

Encryption Using Dictionary and Locations

M. Yamuna¹, Poorva Arora²
SAS, VIT University
SCSE, VIT University

Abstract: In current communication system providing personal information becomes unavoidable. One is in need to provide personal information while banking, purchasing and so on in a number of situations. For any concern, it is important to maintain these kind of personal information confidential. This is at most important for the growth of any concern. The safety of such details is important right from the safety of common man to national security. Various encryption methods are adopted to maintain the confidentiality of these details. The latitude and longitude best represents any location on this earth. Use of dictionary for encryption is not in common use. In this paper we propose a method for encryption of the name and location of a person using dictionary, latitude and longitude. This method also aims to use grammar and language as an additional parameter to encrypt the data.

Keywords: Latitude, Longitude, Grammar, Language, Dictionary.

I. Introduction

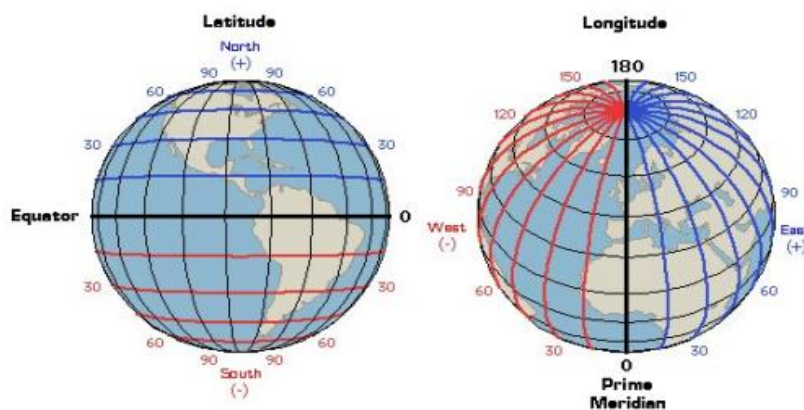
In current communication system, providing personal information becomes unavoidable. Same way various concerns collecting these data are very particular about the privacy of these data, because it is a matter of trust of the public on the concern. They protect this information by maintaining physical, electronic, and procedural safeguards that meet applicable law. They train their employees in the proper handling of personal information. They the service of other companies to protect the confidentiality of personal information. Encryption is one way in which this can be achieved [1]. In this is paper we propose one method for encrypting the name and location of a person using dictionary and location. This method aims to use language and grammar as an additional parameter to encrypt the data.

II. Preliminary Note

In this section we provide the details that are used in the proposed encryption scheme.

A. Latitude and Longitude

The latitude 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. 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 Longitude 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.



The Earth is not a sphere, but an irregular shape approximating a biaxial ellipsoid. 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 degree representation of the latitude and longitude can be seen in the above image [3].

B. Dictionary

According to Nielsen (2008) a dictionary may be regarded as a lexicographical product that is characterized by three significant features: (1) it has been prepared for one or more functions; (2) it contains data that have been selected for the purpose of fulfilling those functions; (3) its lexicographic structures link and establish relations between the data so that they can meet the needs of users and fulfill the functions of the dictionary [4].

C. Grammar and Language

In formal language theory, a grammar is a set of production rules for strings in a formal language. The rules describe how to form strings from the language's alphabet that are valid according to the language's syntax. A grammar does not describe the meaning of the strings or what can be done with them in whatever context only their form. Formal language theory, the discipline which studies formal grammars and languages, is a branch of applied mathematics. Its applications are found in theoretical computer science, theoretical linguistics, formal semantics, mathematical logic, and other areas. A formal grammar is a set of rules for rewriting strings, along with a "start symbol" from which rewriting starts. Therefore, a grammar is usually thought of as a language generator. However, it can also sometimes be used as the basis for a "recognizer"—a function in computing that determines whether a given string belongs to the language or is grammatically incorrect. [5].

III. Proposed Encryption Scheme

Our aim is to encrypt the name of a person and his location. The proposed encryption scheme is explained in this section.

A. Encrypting Location

We initially determine the latitude and longitude of the location. We propose to use dictionary for this. We shall find suitable words from the dictionary that will represent the degree minutes and second. Our aim is to cover all the pages of the dictionary. We know that the latitude varies from -90 to 90 degrees. So the first page of the dictionary shall denote -90 degrees, the second page -89 degrees and so on, the 180^{th} page will denote 180 degrees. Since we have exhausted all the degrees we shall repeat the cycle once again, that is the 181 page will again represent -90 degrees, 182^{nd} page will be represented by -89 degrees and so on till all the pages of the dictionary is covered. This can be generalized as formula 1.

Formula 1

$(180n + n) \text{ page} = -90 \text{ degrees}, ((180 + (n + 1))) = -89 \text{ degrees} \dots ((180n + (n + 90))) = 0 \text{ degrees}, \dots ((180n + (n + 180))) \text{ page} = 90.$

pages 0, 181, 362, 543, 724 etc will be represented by -90 degrees.

page 1, 182, 363, 544, 725 etc will be represented by -89 degrees.

... page 90, 271, 452, 633 etc will be represented by 0 degrees...

pages 180, 361, 542, 723 etc will be represented by 90 degrees.

For encrypting minutes and seconds we will pick any word randomly from the dictionary that corresponds to the value of minute and second, that is the word of that specified value from the top left of any page.

B. Encrypting Longitude

This is done similar to latitude. Since longitude varies from -180 to 180 degrees, the formula for longitude is

Formula 2

Every $(360n + n) \text{ page} = -180 \text{ degrees}, ((360n + (n + 1))) = -179 \text{ degrees} \dots ((360n + (n + 180))) = 0 \text{ degrees}$ and $((360n + (n + 360))) \text{ page} = 180 \text{ degrees}.$

that is

page 0, 361, 722, 1083 etc will be represented by -180 degrees.

page 1, 362, 723, 1084 etc will be represented by -181 degrees...

page 180, 541, 902 etc will be represented by 0 degrees...

page 360, 721, 1082 etc will be represented by 180 degrees.

For encrypting minutes and seconds we will pick any word randomly from the dictionary that corresponds to the value of minute and second, that is the word of that specified value from the top left of any page.

C. Encrypting Name

We use page numbers for representing the alphabets in the names. Say 0 page for A, 1 for B, ..., 25 for Z, again 26 for A, 27 for B and so on until all the pages of the dictionary are covered. This can be generalized as

Formula 3

Every $(25n + (n + 0)) = A, ((25n + (n + 1))) = B \dots$ that is

page 0, 26, 52, 79 etc will be represented by A..

page 1, 27, 53 etc will be represented by B..

page 25, 51, 77 etc will be represented by Z..

We now randomly pick a noun or verb or adjective from the page that represents the first alphabet in the name, randomly pick a noun or verb or adjective from the page that represents the first alphabet in the name, and so on till all the alphabets in the name are covered and form a statement S1 shuffling these words in a random order (For encryption purpose we use N1 for the first noun, N2 for the second noun,... V1 for the first verb, V2 for the second verb,..., A1 for the first adjective, A2 for the second adjective....).

The statement S1 is arranged in any random order. We need a method to arrange back the words in the correct order as they occur in the name. We use grammar and language for this. Using the notations N1, N2,..., V1, V2,..., A1, A2,...we design a suitable set of production rules so that the final result of the grammar will provide the ordering of the words in S1.

Finally we send a statement S and the production rules to the receiver. The first three words of S will represent latitude, the last three longitude and the remaining name of the person. This can be summarized in the following encryption algorithm.

D. Encryption Algorithm

Let latitude = (A[°] B' C'') and Longitude = (D[°] E' F'')

Step 1 Determine the value generated (say X) from the formula

$(180n + n) \text{ page} = -90 \text{ degrees}, ((180 + (n + 1)) = -89 \text{ degrees} \dots ((180n + (n + 90)) = 0 \text{ degrees}, \dots ((180n + (n + 180)) \text{ page} = 90 \text{ degrees}.$
that corresponds to A.

Step 2 Choose any word W1 randomly from page X of the dictionary.

Step 3 Choose the Bth word W2 from any page of the dictionary.

Step 4 Choose the Cth word W3 from any page of the dictionary.

Step 5 Determine the value generated (say Y) from the formula

$(360n + n) \text{ page} = -180 \text{ degrees}, ((360n + (n + 1)) = -179 \text{ degrees} \dots ((360n + (n + 180)) = 0 \text{ degrees and } ((360n + (n + 360)) \text{ page} = 180 \text{ degrees}$
that corresponds to D.

Step 6 Choose any word W4 randomly from page Y of the dictionary.

Step 7 Choose the Eth word W5 from any page of the dictionary.

Step 8 Choose the Fth word W6 from any page of the dictionary.

Step 9 Generate numbers say Z1, Z2, ..., Zk using the formula

$(26n) = A, ((25n + (n + 1)) = B \dots$

Where k is the length of the name to be encrypted.

Step 10 Choose k words randomly from the pages Z1, Z2, ..., Zk.

Step 11 Form a random statement S1 using Z1, Z2, ..., Zk.

Step 12 Determine the nouns, verbs and adjectives in S1 and design a set of production rules P suitable to generate the name.

Step 13 Let $S = \langle W1 W2 W3 \rangle \langle S1 \rangle \langle W4 W5 W6 \rangle$, that is S is a statement constructed by combining the words and statement S1 in the order given.

Step 14 Send S and P to the receiver.

Decryption can be done by reversing the procedure.

IV. Illustration

In this section we provide illustration for the proposed encryption scheme. In the dictionary we use [6], the pages start from 16, so we add a value 16 to the generated page value. This value varies from dictionary to dictionary.

Suppose we want to encrypt the name of the person JUBIN residing at GURAGON. Using Google map the latitude and longitude corresponding to GURAGON is as seen in snapshot 1 [7].

From snapshot 1 we observe that for Gurgaon the latitude is 28[°] 24' 38'' and longitude is 76[°] 47' 39''.

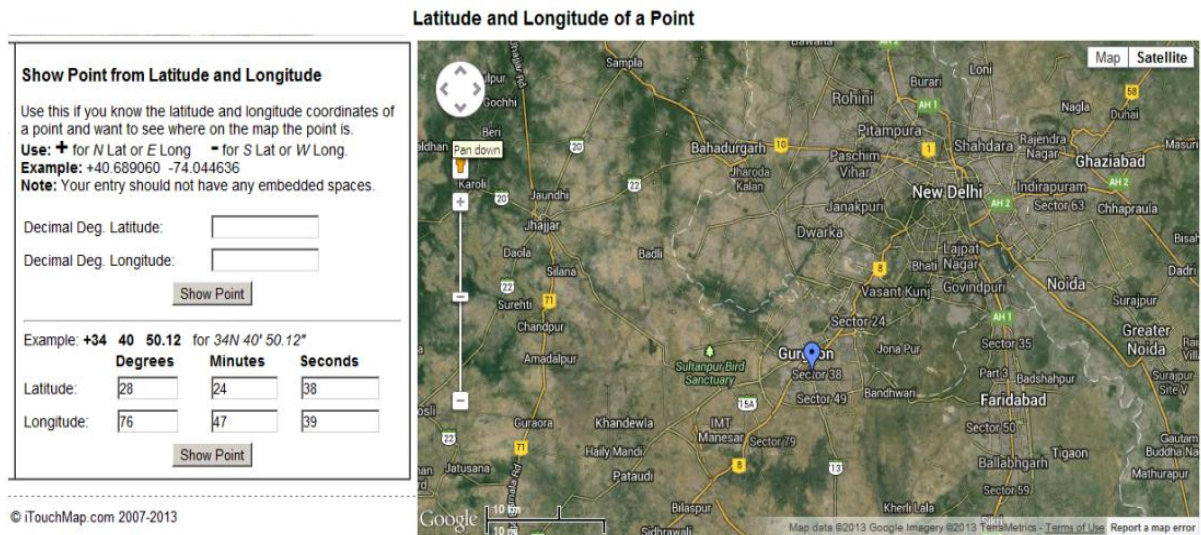
Latitude

For encrypting latitude as discussed we use formula 1. Let us take n = 1 we get

$(1 * 180 + (1 + 118)) = 299$. Adding 16 to this value gives us 315. So we look into page 315 of the dictionary and choose any word say Force from that page. Since the minutes and degree is 24 and 38, we can choose the 24th and 38th word from any page of the dictionary. In this example we choose Hold and Expire which are words 24 and 38 respectively.

Longitude

Similarly to encrypt longitude we choose formula 2. Let n = 1 then we get $(2 * 1 * 180 + (1 + 256)) = 617$.



Snapshot 1

Adding 16 to this value we get 633. Choose any word randomly from this page. We shall choose the word as Polo.

Since the minutes and degree is 47 and 39, we can choose the 47th and 39th word from any page of the dictionary. In this example we choose Rebirth and Autograph which are words 47 and 39 respectively.

Name

For the name we use the third formula. We encrypt as follows

$$B = 25 * 1 + (1 + 1) = 27 \text{ choosing } n = 1.$$

$$J = 25 * 4 + (4 + 9) = 113 \text{ choosing } n = 4.$$

$$I = 25 * 2 + (2 + 8) = 60 \text{ choosing } n = 2.$$

$$N = 25 * 1 + (1 + 13) = 39 \text{ choosing } n = 1.$$

$$U = 25 * n + (n + 20) = 20 \text{ choosing } n = 0.$$

Adding 16 to these values we generate the page numbers as 43, 129, 76, 55, 36 respectively. We choose the words Announcer, Carry, Beach, Also, Aside from these pages. We now frame the statement as Force hold expire the announcer to carry beach also aside and polo rebirth autograph.

In this statement announcer is noun 1, carry is verb 1, beach is noun 2, also is adjective 1, aside is adjective 2.

Using this we frame the grammar as

$$S \rightarrow A1; A1 \rightarrow \text{to}A1; \text{to} \rightarrow V1\text{the}; \text{the}A1 \rightarrow A1N1; N1 \rightarrow N1\text{and}; \text{and} \rightarrow N2A2$$

this will generate JUBIN.

Finally we send the message to the receiver as

Force hold expire the announcer to carry beach also aside and polo rebirth autograph.

$$S \rightarrow A1; A1 \rightarrow \text{to}A1; \text{to} \rightarrow V1\text{the}; \text{the}A1 \rightarrow A1N1; N1 \rightarrow N1\text{and}; \text{and} \rightarrow N2A2$$

Now, we provide illustration for the proposed decryption scheme.

Suppose the received message is

Rediscover Faintly Choreography the Chinless Angry and Addict Doorman of Bonanza Factory Bloat license Grayling Fandango

Grammar:

$$S \rightarrow N1; N1 \rightarrow \text{and}A2N1; \text{and} \rightarrow A1A3N2; A2N1 \rightarrow A2N1\text{of}; \text{of} \rightarrow V1\text{the}; \text{the} \rightarrow N2$$

Latitude

The first three words is Rediscover, Faintly, Choreography.

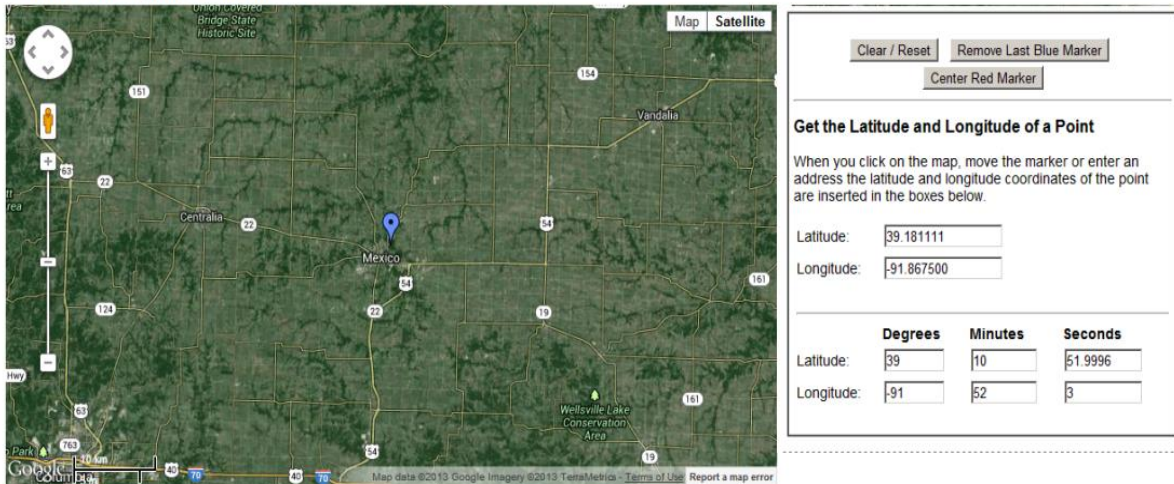
Rediscover is found in page 688. $688 - 16 = 672$. 688 divided by 180 is approximately 3. So take $n = 3$. Hence $540 + (3 + 90 + x) = 672$, because $180 * n + (n + 90) = 0^\circ$, $672 - 633 = 39$. Faintly is the 10th and choreography is the 52nd word. So latitude is $39^\circ 10' 52''$.

Longitude

The last three words are License, Grayling, Fandango. License is on page number 466 so $466 - 16 = 450$. Substituting $n = 1$, we get $360 + 1 + x = 450$ and hence $x = 89$. Since $-180 + x = \text{degrees}$ we get degrees = -91. Grayling is the 52nd word and Fandango 3rd word.

So longitude is $-91^\circ 52' 3''$. Hence feeding these latitude and longitude values on google map we get location MEXICO as seen in snapshot 2 [7].

Latitude and Longitude of a Point



Snapshot 2

Name

The remaining statement is

the Chinless Angry and Addict Doorman of Bonanza Factory Bloat.

Now Chinless is on pg no. 148. So $148 - 16 = 132$. But $132 = 26 * 5 + 2$. Hence ie., $n = 5$ so that $25 * 5 + ((5 + 2)) = 132$. So the corresponding letter is C from formula 3. Doorman lies on page number 241. So $241 - 16 = 225$. Also $26 * 8 + 17 = 225$, $25 * 8 + ((8 + 17)) = 225$ which gives letter R. Similarly Angry gives A Addict gives I Bonanza gives E Factory gives H Bloat gives L.

Now from the sentence we get Chinless as adjective 1 (A1), Angry is adjective 1(A2) , Addict Verb 1 (V1) , Doorman is noun 1 (N1), Bonanza is noun 2 (N2) , Factory is noun 3 (N3), Bloat is verb 2 (V2).

From the grammar received we obtain the order of the letters as follows

Grammar Received	Conversion
S→N1	N1
N1→andA2N1	andA2N1
and→A1A3N2	A1A3N2A2N1
A2N1→A2N1of	A1A3N2A2N1of
of→V1the	A1A3N2A2N1V1the
the→N2	A1A3N2A2N1V1N2

So the order of the received words is A1A3N2A2N1V1N2. Rearranging the statement in this order we get Chinless Factory Angry Doorman Bloat Addict Bonanza. We have already decrypted these words which generates the name received as **CHARLIE**.

Hence the message received is decrypted as **CHARLIE** residing in **MEXICO**.

V. Conclusion

We use different methods for encrypting latitude and longitude. So even if the latitude is decrypted since longitude is encrypted using different formula decryption of the location becomes not possible until the second formula is also known. Even if one manages to decrypt the location, they cannot decrypt the name since it uses a new formula and also uses grammar and language for encryption. This increases the security of the encrypted message. Also since random words are picked from the dictionary and used it becomes more tough for decryption. Also dictionary is not a common tool of encryption. So the proposed encryption method is good for maintaining security of the encrypted data. The same method can be used for encrypting the complete address also.

VI. References

- [1] <http://www.citigroup.com/citi/privacy>.
- [2] URL: http://en.wikipedia.org/wiki/Geographic_coordinate_system.
- [3] URL: http://www.geographyalltheway.com/ks3_geography/maps_atlases/imagesetc/latitudeandlongitude.
- [4] <http://en.wikipedia.org/wiki/Dictionary>.
- [5] http://en.wikipedia.org/wiki/Formal_Grammar.
- [6] Oxford Dictionary, Dorling Kindersley Limited and Oxford University press, 2003.
- [7] www.itouchmap.com/latlong
- [8] Jin Kwak, Sungpyo Hong, Linear Algebra, Springer 2004.