International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 1, January 2013 ISSN 2319 - 4847

Encryption and Decryption of Locations Using Linear Algebra and ASCII Values

M. Yamuna[1], Arpita Das[2], Debjit Paul[3]
[1]Asst Prof (Sr), VIT University, Tamilnadu, India, 632 014

[2]MCA Student VIT University, Tamilnadu, India, 632 014

[3] MCA Student VIT University, Tamilnadu, India, 632 014

ABSTRACT

In current communication providing personal details becomes unavoidable. One need to provide personal information while banking, online purchase and so on. For any concern it is important to maintain these information confidential. So safe encryption and decryption of any location becomes important. The latitude and longitude best represents any location on earth. In this paper we propose a method for encrypting and decrypting any location using ASCII values and basic mathematics.
Keywords: Latitude, Longitude, ASCII

1. INTRODUCTION

In cryptography, encryption is the process of encoding some information in a manner that hackers or eavesdroppers cannot read it. It is becomes readable only with a decryption code. The use of encryption/decryption is as old as the art of communication. Various secret or important messages have to be sent without any third party being able to read it. Encryption has long been used by militaries and governments to facilitate secret communication. Now a days, encryption is also used in protecting information within many kinds of civilian systems.
In an encryption scheme, the message or information (or simply the plaintext) is encrypted using an encryption algorithm, turning it into an unreadable form called as “cipher text”. The main purpose of encryption is the encrypted message or information should not be able to determine anything about the original message. Only authorized party, however, will be able to decode this cipher text using the corresponding decryption algorithm. The stronger the cipher text, that is, the harder it is for unauthorized people to break it, the better, in general. But this however means that as the strength of encryption/decryption increases, so does the cost.

2. PRELIMINARY NOTE

The latitude (abbreviation: Lat, φ, or phi) of a point on the Earth's surface is the angle between the equatorial plane and a line that passes through that point and is normal to the surface of a reference ellipsoid which approximates the shape of the Earth. This line passes a few kilometers away from the center of the Earth except at the poles and the equator where it passes through Earth's center. Lines joining points of the same latitude trace circles on the surface of the Earth called parallels, as they are parallel to the equator and to each other. The north pole is 90° N; the south pole is 90° S. The 0° parallel of latitude is designated the equator, the fundamental plane of all geographic coordinate systems. The equator divides the globe into Northern and Southern Hemispheres. The Longitude (abbreviation: Long., λ, or lambda) of a point on the Earth's surface is the angle east or west from a reference meridian to another meridian that passes through that point [2].

The Earth is not a sphere, but an irregular shape approximating a biaxial ellipsoid. It is nearly spherical, but has an equatorial bulge making the radius at the equator about 0.3% larger than the radius measured through the poles. The shorter axis approximately coincides with axis of rotation. Map-makers choose the true ellipsoid that best fits their need for the area they are mapping. They then choose the most appropriate mapping of the spherical coordinate system onto that ellipsoid [2].

The determinant of a 3×3 matrix [3] $\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ is defined by $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a\begin{vmatrix} e & f \\ h & i \end{vmatrix} - b\begin{vmatrix} d & f \\ g & i \end{vmatrix} + c\begin{vmatrix} d & e \\ g & h \end{vmatrix}$

$= aei + bfg + cdh - ceg - bdi - afh$

The American Standard Code for Information Interchange (ASCII) [4] is a character - encoding scheme originally based on the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that use text. Most modern character-encoding schemes are based on ASCII, though they support many additional characters.

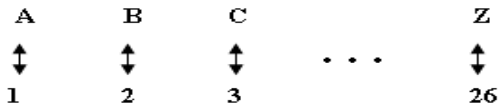
Here we propose a new encryption algorithm which uses a combination of linear algebra and ASCII values. We use this encryption technique to encode messages which contains address of some classified location or in any situation where we don't want a third party to know where the other person is.

3. PROPOSED CRYPTOSYSTEM

Here we propose a method of encrypting any location in the world. We first determine the latitude and longitude of the location to be encrypted, so that the location to be encrypted is now available as numbers.
To encrypt the latitude we pick two matrices whose determinant values match with the degree and minute of the latitude. We decide a key matrix by choosing any statement. We then encrypt the latitude value using a key matrix and an encoding chart.
To encrypt longitude we determine a string (of symbols and numbers and letters) so that the string satisfies the encoding formula for longitude. We then encode the longitude using ASCII values of the symbols used in the string.

3.1 Encryption Chart

The encoding chart can be decided as per the convenience of the user. The number of symbols need to be used can also be decided. Here we use the chart only for alphabets [1].

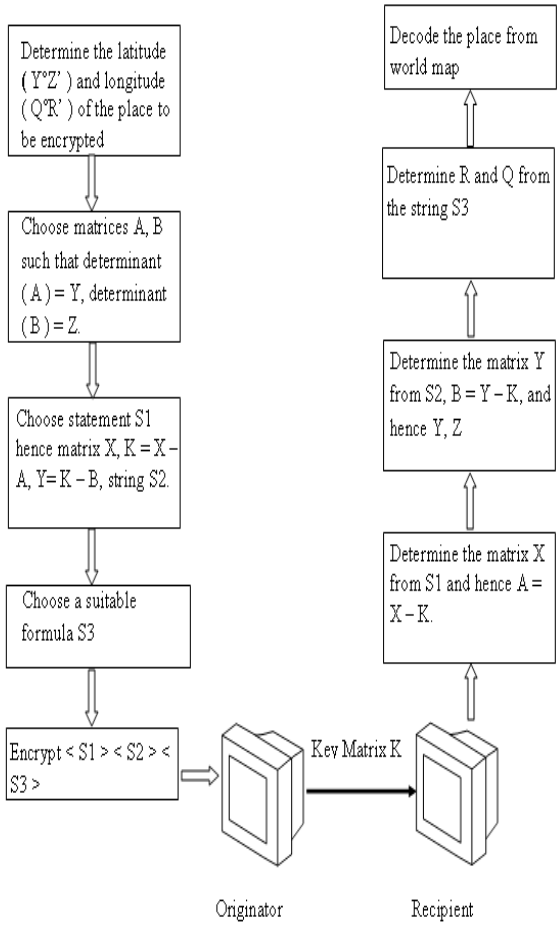


3.2 ASCII Values

Here we provide the ASCII values of the symbols used in this paper

SYMBOL	ACSII VALUE
E	69
W	87
X	120
!	33
^	94
%	37
*	42
+	43
<	60
•	46

3.3 System Model For the Proposed Cryptosystem



Encoding Algorithm

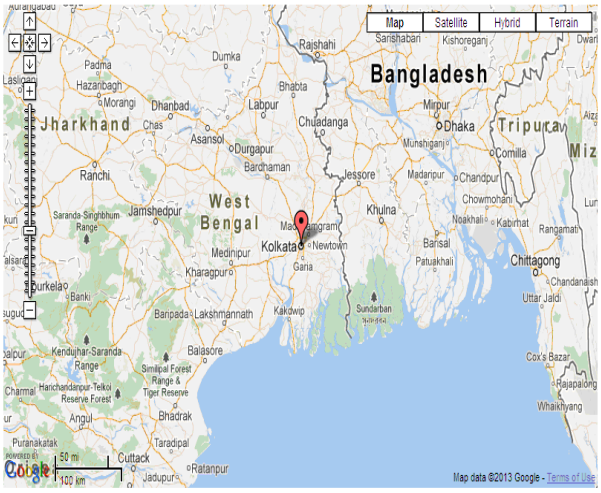
- Find the latitude (Y°Z') and longitude (Q°R') of the location you want to encode.
- Encoding the latitude (Y°Z') Take any two 3 x 3 matrices A, B such that determinant (A) = Y, determinant (B) = Z.
- Take any sentence S1 in English language. Form a 3 x 3 matrix X, where the entry values of the matrix represent the first nine letters of the sentence.
- Determine K = X – A, Y= K – B.
- Write all the entry of Y row wise and convert them into a string of letters using the encoding chart. Prefix and suffix this string with N or S depending on the north or south position in the latitude to obtain a string S2
- Encoding the longitude (Q°R')
- Construct a string S3 using numbers letters and symbols. This string will start with 6 and end with 9 if the location is to the east, else string will start with 8 and end with 7 if the location is to the west.
- R = the 2 symbols of S3 with less ASCII value added with each other and the result will be subtracted from the symbol with greatest ASCII value of symbols in S3.
- Q = addition of the ASCII values of the remaining symbols in S3.
- Encrypt < S1 > < S2 > < S3 > to the receiver.

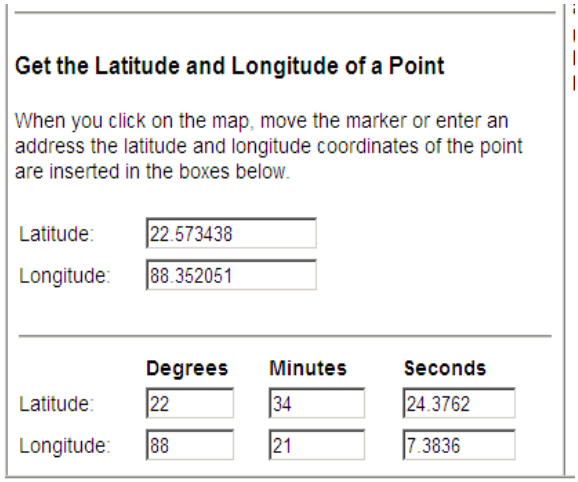
Decryption Algorithm

- Determine the matrix X from S1 and hence A = X – K.
- Determine the matrix Y from S2 and hence B = Y – K.
- Determinant A and determinant B decides the latitude.
- Determine the values of R and Q using the formula in the string S3 which decides the longitude.
- Decode the location from world map.

4. EXAMPLE

Suppose we want to encode the name of the city say KOLKATA. We determine the latitude and longitude of KOLKATA from the world map. As we place the pointer at KOLKATA the latitude and longitude gets displayed [5].





As seen from the Google map result we find the latitude and longitude of KOLKATA from the map as 22˚34' N and 88˚24'E.

Encoding Latitude

Let $A=\begin{bmatrix}3 & 1 & 1\\ 0 & 4 & 2\\ 1 & 0 & 2\end{bmatrix}$ so that determinant (A) = 22.

Let $B=\begin{bmatrix}4 & 1 & 0\\ 0 & 4 & 2\\ 1 & 0 & 2\end{bmatrix}$ so that determinant (B) = 34.

Now we take a sentence say: MY CAT DRINKS MILK
Removing the spaces we get: MYCATDRINKSMILK
From the first nine characters MYCATDRIN we get the nine numbers 13 25 3 1 20 5 4 18 9 from the encoding chart so that

$X=\begin{bmatrix}13 & 25 & 3\\ 1 & 20 & 5\\ 4 & 18 & 9\end{bmatrix}$ and hence the key matrix $K=X-A=\begin{bmatrix}10 & 24 & 2\\ 1 & 16 & 3\\ 5 & 18 & 7\end{bmatrix}$ and hence $Y=K-B=\begin{bmatrix}6 & 32 & 2\\ 1 & 12 & 1\\ 4 & 18 & 5\end{bmatrix}$

We obtain 6 23 2 1 12 1 4 18 5 writing the entry of Y row wise.
The alphabets from the encoding chart is F W B A L A D R E
Now just to hide the actual code the sender places the word N in the front and at the last
the code become NFWBALADREN

Encoding Longitude

We choose the string S3: 6((5!)^2)%5*2.39
The first and last value 69 represents the ASCII value of east.
The ASCII values of the symbols is ! ^ % * . is 33, 37, 94, 42, 46. The largest value is 94 and the smallest two values is 33, 37 so that 94 – (33 + 37) = 24. Adding the values of the remaining symbols we get 46 + 42 = 88 which matches with the latitude to be encoded.
Finally we send
My cat drinks milk nfwbaladren 6((5!)^2)%5*2.39
to the receiver (the three data are separated by blank space).

Suppose the received message is
My puppy is sick nbvmpnjyfpn (3+5)<[4x+7%4]

Decoding Latitude

Consider MY PUPPY IS SICK . The first nine characters is MYPUPPYIS. Using the Decoding chart we get the corresponding values as 13 25 16 21 16 16 25 9 19. Converting this into a matrix we get

$$X = \begin{bmatrix} 13 & 25 & 16 \\ 21 & 16 & 16 \\ 25 & 9 & 19 \end{bmatrix}$$

Consider the key matrix known to the coder and decoder is known as

$$K = \begin{bmatrix} 11 & 24 & 14 \\ 18 & 15 & 13 \\ 25 & 8 & 17 \end{bmatrix}$$

Using this key matrix and X we generate

$$A = X - K = \begin{bmatrix} 2 & 1 & 2 \\ 3 & 1 & 3 \\ 0 & 1 & 2 \end{bmatrix}$$

Consider the second part NBVMPNJYFN. Eliminating n we get BVMPNJYF. This converted from the decoding chart gives 2 21 13 16 14 10 25 6 16 and hence

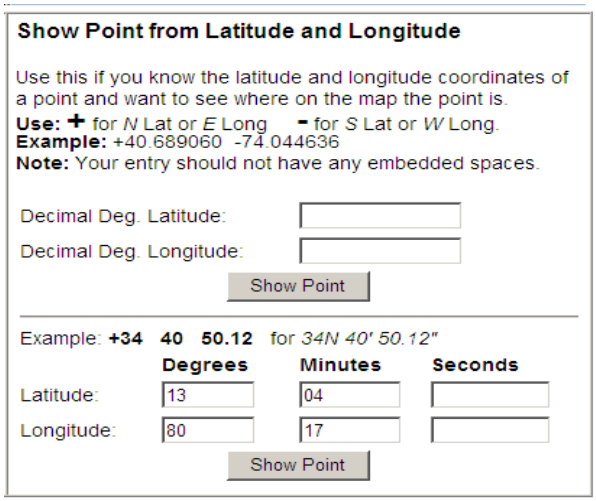
$$Y = \begin{bmatrix} 2 & 21 & 13 \\ 16 & 14 & 10 \\ 25 & 6 & 16 \end{bmatrix} \text{ and } B = K - Y = \begin{bmatrix} 13 & 3 & 1 \\ 3 & 1 & 3 \\ 0 & 2 & 1 \end{bmatrix}$$

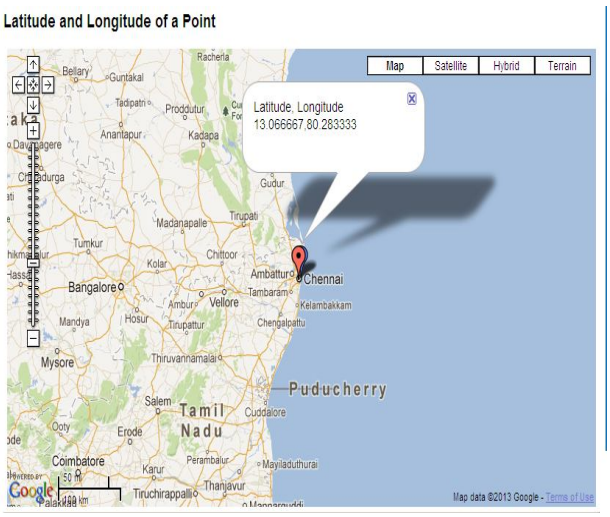
. Also determinant (A) = 13, determinant (B) = 3. Also we had eliminated n in the second sequence which represents north. So the latitude is 13 degrees, 4 minutes North.

Decoding Longitude

Consider the equation **6(3 + 5) < [4x + 7 % 4]9**. Considering symbols only in the given order we get **+ < x + % .** Converting them to their ASCII values we get Now from the 1st 3 symbols **x** is the largest so 120 – (43 + 77) = 17
The next two symbols give us: 42 + 38 = 80.
The first element in the string is 6 and the last is 9. 69 is the ASCII value of east.

So according to the algorithm the longitude is 80 degrees 17 minutes E. We enter the decrypted latitude longitude values in the location search [5]





From the map we see that the location that was encrypted is CHENNAI.

5. CONCLUSION

Until the key matrix is known determining the latitude and unless the formula is known decrypting the longitude is not possible. Different keys and different methods for encoding the latitude and longitude is the strength of this proposed method since even if one breaks the encoding method for latitude, decoding will not be possible since the longitude is encoded in a different method. This guarantees the proposed method secure.

REFERENCES

[1] Jin Ho Kwak and Sungpyo Hong, Linear Algebra, Second edition, Springer (2004)
[2] URL:http://en.wikipedia.org/wiki/Geographic_coordinate_system
[3] URL: http://en.wikipedia.org/wiki/Determinant
[4] URL: http://en.wikipedia.org/wiki/ASCII
[5] URL: http://itouchmap.com/latlong.html

AUTHOR

M. Yamuna received her doctorate in Mathematics, Alagappa University, Karaikudi, India. She is currently working as an Asst Professor (Sr) at VIT University, Vellore, India. Arpita Das are Debjit Paul are first year MCA students at VIT University, Vellore, India.