Int. J. Nonlinear Anal. Appl. 12 (2021) No. 2, 2345-2350
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2021.5379

Hybrid encryption using playfair and RSA cryptosystems

Raghad K. Salih [a,*], Madeha Sh. Yousif[a]

[a]Department of Applied Sciences, Mathematics and Computer Applications, University of Technology, Baghdad, Iraq

(Communicated by Madjid Eshaghi Gordji)

Abstract

Security is demanded to transport important data over the network. In this work, a hybrid encryption depending on playfair cipher and RSA algorithm is proposed to give more confidentially and get rid of the defects of the two methods. The first cipher text is obtained by playfair cipher by using (812) expanded key matrix that is filled by decimal ASCII characters of Alphabets, numbers and common characters of ASCII table while the final cipher text is obtained by RSA cryptosystem by applying it for blocks of two characters. The proposed hybrid encryption avoids taking large numbers in RSA algorithm and performs complex operations that need a long time to do. The proposed hybrid cipher is tight security that is difficult to analyze and detect from hackers and intruders.

Keywords: Playfair, RSA algorithm, ASCII and Hybrid encryption.

1. Introduction

Encryption is a Greek word for confidential writing, encryption technology protects electronic private records while transmitted and ensures that only intended recipients are able to see them. RSA is a type of public key encryption algorithm that was first announced in 1987. The integrity of RSA depends on the factor of large numbers, that meaning it is difficult to get a password every time; As the key is hard to generate, it is limited by the prime number technique plus the packet length is very large. To ensure security, n must be at least 600 bits, which makes the calculation cost is very high, it takes a long time to implement [1, 2].

The playfair cipher was firstly introduced by Charles Wheatstone in 1854. It is substitution procedure. It has a 5 ×5 key square matrix of characters. Since the playfair array contains only 25

*Corresponding author
Email addresses: Raghad.k.Salih@uotechnology.edu.iq (Raghad K. Salih), Madeha.s.Yousif@uotechnology.edu.iq (Madeha Sh. Yousif)

Received: March 2021 *Accepted:* July 2021

characters, one character is usually J discarded from the table. If the plain text contains a J, it must be changed by I [7].

In this work, a hybrid encryption has been achieved that overcomes the shortcomings of RSA and playfair schemes whereas integrating the advantages of the two schemes in order to get a safety ciphertext with little computational complexity. In the hybrid cipher, we do not need to take large numbers in RSA due to including modified playfair layer that gives strong protection from attacks and hackers

2. Related work

S. Y. Kayode, et .al [2], proposed a parallel application technique in RSA by Chinese remainder theorem and thread in enciphering operations and deciphering. Islam, M. et.al [1] modified RSA cryptosystem basing on "n" distinct prime number. Shireen, et al. [5] hid confidential patient data via zigzag procedure utilizing RSA algorithm in a RGB medical cover image. Pal, et al,[4] varied the substitution rule of playfair with model has 6x6 array containing decimal digits, underscore and some characters. Yousif et al. [7] developing the playfair key matrix into with applying permutation key to it, supplements a further layer of security for the crypto system. Licayan, et al [3] Enhance Playfair scheme by Seed Based Color Substitution. Villafuerte, et al [6] improve 3D-Playfair algorithm by generating random numbers.

3. The proposed hybrid Encryption

There are two keys in hybrid algorithm. The first one is a vector ($k1_{1\times12}$) filling by 12 numbers 01,02, 3,4,. . . ,12 with specific order used to rearrange the columns of the expanded (8×12) playfair key matrix shown in Table. 1 and the second key is the public key (e,r) of RSA algorithm. The first key is applied to obtain the first ciphertext C. The second key is applied to C after C is split into blocks of two decimal characters to get the final ciphertext. The hybrid encryption provides strong protection against breaches.

Table 1: The Expanded playfair matrix.

32	*33*	*34*	*35*	*36*	*37*	*38*	*39*	*40*	*41*	*42*	*43*
44	*45*	*46*	*47*	*48*	*49*	*50*	*51*	*52*	*53*	*54*	*55*
56	*57*	*58*	*59*	*60*	*61*	*62*	*63*	*64*	*65*	*66*	*67*
68	*69*	*70*	*71*	*72*	*73*	*74*	*75*	*76*	*77*	*78*	*79*
80	*81*	*82*	*83*	*84*	*85*	*86*	*87*	*88*	*89*	*90*	*91*
92	*93*	*94*	*95*	*96*	*97*	*98*	*99*	*100*	*101*	*102*	*103*
104	*105*	*106*	*107*	*108*	*109*	*110*	*111*	*112*	*113*	*114*	*115*
116	*117*	*118*	*119*	*120*	*121*	*122*	*123*	*124*	*125*	*126*	*127*

3.1. Hybrid Enciphering Algorithm

Input :

- The vector $k1_{1\times 12}$.
- The (8×12) playfair matrix
- Two prime numbers a and b.
- Plaintext p.

Output :
Ciphertext (Cf).

1. Compute $r = a \times b$ *and* $\varnothing(r) = (a-1) \times (b-1)$
2. Choose e such that $1 < e < \varnothing(r)$ and $\gcd(e, \varnothing(r)) = 1$
3. Find the first ciphertext C by using playfair scheme as:
   - Apply $k1_{1\times 12}$ to create a (8×12) playfair matrix.
   - Convert the characters of the plaintext p into the corresponding decimal ASCII characters, then split them into a set of two decimal characters. If two decimal ASCII characters are the same then add 38.
   - Whether the character at the final set is single, add 32.
   - When the both decimal characters located in the same row. Take the character on the right side of it, taking into account if it is the last character in the row, we start from the beginning of the row.
   - When the both decimal characters lie in the same column. Take the character below it, considering whether it is the last character in the column, we start from the beginning of the column.
   - Else, they should be substituted with the same decimal ASCII characters on the same row respectively, but at the other pair of corners of the rectangle which is demarcated by those pairs.
4. Find the final cipher text Cf which is hybrid cipher by using RSA cryptosystem as:
   - Split the ciphertext C in step 3 into blocks each block has two decimal characters of C.
   - Compute Cf=$(C)^e$ mod r .

3.2. Hybrid Deciphering Algorithm

Input :

- The vector $k1_{1\times 12.}$
- Two prime numbers a and b.
- The inverse of the second key $d = e^{-1} mod\ \varnothing(r)$ $where$ $e \times d(mod\ \varnothing(r)) = 1$
- Ciphertext (Cf).

Output
Plaintext Pf.

1. Find the first plain text P_1 by using RSA cryptosystem as:
   - Separate the blocks formed in step 4 in the hybrid encryption algorithm.
   - $p_1 = (Cf)^d \text{mod r}$.
2. By using the vector $k1_{1\times 12.}$, create 8×12 key matrix.
3. Utilize the same operations of playfair cipher in step 3 of hybrid encryption algorithm for p_1 but in converse to get the final plaintext Pf.

4. Results and Secrecy Discussion

4.1. Results

$$\begin{aligned}&\text{Consider } k1 = [02\ \ 8\ \ 01\ \ 4\ \ 3\ \ 5\ \ 6\ \ 7\ \ 11\ \ 12\ \ 9\ \ 10]\\&k_2 = (e, r) = (23, 10807)\\&\text{where } \alpha = 101,\ \ b = 107,\ \ r = a \times b = 10807\\&\varnothing\,(r) = (a-1) \times (b-1) = 10600\end{aligned}$$

The plaintext $p =$ white colour.
Applying $k1$, the expanded (8×12) playfair matrix is shown in Table (2).

Table 2: The Expanded playfair matrix using k1.

33	*39*	*32*	*35*	*34*	*36*	*37*	*38*	*42*	*43*	*40*	*41*
45	*51*	*44*	*47*	*46*	*48*	*49*	*50*	*54*	*55*	*52*	*53*
57	*63*	*56*	*59*	*58*	*60*	*61*	*62*	*66*	*67*	*64*	*65*
69	*75*	*68*	*71*	*70*	*72*	*73*	*74*	*78*	*79*	*76*	*77*
81	*87*	*80*	*83*	*82*	*84*	*85*	*86*	*90*	*91*	*88*	*89*
93	*99*	*92*	*95*	*94*	*96*	*97*	*98*	*102*	*103*	*100*	*101*
105	*111*	*104*	*107*	*106*	*108*	*109*	*110*	*114*	*115*	*112*	*113*
117	*123*	*116*	*119*	*118*	*120*	*121*	*122*	*126*	*127*	*124*	*125*

Using the hybrid encryption algorithm, the following results were obtained:

$$P = wh\ it\ ec\ ol\ ou\ r32$$
$$P = 87\ 104\ 105\ 116\ 101\ 99\ 111\ 108\ 111\ 117\ 114\ 32$$
$$C = 80\ 111\ 104\ 117\ 93\ 92\ 104\ 109\ 105\ 123\ 104\ 42$$
$$C = \mathbf{80111}\ 104117\ \mathbf{9392}\ 104109\ \mathbf{105123}\ 10442$$
$$Cf = C^{23} mod\ \ 10807$$
$$Cf = 9047\ 626\ 10253\ 6941\ 328\ 5586$$

To decipher the ciphertext (Cf) , we use hybrid deciphering algorithm to show the results:

$$d = e^{-1} mod\ \varnothing(r) = 3687$$
$$p_1 = (Cf)^{3687} mod\ \ 10807$$
$$p_1 = 80111\ 104117\ 9392\ 104109\ 105123\ 10442$$
$$p_1 = 80\ 111\ 104\ 117\ 93\ 92\ 104\ 109\ 105\ 123\ 104\ 42$$
$$Pf = \text{the final plaintext} = 87\ 104\ 105\ 116\ 101\ 99\ 111\ 108\ 111\ 117\ 114\ 32$$

The plaintext = white colour

4.2. Secrecy Discussion

The hybrid encryption algorithm overcomes the weakness of playfair procedure and the complex computations of the RSA cipher system. In return, we get a highly confidential cipher as explained below

1. The size of playfair key matrix is 5×5 where it contains 25 Alphabets, this leads to the two letters 'I' and 'J' is treated as one letter. So, ambiguity is happened in the deciphering procedure. In the hybrid algorithm this shortcoming is overridden by extending the matrix to 8×12 which results in a matrix containing all the Alphabets, numbers and common characters of ASCII table.
2. In RSA cryptosystem when the choice of the encryption exponents e is low (e.g., e = 3) and small values of the plaintext p, (i.e., $p < r^{1/e}$) the result of p^e leads to strictly less than the modulo r. so the ciphertexts can be easily deciphered by taking the e^{th} root of the ciphertext over the integers. Therefore, it needs large complicated numbers that leads to difficult computations as well as a long time to do it whereas in the hybrid algorithm due to the presence of the hybrid layer we do not need that, the small numbers are enough to provide more protection and security than usual.
3. In the attack, the hacker must decrypt hybrid ciphertext that has two keys and two layers, substitution layer and RSA layer, which makes parsing this very intricate.
4. When the RSA cipher system is implemented, the repetition of the numbers in the plaintext indicates the repetition of characters in the ciphertext, and this gives an opportunity for hackers to analyze them statistically and reveal the ciphertext. But in the hybrid ciphertext it is different, because the repetition of the numbers in the plaintext does not indicate the repetition of characters in the cipher text. Recall the example in section (4.1) although the letter o is repeated in the plaintext, there is no repeat of the decimal characters in the ciphertext, due to the hybrid encryption. So, the hybrid method provides robust protection and security in the ciphertext that gives more confusion and hardness to cryptanalyst.

5. Conclusion

The current work introduced a hybrid algorithm by combining playfair and RSA algorithms. It was verified that the hybrid algorithm enhanced the secrecy level of the cipher text as well as avoiding the weakness of playfair scheme via expanding the key matrix to 8×12 in addition to averting the complexity, very large numbers and arithmetic operations that need long time in RSA algorithm. In hybrid algorithm the first ciphertext encrypted by playfair process was split to blocks and then encrypted them. Hybrid layer encryption provides sufficient protection and robust security.

References

[1] M.A. Islam, N. Islam and B. Shabnam, *A modified and secured RSA public key cryptosystem based on "n" prime numbers*, J. Comput. Commun. 6 (2018) 78.

[2] S.Y. Kayode and G.K. Alagbe, *An Improved RSA Cryptosystem Based on Thread and CRT*, e-Academia J. 6 (2017).

[3] A.C. Licayan, B.D. Gerardo and A.A. Hernandez, *Enhancing playfair cipher using Seed based color substitution*, 16th IEEE Int. Colloq. Signal Proc. Appl. 2020, pp. 242-246.

[4] P. Pal, G.S. Thejas, S.K. Ramani, S.S. Iyengar and N.R. Sunitha, *A variation in the working of playfair cipher*, In IEEE 4th Int. Conf. Comput. Syst. Inf. Tech. Sust. Solution, India, 2019.

[5] S.S. Shireen, B.M. Krishna, K.N.L. Prasanna and A.P.C. Reddy, *FPGA based RSA authenticated data hiding in image through steganography*, Int. J. Innov. Tech. Explor. Engin. 8(4) (2019) 550–554.

[6] R.S. Villafuerte, A. M. Sison, A. A. Hernandez and R. P. Medina, *Randomness Evaluation of the Improved 3D-Playfair (i3D) Cipher Algorithm*, 12th Int. Conf. Commun. Software Networks 2020, pp. 240–245.

[7] M.S. Yousif, R.K.Salih and N.M.G. Alsaidi, *A new modified playfair cipher*, AIP Conf. Proc. 2019