IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 12, Issue 1 Ver. III (Jan. - Feb. 2016), PP 04-06
www.iosrjournals.org

A New Approach to Public Key Transferring Algorithm Scheme Using Metric Space

Asha Rani[1], Kumari Jyoti[2]
Department of Mathematics, SRM University, Haryana, Sonepat- 131001, India

Abstract: *In this paper, we introduce a new algorithm for the public key transferring which is based upon functional analysis and metric spaces with basic properties of circles. Furthermore, we introduce an algorithm to make the changes in keys without meeting. The algorithms presented in this paper promises a high level of security as it uses metric distances, in spite of the large prime numbers used in the present algorithms. The security analysis of the new scheme is also discussed.*

I. Introduction

To send a message secretly is a great challenge for most of the armies and secret agencies. One of the very common techniques to send a secret message is public key transferring. RSA, Rabin, AlGamal, McEliece, Knapsack, and Probabilistic public key transferring are the common public key algorithms used in practice[1]. All of these algorithms in the present literature are based on large prime numbers or on a part of number theory. None of the pioneers have concentrated on the functional analysis or metric spaces. We introduce an algorithm which is based on the metric spaces and uses certain properties of balls in a metric space or circles.
In this paper, we have considered the Euclidean metric or 2- metric. In Euclidean metric a ball is same as a circle on a plane.

In present scenario, the hackers are always in the need to break the codes and the private keys can be guessed. So, it is always safe to change the keys frequently. In the last section of the paper we introduce an algorithm to make changes in the keys by using the same coding when meeting personally is not feasible.

II. Preliminaries

Definition 2.1[2]: Let X be a set and $d: X^2 \to R$ a function with the following properties:

(i) $d(x, y) \geq 0$ for all $x, y \in X$.
(ii) $d(x, y) = 0$ if and only if $x = y$.
(iii) $d(x, y) = d(y, x)$ for all $x, y \in X$.
(iv) $d(x, y) + d(y, z) \geq d(x, z)$ for all $x, y, z \in X$.

Then, we say that d is a metric on X and that (X, d) is a metric space.

Examples 2.2[3]:

1.) The prototype: The line R with its usual distance $d(x, y) = |x - y|$.
2.) The plane R^2 with the "usual distance" (measured using Pythagoras's theorem): $d\big((x_1, y_1), (x_2, y_2)\big) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$. This is sometimes called the 2- metric d_2.
3.) The metric on the complex numbers $\mathbb{C}$ interpreted as the Argand plane. In this case the formula for the metric is now: $d(z, w) = |z - w|$, where the $|.|$ in the formula represent the modulus of the complex number rather than the absolute value of a real number.
4.) The plane with the taxi cab metric $d\big((x_1, y_1), (x_2, y_2)\big) = |x_1 - x_2| + |y_1 - y_2|$. This is often called the 1- metric d_1.
5.) The plane with the supremum or maximum metric $d\big((x_1, y_1), (x_2, y_2)\big) = \max(|x_1 - x_2|, |y_1 - y_2|)$. It is often called the infinity metric d_∞.

Definition 2.3[4]: In Euclidean n-space, an (open) n-ball of radius r and center x is the set of all points of distance < r from x. A closed n-ball of radius r is the set of all points of distance ≤ r away from x.
Defintion 2.4[4]: A hyperball (hypersphere) is the set of all points of distance = r away from x.
Remark 2.5[4]: In Euclidean n-space, every ball is the interior of a hypersphere (a **hyperball**), that is a bounded interval when n = 1, the interior of a circle (a **disk**) when n = 2, and the interior of a sphere when n = 3.
Theorem 2.6[5]: The line joining the centre of the circle to the midpoint of a secant is perpendicular to the secant.

III. Main Results

In this algorithm, first we have to fix the shared keys and the encryption scheme. In this paper we use the ASCII system which is an easy and handy tool for both encrypting and decrypting. The algorithm is based on the properties of three circles.

Result 3.1[6]: If we take three circles centred at $(a_1, b_1), (a_2, b_2), (a_3, b_3)$ with radii d_1, d_2, d_3, respectively. The intersection of these three circles can be discussed in three cases:

(i) No intersection
(ii) One point intersection
(iii) Two point intersection

Theorem 3.2: If three circles intersect in two common points then the centres of the three circles are collinear.
Proof: We know that two circles intersect each other at exactly two points. Consider two circles with centres C_1 and C_2. There can be three cases:
The circles:

(i) Do not intersect
(ii) Intersect tangentially
(iii) Intersect in two points

Let us assume that the three circles intersect at two points so we take the case of intersection of two circles intersecting at the points A and B(say). Let the midpoint of the line AB be O. Now, the third circle must pass from the points A and B. Now, as we know that the line joining the centre of the circle to the midpoint of a secant is perpendicular to the secant. So the points C_1, C_2 and O are collinear and similarly the points C_1, C_3 and O are also collinear, which is to say that C_1, C_2 and C_3 are collinear.
So, if the three circles intersect at two points there centres are collinear.

Corollary 3.3: If the centres of three intersecting circles are not collinear then the circles intersect at a unique point.

Remark 3.4: If we take distances d_1, d_2 and d_3 of a fixed point X from three points A, B and C respectively. We draw three circles with centres A, B and C and $d_1, d_2$and d_3 as radii. Then, the point X must lie on all of the three circles.

Example 3.5: Let us take the three non collinear points $A(0,1), B(1,0)$ and $C(1,1)$ and an arbitrary point $X(3,4)$. Consider the Euclidean metric

$$d\big((x_1, y_1), (x_2, y_2)\big) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Now, $d_1 = d\big((3,4), (1,0)\big) = \sqrt{20} = 4\sqrt{5}$, $d_2 = d\big((3,4), (0,1)\big) = \sqrt{18} = 3\sqrt{2}$, and $d_3 = d\big((3,4), (1,1)\big) = \sqrt{13}$. Then the intersection of the circles $C_1\left((1,0), 4\sqrt{5}\right)$, $C_2\left((0,1), 3\sqrt{2}\right)$ and $C_3\left((1,1), \sqrt{13}\right)$ will be $(3,4)$.

IV. Basic Encryption Strategy

To first encrypt the message as an integer we use ASCII algorithm. We first bifurcate the message into parts by keeping words in odd places in one place and the words in even places in another. For example if the message is "Gauss was a genius!" then it will be bifurcated as "Gauss a!" and "was genius". Then we will encrypt the two strings according to the ASCII scheme of encryption. That is the above strings will be encrypted as "071097117115115126097033" and "119097115126103101110105117115", respectively. Now the required point of the message in the space will be $(071097117115115126097033, 119097115126103101110105117115)$.The corresponding decryption will be on the same lines as in regular ASCII scheme. That is both the numerical strings are decoded by first grouping the digits in the pair of three from right to left. That is $(\overline{071}\ \overline{097}\ \overline{117}\ \overline{115}\ \overline{115}\ \overline{126}\ \overline{097}\ \overline{033}$, 119 097 115 126 103 101 110 105 117 115. Then decoding as per ASCII scheme we get "Gauss a!" and "was genius". And hence the message can be rearranged as "Gauss was a genius!"
We propose the following algorithms:

4.1. Algorithm for Encryption Of The Message To Be Sent

1.) Bifurcate the message in two parts by collecting the words in odd places in one part and the one's in even places in one part.
2.) Encrypt the two parts by ASCII scheme.
3.) Mark the encryption as a point in R^2 as $X(x_1, x_2)$.

4.) Find the square of the distances of X from the keys A, B and C as d_1, d_2 and d_3.
5.) The distances d_1, d_2 and d_3 are the required message coding.

4.2. Algorithm for decryption of the message recieved:
1.) Find the unique intersection of the three circles centred at A, B and C with radii d_1, d_2 and d_3.
2.) Decrypt the point X using ASCII scheme.
3.) Arrange the two strings keeping the words in first coordinate in odd places and in second in even places.
4.) The message so retrieved is the required message.

4.3. Algorithm to send the changes in the keys:
1.) Choose the new keys A_1, B_1 and C_1.
2.) Find the distances of A_1 from A, B and C as d_{11}, d_{12} and d_{13}.
3.) Similarly, the find the distances of B_1 from A, B and C as d_{21}, d_{22}, and d_{23} and of C_1 from A, B and C as d_{31}, d_{32} and d_{33}.
4.) Form the matrix: $\begin{bmatrix} d_{11} & d_{12} & d_{13} \\ d_{21} & d_{22} & d_{23} \\ d_{31} & d_{32} & d_{33} \end{bmatrix}$.

4.4. Algorithm to trace the required changes in the keys:
1.) Find the intersection of the three circles centred at A, B and C and radii d_{11}, d_{12} and d_{13}, respectively.
2.) Similarly, find the intersection of the circles centred at A, B and C and radii d_{21}, d_{22}, and d_{23}, respectively.
3.) Finally, find the intersection of the circles centred at A, B and C and radii d_{31}, d_{32} and d_{33}, respectively.
4.) The intersection points so found are the new keys.

V. Level Of Security Proposed

The basic algorithms in the practice are all based on large prime numbers and number theory. However large the prime number, in the age of supercomputers if we know the length of the prime number we can get our hands on the private keys used to decrypt the message by an efficient programming. Suppose we take the case of the basic theory of taking two prime numbers both of 100 digits. Now, multiplication of these two numbers will be a large number of about 200 digits. If somehow a person get to know the message sent. Then, he need to find those two prime numbers to understand the message, guessing of which is a cumbersome task. But all we have to do is first find $9 \times \binom{99}{9}$ 100 digit numbers and see how many of them are prime numbers. Now, in list we have our unique combination of prime numbers. However these calculations will take many years of hard work. But still we can take the possibility of breaking into the codes using an efficient programming skill.

Now, in the present algorithm proposed if somehow one hacks the message and get to know the three distances d_1, d_2 and d_3. To get the hands on the message one has to first guess the three points from where the distance has been taken. For example, take the simplest distance of 1 unit. There are infinite points which are 1 unit apart from each other. So, to guess these three points however efficient the programmer is, one has to find three points out of infinite number of points. This will render the programmer with the problem of infinite loops.

VI. Conclusion

The algorithms currently practised in security purposes to send a secret message are all based on the prime numbers. In this paper, we propose the coding to be done using metric distances. This leaves the hacker to rely on pure guessing to actually decode the message. The message can be properly decoded only when the person has the access to the private keys.

VII. Scope Of The Study

The paper considers the Euclidean space forn $= 2$. The same purpose can be solved taking other metric spaces also and also in more than 2- dimensions.

References

[1]. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone "Handbook of Applied Cryptography", CRC Press ISBN: 0-8493-8523-7, 1996, 816 pages.
[2]. S. Punnusamy, "Foundations of Functional Analysis", CRC Press, 2002,457 pages. http://www-history.mcs.st-and.ac.uk/~john/MT4522/Lectures/L5.html. https://en.wikipedia.org/wiki/Ball_(mathematics).
[3]. R. D. Sharma, "Mathematics Class- IX," Dhanpat Rai Publications.
[4]. C. I. Delman, G. C. Galperin, "A Tale of Three Circles," Mathematics Magazine, Santa Clara University, Vol. 76, no. 1, 2003.