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

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 Cipher cryptosystem proposed by Lester S. Hill for encrypet 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 Caesar 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’s phi function, RSA cryptosystem, Matrix

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 1080s 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 function.Secret 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 \( ax \equiv b \pmod{n} \) is called a linear congruence and by a solution of this equation we mean an integer \( x_0 \) for which \( ax_0 \equiv b \pmod{n} \) by definition \( ax_0 = b \pmod{n} \) 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
A Perfect Implantation of Euler’s Phi-Function in Hill Cipher Cryptosystems

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

\[ n \in \mathbb{Z}, e \in \mathbb{N} \]

\[ e = c \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

\[ e = 2 \]

IV. Hill Cipher Cryptosystem

Let \( n \) be a product of two distinct primes \( p \) and \( q \). Let us define \( K = (n, p, q, e, d) : ed = l (\text{mod} \phi(n)) \) 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 \( e_1(x) = x^e \pmod{n} \) and \( d_1(y) = y^d \pmod{n} \) where \( x, y \in \mathbb{Z}_n \). The values \( n \) and \( e \) are public and the values \( p, q \) and \( d \) are used as public key.

**Enciphering step 01:** Choose a \( 2 \times 2 \) 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 \( plp2 \) 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 \( clc2 \) 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 \( 2 \times 5 \) matrix \( P \) for the values of \( M \)

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

Let a \( 2 \times 2 \) matrix \( A \) as

\[ A = \begin{bmatrix} 2 & 3 \\
3 & 4 \end{bmatrix} \]

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

Now the encoding matrix \( E \) is

DOI: 10.9790/5728-1402026873 www.iosrjournals.org 69 | Page
E = AP = \[
\begin{bmatrix}
2 & 3 \\
3 & 4
\end{bmatrix}
\begin{bmatrix}
01 & 18 & 19 & 27 & 15 \\
18 & 05 & 20 & 14 & 23
\end{bmatrix}
\]
= \[
\begin{bmatrix}
2.1 + 3.18 & 2.18 + 3.5 & 2.19 + 3.2 & 2.27 + 3.19 & 2.15 + 3.23 \\
3.1 + 4.8 & 3.18 + 4.5 & 3.19 + 4.2 & 3.27 + 4.14 & 3.15 + 4.23
\end{bmatrix}
\]
= \[
\begin{bmatrix}
56 & 51 & 98 & 96 & 99 \\
75 & 74 & 137 & 137 & 137
\end{bmatrix}
\]
Now we use congruence we have
56 ≡ 02(mod27)
51 ≡ 24(mod27)
98 ≡ 17(mod27)
96 ≡ 15(mod27)
99 ≡ 18(mod27)
75 ≡ 21(mod27)
74 ≡ 20(mod27)
137 ≡ 02(mod27)
137 ≡ 02(mod27)
137 ≡ 02(mod27)
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 \ 21 \ 24 \ 20 \ 17 \ 02 \ 15 \ 02 \ 18 \ 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
\((02) = -185(\text{mod}187)\)
\((02)^4 = 33489(\text{mod}187)\)
\((02)^4 = 16(\text{mod}187)\)
\((02)^8 = 256(\text{mod}187)\)
\((02)^8 = 69(\text{mod}187)\)
\((02)^{16} = 4761(\text{mod}187)\)
\((02)^{16} = 86(\text{mod}187)\)
\((02)^{23} = (02)^{16} \times (02)^{4} \times (02)^{2} \times (02)(\text{mod}187)\)
\((02)^{23} = 86 \times 16 \times (-183) \times (-185)(\text{mod}187)\)
\((02)^{23} = 46584480(\text{mod}187)\)
\((02)^{23} = 162(\text{mod}187)\)
\[(02)^{23} = 162 \pmod{187}\]

Now for the entity (21)

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

\[\therefore (21)^{23} = 98 \pmod{187}\]

Now similarly we have

\[(24)^{23} = 63 \pmod{187}\]
And
\[(20)^{23} = 113 \pmod{187}\]
And
\[(17)^{23} = 51 \pmod{187}\]
And
\[(02)^{23} = 162 \pmod{187}\]
And
\[(15)^{23} = 42 \pmod{187}\]
And
\[(02)^{23} = 162 \pmod{187}\]
And
\[(18)^{23} = 35 \pmod{187}\]
And
\[(02)^{23} = 162 \pmod{187}\]

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

\[(162)^2 = 64 \pmod{187}\]
\[(162)^4 = 4096 \pmod{187}\]
\[(162)^8 = 169 \pmod{187}\]
\[(162)^7 = 169 \times 64 \times 162 \pmod{187}\]
\[(162)^7 = 1752192 \pmod{187}\]
\[(162)^7 = 02 \pmod{187}\]
\[\therefore (162)^7 = 02 \pmod{187}\]

Now for the entity (98)

Now similarly we have

\[(63)^7 = 24 \pmod{187}\]
And
\[(113)^7 = 20 \pmod{187}\]
And
\[(51)^7 = 17 \pmod{187}\]
And
\[(162)^7 = 02 \pmod{187}\]
And
\[(42)^7 = 15 \pmod{187}\]
A Perfect Implantation of Euler’s Phi-Function in Hill Cipher Cryptosystems

And  
\[(162)^7 \equiv 02 \pmod{187}\]
And  
\[(35)^7 \equiv 18 \pmod{187}\]
And  
\[(162)^7 \equiv 02 \pmod{187}\]

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 \(A^{-1}\)

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

\[D = A^{-1}E = \begin{bmatrix} -4 & 3 \\ 3 & -2 \end{bmatrix} \begin{bmatrix} 02 & 24 & 17 & 15 & 18 \\ 21 & 20 & 02 & 02 & 02 \end{bmatrix} = \begin{bmatrix} -4\times2+3\times21 & -4\times24+3\times20 & -4\times17+3\times2 & -4\times15+3\times2 & -4\times18+3\times2 \\ 3\times2+(-2)\times21 & 3\times24+(-2)\times20 & 3\times17+(-2)\times2 & 3\times15+(-2)\times2 & 3\times18+(-2)\times2 \end{bmatrix} = \begin{bmatrix} 55 & -36 & -62 & -54 & -66 \\ -36 & 32 & 47 & 41 & 50 \end{bmatrix}\]

Now we using congruence:

\[55 \equiv 01 \pmod{27}\]
\[-36 \equiv 18 \pmod{27}\]
\[-62 \equiv 19 \pmod{27}\]
\[-54 \equiv 27 \pmod{27}\]
\[-66 \equiv 15 \pmod{27}\]
\[-36 \equiv 18 \pmod{27}\]
\[32 \equiv 05 \pmod{27}\]
\[47 \equiv 20 \pmod{27}\]
\[41 \equiv 14 \pmod{27}\]
\[32 \equiv 05 \pmod{27}\]
\[47 \equiv 20 \pmod{27}\]
\[41 \equiv 14 \pmod{27}\]
\[50 \equiv 23 \pmod{27}\]

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

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:

Chapters in Books:

Thesis:

Books: