Abstract—Pythagorean Triple Algorithm represents a genuine result of our work which has been theoretically and practically proven. Through the New Pythagorean Triple algorithm we can extend the definition of the Pythagorean Theorem which states that for any $p$ and $q$ (one of them is odd and the other even), there is only one fundamental solution $(x, y, z)$. Using the New Pythagorean Triple algorithm formulas, this definition can be re-stated to: for any numbers $p$ and $q$ (one of them is odd and the other even) there are at least two fundamental solutions $(x_1, y_1, z_1)$ and $(x_2, y_2, z_2)$, but there are also special cases when even three fundamental solutions are possible $(x_1, y_1, z_1), (x_2, y_2, z_2)$ and $(x_3, y_3, z_3)$. Based on these solutions we can easily create the encryption and decryption key that can be used in a simple symmetric cryptosystem.

Pythagorean triples, cryptography, symmetric cryptosystems

1 Introduction

A Pythagorean triple represent an ordered triple of the type $(x, y, z) \in \mathbb{Z}^3$ such that [9]:

$$x^2 + y^2 = z^2$$

The conventional way of interpretation of the above mentioned equation is that there is one solution $(x_1, y_1, z_1)$ to the aforementioned equation [6],[7],[8].

There are many ways of generating Pythagorean triples. One of the most known methods is the Euclids formula which is a fundamental formula for Pythagorean triples for given arbitrary pair of positive integers $p$ and $q$ where $p > q$. The formula states that the integers derived from Euclids formula as given below:

$$x = p^2 - q^2$$
$$y = 2pq$$
$$z = p^2 + q^2$$

represent a Pythagorean triple.

Another approach for generating Pythagorean triples lies in Newtons method which is based on the identity:

$$(p^2 - q^2)^2 + (2pq)^2 \equiv (p^2 + q^2)^2$$

From the identity it is clearly visible that integer solutions to the equation $x^2 + y^2 = z^2$ are of the form:

$$x = d(p^2 - q^2), y = 2dxy, z = d(p^2 + q^2)$$

with $p > q > 0$.

Where $(p, q) = 1$, $p$ and $q$ are of opposite parity (one even and one odd) and $(x, y, z) = d$. It can be also proved that every Pythagorean Triple can be written in this way so it is essentially useful to observe these $x$, $y$ and $z$ values. If $d = 1$ the triples are considered to be Primitive. In this paper we extend the above mentioned equations by at least one (in special cases by two) other solutions to Pythagorean Triples.

The rest of this paper is structured as follows: In section 2 we elaborate in detail the derivation of two new solutions to Pythagorean Triples, section 3 illustrates a symmetric cryptosystem based on the newly generated Pythagorean Triples and section 4 concludes this paper.

2 New Pythagorean Triple Algorithm

Let us have $x^2 + y^2 = z^2$ and $gcd(x, y) = 1$. There is a number $z$ so that:

$$\begin{cases} z = x + u \\ z = y + v \end{cases} \tag{1}$$

where $gcd(x, u) = 1$ and $gcd(y, v) = 1$. As a consequence, from the last system of equations, we have:

$$\begin{cases} x + u = y + v \\ x - v = y - u \end{cases}$$
Let us mark \( y - u = x - v = \lambda \), then:

\[
\begin{align*}
  x &= v + \lambda \\
  y &= u + \lambda \\
  z &= u + v + \lambda
\end{align*}
\]

If we replace \( x \) in equation 1 from 2 we get:

\[ z = u + v + \lambda \quad (3) \]

Equations 2 and 3 given as:

\[
\begin{align*}
  x &= v + \lambda \\
  y &= u + \lambda \\
  z &= u + v + \lambda
\end{align*}
\]

represent the new fundamental solutions to the Pythagorean theorem. If we replace these expressions in \( x^2 + y^2 = z^2 \) we will get:

\[(u + \lambda^2) + (v + \lambda^2) = (u + v + \lambda)^2\]

from which, after further extension, we have:

\[ \lambda^2 = 2uv \quad (5) \]

Values of \( v \) and \( u \) will be selected that way so that they determine \( \lambda \), out of which we derive the Pythagorean fundamental solutions:

\[
\begin{align*}
  v &= 2p^2 \\
  u &= q^2 \\
  \text{where } v > u, \gcd(p, q) = 1
\end{align*}
\]

If \( u \) and \( v \) are replaced in 5 we get:

\[ \lambda^2 = 4p^2q^2 \]

and then:

\[ \lambda = \pm 2pq \quad (7) \]

If now 6 and 7 are replaced in 4 we have:

\[
\begin{align*}
  x &= 2p^2 + 2pq \\
  y &= q^2 + 2pq \\
  z &= 2p^2 + q^2 + 2pq
\end{align*}
\]

From the conventional definition of Pythagorean triple, it results that only one fundamental solution \((x, y, z)\) exists for \( p \) and \( q \) (one of which is odd and the other even).

Based on 8, the previous definition is re-defined to: for any numbers \( p \) and \( q \) (one of which is odd and the other even) there are at least two fundamental solutions \((x_1, y_1, z_1)\) and \((x_2, y_2, z_2)\) which can be expressed in the form of New Pythagorean Triple formulas:

\[
\begin{align*}
  x_1 &= 2p^2 + 2pq \\
  y_1 &= q^2 + 2pq \\
  z_1 &= 2p^2 + q^2 + 2pq
\end{align*}
\]

\[
\begin{align*}
  x_2 &= 2p^2 - 2pq \\
  y_2 &= q^2 - 2pq \\
  z_2 &= 2p^2 + q^2 - 2pq
\end{align*}
\]

\[
\begin{align*}
  x_3 &= 2pq \\
  y_3 &= p^2 - q^2 \\
  z_3 &= p^2 + q^2
\end{align*}
\]

Table 1: New Pythagorean Triple Algorithm

<table>
<thead>
<tr>
<th></th>
<th>p</th>
<th>q</th>
<th>x1</th>
<th>y1</th>
<th>z1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td>24</td>
<td>7</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>3</td>
<td>80</td>
<td>39</td>
<td>89</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>2</td>
<td>126</td>
<td>32</td>
<td>130</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>4</td>
<td>154</td>
<td>72</td>
<td>170</td>
</tr>
<tr>
<td>5</td>
<td>p</td>
<td>q</td>
<td>x2</td>
<td>y2</td>
<td>z2</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td>12</td>
<td>-5</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>3</td>
<td>20</td>
<td>-21</td>
<td>29</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>2</td>
<td>70</td>
<td>-24</td>
<td>74</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>4</td>
<td>42</td>
<td>-40</td>
<td>58</td>
</tr>
<tr>
<td>6</td>
<td>p</td>
<td>q</td>
<td>x3</td>
<td>y3</td>
<td>z3</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>3</td>
<td>10</td>
<td>16</td>
<td>34</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>2</td>
<td>28</td>
<td>45</td>
<td>53</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>4</td>
<td>56</td>
<td>33</td>
<td>65</td>
</tr>
</tbody>
</table>

Table 2: The English Alphabet

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>h</td>
<td>i</td>
<td>j</td>
<td>k</td>
<td>l</td>
<td>m</td>
<td>n</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>o</td>
<td>p</td>
<td>q</td>
<td>r</td>
<td>s</td>
<td>t</td>
<td>u</td>
</tr>
<tr>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>v</td>
<td>w</td>
<td>x</td>
<td>y</td>
<td>z</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 Data Encryption and Decryption

We will now see how we can encrypt and decrypt a text by using the New Pythagorean Triple Algorithm formulas for creating the key. Let us mark with \( m \) the plaintext \([2],[3]\), whereas with \( k \) the key and with \( c \) encrypted message (ciphertext) \([1],[4],[5]\). If we want to encrypt a message, we will use the formula:

\[ c = m + k(\mod 26) \]

If we want to decrypt a message, we use:

\[ m = c - k(\mod 26) \]

Let us now show how the key is going to be created. Numbers \( p \) and \( q \) are put within the New Pythagorean
Triple Algorithm formulas given below to create the key.

After we have found the values:

\[ x_1 = 2p^2 + 2pq \]
\[ x_2 = 2p^2 - 2pq \]
\[ y_1 = q^2 + 2pq \]
\[ y_2 = q^2 - 2pq \]
\[ z_1 = 2p^2 + q^2 + 2pq \]
\[ z_2 = 2p^2 + q^2 - 2pq \]

\[ x_3 = 2pq \]
\[ y_3 = p^2 - q^2 \]
\[ z_3 = p^2 + q^2 \]

\[ (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3) \mod 26 \]

The message is now being converted into numbers. In order to convert each letter of the text into numbers, we use Table II. As a result, we get values as in Table 4. The person whom we want to send the encrypted message to, needs to have the pair of number \((p, q) = (5, 3)\). The received message can now be decrypted, by finding the key.

Based on the New Pythagorean Triple algorithm formulas, we find the key values:

\[ x_1 = 2 \cdot 5^2 + 2 \cdot 5 \cdot 3 = 80 \]
\[ y_1 = 3^2 + 2 \cdot 5 \cdot 3 = 39 \]
\[ z_1 = 2 \cdot 5^2 + 3^2 + 2 \cdot 5 \cdot 3 = 89 \]

\[ x_2 = 2 \cdot 5^2 - 2 \cdot 5 \cdot 3 = 20 \]
\[ y_2 = 3^2 - 2 \cdot 5 \cdot 3 = -21 \]
\[ z_2 = 2 \cdot 5^2 + 3^2 - 2 \cdot 5 \cdot 3 = 29 \]

\[ x_3 = 2 \cdot 5 \cdot 3 = 30 \]
\[ y_3 = 5^2 - 3^2 = 16 \]
\[ z_3 = 5^2 + 3^2 = 34 \]

After we have found these values:

\[ (80, 39, 89, 20, -21, 29, 30, 16, 34) \mod 26 \]

we get the key:

\[ (2, 13, 11, 20, 5, 3, 4, 16, 8) \]
The decrypted message is given as in table 5.

<table>
<thead>
<tr>
<th>U</th>
<th>B</th>
<th>F</th>
<th>N</th>
<th>M</th>
<th>H</th>
<th>E</th>
<th>I</th>
<th>B</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>15</td>
<td>18</td>
<td>14</td>
<td>20</td>
<td>19</td>
<td>19</td>
<td>17</td>
<td>4</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>13</td>
<td>11</td>
<td>20</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>16</td>
<td>8</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>18</td>
<td>14</td>
<td>20</td>
<td>19</td>
<td>17</td>
<td>4</td>
<td>0</td>
<td>18</td>
<td>19</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>s o u t h e a s t e u</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>I</td>
<td>U</td>
<td>H</td>
<td>E</td>
<td>D</td>
<td>C</td>
<td>P</td>
<td>V</td>
<td>G</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>20</td>
<td>7</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>15</td>
<td>21</td>
<td>6</td>
<td>24</td>
</tr>
<tr>
<td>11</td>
<td>20</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>16</td>
<td>8</td>
<td>2</td>
<td>13</td>
<td>11</td>
<td>20</td>
</tr>
<tr>
<td>17</td>
<td>14</td>
<td>15</td>
<td>4</td>
<td>0</td>
<td>13</td>
<td>20</td>
<td>13</td>
<td>8</td>
<td>21</td>
<td>4</td>
</tr>
<tr>
<td>r o p e e a n u n i v e</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>W</td>
<td>V</td>
<td>M</td>
<td>J</td>
<td>G</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>21</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>4</td>
<td>16</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>18</td>
<td>8</td>
<td>19</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r s i t y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 Conclusion

The aim of the New Pythagorean Triple algorithm is to extend the definition of the Pythagorean Theorem which says: For any numbers p and q (one of which is odd and the other even), there is only one fundamental solution \((x, y, z)\). On the other hand, based on the New Pythagorean Triple algorithm formulas, this definition is extended to: for any numbers \(p\) and \(q\) (one of which is odd and the other even) there are at least two fundamental solutions \((x_1, y_1, z_1)\) and \((x_2, y_2, z_2)\), but there are also some special cases when we can even get three fundamental solutions \((x_1, y_1, z_1), (x_2, y_2, z_2)\) and \((x_3, y_3, z_3)\). This algorithm can also be used for creating the key for data encryption and decryption.

References