Text Cryptography Using Mix Modular Representation of codes

Imad Matti Bakko

Dr. taif sami hasan

.Dr.Saad AbdualAsize Abdual Rahman

Al-Ma‘moon University College

Abstract

In this paper, the basis of our work is focused on converting any text required to be ciphered into corresponding ASCII codes, and then transferring these codes into suitable mix modular representation, where more than one different modulus is used to represent each code in the text. In addition to that, we used and represent many keys such as public key, private key and secret key which are used in this work as modular representation to encrypt plain text and to decrypt cipher text.

Keywords: modular arithmetic, public key, private key, secret key, plain text, cipher text.

1. Introduction

Modular arithmetic can be handled mathematically by introducing a congruence relation (≡). for a positive integer m, two integers a and b are said to be congruent modulo m, written: a ≡ b (mod m), if their deference a-b is an integer multiple of m or m divides (a-b). The number m is called the modulus of the congruence, for example 38 ≡ 14 (mod 12), i.e. 38 is equivalent to 14 modulus 12, because 38 – 14 = 24, which is a multiple of 12. The same rule holds for negative values: -8 ≡ 7 (mod 5), 2 ≡ -3 (mod 5), -3 ≡ -8 (mod 5). [1][2][3]

Now, if we have an integer number **u** and three different modulus such as m_1, m_2, m_3, The idea behind our work is to have different modulus m_1, m_2, m_3 and to work indirectly with residues u mod m_1, u mod m_2, u mod m_3 instead of working directly with the integer number u. we can find the representation of u in modular form by means of division and as follows:

u_1 = u mod m_1, u_2 = u mod m_2, u_3 = u mod m_3 where u_1, u_2, u_3, are called residues. Therefore we can regard (u_1, u_2, u_3) as a new type of representation “modular representation “for the integer number u.

hence, the modular representation of the number u will be as follows:

u = (u_1 mod m_1, u_2 mod m_2, u_3 mod m_3). [1][2][3][4]

a decimal number for example the digit 3 can be converted to modular representation as follows:

Let u = 3 which is a decimal number and let m_1 = 2, m_2 = 3, m_3 = 5, be three different residues, then by division and taking the reminder we get: 3 mod 2 = 1, 3 mod 3 = 0, 3 mod 5

= 3. Hence the modular representation of the decimal number 3 is: u = 3 = (1 mod 2, 0 mod 3, 3 mod 5).

1.1 Converting a number from modular representation to its decimal.

H. L. Garner [4][5][6], introduced a usable method for converting from modular representation formula($u_1, \dots , u_r$) back to a decimal number u, such a method can be carried out by using constants $C_{i\,j}$ for $1 \le i \le j \le r$, where

$C_{i\,j}\ m_i \equiv 1$ (modulo m_j) , and gcd (m_i , m_j) = 1 ……………………… **(1)**

(Note: **gcd** stand for greatest common divisor). [3]

Once the constants $C_{i\,j}$ have been determined and satisfying (1), we can get:

$v_1 = u_1 \bmod m_1$, ………………………… **(2)**

$v_2 = (u_2 - v_1)\ C_{1\,2} \bmod m_2$, ………………………… **(3)**

$v_3 = ((u_3 - v_1)\ C_{2\,3} \bmod m_3$ …………………………… **(4)**

and $u = v_3\ m_2\ m_1 + v_2\ m_1 + v_1$ …………………………… **(5)**

previously, we found that the modular representation of the decimal number 3 is: (1 mod 2, 0 mod 3, 3 mod 5), where, $u_1 = 1$, $u_2 = 0$, $u_3 = 3$, and $m_1 = 2$, $m_2 = 3$, $m_3 = 5$.

To return this modular representation back to its decimal number, we use the above laws of Garner (1, 2, 3, 4, and 5). First we find $C_{1\,2}$, $C_{1\,3}$, $C_{2\,3}$ according to Garner law (1), and as follows:

$C_{1\,2} \times m_1 \equiv 1 \bmod m_2$

$C_{1\,2} \times 2 \equiv 1 \bmod 3 \quad \rightarrow C_{1\,2} = 2$

$C_{1\,3} \times m_1 \equiv 1 \bmod m_3$

$C_{1\,3} \times 2 \equiv 1 \bmod 5 \quad \rightarrow C_{1\,3} = 3$

$C_{2\,3} \times m_2 \equiv 1 \bmod m_3$

$C_{2\,3} \times 3 \equiv 1 \bmod 5 \quad \rightarrow C_{2\,3} = 2$

Secondly, we find v_1, v_2, v_3 according to Garner laws (2, 3, and 4), and as follows:

$v_1 = u_1 \bmod m_1$

$v_1 = 1 \bmod 2 \quad \rightarrow v_1 = 1$

$v_2 = (u_2 - v_1) \times C_{1\,2} \bmod m_2$

$v_2 = (0 - 1) \times 2 \bmod 3$

$= -2 \bmod 3 = (-2 + 3) \bmod 3 = 1 \bmod 3 \quad \rightarrow v_2 = 1$

$v_3 = ((u_3 - v_1) \times C_{1\,3} - v_2)\ C_{2\,3} \bmod m_3$

$= ((3 - 1) \times 3 - 1) \times 2 \bmod 5$

$= 10 \bmod 5 \quad \rightarrow v_3 = 0$

Finally, by using Garner law (5), we find the decimal number **u** as follows:

u $= v_3 \times m_2 \times m_1 + v_2 \times m_1 + v_1$

$= 0 \times 3 \times 2 + 1 \times 2 + 1$

u = 3 the decimal number 3. Which is the corresponding decimal number of the modular representation (1 mod 2, 0 mod 3, 3 mod 5).

2. Ciphering a plain text

We shall use stream cipher to cipher any symbol (letter, number, special character) exist in the plain text. The symbols in the plain text will be converted into their corresponding ASCII codes, then each code will be transferred to its corresponding modular representation in the form of three different modulus and residues, for example the ASCII code of the operation '+' is 43(according to the ASCII character set table and their decimal values). Then we convert 43 to a modular representation with three different modulus and residues as follows:

43 = (1 mod 3, 3 mod 5, 1 mod 7).

Where $u_1 = 1, u_2 = 3, u_3 = 1$ are the residues of division ,

and m1 = 3, $m_2 = 5, m_3 = 7$ are the modulus's.

It should be noted that the choice of m_1, m_2, m_3 is not selected randomly, it subject to the following rules:

Rule (1): gcd (m_i , m_j) = 1. [3]

For example: gcd (3, 5) = 1, gcd (3, 7) = 1, gcd (5, 7) = 1

Rule (2): the number 43 must be in between the following dynamic range. [7][8]

Dynamic range = [0, $\prod_{i=1}^{n} mi$ -1].

For example the dynamic range of (43) = [0, $m_1 \times m_2 \times m_3 - 1$] = [0, 3 × 5 × 7 -1] = [0, 104],

which satisfy rule(2). [8][9]

2.1 Suggested protocol between sender and receiver to get a secret key

a. The sender chooses randomly any decimal number as a public key such as u and convert it to its corresponding modular representation whose residues are m_1 , m_2 , m_3 and by division we get:

(u_1 mod m_1 , u_2 mod m_2 , u_3 mod m_3) …………….. Public key

b. The sender send this key(which is in modular representation) to the receiver.

c. The receiver chooses randomly any decimal number such as y and raise the residues of the key received from the sender to power of y and send it to the sender , and as follows:

($(u_1)^y$ mod m_1 , $(u_2)^y$ mod m_2 , $(u_3)^y$ mod m_3) ……………. receiver private key

d. The sender chooses randomly any decimal number such as x and raise the residues of the primary key to power of x and send it to the receiver , and as follows:

($(u_1)^x$ mod m_1 , $(u_2)^x$ mod m_2 , $(u_3)^x$ mod m_3) ……………….. Sender private key

e. The sender raise the residues of the key received from the receiver to power of x, and as follows:

($((u_1)^y)^x$ mod m_1 , $((u_2)^y)^x$ mod m_2 , $((u_3)^y)^x$ mod m_3)

= ($(u_1)^{yx}$ mod m_1 , $(u_2)^{yx}$ mod m_2 , $(u_3)^{yx}$ mod m_3) ………….. (4)

f. The receiver raise the residues of the key received from the sender to power of y, and as follows:

($((u_1)^x)^y$ mod m_1 , $((u_2)^x)^y$ mod m_2 , $((u_3)^x)^y$ mod m_3)

= ($(u_1)^{xy}$ mod m_1 , $(u_2)^{xy}$ mod m_2 , $(u_3)^{xy}$ mod m_3) ………….. (5)

Since the modular representation of (1) and (2) are the same, hence both sender and receiver have arrived to the same value and can be used as a secret key to exchange information without worrying about any intruders and because this secret key is sent without using any transmission channel. Figure (1) illustrates this. [10]

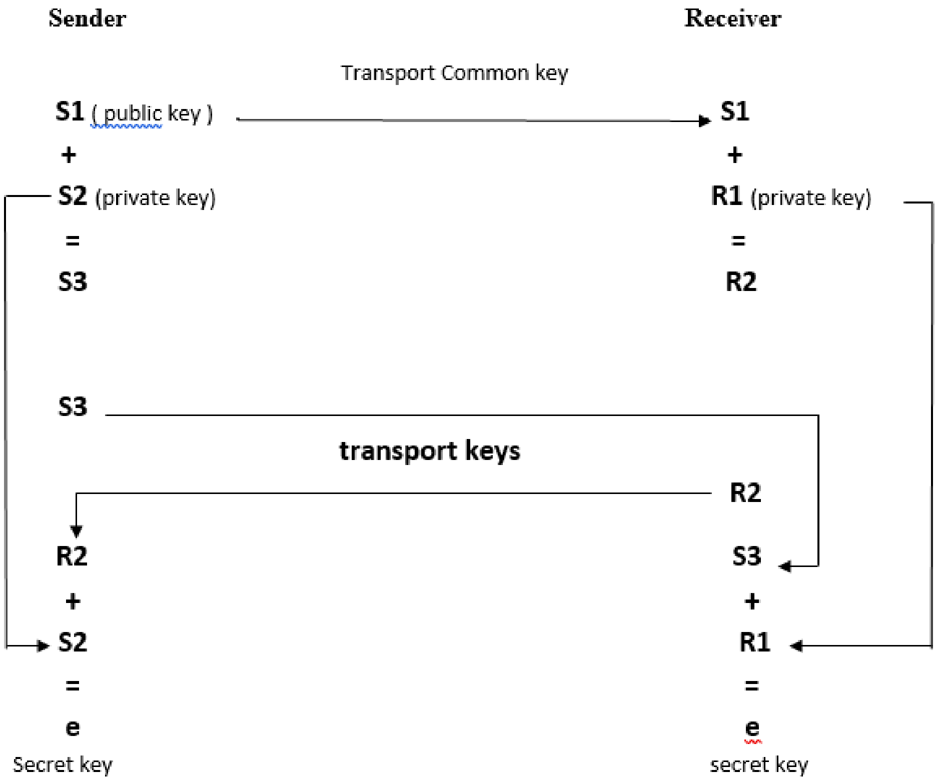


Figure (1): protocol used between sender and receiver to get secret key (known to both) without using transmission channel.

Now suppose for example a sender chooses randomly a decimal number 19, then it will be converted to suitable modular representation and as follows:

19 = (1 mod 3, 5 mod 7, 8 mod 11) , this will be converted to : 010305070811

and then to binary system as : 000100110101011110001011 and send it to the receiver as a **public key**.

The sender chooses randomly another decimal number such as 2 and raises the residues of the modular representation of the number 19 to the power of 2 and as follows:

(1^2 mod 3 , 5^2 mod 7 , 8^2 mod 11) = (1 mod 3 , 4 mod 7 , 9 mod 11). This will be converted to:

010304070911 and then to binary system as: 000100110100011110011011

This will be send also to the receiver as a **sender private key**.

The receiver return the sender public key to decimal system, and then to its modular representation:

000100110101011110001011 = 010305070811 = (1 mod 3, 5 mod 7, 8 mod 11).

The receiver chooses randomly a decimal number such as 3 and raises the residues of the modular representation of the sender public key to the power of 3 and as follows:
$(1^3 \bmod 3 , 5^3 \bmod 7 , 8^3 \bmod 11)=(1 \bmod 3, 6 \bmod 7, 6 \bmod 11)$. This will be converted to: 010306070611 and then to binary system as: 000100110110011101101011
This will be send back to the sender as a **receiver private key**.

The sender receive the private key from the receiver and change it to decimal system and then to its modular representation as follows:
Receiver private key=00010011011001110110101=010306070611=(1mod3,6mod7,6mod11)

The sender raises the residues of the modular representation of the reliever private key to the second random key which is 2, as follows:
$(1^2 \bmod 3 , 6^2 \bmod 7 , 6^2 \bmod 11) = (1 \bmod 3, 1 \bmod 7, 3 \bmod 11)$. ………………. (x)

The receiver receives the private key from the sender and changes it to decimal system and then to its modular representation as follows:
Sender private key = 000100110100011110011011 = 010304070911 = (1 mod 3, 4 mod 7, 9 mod 11).

The receiver raise the residues of the modular representation of the sender private key to the random key selected by the receiver which is 3, as follows:
$(1^3 \bmod 3 , 4^3 \bmod 7 , 9^3 \bmod 11) = (1 \bmod 3, 1 \bmod 7, 3 \bmod 11)$. ………………. (y)

Now both sender and receiver have the same value, since x is identical to y without using transmission channel. This x or y is the **secret key** between both sender and receiver.

Now both sender and receiver need to know the decimal number of x or y,
Using the laws of Garner, we can find the decimal number of the secret key x or y. the representation of (1 mod 3, 1 mod 7, 3 mod 11), is as follows: modular
$u_1 = 1 , u_2 = 1 , u_3 = 3$ are the residues of the secret key.
$m_1 = 3 , m_2 = 7 , m_3 = 11$ are the modulus's of the secret key.

First we find C_{12}, C_{13}, C_{23} according to Garner law (1), and as follows:
$C_{12} \times m_1 \equiv 1 \bmod m_2$
$C_{12} \times 3 \equiv 1 \bmod 7 = (C_{12} \times 3) \bmod 7 = 1$ → $C_{12} = 5$
$C_{13} \times m_1 \equiv 1 \bmod m_3$
$C_{13} \times 3 \equiv 1 \bmod 11 = (C_{13} \times 3) \bmod 11 = 1$ → $C_{13} = 4$
$C_{23} \times m_2 \equiv 1 \bmod m_3$
$C_{23} \times 7 \equiv 1 \bmod 11 = (C_{23} \times 7) \bmod 11 =1$ → $C_{23} = 8$

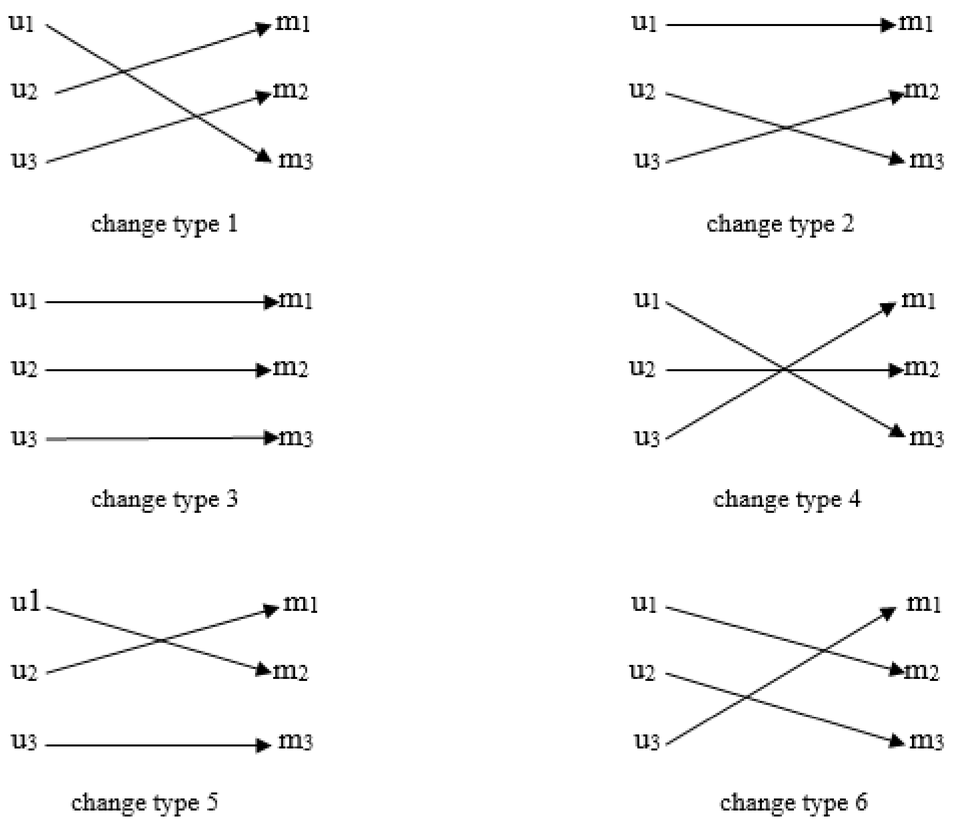
Secondly, we find v_1, v_2, v_3 according to Garner laws (2, 3, 4), and as follows:
$v_1 = u_1 \bmod m_1$
$v_1 = 1 \bmod 3$ → $v_1 = 1$
$v_2 = (u_2 - v_1) \times C_{12} \bmod m_2$
$v_2 = (1 - 1) \times 5 \bmod 7$ → $v_2 = 0$
$v_3 = ((u_3 - v_1) \times C_{13} - v_2) C_{23} \bmod m_3$
$= ((3 -1) \times 4 - 0) \times 8 \bmod 11$
$= 64 \bmod 11$ → $v_3 = 9$

Finally, by using Garner law(5), we find the decimal number u as follows:
$u = v_3 \times m_2 \times m_1 + v_2 \times m_1 + v_1$

$= 9 \times 3 \times 7 + 0 \times 3 + 1$

$u = 190 \bmod 6 = 4.$

This leads that the sender and receiver independently to have the secret key number 4 without any transmission, which means that we will use the change type 4 (according to the six different possible changes which are illustrated in figure (2)) to encrypt each character in the plain text before sending it to the receiver and this is from sender point of view. [10][11][12]



change type 1

change type 2

change type 3

change type 4

change type 5

change type 6

Figure (2): schematic encryption scheme

But from receiver point of view, he must return the encryption of each character received from the sender to its original, i.e. return the encryption from change type 4 to change type 3 before making any decryption since he knows the secret key 4, as illustrated in figure (2) above.

3. Summary of the results.

From the program mentioned above the sender and the receiver will agree and get the secrete key = 4. The sender will encrypt every character or symbol by using this secrete key, (i.e. the change type 4 according to figure (2)). From receiver point of view, he must return the encryption of each character received from the sender to its original form, i.e. return the encryption from change type 4 to change type 3 before making any decryption since he knows the secret key 4, as illustrated in figure (2) above.

For example to encrypt the number 19, the sender will change it to its modular representation and as follows:
19 = (1 mod 3, 5 mod 7, 8 mod 11), and then to the following form:
010305070811 where
u1 = 01,   m1 = 03
u2 = 05,   m2 = 07
u3 = 08,   m3 = 11
This is the original case (change type 3)
The sender will send 19 as:
011105070801 where
u1 = 01,   m1 = 11
u2 = 05,   m2 = 07
u3 = 08,   m3 =01
This is encrypted type (change type 4)
The receiver will receive this encrypted type 011105070801 and return it to change type 3, and by using garner laws; the receiver will get the encrypted number 19.

Conclusion

1. In this work, we used three different moduli to encrypt plain text codes and to decrypt a cipher text codes. We can extend this subject to be more secure to four, five, six or more different moduli for the same purpose. For example the modular representation of the decimal number 19 maybe in the following different modular representations:

19 = (1 mod 2 , 1 mod 3 , 4 mod 5) ……………………… format 1
19 = (1 mod 2 , 1 mod 3 , 4 mod 5 , 5 mod 7) ……………….. format 2
19 = (1 mod 2 , 1 mod 3 , 4 mod 5 , 5 mod 7 , 1 mod 9) …………… format 3
19 = (1 mod 2 , 1 mod 3 , 4 mod 5 , 5 mod 7 , 1 mod 9 , 8 mod 11) ………. format 4

Format 3 and 4 need more extension for Garner's laws therefore it is recommended.

2. Ciphering and deciphering of a text by using different modules such as format 2, 3, and 4 will be more secure, therefore it is recommended.

3. The choice of these formats as in 1 are not random, it is subjected to the two rules mentioned earlier in this work to be true. In case of format 1, there are three different moduli and residues; hence the number of permutations is 3! = 6. In case of format 2, there are four different moduli and residues, hence the number of permutations is 4! = 24. In case of format 3, there are five different moduli and residues; hence the number of permutations is 5! = 120. In case of format 6, there are six different moduli and residues; hence the number of permutations is 6! = 720. In general its n!.

5. Much larger values for any keys selected randomly by sender and receiver and larger modulus's such as m_1, m_2, m_3, m_4, make the problem more secure.

References

[1] **BAKKO**. I.M, "Proposing a method to perform modular arithmetic operations on integer numbers with different modules ", international journal of research in computer application and robotics, Volume 3, Issue 3, March 2015.

[**2**] ALFRED. J. MENEZES, PAUL C. VAN OORSCHET, SCOTT A. VANSTONE, "Hand book of Applied Cryptography", CRC PRESS, India, 1997.
[**3**] DONALD KNUTH, “The Art of Computer Programming”, volume 2: Semi Numerical Algorithms. Third Edition, Addison-Wesley, 1997.
[**4**] GARNER .H.L., “The Residue Number System”, IRE Trans. Electro Comp. vole EC8, 1959.
[**5**] History of Residue Number System – University of Jordan-A www.yahoo.com.
[**6**] HOFFSTEIN, J., PIPHER, J., SIVERMAN.,J.H., and SILVERMA, J.H." An introduction to mathematical cryptography" (Vol. 1). New York: Springer (2008).
[**7**] NEAL kABLITZ, “ A Course in Number Theory and Cryptography”, Springer-verlag, Second Edition, 2011, Page 19, 21, 24,
[**8**] BALDONI M.W., CILIBERTO C. , PIACENTINI CATTANEO G.M. “ Elementary Number theory, Cryptography and Codes” Springer-verlag Berlin Heidelberg, 2008, Page 122.
[**9**] THOMAS KOSHY, “Elementary Number Theory with Applications”, ELSEVIER INC. Page 212,241, second Edition 2007.
[**10**] Diffie Whitfield, Martin Hellman."New Directions in Cryptography." IEEE transactions on information theory 22.6.(1976).
[**11**] HANS DELFS, HELMUT KNEBL,”Introduction to Cryptography, Principles and Springer-verlag Berlin Heidelberg, 2007, page 35. Applications”,
[**12**] Hoffstein, J., Pipher, J., Silverman.,J.H., and Silverman, J.H." An introduction to mathematical cryptography" (Vol. 1). New York: springer. (2008)