IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 14, Issue 2 Ver. II (Mar. - Apr. 2018), PP 68-73
www.iosrjournals.org

A Perfect Implantation of Euler's Phi-Function in Hill Cipher Cryptosystem

Mohiuddin Ahmed
[1](*Mathematics, North Western University Khulna, Bangladesh)*
Corresponding Author: Mohiuddin Ahmed

Abstract: *In This Paper, we have discussed the RSA public key crypto system proposed by R, River, A, Shamir & L. Adeleman and Hill Chiper cryptosystem proposed by Lester S. Hill for encrypte the text. To Discuss these we use Euler-phi function, congruence and simple Matrix Application in cryptography to decrypt and encrypt the message. In Our analyses we combined two cryptosystem which is more secure than conventional cryptographic system such as Ceaser cipher. We use both secret key cryptography and public key cryptography which differ from conventional cryptography. In our thesis we use two keys for encryption & two for decryption. Decryption two keys effect inverse operations encryption keys. Therefore these keys are related each other.*

Keywords – *Cryptography, Congruence, Euler' phi function, RSA cryptosystem, Matrix*

Date of Submission: 11-04-2018 Date of acceptance: 26-04-2018

I. Introduction

Organizations in both the public and private sectors have become increasingly dependent on electronic data processing. Vast amount of digital data are now gathered and stored in large, computer data bases and transmitted between computers and terminal devices linked together in complex communication networks. Without appropriate safeguard, these data are susceptible to interception during transmission or they may be physically removed or copied while in storage. This could result in unwanted exposures of data and potential invasions of privacy. Cryptography is quickly becoming a crucial part of the world economy. Before the 1080 cryptography was used primarily for military and diplomatic communications and fairly limited contexts. In today's world, communication is moving rapidly to internet and a computer hacker can rapidly snoop computer transmissions for valuable information. We need to protect our access to computers (via passwords and encrypted remote access), our commercial transaction (credit card data and band data), our medical data (which may soon be stored on smart cards) and other information. In fact, cryptography has broadened greatly, from the study of secret writing to the study of information security.

II. The Purpose Of Cryptography

Cryptography is the science of writing in secret code and is an ancient art. The first documented use of cryptography in writing dates back to circa 1900 B.C when an Egyptian scribe used nonstandard hieroglyphs in an inscription. Some expert argue that cryptography appeared spontaneously sometime after writing was invented, with application ranging from diplomatic missives to war time battle plan. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communication. In data and telecommunications cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the internet.

Cryptography, then. Not only protects data from theft or alteration, but can also be used for user authentication. There are general three types of cryptographic schemes typically used to accomplish these goals: secret key cryptography, public-key cryptography and hash functionSecret Key cryptography (SKC): Uses a single key for both encryption and decryption.Public Key cryptography (PKC): Uses one key for encryption and another one for decryption.Hash Function: Uses a mathematical transformation to irreversibly encrypt information.

III. Linear Congruence

An equation of the form ax $ax \equiv b(\mathrm{mod} n)$ is called a linear congruence and by a solution of this equation we mean an integer x_0 for which $ax_0 \equiv b(\mathrm{mod}\ n)$ by definition $ax_0 = b(\mathrm{mod}\ n)$ if and only if $n / ax_0 - b$ what amounts to the same thing if and only if $ax_0 = b = ny_0$ for some integer y_0 . Thus the

problem of finding all integers satisfying the linear congruence $ax = b(\mathrm{mod} n)$ is identical with that of obtaining all solutions of the linear Diophantine equation $ax - ny = b$

RSA CRYPTOSYSTEM

Let n be a product of two distinct primes p and q .Let p=c= z_n .Let us define $K = (n, p, q, e, d) : ed = 1(\mathrm{mod}\phi(n))$ where $\phi(n)$ called Euler's function is the number of positive integers less than n which are relatively prime to n for each $K = (n, p, q, e, d)$ we define $e_k(x) = x^e (\mathrm{mod}\ n)$ and $d_k(y) = y^d (\mathrm{mod}\ n)$ where $x, y \in z_n$. The values n and e are public and the values p, q and d are used as public key.

IV. Hill Cipher Cryptosystem

For Hill Cipher we assign numerical values to each 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 2×2 matrix **A with** integer entries to perform the encoding. The matrix has to be invertible modulo m but we will discuss later.

Enciphering step 02: Group successive plaintext letters into pairs. If we end up with one single letter at the end simply add an arbitrary "dummy" letter to fill out the last pair of letters.

Enciphering step 03: Convert each plaintext pair $p1p2$ into a column vector **P.**
To encrypt the message we multiply our plaintext matrix P by our transformation matrix **A** to form the product

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

This was the encoding procedure.
Now we decipher our enciphered message.

Deciphering step 01: Now we group the successive cipher text letters into pairs and convert each cipher text pair $c1c2$ into a column vector **C**. Then form 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 deciphered message.

AN EXAMPLE OF THESE SYSTEM
If anybody wants to send a plaintext message to the user such as

ARREST NOW

To encrypt the message "ARREST NOW" First translates each letter into its digital equivalent using the substitution mention in Hill cipher cryptosystem. This yields the plain text number
M=01181805192027141523
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

$56 \equiv 02(\text{mod}27)$

$51 \equiv 24(\text{mod}27)$

$98 \equiv 17(\text{mod}27)$

$96 \equiv 15(\text{mod}27)$

$99 \equiv 18(\text{mod}27)$

$75 \equiv 21(\text{mod}27)$

$74 \equiv 20(\text{mod}27)$

$137 \equiv 02(\text{mod}27)$

$137 \equiv 02(\text{mod}27)$

$137 \equiv 02(\text{mod}27)$

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

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 more security of the system we will encrypt the cypher text E into another cipher text N with the help of Euler's phi function. For this case we first select primes P=11, Q=17 of an unrealistic small size. In practice P and Q would large enough so that the factorization of the nonsecret n=PQ is not feasible. Our enciphering modulus is $n = 11.17 = 187$ and $Q(n) = 10.16 = 161 = 23.7$

Suppose the enciphering exponent is chosen to be k=23, then the recovery component the unique integer j satisfying the congruence $kj \equiv 1(\text{mod}Q(n))$ j=7. To encrypt N we need every block of N to be an integer less than 187. Now for the first block the calculation is

$(02) = -185(\text{mod}187)$

$(02)^4 = 33489(\text{mod}187)$

$(02)^4 = 16(\text{mod}187)$

$(02)^8 = 256(\text{mod}187)$

$(02)^8 = 69(\text{mod}187)$

$(02)^{16} = 4761(\text{mod}187)$

$(02)^{16} = 86(\text{mod}187)$

$(02)^{23} = (02)^{16} \times (02)^4 \times (02)^2 \times (02)(\text{mod}187)$

$(02)^{23} = 86 \times 16 \times (-183) \times (-185)(\text{mod}187)$

$(02)^{23} = 46584480(\text{mod}187)$

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

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

Now for the entity (21)

$(21)^2 = 67(\text{mod}187)$

$(21)^4 = 4489(\text{mod}187)$

$(21)^4 = 1(\text{mod}187)$

$(21)^8 = 1(\text{mod}187)$

$(21)^{16} = 1(\text{mod}187)$

$(21)^{23} = 21^{16} \times 21^4 \times 21^2 \times 21(\text{mod}187)$

$(21)^{23} = 1 \times 1 \times 67 \times 21(\text{mod}187)$

$(21)^{23} = 1407(\text{mod}187)$

$(21)^{23} = 98(\text{mod}187)$

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

Now similarly we have $(24)^{23} = 63(\text{mod } 187)$

And $(20)^{23} = 113(\text{mod } 187)$

And $(17)^{23} = 51(\text{mod } 187)$

And $(02)^{23} = 162(\text{mod } 187)$

And $(15)^{23} = 42(\text{mod } 187)$

And $(02)^{23} = 162(\text{mod } 187)$

And $(18)^{23} = 35(\text{mod } 187)$

And $(02)^{23} = 162(\text{mod } 187)$

Now the total encrypt message is:

162 98 63 113 51 162 42 162 35 162

Now we will recovery the message by using recovery component $j = 7$. We can recover the original text

$(162)^2 = 64(\text{mod}187)$

$(162)^4 = 4096(\text{mod}187)$

$(162)^4 = 169(\text{mod}187)$

$(162)^7 = 169 \times 64 \times 162(\text{mod}187)$

$(162)^7 = 1752192(\text{mod}187)$

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

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

Now for the entity (98)

Now similarly we have $(63)^7 = 24(\text{mod } 187)$

And $(113)^7 = 20(\text{mod } 187)$

And $(51)^7 = 17(\text{mod } 187)$

And $(162)^7 = 02(\text{mod } 187)$

And $(42)^7 = 15(\text{mod } 187)$

And $(162)^7 = 02 (\text{mod } 187)$

And $(35)^7 = 18 (\text{mod } 187)$

And $(162)^7 = 02 (\text{mod } 187)$

Now the decrypted message after applying 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 recover the original 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 using 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 decrypt message is
M= (01 18 18 05 19 20 27 14 15 23)
Now to recover the message translate each number of M into its digital equivalent using the substitution mentioned earlier this yields the plaintext

V. Conclusion

The security of our combined Hill cipher and RSA cryptography system is based on several facts: First is that we use a key matrix A, which is only known to first party and second party. The second is that knowing n and k do not allow you to determine the value of j. Third since you know n it will be relatively easy to find j if you just factor n to determine the primes p and however no one has found a time effective way to factor n when n only two very large prime factors and fourth the combination of these two cryptosystem gives a security where the plaintext is quite impossible to find out for the third parties.

References

Books:

[1] M.R Adhikari & Avishek Adhikari, Introduction to linear algebra with application to basic cryptography (New Delhi 2007):)

[2] Niven IHerbert S.Z Hugh L.M An introduction to the theory of numbers (5th edition Willy and Sons 1980)

[3] Burton M.D Elementary Number theory (2nd edition New Delhi W.M.C Brown publishers 1989)

Chapters in Books:

[4] L.M Adleman, R.l Rivest, A shamir A method for obtaining digital signature and public key cryptosystems (Comm. Of ACM21(1978)120- 126)

Thesis:

[5] W, Diffine M.E Hellman-New direction in cryotography(IEEE Trans. Information Thesis 22(1976)) volume 644-654

Books:

[6] H. Cohen A course in computational Algebric Number theory (Springer 1994)

[7] N.Koblitz Algebraic aspects of Cryptography (Springer 1998)

Mohiuddin Ahmed "A Perfect Implantation of Euler's Phi-Function in Hill Cipher Cryptosystem. IOSR Journal of Mathematics (IOSR-JM) 14.2 (2018) PP: 68-73.