Indian Journal of Cryptography and Network Security (IJCNS)
ISSN: 2582-9238 (Online), Volume-4 Issue-2, November 2024

An Analytical Approach to Understanding the Principles of Cryptography within the *kaṭapayādi* System as Reflected in the Works of Nemicandra

Prajna Jadhav

Abstract: ***The kaṭapayādi system is an alphabetic system of numeral notation developed in India. This paper aims to understand the ideas related to cryptography within the kaṭapayādi system, although this system was not developed to hide information. To do this, this paper studies the use of this system in the Gommaṭasāra-Jīvakāṇḍa and Trilokasāra of Nemicandra (981 CE) using an analytical approach. This paper finds that, like the Caesar cipher and Vigenère cipher, the ciphertext in this system is also a substitution cypher, but unlike them, the letters of the Sanskrit alphabet substitute the digits of a number in it with no shift. This system provides multiple ways to encrypt a number. It has symmetric encryption. Correctness property is ensured in it. In it, the writer is the one who encrypts the number into ciphertext, and the one who decrypts the ciphertext into a number is the reader. The key in this system was not a public key, although it was publicly available.***

Keywords: Cryptographic Ideas, India, kaṭapayādi System, Nemicandra

I. INTRODUCTION

In ancient India, texts were composed in verse. The various words composing a verse were selected in such a way that they could fit with the meter prescribed for the verse. While writing numbers in verse, number-symbols could not fulfill this condition. Therefore, number-words were employed to write them [1]. See ordinary mode in Appendix. To achieve greater convenience, two major schemes of expressing numbers in the metrical pattern of Sanskrit verses were developed [2]. In the first scheme, commonly known as object-numerals, the digits 1 to 9 and zero were expressed by certain significant words [3]. In the second scheme they were represented by the Sanskrit alphabets. Two main systems, the system found in the *Āryabhaṭīya* (499 CE) of Āryabhaṭa I (born 476 CE) and the *kaṭapayādi* system, fall under this second scheme [1]. Later these schemes were extended to other Indic languages like Prakrit, Malayalam, etc [2].

The *kaṭapayādi* system is an alphabetic system of numeral notation.

Manuscript received on 25 October 2024 | Revised Manuscript received on 11 November 2024 | Manuscript Accepted on 15 November 2024 | Manuscript published on 30 November 2024.
*Correspondence Author(s)
Prajna Jadhav*, Ph.D. Student, Department of Chinese Language, Sanchi University of Buddhist-Indic Studies, Sanchi, Dhakna Chapna, (Madhya Pradesh), India. Email ID: prajnajadhav07@gmail.com, ORCID ID: 0009-0007-3302-3320

In this system, letters of the Sanskrit alphabet are used in place of digits (i.e., 1 to 9 and 0) to express numbers. Nemicandra (c. 981 CE) composed seventeen numbers using this system in his works, which he wrote in Prakrit.

Recent studies show that cryptographic concepts such as hashing functions, encryption, and decryption are also associated with the *kaṭapayādi* system. Anand V. Raman finds that the *kaṭapayādi* system can be considered an early precursor to modern hash functions [4]. Applying the *kaṭapayādi* system with the idea of transpose, Priya and Parameswaran encrypted 3570232422 into the Vigenère cipher

satyameva jayate nānṛtam,

which literally means *truth alone triumphs, not falsehood*. Here they took *bhāratam* (= 624) as a key. They also applied the *kaṭapayādi* system to create Affine cipher [5].

All of the above leads us to study the *kaṭapayādi* system in the context of cryptography. Therefore, the purpose of this paper is to understand the ideas related to cryptography within the *kaṭapayādi* system. We will do this through the use of this system in Nemicandra's works using an analytical approach.

II. CRYPTOGRAPHY

Cryptography is the science of writing and breaking codes [6]. This definition accurately captures the essence of classical cryptography, but modern cryptography is heavily based on mathematics and computer science and is used to write a message with the intention of hiding its meaning [7]. When we say classical cryptography, we are talking about cryptography that predates computers. A message that can be read and understood without any special processing is called plaintext. Cryptography enables us to store sensitive information or transmit it over insecure networks so that it cannot be read by anyone except the intended recipient. Encryption is a major application of cryptography. It is used to conceal information from prying eyes. It uses an algorithm called a *cipher* and a secret value called a *key*. The key is used to encrypt the plaintext into a ciphertext. The process of reverting ciphertext to its original plaintext is called decryption. Cryptanalysis is the science of breaking cryptosystems. Classical cryptanalysis involves an interesting combination of analytical reasoning, pattern searching, etc [8]. Cryptography and cryptanalysis together are called cryptology [6].

Table 1: Key in *kaṭapayādi* System

	1	2	3	4	5	6	7	8	9			0		
Consonant	क्	ख्	ग्	घ्	ङ्	च्	छ्	ज्	झ्	ञ्	Vowel (when standing alone)	अ	आ	इ
	k	*kh*	*g*	*gh*	*ṅ*	*c*	*ch*	*j*	*jh*	*ñ*		*a*	*ā*	*i*
	ट्	ठ्	ड्	ढ्	ण्	त्	थ्	द्	ध्	न्		ई	उ	ऊ
	ṭ	*ṭh*	*ḍ*	*ḍh*	*ṇ*	*t*	*th*	*d*	*dh*	*n*		*ī*	*u*	*ū*
	प्	फ्	ब्	भ्	म्							ऋ	ए	ऐ
	p	*ph*	*b*	*bh*	*m*							*ṛ*	*e*	*ai*
	य्	र्	ल्	व्	श्	ष्	स्	ह्				ओ	औ	आदि
	y	*r*	*l*	*v*	*ś*	*ṣ*	*s*	*h*				*o*	*au*	*etc.*

III. *KAṬAPAYĀDI* SYSTEM

The *kaṭapayādi* system originated in Kerala. The earliest text employing this system is the *Candra-vākyas*. These *vākyas* are attributed to the Kerala astronomer Vararuci. He is traditionally ascribed to the fourth century CE. The *kaṭapayādi* system was employed continuously not only in astronomical and mathematical literature, but also in other genres until the present times [2].

"Though the *kaṭapayādi* system," writes S. R. Sarma, "was followed extensively for a very long time in Kerala, it is strange that there are no definitions earlier than the one in the *Sadratnamālā* of the nineteenth century! Perhaps it was thought unnecessary to define it as it was universally known [2]."

Apart from facilitating the development of mnemonic tables like the *Candra-vākyas*, the *kaṭapayādi* system in Kerala helped to develop a uniform mode of dating events in terms of the civil days elapsed since the commencement of the present Kali era, which began at sunrise on Friday, February 18, 3102 BCE [2]. The *kaṭapayādi* system was also famous in northern India. Sarma refutes B. B. Datta and A. N. Singh's contention that four distinct variants of this system existed [1]. He shows that there were only two genuine variants of the system. The first is with the sinistral move, which is the Kerala system. The second is with the dextral move [2].

The *kaṭapayādi* system is defined prior to the *Sadratnamālā* in the following verse [9], which Ṭoḍaramala (1720-1767 CE) refers to in his commentary, called the *Samyakjñānacandrikā*, on the *Gommaṭasāra-Jīvakāṇḍa* of Nemicandra (981CE) [10].

कटपय पुरस्थवर्णैर्नवनव पञ्चाष्ट कल्पितैः क्रमशः।
स्वरञन शून्यं संख्या मात्रो परिमाक्षरं त्याज्यं॥

"The consonants [in succession], standing before [the vowels standing as strokes], beginning [severally] with *ka*, *ṭa*, *pa*, and *ya* denote [from one to] nine, nine, five, and eight respectively. The vowel [standing alone], *ña*, and *na* [each] represent zero. The vowel symbols [i.e., the vowels attached to the consonants as strokes] and the upper letter [i.e., the first consonant in a conjunct consonant] are to be ignored."

This is detailed in Table-I.

IV. USE OF *KAṬAPAYĀDI* SYSTEM IN NEMICANDRA'S WORKS

Ācārya Nemicandra "Siddhānta Cakravartī" was a Jaina ascetic. The *Gommaṭasāra-Jīvakāṇḍa* and *Trilokasāra* are two of his many works. The first is on Karma system while the second deals with cosmology. His disciple Cāmuṇḍarāya, who was a celebrated commander-in-chief and wise minister of the *Gaṇga* dynasty from 953 CE to 985 CE, erected the world famous colossal image of Bāhubalī at Śravaṇabeḷagoḷa. Nemicandra is said to have been in attendance at the first consecration ceremony of this image. This ceremony was held on 13th March of 981 CE [11].

In addition to the ordinary mode of expressing numbers, i.e., in words, not in number-symbols, Nemicandra occasionally employs the *kaṭapayādi* system in his above two works. He composed seventeen numbers using this system, sixteen in the *Gommaṭasāra-Jīvakāṇḍa* and only one in the *Trilokasāra*. Of them, two notations are written in sinistral move while the rest are in dextral move [12]. These seventeen notations are shown in Table-II. For details, see Appendix.

V. RESULTS AND DISCUSSION

There are two types of encryptions. One is symmetric and the other is asymmetric. In asymmetric encryption, the key used to decrypt is different from the key used to encrypt, while in symmetric encryption, the key used to decrypt is the same as the key used to encrypt [8]. Therefore, the *kaṭapayādi* system can be said to be a symmetric encryption

There are many classical ciphers, but the most famous are the Caesar cipher and Vigenère cipher. They are so named because Julius Caesar (100 BCE-44 BCE) used the Caesar cipher and Blaise de Vigenère (sixteenth century) invented the Vigenère cipher. The Caesar cipher encrypts a message by shifting each letter down three positions in the alphabet.

Table II: Alphabetic Notations Composed by Nemicandra

Alphabetic notation	Number denoted	Move used
rā-ga	32	sinistral
ta-la-lī-na-ma-dhu-ga-vi-ma-laṃ-dhu-ma-si-lā-gā-vi-co-ra-bha-ya-me-rū-ta-ṭa-ha-ri-kha-jha-sā	792281625142643375935439503 36	sinistral
vā-pa-ṇa-na-ra-no-nā-na	41502000	dextral
ka-na-ja-ta-ja-ma-ṭā-na-na-ma	108685005	dextral
ja-na-ka-na-ja-ya-sī-ma	80108175	dextral
ga-ta-na-ma[*-no-na-naṃ*]	3605000	dextral
ma-na-gaṃ[*-no-na-naṃ*]	503000	dextral
go-ra-ma[*-no-na-naṃ*]	325000	dextral
ma-ra-ga-ta[*-no-na-naṃ*]	5236000	dextral
ja-va-gā-ta-no-na-naṃ	8436000	dextral
ja-ja-lakkha	8800000	dextral
ma-na-na-na	5000	dextral
dha-ma-ma-na-no-na-na-nā-maṃ	955000005	dextral
ra-na-dha-ja-dha-rā-na-na	20989200	dextral
yā-ja-ka-nā-me-nā-na-na	18105000	dextral
kā-na-va-dhi-vā-ca-nā-na-na	104946000	dextral
va-ṭa-la-va-ṇa-ro-ca-go-na-ga-na-ja-ra-na-gaṃ-kā-sa-sa-sa-gha-dha-ma-pa-ra-ka-dha-raṃ	4134526303082031777495121 92	dextral

For example, ZEBRA encrypts to CHEUD, which we can show as

$$\begin{matrix} Z & E & B & R & A \\ 3 & 3 & 3 & 3 & 3 \\ C & H & E & U & D \end{matrix}.$$

The Vigenère cipher is similar to the Caesar cipher, except that the letters are not shifted by three places, but rather by values defined by a key. For example, when CAT is used as the key, ZEBRA encrypts to CFVUB [8], which we can show as

$$\left(\underset{C}{\overset{Z}{=3}}\right)\left(\underset{F}{\overset{E}{A=1}}\right)\left(\underset{V}{\overset{B}{T=20}}\right)\left(\underset{U}{\overset{R}{=3}}\right)\left(\underset{B}{\overset{A}{A=1}}\right).$$

Based on the observation of Table-II, we can say that the *kaṭapayādi* system like the Caesar cipher and Vigenère cipher is also a substitution cipher, but unlike them in the *kaṭapayādi* system the letters of the Sanskrit alphabet substitute the digits of a number with no shift. The key is such that the consonants for substitution are arbitrarily chosen from their respective fixed sets. For example, Nemicandra arbitrarily chose *r* and *g* for the ciphertext *rā-ga* from the sets {*kh*, *ṭh*, *ph*, *r*} and {*g*, *ḍ*, *b*, *l*} respectively. Not only this, the vowels attached to the consonants as strokes are also chosen arbitrarily. In this ciphertext he has chosen *ā* and *a* as the strokes for *r* and *g* respectively. Since there are four consonants available for each of 1, 2, 3, 4, and 5, three consonants for each of 6, 7 and 8, two consonants for 9, two consonants plus all vowels for 0 and any vowel can be attached to the consonant as stroke, we have a variety of ways to encrypt a number. This type of feature of the *kaṭapayādi* system makes the ciphertext quite secure.

While doing all this, there is a condition that the meter of the respective verse should remain intact. While encrypting plaintext into ciphertext, it is up to the author to create a ciphertext that has literal sense or not. Each of the seventeen ciphertexts created by Nemicandra has no literal sense. On the other hand, the ciphertext

āyurārogyasaukhyam,

created by Nārāyaṇa Bhaṭṭatiri, a great Sanskrit poet from Kerala, at the end of his devotional poem *Nārāyaṇīyam*, is a chronogram indicating Kali-day 1712210, the date of completion of his work, which corresponds to 8 December 1586 (Gregorian) and is also a benediction for longevity, health and bliss for himself and his readers [2].

A Shannon cipher (*S*), the concept of which was first introduced by its namesake Claude Elwood Shannon (1916-2001) in his 1949 paper [13], is a simplified cipher mechanism for encrypting a message using a shared key. Mathematically, it is a pair of functions. That is, $S=(E,D)$. *E*, the encryption function, takes as input a key *k* and a plaintext *p*, also called a message, and produces as output a ciphertext *c*. That is, $c=E(k,p)$. *c* is said the encryption of *p* under *k*. *D*, the decryption function, takes as input a key *k* and a ciphertext *c* and produces as output a plaintext *p*. That is, $p=D(k,c)$. *p* is said the decryption of *c* under *k* [14]. On comparison, we find that number and alphabetic notation in Table-II are *p* and *c* respectively and Table-I is *k*. We are able to see through Table-II that $D(k,E(k,p))=p$, called the correctness property, is ensured in the *kaṭapayādi* system.

Jean-Philippe Aumasson writes that, “Based on simplistic ciphers like the Caesar and Vigenère ciphers, we can try to abstract out the workings of a cipher, first by identifying its two main components: a permutation and a mode of operation. A *permutation* is a function that transforms an item such that each item has a unique inverse. A *mode of operation* is an algorithm that uses a permutation to process messages of arbitrary size. The mode of the Caesar cipher is trivial: it just repeats the same permutation for each letter, but …, the Vigenère cipher has a more complex mode, where letters at different positions undergo different permutations. … [Now we will see how] they [i.e., permutation and its mode] relate to a cipher’s security. In order to be secure, a cipher’s permutation should satisfy three criteria. (1) The permutation should be determined by the key, so as to keep the permutation secret as long as the key is secret. In the Vigenère cipher, if you don’t know the key, … you can’t easily decrypt. (2) Different keys should result in different permutations. In the Vigenère cipher, each letter from the key determines a substitution. … (3) The permutation should look random … There should be no pattern in the ciphertext after performing a permutation, because patterns make a permutation predictable for an attacker, and

therefore less secure. … The word BANANA therefore encrypts to MXLXLX … But analyzing these duplicates, you might not learn the entire message, but you will learn something about the message… You do not need the key to guess that the plaintext has the same letter at the three X positions and another same letter at the two L positions. So if you know, for example, that the message is a fruit's name, you could determine that it is BANANA rather than CHERRY, …, or another six-letter fruit. The mode of operation of cipher mitigates the exposure of duplicate letters in the plaintext by using different permutations for duplicate letters. The mode of the Vigenère cipher partially addresses this: … To build a secure cipher, you must combine a secure permutation with a secure mode [8]."

Based on this, we can say that the *kaṭapayādi* system satisfies the first criterion if its key is kept secret. Since a consonant from the respective fixed set is arbitrarily chosen instead of a fixed consonant to substitute the digit of a given number, the system satisfies the last two criteria, if not completely, to a large extent. Despite the availability of the facility, Nemicandra used mostly the same consonants for duplicates, i.e., repeated digits. But he chose *r*[*i*]-*kh*[*a*] for 22 and *l*[*ā*]-*g*[*ā*] for 33 in *ta-la-lī-…-lā-gā-…-ri-kha-jha-sā*. See Table-II. Since the *kaṭapayādi* system can use different permutations for duplicate entire numbers, it is capable, especially more so when the vowels attached as strokes to the consonants are also arbitrarily chosen, to provide a secure mode. However, the one-time pad is the most secure cipher.

In addition to the above, Nemicandra's ciphertexts have three features worth noting: the use of two types of move, four ciphertexts in which *no-na-naṃ* is not written, and the use of the ciphertext with the plaintext. To decrypt a ciphertext with one or two or three of these three features, the decoder must include knowledge of the plaintext, the context in which it is discussed and its various aspects in his cryptanalysis, even if the key is available. It was up to the author to decide which move to apply in writing the ciphertext so as to maintain the meter of the verse in question. Except for "*kā-na-va … ka-dha-raṃ*," the *ciphertexts* written by Nemicandra in the dextral move ends either at zero, encoded by him using *n*, or at five, encoded by him using *m*. This is because these two consonants sound sweet at the end of a word. If the dextral move is standard, the sinistral move is its transpose. We are able to see that he did not write *no-na-naṃ* with *ga-ta-na-ma*, *ma-na-gaṃ*, *go-ra-ma*, and *ma-ra-ga-ta*, but has written with *ja-va-gā-ta*. See Table-I and Appendix. No doubt, by doing this he saved space and avoided repetition. *ja-ja-lakkha* is a partial ciphertext as *lakkha* means one hundred-thousand.

These features make the ciphertext more secure because such ciphertext is harder to decode.

VI. CONCLUSION

Based on the above study, we can say that the elements of cryptography are found in the *kaṭapayādi* system although the fact is that this system was not developed to keep information concealed. This system by default protected the data from being corrupted by the manuscript-copyist although there was no threat to the data, but the data would have been corrupted if it had been written using number-symbols. In this system the author is the one who encrypts the number into ciphertext and the one who decrypts the ciphertext into number is the reader. Since the key was universally known in Indian literature, the author used not to provide the key along with the verse containing the ciphertext. Sometimes commentators like Ṭoḍaramala would provide the key. Although the key was publicly available, it was not a public key because it was not the key of an asymmetric key pair. The key, i.e., Table-I, is very long in size and static in use.

APPENDIX

Nemicandra's Modes of Expressing Numbers

Ordinary Mode

बारुत्तरसयकोडी तेसीदी तह य होंति लक्खाणं।
अट्ठावण्णसहस्सा पंचेव पदाणि अंगाणं॥
[15] (v. 350, p. 199)

"[The total number of] the words in the [twelfth] *Aṅga* [of the Jain canon] is one hundred and twelve ten-million, eighty-three hundred-thousand, fifty-eight thousand and five [i.e., 1128358005]."

kaṭapayādi Mode

इगिवितिचखचडवारं खसोलरागट्ठदालचउसट्ठिं।
संठविय पमदठाणे णट्ठुद्दिट्ठं च जाण तिट्ठाणे॥
[15] (v. 44, p. 34)

"One, two, three, four; zero, four, eight, twelve; zero, sixteen, *rā-ga* [i.e., 32], sixty-four. To find out [the structure of a] lost [tuple] and [the position of a] mentioned [tuple], place these in three rows of carelessness."

तललीनमधुगविमलं धूमसिलागाविचोरभयमेरू।
तटहरिखझसा होंति हु माणुसपज्जसंखंका॥
[15] (v. 158, p. 104)

"The digits of the number of the developable human souls is *ta-la-lī-na-ma-dhu-ga-vi-ma-laṃ dhu-ma-si-lā-gā vi-co-ra-bha-ya-me-rū ta-ṭa-ha-ri-kha-jha-sā* [i.e., 792281625142643375935439503 36]."

वापणनरनोनानं एयारंगे जुदा हु वादम्मि।
कनजतजमताननमं जनकनजयसीम बाहिरे वण्णा॥
[15] (v. 360, p. 203)

"[The total number of the words] in the eleven *Aṅgas* [is] *vā-pa-ṇa-na-ra-no-nā-na* [i.e., 41502000]. And in the [*Dṛṣṭi*]*vāda* [i.e., the twelfth Aṅga], it is *ka-na-ja-ta-ja-ma-tā-na-na-ma* [i.e., 108685005]. And in the Bāhira (Skt. Bāhya, i.e., Aṅgabāhya), the [total number of] letters [is] *ja-na-ka-na-ja-ya-sī-ma* [i.e., 80108175]."

गतनम मनगं गोरम मरगत जवगातनोननं जजलक्खा।
मननन धममननोननननामं रनधजधरानन जलादी॥
याजकनामेनाननमेदाणि पदाणि होंति परिकम्मे।
कानवधिवाचनाननमेसो पुण चूलियाजोगो॥
[15] (vv. 363-364, p. 204)

"[The number of the words in the *Candraprajñapti*, *Sūryaprajñapti*, *Jambūdvīpaprajñpti*, *Dvīpasāgara- prajñpti* and *Vyākhyāprajñpti* are] *ga-ta-na-ma* [*-no-na-naṃ*, i.e., 3605000], *ma-na-gaṃ* [*-no-na-naṃ*, i.e., 503000], *go-ra-ma* [*-no-na-naṃ*, i.e., 325000], *ma-ra-ga-ta* [*-no-na-naṃ*, i.e., 5236000], and *ja-va-gā-ta-no-na-naṃ* [i.e., 8436000] [respectively]. [In the Sūtras, it is] *ja-ja lakkha* (Skt. *lakṣa*) [i.e., 8800000]. [In the *Prathamānuyoga*, it is] *ma-na-na-na* [i.e., 5000. [In the fourteen *Pūrvas*, it is] *dha-ma-ma-na-no-na-na-nā-maṃ* [i.e., 955000005]. [In each of the five *Cūlikās*, namely], *Jala*[*gatā*], etc., [it is] *ra-na-dha-ja-dha-rā-na-na* [i.e., 20989200]. [The total number of the words in the above first five is] *yā-ja-ka-nā-me-nā-na-na* [i.e., 18105000]. The sum [of the words] in the *Cūliyā* (Skt. *Cūlikā*) [is] *kā-na-va-dhi-vā-ca-nā-na-na* [i.e., 104946000]."

वटलवणरोचगोनगनजरनगंकाससघधमपरकधरं।
विगुणणवसुण्णसहिया पल्लस्स दु रोमपरिसंखा॥
[16] (v. 98, p. 92)

"The number of hairs in a cylinder [of diameter one *yojana* and depth one *yojana*] is obtained when two-multiplied-by-nine [i.e., eighteen] zeros follow *va-ṭa-la-va-ṇa-ro-ca-go-na-ga-na-ja-ra-na-gaṃ-kā-sa-sa-sa-gha-dha-ma-pa-ra-ka-dha-raṃ* [i.e., 413452630308 20317774 9512192]."

ABBREVIATIONS

Skt.	Sanskrit
v.	verse
vv.	verses

NOTATION

[…]	A pair of square brackets, wherever used except for numbering citations, contains a paraphrase inserted by me to achieve clear comprehensiveness.

GLOSSARY

ārogya	health
āyur	longevity
ca (Skt. *catuḥ*)	four
Candra-vākyas	"Moon-sentences" or "Longitudes of the Moon"
ca^usaṭṭhi (Skt. *catuḥṣaṣṭi*)	sixty-four
ḍa (Skt. *aṣṭa*)	eight
ega (Skt. eka)	one
Gommaṭasāra	"An essence extracted on the *karma* system and composed for *Gommaṭa*, i. e. Cāmuṇḍarāya"
Jīvakāṇḍa	"Section regarding soul"
kha	zero
koḍi	ten-million
lakkha (Skt. *lakṣa*)	hundred-thousand
māṇusapajja (Skt. *mānuṣa-paryāpta*)	developable human souls
mātrā	vowel symbol
ṇaṭṭha (Skt. *naṣṭa*)	lost
pada	word
pamada (Skt. *pramāda*)	carelessness
palla (Skt. *palya*)	cylinder
purastha	standing before
roma	hair
saṃkhaṃka (Skt. *saṅkhyā-aṅka*)	digits of the number
śūnya	zero
saukhya	bliss
sola (Skt. *ṣoḍaśa*)	sixteen
svara	vowel
ti (Skt. *tri*)	three
Trilokasāra	"Essence of the three regions of the universe"
uddiṭṭha (Skt. *uddiṣṭa*)	mentioned
vāra (Skt. *dvādaśa*)	twelve
varṇa	consonant
vaṇṇa (Skt. *varṇa*)	letter
vi (Skt. *dvi*)	two
yoga	sum

ACKNOWLEDGMENT

Barring a few changes, including its title, I presented this paper online at the International Conference on the History of Mathematics 2023-24, held at the Indian Institute of Technology, Guwahati on January 19-21, 2024. I take this opportunity to thank the organizers of the conference for giving me the opportunity. I am grateful to the editor of this journal and the anonymous reviewer of this paper for their comments and suggestions. I would like to thank my mentors Dr. Prachi Aggarwal (Delhi University) and Dr. Santosh Priyadarshi (Sanchi University of Buddhist-Indic Studies) for their guidance. Last but not least, I would like to put on record the guidance I received from my father Dr. Dipak Jadhav (Barwani).

DECLARATION STATEMENT

I, Prajna Jadhav, declare that the research paper titled "An Analytical Approach to Understanding the Principles of Cryptography within the *kaṭapayādi* System as Reflected in the Works of Nemicandra" submitted for publication in the *Indian Journal of Cryptography and Network Security* is my original work.

I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed solely.

REFERENCES

1. B. B. Datta and A. N. Singh, *History of Hindu Mathematics*, Part I. Lahore: Motilal Banarsidass, 1935, pp. 63-74. https://archive.org/details/history-of-hindu-mathematics-1-bibhutibhusan-datta-avadesh-narayan-singh/page/n17/mode/2up
2. S. R. Sarma, "The *katapayādi* system of numerical notation and its spread outside Keral," *Revue d'histoire* des *mathématiques* vol. 18, issue 1, 2012, pp. 37-66. https://doi.org/10.24033/rhm.167
3. D. Jadhav, "A mathematical study in historical perspective on early chronograms from Cambodia, Vietnam and Indonesia," *Vidyottama Sanatana*, vol. 7, issue 2, 2023, pp. 289-309. https://doi.org/10.25078/vidyottama.v7i2.2480
4. A. V. Raman, "The *katapayadi* formula and the modern hashing technique," in *Computing Science in Ancient India* (edited by T. R. N. Rao and Subhash Kak). Lafayette, LA: The Centre for Advanced Computer Studies, University of Southwestern Louisiana, 1998, p. 48. https://www.scribd.com/document/345288436/Computing-Science-in-Ancient-India-By-T-R-N-RAO-and-SUBHASH-KAK-pdf *IEEE Annals of the History of Computing*, vol. 19, issue 4, Oct.-Dec. 1997, pp. 49-52. https://doi.org/10.1109/85.627900
5. K. L. Priya and R. Parameswaran, "A study on the encoding systems in Vedic era and modern era," *International Journal of Pure and Applied Mathematics*, vol. 114, (special) issue 7, 2017, pp. 425-433. https://acadpubl.eu/jsi/2017-114-7-ICPCIT-2017/articles/7/39.pdf
6. C. Paar and J. Pelzl, *Understanding Cryptography*. Springer, 2010, p. 3. https://doi.org/10.1007/978-3-642-04101-3
7. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman And Hall/CRC Press, 2007, pp. 3-4. https://doi.org/10.1201/9781420010756
8. Jean-Philippe Aumasson, *Serious cryptography: A Practical Introduction to Modern Encryption*. San Francisco: No Starch Press, 2018, pp. 1-6. ISBN-13: 978-1-59327-826-7.
9. Paṇḍita Dineśabhāī Śahā (ed.), *Samyagjñānacandrikā (Jīvakāṇḍa and Arthasaṃdṛṣṭi)* of Toḍaramala, Part I (Translated into Hindi by Dr. Śrīmati Ujjvalā Śahā). Mumbai: Vītarāgavāṇīprakāśaka, 2018, under v. 158, p. 290. https://jainelibrary.org/book-detail/?srno=035932
10. L. C. Jain and R. K. Trivedi, "Ṭoḍaramala of Jaipur (A Jaina philosopher-mathematician)," *Indian Journal of History of Science*, vol. 22, issue 4, 1987, pp. 359-371. https://insa.nic.in/(S(n5lexmc3fnnxz3jwkiqawfrh))/writereaddata/UpLoadedFiles/IJHS/Vol22_4_9_RKTrivedi.pdf
11. D. Jadhav, "Why do I assign 981 A. D. to Nemicandra?," *Arhat Vacana*, vol. 18, issue 1, 2006, pp. 75-81.
12. D. Jadhav, "Nemicandrācāryakṛta granthoṃ meṃ akṣara-saṃkhyāoṃ kā prayoga," *Arhat Vacana*, vol. 10, issue 2, 1998, pp. 47-59.
13. C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, issue 4, October 1949, pp. 656-715. Doi: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x
14. D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*. Version 0.6 of a free online book, 1116 pages, January 2023, pp. 4-5. Available at: http://toc.cryptobook.us/.
15. J. L. Jaini (ed. & tr.), *Gommaṭasāra (Jīvakāṇḍa) of Nemicandra*. Lucknow: The Central Jaina Publishing House, 1927. https://jainelibrary.org/book-detail/?srno=001612
16. R. C. Jain Mukhtara and C. P. Patni (eds.), *Trilokasāra of Nemicandra* (with Mādhavacandra Traividya's Sanskrit Commentary and Āryikā Viśuddhamati's Hindi Commentary). Śrī Mahāvīrajī: Śrī Śivasāgara Granthamālā, 1975. https://jainelibrary.org/book-detail/?srno=090512

AUTHOR PROFILE

Prajna Jadhav, first completed her B. Sc. (Hons) degree in Mathematics at Institute for Excellence in Higher Education, Bhopal in 2017 and then completed a one-year certificate course in Chinese language from Sanchi University of Buddhist-Indic Studies in 2018. She further obtained her *Master of Cyber Law and Information Security* degree from National Law Institute University, Bhopal in 2020. In June 2014, she was awarded a cheque of ₹ twenty-five thousand by the Madhya Pradesh government for securing 89 percent marks in the Higher Secondary Examination. Her paper published before this one in *Indian Law Review* (vol. 9-12, 2017-2020, pp. 353-364) was "Vocaloid and IPR issues," co-authored with Revathi S.