Proceedings of the World Congress on Engineering 2014 Vol I,
WCE 2014, July 2 - 4, 2014, London, U.K.

Data Encryption and Decryption Using New Pythagorean Triple Algorithm

Artan Luma*† and Bujar Raufi ‡

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 $(x, y, z) \in Z^3$ 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:

$$\begin{cases} x + u = y + v \\ x - v = y - u \end{cases}$$

*Manuscript received January 14th, 2014; revised March 22, 2014.

†Artan Luma is with the Faculty of Contemporary Sciences and Technologies, South East European University, Ilindenska 335, 1200 Tetovo, Macedonia. e-mail: a.luma@seeu.edu.mk. Website: http://www.seeu.edu.mk/ã.luma

‡Bujar Raufi is with the Faculty of Contemporary Sciences and Technologies, South East European University, Ilindenska 335, 1200 Tetovo, Macedonia. e-mail: b.raufi@seeu.edu.mk. Website: http://www.seeu.edu.mk/b̃.raufi

Let us mark $y - u = x - v = \lambda$, then:

$$\begin{cases} x = v + \lambda \\ y = u + \lambda \end{cases} \tag{2}$$

If we replace x in equation 1 from 2 we get:

$$z = u + v + \lambda \tag{3}$$

Equations 2 and 3 given as:

$$\begin{cases} x = v + \lambda \\ y = u + \lambda \\ z = u + v + \lambda \end{cases} \tag{4}$$

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:

$$\lambda^2 = 2vu \tag{5}$$

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

$$\begin{cases} v = 2p^2 \\ u = q^2 \end{cases} , v > u, gcd(p, q) = 1 \tag{6}$$

If u and v are replaced in 5 we get:

$$\lambda^2 = 4p^2q^2$$

and then:

$$\lambda = \pm 2pq \tag{7}$$

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

$$\begin{cases} x = 2p^2 \pm 2pq \\ y = q^2 \pm 2pq \\ z = 2p^2 + q^2 \pm 2pq \end{cases} \tag{8}$$

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:

$$x_1 = 2p^2 + 2pq \qquad x_2 = 2p^2 - 2pq$$
$$y_1 = q^2 + 2pq \qquad y_2 = q^2 - 2pq$$
$$z_1 = 2p^2 + q^2 + 2pq \qquad z_2 = 2p^2 + q^2 - 2pq$$

There is a special case for numbers p and q, when we get three fundamental solutions:

$$x_3 = 2pq$$
$$y_3 = p^2 - q^2$$
$$z_3 = p^2 + q^2$$

A short list of solutions for the Pythagorean triples for values $(3, 1), (5, 3), (7, 2)$ and $(7, 4)$ is illustrated as in Table 1. Table 2 illustrates the number encodings of the English alphabet which will be used further on for encruption/decryption purposes. This will be elaborated in the following section.

Table 1: New Pythagorean Triple Algorithm

p	q	x_1	y_1	z_1
3	1	24	7	25
5	3	80	39	89
7	2	126	32	130
7	4	154	72	170
p	q	x_2	y_2	z_2
3	1	12	-5	13
5	3	20	-21	29
7	2	70	-24	74
7	4	42	-40	58
p	q	x_3	y_3	z_3
3	1	6	8	10
5	3	30	16	34
7	2	28	45	53
7	4	56	33	65

Table 2: The English Alphabet

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

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:

$$c = m + k(mod26)$$

If we want to decrypt a message, we use:

$$m = c - k(mod26)$$

Let us now show how the key is going to be created. Numbers p and q are put within the New Pythagorean

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Triple Algorithm formulas given below to create the key. After we have found the values:

$$x_1 = 2p^2 + 2pq \qquad x_2 = 2p^2 - 2pq$$
$$y_1 = q^2 + 2pq \qquad y_2 = q^2 - 2pq$$
$$z_1 = 2p^2 + q^2 + 2pq \qquad z_2 = 2p^2 + q^2 - 2pq$$

$$x_3 = 2pq$$
$$y_3 = p^2 - q^2$$
$$z_3 = p^2 + q^2$$

$$(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3)(mod 26)$$

We can freely create the encryption key in the form:

$$x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3$$

For example: If we have a plaintext, *South East European University* (as given in Table 3)

Table 3: Message encoding for the word "southeasteuropeanuniversity"

s	o	u	t	h	e	a	s	t	e	u
18	14	20	19	7	4	0	18	19	4	20
r	o	p	e	a	n	u	n	i	v	e
17	14	15	4	0	13	20	13	8	21	4
r	s	i	t	y						
17	18	8	19	24						

which we want to encrypt, we will have to use numbers $p = 5$ and $q = 3$, and use them in the New Pythagorean Triple algorithm formulas:

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

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

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

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 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

Table 4: Message Encryption

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

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:

$$(2, 13, 11, 20, 5, 3, 4, 16, 8)$$

Once the key has been created, it is quite easy to decrypt the encrypted message, by using the formula:

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$m = c - k(mod 26)$$

The decrypted message is given as in table 5.

Table 5: Message Decryption

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

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

[1] W. Trappe and L.C. Washington. "Introduction to cryptography: with coding theory". Saddle River, Pearson Prentice Hall. 2006.

[2] D.C. Hankerson, G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, and J.R. Wall. Coding Theory and Cryptography: The Essentials. Chapman & Hall. 2000

[3] B. Feng, R. Deng, and Z. Jianying. Public Key Cryptography - PKC 2004: 7th International Workshop on Practice and Theory in Public Key Cryptography. 2004. LNCS

[4] D. R. Stinson. "Cryptography: Theory and Practice". Chapman & Hall / CRC. 2002

[5] S. Vaudenay. "Public Key Cryptography - PKC 2005". In. 8th International Workshop on Theory and Practice in Public Key Cryptography. LNCS. Springer. 2005

[6] D. MacHale and C. van den Bosch. "Generalizing a result about Pythagorean triples", In J. Mathematical Gazette 96: pp. 9196. 2012

[7] F. Bernhart and H. L. Price. "Heron's formula, Descartes circles, and Pythagorean triangles". 2007. J. Number Theory

[8] J. Stillwell. "Pythagorean Triples", In Elements of Number Theory, Springer, pp. 110. 2002

[9] P.L. Clark. "Pythagorean Triples". Number Theory. 2009. http://math.uga.edu/ pete/numbertheory2009.html

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)