International Journal of Pure and Applied Mathematics
Volume 114 No. 7 2017, 425-433
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A Study on the Encoding Systems in Vedic Era and Modern Era

[1]K. Lakshmi Priya and [2]R. Parameswaran

[1]Department of Mathematics,

School of Arts and Sciences,

Amrita University, Kochi.

lakshmiraman.priya@gmail.com

[2]Department of Mathematics,

School of Arts and Sciences,

Amrita University, Kochi.

ramanparameswaran@gmail.com

Abstract

Encoding is the action of transferring a message in to codes. In this paper I present a study on the encoding systems in vedic era and modern era. The Sanskrit verses written in the vedic era are not just the praises of the Gods they are also numerical codes. In ancient India there were three means of recording numerals in Sanskrit words which are Katapayadi system, Bhutasamkhya system and Aryabhata numeration. These systems were used by many ancient mathematicians in India. In this paper the Katapayadi system used in vedic times is applied to modern ciphers– Vigenere Cipher and Affine Cipher.

Key Words: Katapayadi system, vigenere cipher, affine cipher.

1. Introduction

Encoding is the process of transforming messages into an arrangement required for data transmission, storage and compression/decompression. In cryptography, encryption is the method of transforming information using an algorithm to make it illegible to anyone except those owning special information, usually called as a key.

In vedic era, Sanskrit is the language used. It is supposed to be the ancient language, from which most of the modern dialects are developed. All the sacred manuscripts of Hinduism such as Vedas, Upanishads, Puranas, etc. are engraved in Sanskrit. These scriptures contain high level mathematics in the encoded form, not as an equation or theorem but as verses. One of the four Vedas, Rig Veda discusses geometry while Yajur, another Veda, states about the concept of infinity and arithmetic series. Yajur Veda also mention about counting numbers up to 10^{18}. Another Veda, Atharva states the fact that $1 \times 1 = 1$. In Atharva Veda zero or shunya is defined as the transition point between opposites [6].

The method of encrypting the message to be sent began thousands of year ago. In ancient period encrypted messages were sent mainly during war. In the modern era, the spontaneous growth in the field of communication encryption of messages becomes the necessary for ensuring that the information sent become secured and made hard for deciphering.

2. Encoding Systems

Here we are discussing about three encoding systems.

1. Katapayadi system
2. Vignere Cipher
3. Affine Cipher

Then Katapayadi system is applied to the other two ciphers – Vigenere and Affine ciphers.

Katapayadi System

The origin of this system is still a topic for argument. Some consider that this system was found by *Vararuci*, an astronomer from Kerala. He is traditionally assigned to the 4^{th} century. His book *Chandravakyani* is said to comprise the hymns which, when interpreted gives the longitudes of Moon at different time interval. *Grahacāraṇibandhana* by *Haridatta* in 683 CE and *Laghu bhāskarīya vivaraṇa* by *Shankara Narayana* in *869 CE* etc. are also the evidences of Katapayadi system. The system is named Katapayadi since the number 1 is allocated to the letters Ka *Ta Pa* and *Ya.* In this method numerals from 0 to 9 are used. Thus more than one letter is allocated to a single numeral [6]. The rule for this process is given by a Sanskrit stanza [2],

नञावचश्च शून्यानि संख्याः कटपयादयः ।
मिश्रे तूपान्त्यहल् संख्या न च चिन्त्यो हलस्वरः ॥

Transliteration:

nanyāvacaśca śūnyāni saṃkhyāḥ kaṭapayādayaḥ

miśre tūpāntyahal saṃkhyā na ca cintyo

halasvaraḥ

The rule is

ka (क), *ṭa* (ट), *pa* (प) and *ya* (य) denote *1*

kha (ख), *ṭha* (ठ), *pha* (फ), and *ra* (र) indicate *2*

ga (ग), *ḍa* (ड), *ba* (ब) and *la* (ल) stand for *3*

gha (घ), *ḍha* (ढ), *bha* (भ) and *va* (व) symbolize *4*

gna (ङ), *ṇa* (ण), *ma* (म), and *śha* (श) represent *5*

ca (च), *ta* (त), and *sha* (ष) stand for *6*

cha (छ), *tha* (थ), and *sa* (स) means *7*

ja (ज), *da* (द), and *ha* (ह) stand for *8*

jha (झ) and *dha* (ध) characterize *9*

nya (ञ), *na* (न) and all vowels means *0*

In conjunct consonants, only the last consonant is to be taken into account. A vowel not preceded by consonant is represented by 0 and vowels following consonants have no value. In this method the numbers are read from right to left. There is no way of decimal separator in the system [1].

Madhava's sine table constructed by Madhava of Sangamagrama (14th century) uses Katapayadi system to give the values of sine for different angles. *Narayaneeyam* written by Melpathur Narayana Bhattathiri also uses this systems. *Narayaneeyam* ends with the verse

आयुरारोग्यसौख्यम्

When this is translated using Katapayadi system 0122171, which should be read from right to left, i.e. 1712210.

This represent the date as per Malayalam calendar on which the *Narayaneeyam* was completed[6].

Vigenere Cipher

Vigenere cipher is a simple symmetric key cryptosystem. This cipher need a plain text to be encrypted, a key word [3].

Algorithm of Vigenere cipher [4]

If the letters A-Z are taken to be the numbers 0-25 and addition is performed modulo 26 then Vigenere encryption E using the key K can be written

$C_i = E_K(M_i) = (M_i+K_i) \bmod 26$ And decryption D using key K,

$M_i=D_K(C_i) = (C_i-K_i) \bmod 26$ where $M = M_1,M_2,\ldots\ldots,M_n$ is the message

$C = C1,C2,\ldots\ldots..,Cn$ is the cipher text,

$K = K1,K2,\ldots\ldots Kn$ is the key obtained by repeating the keyword [n/m] times where m is the keyword length.

Affine Cipher

The affine cipher works over a mixture of modular multiplication and modular addition. In this cipher also the letters A-Z are taken. The encryption E can be written as [5]

$$e_k(x) = (ax+b) \bmod 26$$

and

$$d_k(y) = a^{-1}(y-b) \bmod 26$$

where x, y, a, b $\in Z_{26}$

with the key k = (a, b) and gcd (a, 26) = 1

For decryption a has to be inverted, this is the reason for the restriction gcd (a,26) =1, also $a.a^{-1} = 1 mod 26$

Thus 'a' must be in the set:

$$a \in \{1, 3, 5, 7, 11, 15, 17, 19, 21, 23, 25\}$$

3. Practical Relevance in Modern Era

The Katapayadi system of encoding can be applied to both Vigenere cipher and Affine cipher by making necessary changes in the rules of encryption and decryption.

Vigenere Cipher

If the Katapayadi system is used in Vigenere cipher, then numbers are chosen from $\mathbb{Z}$ 10, so addition is performed modulo 10. Thus the Vigenere encryption E using the key K can be written as

$$C_i = E_k(M_i) = (M_i+K_i) \bmod 10$$

And decryption using the key K

$M_i = D_k(C_i) = (C_i - K_i) \bmod 10$ For Example:

Encryption

M = सत्यमेव जयते नानृतं

K = भारतम्

When these are translated using Katapayadi system we get,

M = 6006184517

K = 624

Then,

C1 = (6+6) mod 10 = 2

C2 = (0+2) mod 10 = 2

C3 = (0+4) mod 10 = 4

C4 = (6+6) mod 10 = 2

C5 = (1+2) mod 10 = 3

C6 = (8+4) mod 10 = 2

C7 = (4+6) mod 10 = 0

C8 = (5+2) mod 10 = 7

C9 = (1+4) mod 10 = 5

C10 = (7+6) mod 10 = 3

Thus,

C = 3570232422

Then again by using Katapayadi system we get the cipher text as,

C = लश सनर गरा वठर

Decryption

C = 2242320753

K = 624

Then,

M1 = (2-6) mod 10 = 6

M2 = (2-2) mod 10 = 0

M3 = (4-4) mod 10 = 0

M4 = (2-6) mod 10 = 6

M5 = (3-2) mod 10 = 1

M6 = (2-4) mod 10 = 8

M7 = (0-6) mod 10 = 4

M8 = (7-2) mod 10 = 5

M9 = (5-4) mod 10 = 1

M10 = (3-6) mod 10 =7

Thus,

M = 7154816006

By Katapayadi system

M = सत्यमेव जयते नानृतं

Affine Cipher

Similarly, if the Katapayadi system is used in affine cipher, then numbers are chosen from $\mathbb{Z}$ 10, so addition is performed modulo 10.Thus the encryption e becomes

$$e_k(x) = (ax+b) \bmod 10$$

And decryption rule changes to

$$d_k(y) = a^{-1}(y-b) \bmod 10$$

where x, y, a, b ∈ z_{10}

with the key k = (a, b) and gcd (a, 10) = 1 Thus 'a' must be in the set:

$$a \in \{1, 3, 7, 9\}$$

For example:

Let the key k = (3, 5)

$$a = 3 b = 5$$

$$a.\, a^{-1} = 1 mod 10$$

$$a^{-1} = 7$$

Encryption

M = वायुः सर्वत्र अस्ति

When this message is translated using Katapayadi system we get,

M = 6064714

e_k (6) = (3×6+5) mod 10 = 3

e_k (0) = (3×0+5) mod 10 = 5

e_k (6) = (3×6+5) mod 10 = 3

e_k (4) = (3×4+5) mod 10 = 7

e_k (7) = (3×7+5) mod 10 = 6

e_k (1) = (3×1+5) mod 10 = 8

e_k (4) = (3×4+5) mod 10 = 7

So,

C = 7867353

Again by using Katapayadi system we get the cipher text as,

C = छद तासाम् लामाब

Decryption C = 3537687

d_k (3) = 7(3−5) mod 10 = 6

d_k (5) = 7(5−5) mod 10 = 0

d_k (3) = 7(3−5) mod 10 = 6

d_k (7) = 7(7−5) mod 10 = 4

d_k (6) = 7(6−5) mod 10 = 7

d_k (8) = 7(8−5) mod 10 = 1

d_k (7) = 7(7−5) mod 10 = 4

Thus,

D = 4174606

By Katapayadi system

D = वायुः सर्वत्र अस्ति

4. Conclusion

We have presented a method of recording numerals in Sanskrit language that existed in our culture, and two methods of encryption used in the modern era. Application of the Katapayadi system to the Vigenere cipher and Affine cipher is made. The observation is that this system gives more than one interpretation when we get the cipher text, C as a string of number each number may represent more than one letter which make the decryption a troublesome job. If we can overcome this ambiguity, this system can be implemented to a very effective cipher system.

References

[1] Jagadguru Swami Sri Bharati Krisna Tirthaji Maharaja, Vedic Mathematics, Delhi: Motilal Banarsidas, Varanasi (1986), 194-

195.

[2] Sweeney J.F., Rig Veda Magic Squares.

[3] Luenberger D.G., Information sciences,Princeton University Press (2000), 171-174.

[4] Kester Q.A., A cryptographic algorithm based on words database, International Journal of Science, Engineering and Technology Research 2(4) (2013).

[5] Paar C., Pelzl J., Understanding cryptography: a textbook for students and practitioners, Springer Science & Business Media (2009).

[6] Lakshmi Priya K., Parameswaran R., Encoding systems in vedic mathematics, National Seminar on Kerala School of Astronomy and Mathematics: Contributions and Contemporary Relevance (2016).