. Proceedings of S-JPSET. 2010;1(1).
7. Cuarto PM. Algebraic Algorithm for Solving Linear Congruences: Its Application to Cryptography. Asia Pacific Journal of Education, Arts and Sciences. 2014;1(1):1.
8. Ramandeep Sharman. Classical Encryption Techniques, International Journal of computers and technology.2012; 3(1):84-90.
9. Rushdi A. Harmamreh, Mousa Farajallah. Design of a robust cryptosystem Algorithm foe Non-Invertible Matrices Based on Hill Cipher, IJCSNS International Journal of computer-Science and network security. 2009; 9(5): 11-15.
10. Vijayaraghavan N. A study on the Analysis of Hill's Cipher in Cryptography, International journal of Mathematics trends and technology.2018; 54(7): 519-522.