SOME TECHNIQUE ALGORITHMS OF CLASSICAL CRYPTOSYSTEMS USING RESIDUE MODULO PRIME NUMBER

Dr. P. Sundarayya
Department of Mathematics
GITAM University, Visakhapatnam, Andhra Pradesh, India

M. G. Vara Prasad
Department of Mathematics
NSRIT, Visakhapatnam Andhra Pradesh, India

P. Pari Purna Chari
Department of Mathematics
NSRIT, Visakhapatnam Andhra Pradesh, India

Abstract—The paper discusses about some classical techniques to introduce some strength to these classical encryption and decryption process. For that purpose focused on classical encryption with some techniques using residue modulo prime. The proposed method shown that it is better in terms of providing more security to given text message but it will be more difficult for the attacker to get the key using modulation of prime numbers.

Keywords—Encryption algorithm, Decryption algorithm, Residue modulo prime

I. INTRODUCTION

Cryptography is the mathematical science of writing or solving ciphers. A cipher is a mathematical secret code used in cryptography, the process of convert a plaintext into cipher text is called encryption and reverse process is called decryption. Cryptography is branch of both mathematics and computer science and it is mathematical function of ciphers included drawing from computer science and number theory. A Cipher is a mathematical function which is used in encryption and decryption algorithms. A Cipher can be divided into Symmetric cipher and Asymmetric Cipher. Symmetric Cipher is also called as a public key cryptography and Asymmetric Cipher is also called as a public key cryptography. A Symmetric Cipher can be divided into stream cipher and block cipher. Stream cipher can break the plain text messages into successive characters or bits p1,p2,p3…………. And encrypt each pk with ith element ki of a key stream K=k1k2k3…………..that is ek(p)=ek1(p1)ek2(p2)………….. Symmetric key cryptography is a classical cryptography. It is divided into four parts.

- The encryption algorithm: The encryption algorithm fulfills various transformations on the plain text.
- The decryption algorithm: The decryption algorithm fulfills various transformations on the cipher text.
- The decryption key: The decryption key is input to the decryption algorithm.
- The decryption key: The decryption key is input to the decryption algorithm.

In the symmetric key algorithm authentication and confidentiality are the same because the sender and receiver knows secret keys, the sender sent messages to receiver using secret key and receiver will open the messages using secret key. In this paper we discuss about similar technique of linear cipher and affine cipher. The Proposed method showed that it is better in terms of providing more security to given text message but it will be more difficult for the attacker to get the key using modulation of prime numbers.

II. PRELIMINARIES

P is finite set of possible plain text
C is finite set of possible cipher text
K is finite set of possible keys

For Key k ∈ K, there is encryption e_k: P → C, decryption d_k: C→ P such that d_k(e_k(x))=x for every plaintext x∈ P [1].

A. Linear (transformation) cipher-

In linear cipher , the cipher text is to be getting from the plain text .Let P=C=Z_m and K={a}, Key a∈ K ,where Z_m is ring of integers and m>1. Define encryption e_k(x)=a x(mod m) and decryption d_k(y)=-a^-1 x(mod m )[1].

B. Affine cipher-

Let P=C=Z_m and K={(a, b)}, Key k=(a, b)∈ K ,where Z_m is ring of integers and m>1. Define encryption e_k(x)=(a x +b)(mod m) and decryption d_k(y)= a^-1 (y-b) (mod m)[1].
III. PROPOSED WORK

A. Computational requirements-

Linear congruence in one variable-

A congruence of a form \( ax \equiv b \pmod{m} \), where ‘x’ is an unknown integer is called linear congruence in one variable

Inverse of a modulo prime number q-

Given an integer \( a \) with \( (a,q)=1 \), a solution of \( ax \equiv 1 \pmod{q} \) is called Inverse of \( a \) modulo prime number \( q \).

B. Proposed technique#1-

Let \( P=C=Z \)

Let \( K=\{(a,b,c,d) / \text{ad-bc \neq 0, g.c.d}(cx+d,q)=1, \text{g.c.d}((cy-a),q)=1 \} \).

Where \( q \) is prime number, for all \( x, y \in Z_q \).

Encryption: \( e_c(x) = \frac{ax+b}{cx+d} \pmod{q} \)

Decryption: \( d_c(y) = \frac{-dy+b}{cy-a} \pmod{q} \)

For all \( x, y \in Z_q \)

C. Encryption algorithm of proposed technique#1-

- step1: Choose \( a, b, c, d \) so that \( \text{g.c.d}(cx+d,q) = 1, \text{g.c.d}((cy-a),q) = 1 \) for all \( x, y, a, b, c, d \in Z_q \). Where \( q \) is prime number
- step2: Write \( \frac{ax+b}{cx+d} = (ax+b)(cx+d)^{-1} \)
- step3: Calculate \( (cx+d)^{-1} \)
- step4: Calculate \( e_c(x) = (ax+b)(cx+d)^{-1} \pmod{q} \)
- step5: Write Cipher text

Where \( q \) is prime number, for all \( x, y \in Z_q \)

D. Decryption algorithm of proposed technique#1-

- step1: Write \( \frac{-dy+b}{cy-a} = (-dy+b)(cy-a)^{-1} \)
- step2: Calculate \( (cy-a)^{-1} \)
- step3: Calculate \( d_c(y) = (-dy+b)(cy-a)^{-1} \pmod{q} \)
- step4: Write Plain text

E. Tables

<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>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
<th>!</th>
<th>?</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
</tr>
</tbody>
</table>

Table-1

The letters corresponding 29 letters where \( q=29 \) is prime number

<table>
<thead>
<tr>
<th>x \pmod{29}</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 \pmod{29}</td>
<td>1</td>
<td>15</td>
<td>10</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>25</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>x \pmod{29}</td>
<td>10</td>
<td>1</td>
<td>12</td>
<td>13</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>2 \pmod{29}</td>
<td>3</td>
<td>8</td>
<td>17</td>
<td>9</td>
<td>27</td>
<td>2</td>
<td>20</td>
<td>12</td>
<td>21</td>
</tr>
<tr>
<td>x \pmod{29}</td>
<td>9</td>
<td>19</td>
<td>2</td>
<td>21</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>20</td>
<td>12</td>
</tr>
</tbody>
</table>

Table-2

Multiplicative inverse modulo 29

<table>
<thead>
<tr>
<th>x \pmod{29}</th>
<th>9</th>
<th>19</th>
<th>2</th>
<th>21</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>20</th>
<th>12</th>
<th>21</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>6</td>
<td>16</td>
<td>18</td>
<td>4</td>
<td>24</td>
<td>23</td>
<td>7</td>
<td>19</td>
<td>14</td>
<td>28</td>
</tr>
</tbody>
</table>

Table-3

The letters corresponding 37 letters where \( q=37 \) prime

<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>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>K</td>
<td>L</td>
<td>M</td>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
<td>SPACE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>SPACE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
<td>40</td>
</tr>
</tbody>
</table>

Table-4

Multiplicative inverse modulo 37

<table>
<thead>
<tr>
<th>X</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>1\pmod{37}</td>
<td>1</td>
<td>19</td>
<td>25</td>
<td>28</td>
<td>15</td>
<td>31</td>
<td>16</td>
<td>14</td>
<td>33</td>
</tr>
<tr>
<td>X</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>2\pmod{37}</td>
<td>26</td>
<td>27</td>
<td>34</td>
<td>20</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>24</td>
<td>35</td>
</tr>
<tr>
<td>X</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>3\pmod{37}</td>
<td>26</td>
<td>27</td>
<td>34</td>
<td>20</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>24</td>
<td>35</td>
</tr>
<tr>
<td>X</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>4\pmod{37}</td>
<td>4</td>
<td>23</td>
<td>21</td>
<td>6</td>
<td>22</td>
<td>9</td>
<td>12</td>
<td>18</td>
<td>36</td>
</tr>
</tbody>
</table>
F. Example of Proposed technique#1

Plain text="YEAR 2016"

From the table-3 assigning labels to YEAR 2016

<table>
<thead>
<tr>
<th>Y</th>
<th>E</th>
<th>A</th>
<th>R</th>
<th>SPACE</th>
<th>2</th>
<th>0</th>
<th>1</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>5</td>
<td>1</td>
<td>18</td>
<td>37</td>
<td>29</td>
<td>27</td>
<td>28</td>
<td>33</td>
</tr>
</tbody>
</table>

Encryption:

Choose \(a, b, c, d\) so that \(\gcd((cx+d),q)=1, \gcd((cy-a),q)=1\) for all \(x, y, a, b, d \in \mathbb{Z}_q\)

Choose \(q=37. a=2, b=5, c=3, d=3, \) ad-bc \(\neq 0\)

\(\gcd((3x+3),37)=1, \gcd((3y-2),37)=1\) for all \(x, y \in \mathbb{Z}_{37}\)

\[e_k(25)=\frac{2(25)+5}{3(25)+3} = (55)\mod 37 = (18)(4)^{-1}\mod 37 = (18)(28)(\mod 37)= 23\]

\[e_k(5)=\frac{2(5)+5}{3(5)+3} = (15)(18)^{-1}\mod 37 = 7\]

\[e_k(1)=\frac{2(1)+5}{3(1)+3} = (7)(6)^{-1}\mod 37 = 32\]

\[e_k(18)=\frac{2(18)+5}{3(18)+3} = (40)(20)^{-1}\mod 37 = 15\]

\[e_k(37)=\frac{2(37)+5}{3(37)+3} = (20)(20)^{-1}\mod 37 = 14\]

\[e_k(29)=\frac{2(29)+5}{3(29)+3} = (26)(16)^{-1}\mod 37 = 34\]

\[e_k(27)=\frac{2(27)+5}{3(27)+3} = (22)(10)^{-1}\mod 37 = 17\]

\[e_k(28)=\frac{2(28)+5}{3(28)+3} = (24)(13)^{-1}\mod 37 = 36\]

\[e_k(33)=\frac{2(33)+5}{3(33)+3} = (34)(28)^{-1}\mod 37 = 25\]

\[
\begin{array}{cccccccc}
23 & 7 & 32 & 15 & 14 & 34 & 17 & 36 & 25 \\
W & G & S & O & N & 7 & Q & 9 & Y \\
\end{array}
\]

Cipher text="WG5ON7Q9Y"

G. Proposed technique#2

Let \(P=C=\mathbb{Z}_q\)

\(K=\{(a,b,c,d,e) | ad-bc \neq 0, \gcd((cx+d),q)=1, \gcd((cy-a),q)=1\}\)

\(a, b, c, d, e \in \mathbb{Z}_q\)

Encryption: \(e_k(x)= (\frac{ax+b}{cx+d} + e)\mod q\)

Decryption: \(d_k(y)= (\frac{-d(y-e)+b}{c(y-a)-a})\mod q\)

Where \(q\) is prime number, \(\text{for all } x, y \in \mathbb{Z}_q\)

H. Encryption algorithm of proposed technique#2

1. Choose \(a, b, c, d, e\) so that \(\gcd((cx+d),q)=1, \gcd((cy-a),q)=1\) for all \(x, y, a, b, d, e \in \mathbb{Z}_q\)
2. Write \(\frac{ax+b}{cx+d}\)
3. Calculate \((cx+d)^{-1}\)
4. Calculate \(e_k(x)= ((ax+b)(cx+d)^{-1}+e)\mod q\)
5. Write Cipher text
step1: Write $-\frac{dy+b}{cy-a}=(dy+b)(cy-a)^{-1}$
step2: Calculate $(cy-a)^{-1}$
step3: Calculate 
\[ d_k(y) = (-d(y-e) + b)(c(y-a) - a)^{-1}(mod \ q) \]
step4: Write plain text

I. Example of Proposed technique#2-

Plain text=ÝES

From the Table-1 assigning labels to YE

<table>
<thead>
<tr>
<th>Y</th>
<th>E</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>5</td>
<td>19</td>
</tr>
</tbody>
</table>

Encryption:

Choose $a, b, c, d, e$ so that $g.c.d \left( (cx + d), q \right) = 1$, $g.c.d \left( (cy - a), q \right) = 1$ for all $x, y, a, b, d, e \in \mathbb{Z}_q$

Choose $q = 29$, $a = 6$, $b = 1$, $c = 6$, $d = 5$, $ad - b = 24$

\[ e_1(25) = 6(25) + 1 \equiv 5 \pmod{29} \]
\[ e_1(5) = 6(5) + 1 \equiv 5 \pmod{29} \]
\[ e_1(19) = 6(19) + 1 \equiv 5 \pmod{29} \]

\[
\begin{array}{c|c|c|c}
23 & 15 & 24 \\
W & O & X \\
\end{array}
\]

Cipher text="WOX"

Decryption:

\[ d_k(23) = -\frac{5(23-5) + 1}{6(23-5) - 6} = 23 \]
\[ d_k(15) = -\frac{5(10) + 1}{6(10) - 6} = 5 \]
\[ d_k(24) = -\frac{5(19) + 1}{6(19) - 6} = 19 \]

Plain text=ÝES'

IV. SECURITY ANALYSIS

Proposed technique #1 consists four tuple keys so it is more secure whereas proposed technique #2 is more secure than Proposed technique #1 as it has five tuple keys but Proposed technique #1 and Proposed technique #2 must satisfy the following conditions

\[ g.c.d \left( cx + d, q \right) = 1 \quad \text{and} \quad (cy-a, q) = 1 \]

for all $x, y \in \mathbb{Z}_q$

As the two techniques satisfy above conditions then

These two techniques overcome the known plain text attack, chosen cipher text attack and chosen plain text attack.

V. CONCLUSION

This paper presents a classical cryptosystem that is variation of the linear cipher and the affine cipher because of proposed technique#1 has 4 tuple keys and proposed technique#2 has 5 tuple keys. The proposed algorithms providing some classical cryptosystems increasing its defiance to various attacks such as a known plain text attacks. The proposed algorithm is more secure in encryption and decryption under modulation prime numbers than original linear and affine cipher. Since the modulus is a prime number and the proposed key security greatly increased and the cipher text-only attack is also to oppose successfully.

VI.REFERENCE