Open Access | **Baghdad Science Journal** | **P-ISSN: 2078-8665**
Published Online First: May, 2023 | **2024, 21(1): 151-160** | **E-ISSN: 2411-7986**

DOI: https://doi.org/10.21123/bsj.2023.8361

Proposed Hybrid Cryptosystems Based on Modifications of Playfair Cipher and RSA Cryptosystem

Saja Mohammed Suhael[1*] ***Zaynab Anwer Ahmed***[1] ***Abir Jaafer Hussain***[2]

[1] Department of Mathematics, College of Science for Women, University of Baghdad, Baghdad, Iraq.
[2] Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK
[2] Department of Electrical Engineering, College of Engineering, University of Sharjah, Sharjah UAE
[*]Corresponding author: saja.mohammed1203a@csw.uobaghdad.edu.iq
E-mails addresses: zainabaa_math@csw.uobaghdad.edu.iq, abir.hussain@sharjah.ac.ae

Received 12/1/2023, Revised 2/4/2023, Accepted 3/4/2023, Published Online First 20/5/2023, Published 01/1/2024

Abstract:

Cipher security is becoming an important step when transmitting important information through networks. The algorithms of cryptography play major roles in providing security and avoiding hacker attacks. In this work two hybrid cryptosystems have been proposed, that combine a modification of the symmetric cryptosystem Playfair cipher called the modified Playfair cipher and two modifications of the asymmetric cryptosystem RSA called the square of RSA technique and the square RSA with Chinese remainder theorem technique. The proposed hybrid cryptosystems have two layers of encryption and decryption. In the first layer the plaintext is encrypted using modified Playfair to get the cipher text, this cipher text will be encrypted using squared RSA to get the final cipher text. This algorithm achieved higher security to data but suffers from a long computational time. So Chinese remainder theorem has been used in the second hybrid cryptosystem to obtain less encryption and decryption time. The simulation results indicated that using the modified Playfair with the proposed square RSA has improved security. Moreover, using the Chinese remainder theorem achieved less encryption and decryption time in comparison to our first proposed and the standard algorithms.

Keywords: Ciphertext, CRT, Cryptosystem, Plaintext, Playfair cipher, Private and public key, RSA cipher.

Introduction:

Cryptography techniques are used to secure information from unauthorized personal intruders [1]. There are various cryptography algorithms to encrypt information. These algorithms can be classified into three types which are symmetric, asymmetric and hybrid cryptosystems. In the symmetric cryptosystem, the sender and receiver should have a specified secure channel to exchange the secret key and the initiation of this channel may cause problem. However, the advantage of using the symmetric algorithm is simplicity and hence less time consumption. Playfair cipher is one of the simplest symmetric cryptosystem. Playfair encryption from the ease of access can be revealed by cryptanalysis. Hence, the ease of utilize of this symmetric cipher has led many researchers to enhance and modify it, then use it in a hybrid cryptosystem to offer higher security and lower complexity.

The second type is an asymmetric cryptosystem which uses two different keys, public and private keys. The public key for encryption be publicly known and the private key is known only to the receiver to decrypt the message. RSA is one of the asymmetric algorithm. It consists of three steps, the first step is the generation of keys (public and private) that is used to encrypt and decrypt data, the second step is encryption, performs actual process of transformation of the encryption into ciphertext, and the third step is decryption, where decrypted ciphertext is translated into plaintext at the receiver[1, 2]. The idea of RSA cryptosystem that it is easy to multiply two large prime numbers and it is extremely difficult to factorize their product. [3].

RSA algorithm based on a mathematical formula is a powerful algorithm because this algorithm is not easy to attack, but it takes longer time to process than a symmetric algorithm[4, 5].

The third type is a hybrid cryptosystem that combines symmetric and asymmetric to provide high security and more complexity against hackers[6].

There are lots of hybrid cryptography methods that combine the Playfair cipher with the RSA cryptosystem technique[7-9]. Most of them used modified Playfair and the RSA cryptosystem without modification.

In this work, the modified Playfair cipher and two modifications of the RSA will be made to increase the level of security and reduce the time required for encryption and decryption.

This research proposed two new cryptosystems, one of them called the hybrid cryptosystem using the Playfair cipher with the RSA square (HRSASQ). The second is a hybrid cryptosystem using the Playfair with the RSA square and Chinese remainder theorem (HRSASQ-CRT). These systems used two layers of encryption: First, encrypt with the Playfair cipher which used the modified Playfair matrix 7×13 to obtain the first ciphertext. Second, it used RSASQ or RSASQ-CRT to obtain the final ciphertext. The hybrid cryptosystem Playfair with RSASQ provides high security and more complexity against hackers to find the private keys since it does not use the public key directly. However, this technique suffers from computational complexity due to RSASQ. To overcomes, this problem proposed the use of CRT[10] in the second hybrid cryptosystem.

The remainder of this paper is organized as follows. Section 3 provides related work, Section 4 shows the proposed hybrid cryptosystem including modified Playfair with RSASQ and modified Playfair with RSASQ-CRT, while Section 5 discusses the simulation results and Section 6 demonstrates the conclusion and future works.

Related Work

Playfair was introduced by Charles Wheatstone in 1854[11]. Playfair cipher is the most widely used of all symmetric multialphabetic cipher techniques, in which a pair of characters is utilized instead of a single character[12]. Playfair cryptosystem uses a matrix of 5×5 characters. The 26 alphabetic letters are distributed to 25 cells, hence the J and I characters are shared with the same cell. To use Playfair encryption must arrange the keyword in the matrix from left to right sides and from top to bottom without duplicate[13,14].

Reviser, **S**hamir, and **A**d leman described an asymmetric RSA algorithm at the Massachusetts Institute of Technology [15,16]. RSA cryptosystem relies on Euler's theorem and the existence of unique inverse to the integer that are relatively prime to the modulo[2, 7]. Modified RSA by using CRT has been proposed by Samir et al. in[10] to decrease the time of RSA cipher.

There are lots of hybrid cryptography methods that combine RSA and Playfair cryptosystem techniques[7-9]. These hybrid methods overcome the disadvantages of RSA and Playfair methods [11,17,18]. While combining their advantages to produce a safer ciphertext with a low computational complexity[15]. They can be classified into four types. In 2021, Salih and Yousif [7] suggested a hybrid cryptosystem that provides high security by encrypting plaintext using two layers in which the first layer encrypts plaintext by Playfair then the second layer encrypts by RSA technique. Singh Chauhan et al.[9] Zakariyau et al.[17] and Mathur and Srivastava[11] in 2014, 2015 and 2017 respectively suggested hybrid cryptography that encrypts plaintext by Playfair and encrypts the key of Playfair by RSA. In 2017, Naga[8] presented a hybrid cryptosystem of Playfair and RSA with an XOR process that provides a complex process that is difficult to be attacked. In 2015, Iqbal et al.[18] suggested a hybrid cryptosystem of Playfair and a modified RSA in which hybrid cryptography that encrypts plaintext by Playfair and encrypts Playfair key by modified RSA that used dual levels for key exchanges.

Hybrid Cryptosystems: Modified Playfair with RSASQ and Modified Playfair with RSASQ-CRT

The proposed methods combine Playfair with RSASQ and RSASQ-CRT. They use the same steps to generate public and private keys but are different in some encryption and decryption steps. These hybrid methods consist of three phases: the key generation steps, encryption steps and decryption steps.

Fig 1 shows the block diagram of the proposed hybrid methods (RSASQ & RSASQ-CRT) between the sender and receiver.

Baghdad Science Journal
2024, 21(1): 151-160
P-ISSN: 2078-8665
E-ISSN: 2411-7986

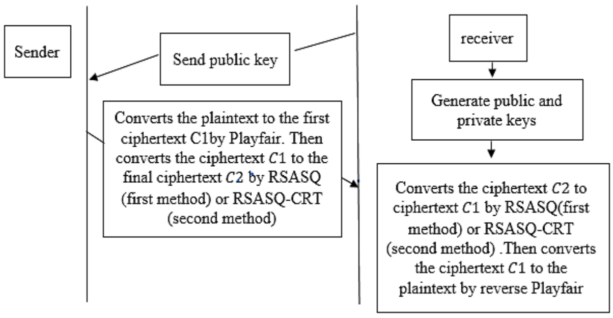

Figure 1.The diagram of RSASQ and RSASQ-CRT algorithms

The steps to generate public and private keys of RSASQ and RSASQ-CRT are as follows:
Step 1: Select two prime number p and q. It should be noted that choosing large prime numbers of p and q will give more security but need more computational complexity. Since the proposed technique will use two layers, hence p and q will be sufficiently bigger than the corresponding numbers of the Plaintext to satisfy Euler's theorem condition of getting relatively prime between the prime numbers and the corresponding numbers of the Plaintext[2, 19].
Step 2: Calculate N, N^2 where $N = p \times q$ and $N^2 = p^2 \times q^2$.
Step 3: Choose public exponent e such that $1 < e < \phi(N)$ and the greatest common divisor between e and $\phi(N)$ is 1. Then the greatest common divisor between e^2 and $\phi(N^2)$ is 1 ($gcd\,(e^2, \phi(N^2)) = 1$).
Step 4: Find the secret exponent $d2$ which is unique multiplication invers of $e^2 \; mod\, \phi(N^2)$ [20]. (the existence and the uniqueness of the invers are satisfying since e^2 *and* $\phi(N^2)$ are relatively prime, therefore $e^2x \equiv 1\,(mod\, \phi(N^2))$ has a unique solution which is the multiplicative inverse of e^2 modulo $\phi(N^2))$ (see the corollary off theorem (A.2.73) in[20]). Then $(d2, N^2)$ will be private key.
Step 5: The receiver shares the public key (e, N) with the others.
The following pseudocode shows the algorithm of generating the public and private keys of RSASQ and RSASQ-CRT.

Input
- Create a pair of sufficiently enough random prime numbers p and q.

Key generated
- Calculate N , N^2 where $N = p \times q$ and $N^2 = p^2 \times q^2$.
- Compute$\emptyset(N) = (p-1)(q-1)$ and $\phi\,(N^2) = (p^2 - p)(q^2 - q)$.
- Choose public exponent e such that $1 < e < \phi\,(N)$, and $gcd\,(e, \phi\,(N)) = 1$, ➔ $gcd\,(e^2, \phi(N^2)) = 1$.
- Find the secret exponent $d2$ such that $e^2 \times d2 \equiv 1(mod\, \phi(N^2))$

Output
- (e, N) as the public key
- $(d2, N^2)$ as the private key

Steps the Encryption of the Proposed Cryptosystems

Step 1: Design the modified Playfair matrix 7×13 which contains all characters and letters on the keyboard as shown in Table 1.

Table 1. Modified Playfair 7 ×13

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	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	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	!	@	#
$	%	^	&	*	(	)	−	=	_	+	[	]
{	}	;	:	‘	“	,	.	<	>	/	?	space

Step 2: Let the keyword $K1$ be "Mathematics", then the duplicate characters should be eliminated and the rest will be "Mathemics". Apply the key $K1$ of Playfair on the modified Playfair matrix 7× 13 as shown in
Table 2.

Table 2. Modified Playfair key matrix 7×13

M	a	t	h	e	m	i	C	S	A	B	C	D
E	F	G	H	I	J	K	L	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	b	d	f	g	j
k	l	n	o	p	q	r	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	!	@	#
$	%	^	&	*	(	)	−	=	_	+	[	]
{	}	;	:	‘	“	,	.	<	>	/	?	space

Step 3: The plaintext M splits into a blocks of two characters. (If two characters are the same then add W between them, while if the character at the final set is single then add the character Q).
Step 4: Transform the plaintext M into ciphertext $(C1)$ by the Playfair algorithm.
Step 5: Convert the 91 characters of the Playfair matrix to suitable corresponding number from 2-93. It should be noted that ASCII table has not been used in this work due to computation complexity.
Step 6: The sender Bob will use the public key (e, N) of the hybrid cryptosystem algorithm received from Alice. Then square it and use the square key in RSASQ and RSASQ-CRT as follows:

In RSASQ

$C2 \equiv C1^{e^2} \ mod \ N^2$

In RSASQ-CRT

$Cp \equiv C1 \ mod \ p^2, Cq \equiv C1 \ mod \ q^2$

$E_p \equiv e^2 \ mod \ \emptyset \ (p^2), Eq \equiv e^2 \ mod \ \emptyset \ (q^2)$

$Mp \equiv \left(C_p\right)^{E_p} mod \ p^2 \ , Mq \equiv \left(C_q\right)^{E_q} \ mod \ q^2$

Find $x_1$such that $x_1 q^2 \equiv 1 \ mod \ p^2$. Find x_2 such that $x_2 p^2 \equiv 1 \ mod \ q^2$

$C2 \equiv (q^2 \times Cp \times x_1 + p^2 \times Cq \times x_2) \ mod \ N^2$.

Figs 2 and 3 show the block diagrams of the encryption algorithm of the two proposed. cryptosystems.

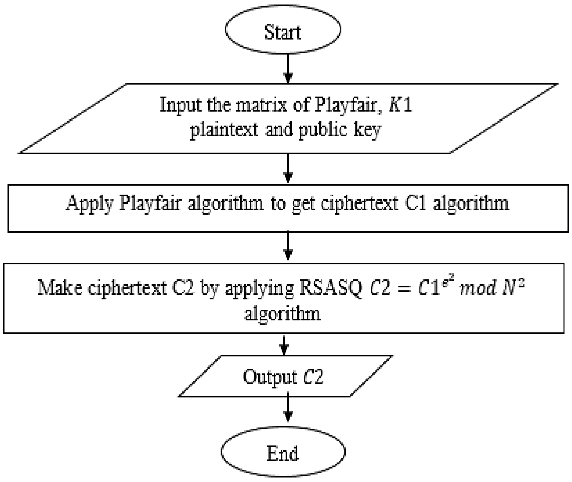

Figure 2. The diagram of HRSASQ encryption

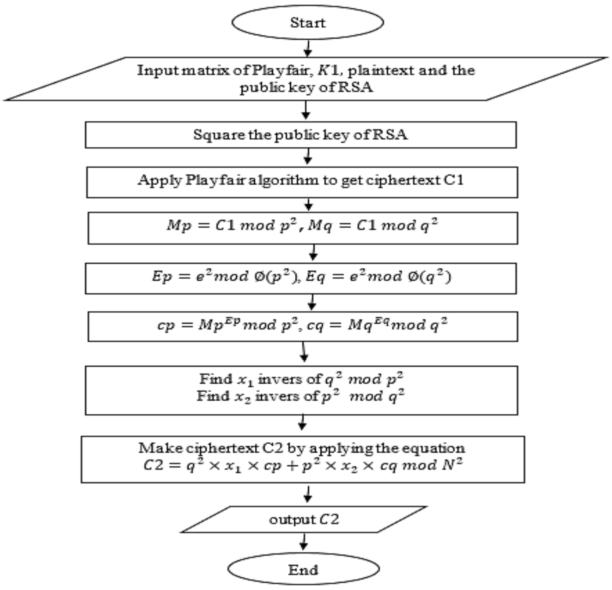

Figure 3. The diagram of HRSASQ-CRT encryption

The following pseudocodes show the encryption algorithms of HRSASQ and HRSASQ-CRT

Input:
- The key $K1$ of Playfair
- The matrix of Playfair 7 × 13 as shown in Table 1.
- Public key (e, N)
- The plaintext M

Hybrid encryption method:
- Apply the Playfair key K1 on the modified Playfair matrix to create the key matrix as shown in
- Table 2
- Split the plaintext M into the blocks of two characters. If two characters are the same then add W and If the character at the final set is single, add the character "Q".
- Find the first ciphertext $C1$ by applying Playfair algorithm
- Square the public key
- Applying RSASQ for C1 to get $C2$
- $C2 \equiv C1^{e^2} mod \ N^2$

Output:

Input:
- The key $K1$ of Playfair
- The matrix of Playfair 7 × 13 as shown in Table 1.
- Public key (e, N)
- The plaintext M

Hybrid encryption method:
- Apply the Playfair key K1 on the modified Playfair matrix to create the key matrix as shown in
- Table 2
- Split the plaintext M into the blocks of two characters. If two characters are the same then add W and If the character at the final set is single, add the character "Q".
- Find the first ciphertext $C1$ by applying Playfair algorithm
- Square the public key
- Applying RSASQ-CRT for C1: Compute $Cp \equiv C1 \ mod \ p^2$,$Cq \equiv C1 \ mod \ q^2$
- $E_p \equiv e^2 \ mod \ \emptyset \ (p^2), Eq \equiv e^2 \ mod \ \emptyset \ (q^2)$
- $Mp \equiv (C_p)^{E_p} \ mod \ p^2, \ Mq \equiv (C_q)^{E_q} \ mod \ q^2$
- Find $x_1$such that $x_1 q^2 \equiv 1 \ mod \ p^2$. Find x_2 $, x_2 p^2 \equiv 1 \ mod \ q^2$
- $C2 \equiv (q^2 \times Cp \times x_1 + p^2 \times Cq \times x_2) \ mod \ N^2$

Output:

Steps of Decryption of the Proposed Hybrid Cryptosystems:

Step 1: Alice received $C2$ from Bob. Decrypt $C2$ to get $C1$ by using the private key $(d2, N^2)$ as follows:

In SRASQ

$C1 \equiv C2^{d2} \ mod \ N^2$

In RSASQ-CRT

$Cp \equiv \mathrm{C2} \ mod \ N^2 \ , Cq \equiv C2 \ mod \ \mathrm{N}^2$

$D_p \equiv d2 \ mod \ \emptyset \ (p^2) \ \ ,Dq \equiv d2 \ \ mod \ \emptyset \ (q^2)$

$Mp \equiv (C_p)^{D_p} \ mod \ p^2, Mq \equiv (C_q)^{D_q} \ mod \ q^2$

$C1 \equiv (q^2 \times Mp \times x_1 + p^2 \times Mq \times x_2) \ mod \ N^2$

Step 2: Create the key matrix 7 × 13 as shown in Table 2 by using the secret key $K1$.

Step 3: Utilize the same operations of Playfair cipher of encryption algorithm for C1 but in converse to get the final plaintext M.

Figs 4 and 5 show the block diagrams of decryption algorithm of two proposed cryptosystems.

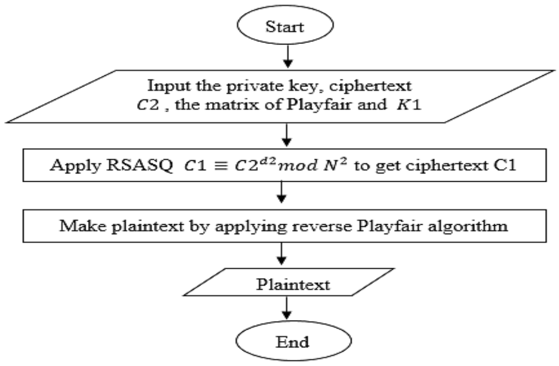

Figure 4. The diagram of HRSASQ decryption

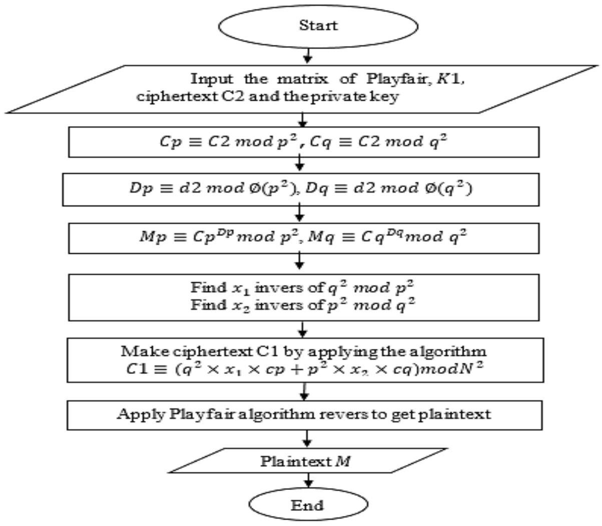

Figure 5. The diagram of HRSASQ-CRT decryption

The following pseudocodes show the decryption algorithms of HRSASQ and HRSASQ-CRT.

Input:
- The key $K1$ of Playfair ($K1_{1\times 12}$)
- The matrix of Playfair 7 × 13 as shown in Table 1.
- Private key $(d2, N^2)$
- The ciphrtext $C2$

Hybrid decryption method:
- Using private key to decrypt $C2$ as follows :
- $C1 = \mathrm{C2}^{\mathrm{d2}} \ mod \ N^2$
- Create the key matrix 7 × 13 as shown in
- Table 2 by using the key $K1$.
- Utilize the same operations of Playfair cipher of encryption algorithm for $C1$ but in converse to get the final plaintext M

Output:
- plaintext M

Input:

- The key $K1$ of Playfair ($K1_{1\times12}$)
- The matrix of Playfair 7 × 13 as shown in Table 1.
- Table 1Private key $(d2, N^2)$
- The ciphrtext $C2$

Hybrid decryption method:

- Using privet key to decrypt $C2$ as follows :
- $Cp \equiv C2 \, mod \, N^2$, $Cq \equiv C2 \, mod \, q^2$
- $D_p \equiv d2 \, mod \, \emptyset \, (p^2)$,$Dq \equiv d2 \; mod \, \emptyset \, (q^2)$
- $Mp \equiv (C_p)^{D_p} \, mod \, p^2$, $Mq \equiv (C_q)^{D_q} \, mod \, q^2$
- $C1 = (q^2 \times Mp \times x_1 + p^2 \times Mq \times x_2) \, mod \, N^2$
- Create the key matrix 7 × 13 as shown in
- Table 2 by using the key $K1$.
- Utilize the same operations of Playfair cipher of encryption algorithm for $C1$ but in converse to get the final plaintext M

For more explanation, the following example illustrates the encryption and decryption of HRSA-CRT

Key generation process at the receive

- First create the public and private key at the receiver, let $p = 101, q = 107$ then $N = p \times q = 10807$ and $\emptyset \, (N) = (p-1) \times (q-1) = 10600$, $p^2 = 10201$, $q^2 = 11449$ Compute $N^2 = p^2 \times q^2$ then $N^2 = 116791249$
- Choose e such that 1< e < ∅ (N) such that $gcd \, (e, \emptyset \, (N)) = 1$and hence $gcd \, (e^2 , \emptyset \, (N^2)) = 1$
- $\emptyset \, (N^2) = (p^2 - p) \times (q^2 - q)$ then $\emptyset \, (N^2) = 114554200$
- The public key is $(e \, , \, N) = (23{,}10807)$
- Use the secret exponent d2 as invers multiplication of e^2 mod $\emptyset \, (N^2)$ such that $e^2 d2 \equiv 1 (mod \, \phi \, (N^2 \,))$ Then d2=65830769

Encryption

- Let the plaintext (M) = University of Baghdad
- Let the key of Playfair (K1) = Mathematics
- Split M into a blocks of two characters M = Un iv er si ty space o fspace Ba gh da dQ
- Applying the key or Playfair on the Playfair matrix 7 ×13 as shown in Table 1
- **Find ciphertext $C1$ by encrypt the plaintext by applying Playfair algorithm using the key matrix as shown**

Table 2

- $\mathbf{C1 = n2sripAcCn{:}\, zj/CtVTAOg}$ equivalent to 41 56 46 45 36 43 2 30 4 41 83 53 37 90 4 47 23 4 21 2 61 43

Find the ciphertext $C2$ by using RSASQ-CRT encryption

- $Mp \equiv M \, mod \, p^2 \equiv$41 56 46 45 36 43 2 30 4 41 83 53 37 90 4 47 23 4 21 2 16 34
- $E_p \equiv e^2 \, mod \, \emptyset \, (p^2) \equiv 529$
- $Cp \equiv (M_p)^{E_p} \, mod \, p^2 \equiv$
7304 9216 6517 6439 390 6311 9755 10019 5097 7 4915 9217 4954 4888 5097 1144 4171 5097 2166 9755 7663 2677
- $Mq \equiv M \, mod \, q^2 \equiv$ 41 56 46 45 36 43 2 30 4 41 83 53 37 90 4 47 23 4 21 2 16 34
- $E_q \equiv e^2 \, mod \, \emptyset \, (q^2) \equiv 529$
- $Cq \equiv (C_{Mq})^{E_q} \, mod \, q^2 \equiv$
11389 4473 4929 1693 1073 11026 3478 48 40 6340 11389 1119 1175 1044 3468 6340 4963 4080 6340 7434 3478 9610 2332
- Find $x_1$such that $x_1 q^2 \equiv 1 \, mod \, p^2$. Find x_2 ,$x_2 p^2 \equiv 1 \, mod \, q^2$
- $x1 = 188$,$x2 = 11238$
- $C = (q^2 \times Mp \times x_1 + p^2 \times Mq \times x_2) mod \, N^2$
- $C =$
83543293 48055926 31088964 54510382 48189914 12227109 79699967 52177933 10756951
83543293 111960890 24593627 6962036 19856034 10756951 72122214 79082323 10756951 106643420 79699967 13748410 41836978

Decrypt $C2$

Get ciphertext C1 by using CRT - RSASQ decryption

- $Cp \equiv C_2 \, mod \, p^2 \equiv$ 7304 9216 6517 6439 390 6311 9755 10019 5097 7304 4915 9217 4954 4888 5097 1144 4171 5097 2166 9755 7663 2677
- $D_p \equiv D \, mod \, \emptyset \, (p^2) \equiv 9069$
- $Mp \equiv (C_p)^{D_p} \, mod \, p^2 \equiv$
41 56 46 45 36 43 2 30 4 41 83 53 37 90 4 47 23 4 21 2 16 34
- $Cq \equiv C_2 \, mod \, q^2 \equiv$ 11389 4473 4929 1693 1073 11026 3478 4840 6340 11389 1119 1175 1044 3468 6340 5963 4080 6340 7434 3478 9610 2332
- $D_q \equiv D \, mod \, \emptyset \, (q^2) \equiv 1801$
- $Mq \equiv (C_q)^{D_q} \, mod \, q^2 \equiv$
41 56 46 45 36 43 2 30 4 41 83 53 37 90 4 47 23 4 21 2 16 34
- $C1 = (q^2 \times Mp \times x_1 + p^2 \times Mq \times x_2) mod \, N^2$

$C =$ 41 56 46 45 36 43 2 30 4 41 83 53 37 90 4 47 23 4 21 2 16 34
$C1$ equivalent to n2sripAcCn: zj/CtVTAOg

Baghdad Science Journal
2024, 21(1): 151-160
P-ISSN: 2078-8665
E-ISSN: 2411-7986

- **Decryption $C1$ by Playfair algorithm to get the plaintext**
- M = University of Baghdad

Simulation Results

Various simulations are performed to test the performance of our proposed HRSASQ and HRSASQ-CRT. The simulation results of the processing time determined using Matlab 14a software with an 'Intel(R) Core(TM) i7-7600 CPU@ 2.80GHz 2.90 GHz' process.

In the symmetric layer, the modified Playfair algorithm utilized 7×13=91 characters that covered all the keyboard characters which are easy for users in comparison to some other modified Playfair[ref]. It expands the 5x5 matrix that using 25 characters. Moreover, the ciphertext of Playfair 7×13 is more protected against hackers in comparison to the 5×5 Playfair since the hacker must find in 7×13 =91 characters. Expanding the matrix causes the key size to be increased and hence reduces the probability to break the code. The chance to break the code in Playfair 5×5 is 1/26 = 0.0384 [15], while the likelihood to break the modified Playfair is 1/91=0.010989011.

In the asymmetric layer, the proposed RSASQ technique provides more security when benchmarked with the RSA algorithm which utilizes the public key directly. RSASQ depends on the square of the public key indicating that if the public key was hacked, it would be difficult to break it. The second proposed technique uses CRT enhance the speed and simplify complex computations. The computations can be reduced by using modulo, this reduces computation time.

shows that the encryption time of Table 3 RSASQ is about 3.03 times than RSA time in total. While the encryption time of our proposed RSASQ-CRT is about 0.5 of RSA encryption time and 0.17 of RSASQ encryption time in total. Figs 6 and 7 provide analysis diagrams of encryption time.

Table 4 shows the decryption time of RSASQ is about 8.3 times than RSA time in total. While the decryption time of the proposed RSASQ-CRT is about 0.3 of RSA decryption time and 0.03 of RSASQ decryption time in total. Figs 8 and 9 provide analysis diagrams of decryption time.

Table 3. Time table of encryption

Data \ Time	Time encryption of RSA	Time encryption of RSASQ	Time encryption of RSASQ- CRT
n≡41	0.0424	0.0732	0.0133
2≡56	0.0305	0.0928	0.0173
s≡46	0.0258	0.0568	0.0109
r≡45	0.0309	0.0651	0.0118
i≡36	0.0272	0.0629	0.014
p≡43	0.0173	0.0697	0.0108
A≡2	0.0182	0.07	0.012
c≡30	0.021	0.0629	0.0107
C≡4	0.0179	0.0823	0.0119
n=41	0.0287	0.0783	0.0152
:=83	0.0278	0.0622	0.0102
z=53	0.0193	0.066	0.0102
j=37	0.0166	0.0588	0.0089
/=90	0.0169	0.0602	0.0103
C=4	0.0179	0.0823	0.0119
t=47	0.0184	0.048	0.0134
V=23	0.0159	0.0514	0.0104
C=4	0.0179	0.0823	0.0119
T=21	0.0187	0.0612	0.0087
A≡2	0.0182	0.07	0.012
O=16	0.0198	0.0653	0.0112
g=34	0.0206	0.0546	0.0108
sum	0.4879	1.4763	0.2578

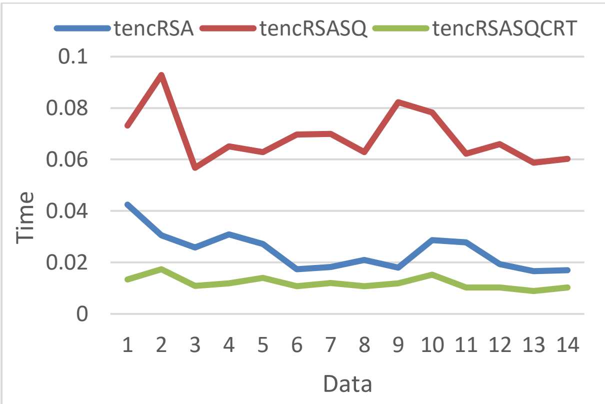

Figure 6. Data of encryption

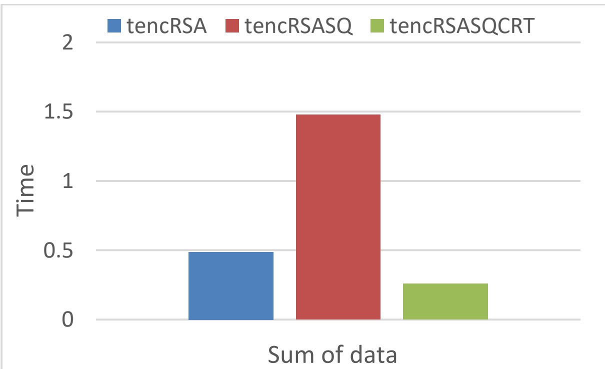

Figure 7. Sum data of encryption

Table 4. Time table of decryption

Time / Data	Time Decryption of RSA	Time decryption of RSASQ	Time decryption of RSA– CRT
n=41	0.0129	0.124	0.0052
2=56	0.014	0.0824	0.0044
s=46	0.0176	0.1113	0.0048
r=45	0.0259	0.136	0.0056
i=36	0.0223	0.1358	0.0065
p=43	0.0166	0.0977	0.005
A=2	0.0228	0.1327	0.0045
c=30	0.014	0.1198	0.0081
C=4	0.0138	0.0984	0.0059
n=41	0.0136	0.0836	0.0041
:=83	0.0161	0.0862	0.0038
z=53	0.0149	0.874	0.0043
j=37	0.0157	0.0957	0.0051
/=90	0.0143	0.0896	0.0049
C=4	0.0138	0.0984	0.0059
t=47	0.0052	0.0876	0.0052
V=23	0.0179	0.0964	0.0047
C=4	0.0138	0.0984	0.0059
T=21	0.0187	0.01142	0.0058
A=2	0.0166	0.0977	0.005
O=16	0.0179	0.1032	0.004
g=34	0.0187	0.1089	0.0043
sum	0.3571	2.96922	0.113

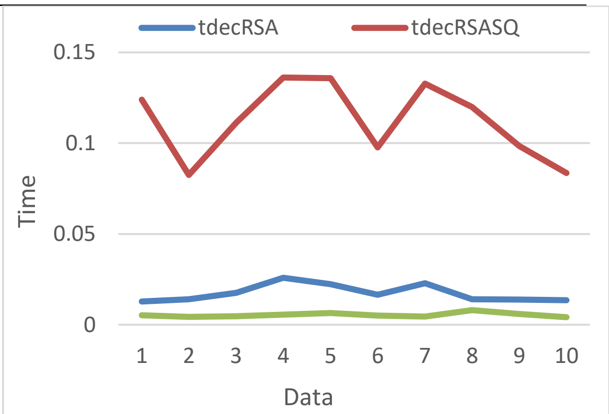

Figure 8. Data of decryption

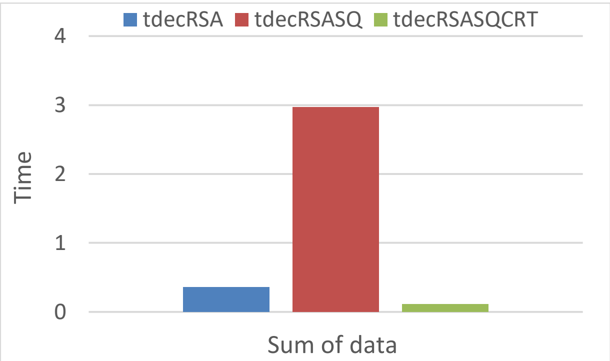

Figure 9. Sum data of decryption

Conclusion and Future works

In this work two hybrid cryptosystems have been proposed, that combine a modification of the symmetric cryptosystem Playfair cipher and two modifications of the asymmetric cryptosystem RSA. These proposed techniques depend on two layers of encryption and decryption.

Our extensive research and simulation results showed that the first layer modification of the symmetric cryptosystem Playfair improved the standard Playfair and gives more security. Moreover, the second layer for our proposed RSASQ and RSASQ-CRT is more secure when benchmarked with the original RSA algorithm. The complexity of the RSASQ algorithm was overcome by using CRT in RSASQ-CRT which gives the less computational time when benchmarked with the RSA and RSASQ.

The future works will overcome the limitation of RSASQ by using simplified equation instead of square to give less complexity such that Euler theorem can still be satisfied, for example square root can be taken especially the domain is positive. Moreover, using another symmetric cryptosystem in hybrid cryptosystem combined with the modified RSA.

Authors' Declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Baghdad.

Authors' Contributions Statement:

Z.A. A. and A. H. J contributed to the interpretation and review of the research, checking the results and verifying the validity of what was stated in the research. S. M. S. contributed in designing and implementing the research, analyzing the results and writing this manuscript. The authors discussed the results and contributed to the final manuscript.

References:

1. Din M, Pal SK, Muttoo SK, Madan S. A Hybrid Computational Intelligence-based Technique for Automatic Cryptanalysis of Playfair Ciphers. Def Sci J. 2020; 70(6): 612–618. http://dx.doi.org/10.14429/DSJ.70.15749
2. Somsuk K. A new methodology to find private key of RSA based on euler totient function. Baghdad Sci J. 2021; 18(2): 338–348. http://dx.doi.org/10.21123/bsj.2021.18.2.0338

3. Khudhair ZN, Nidhal A, El Abbadii NK. Text Multilevel Encryption Using New Key Exchange Protocol. Baghdad Sci J. 2022; 19(3): 619–630. http://dx.doi.org/10.21123/bsj.2022.19.3.0619
4. Ibraheem NA, Hasan MM. Combining several substitution cipher algorithms using circular queue data structure. Baghdad Sci J. 2020;17(4): 1320–1327. http://dx.doi.org/10.21123/bsj.2020.17.4.1320
5. Amalia Budiman MA, Sitepu R. File text security using Hybrid Cryptosystem with Playfair Cipher Algorithm and Knapsack Naccache-Stern Algorithm. J Phys. 2018; 978(1): 1–8. http://dx.doi.org/10.1088/1742-6596/978/1/012114
6. Sohail A, Wasiq K, Abir H. Phishing Attacks and Websites Classification Using Machine Learning and Multiple Datasets (A Comparative Analysis), Int Conf Comput. Springer. 2020; 12465: 301–313. http://dx.doi.org/10.1007/978-3-030-60796-8_26
7. Salih RK, Yousif MS. Hybrid encryption using playfair and RSA cryptosystems. Int J Nonlinear Anal Appl. 2021; 12(2): 2345–2350. http://dx.doi.org/10.22075/IJNAA.2021.5379
8. Hemanth PN, Abhinay Raja N, Yadav N. Secure message transfer using RSA algorithm and improved playfair cipher in cloud computing. 2nd Int Conf Converg Technol. (I2CT). IEEE. 2017; 931–936. http://dx.doi.org/10.1109/I2CT.2017.8226265
9. Chauhan SS, Singh H, Gurjar RN. Secure Key Exchange using RSA in Extended Playfair Cipher Technique. Int J Comput Appl. 2014; 104(15): 13–19. http://dx.doi.org/10.5120/18277-9180
10. Samir R, Abdulkader H, Hussein R. Improved RSA security using Chinese Remainder Theorem and Multiple Keys. Futur Comput Informatics J. 2019; 4(1): 1–9. http://dx.doi.org/10.54623/fue.fcij.4.1.1
11. Mathur SK, Srivastava S. Extended 16x16 Play-Fair Algorithm for Secure Key Exchange Using RSA Algorithm. Int J Futur Revolut Comput Sci Commun Eng. 2018; 4(2): 496–502. http://www.ijsir.in/images/pdf/paper9/paper12.pdf
12. Balaraman D, Veerasamy M, Balaji V. An Efficient Cryptosystem Using Playfair Cipher Together With Graph Labeling Techniques. J Phys. 2021; 1964(2): 1–15. http://dx.doi.org/10.1088/1742-6596/1964/2/022016
13. Sumarsono, Anshari M, Mujahidah A. Expending technique cryptography for plaintext messages by modifying playfair cipher algorithm with matrix 5 x 19. Int Conf Electr Eng Comput Sci. (ICECOS). IEEE. 2019: 10–13. http://dx.doi.org/10.1109/icecos47637.2019.8984560
14. Villafuerte RS, Sison AM, Medina RP. I3D-Playfair: An Improved 3D Playfair Cipher Algorithm. IEEE Eurasia Conf IOT, Commun Eng. IEEE. 2019; 538–541. http://dx.doi.org/10.1109/ECICE47484.2019.8942655
15. Challa RK, Gunta VK. A modified symmetric key fully homomorphic encryption scheme based on Read-Muller Code. Baghdad Sci J. 2021; 18(2): 899–906. http://dx.doi.org/10.21123/bsj.2021.18.2(Suppl.).0899
16. Yakub S, Gbolagade K. An improved rsa cryptosystem based on thread and crt. e-Academia . 2017; 6(2): 70–79. https://www.researchgate.net/publication/328430355
17. Zakariyau YB, Jibril LM, Usman AM, Garba A. Combined model of 9x9 Playfair and RSA for securing confidential information. J Comput Sci Appl. An Int J Niger Comput Soc. 2015; 22(12): 48–53. https://www.researchgate.net/publication/305766008
18. Iqbal Z, Gola KK, Gupta B, and Kandpal M. Dual level security for key exchange using modified RSA public key encryption in playfair technique. Int J Comput Appl. 2015; 111(13): 5–9. http://dx.doi.org/10.5120/19596-1408
19. Somsuk K. The new integer factorization algorithm based on Fermat's Factorization Algorithm and Euler's theorem. Int J Electr Comput Eng. 2020; 10(2): 1469–1476. http://dx.doi.org/10.11591/ijece.v10i2.pp1469-1476
20. Douglas RS, Maura BP. Cryptography Theory and Practice. fourth edi. Boca Raton: CRC Press, Taylor & Francis Group; 2018: 1–580. https://www.ic.unicamp.br/~rdahab/cursos/mo421-mc889/Welcome_files/Stinson-Paterson_CryptographyTheoryAndPractice-CRC%20Press%20%282019%29.pdf

أنظمة التشفير الهجينة المقترحة التي تعتمد على شفرة بلايفير المعدلة ونظام التشفير ار اس أي المعدل

سجى محمد سهيل [1]　　زينب أنور احمد [1]　　عبير جعفر حسين [2]

1 قسم الرياضيات، كلية العلوم للبنات، جامعة بغداد، بغداد، العراق.
2علوم الحاسوب والرياضيات ، جامعة ليفربول جون مورس ، ليفربول ، المملكة المتحدة
2 قسم الهندسة الكهربائية ، كلية الهندسة ، جامعة الشارقة ، الشارقة الإمارات العربية المتحدة

الخلاصة:

امان النص المشفر أصبح خطوة مهمة في نقل المعلومات المهمة عبر الشبكات. تلعب خوارزميات التشفير دورا رئيسيا في توفير الأمان وتجنب هجمات القراصنة. في هذا البحث، تم اقتراح نظامي تشفير هجينين يجمعان بين نظامي التشفير المتماثل المعدل بلايفير والذي يسمى شفرة بلايفير المعدلة ونظامي التشفير غير المتماثل المعدل الذي يسمى تقنية مربع *RSA* وتقنية مربع *RSA* مع نظرية البواقي الصينية. أنظمة التشفير الهجينة المقترحة لها طبقتان من التشفير وفك التشفير. في الطبقة الأولى، يتم تشفير النص العادي باستخدام بلايفير المعدل للحصول على النص المشفر وسيتم تشفير هذا النص باستخدام *RSA* التربيعي للحصول على نص التشفير النهائي. حققت هذه الخوارزمية أمانًا أعلى للبيانات ولكنها تعاني من وقت حسابي طويل. لذلك تم استخدام نظرية البواقي الصينية في نظام التشفير الهجين الثاني للحصول على وقت أقل للتشفير وفك التشفير. أشارت نتائج المحاكاة إلى أن استخدام بلايفير المعدل مع المربع المقترح *RSA* قد أدى إلى تحسين الأمان. علاوة على ذلك، فإن استخدام نظرية البواقي الصينية حقق وقتًا أقل للتشفير وفك التشفير مقارنةً بالخوارزميات المقترحة الأولى والخوارزميات القياسية.

الكلمات المفتاحية: النص المشفر، نظرية البواقي الصينية، نظام التشفير، النص العادي، شفرة بلايفير، المفتاح الخاص والعام، شفرة *RSA*.