ISSN No:-2456-2165

Formulation of an Improved Hybrid Cipher System

[1]AhmadRufa'i
Department of Mathematics
Sokoto State University

[2]Anas Tukur Balarabe
Department of Computer Sci.
Sokoto State University

[3]Isah Muazu
Department of Mathematics
Sokoto State University

[4]Muhammad Sirajo
Department of Chemistry
Sokoto State University

Abstract:- Data security has turned-out to be a very important aspect in recent years due to drastic progress in the use of internet, data is frequently transferred from one place to another especially with the use of internet in recent years. Sensitive information can be shared through internet but this information sharing is vulnerable to certain attacks. Cryptography was introduced to solve this problem. Cryptography is the art of achieving security by encoding the plaintext message to cipher text. Many ciphers have been developed to provide data security, such as Caesar cipher, Hill cipher, Vigenere cipher, Rail fencing cipher, Playfair cipher and so on, but all the conventional encryption techniques have proved to be weak and amenable to attack even by use of brute force and traditional cryptanalysis. In this work three of those existed ciphers will be considered (i.e. Caesar cipher, Hill cipher and RSA Algorithm) and their weaknesses will be proved. The three ciphers will be measured as functions (bijection) and idea of composition of functions will be used to combine and compose the functions so as to provide an improved encryption technique (hybrid cipher system) by combining RSA Algorithm together with Shifting and Hill ciphers.

I. INTRODUCTION

In recent time, the internet has placed itself to providing essential communication between millions of people and is being increasingly used as a tool for paperless transaction in business, private or governmental offices by means of e-mail messages, e-cash transactions and so on. Due to this development there is a great need for transmission of data through internet in various businesses, private and governmental sectors. Part of this information is sensitive and confidential like banking transactions, credit information, governmental information and so on.

The confidentiality, authentication and integrity of such important information need to be maintained and protected. To protect this type of sensitive information from an unauthorized access, experts have come up with solutions embodied in the concept of 'cryptography'. This is the art of achieving security by encrypting the data into an unreadable form and later on, decoding it into readable form for specific purposes.

The process of encryption and decryption of data is shown below:

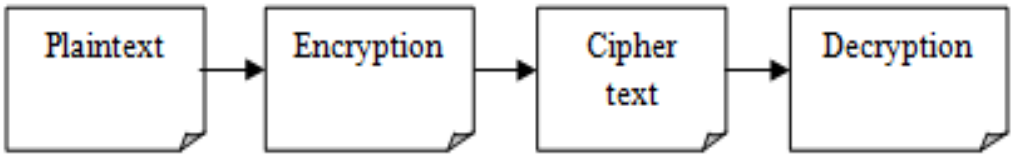

Fig.1.1.1: Encryption and Decryption, (Stallings, 2010).

By using cryptography many goals can be achieved. These goals can be either all achievable in some applications at the same time or only one of them being achieved. The goals of cryptography include:

(i) Confidentiality: this is the most important goal which ensures that nobody can understand the received message except the one who has the deciphering key.
(ii) Authentication: this is the process of providing the identity that assures communicating entity is the one that it claimed to be, which applies to both entities and information itself.
(iii) Data Integrity: this is a service which addresses the unauthorized alteration of data
(iv) Non-Repudiation: it is a mechanism used to prove that the sender really sent message and message was received by the specified party, so the recipient cannot claim the message was not sent.
(v) Access control: it is the process of preventing an unauthorized use of resources. This goal controls who can access the resources, (AbuTaha *e tal;* 2011).

II. PROBLEM STATEMENT

In today's world it is impossible to imagine without web or internet. This modern era is dominated by paperless transaction in business, private or governmental offices by means of e-mail messages and so on. Due to this, there is a great need of transmission of data through internet, the confidentiality and integrity of such important information should be maintained and protected. Many ciphers have been developed to protect the confidentiality of such information, but almost all the conventional ciphers are proved to be weak and amenable to attack even by the use of brute force and traditional cryptanalysis. Hence there is a need to develop stronger and more secure ciphers that will

overcome the shortcomings and weaknesses of the conventional ciphers, either by modification, combination and so on. In this research, we propose a modification and combination of some ciphers.

III. AIM AND OBJECTIVES

The main aim of this research is to come up with an improved cipher that provides better security in data transmission compared to combined ciphers method. This aim can be achieved through the following objectives:

1. To analyze the weaknesses of the combined ciphers if operated to work independently.
2. To come up with improved cryptographic technique by combining the three ciphers, which will overcome the weakness of the ciphers if operated to work independently.
3. To use the proposed system to encrypt and decrypt a message.
4. To analyze the improved cipher.

IV. LITERATURE REVIEW

Previously, there were several attempts by researchers to improve the conventional ciphers by means of modification, implementation or combination.

Krishna and Vinaga (2007), modified a Hill cipher for more secure and stronger encryption of data. In the work an attempt was made to provide randomization to the output of Hill cipher to make it free from chosen plaintext and ciphertext attacks. By generating the initial ciphertext from plaintext using Hill cipher; considering a session key using circulant matrix and converting it into matrix match the diversion of quandary vector; generating basins by multiplying quandary vector with circulant matrix and considering mod n; mapping basins on the output of Hill cipher to generate multiple ciphertext for one plaintext.

Rizvi *et al.* (2010), in their study combined private and public encryption techniques that offers numerous secured services to both students and faculty.

Ajit *et al.* (2012), in their work combined two techniques of cryptosystem i.e. Caesar and rail fencing ciphers to enhance security. “The work presented a perspective on combination of techniques, substitution and transposition. Combining the two ciphers can eliminate their fundamental weaknesses and produce a ciphertext that is hard to crack.

Srikantaswamy and phaneendra (2012), in their work, proposed a method to improve Caesar cipher with random number of encryption technique. The cipher has been expanded to include alphabet, numbers and symbols. In the paper, a method has been proposed to improve Caesar cipher with random number generation technique for key generation operations. The method is resistant against brute force attack with 93! combination of keys, for Caesar encryption.

Harinandam and Soumen (2012), in their paper improve the conventional Playfair cipher. In their work they propose some ways for removal of the traditional Playfair drawbacks. Such as multiple array of structure to store information about the spaces and to store the information about whether an ‘X’ has appeared in the alphabet matrix, password mechanism to increase the level of security, extending the key table from 5×5 matrix to 16×16 matrix.

Sanjay and Uptal (2012), in their study proposed a rectangular matrix having 10 columns and 9 rows to overcome the drawbacks of 5 $\times5$ playfair and which can support almost all the printable characters including spaces.

Zulkarnaini and Mohammed (2013), combined RSA and Elgamal cryptosystem for improved cryptosystem. The work is a combination of RSA and ElGamal cryptosystems based on their problems. These algorithms give additional difficulties because of the employment of DLF and IFP in the proposed algorihm.

Sreenivasulu (2013), dev eloped a new model of Hill cipher using non-quadratic Residues which modified the conventional Hill cipher for improved cipher. The model is an improvement to the security of Hill cipher by using Non-quadratic residues of a prime number $p \geq 53.$ In Hill cipher a plaintext is encrypted using a fixed value 26.

Gupta and Kumar (2010), came up with new concept in modern cryptography where original data is encrypted many times with strong encryption algorithm at each phase. In the work original data is encrypted many times with different encryption keys. The encryption algorithm is:

$C = EK_3(DK_2(EK_1(P)))$ for encryption and,

$P = DK_1(EK_2(DK_3(C)))$ for decryption.

i.e. decrypt with K_3, encrypt with K_2 then decrypt with K_1.

Aflab*et al.* (2013), modified the normal 5×5 matrix playfair cipher into 7×4 Matrix. The problem in the 5 by 5 matrix arises when either i or j or both appear in the keyword. Also when the plaintext words consist of odd number of characters, a spare letter ‘x’ is padded with the word to complete the pair, but in the decryption process this ‘x’ is ignored. This creates confusion because ‘x’ is a valid character and it can be the part of plaintext.

Chalapathi (2013), imported innovative advancement to the popular Caesar cipher which perfectly eliminates it constitutional weakness, where spaces in between words are ignored and encrypted characters are scrambled.

Rajan and Shantanu (2013), modified the normal RSA model for secured file transmission. The modified algorithm (RSA and MREA) has many important parameters affecting its level of security and speed, by increasing the modulus

length. This also increases the length of private key and hence difficult to defeat the key. They introduced another parameter which is modular multiplicative inverse μ where μ is a new factor of private key, which makes it more difficult to choose μ by trying all possible private keys(brute force attack), hence the security also increases as well as difficulty in detecting the private key.

Kashish and Supriya (2013), expanded Caesar cipher so as to include alpha numeric and symbols since original Caesar cipher was restricted only for alphabets. The key used has been derived using a key matrix trace value restricted to modulo 94. They made an effort to incorporate modern cipher properties to classical cipher.

Anupama (2013), proposed an algorithm which is the combination of both the transposition and substitution method and which provides much more secure cipher.

Ajin and Manjala (2013), amalgamated many ciphers to eliminate repetitive terms so that hackers do not hava a room for analyzing. They proposed an algorithm used for encryption, the encryption algorithm which converts the original message mathematically based on the key to create encrypted message. The whole system architecture depends on three models which are:

1. Modified Caesar cipher,
2. NJJSAA and function encryption,
3. Bit rotation and Reversal method.

Krishma and Chanhan (2014), proposed modified version of Playfair cipher with random generation methods combining with vegenere cipher.

YashPalsingh and Mane (2014), proposed an improved cryptographic technique using double encryption. They combined Caesar cipher with Hill cipher to make the encryption technique more secure and stronger. The idea used in the work is to encrypt the plaintext message into two main phases.

Phase I: improved substitution cipher
Phase II: Hill cipher technique.

V. CRYPTANALYSIS OF THE COMBINED CIPHERS

(i) Ceasar Cipher

Suppose we intercepted the above ciphertext and we suspected that it had been encrypted with shifting cipher.

For shift 1:

Ciphertext	M	J	Q	Q	T	B	T	W	Q	I
Plaintext	L	I	P	P	S	A	S	V	P	H

It is clear that ‘1’ is not the key and we may continue with ‘2’ and so on. With k = 5, we finally get an intelligible result, using Table 3.1.3.

Ciphertext	I	F	M	M	P	X	P	S	M	E
Plaintext	H	E	L	L	O	W	O	R	L	D

(ii) Hill Cipher

Since Hill cipher is linear; we only need to find two bigram correspondences to determine the key matrix. For example, if we knew that 'th' was encrypted to 'gk' and 'er' was encrypted to 'bd', we could solve a set of simultaneous equations and find the encryption key matrix. We will capitalize on this fact to break the cipher. Suppose we know that ‘HE’ is encrypted to ‘SL’ and ‘LL’ is encrypted to ‘HZ’ we can then set up an equation (replacing letters with their corresponding numbers).

$$\text{i.e. } A\begin{pmatrix}18\\11\end{pmatrix}=\begin{pmatrix}7\\4\end{pmatrix}\bmod 26,\ldots,(i)$$

$$A\begin{pmatrix}7\\25\end{pmatrix}=\begin{pmatrix}11\\11\end{pmatrix}\bmod 26,\ldots,(ii)$$

Combining the two equations to obtain A we have,

$$A\begin{pmatrix}18&7\\11&25\end{pmatrix}=\begin{pmatrix}7&11\\4&11\end{pmatrix}\bmod 26$$

$$\text{Thus, } A=\begin{pmatrix}7&11\\4&11\end{pmatrix}\left[\begin{pmatrix}18&7\\11&25\end{pmatrix}^{-1}\right] \text{ but}$$

$$A^{-1}=(\det(A))^{-1}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}\bmod 26$$

$$\text{Therefore to find } \left[\begin{pmatrix}18&7\\11&25\end{pmatrix}^{-1}\right] \text{ we've,}$$

det(A) = 18 * 25 – 11 * 7 = 373, so the modular inverse of 373 is 3 , since

373*3 = 1119 and 1119 = 26 * 43 + 1 (i.e. 1119 mod26 = 1).

$$=3\begin{vmatrix}25&-7\\-11&18\end{vmatrix}\bmod 26=\begin{vmatrix}75&-21\\-33&54\end{vmatrix}\bmod 26=\begin{pmatrix}23&5\\19&2\end{pmatrix}$$

ISSN No:-2456-2165

$$\therefore \quad A=\begin{pmatrix}7 & 11\\ 4 & 11\end{pmatrix}\begin{pmatrix}23 & 5\\ 19 & 2\end{pmatrix}\bmod 26=\begin{pmatrix}161+209 & 35+22\\ 92+209 & 20+22\end{pmatrix}\bmod 26=\begin{pmatrix}370 & 57\\ 301 & 42\end{pmatrix}\bmod 26$$

$=\begin{pmatrix}6 & 5\\ 15 & 16\end{pmatrix}$ Therefore the decryption matrix is $A=\begin{pmatrix}6 & 5\\ 15 & 16\end{pmatrix}$ as required.

(iii) RSA Algorithms

There are several approaches, all equivalent in effort to factoring the product of two primes. We can identify three approaches to attacking RSA mathematically.

1. Factor *n* into its two prime factors. This enables calculation of $\varphi(n) = (p - 1) \times (q - 1)$, which in turn enables determination of $d = e^{-1} \pmod{\varphi(n)}$.

2. Determine $\varphi(n)$ directly, without first determining *p* and *q*. Again, this enables determination of $d = e^{-1} \pmod{\varphi(n)}$.

3. Determine *d* directly, without first determining $\varphi(n)$.

VI. PROPOSED ALGORITHM

Simple transposition and substitution ciphers individually do not provide a very high level of security; however by combining these transformations, it is possible to obtain strong ciphers. In cryptography, by encrypting a message twice with some block ciphers, either with the same or by using two different keys, then we would expect the resultant encryption to be stronger in all but some exceptional circumstances. And by using three encryptions we would expect to achieve a yet greater level of security. For instance, the use of double encryption does not provide the expected increase in security when compared with the increased implementation requirements, and it cannot be recommended as a good alternative. Instead triple-encryption is the point at which multiple encryption gives substantial improvements in security (Himanshu and Vinoid, 2013).

This algorithm will combine three encryption techniques of cryptosystem i.e. RSA model, Hill cipher and shifting cipher. Each cipher will be considered as a function. Suppose $f: A \to B, g: B \to C, h: C \to D$ be Hill cipher, shifting cipher and RSA algorithm respectively, the three functions can be composed as $(fogoh)p = f(g(h(p)))$.

If $f(p) = pk \mod 26$, $g(p) = (p+3) \bmod 26$ $h(p) = p^e \bmod 26$, where k and e are known. Given $p = owor$, then we can compose the three functions .

Thus, the proposed algorithm will consider these ciphers as functions and combine them by constructing encryption and decryption algorithms. The proposed algorithm for encryption and decryption are given in the next chapter stepwise, for all $P \ni Z_N$. Where N is the size or number of characters.

6.1 Encryption algorithm

Step 1: choose a key $k_1 = \begin{pmatrix}\lambda_{11} & \lambda_{12} \dots & \lambda_{1m}\\ \lambda_{21} & \lambda_{22} \dots & \lambda_{2m}\\ \vdots & \vdots & \vdots\\ \lambda_{m1} & \lambda_{m2} \dots & \lambda_{mm}\end{pmatrix}$ where k_1 is any $m \times m$ invertible matrix and $\lambda_{11}, \lambda_{mm}$ are prime numbers.

Step 2: split the plaintext P, into m-grams aligned as column vectors and replace with their numerical values. i.e.

$$P=\begin{pmatrix}p_1\\ .\\ .\\ .\\ p_m\end{pmatrix},\begin{pmatrix}p_{m+1}\\ .\\ .\\ .\\ p_{m+m}\end{pmatrix},\dots,\begin{pmatrix}p_{m+m+\dots+1}\\ .\\ .\\ .\\ p_{m+m+\dots+m}\end{pmatrix}$$

Step 3: compute $C_1 = k_1 P \bmod N =$

$$\begin{pmatrix}a_1\\ .\\ .\\ .\\ a_m\end{pmatrix},\begin{pmatrix}a_{m+1}\\ .\\ .\\ .\\ a_{m+m}\end{pmatrix},\dots,\begin{pmatrix}a_{m+m+\dots+1}\\ .\\ .\\ .\\ a_{m+m+\dots+m}\end{pmatrix}$$

And write $C_1 = (a_1, \dots, a_{m+\dots+m})$

Step 4: compute $C_2 = (C_1 + k_2) \bmod N = (b_1, \dots, b_{m+\dots+m})$ where $k_2 =$ number of entries in k_1.

Step 5: choose $n = \lambda_{11}\lambda_{mm}$ and compute $\varphi(n) = (\lambda_{11} - 1)(\lambda_{mm} - 1)$

Step 6: select $e: \gcd(e, \varphi(n)) = 1$ and establish $p_k = (e, n)$

Step 7: Compute $C_3 = C_2^e \bmod n = (d_1,...,d_{m+...+m})$

And write $C_3 = (d_1 d_2 ....d_{m+...+m})$ (i.e. the ciphertext, C).

6.2 Decryption algorithm

Step 1: Read C_3 (i.e. ciphertext) and split into number of digits of n,

i.e. $C_3 = (d_1,...,d_{m+....+m})$ and compute $P_2 = C_3^e \bmod n = (b_1,...,b_{m+....+m})$.

Step 2: Compute $P_1 = (P_2 - k_2) \bmod N = (a_1,...,a_{m+.....+m})$ where $k_2 =$ number of entries in k_1.

Step 3: Split P_1 into m-grams and align as column vectors

$$P_1 = \begin{pmatrix} a_1 \\ . \\ . \\ . \\ a_m \end{pmatrix}, \begin{pmatrix} a_{m+1} \\ . \\ . \\ . \\ a_{m+m} \end{pmatrix}, ..., \begin{pmatrix} a_{m+m+.....+1} \\ . \\ . \\ . \\ a_{m+m+.....+m} \end{pmatrix}$$

Step 4: Compute $P = P_1 k_1^{-1} \bmod N =$

$$\begin{pmatrix} p_1 \\ . \\ . \\ . \\ p_m \end{pmatrix}, \begin{pmatrix} p_{m+1} \\ . \\ . \\ . \\ p_{m+m} \end{pmatrix}, ..., \begin{pmatrix} p_{m+m+.....+1} \\ . \\ . \\ . \\ p_{m+m+.....+m} \end{pmatrix}$$

Step 5: write P as $P = (p_1....p_{m+....+m})$

VII. ENCRYPTION AND DECRYPTION WITH THE IMPROVED ALGORITHM

Suppose we want to encrypt the message 'HELLO WORLD'.

7.1 Encryption

Step 1: let $k_1 = \begin{pmatrix} 13 & 5 \\ 4 & 3 \end{pmatrix}$

Step 2: $P =$ HELLOWORLD (ignoring space)

$$\Rightarrow P = \begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ L \end{pmatrix}, \begin{pmatrix} O \\ W \end{pmatrix}, \begin{pmatrix} O \\ R \end{pmatrix}, \begin{pmatrix} L \\ D \end{pmatrix}$$

Thus, $\begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix}$ $\begin{pmatrix} L \\ L \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \end{pmatrix}$ $\begin{pmatrix} O \\ W \end{pmatrix} = \begin{pmatrix} 14 \\ 22 \end{pmatrix}$

$\begin{pmatrix} O \\ R \end{pmatrix} = \begin{pmatrix} 14 \\ 27 \end{pmatrix}$ $\begin{pmatrix} L \\ D \end{pmatrix} = \begin{pmatrix} 11 \\ 3 \end{pmatrix}$

Step 3: $C_1 = \begin{pmatrix} 13 & 5 \\ 4 & 3 \end{pmatrix} P \bmod 26$

$$\Rightarrow \begin{pmatrix} 13 & 5 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} \text{mod26} = \begin{pmatrix} 91+20 \\ 28+12 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 14 \end{pmatrix}$$

$$\begin{pmatrix} 13 & 5 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 11 \\ 11 \end{pmatrix} \text{mod26} = \begin{pmatrix} 143+55 \\ 44+33 \end{pmatrix} \bmod 26 = \begin{pmatrix} 16 \\ 25 \end{pmatrix}$$

$$\begin{pmatrix} 13 & 5 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 14 \\ 22 \end{pmatrix} \text{mod26} = \begin{pmatrix} 182+110 \\ 56+66 \end{pmatrix} \bmod 26 = \begin{pmatrix} 6 \\ 18 \end{pmatrix}$$

$$\begin{pmatrix} 13 & 5 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \text{mod26} = \begin{pmatrix} 182+85 \\ 56+51 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 3 \end{pmatrix}$$

$$\begin{pmatrix} 13 & 5 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 11 \\ 3 \end{pmatrix} \text{mod26} = \begin{pmatrix} 143+15 \\ 44+9 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

Therefore, $C_1 =$ (7, 14, 16, 25, 6, 18, 7, 3, 2, 1)

Step 4: $C_2 = (C_1 + 4) \bmod 26$

(7 + 4) mod26 = 03
(14 + 4) mod26 = 19
(16 + 4) mod26 = 24
(25 + 4) mod26 = 11
(6 + 4) mod26 = 18
(18 + 4) mod26 = 10
(7 + 4) mod26 = 03
(3 + 4) mod26 = 00
(2 + 4) mod26 = 00
(1 + 4) mod26 = 21

Thus, $C_2 =$ (11, 18, 20, 03, 10, 22, 11, 07, 06, 05)

Step 5: $n = \lambda_{11}\lambda_{22} = 13*3 = 39$

$\phi(n) = (13-1)(3-1) = 12*2 = 24$

$\varphi(n) = 24$

Step 6: choose $e = 5$ since gcd (5, 24) = 1, thus $p_k = (5,39)$

Step 7: $C_3 = C_2^5 \bmod 39$

i.e. $11^5 \bmod 39 = 20$

$18^5 \bmod 39 = 18$

$20^5 \bmod 39 = 11$

$03^5 \bmod 39 = 09$

$10^5 \bmod 39 = 04$

$22^5 \bmod 39 = 16$

$11^5 \bmod 39 = 20$

$07^5 \bmod 39 = 37$

$06^5 \bmod 39 = 15$

$05^5 \bmod 39 = 05$

Therefore, $C_3 = (20181109041620371505)$ i.e the cipher text.

7.2 Decryption

Step 1: $C_3 =$ (20181109041620371505)

$$P_2 = C_3^5 \bmod 39$$

Thus, $20^5 \bmod 39 = 11$

$18^5 \bmod 39 = 18$

$11^5 \bmod 39 = 20$

$09^5 \bmod 39 = 03$

$04^5 \bmod 39 = 10$

$16^5 \bmod 39 = 22$

$20^5 \bmod 39 = 11$

$37^5 \bmod 39 = 07$

$15^5 \bmod 39 = 06$

$05^5 \bmod 39 = 05$

Therefore, $P_2 = (11, 18, 20, 03, 10, 22, 11, 07, 06, 05)$

Step 2: $P_1 = (P_2 - 4) \bmod 26$

i.e. (11 - 4) mod26 = 07
(18 - 4) mod26 = 14
(20 - 4) mod26 = 16
(03 - 4) mod26 = 25
(10 - 4) mod26 = 06
(22 - 4) mod26 = 18
(11 - 4) mod26 = 07
(07 - 4) mod26 = 03
(06 - 4) mod26 = 02
(05 - 4) mod26 = 01

Thus, $P_1 = (07,14,16,25,06,18,07,03,02,01)$

Step 3: $P_1 = \begin{pmatrix}07\\14\end{pmatrix},\begin{pmatrix}16\\25\end{pmatrix},\begin{pmatrix}06\\18\end{pmatrix},\begin{pmatrix}07\\03\end{pmatrix},\begin{pmatrix}02\\01\end{pmatrix}$

Step 4: $P = P_1 k_1^{-1} \bmod 26$,

where $k_1^{-1} = \det(k_1)^{-1}\begin{pmatrix}\lambda_{22} & -\lambda_{12}\\ -\lambda_{21} & \lambda_{11}\end{pmatrix} \bmod 26$

Given $k_1 = \begin{pmatrix}13 & 5\\ 4 & 3\end{pmatrix}$, $\det(k_1) = 39 - 20 = 19$ and the modular inverse of 19 is 11. Since 11*19 = 209 = (8 *26) +1.

Thus,

$$k_1^{-1} = 11\begin{vmatrix}3 & -5\\ -4 & 13\end{vmatrix} \bmod 26 = \begin{vmatrix}33 & -55\\ -44 & 143\end{vmatrix} \bmod 26 = \begin{pmatrix}7 & 23\\ 8 & 13\end{pmatrix} \bmod 26$$

$$\Rightarrow \quad k_1^{-1} = \begin{pmatrix}7 & 23\\ 8 & 13\end{pmatrix}$$

Therefore, $P = \begin{pmatrix}7 & 23\\ 8 & 13\end{pmatrix} P_1 \bmod 26$

i.e

$$\begin{pmatrix}7 & 23\\ 8 & 13\end{pmatrix}\begin{pmatrix}07\\14\end{pmatrix} \bmod 26 = \begin{pmatrix}49+322\\56+182\end{pmatrix} \bmod 26 = \begin{pmatrix}07\\04\end{pmatrix}$$

$$\begin{pmatrix}7 & 23\\ 8 & 13\end{pmatrix}\begin{pmatrix}16\\25\end{pmatrix} \bmod 26 = \begin{pmatrix}112+575\\128+325\end{pmatrix} \bmod 26 = \begin{pmatrix}11\\11\end{pmatrix}$$

$$\begin{pmatrix}7 & 23\\ 8 & 13\end{pmatrix}\begin{pmatrix}06\\18\end{pmatrix} \bmod 26 = \begin{pmatrix}42+414\\48+234\end{pmatrix} \bmod 26 = \begin{pmatrix}14\\22\end{pmatrix}$$

$$\begin{pmatrix}7 & 23\\ 8 & 13\end{pmatrix}\begin{pmatrix}07\\03\end{pmatrix} \bmod 26 = \begin{pmatrix}49+69\\56+39\end{pmatrix} \bmod 26 = \begin{pmatrix}14\\17\end{pmatrix}$$

$$\begin{pmatrix}7 & 23\\ 8 & 13\end{pmatrix}\begin{pmatrix}02\\01\end{pmatrix} \bmod 26 = \begin{pmatrix}14+23\\16+13\end{pmatrix} \bmod 26 = \begin{pmatrix}11\\03\end{pmatrix}$$

Step 5: $P =$ (07 04 1111 14 22 14 17 11 03)

Thus, plaintext is HELLOWORLD

VIII. CONCLUSION

The improved method is a combination of three conventional techniques of cryptosystem (i.e. RSA model, Hill and shifting ciphers) which provides more secured and stronger cipher. The improved system results from the merger of these three algorithms and so it becoming more complicated than each algorithm operated to work independently. The advantage of the improved system is that, it provides better security because even if some component ciphers are broken or some of the secret keys are recognized, the confidentiality of the original data can still be maintained.

REFERENCES

[1]. Ajit, S., Nandal, A. and Malik, S. (2012). Implementation of Caesar cipher with Rail Fence for Enhancing Data security. *International Journal of Advanced Research in Computer Software Engineering, 2(12), 78-80.*
[2]. Anupama, M. (2013).Enhancing Security of Caesar Cipher Using Different Methods. *International Journal of Research in Engineering and Technology, 327-332.*
[3]. Avinash, K.J., (2014). Lecture notes on computer and network society, Purde University.
[4]. Boneh, D. and Durfe, G. (1999). Cryptanalysis of RSA with private key $d < N^{.292}$, *Proceedings of Eurocrypt, 98, 1-11.*
[5]. Chalapathi, D. (2013). Implementation of Strong Encryption Method Using Caesar
[6]. Cipher Algorithm. *International Journal of Advanced Research in Computer Software Engineering, 2(11), 1264-1268.*
[7]. Deepak, G. and Seema, V. (2009). Improvement over Public Key Cryptographic
[8]. Algorithm.*International Advanced Computing Conference*, Thapar University, Patiala,India.
[9]. Doyle, R., (2011). Hill cipher: linear Algebra in cryptography, lecture notes.
[10]. Gupta, H. and Kumar, V. (2010). Multiphase Encryption: A New Concept in Modern
[11]. Cryptography.*International Journal of Computer Theory and Engineering,2, 5-22.*
[12]. Harinadan, T. and Soumen, A. (2012). New Modified Playfair Algorithm Based on Frequency Analysis.*International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, 2(1), 2-4.*
[13]. Judson, W.T., (2010). Abstract Algebra Theory and Aplications, Austin State University, P.100 – 101.
[14]. Kashish, G., and Supriya, K. (2013).Modifed Caesar Cipher for Better Security Enhancement. *International Journal of Computer Applications, 3(73), 26-28.*
[15]. Krishna, A.V.N. and Vinaga, A. B. (2007). A modified Hill Cipher Algorithm for Encryption of Data in Data Transmission. *Georgian Electronic Scientific Journal: Computer Science and Telecommunications, 3(14), 78-80.*
[16]. Krishma, A. and Chanhan, V. (2014). A Modified Hill Cipher Algorithm for Encryption of Data in Data Transmission. *International Journal of Emerging Technology and Advanced Engineering, 3(14), 78-80.*
[17]. Kwang, H.L. (2010). Chapter 2: Basic Encryption and Decryption, *lecture note*, Department of Electrical engineering and computer Science.
[18]. Menezes, A.P. (1996). *Hand book of Applied Cryptography.* Retrieved from www.cacr.math.uwaterloo.calhac, pp, 5-22.
[19]. Mukhofadhyay, D. (2010). *Classical cryptosystems.* Department of Computer Science, Indian Institute of technology Khargpur, lecture note.
[20]. Mohd, Z.W.M.Z. (2008). *Attack on cryptography*, lecture note.
[21]. Rajan, S.J. and Shantanu, G.J. (2013). File encryption and Decryption Using Secure RSA.
[22]. *International Journal of Emerging Science and Engineering(IJESE), 1, ISSN: 2319-6378.*
[23]. Rizvi, S.S., Riasat, A. and Khaled, M.E. (2010). Combining Private and Public Key Encryption Techniques for Providing Extreme Secure Environment for an Academic Institution Application. International *Journal of Network Security and its Application (IJNSA), 2(1), 82-84.*
[24]. Sanjay, B. and Uptal, K.R. (2012).Modified Playfair Cipher Using Rectangular Matrix.
[25]. *International Journal of Computer Application, 46(9), 28-29.*
[26]. Schneier, B. *Aplied cryptography, second edition*. p. 300-310.
[27]. Sreenivasulu, L. R. (2013). A New Modal of Hill Cipher Using Non- Quadratic Residues.
[28]. *International Journal of Soft Computing and Engineering, 2(2), 73-74.*
[29]. Srikantaswamy, S.G. and Phaneendra, H.D. (2012). Improved Caesar Cipher with Random
[30]. Number Generation Technique and Multistage Encryption.*International Journal on Cryptography and Information Security (IJCIS), 2(4), 40-46.*
[31]. Stallings, W. (2010).*Cryptography and Network security, principles and practice*. Fifth edition, Prentice Hall, New York, pp. 243-323.
[32]. Tuchman, W. (1551).Data Encryption Gurus.Cryptologia, *2(4), 371.*
[33]. Yashpalsingh, R.D.N. and Mane, C. (2014). An Improved Cryptographic Technique to
[34]. Encrypy Text Using Double Encryption, *International Journal of Computer Application, 86(6), 1-5.*
[35]. Zulkarnaini, M.D. and Mohammed, A.J. (2013). New Computation Technique for
[36]. Encryption and Decryption Based on RSA and Elgamal Cryptosystems. *Journal of Theoretical and applied Information Technology, 47(1), 74-76.*