International Journal of Students Research in Technology & Management

Vol 1(2), April 2013, pg 214-219

KUNAL ASTROCRYPTOGRAHY SECURITY USING DISTANCE FORMULA AND 3D GEOMETRY

Kush Jain

Department of IT, Army Institute of Technology, Pune, Maharashtra, India

kushjain@gmail.com

Abstract

In real world, data security plays an important role where confidentiality, authentication, integrity, non repudiation are given importance. The universal technique for providing confidentiality of transmitted data is cryptography. This paper provides a technique to encrypt the data using distance formula and 3D geometry.

Keywords - Distance Formula, 3D Geometry, data security, authentication, cryptography, ASCII

I. INTRODUCTION

In the present world scenario it is difficult to transmit data from one place to another with security. This is because hackers are becoming more powerful nowadays. To ensure secured data transmission there are several techniques being followed. One among them is cryptography which is the practice and study of hiding information. [1]

In the modern era of computers we can create more secure cipher text. In this paper we create cipher text using ASCII values of characters and 3D Geometry.

II. LITERATURE SURVEY

A. Cryptography

Cryptography, to most people, is concerned with keeping communications private. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decryption is the reverse of encryption; it is the transformation of encrypted data back into the same plain text from which the cipher text was generated. [1]

Encryption and decryption require the use of some secret information, usually referred to as a key. [1] The data to be encrypted is called as plain text[1] The encrypted data obtained as a result of encryption process is called as cipher text[1]

B. 3D Geometry

A point in 3D plane can be represented using 3 coordinates (x, y and z). A point on a sphere of radius r and center (x_0,y_0,z_0) can be represented as[3]

$x = x_0 + r \times \cos\theta \times \sin\varphi$

$y = y_0 + r \times \sin\theta \times \sin\varphi$

$z = z_0 + r \times \cos\varphi$

Where $0 <= \theta <= 2\pi$, and $-\pi/2 <= \varphi <= \pi/2$

C. Distance Formula

Distance between two points A (x_1, y_1, z_1) and B(x_2, y_2, z_2) can be calculated as [2]

Distance

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2}$$

$$\Rightarrow d^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2$$

III. PROPOSED METHODOLOGY

In this method the first step is to assign a unique set of coordinates known only to receiver and sender. These coordinates are the origin of the Cartesian plane they are going to use for communication Another set of points known as stars should also be shared only between the sender and receiver. There should be at least 1 star. A constant m which signifies the maximum number of concentric spheres to consider is also decided. E.g. m = 10

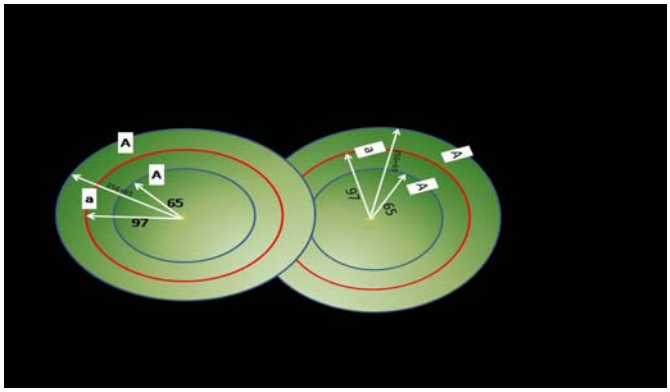

Fig. 1 Multiple Stars

Another set of spheres (specifying the radius and the center point (which should not enclose the sphere made by taking any stars center point and radius as the m × maximum range of ASCII)) known as black holes is also shared between the sender and receiver. There can be any number of such spheres (black holes) (The only restriction being that there is a possibility to encode all ASCII characters using stars)

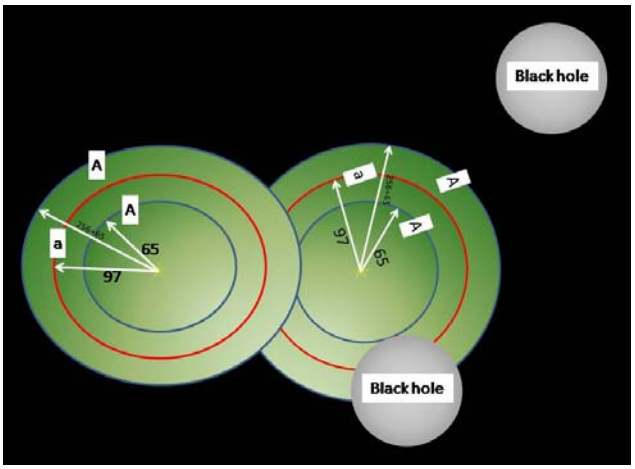

Fig. 2 Blackholes

The next step is to calculate the ASCII equivalent of each character in the message and add it with any multiple of the range of ASCII characters. Let's call this value d

Then we plot a point on the sphere with any star chosen at random from given stars and radius d. The point is plotted by taking any random value of θ and φ.

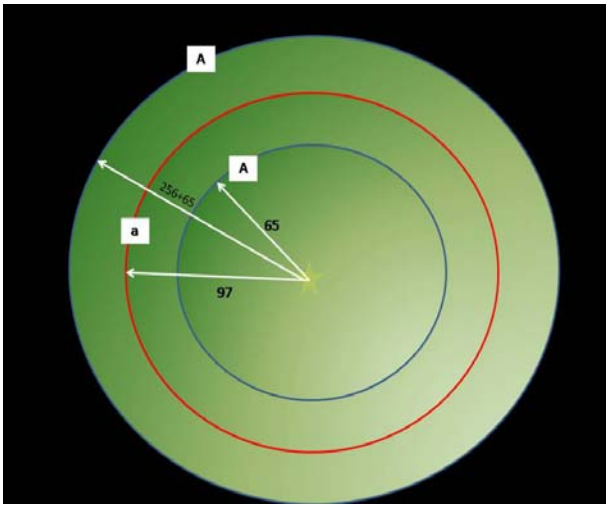

Fig. 3 Position of letter A

We check if this point lies inside or on any black hole. If it does then we regenerate the point by going back to step involving generation of point.

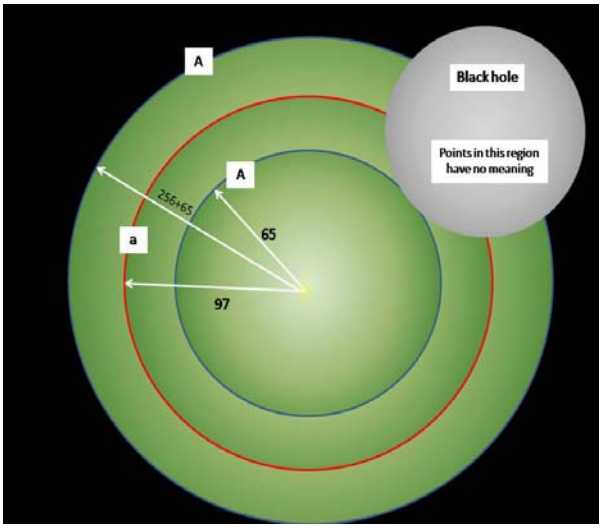

Fig. 4 Points inside blackhole are ignored at the time of decryption

We check that if this point already exists in the cipher text. If it does then we regenerate the point to get a different set of coordinates by regenerating the point by going back to step involving generation of point. If we keep getting the same result after trying many times, then only we repeat the point.

We now check if this point is closest to the star from which it is generated in comparison to other stars. If not, then we regenerate the point by going back to step involving generation of point.

Now we round the point to 2 decimal places and remove the decimal point and append it in cipher text by separating the coordinates with a comma.

While generating points for each character, we also place any random number of points that lie in or on the black hole at the starting, in between or at the end of cipher text to generate a certain number of points that lie in or on the black hole

To decode it, first retrieve the triplet from cipher text each of which is separated by comma. Then divide each number by 100. This will be the x, y and z values of the point.

Check if this point lies on or inside a black hole, if it does then generate nothing.

If it does not come in or on a black hole then find the star closes to this point and the distance of that star from this point. Round off this distance to nearest whole number. Take remainder by dividing this

rounded distance with the maximum range of ASCII characters. This remainder is the ASCII equivalent of plain text character. Convert this ASCII value to character to get the plain text

The entire coordinate system has origin which is shared just between the sender and receiver

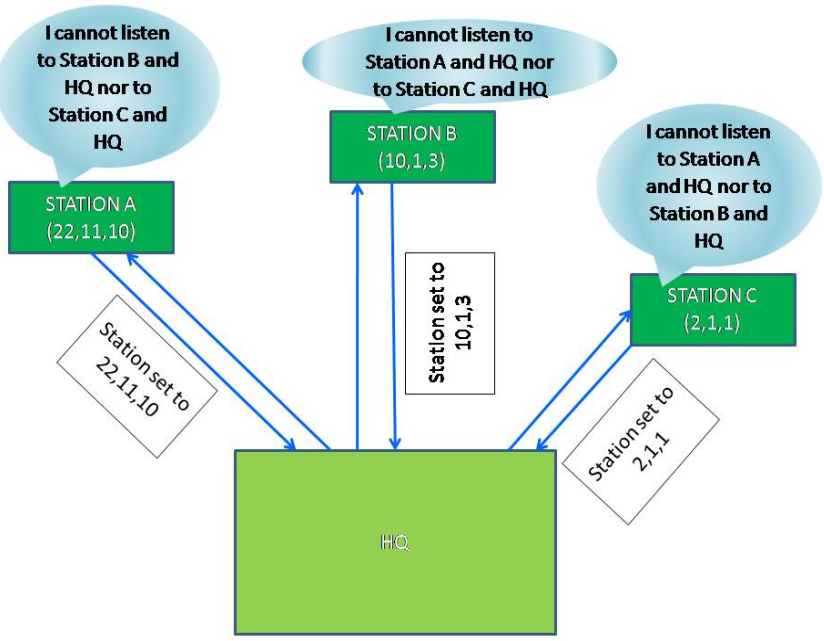

Fig. 5

Station A,B,C have same stars and blackhole but it is difficult for them to see messages meant for other station as they have different origin

IV. ADVANTAGES

1. Since it uses ASCII, it can encrypt any character including A-Z, a-z, 0-9, spaces as well as special characters supported by ASCII[4][7]

2. Since it generates random points on a sphere of random radius for a particular character. There can be 360×180×m points for a particular character by trying not to repeat the same point again for the same character.

3. It generates random useless points in between, thus fixed size messages can be generated providing more security compared to other cryptographic algorithms[5][6][1] as the number of characters in original message cannot be found from encrypted message without the knowing the black holes

4. There can be many stars, thus even if only 1 star is leaked, the message can only be partially decrypted

5. The receiver also needs to know the origin; if he does not know it then it is difficult to read the message

6. Message cannot be decrypted completely till all the stars and origin are known

7. Even if the algorithm is known, it is almost impossible to extract the original text without knowing the stars and origin

8. Even with the same set of stars, blackholes and origin , we get many different points for the same character, thus making it more secure.

V. CONCLUSION

The above cryptography can be applied mainly in military where data security is given more importance. Instead of ASCII Unicode can also be used, which would provide the ability to encode and decode messages in one's native language and thus increasing security. Thus usage of stars, black holes and origin ensures that the data is read only by authorized personnel

REFERENCES

1. S. Pavithra Deepa, S. Kannimuthu, V. Keerthika ,"Security Using Colors and Armstrong Numbers", Proceedings of the National Conference on Innovations in Emerging Technology-2011 Kongu Engineering College, Perundurai, Erode, Tamilnadu, India.17 & 18 February, 2011.pp.157-160
2. An article on Distance http://en.wikipedia.org/wiki/Distance
3. An Article on Sphere http://en.wikipedia.org/wiki/Sphere
4. An article on ASCII codes http://en.wikipedia.org/wiki/ASCII
5. Dr.M.Mohamed Sathik, A. Kalai Selvi, " Secret sharing scheme for data encryption based on polynomial coefficient", 2010 Second International conference on Computing, Communication and Networking Technologies
6. Mohammad Zakir Hossain Sarker, Md. Shafiul Parvez , "A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of data"
7. Ahmed Desoky, "Cryptography: Algorithms and Standards", 2005 IEEE International Symposium on Signal Processing and Information Technolog