An Inimitable Cryptographic Creation: Siri Bhoovalaya

Anil Kumar Jain
SMIEEE, FIETE, FIE(1),SMCSI
ak.jain@ieee.org

ABSTRACT
Muni Kumudendra, a great genius, created a unique treasure house of knowledge known as ‘Siri Bhoovalaya’ about a thousand years ago in Karnataka, India. The unique feature of this literature is that it is scripted in numerals only and enciphered in such manner that deciphering could be done in different fashions which result in plain-texts in different languages. One page of this epic corresponds to one ‘Chakra’. A scheme for deciphering of Chakra is termed as ‘Bandha’. Only 1270 of Chakras available this day. A Chakra is a 27x27 matrix of integers in range from 1 to 64 only. Each of the Integers is associated or encoded with a phonetic character primarily of origin in Kannada Language. Deciphering of a Chakra in specific manners or applying corresponding Bandhas reveals poetry and verses in different languages. In addition to primarily in Kannada, the languages in which the Chakras manifest poetry and verses include Prakrita, Sanskrit, Telugu, Tamil, Aapabhransha and Pali etc.. It is considered that this wonderful design contains verses in 18 major languages and 700 minor one thus totaling 718 of dialects. The subject matter covers religious scriptures of Jains, Vedas, Ayurveda, Astrology and Mathematics too. This unique piece of literature could not attract attention of masses because it is scripted in numerals and decipherment is a very tedious job. This led to loss of not only the original manuscript of this precious work but also of five of the copies during the course of time. After this being laid dormant for about thousand years, great efforts of Pandit Yellappa Shastri brought it to light with the only available copy of it in existence. We all owe sincere gratitude to Pandit Yellappa Shastri for protecting and revealing this magnificent heritage. Sizeable content of this composition has not come to light due to difficulty in deciphering the schemes in respective Chakras.

The object of the proposed paper is to investigate some of the decipherment schemes which are deployed on Chakras to reveal plain-text. These schemes are labeled as Bandhas by Muni Kumudendra and he himself has described many of these Bandhas with associated nomenclature. It is remarkable to note that Bandhas implement many of Cryptographic algorithms, which have contemporary relevance and those were envisioned by Muni Kumudendra thousand years ago. These algorithms largely include substitution, transposition or permutation, and principles of Steganography etc. It may be another subject of investigation that how could Muni Kumudendra accomplish this unique highly complicated and complex mission which not only involved mathematical brilliance but also dexterity to put in great literature and enormous knowledge in it.

KEYWORDS
Chakra, Bandha, ChitraKavya, Substitution Cipher, Transposition Cipher, Steganography.

1. INTRODUCTION
Siri Bhoovalaya is an amazing piece of literature which is yet to be well discovered, assimilated and its content made accessible through conventional means of cognition. In its intrinsic structure it is a very strange conundrum even to highly learned readers. It is for this reason that this creation remained obscure for Centuries, until it found a great savior in the form of Pandit Yellappa Shastri in 1950s. He not only put years of tireless efforts to manually decipher part of this giant jigsaw, but also drew notice of broad class of scholars to this repository of knowledge.[1][2]

The objective of this dissertation is to identify Computer Assisted Methodologies which are suitable for dissemination of hidden text in this grand cryptic work. This involves study of algorithmic and non-algorithmic computational methods which may be employed in this framework.

We inferred that many of standard Cryptographic Algorithms could be suitably applied in deciphering the Chakras. Schemes on the implementation of Substitution, Transposition and Steganography algorithms are brought out in this paper. All of 1270 Chakras are divided into 56 Chapters and it is estimated that the whole subject matter consist of 600000 Shlokas or 140000 Characters. Huge coordinated effort is required to unearth entire multilingual content by expert linguists and technical geeks.[1][2]

2. APPLICATION OF CRYPTOGRAPHIC ALGORITHMS
Encryption schemes used by Muni Kumudendra included algorithmic and non-algorithmic ones. The intention was not to make decipherment computationally secure, as many of decipherment schemes are described by the author himself, but construct a structure that embedded Multilingual content in same cipher text. This was an inimitable act and nowhere else exists anything comparable to even on a miniature scale.

Following paragraphs contain description of these schemes.

A. Mono-alphabetic Substitution Cipher
In this encryption technique, a single cipher alphabet is substituted to a particular plaintext alphabet. A substitution table is used for mapping from plain alphabet to cipher
alphabet. For decryption of the cipher text into plaintext same substitution table is used for mapping from cipher alphabet to plain alphabet. [4]

All of the Chakras have stage one encryption using this technique; where by a plain alphabet is substituted with an Integer (range 1 to 64) arranged in a substitution table. In order to decipher a Chakra this substitution is done after applying other transformations to extract out plaintext.

Table 1 contains representation of Kannada Characters to be substituted with respective Integers.

Table 1: Mono-Alphabetic Substitution Table

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td></td>
</tr>
</tbody>
</table>

B. Transposition Cipher

A scheme based on permutation of the characters in the plaintext is termed as Transposition Cipher. [4] In Siri Bhoovalaya a variety of transposition cipher schemes are deployed. We are elaborating few of common ones.

1) Chakra-Bandhas:

In these transposition schemes whole of a Chakra (27x27 matrix) is transposed in different orientations described North, South, East and West. These different orientations are achieved transposing rows and columns or rotation in one direction sequentially. This cipher is termed as Chakra-Bandha by Muni Kumudendu.

Figure 1 illustrates Chakra-Bandha Transposition Matrix with North Orientation.

To decipher a Chakra-Bandha the 27x27 Matrix of the Chakra, all cells are traversed in the sequence as illustrated in the figure starting from cell designated as 1 to 729. Cell 1 is located at Row-1 and Column-14, Cell 2 is located at Row-27 Column-15 and so on until last Cell 729 at Row-27 Column-14 is traversed. Substitution of Integers in respective Cells with corresponding alphabets results in plaintext in Kannada composed in ‘Sangatya Chhanda’.

Deciphered Output of Chakra -1 in Chapter -1 is shown here in Figure 3. For this Transposition Table as shown in Figure -1 has been used.

Table 2: Transposition table for navamaank bandha

<table>
<thead>
<tr>
<th>Relative Column Positions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

Table 3: Relative Rows

<table>
<thead>
<tr>
<th>Relative Rows</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
</tbody>
</table>
Table 3: a chakra (27x27) divided in nine tiles (9X9)

As illustrated in the TABLE IV tiles (each one a 9x9 sub matrix) are transposed in Chakras described in Chapters 1 to 8. Tiling Scheme is illustrated in TABLE III

Table 4: Tile tranposition scheme

C. Algorithm for deciphering Chakra Bandha

Following is description for the algorithm to decipher transposition in 27x27 matrix of a Chakra as shown in FIGURE1 above. This algorithm is described as Chakra-Bandha by Muni Kumudendu.

```
Initialise ROW = 1 ; Column = 14;
:Outerloop ‘iterate for 27 times
   Initialise with New Row and Previous Column Values
   :Innerloop ‘iterate for 27 times
      GET Integer Value in Cell[I,J]
      Substitute Integer from Code-Table
      Append Character to Output file
      Compute Column = Column + 1
      If Column > 27 then Column = 1
   End Innerloop
   Compute Row = Row - 1
End Outerloop;
Close Output File;
END of Program.
```

Figure 2: Algorithm for Chakra-Bandha

Same algorithm applies to transpose 9x9 matrix as in Navamaank-Bandh. In that algorithm initialization and loop parameters need to be specified accordingly. [3]

D. Implementation and Outcome

We used MicroSoft Small Basic to implement these algorithms. It was a rigorous exercise to create error frees Chakra Files which are Input to the program. [3]

Figure 3: Screenshot of Deciphered Chakra

3. STENOGRAPHIC SCHEMES

In Steganography the intended message is hidden either to conceal its existence or render it unintelligible to outsiders.[4]

We find that principles of Steganography have been used in numbers ways in Siri Bhoovalaya. For example if the Chakra 1-1-1 is deciphered using Chakra-Bandha the resulting text is in Kannada. If first Character of each of the lines of this Kannada Text is picked up, and assembled it results in a Gatha in Prakrit. If the character in the center of each of the Kannada text is picked up it aggregates to a Shloka in Sanskrit.

Beside this technique of Steganography where a message is hidden inside a message, Muni Kumudendu has applied a number of Graphical Patterns which when transposed on the Chakra Matrix reveal poetry and verses. This technique has been practiced in small extents by some Sanskrit poets and is described as Chitra Kavya. A large variety of Chitra-Bandhas or Chitra-Kavyas have been used by Muni Kumedendu.

Figure 4: Example of ChitraKavya Bandh

Herein above example the numbers are indicative of the relative cell numbers (range 1 to 729) in the 27x27 matrix of the chakra. Each cell contains a number (range 1 to 64). Stating from cell 1 its content is substituted with corresponding Character and appended into a text-string with corresponding character in next Cell. Thus all characters add up from the contents in Cells starting from 1 to the last in the ChitraBandh.

CONCLUSION

We have attempted to analyze the decipherment schemes to a level, but we estimate that there lies much more to explore when further investigations are conducted. One of the vital requirement of this project is to have a team of programmers and analysts together with team of experts in Literature in major Languages viz. Kannada, Prakrit, Sanskrit etc.
Author would like to admit that he has only been able to get a glimpse of the great ocean of potentials in this dissertation. A well-coordinated multi-disciplinary group of research participants is required to comprehend underlying knowledge for the benefit of humankind.

FUTURE SCOPE

Further analysis and design of algorithms to extract the multilingual contents is a major assignment of the future work. A very important addition that we propose is to make decipherment in phonetic scheme so that audible output is generated which would be neutral or free of the scripts in specific languages and thus may be easily comprehended by larger class of people in their own language of perception. This will accomplish the spirit of this Multilingual epic which is also described as ‘Sarva Bhashamayi Kavya’ meaning poetry encompassing all languages.

REFERENCES


