A new approach for Encryption using radix modular

Associate prof. Dr. Saad AbdualAzize abdual Rahman
saad.a.azize@almamonuc.edu.iq
Associate prof. Imad Matti Bakko
Imad.m.abona@almamonuc.edu.iq
Associate prof. Dr. Sanaa Ahmed Kadhim
Sana.a.kadhim@almamonuc.edu.iq
AL_Ma'moon University College, Computer science dept.

Abstract

Secure communication over open networks is a basic stone of commercial transactions and government services. The continuity of these fields and many others are only conceivable if security is ensured. This paper produces a cryptography system that uses Arithmetic Modules law and logical operations. Using three different modular arithmetic modules increases the security of converting the decimal number to six residue numbers and three modular. Operations like add and Xor are used to generate a key. Each character in a plain text will be converted using modular then encrypted to obtain a cipher text which will be decrypted using L.H Gerner's law.

Keywords: Cryptography; Transmission; Mathematical equations, additive, radix modular.

1-Introduction.

Hundreds of people and computers around the world may be linked together in a virtual world called cyberspace. One of the maximum essential components of an advancements in the subject of pc era is the insurance of data and application

safety. Regrettably, technological advances are continually accompanied with the aid of a downside to the technology itself. One is the susceptibility of data safety, giving upward thrust to the demanding situations and needs. Security is to shield information transmitted through a communication community [1].

There are several ways to obtain data security through one channel which is cryptography. In cryptography, data transmitted via the network will be disguised in a way that even if the data can be read then it cannot be understood by unauthorized parties. Data to be transmitted and not experienced is an encoding known as plaintext. Camouflaged the way of encoding will convert plaintext into a cipher text. The functions that are fundamental in cryptography is encryption [2]. Many cryptographic techniques are implemented to safeguard information, but the present condition is much too way or the work done by cryptanalysis to break it.

Though an important thing in the delivery of a message, is to maintain the security of the information that are not easily known or manipulated by other parties. One solution that can be done is to modify the cryptography solved or create a new

cryptography so that it can be an alternative for securing messages [3]

2. Additive Techniques

Additive technique is one of the earliest and simplest methods of encryption. It is simply a type of substitution cipher.[4].

The action of an Additive cipher is to replace each plaintext letter with a different one a fixed number of places down the alphabet. The cipher illustrated here uses a left shift [5][6]

Ciphering:

$$Ci = E_k (pi) = pi + keyi \bmod 26 \quad \ldots\ldots (1)$$

Where:

i=1 ……..n

n = number of characters in a plain text

p = original message

E = encryption process

C = coded message (cipher text)

K= key

Deciphering:

$$Pi = Dk (Ci) = Ci - keyi \bmod 26 \quad \ldots\ldots (2)$$

Where:

D = the decryption process

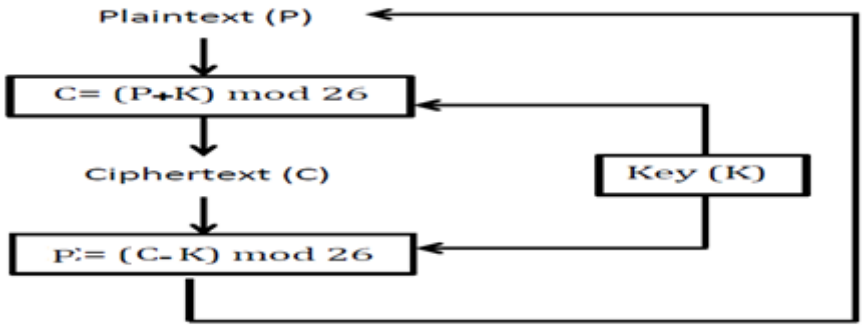

Figure 1: encryption and decryption process

3. Modular

A singular number gadget known as the residue quantity device is advanced from the linear congruence viewpoint. The residue wide variety machine is of particular hobby due to the fact of mathematics operations of addition, subtraction and multiplication can be done in an equal time with no need for a carry. The primary difficulties of the residue code pertain to the power of the relative significance of two residue representations, and to the division procedure. A discussion of the arithmetic operations and the conversion system required to convert from a residue code to a weighted code is given below. Its miles concluded that in its gift state the residue code might be not appropriate for wide

spread purpose computation however is appropriate for a unique magnificence of control troubles.

Similarly studies in both additives and arithmetic is required if a residue code suitable for popular motive computation is to be obtained [7]

Suppose an integer number U with tree modulus's m1 , m2 , m3 can represent U in modular by:

u1 = u mod m1 , u2 = u mod m2 , u3 = u mod m3
u = (u mod m1 , u mod m2 , u mod m3)
Where:
u1, u2, u3 are residue integer numbers
m1, m2, m3 are modular

H. L. Garner [8] , [9] , introduced a practical technique for transformation from (u1, … , ur) to u, such a way can be finished using constants Cij for $1 \leq i < j \leq r$, (5) in which

Cij mi $\equiv$ 1 (modulo mj) , and gcd(mi, mj) = 1

Note 1: the image stand for congruence).
Note 2: gcd stand for finest common divisor)[3].
Once the constants Cij has been decided pleasurable (5) ,we will get: (6)
$v_1 = u_1 \bmod m1$,
$v_2 = (u_2 - v_1) C_{12} \bmod m_2$,
$v_3 = ((u_3 - v_1) C_{13} - v_2) C_{23} \bmod m_3$.
…
vr = (… ((ur – v1) C1r – v2) C2r - … - vr-1) Cr-1 mod mr
Then:
$u = v_r m_{r-1} \dots m_2 m_1 + \dots + v_3 m_2 m_1 + v_2 m_1 + v_1$
Where:
u is the number satisfying the conditions : $0 \leq u < m$, u uj (mod mj) for $1 \leq j \leq r$

4- The suggested method

The proposed method consists of many stages each has a basic roll in the algorithm. The first stage is to generate the key, the second is the encryption process and finally the decryption process.

4-1 key generation Algorithm

1-Choose key as one character or more than one character
2-convert Key to AscII given keyA
3- Convert the keyA to modular
KeyA mod x2 = x1
KeyA mod x4 =x3

KeyA mod x6 = x5
KeyA written (x1 ,x2 ,x3, x4,x5 ,x6)
Where:
x1,x3,x5 residue
x2,x4,x6 modular

4-Change the order of keyA given (x1 x6 x2 x4 x3 x5)
5- Convert to binary
6-Add x1 to x6 given x7
7- Add x2 to x4 given x8
8- Add x5 to x3 given x9
9-Xor x7 with x8 given x10
10- Xor x10 with x9 given x11
11- Convert x11 to decimal, obtain mod 26 to get the key as shown in figure 2.

4-2 Encryption algorithm for one character

1- Read the plain text
2- Convert the plain text to AscII given PL
3- Find modular to p
PL mod p2 = p1
PL mod p4 = p3
PL mod p6 =p5
PL is written (p1,p2,p3,p4,p5,p6)
Where:
p1 ,p3 ,p5 residue
P2 ,p4 ,p6 modular

4- Encrypt each p with the key using Additive Algorithm obtaining the cipher text

(c1,c2,c3,c4,c5,c6)
C1 = P1 + key mod 26
C2 = P2 + key mod 26
C3 = P3 + key mod 26
C4 = P4 + key mod 26
C5 = P5 + key mod 26
C6 = P6 + key mod 26

5-Send the cipher text(c1,c2,c3,c4,c5,c6)

4-3 Decryption algorithm for one character

1- Read the cipher text (c1,c2,c3,c4,c5,c6)
2- Decrypt the cipher text using Additive algorithm (c1 ,c2 ,c3 ,c4 ,c6)
   P1= C1- key mod 26
   P2= C2 - key mod 26
   P3= C3 - key mod 26
   P4= C4 - key mod 26
   P5= C5 - key mod 26
   P6= C6 - key mod 26
   P=(p1 ,p2 ,p3 ,p4 ,p5 ,p6)
3- Use H. L. Garner's law to convert P to decimal
4- Find y1 using the formula y1 + p4 mod p5 =1
5- Find y2 using the formula (y2 * p4) mod p6 =1
6- Find y3 using the formula (y3 * p5) mod p6 =1
7- Find h1 using the formula h1 = p1 mod p2
8- Find h2 using the formula h2= (p1 - h1) * y1 mod p5
9- Find h3 using the formula h3=((p3 –h1) *y2 –h2)*y3 mod p6
10- The plain text =h3

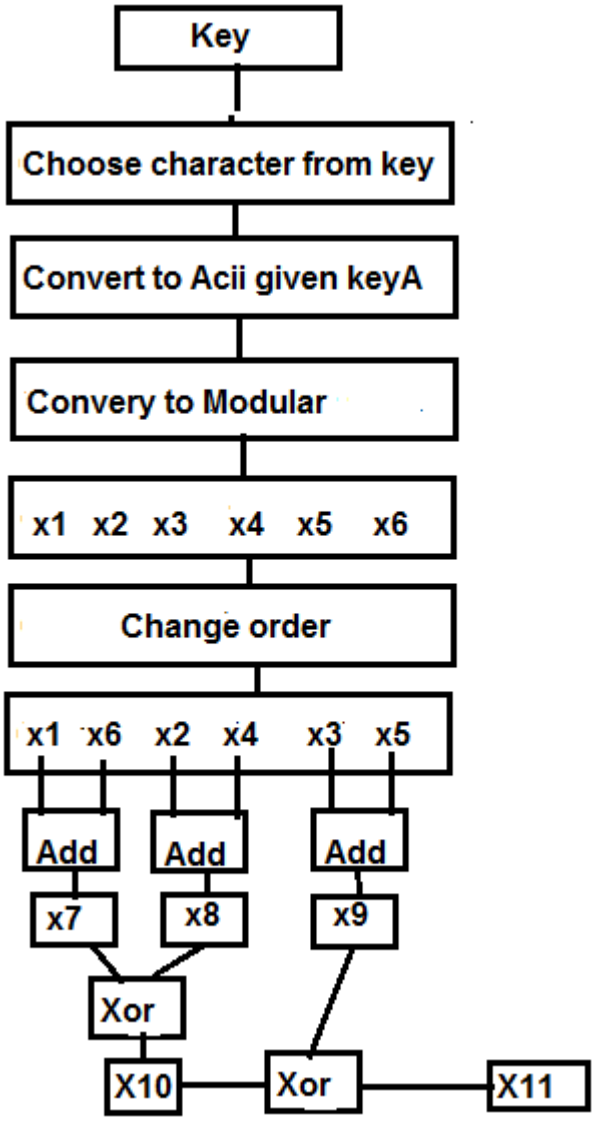

Figure 2: Key generation algorithm

5-Algorithm implementation

5-1 Key generation

1- Let K='C'
2- Convert to AscII =67
3- Took the modular of 67 (1 2 4 7 4 9) given (x1 x2 x3 x4 x5 x6)

4- Rearrange the sequence as (1 9 2 7 4 4) given =(x1 x6 x2 x4 x3 x5)
5- Convert to binary x1=0001 x2= 1001 x3= 0010 x4= 0111 x3= 0100 x5=0100
6- Add x1 with x6 given x7=1010
7- Add x2 with x4 given x8 = 1001
8- Add x3 with x5 given x9 = 1000
9- Xor x7 with x8 given x10= 1011
10- Xor x10 with x9 given x11= 1011
11- Convert to decimal (11)
12- Took modular 26 given the key =11

5-2 Encryption

1- Plain text = "A"
2- ASCII of plain text 65
3- P1 = 65 mod 2 = 1
4- P3 = 65 mod 7 = 2
5- P5= 65 mod 9 = 2
6- PL=(1 2 2 7 2 9)
7- Encrypt E_k (p) = p+ k mod 26
8- c1 = p1 + Key Mod 26 = 1+11 mod 26 = 12
9- c2 = p3 + Key Mod 26 = 13
10- c3 = p5 + Key Mod 26 = 13
11- c4 = p2 + Key Mod 26 = 13
12- c5 = p4 + Key Mod 26 = 18
13- c6 = p6 + Key Mod 26 = 20
14- C =(12 13 13 13 18 20)
15- decrypt D_k (c) = c - k mod 26
16- p1 = c1 - Key Mod 26 =1
17- p2 = c4 - Key Mod 26 =2
18- p3 = c2 – Key Mod 26 =2
19- p4 = c5 - Key Mod 26 = 7
20- p5 = c3 – Key Mod 26 =2
21- p6 = p6 – Key Mod 26 =9
22- PL= (1 2 2 7 2 9)

23- Use L.H Gerner's law to convert to decimal
24- Find y1 * p2 = 1 mod p4 y1= 4
25- Find y2 * p2 = 1 mod p6 y2=5
26- Find y3 * p6 = 1 mod m3 y3= 4
27- Find h1 = p1 Mod p2 h1 = 1
28- Find y2 * p2 = 1 mod p6 h2=4
29- Find y3 * p6 = 1 mod m3 h3= 4
30- Find u = h3 * p4 * p2 + h2 * p2 + h1 =65
31- The plain text = "A"

Figure 3 below illustrate the implementation of the algorithm:

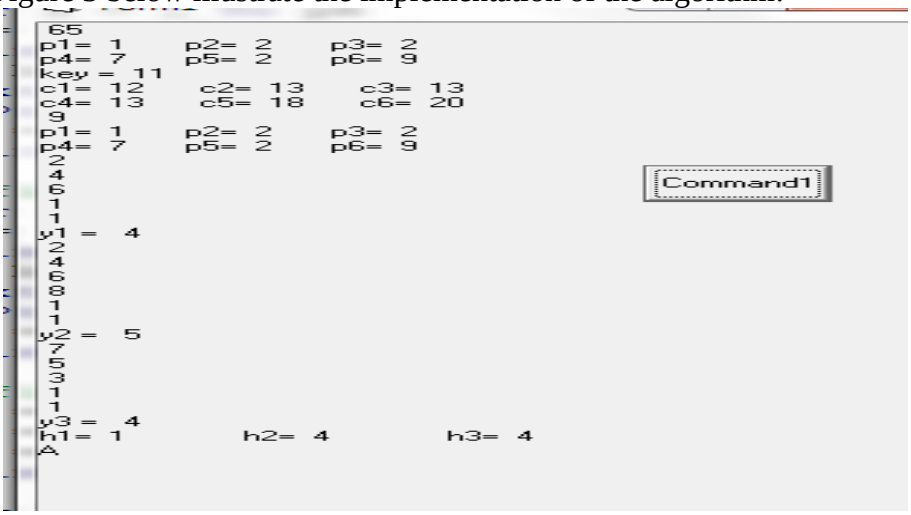

Figure 3: implementation of encryption algorithm

6-Conclusion

Mathematic is one of the applied sciences that interfere with most scientific fields. Computer science is one of these fields and specially the security of computer which depends on cryptographic methods. Key generation is considered to be a back bone for security system. Mathematic was employed in

generating a symmetric key and send it to other side taking an advantage of "mathematic power"

The plaintext was converted mathematically to arithmetic modularity to be encrypted with the symmetric key .This conversion gave the algorithm extreme power full for resisting cryptanalyst to find the key or the plain text.

This research proposes a new algorithm based on Additive Cipher with increasing complexity of the algorithm. The key used has being optimized to improve the strength and complexity from key determination.

References

[1] Widodo Achmad, "Block Cipher Cryptography Design Based on Planting Paddy and Rice Field Techniques". Bandung, April 2015.

[2] Dunkom. Binary Numbers, (Binary), http: //www.dunovtek. Wordpress. Com / 2011/08/05 / number-binary-binary, 2011.

[3] Ridwan, "Designing The Key Symmetry Cryptography Algorithm By Expanding the Vigenere Algorithm and Analysis of Kasiski's Methods"

[4] Vittal Kumar Mittal1, Manish Mukhija2 , Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique, International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 3 Issue 5, August 2019

[5] Cryptosystem Using New Strategy for Generating key, International Journal of Advanced Research in Science, Engineering and Technology, Vol. 4, Issue 8 , August 2017,

[6] One Time Pad Key Generation Using Elliptic Curve Key Exchange , International Journal of Research in Information Technology, Volume 1, Issue 2, Dec 2017

[7] https://www.geeksforgeeks.org/caesar-cipher-in-cryptography

[8] Imad Matti Bakko , "PROPOSING A METHOD TO PERFORM MODULAR ARITHMETIC OPERATIONS ON INTEGER NUMBERS WITH DIFFERENT MODULI", international journal of research in computer applications and robotics, Vol.3 Issue.3, March 2015

[9] Alfred J. Menezes, Paul C. Van Oorschet, Scott A. Vanstone, "Hand book of Applied Cryptography", CRC PRESS, India, 1997.

[10] Donald Knuth, “The Art of Computer Programming”, volume 2: Semi Numerical Algorithms. Third Edition, Addison-Wesley, 1997

[11] H.L. Garner, “The Residue Number System”, IRE Trans. Electro Comp. vole EC8, 1959.

[12]http://sylvainavenel.esy.es/DNL_SI/TheBlackChamber/TheBlackChamber/Caesarcipher.html

[13] Dr.Sana Ahmed Kadhim , Dr.Saad Abdual Azize Abdual Rahman," A Proposed Method for Image Verification by Encrypted Hidden Text using a Chaotic Polynomial and Random Locations”, International Journal of Civil Engineering and Technology (IJCIET), CiteScore:2.76, SJR:0.246, SNIP:0.153, Impact Factor:9.7820 , ISSN:0976-6316.