American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-3, pp-156-160
www.ajer.org
Research Paper Open Access

Cryptography Using Congruence Modulo Relations

Isa Sani[1] and Abdulaziz B.M. Hamed[2]
[1]*Department of Mathematics and Statistics, Yobe State University Damaturu, Nigeria)*
[2]*Department of Mathematics and physics, Faculty of Education West Kordofan University, Sudan)*

ABSTRACT: *This study deals with the problem of coding and decoding messages. The messages has been encrypted using the secret keys(k) and(m,n) . Linear transformation and arithmetic congruent (modulo 26 and 28) relations corresponding to English alphabetic letter using cipher transformation. The numeric negative integer equivalents of English capital Letters have been generated. It was found that cipher transformation depend on the secret keys and the knowledge of congruence relations.*
Keyword: *Encrypt Decrypt, Congruence, Linear, Transformation.*

I. INTRODUCTION

Today crime is increasingly on daily basis and takes different forms. The significance of information in checking this cannot be overemphasized. Not all but some information need to be secure from other partners, especially the information or data obtained from internet. We have to know that all information send by email, third partners are allowed to have access to the messages that we send (router).

Cryptography has for long been an important issue in computer science. It was mainly used for the security needed for passwords, but now cryptography is very important due to the Internet's flow of sensitive information such as credit cardinformation and other sensitive information which is fairly easy to monitor by unintended third party. The main concern of this study is messages between two persons and many of the partners between them they want to communicate with. If X wanted to send a secure message to Y can be achieved by sending an encrypt message. Then, a key(k) to encrypt and decrypt the message must be known to only to X and Y.

Definition 1.1: (Menzes *et al*, 1997) defines Cryptography as the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entry authentication, and data origin authentication.

From this definition the following can be deduce;

i. Confidentiality is a service used to keep the content of information from all but those authorized to have it. There are many approaches to providing privacy, ranging from physical protection to mathematical algorithms which make data unintelligible.
ii. Data integrity is a service which addresses the unauthorized change of data. To guarantee data integrity, one must have the ability to identify data manipulation by unauthorized parties.
iii. Authentication is a service related to identification.
iv. Non-Repudiation is a service which prevent an entry from denying previous commitment or actions

To achieve the above deductions a simple method of enciphering and deciphering a message using linear transformations and congruence modular arithmetic, using the English alphabet corresponding to the number (modulo 26) and show how algebraic operations can sometimes be used to coding and decoding a messages. Cryptography is the study of encoding and decoding secret messages. In the language of cryptography, codes are called the ciphers and coded messages are called ciphertext otherwise known as plaintext.

II. INTEGER CONGRUENCE

The notion of congruent integers with respect to a modulus, and applications of modular arithmetic to divisibility tests and blocking ciphers in cryptography is important in this study.

Definition 2.1: (Raji, 2016). The greatest common divisor of two integers a and b is the greatest integer that divides both a and b , we denote by gcd (a,b).

Definition 2.2: (Shoup, 2008). Let m be a positive integer for $a, b, k \in \mathbb{Z}$, then, we say that a and b are congruent modulo m if $m|(a-b)$, $(a = b + km)$.
This is written as $a \equiv b(mod\ m)$. If $m \nmid (a-b)$ then, we write $a \not\equiv b(mod\ m)$.

Equivalently, $a \equiv b(mod\ m)$, if and only if $a = b + my$ for some $\in \mathbb{Z}$. The relation $a \equiv b(modm)$ is called congruence relation or simply congruence, where the number m is called the modulus of congruence.

Theorem 2.3: (Raji, 2016). Let a, b, c and d be integers and let m be a positive integer then the following holds; If,

a. $a \equiv b(modm)$ then $b \equiv a(modm)$
b. $a \equiv b(modm)$ and $b \equiv c(modm)$ then $a \equiv c(modm)$
c. $a \equiv b(modm)$ then $a + c \equiv b + c(modm)$
d. $a \equiv b(modm)$ then $a - c \equiv b - c(modm)$
e. $a \equiv b(modm)$ then $ac \equiv bc(modm)$.
f. $a \equiv b(modm)$ then $ac \equiv bc(modmc)$, for $c > 0$
g. $a \equiv b(modm)$ and $c \equiv d(modm)$, then $a + c \equiv b + d(modm)$
h. $a \equiv b(modm)$ and $c \equiv d(modm)$, then $a - c \equiv b - d(modm)$
i. $a \equiv b(modm)$ and $c \equiv d(modm)$, then $ac \equiv bd(modm)$

Definition 2.4: An equation of the form $ax \equiv b(mod\ m)$, where a, b, and m are integers and x is a variable is call a linear congruence

Definition 2.5: Inverse of an integer a to modulo m is a^{-1} such that $a * a^{-1} \equiv 1(mod\ m)$, where $a^{-1}$is called inverse of a.

Definition 2.6: (Gries and Schenider, 2002). A function f from a set X to a set Y is called a one way function if f(x) is easy to compute for all x $\in$ X but for essentially all element y Im(f).

We are now set to define Cryptosystems (Ciphers) by transforming each letter of the plaintext into a different letter to produce ciphertex . Such cipher are called character substitution or monographic ciphers, since each letter is shifted individually to another letter by a substitution.

The following two tables show numerical (positive / negative integer) equivalents of an ordered English capital Letters.

Table I: Positive integer's equivalents of English capital Letter

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

Table II: Negative integer's equivalents of English capital Letters

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

III. LINEAR FUNCTIONS

Suppose a sender X wants to send a message M to a receiver Y, he encrypts the message by using shift transformation and key k, such that k is only known to sender X and the receiver Y. This is explained in the following mathematical relations:

$$X: \mathcal{M} \xrightarrow{k} C \rightarrow Y \quad (1)$$

Where C is an encrypted message

$$Y: C = E_k(M), \quad (2)$$

Where $M \in \mathcal{M}$ and $C \in \mathsf{C}$, which is the cipher text obtained from (1). Now the message C can transmit over the public insecure channel. The key also should transmit to the receiver Y in a secure way to decrypt the message. Since the legitimated receiver Y knows the key k, he can decrypt C, using the following transformation function

$$X^{-1}: C \xrightarrow{k} \mathcal{M} \quad (3)$$

Also,

$D_k(C) = D_k(E_k(M)) = M$, Where $M \in \mathcal{M}$ and $C \in \mathsf{C}$

The idea of coding and decoding the message M, using k is as follows;

$$f_k = E_k(m) \equiv m + k(mod26)\ ,\ 0 \leq m, k \leq 25 \quad (4)$$

$$f^{-1}{}_k = D_k(c) \equiv c - k(mod26)\ ,\ 0 \leq c, k \leq 25 \quad (5)$$

Example 3.1: Encrypt the following message, E_4(YOBESTATEUNIVERSITY)

Solution: $k = 4$

Table III: Positive integer's corresponding English capital letters Modulo 26.

$\mathcal{M}$	A	B	C	D	E	F	G	H	I	J	K	L	M
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
Shift	4	5	6	7	8	9	10	11	12	13	14	15	16
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
C	E	F	G	H	I	J	K	L	M	N	O	P	Q

□	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Shift	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	17	18	19	20	21	22	23	24	25	0	1	2	3
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
C	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Therefore, the Encrypted message using k is obtained as follows,

E_4(YOBESTATEUNIVERSITY) = CSFIWXEXIYRMZIVWMXC

This is the encrypted received message, to be decrypted by receiver using k.

Normal message consists of words; space and comma. Encryption/Decryption of this type of messages is achieved as we proposed here by the congruence modulo 28 instead of 26.

Table III: Space, Comma and Positive integer's corresponding English capital letters Modulo 28

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**Space**	**comma**
15	16	17	18	19	20	21	22	23	24	25	26	27	0

Table IV: Space, Comma and Negative integer's corresponding English capital letters Modulo 28

A	B	C	D	E	F	G	H	I	J	K	L	M	N
-27	-26	-25	-24	-23	-22	-21	-20	-19	-18	-17	-16	-15	-14
O	P	Q	R	S	T	U	V	W	X	Y	Z	Space	comma
-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0

IV. Conclusion

In this work we have applied the linear transformation and congruence modulo 26 and modulo 28 to code and decode the messages using one or two private keys.

REFERENCE

[1] Menzes A.,Van Oorschot P. and Vanstone, S. 1997, Hand Book of Applied Cryptography, CRC press.
[2] Victor Shoup, 2008, A computational Introduction to Number Theory and Algebra, Cambridge University press.
[3] Bruce Schneier, 1996, Applied Cryptography, Second Edition. John Wiley and Sons.
[4] David Gries and Fred B. Schenider, 2002, Applied Number Theory in Computing and Cryptography. Springer.
[5] Wissam Raji, 2016, an Introductory Course in Elementary Number Theory. Saylor Foundation.