UniversePG

Publisher homepage: www.universepg.com, ISSN: 2707-4625 (Online) & 2707-4617 (Print)

https://doi.org/10.34104/ijmms.020.0990103

International Journal of Material and Mathematical Sciences

Journal homepage: www.universepg.com/journal/ijmms

Conference Paper

An Execution of a Mathematical Example Using Euler's Phi-Function in Hill Chiper Cryptosystem

Mohiuddin Ahmed[1]* and Md. Ashik Iqbal[1]

[1]Faculty Member in Mathematics, Department of Computer Science and Engineering, North Western University (NWU), Khulna, Bangladesh.

*Correspondence: mohiuddina6@gmail.com (Mohiuddin Ahmed, Faculty Member in Mathematics, Department of Computer Science and Engineering, NWU, Khulna, Bangladesh).

§ Presented at the International conference on Applied Science Mathematics and Statistics (ICASMS - 2020), 25-26 November 2020, organized by SciencePlus Global Research Forum.

ABSTRACT

In this article, we have explained the RSA public-key cryptosystem initiate by Rivest and Hill Chiper cryptosystem initiate by Lester. Hill for coding and decoding the text. To explain these we apply the Euler-phi function, congruence, and simple Matrix Application in cryptography to decode and encode the message. In our analyses, we were collaborated two cryptosystems which is more assured than standard cryptographic process such as Ceaser cipher. We apply both secret-key cryptography and public-key cryptography which differ from standard cryptography. In our presentation, we use two keys for coding and two for decoding.

Keyword: Cryptography, Congruence, Euler' phi function, Hill Chiper, RSA cryptosystem, and Matrix.

INTRODUCTION:

Institutions in both the public and private sectors have become progressively based on electronic data processing. Huge volume of digital data are now assemble and preserved in macro scale, computer data circulated between computers and terminal devices connected jointly in transmission networks. Except suitable prevention, these data are permitting to blocking during transference or they might be materially disconnect or duplicate while in storage. This could effect in unwelcome submission of data and future annexation of privacy (Diffine and Hellman, 1976).

In this conference paper, we have explained the RSA public-Key cryptosystem and Hill Chiper crypto system and exécute a math metical exemple of combinaient those crypto system to Secure the data (Cohen, 1994 ; Adhikari and Adhikari, 2007).

LINEAR CONGRUENCE

This form ax $ax \equiv b(\mathrm{mod}\ n)$ is said to be a linear congruence and by a outcome of this equation we denote an integer x_0 for which $ax_0 \equiv b(\mathrm{mod}\ n)$ by explanation $ax_0 = b(\mathrm{mod}\ n)$ and only if $n / ax_0 - b$ what quantity to the identical if and only if $ax_0 = b = ny_0$ for some integer y_0. Thus the matter of determinations of all integers holds the linear congruence $ax = b(\bmod n)$ is uniform with that of getting all solutions of the linear Diophantine equation $ax - ny = b.$

RSA Cryptosystem

Let n be a multiply of two individual primes p and q. Let p=c= z_n. Let us destine –

$$K = (n, p, q, e, d) : ed = 1(\bmod \phi(n))$$

Where, $\phi(n)$ called Euler's function is the positive integers less than n which are relatively prime to n for each –

$K = (n, p, q, e, d)$ We define $e_k(x) = x^e (\bmod n)$ and $d_k(y) = y^d (\bmod n)$ where $x, y \in z_n$. The values p, q and d are used as public key.

Hill Cipher Cryptosystem

For Hill Cipher we imposed arithmetical values to every plaintext and cipher text letter so that –

$$A = 01, B = 02, C = 03, D = 04, E = 05, F = 05, G = 06, H = 07, I = 08, J = 09, J = 10, K = 11, L = 12$$
$$M = 13, N = 14, O = 15, P = 16, Q = 17, R = 18, S = 19, T = 20, U = 21, V = 22, W = 23, X = 24, Y = 25, Z = 26$$

With 27 indicating a space between words.

Enciphering step 01: Choose a square matrix A of order 2×2 **with** integer listings to perform the encoding. The matrix has to be revertible modulo m but we will explain later.

Enciphering step 02: Grouping sequential plaintext letters into pairs. If we result in with one single letter at the end directly add an arbitrary "chump" letter to complete the next last pair of letters.

Enciphering step 03: Transform each plaintext pair $p1p2$ into a column vector **P**.

To encrypt the message we multiply our plaintext matrix P by our converted matrix **A** to form the product **AP**.

The resultant of our matrix multiplication is the cipher text matrix **C**.

This was the encoding technique. Now we decode our enciphered message.

Deciphering step 01: Now we sort the consecutive cipher text letters into pairs and transform each cipher text pair $c1c2$ into a column vector **C**. Then construct the cipher text matrix **C** of all our cipher text column vectors.

Deciphering step 02: Multiply the cipher text matrix **C** with the inverse of our enciphering matrix **A** to obtain the decoded message.

An Example of these System

If someone wants to convey a plaintext message to the user such as

ARREST NOW

To convert the message "ARREST NOW" First converts each letter into its digital identical using the replacement indication in Hill cipher cryptosystem (Rivest *et al.*, 1978). This capitulate the plain text number M=01181805 192027141523

Now we take a 2×5 matrix P for the values of M

$$P = \begin{bmatrix} 01 & 18 & 19 & 27 & 15 \\ 18 & 05 & 20 & 14 & 23 \end{bmatrix}$$

Let a 2×2 matrix A as

$$A = \begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} \text{ Then } A^{-1} = \begin{bmatrix} -4 & 3 \\ 3 & -2 \end{bmatrix}$$

Now the encoding matrix E is

$$E = AP = \begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} \left[\begin{bmatrix} 01 & 18 & 19 & 27 & 15 \\ 18 & 05 & 20 & 14 & 23 \end{bmatrix} \right]$$

$$= \begin{bmatrix} 2.1 + 3.18 & 2.18 + 3.5 & 2.19 + 3.20 & 2.27 + 3.19 & 2.15 + 3.23 \\ 3.1 + 4.8 & 3.18 + 4.5 & 3.19 + 4.20 & 3.27 + 4.14 & 3.15 + 4.23 \end{bmatrix}$$

$$=\begin{bmatrix} 56 & 51 & 98 & 96 & 99 \\ 75 & 74 & 137 & 137 & 137 \end{bmatrix}$$

Now we use congruence we have:

$$56 \equiv 02(\bmod 27)$$
$$51 \equiv 24(\bmod 27)$$
$$98 \equiv 17(\bmod 27)$$
$$96 \equiv 15(\bmod 27)$$
$$99 \equiv 18(\bmod 27)$$
$$75 \equiv 21(\bmod 27)$$
$$74 \equiv 20(\bmod 27)$$
$$137 \equiv 02(\bmod 27)$$
$$137 \equiv 02(\bmod 27)$$
$$137 \equiv 02(\bmod 27)$$

$$E=\begin{bmatrix} 02 & 24 & 17 & 15 & 18 \\ 21 & 20 & 02 & 02 & 02 \end{bmatrix}$$

Now we use RSA encoding system in the matrix E

E=

$$(02 \quad 21 \quad 24 \quad 20 \quad 17 \quad 02 \quad 15 \quad 02 \quad 18 \quad 02)$$

Now for the farther safety of the system we will code the cipher text E into another cipher text N with the support of Euler's phi function. For this sample we initially choose primes P=11, Q=17 of an impractical tiny size. In real P and Q would huge enough so that the multiplication of the number n=PQ is impractical (Niven *et al.*, 1980; Burton, 1989). Our enciphering number is –

$n = 11.17 = 187$, and

$Q(n) = 10.16 = 161 = 23.7$ Modulo.

Assume the enciphering proponent is nominated to be k=23, then the recapture element the individual integer j fulfilling the congruence $kj \equiv 1(\bmod Q(n))$ j=7.

To code N we require each part of N to be an integer less than 187. Now for the first part of the calculation is:

$$(02) = -185(\bmod 187)$$
$$(02)^4 = 33489(\bmod 187)$$
$$(02)^4 = 16(\bmod 187)$$
$$(02)^8 = 256(\bmod 187)$$
$$(02)^8 = 69(\bmod 187)$$
$$(02)^{16} = 4761(\bmod 187)$$
$$(02)^{16} = 86(\bmod 187)$$
$$(02)^{23} = (02)^{16} \times (02)^4 \times (02)^2 \times (02)(\bmod 187)$$
$$(02)^{23} = 86 \times 16 \times (-183) \times (-185)(\bmod 187)$$
$$(02)^{23} = 46584480(\bmod 187)$$
$$(02)^{23} = 162(\bmod 187)$$

$$\therefore (02)^{23} = 162(\bmod 187)$$

Now for the values (21)

Then,

$$(21)^2 = 67(\bmod 187)$$
$$(21)^4 = 4489(\bmod 187)$$
$$(21)^4 = 1(\bmod 187)$$
$$(21)^8 = 1(\bmod 187)$$
$$(21)^{16} = 1(\bmod 187)$$
$$(21)^{23} = 21^{16} \times 21^4 \times 21^2 \times 21(\bmod 187)$$
$$(21)^{23} = 1 \times 1 \times 67 \times 21(\bmod 187)$$
$$(21)^{23} = 1407(\bmod 187)$$
$$(21)^{23} = 98(\bmod 187)$$

$$\therefore (21)^{23} = 98(\bmod 187)$$

Now similarly we have

$$(24)^{23} = 63(\bmod 187)$$

Then

$$(20)^{23} = 113(\bmod 187)$$

Then

$$(17)^{23} = 51(\bmod 187)$$

Then

$$(02)^{23} = 162(\mathrm{mod}\,187)$$

Then

$$(15)^{23} = 42(\mathrm{mod}\,187)$$

Then

$$(02)^{23} = 162(\mathrm{mod}\,187)$$

Then

$$(18)^{23} = 35(\mathrm{mod}\,187)$$

Then

$$(02)^{23} = 162(\mathrm{mod}\,187)$$

Now the total coded message is:

162 98 63 113 51 162 42 162 35 162

Now we will decoded the message by using recapture element $j = 7$. We can recapture the earliest text:

$$\begin{aligned}
(162)^{2} &= 64(\mathrm{mod}\,187)\\
(162)^{4} &= 4096(\mathrm{mod}\,187)\\
(162)^{4} &= 169(\mathrm{mod}\,187)\\
(162)^{7} &= 169\times 64\times 162(\mathrm{mod}\,187)\\
(162)^{7} &= 1752192(\mathrm{mod}\,187)\\
(162)^{7} &= 02(\mathrm{mod}\,187)
\end{aligned}$$

$$\therefore (162)^{7} = 02(\mathrm{mod}\,187)$$

Now for the number (98)

$$\begin{aligned}
(98)^{2} &= 67(\mathrm{mod}\,187)\\
(98)^{4} &= 4489(\mathrm{mod}\,187)\\
(98)^{4} &= 1(\mathrm{mod}\,187)\\
(98)^{7} &= (98)^{4}\times(98)^{2}\times 98(\mathrm{mod}\,187)\\
(98)^{7} &= 6566(\mathrm{mod}\,187)\\
(98)^{7} &= 21(\mathrm{mod}\,187)\\
\therefore (98)^{7} &= 21(\mathrm{mod}\,187)
\end{aligned}$$

Now similarly we have

$$(63)^{7} = 24(\mathrm{mod}\,187)$$

Then

$$(113)^{7} = 20(\mathrm{mod}\,187)$$

Then

$$(51)^{7} = 17(\mathrm{mod}\,187)$$

Then

$$(162)^{7} = 02(\mathrm{mod}\,187)$$

Then

$$(42)^{7} = 15(\mathrm{mod}\,187)$$

Then

$$(162)^{7} = 02(\mathrm{mod}\,187)$$

Then

$$(35)^{7} = 18(\mathrm{mod}\,187)$$

Then

$$(162)^{7} = 02(\mathrm{mod}\,187)$$

Now the decoded message after introducing R.S.A system is -

M= (02 21 24 20 17 02 15 02 18 02)

$$\therefore E = \begin{bmatrix} 02 & 24 & 17 & 15 & 18\\ 21 & 20 & 02 & 02 & 02 \end{bmatrix}$$

Now we can recapture the earlier l text by using the inverse matrix A^{-1}

$$A^{-1} = \begin{bmatrix} -4 & 3\\ 3 & -2 \end{bmatrix}$$

$$D = A^{-1}E$$

$$= \begin{bmatrix} -4 & 3\\ 3 & -2 \end{bmatrix}\begin{bmatrix} 02 & 24 & 17 & 15 & 18\\ 21 & 20 & 02 & 02 & 02 \end{bmatrix}$$

$$= \begin{bmatrix} -4\times 2+3\times 21 & -4\times 24+3\times 20 & -4\times 17+3\times 2 & -4\times 15+3\times 2 & -4\times 18+3\times 2\\ 3\times 2+(-2)\times 21 & 3\times 24+(-2)\times 20 & 3\times 17+(-2)\times 2 & 3\times 15+(-2)\times 2 & 3\times 18+(-2)\times 2 \end{bmatrix}$$

$$= \begin{bmatrix} 55 & -36 & -62 & -54 & -66 \\ -36 & 32 & 47 & 41 & 50 \end{bmatrix}$$

Now we are applying congruence:

$$55 \equiv 01 (\text{mod } 27)$$
$$-36 \equiv 18 (\text{mod } 27)$$
$$-62 \equiv 19 (\text{mod } 27)$$
$$-54 \equiv 27 (\text{mod } 27)$$
$$-66 \equiv 15 (\text{mod } 27)$$
$$-36 \equiv 18 (\text{mod } 27)$$
$$32 \equiv 05 (\text{mod } 27)$$
$$47 \equiv 20 (\text{mod } 27)$$
$$41 \equiv 14 (\text{mod } 27)$$
$$32 \equiv 05 (\text{mod } 27)$$
$$47 \equiv 20 (\text{mod } 27)$$
$$41 \equiv 14 (\text{mod } 27)$$
$$50 \equiv 23 (\text{mod } 27)$$

$$D = \begin{bmatrix} 01 & 18 & 19 & 27 & 15 \\ 18 & 05 & 20 & 14 & 23 \end{bmatrix}$$

The total decoded message is –

$M = (01 \quad 18 \quad 18 \quad 05 \quad 19 \quad 20 \quad 27 \quad 14 \quad 15 \quad 23)$

Now to recapture the message translate every number of M into its digital equivalent using the substitution mentioned earlier this capitulate the original plaintext.

ARREST NOW

CONCLUSION:

The safety of our collaborate Hill cipher and RSA cryptography system is ground on various factors: First is that we utilize a key matrix A, which is only recognized to first party and second party (Koblitz, 1998). The second is that remembering n and k do not authorize you to know the value of j. Third since you recognize n it will be relatively simple to find j if you just divide n to determine the primes p and never less no one has enough time effectively to factor n when n only two very large prime factors and fourth the collaborate of these two cryptosystem gives a safety where the plaintext is entirely unthinkable to find out for the third parties.

ACKNOWLEDGEMENT:

Thanks to the authority of the Department and co-author that supported with proper assistance and writing to conduct successful research.

CONFLICTS OF INTEREST:

The authors declare no conflict of interest.

REFERENCES:

1) Adhikari M.R and Avishek Adhikari, (2007). Introduction to linear algebra with application to basic cryptography, (New Delhi 2007). https://www.amazon.com/Introduction-Linear-Algebra-Application-Cryptography/dp/8184120346
2) Burton M.D. (1989). Elementary Number theory, 2nd edition New Delhi, *W.M.C Brown publishers*.
3) Cohen H. (1994). A course in computational Algebric Number theory, *Springer*. https://www.springer.com/gp/book/9783540556404
4) Diffine W., and Hellman M.E. (1976). New direction in cryotography (IEEE Trans. Information Thesis 22(1976), 644-654. https://www.bibsonomy.org/bibtex/1252b1ee0e74b97af1dfeba816199860c/dret
5) Koblitz N. (1998). Algebraic aspects of Cryptography, *Springer*. https://www.springer.com/gp/book/9783540634461
6) Niven I, Herbert S.Z, Hugh L.M. (1980). An introduction to the theory of numbers (5th edition, *Willy and Sons*).
7) Rivest R., Adleman L.M, and Shamir A. (1978). A method for obtaining digital signature and public key cryptosystems "(Comm. Of ACM21 (1978)120- 126). https://doi.org/10.1145/359340.359342

Citation: Ahmed M, and Iqbal MA. (2020). An execution of a mathematical example using Euler's Phi-function in Hill Chiper cryptosystem, *Int. J. Mat. Math. Sci.*, **2**(6), 99-103. https://doi.org/10.34104/ijmms.020.0990103