

An Inimitable Cryptographic Creation: Siri Bhoovalaya

Anil Kumar Jain

SMIEEE, FIETE, FIE(I),SMCSI

ak.jain@ieee.org

ABSTRACT

Muni Kumudendu, 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, Apabhramsha 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 Kumudendu 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 Kumudendu 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 Kumudendu 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 obscured 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 1400000 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 Kumudendu 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.

[1] = "ಅ"	[9] = "ಙ"	[17] = "ಠ"	[25] = "ಱ"	[33] = "ಲ"	[41] = "ಳ"	[49] = "಴"	[57] = "ವ"
[2] = "ಆ"	[10] = "ಚ"	[18] = "ಠಾ"	[26] = "ಱಾ"	[34] = "ಲಾ"	[42] = "ಳಾ"	[50] = "಴ಾ"	[58] = "ವಾ"
[3] = "ಇ"	[11] = "ಛ"	[19] = "ಠಿ"	[27] = "ಱಿ"	[35] = "ಲಿ"	[43] = "ಳಿ"	[51] = "಴ಿ"	[59] = "ವಿ"
[4] = "ಏ"	[12] = "ಞ"	[20] = "ಠೀ"	[28] = "ಱೀ"	[36] = "ಲೀ"	[44] = "ಳೀ"	[52] = "಴ೀ"	[60] = "ವೀ"
[5] = "ಓ"	[13] = "ತ"	[21] = "ಠೋ"	[29] = "ಱೋ"	[37] = "ಲೋ"	[45] = "ಳೋ"	[53] = "಴ೋ"	[61] = "ವೋ"
[6] = "ಔ"	[14] = "ಥ"	[22] = "ಠೊ"	[30] = "ಱೊ"	[38] = "ಲೊ"	[46] = "ಳೊ"	[54] = "಴ೊ"	[62] = "ವೊ"
[7] = "ಋ"	[15] = "ದ"	[23] = "ಠೊ"	[31] = "ಱೊ"	[39] = "ಲೊ"	[47] = "ಳೊ"	[55] = "಴ೊ"	[63] = "ವೊ"
[8] = "ೠ"	[16] = "ಧ"	[24] = "ಠೊ"	[32] = "ಱೊ"	[40] = "ಲೊ"	[48] = "ಳೊ"	[56] = "಴ೊ"	[64] = "ವೊ"

Table 1: Mono-Alphabetic Substitution 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

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	
1	380	409	438	467	496	525	554	583	612	641	670	699	728	1	30	59	88	117	146	175	204	233	262	291	320	349	378
2	408	437	466	495	524	553	582	611	640	669	698	727	27	29	58	87	116	145	174	203	232	261	290	319	348	377	379
3	436	465	494	523	552	581	610	639	668	697	726	26	28	57	86	115	144	173	202	231	260	289	318	347	376	405	407
4	464	493	522	551	580	609	638	667	696	725	25	54	56	85	114	143	172	201	230	259	288	317	346	375	404	406	435
5	492	521	550	579	608	637	666	695	724	24	53	55	84	113	142	171	200	229	258	287	316	345	374	403	432	434	463
6	520	549	578	607	636	665	694	723	23	52	81	83	112	141	170	199	228	257	286	315	344	373	402	431	433	462	491
7	548	577	606	635	664	693	722	22	51	80	82	111	140	169	198	227	256	285	314	343	372	401	430	459	461	490	519
8	576	605	634	663	692	721	21	50	79	108	110	139	168	197	226	255	284	313	342	371	400	429	458	487	489	518	547
9	604	633	662	691	720	20	49	78	107	109	138	167	196	225	254	283	312	341	370	399	428	457	486	488	517	546	575
10	632	661	690	719	19	48	77	106	135	137	166	195	224	253	282	311	340	369	398	427	456	485	487	516	545	574	603
11	660	689	718	18	47	76	105	134	136	165	194	223	252	281	310	339	368	397	426	455	484	513	515	544	573	602	631
12	688	717	17	46	75	104	133	162	164	193	222	251	280	309	338	367	396	425	454	483	512	514	543	572	601	630	659
13	716	16	45	74	103	132	161	163	192	221	250	279	308	337	366	395	424	453	482	511	540	542	571	600	629	658	687
14	15	44	73	102	131	160	189	191	220	249	278	307	336	365	394	423	452	481	510	539	541	570	599	628	657	686	715
15	43	72	101	130	159	188	190	219	248	277	306	335	364	393	422	451	480	509	538	567	569	598	627	656	685	714	14
16	71	100	129	158	187	216	218	247	276	305	334	363	392	421	450	479	508	537	566	568	597	626	655	684	713	13	42
17	99	128	157	186	215	217	246	275	304	333	362	391	420	449	478	507	536	565	594	596	625	654	683	712	12	41	70
18	127	156	185	214	243	245	274	303	332	361	390	419	448	477	506	535	564	593	595	624	653	682	711	11	40	69	98
19	155	184	213	242	244	273	302	331	360	389	418	447	476	505	534	563	592	621	623	652	681	710	10	39	68	97	126
20	183	212	241	270	272	301	330	359	388	417	446	475	504	533	562	591	620	622	651	680	709	9	38	67	96	125	154
21	211	240	269	271	300	329	358	387	416	445	474	503	532	561	590	619	648	650	679	708	8	37	66	95	124	153	182
22	239	268	297	299	328	357	386	415	444	473	502	531	560	589	618	647	649	678	707	7	36	65	94	123	152	181	210
23	267	296	298	327	356	385	414	443	472	501	530	559	588	617	646	675	677	706	6	35	64	93	122	151	180	209	238
24	295	324	326	355	384	413	442	471	500	529	558	587	616	645	674	676	705	5	34	63	92	121	150	179	208	237	266
25	323	325	354	383	412	441	470	499	528	557	586	615	644	673	702	704	4	33	62	91	120	149	178	207	236	265	294
26	351	353	382	411	440	469	498	527	556	585	614	643	672	701	703	3	32	61	90	119	148	177	206	235	264	293	322
27	352	381	410	439	468	497	526	555	584	613	642	671	700	729	2	31	60	89	118	147	176	205	234	263	292	321	350

Figure 1: Chakra-Bandha Transposition table

2) Navmaank-Bandha:

In these Transposition Scheme, whole of a Chakra i.e. 27x27 matrix is tiled into 3x3 matrices where each of the tiles is a 9x9 matrix Units. Transposition Sequence of these tiles is different for different chapters.

Transposition sequence inside a tile is illustrated in TABLE III and Tile Sequencing Scheme in different Chapters is mentioned in TABLE IV.

		<i>Relative Column Positions</i>								
		1	2	3	4	5	6	7	8	9
<i>Relative Rows</i>	1	47	58	69	80	1	12	23	34	45
	2	57	68	79	9	11	22	33	44	46
	3	67	78	8	10	21	32	43	54	56
	4	77	7	18	20	31	42	53	55	66
	5	6	17	19	30	41	52	63	65	76
	6	16	27	29	40	51	62	64	75	5
	7	26	28	39	50	61	72	74	4	15
	8	36	38	49	60	71	73	3	14	25
	9	37	48	59	70	81	2	13	24	35

Table 2: Transposition table for navamaank bandha

Columns : 1 to 27 of the Chakra			
Rows : 1 to 27	Tile 1 9x9 Matrix	Tile 2 9x9 Matrix	Tile 3 9x9 Matrix
	Tile 4 9x9 Matrix	Tile 5 9x9 Matrix	Tile 6 9x9 Matrix
	Tile 7 9x9 Matrix	Tile 8 9x9 Matrix	Tile 9 9x9 Matrix

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

CH-2	CH-3	CH-4	CH-5	CH-6	CH-7	CH-8
3 4 5	2 3 4	9 2 3	8 9 2	7 8 9	6 7 8	5 6 7
2 1 6	9 1 5	8 1 4	7 1 3	6 1 2	5 1 9	4 1 8
9 8 7	8 7 6	7 6 5	6 5 4	5 4 3	4 3 2	3 2 9

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 free Chakra Files which are Input to the program. [3]

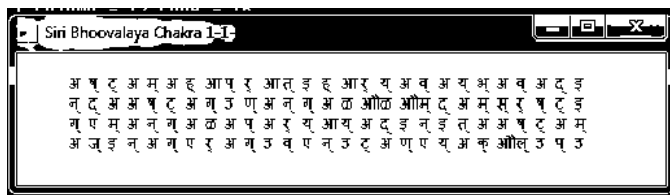


Figure 3: Screenshot of Deciphered Chakra

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.

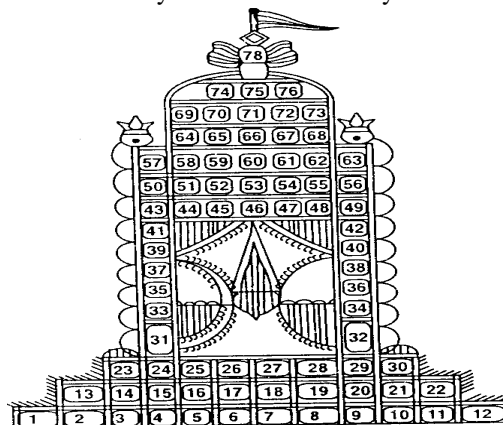


Figure 4: Example of ChitraKavya Bandh

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). Starting 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 multi-lingual 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

- [1]. Sri Kumudendu Muni: Hindi Translation: Swarna Jyothi : "*Siribhoovalaya Hindi Vol 1*": Edited and Revised by Hon.Editorial Board, Pustakshakti: Pustak Shakti Publication, Bangalore, 2008.
- [2]. Sri Kumudendu Muni: "*Siribhoovalaya Volume - 2 (Chapters 9 - 20)*": Edited and Revised by Hon.Editorial Board, Pustakshakti: Pustak Shakti Publication, Bangalore, 2008..
- [3]. Anil Kuamr Jain ; "Siri Bhoovalaya : A Unique Multilingual Epic scripted in numerals" : Submitted at 3rd National Conference on India Language Computing – 2013. Cochin, India.
- [4]. William Stallings : '*Cryptography and Network Security - Principles and Practices*': Fourth Edition : Pearson Education India: 2006.