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

Saja Mohammed Suhael1*  Zaynab Anwer Ahmed1 Abir Jaafer Hussain2

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

*Corresponding author: saja.mohammed1203a@csw.uobaghdad.edu.iq
E-mails addresses: zainaba_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

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 receiver1.2 The idea of RSA cryptosystem that it is easy to multiply two large prime numbers and it is extremely difficult to factorize their product.
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 algorithm4–5.

The third type is a hybrid cryptosystem that combines symmetric and asymmetric to provide high security and more complexity against hackers6.

There are lots of hybrid cryptography methods that combine the Playfair cipher with the RSA cryptosystem technique7–9. 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 overcome, this problem proposed the use of CRT 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 185410. 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 character11. 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 duplicate12,13. Reviser, Shamir, and Ad leman described an asymmetric RSA algorithm at the Massachusetts Institute of Technology14,15. RSA cryptosystem relies on Euler’s theorem and the existence of unique inverse to the integer that are relatively prime to the modulo16, 17. Modified RSA by using CRT has been proposed by Samir et al. in18 to decrease the time of RSA cipher.

There are lots of hybrid cryptography methods that combine RSA and Playfair cryptosystem techniques7–9. 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 complexity15. They can be classified into four types. In 2021, Salih and Yousif7 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 Srivastava11 in 2014, 2015 and 2017 respectively suggested hybrid cryptography that encrypts plaintext by Playfair and encrypts the key of Playfair by RSA. In 2017, Naga8 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.
The steps to generate public and private keys of RSASQ and RSASQ-CRT are as follows:

Step 1: Select two prime numbers 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.

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 \((\text{gcd}(e^2, \phi(N^2)) = 1)\).

Step 4: Find the secret exponent \( d_2 \) which is unique multiplication invers of \( e^2 \mod \phi(N^2) \) \( (e^2 \mod \phi(N^2)) \) has a unique solution which is the multiplicative inverse of \( e^2 \) modulo \( \phi(N^2) \) \( (\text{see the corollary off theorem (A.2.73) in}^{20}) \). Then \( (d_2, N^2) \) 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.

---

**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>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
<tr>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
<td>g</td>
<td>h</td>
<td>i</td>
<td>j</td>
<td>k</td>
<td>l</td>
<td>m</td>
</tr>
<tr>
<td>n</td>
<td>o</td>
<td>p</td>
<td>q</td>
<td>r</td>
<td>s</td>
<td>t</td>
<td>u</td>
<td>v</td>
<td>w</td>
<td>x</td>
<td>y</td>
<td>z</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td>!</td>
<td>@</td>
<td>#</td>
<td>$</td>
<td>%</td>
<td>^</td>
<td>&amp;</td>
<td>*</td>
<td>(</td>
<td>)</td>
<td>_</td>
<td>+</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>M</th>
<th>a</th>
<th>t</th>
<th>h</th>
<th>e</th>
<th>m</th>
<th>i</th>
<th>C</th>
<th>S</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td>J</td>
<td>K</td>
<td>L</td>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
</tr>
<tr>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
<td>b</td>
<td>d</td>
<td>f</td>
<td>g</td>
<td>j</td>
</tr>
<tr>
<td>k</td>
<td>l</td>
<td>n</td>
<td>o</td>
<td>p</td>
<td>q</td>
<td>r</td>
<td>u</td>
<td>v</td>
<td>w</td>
<td>x</td>
<td>y</td>
<td>z</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td>!</td>
<td>@</td>
<td>#</td>
<td>$</td>
<td>%</td>
<td>^</td>
<td>&amp;</td>
<td>*</td>
<td>(</td>
<td>)</td>
<td>_</td>
<td>+</td>
</tr>
</tbody>
</table>

---

Figure 1. The diagram of RSASQ and RSASQ-CRT algorithms
Step 3: The plaintext M splits into 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

\( Cp \equiv C1 \mod p^2, Cq \equiv C1 \mod q^2 \)

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

\( M_p \equiv (C_p)^{E_p} \mod p^2, M_q \equiv (C_q)^{E_q} \mod q^2 \)

Find \( x_1 \) such that \( x_1 q^2 \equiv 1 \mod p^2 \). Find \( x_2 \) 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**

**Input:**
- The key \( K1 \) of Playfair
- The matrix of Playfair 7 \times 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:**
- Ciphertext \( (C2) \)
Steps of Decryption of the Proposed Hybrid Cryptosystems:

Step 1: Alice received $C_2$ from Bob. Decrypt $C_2$ to get $C_1$ by using the private key $(d_2, N)$ as follows:

**In SRASQ**

$$C_1 \equiv C_2^{d_2} \mod N^2$$

**In SRASQ-CRT**

$$\begin{align*}
C_p &\equiv C_2 \mod N^2, \\
C_q &\equiv C_2 \mod N^2 \\
D_p &\equiv d_2 \mod \phi(p^2), \\
D_q &\equiv d_2 \mod \phi(q^2) \\
M_p &\equiv (C_p)^{D_p} \mod p^2, \\
M_q &\equiv (C_q)^{D_q} \mod q^2 \\
C_1 &\equiv (q^2 \times M_p \times x_1 + p^2 \times M_q \times x_2) \mod N^2
\end{align*}$$

Step 2: Create the key matrix $7 \times 13$ as shown in Table 2 by using the key $K_1$.

Step 3: Utilize the same operations of Playfair cipher of encryption algorithm for $C_1$ but in converse to get the final plaintext $M$.

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

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

**Input:**
- The key $K_1$ of Playfair
- The matrix of Playfair $7 \times 13$ as shown in Table 1.
- Public key $(e, N)$
- The plaintext $M$

**Hybrid decryption method:**
- Using private key to decrypt $C_2$ as follows:
  - $C_1 = C_2^{d_2} \mod N^2$
  - Create the key matrix $7 \times 13$ as shown in Table 2 by using the key $K_1$.
  - Utilize the same operations of Playfair cipher of encryption algorithm for $C_1$ 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 $7 \times 13$ as shown in Table 1
- Private key $(d2, N^2)$
- The ciphertext $C2$

Hybrid decryption method:
- Using privet key to decrypt $C2$ as follows:
  - $Cp \equiv C2 \mod N^2$, $Cq \equiv C2 \mod q^2$
  - $Dp \equiv d2 \mod \emptyset (p^2)$, $Dq \equiv d2 \mod \emptyset (q^2)$
  - $Mp \equiv (Cp)^{Dp} \mod p^2$, $Mq \equiv (Cq)^{Dq} \mod q^2$
  - $C1 = (q^2 \times Mp \times x_1 + p^2 \times Mq \times x_2) \mod N^2$
- Create the key matrix $7 \times 13$ 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 $M$
- 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.

Table 3 shows that the encryption time of 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 4. Time table of decryption

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

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:

2. Somsuk K. A new methodology to find private key of

 Analyzer التشفير الهجينة المقترحة التي تعتمد على شفرة بلايفير المعدلة ونظام التشغيل أرس أى المعدل

 زييض أتور أحمد 1
 سجي محمد سيهين 2

1 قسم الرياضيات، كلية العلوم للبنات، جامعة بغداد، بغداد، العراق
2 قسم عموم الرياضيات، كلية ليفربول على مورس، ليفربول، المملكة المتحدة
3 قسم الهندسة الكهربائية، كلية الهندسة، جامعة الشارقة، الإمارات العربية المتحدة
4 قسم الرياضيات، كلية العلوم للبنات، جامعة بغداد، بغداد، العراق
5 قسم الرياضيات، كلية ليفربول على مورس، ليفربول، المملكة المتحدة
الخلاصة:
امان النص المشفر أصبح خطوة مهمة في نقل المعلومات المهمة عبر الشبكات. تلعب خوارزميات التشفير دوراً رئيسيًا في توفير الأمان وتجنب هجمات القرصنة. في هذا البحث، تم اقتراح نظامي تشفير هجينين يجمعان بين نظامي التشفير المتماثل المعدل بلايفير والذي يسمى شفرة بلايفير المعدل ونظام التشفر غير المتماثل المعدل ويسمى تقنية مربع RSA، وأنظمة التشفير الهجينية المُقترحة لها طبقتين من التشفر وفك التشفر. في الطبقة الأولى، يتم تشغيل النص العادي باستخدام شفرة بلايفير المعدل RSA للحصول على النص المشفر، وسنتبع تشفير هذا النص باستخدام تقنية مربع RSA التتربيعي للحصول على نص التشفر النهائي. حققت هذه الخوارزمية أمانًا أعلى للبيانات ولكنها تعاني من وقت حسابي طويل. لذلك تم استخدام نظرية البواقي الصينية في نظام التشفير الهجيني الثاني للحصول على وقت أقل للتشفر وفك التشفر. أشارت نتائج المحاكاة إلى أن استخدام نظرية البواقي الصينية في نظام التشفير المعديل مع المربع المُقترح قد أدى إلى تحسين أمان. علاوة على ذلك، فإن استخدام نظام التشفر الصينية حقق وقتًا أقل للتشفر وفك التشفر مقارنةً بالخوارزميات المُقترحة الأولى والخوارزميات التقاسية.

الكلمات المفتاحية: النص المشفر، نظرية البواقي الصينية، نظام التشفر، النص العادي، شفرة بلايفير، المفتاح الخاص والعامة، شفرة RSA.