The Journal of Computer Science and its Applications
An International Journal of the Nigeria Computer Society (NCS)
Vol.22, No.2 December(2015), pp.48-53

COMBINED MODEL OF 9X9 PLAYFAIR AND RSA FOR SECURING CONFIDENTIAL INFORMATION

Y. B. Zakariyau[1], L. J. Muhammad[2], A. M. Usman[3] A. Garba[4]

[1, 2] Mathematics & Computer Science Department, Federal University, Kashere, Gombe State, Nigeria, Computer Science Department, [3]Federal College of Education Technology, Gombe, Gombe State, [4]Peking University, Beijing China, Information Lab, School of Computer Science and Electronics Engineering

baladada57@yahoo.com[1] , *lawan.jibril@fukashe.edu.ng*[2], *aliakko2000@gmail.com*[3]
abbaggumel@pku.edu.cn[4]

ABSTRACT

In our contemporary world, the confidential information that is transmitting over the network need to be encrypted so as to guarantee its security against intruders. However, the cryptographic algorithms play vital roles in providing security to such confidential information against intruder attacks. RSA algorithm and 9x9 Playfair ciphers are some commonly used cryptographic algorithms. In this paper, we have proposed a new combined cipher model which chooses a key to encrypt the plaintext through the 9x9 Playfair cipher and encrypt the key through the RSA using the public key of the receiver before sending. On arrival, the receiver decrypts the key through RSA using his own private key and finally decrypts the ciphertext through the 9x9 payfair cipher using the recovered key. Therefore, the propose algorithm can be used to secure the confidential information for transmission over the network.

Keywords- Cryptography, RSA, Playfair Cipher, Public and Secret Key

1. INTRODUCTION

In our contemporary world 'information' has become indispensable to both individuals and organizations. When a message is stored or transmitted, there should be some mechanism to protect that information from hacking. If information reaches the wrong person there might arise a lot of problems. Hence there is a need to hide the confidential information so that a third person cannot find out the exact message. However, cryptography plays an important part in securing information in our contemporary world. The term cryptography comes from the Greek origin. It is a combination of two words Crypto and Graphy. Crypto means Secret and Graphy means writing [8].

So the cryptography is the study of creating and using encryption and decryption techniques. In cryptography, the term plaintext is used for the original message that is to be transformed. The message which has been transformed is called Ciphertext. An encryption algorithm works with a key to transform the plaintext into ciphertext while decryption algorithm works in the reverse order and converts the ciphertext into plaintext [7]. The encryption /decryption algorithm is to encrypt/decrypt the message with the help of a key. The process of converting plaintext into ciphertext is called enciphering or encryption. The process of retaining the plaintext from the ciphertext is called deciphering or decryption.

2.0 PRELIMINARIES

Cryptography helps us to store sensitive and classified information or transmit it across insecure and vulnerable networks so that it can reach safely the destination. Cipher systems are classified into two classes which are:

i. Secrete key cipher system is the oldest type of method in which to write things in secret. There are two main type of secrete key cryptography, transposition and substitution. Transposition cipher, encrypt the original message by changing characters order in which they occurred. Whereas in substitution cipher, the original message was encrypted by replacing their characters with other characters. In both types, both the sender and receiver share the same secret keys. However, Play fair cipher is one of the most widely known secret key schemes today [1].

ISSN: 2006-5523
Copyright ⓒ 2015 JCSA

ii. Public-key cipher system is a system in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key.[3] This is used in an attempt to ensure confidentiality. It is often also used to secure electronic communication over an open networked environment such as the Internet, without relying on a covert channel even for key exchange. Open networked environments are susceptible to a variety of communication security problems such as man-in-the-middle attacks and other security threats.

2.1 Encryption and decryption

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypted plaintext called ciphertext. The encryption is used to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

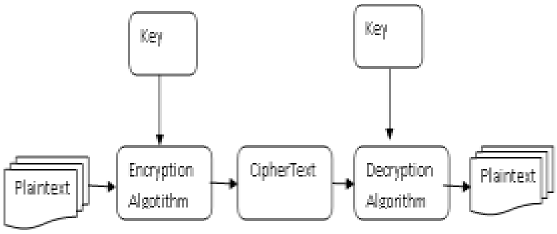

Figure 1: Encryption and Decryption

Plaintext is denoted by M, for message, or P, for plaintext. It can be a stream of bits, a text file, abitmap, a stream of digitized voice, a digital video image whatever. As far as a computer is concerned, M is simply binary data. The plaintext can be intended for either transmission or storage. In any case, M is the message to be encrypted. Ciphertext is denoted by C. size as M, sometimes larger. (By combining encryption with compression, C may be smaller than M. However, encryption does not accomplish this.) The encryption function E, operates on M to produce C. Or, in mathematical notation: $E(M) = C$

In the reverse process, the decryption function D operates on C to produce M: $D(C) = M$

Since the whole point of encrypting and then decrypting a message is to recover the plaintext, the following identity must hold true: [1]

$D(E(M)) = M$

2.2 RSA Algorithm

RSA is an Asymmetric key (also known as public key encryption) uses two different keys to encryption and decryption of the message. The public key is made publicly available and can be used to encrypt messages. The private key is kept secret and can be used to decrypt received messages. RSA is asymmetric key encryption algorithm [9]. RSA uses two different keys for encryption and decryption leading to secure transmission of messages. RSA algorithm involves three different phases [6]:

2.2.1 Algorithm for Generating Key

RSA involves two keys public key and private key. For encryption we use Public key and for decryption we use private key of message. The key generation takes places as follows [2]:

(a) Choose two distinct prime numbers P and Q

(b) Find N such that N= P*Q,

(c) Find the Phi of N, ( )= (P-1)*(Q-1).

(d) Choose an E such that 1 < E < ( ) and such that E and ( ) share no Divisors other than 1 [E and ( ) are relatively prime]. E is kept as the public key exponent.

(e) Determine D which satisfies the congruence relation.

E*D = 1 (mod ( )).

Now, the public key consists of public key exponent E and N. And private key consists of private key exponent D & N.

Public Key: (E, N)

Private Key: (D, N)

2.2.2 Algorithm for Encryption

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure environment. The process of encryption requires two things- a key and an encryption algorithm. Encryption takes place at the sender side. C = M ^ E mod (N)

2.2.3 Algorithm for Decryption

It is a process of converting Cipher Text into Plain Text. This reverse process of encryption is called as Decryption. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. M = C ^ D mod (N)

2.2.4 RSA Illustration

This example is to illustrate the method. In practice the primes p and q will be very large to ensure security.

i. .We pick as prime numbers p=3,q=11

ii. Ø = (p-1) x (q-1) = 2 x 10 = 20

iii. We pick a number relatively prime to 20. We pick 7. The Public key of Mr. A = {7, 33}

iv. To pick private key of Mr. A find d from relation (d x e)mod(ø) = 1
(d x 7) mod (20) =1
This gives d =3. Therefore, the private key of Mr. A = {3, 33} [3]

2.2.5 Encryption and Decryption Using RSA Algorithm

i. Let the message is **ERDIT**. If we use code E=5, R=18,
D=4,I=9, T=20, then the message is 5,18,4,9,20.

ii. .We will **encrypt** one letter at a time. Thus cipher of plaintext 3 is
5**e**mod (n) =57 mod (33)
E - (5)**7**mod (33) =78125 mod (33) =14
R - (18)**7**mod (33) = 612220032 mod (33)=6
D - (4)**7**mod (33) =16384 mod (33) =16
I - (9)**7** mod (33) =4782969 mod (33) = 15
T – (20)7mod (33) = 1280000000 mod(33) =26

iii. Thus cipher text = 14,6,16,15,26

iv. **Decryption**: c**d** mod (n) d=3,n=33
E - 14**3**mod (33) = 2744 mod(33) = 5
R - 6**3**mod(33) = 216 mod(33)=18
D - 16**3**mod(33) = 4096 mod(33) =4
I - 15**3**mod(33) = 3375 mod(33) =9
T - 26**3**mod(33) = 17576 mod(33) =20

Hence the original text 5,18,4,9,20 [3]

2.3 9x9 Playfair Cipher

The 9 x 9 Playfair cipher uses a 9 by 9 matrix containing a key word or phrase. Memorization of the keyword and 7 simple rules was all that was required to create the 9 by 9 table and use the cipher.

2.3.1 Algorithm for Generating Matrix

i. Read a keyword.

ii. Eliminate the repeated characters in keyword.

iii. Construct a matrix by filling the character of keyword from left to right and top to bottom.

iv. Fill the reminder of matrix with the remaining characters from ASCII values 0 to 255.

v. Read a plaintext.

vi. Divide the plaintext into pair of characters.

vii. Add the character “] ” when odd number of character in the message.

2.3.2 Algorithms for Encryption

i. Read a plaintext.

ii. Divide the plaintext into pair of characters.

iii. Add the character “] ” when odd number of character in the message.

iv. If the pair of plaintext falls in the same row of the matrix are replaced by the character to the right, with the first element of the row circularly following left.

v. If the pair of plaintext fall in the same column of the matrix are replaced by the character beneath, with the top element of the column circularly following in the last.

vi. If the pair of plaintext appears on the different row and column, each plaintext character is replaced by the character that lies in its own row and column occupied by the other plaintext character.

2.3.3 Algorithm for Decryption

i. If the pair of ciphertext falls in the same row of the matrix are replaced by the character to the left, with the first element of the row circularly following right.

ii. If the pair of ciphertext fall in the same column of the matrix are replaced by the character at top, with the bottom element of the column circularly following in the last.

iii. If the pair of ciphertext appears on the different row and column, each plaintext character is replaced by the character that lies in its own row and column occupied by the other plaintext character.

ISSN: 2006-5523

Copyright ⓒ 2015 JCSA

2.3.4 A 9x9 Playfair Cipher Illustration

This Playfair algorithm is based on the use of 9x9 matrix of characters constructed using a keyword. The matrix is constructed by filling the characters of keyword (minus duplicates) from left to right and from top to bottom. Then it is filling the remaining characters in ascending order from ASCII value 0 to 255, as shown in Table 1 using keyword "CRYPTO"

Table1: A 9x9 Playfair cipher

C	R	Y	P	T	O	.	/	0
1	2	3	4	5	6	7	8	9
:	;	<	=	>	?	@	A	B
D	E	F	G	H	I	J	K	L
M	N	Q	S	U	V	W	X	Z
[	\	]	^	_	`	a	B	C
D	E	f	G	H	I	J	K	L
M	N	o	P	Q	r	s	T	U
N	W	x	Y	Z	{	|	}	~

2.3.5 Encryption Using 9x9 Playfair Cipher

Let us take the plaintext as Transfer and the keyword as CRYPTO**.** Breaking up the plaintext into digrams we get the following digrams and hence the ciphertext.

Tr They are neither in the same row or column and thus using rule 3 we get **qO**

an They are neither in the same row or column and thus using rule 3 we get **s**

sf They are neither in the same row or column and using rule 3 we get **jo**

er They are neither in the same row or column and using rule 3 we get **ni**

Thus the ciphertext will be **qO s\joni**

2.3.6 Decryption Using 9x9 Playfair Cipher

In case of decryption rules 1 and 2 have to be reversed. Breaking up the cipher text into digrams we get the following digrams and hence the plaintext.

qO They are neither in the same row or column and thus using rule 3 we get **Tr**

s They are neither in the same row or column and thus using rule 3 we get **an**

jo They are neither in the same row or column and using rule 3 we get **sf**

ni They are neither in the same row or column and using rule 3 we get **er**

Thus we get back the original plaintext which we encrypted.

3. RELATED WORK

In the study of [13], proposed combined cipher algorithm which combine RSA and Diophantine equation. The algorithm first applied Diophantine equation on the data to be send and then its outputs is taken as inputs to the RSA algorithm. Euclidian algorithm is used in between the process of the Diophantine equation. On the sender side, Equation "ax+by=c" is used. In this equation 'a' and 'b' are constants and 'x' and 'y' are user datum. Using this equation, Diophantine constant 'c' is calculated. This 'c' is taken as an input for the RSA algorithm. Cipher text that is generated from the RSA algorithm is send to the receiver. On the receiver side, RSA algorithm is applied on the cipher text that is send from the sender. RSA algorithm will generate Diophantine constant 'c' as an output. Apply Diophantine equation and Euclidian algorithm on the Diophantine constant 'c' and then find the values of 'x' and 'y' that satisfy the Diophantine equation "ax+by=c". These 'x' and 'y' are the datum that is send by the sender. However, the complexity of the algorithm is very high because on receiver side, it is not easy to generate plain text.

In the work of [8] proposed combined cipher algorithm which in the first stage, Play Fair Cipher matrix has been used with a modification by adding four iteration steps to it. In the second stage, RSA public key encryption technique with ASCII conversion has been used for authentication.

In the work of [10] also cryptographic algorithm was proposed which used a 12×8 matrix which contain all alphabetic, numeric and special character use in keyboard as input and in the second stage, RSA public key encryption technique is used for sending the key of the PF ciphers securely.

4. COMBINED CIPHERS MODEL

The proposed model combined ciphers model, the sender chooses a key to encrypt the plaintext through the 9x9 palyfair cipher and encrypt the key through the RSA using the public key of the

ISSN: 2006-5523
Copyright ⓒ 2015 JCSA

receiver before sending, on arrival the receiver decrypts the key through RSA using his own private key and finally decrypt the ciphertext through the 9x9 payfair cipher using the recovered key. Figure 2 depicts the model.

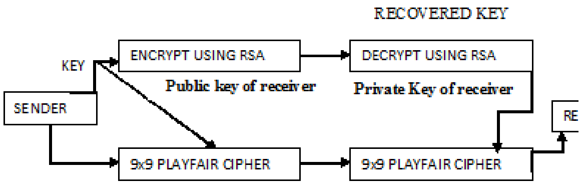

Figure 2: Combined Model 9 x 9 Playfair Cipher and RSA

4.1 Illustration of Encryption and Decryption of Combined Cipher Model

Assuming the sender chooses ERDIT as his password to encrypt a message on the 9x9 playfair cipher. A 9x9 matrix will be generated as shown in table 3 below

Table 3: 9x9 Matrix Based on the Password ERDIT

E	R	D	I	T	.	/	0	1
2	3	4	5	6	7	8	9	:
;	<	=	>	?	@	A	B	C
F	G	H	J	K	L	M	N	O
P	Q	S	U	V	W	X	Y	Z
[	\	]	^	_	`	a	b	c
d	e	f	G	h	I	J	k	l
m	n	o	P	q	r	s	t	u
n	w	x	Y	z	{	|	}	~

4.1.1 Encryption

First of all, the sender encrypts the message **"Come"** using the password **ERDIT** on 9x9 playfair cipher and the cipher text obtained is **" u=dn"**

Secondly, the sender uses public key **[7,33]** to encrypt the password **ERDIT** on RSA and the ciphertext obtained is **14,6,16,15,26**

Finally, the sender sends **u=dn** and **14,6,16,15,26** to the receiver

3.1.2 Decryption

Firstly, the receiver uses his private key [3,33] to decrypt the cipher text **"14,6,16,15,26"** on RSA and the plaintext obtained is **"5,18,4,9,20(ERDIT)".**

Secondly, the receiver uses the recovered key **ERDIT** to decrypt the ciphertext **u=dn** on 9x9 playfair cipher and the plaintext obtained is **"Come"** which is the original

5. CONCLUSION

This paper has practically demonstrated how people can secure their vital and sensitive information stored or transmitted via insecure communication channels from intruders by using combined ciphers model. This technique can withstand many types of attack.

5. REFERENCES

[1] Schneier, B. Applied Cryptography, protocols, algorithms and source code on C.

[2] Diana, W. E-commerce Security, Encryption Methods for secure e-commerce websites.

[3] Electronic Commerce http://nptel.iitm.ac.in/courses/Webcourse-contents/IISc-BANG/System%20Analysis%20and%20Design/pdf/Lecture_Notes/LNm13.pdf Date retrieved 02/11/2015

[4] An Introduction to Cryptograph, ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf
Date retrieved 03/11/2015

[5] Al-Hamami, A. H., & Aldariseh, I. A. (2012, November). Enhanced Method for RSA Cryptosystem Algorithm. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp. 402-408). IEEE.

[6] Malkin, T, Micciancio D, Miner S. Efficient Generic Forward-secure Signatures with an Unbounded Number of Time Periods[C]. Proc. Of Advances in Cryptology EUROCRYPT. 2002 Multi Conference of Engineers and Computer Scientists 2008 Vol I IMECS 2008, 19-21 March, 2008, Hong Kong

[7] Muhammad, S., Nasir, R., Shah, K. & Muhammad, R. (2011). A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case). World Academy of Science, Engineering and Technology http://www.waset.org/journals/waset/v49/v49-160.pdf

[8] Nisarga, C., Bappadittya, R., Krishanu, K. (2013) Designing of an Encryption Technique Suitable For Wireless Ad-Hoc Sensor Network, International Journal of

ISSN: 2006-5523
Copyright ⓒ 2015 JCSA

Advanced Research in Computer Science and Software Engineering. Volume 3, Issue 3, March 2013 ISSN: 2277 128X

[9] Stallings, W. (2004). Cryptography and Network Security – Principles and Practices (3rd Ed.). Pearson Education: Boston

[10] Surendra, S. C, Chauhan, Hawa, S. & Ram, N. G. (2014). Secure Key Exchange using RSA in Extended Playfair Cipher Technique. International Journal of Computer Applications (0975 – 8887) Volume 104 – No 15, October 2014. pg 13 - 15

[11] Elxsi, T. Public Key Cryptography, Applications Algorithms and Mathematical Explanations

[12] Wang, R.; Chen J.; Duan G. (2011) "A k-RSA algorithm," IEEE 3rd International Conference on Communication Software and Networks (ICCSN). 21,24, 27-29 May 2011

[13] Zakir, H. (2013) An efficient Algorithm using Diophantine equation and RSA Algorithm. Unpublished thesis submitted School of Mathematics and Computer Applications, Tharar University Patiala 20-24

[14] Zirra, P. B. & Wajiga, G. M. (2011). Cryptographic Algorithms for Secure Data Communication. International Journal of Computer Science and Security (IJCSS), 5(2), 2-3.

ISSN: 2006-5523
Copyright ⓒ 2015 JCSA