ANCIENT INDIAN CRYPTOGRAPHY

Ganesh Gupta

Independent Researcher
Email: gupta.ganesh298@gmail.com

Cryptography is a feature of ancient literature. Ancient India placed a lot of importance on information reaching only those who could be trusted with the information or not share it at all. Messages were often conveyed in a hidden form visible in ancient texts. In this paper, we will see how the Math term (Pi) is hidden in one Malayalam shloka in *Karana-Paddhati* written by Puthamana Somayaji, using *Kaṭapayādi* system. Subash Kak, a scientist, historian and Indologist felt strongly that there is encrypted and decrypted truth in the oldest of all ancient literature works— the *Rig Veda*, which could support his ideas. His work exposed the knowledge of astronomy of the Vedic civilisation that was hidden in the *Samhita* part of the *Rig Veda*. This paper discusses about how we can connect modern cryptography technology to ancient literature text, monument and war techniques.

Keywords: Cryptography, *Katapayadi* system, Ancient cryptology, Security algorithm

Introduction

The art and science of cryptology has been used to decipher the bright history of ancient cultures, to change the flow of wars, and to stop potential hackers from attacking digital securities. Cryptography is a subject which is part of cryptology that has been studied and applied since ancient times and developing better encryption methods continues to this day. The word cryptology is derived from two Greek words: 'Kryptos', which means 'hidden or secret', and 'logos', which means, 'word or description'. Cryptology means secret speech or communication. Cryptology encompasses two competing skills – cover-up and expose, which are identified as:

- The cover–up portion of cryptology is called cryptography. The aim of cryptography is to give a message in indecipherable form to the unauthorised reader. It is also called encryption. Cryptography is often called "code making."
- The expose part of cryptology is called cryptanalysis. Cryptanalysis is often called "code breaking."

This paper is divided in two major parts: the first part is about the timeline of ancient cryptography in India and the second part discusses how cryptography is not all about hidden message transferring. In ancient literature text, Kaṭapayādi system was used as one of the encryption algorithms, which in the present day can help our country to develop its own unique language. The concept of cryptography is used for designing the structure of monuments. Ancient war techniques help us to make cyber security algorithm during the time of cyber wars.

Timeline of Ancient Cryptography

The timeline for ancient Indian cryptography is not described in proper way. The art of secret

writing and private communication in ancient India was well developed and used in financial, administrative, religious and personal record-keeping and communications. All the important mathematical formulae were sonically encrypted in devotional hymns and lyrics. In 'The Codebreakers' (Khann, 1967), the author has given a brief description of cryptography in ancient India. In the *Kamsutra*, Vatsayana has described mlecchita-viklapa as cryptographic language and its knowledge for women as one of the required arts, essential to maintain secrecy of the personal relation and communication. There was development of two types of writing namely *Kautilayama* in which letters were substituted based on phonetic relation and other is *Muladivaya* in which paired letters were used as cryptographic unit (Kak, 2006). Other versions of private messaging were developed such as methods based on knowledge of languages and messaging by wrist-finger gesture known as *aksharmustikakathanam* (Kalayanraman S.). One of the important ancient cryptographic technique in India was *Katayapadi* in which different consonants are mapped into digits from 0 to 9 and vowels are left free to use as per convenience in forming meaningful words (Kak, 2006). The other very complex type of coding to encrypt astronomical figures into words was used by Aryabhatta (Kak, 2006, 1998). Fascinatingly, in ancient India, even birds had been used to carry secret information and warnings. Similarly, other methods of secret communication were used in different civilisations, however, the idea of modern cryptography, based on mathematical concept, took birth from the work of C.E Shanon in 1948 (Shannon, 1948) and became practical with the advent of microcomputers in 1960. The sound mathematical foundation and invention of digital computers led together development of different encryption or decryption techniques.

Research Methods

Ancient literature text

The oldest evidence of the use of *Kaṭapayādi* (Sanskrit: कटपयादि) system is from *Grahacāraṇibandhana* by Haridatta in 683 CE. It has been used in *Laghu·bhāskarīya·vivaraṇa* written by *Śaṅkara·nārāyaṇa* in 869 CE. Under this method, a number is ascribed to each and every alphabet of the script, a concept highly similar to ASCII method in computers. Following verse found in *Śaṅkaravarman's Sadratnamāla* explains the mechanism of the method (Sarma, 1999).

नञावचश्चशून्यादनसंख्या: कटपयाय:। दिश्रेतूपान्त्यहल्संख्यानचदचन्त्योहलस्वर:॥

Transliteration:

nanyāvacaścaśūnyānisaṃkhyāḥkaṭapay ādayaḥ miśretūpāntyahalsaṃkhyāna ca cintyohalasvaraḥ

Translation: na (न), nya (ञ) and a (अ), i.e., vowels represent zero.

The nine integers are represented by consonant group beginning with *ka*, *ṭa*, *pa*, ya. In a conjunct consonant, the last of the consonants alone will count. A consonant without vowel is to be ignored.

Explanation: The assignment of letters to the numerals are as per the Table 1.

- Consonants have numerals assigned as per the above table. For example,

Table 1: Assignment of Letters

1	2	3	4	5	6	7	8	9	0
ka क ಕ ക	*kha* ख ಖ ഖ	*ga* ग ಗ ഗ	*gha* घ ಘ ഘ	*nga* ङ ಙ ങ	*ca* च ಚ ച	*cha* छ ಛ ഛ	*ja* ज ಜ ജ	*jha* झ ಝ ഝ	*nya* ञ ಞ ഞ
ṭa ट ಟ ട	*ṭha* ठ ಠ ഠ	*ḍa* ड ಡ ഡ	*ḍha* ढ ಢ ഢ	*ṇa* ण ಣ ണ	*ta* त ತ ത	*tha* थ ಥ ഥ	*da* द ದ ദ	*dha* ध ಧ ധ	*na* न ನ ന
pa प ಪ പ	*pha* फ ಫ ഫ	*ba* ब ಬ ബ	*bha* भ ಭ ഭ	*ma* म ಮ മ	-	-	-	-	-
ya य ಯ യ	*ra* र ರ ര	*la* ल ಲ ല	*va* व ವ വ	*śha* श ಶ ശ	*sha* ष ಷ ഷ	*sa* स ಸ സ	*ha* ह ಹ ഹ	-	-

ba (ब) is always 3 whereas 5 can be represented by either nga (ङ) or *ṇ*a (ण) or ma (ि) or *ś*ha (श).All separate vowels like a (अ) and *ṛ* (ऋ) are assigned to zero.

- In case of a conjunct, consonants attached to a non-vowel will not be valueless.
- For example, kya (क्या) is formed by k (क्) + ya (य) + a (अ). The only consonant standing with a vowel is ra (र). So the corresponding numeral for kya (क्या) will be 1.
- There is no way of representing decimal separator in the system.

A working example of the technique above:

गोपीभाग्यिधुव्रात-श्रुग्ङःङशिोदधसग्िग॥
खलजीदवतखातावगलहालारसंधर॥

ಗೋಪೋಭಾಗ್ಯ ಮಧುವ್ರಾ ತ-ಶ್ಿಂ
ಿಂಗಿಶೋದಧಿಸಂಧಿಗ್ ||
ಖಲಜೋವಿತಖಾತಾವಗ್ಲಹಾಲಾರಸಂಧರ ||

So, based on the above method, if the letters in the shloka are replaced by the corresponding numbers, i.e. 'go' by 3, 'pi' by 1, 'bha' by 4, 'ya' by 1 and so on, the following result is obtained: 31415926535897932384 626433832792. The number is the decimal representation of Pi up to 32 decimal places. Encrypting a mathematical concept in a devotional shloka dedicated to Krishna is pretty interesting.

They used this algorithm for two things:

1. They used methodologies like this to check the correct usage and pronunciation of the rhymes, where every variation from the correct mantra or shloka would result in an incorrect rendition of the Pi number (or any other system which they would have encoded).
2. They used concepts like the above to perform encryption and decryption so that the message would reach the intended receiver and no one would be able to catch the real meaning of the message.

In the year 1733 CE, a book *Karaṇa·paddhati*, was published by a mathematician Puthumana Somayaji, which consists of 10 chapters in total. In the 6th chapter, there is a shloka given in Malayalam,

anūnanūnnānananunnanityaissmāhatāścakrak alāvibhaktoḥcaṇḍāṃśucandrādhamakuṃbhipāl airvyāsastadarddhaṃtr ibhamaurvikasyāt.

The above shloka, when translated simply means "The circumference of a circle of diameter *anūnanūnnānananunnanityai* (10,000,000,000) is *caṇḍāṃśucandrādhamakuṃbhipālair* (31415926536), which, in turn, gives the value of Pi till 10 decimal places.

This is similar to the substitution cipher method used in English language. The difference between them is only the language. The example above is one method where we can find out from our literature that there are many methods which are hidden in our text. Inspired by the example above, we can create a security algorithm by using mantras and shlokas in such a way that it is not easily decodable because in coming years we will need a strong Cyber Security algorithms which we can use in our own language.

Ancient monuments

If we talk about monuments, India has one of the biggest heritage sites with elaborate superfluities and wonderful architecture. Indian monuments represent one of the most outstanding facets of the multi-faceted Indian culture. An architectural feat in itself, each Indian monument is a remarkably splendid sample of unbelievable artistry, covering a sense of mystery and sometimes deception. India has many monuments which are mystical in formation from inside and outside. Archaeo cryptography is the study of decoding monuments or structures by determining the underlying mathematical order beneath the proportions, size, and placement to find any re-occurring or unusual data with respect to that which is being studied, or within another monument or structure (Munck, 1997).

Archaeo cryptography is not a recognised branch of archaeology or of any other academic discipline. It is an example of pseudoscience or pseudo archaeology that employs contrived calculations involving many free parameters to achieve an impressive-looking result (Klaus, 2012).

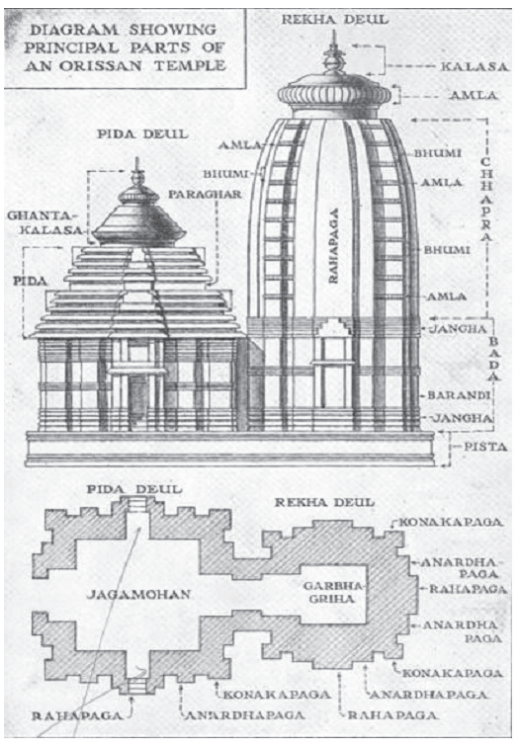

Fig. 1. Konark temple

Archaeo cryptologists try to find underlying correlations in respect to that which is being studied or decoded. Some factors taken into consideration while deciphering an object, structure or megalithic monument can include the features such as faces, stairs, sides, and terraces. The geolocation or mathematical operations are performed on latitude and longitude coordinates as well as astronomical alignments, such as those found in Archaeo astronomy. The incorporation of grids, the use of numerical ordering, mathematical constants, Biblical *gematria*, and any other re-occurring number that might stand out from the decoding process are determining factors.

A great example is the Konark temple as shown in Figure 1, built in 1250 AD by the Ganga King Narasimha Deva. It is one of the outstanding temples of India and referred to as the Black Pagoda. The shells of this temple were discovered in the late 19th century. The tower over the Garbagriha is missing, however the Jagmohana is complete. The whole temple is enclosed within a courtyard measuring 865 ft. by 540 ft. The most popular theory associated with Konark temple is its magnets and the floating idol in the air. The uniqueness of the Sun Temple of Konark lies in the fact that it was constructed with an architectural setup of various magnets. During the construction of the main tower of the temple, the artists put an iron plate between every two stone pieces. There is a lodestone at the top of the temple which is said to be a massive, about 52-ton magnet. According to legend, the statue of the Sun God inside the temple was built of a material with iron content and was said to be floating in air, without any physical support, due to the unique arrangements of the top magnet, the bottom magnet and the reinforced magnets around the temple walls. The placement of the main temple and the Sun God had been aligned in such a way that the first ray of the Sun from the coast would cross the Nata Mandir (Dancing Hall) and would fall and reflect from the diamond placed at the crown of the Sun God (Nath, 2017).

There are thousands of monuments which are still unrecognised, and many secrets are left to unearth. In India, there are many sculptures and monuments with many uncovered mysteries. Mysteries are not always related with treasure we say that it is also uncovered hidden technologies and techniques and calculation which they use to build these monuments at that era when we don't have so many reliable resources and gadgets.

War Techniques in Ancient India

The Mahabharata, a story of a great clan-war, is a source of information on ancient Indian warfare and Indian civilisation, including that of weapons and war techniques. Cropped of mythical embellishments, this information can always teach us a lesson or two even in today's world. The most important thing is that the great emphasis was laid on the theoretical, particularly the psychological side of warfare, but the most fascinating aspect of the ancient Indian warfare techniques was the *vhyuha*-intricate, labyrinthine, (snare-like formations of troops which the enemy could not enter, and if they could, would not know how to extract out of). There were many such formations each with a distinct pattern and a name meaning that was characteristic.

It was considered a test of the general's skill to select and execute the most appropriate *vhyuha*. Needless to say, it required rigorous education in military science at the academics of the gurus. Brihashpati, Shukra, Parashuram and Drona were some of the most famous war gurus. The names of many such *vhyuhas* in the Mahabharata:- *shakata-vhyuha* (cat-shaped formation), *garbha-vhyuha* (womb-shaped formation), *suchi-vhyuha* (needle shaped formation), *Garura-vhyuha* (half- bird, half-man shaped), *ardha-chandravhyuha* (crescent–shaped), *makra- vhyuha* (mythical crocodile–shaped), *krouncha-vhyuha* (crane-shaped), *Mandala-vhyuha* (circular), *Vajra-vhyuha* (thunderbolt-shaped), *Kurma-vhyuha* (tortoise-shaped), *Shringatak-vhyuha* (triangular), Sarabatobhadra- *vhyuha* (a grand *vhyuha* where all the great generals were positioned strategically), *Sarba-shatrujayee* (all-conquering), *chakra-shakat* (cart-wheel), etc.

Fig. 2. *Padma-vhyuha*

In the *Manu Samhita*, some vhyuhas have been particularly inscribed. In her excellent translation and annotation of the work, from which we have copiously quoted, Wendy Doniger throws light on the actual nature of some of these formation. For example, she explains that the *makra-vhyuha* is "an hour glass shaped, narrow in the middle and broad in the front and back." The thunderbolt-shaped *Vajra-vhyuha*, so favored by Arjuna, is "created by making a three-fold divisions of the troops". The lotus-shaped *Padma-vhyuha* is a "circle that spreads out on all sides, with the king in the middle". (Das Gupta, 2007) as shown in Fig. 2.

There are some AI algorithms which help us to understand the war techniques. We can analyse and recreate this technique as encryption technique to protect from cyber-crime. We need to understand importance of this technique and try to reconnect it in our defense system. We have to prepare for cyber war in coming years, looking at the digital world. This technique helps us to create first line defense system which protects us from cyber-crime and economic crashes and our secret remains a secret.

Results and Discussions

India is one of the most versatile countries in arts and literature. As we know India is full of mysteries which we have to decode or decrypt in some way. There are many techniques and mathematical calculations which we can use to solve the many mysteries of India scientifically. There are many ancient techniques which can be recreated by using modern technology. If we talk about literature, there are many ancient literatures which can help us to solve the unsolved problems of

different fields. *Kaṭapayādi* system is just one example of ancient language which helps us to find Pi in shlokas. India could have built its own AI language system by using this ancient literature. There are many monuments which help us to create a different structural based encryption algorithm and technologies in the coming future. Encryption means privacy and security of message which thoroughly depends on languages. Cyber security needs complex algorithm which is not easily decodable. Indian literature languages and structural based algorithm helps us to create ancient war techniques, such as *vhyuha*, which protect our country on different layers in networking and security system. We don't need an encryption algorithm which is easily breakable and known to anyone but at this moment we have so much potential in this field but exploration is still pending.

Conclusion

India has its own encryption and decryption algorithm but due to insufficiency of organisations and funding, we could not create our own cyber security algorithm (which has totally different languages and method). For winning any war, we have to analyse our own roots and find out the reason of different questions like what technology our emperors had used to make historical monuments. Some questions like, 'Why structural based and calculative based techniques were so sufficient at that time?', can help us to answer a lot of the present day questions. During the *Mahabharata* era, *chakravyuhsanrachna* was extremely important and one of the strongest techniques to defeat an enemy. We can use this technique to make our digital India safe from breaching and from cyber-crime.

References

Anurag N. 2017. Bliss. Leo Publishers, India.

Carl.P. M. 1997. "The Code - 1997", Radio Bookstore Press.

Jyoti, B.D.G. 2007. Science, Technology, Imperialism, and War. Pearson Education India, New Delhi.

Shubhash, K. 1988. The Aryabhata Cipher. *Cryptologia*. Vol. 12. pp. 113–117.

———. 2006. "Aryabhatta's Mathematics", RSA Conference San Jose, California.

Shannon, C. E. 1948. A Mathematical theory of communication. *The Bell System. Technical Journal*. Vol. 27. pp. 379 – 423E.

———. 1948. A Mathematical Theory of Communication (part II). *The Bell System. Technical Journal*. pp. 623–56.

Schmeh, K. 2012. The Pathology of Cryptology—A Current Survey. *Cryptologia*. Vol. 36. pp. 14–45.

Sarma. S. R. 1999. Kaṭapayādi Notation on a Sanskrit Astrolabe. *Indian Journal of History and Science*. Vol. 34, No. 4. pp. 273–287.