# *A novelty approach of symmetric encryption algorithm*

Kishore Dasari
C.S.E
Departement,KL University
Guntur, India

Dr.V.Srikanth
Professor and Head of C.S.E.
Department, KL University Guntur, India

B. Veramallu
Associate professor
C.S.E dept, KL University
Guntur, India

S. Satish Kumar
C.S.E
Departement
KL University
Guntur, India

K Srinivasulu Achari
C.S.E
Departement
KL University
Guntur, India

*Abstract*— **Cryptography plays major role in information security and many encryption, decryption algorithms have been developed and in use for information retrieval and storage but still there is a need to research for better algorithms than existing. Recently Multilanguage encryption and decryption approaches throw a light in this area of research. In this paper we propose a novel encryption and decryption technique in which cipher text is brought into Unicode characters of Hindi, an Indian official language. A software cryptographic tool also can be facilitated for the purpose of information security in the organizations.**

***Keywords— Cryptography; Multilanguage; Hindi; Information security;***

## I. INTRODUCTION

Cryptography is used to conceal the information. It is not only used by the sleuth but for phone, fax and e-mail communications, bank transactions, and bank account security PIN'S, passwords and credit card transactions on the web. It is also used for different verities of other information.

In cryptography a misguided version of plaintext is called cipher text. A cryptosystem mainly consists of enciphering algorithm [2] and deciphering algorithm. The word "cipher" is synchronous with cryptosystem. Prior to the invention of public key cryptography it was essentially impossible to provide key management for large scale networks. To ensure security against cryptanalyst attacks, block ciphers in general must have diffusion and non-linearity.

In cryptography the term 'code' [3] is defined as the algorithm for transforming an intelligible message into an unintelligible form using a code-book. The two fundamental different ways the ciphers may be secure are-1.unconditional security: "No matter how much computer power is available; the cipher cannot be broken.2.computational security:" given limited computing resources, the cipher cannot be broken.

In cryptography we have one more term named as "Entropy"- which is defined as 'entropy of a message F(x) is related to the number of bits of information needed to encode a message 'x'. The cryptanalysis' use letter frequency counts to guess a couple of possible letter mappings. The security policy is a set of rules specifying how security should be enforced within a domain. In information security we have one more term named as 'traffic padding'-which is the addition of pretend data to conceal real data volumes. The traffic padding provides traffic flow of confidentiality. Notarization can provide non-repudiation service where notary will typically apply a cryptographic transformation to the data.

To measure the frequency of letters in cipher text we also use –"Index of Coincidence (IC)", which was introduced by William Friedman.

## II. EXISTING SYSTEM

In existing algorithm we have many drawbacks.

***Caesar cipher***: This is a simple structure and is easy to break using 4*10 26 possible keys. It is one type of substitution cipher where each letter in the plain text is replaced by some other letter or some fixed number of the positions down in decreasing way of the alphabet. The steps of encryption that are performed by a Caesar cipher are often incorporated as a part of more complex schemes, such as in the Viegenere cipher. As with all the single alphabet substitution ciphers, the Caesar cipher is easily broken and in the modern technology offers essentially no communication security.

In ***monoalphabetic ciphers*** the frequency distribution of this cipher reflects the distribution of the underlying alphabet. In this the guessing of the work will continue to work to substantiate until you have all the words in place, or until you reach the contradiction. The monoalphabetic cipher uses fixed substitution over the entire message.

The ***play-fair cipher*** is effective for very short messages. But while the complexity of the text is increasing the play-fair cipher not suits well. The "Hill cipher" algorithm is broken with a known Plain text attack. A play-fair cipher is a manual symmetric encryption technique and was the first used literal digraph substitution cipher. The encryption technique pairs the letters instead of single letters as in a simple substitution cipher. The play-fair cipher is significantly hard to break since the frequency analysis used for the simple substitution ciphers does not work. To generate the key table, one should first fill in the spaces in the table with the letters of the keyword, then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for the filling in the 5 × 5 table constitutes the cipher key.

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

The ***Hill Cipher*** is a poly-graphic substitution cipher that is based on the subject of the linear algebra. In this the each letter is represented by a Modulo 26. For encrypting a message, each block of n letters is multiplied by an invertible n*n matrix and again by using Modulo 26. For decrypting a message each block is multiplied by the reverse of the matrix that is used for encryption. The matrix that is used for encryption is the cipher key, and it should be chosen randomly from the set of invertible $n \times n$ matrices (modulo 26). The cipher can, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of using the modulo26. The basic hill cipher is vulnerable to the "known plain-text attack" because it is completely linear.

The above are some of the existing system techniques which are having its own advantages and disadvantages. Now in this modern technology the above techniques are never used anywhere.

## III. PROPOSED SYSTEM

Up to now we come across different cryptographic algorithm techniques in which the cipher text is tuned into the same language text.

In this we propose a new algorithm where the plaintext is taken in English language where the output of the cipher text is in different language (i.e.) in other language. The frequency distribution of letters in our technique is very less when compared to changing the cipher text from same language to same language.

### *A. Procedure*

In our algorithm we have to first generate the keys, these keys are used in the encryption process. It is very difficult to decrypt the text by the adversary. The key can be defined as – some critical information used by the cipher, known only to the sender and receiver.

### *B. Key generation*

Let K1 is coded form of file name and K2 is coded form of combination of employ ID and password then compute k1 and k2 resultant value will be store in k3.

i.e. K3 =k1*k2

Key1=last four event digits from k3

Key2 =number of digits from k3

### *C. Algorithm*

Step1: Message/data is coding from plaintext numeric form using table1

Step2: cipher1=key1*msg

Sep3: cipher2=cipher1*key2

Step4: reverse entire number

Step5: count the number of digits. if count is odd then pad with zero(0).the numeric data is dividing into two digit block.

step6: swap the position in the each and every block

Step7: convert two digit blocks to final cipher text using table2 (in the table2 having 100(00-99) sets of syllables each set having 3 syllables, so we can pick any one syllable.

### *D. Example*

Filename is Tb1, employ ID and password= CSM12AP and message =Hello.

K1 = coded form of file name using table1

K1=203828

K2=coded form of employ ID and password using table1

= 03191328290116

K3= k1*K2

K3 =650482062717764048

Key1=last four even digit from k3

Key1=4048

Key2 = number of digits in k3

*a) =18.*

### *E. Encryption*

Step1: H->08.e->41,l->48,l->48,o->51

Msg = 0841484851

Step2: C1=key1*M.

C1= 4048*0841484851

=3406330676848

Step3: C2 = C1 * key2;

=3406330676848*18

=61313952183264.

Step4: reverse the entire number

46238125931316.

Step5: the number digits are even, so don't need padding divide the above number is two digits blocks

46 23 81 25 93 13 16

Step6: swap the positions in each and every block

64 32 18 52 39 31 61

Step7: Every number represent a set of syllables .pick any one syllables

Final Cipher text

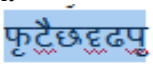

TABLE I. ASSUME EACH KEY OF THE KEYBOARD HAS A UNIQUE NUMBER FOR MAPPING

| | | | | |
|---|---|---|---|---|
| A -> 01 | U -> 21 | e -> 41 | y -> 61 | $ -> 81 |
| B -> 02 | V -> 22 | f -> 42 | z -> 62 | -> 82 |
| C -> 03 | W -> 23 | g -> 43 | + -> 63 | _ -> 83 |
| D -> 04 | X -> 24 | h -> 44 | - -> 64 | # -> 84 |
| E -> 05 | Y -> 25 | i -> 45 | * -> 65 | & -> 85 |
| F -> 06 | Z -> 26 | j -> 46 | ? -> 66 | ~ -> 86 |
| G -> 07 | 0 -> 27 | k -> 47 | ! -> 67 | @ -> 87 |
| H -> 08 | 1 -> 28 | l -> 48 | . -> 68 | -> 88 |
| I -> 09 | 2 -> 29 | m -> 49 | [ -> 69 | ` -> 89 |

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

| | | | | |
|---|---|---|---|---|
| J -> 10 | 3 -> 30 | n -> 50 | ] -> 70 | ; -> 90 |
| K -> 11 | 4 -> 31 | o -> 51 | ( -> 71 | : -> 91 |
| L -> 12 | 5 -> 32 | p -> 52 | ) -> 72 | space ->92 |
| M -> 13 | 6 -> 33 | q -> 53 | { -> 73 | / -> 93 |
| N -> 14 | 7 -> 34 | r -> 54 | } -> 74 | \ -> 94 |
| O -> 15 | 8 -> 35 | s -> 55 | , -> 75 | " -> 95 |
| P -> 16 | 9 -> 36 | t -> 56 | ^ -> 76 | ' -> 96 |
| Q -> 17 | a -> 37 | u -> 57 | < -> 77 | \| -> 97 |
| R -> 18 | b -> 38 | v -> 58 | > -> 78 | |
| S -> 19 | c -> 39 | w -> 59 | % -> 79 | |
| T -> 20 | d -> 40 | x -> 60 | = -> 80 | |

TABLE II. MAPPING WITH TABLE

| | | | | | |
|---|---|---|---|---|---|
| 00 | क,कि,कु | 34 | ठृ,ठू,ठे | 68 | बै,बो,बौ |
| 01 | कृ,कॄ,के | 35 | ठै,ठो,ठौ | 69 | भ,भि,भु |
| 02 | कै,को,कौ | 36 | ड,डि,डु | 70 | भू,भॄ,भे |
| 03 | ख,खि,खु | 37 | डृ,डॄ,ड | 71 | भै,भो,भौ |
| 04 | खृ,खॄ,खे | 38 | डै,डो,डौ | 72 | म,मि,मु |
| 05 | खै,खो,खौ | 39 | ढ,ढि,ढु | 73 | मू,मॄ,मे |
| 06 | ग,गि,गु | 40 | ढृ,ढॄ,ढे | 74 | मै,मो,मौ |
| 07 | गृ,ग्ल,गे | 41 | ढै,ढो,ढौ | 75 | य,यि,यु |
| 08 | गै,गो,गौ | 42 | ण,णि,णु | 76 | यू,यॄ,थे |
| 09 | घ,घि,घु | 43 | णृ,णॄ,णे | 77 | थै,थो,थौ |
| 10 | घृ,घॄ,घे | 44 | णै,णो,णौ | 78 | र,रि,रु |
| 11 | घै,घो,घौ | 45 | त,ति,तु | 79 | रू,रॄ,रे |
| 12 | ङ,ङि,ङु | 46 | तृ,तॄ,ते | 80 | रै,रो,रौ |
| 13 | ङ,ङि,ङु | 47 | तै,तो,तौ | 81 | ल,लि,लु |
| 14 | ङृ,ङॄ,ङे | 48 | थ थि थु | 82 | लृ,लॄ,ले |
| 15 | च,चि,चु | 49 | थृ,थॄ,थे | 83 | लै,लो,लौ |
| 16 | चृ,चॄ,चे | 50 | थै,थो,थौ | 84 | व,वि,वु |
| 17 | चै,चो,चौ | 51 | द,दि,दु | 85 | वृ,वॄ,वे |
| 18 | छ छि छु | 52 | दृ,दॄ,दे | 86 | वै,वो,वौ |
| 19 | छृ,छॄ,छे | 53 | दै,दो,दौ | 87 | श,शि,शु |
| 20 | छै,छो,छौ | 54 | ध,धि,धु | 88 | शृ,शॄ,शे |
| 21 | ज,जि,जु | 55 | धृ,धॄ,धे | 89 | शै,शो,शौ |
| 22 | जृ,जॄ,जे | 56 | धै,धो,धौ | 90 | ष,षि,षु |
| 23 | जै,जो,जौ | 57 | न,नि,नु | 91 | षृ,षॄ,षे |
| 24 | झ,झि,झु | 58 | नृ,नॄ,ने | 92 | षै,षो,षौ |
| 25 | झृ,झॄ,झे | 59 | नै,नो,नौ | 93 | स,सि,सु |
| 26 | झै,झो,झौ | 60 | प,पि,पु | 94 | सृ,सॄ,से |
| 27 | ञ,ञि,ञु | 61 | पृ, पॄ,पे | 95 | सै,सो,सौ |
| 28 | ञृ,ञॄ,ञे | 62 | पै,पो,पौ | 96 | ह,हि,हु |
| 29 | ञै,ञो,ञौ | 63 | फ,फि,फु | 97 | हृ,हॄ,हे |
| 30 | ट,टि,टु | 64 | फृ,फॄ,फे | 98 | है,हो,हौ |
| 31 | टृ,टॄ,टे | 65 | फै,फो,फौ | 99 | अ,इ,उ |
| 32 | टै,टो,टौ | 66 | ब,बि,बु | | |
| 33 | ठ,ठि,ठु | 67 | बृ,बॄ,बे | | |

## IV. CONCLUSION

The novelty approach symmetric algorithm discussed above uses a mapping technique which apart from being simple in implementation and it has an increased the security levels. The aptitude of the proposed algorithm is to work over different type of Language domains will assist the localization of Cryptographic Software tools. We have also seen that the algorithm is protected to intruders. The toughness of this encryption method is attributed to the multiple facet of the algorithm. Further studies will concentrate on encrypted text attribute based encryption during the broadcasting of the information.

## REFERENCES


[1] English to Sanskrit dictionary, *www.lexilogos.com/**english/sanskrit_dictionary**.htm*

[2] M. Bellare, A. Desai, E. Jokipii, P. Rogaway, "*A concrete security treatment of symmetric encryption"*, In Proceedings ofthe 38th Symposium on Foundations of Computer Science, IEEE, 1997.

[3] Francois-Xavier Standaert, Gilles Piret, Jean-Jacques Quisquater, "Cryptanalysis of Block Ciphers: A Survey", *UCL Crypto Group,* 2003..

[4] William C. Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", *National Institute of Standards and Technology,* NIST Special Publication 800-67, 2008..

[5] Kurt Elfering: *Die Mathematik des Aryabhata I. Text, Übersetzung aus dem Sanskrit und Kommentar*. Wilhelm Fink Verlag, München, 1975, ISBN 3-7705-1326-6

[6] Georges Ifrah: *The Universal History of Numbers. From Prehistory to the Invention of the Computer*. John Wiley &Sons, New York, 2000, ISBN 0-471-39340-1.

[7] *http://www.unicode.org*

[8] Collins, R.W., "Software localization for Internet software, issues and methods", *Software, IEEE,* Florida, USA, 2002, pp. 74-80.

[9] Ross J. Anderson, "Why Cryptosystems Fail", *Communications of the ACM,* New York, USA, 1994, pp. 32-40.


Mr. Kishore Dasari received Master of Computer Applications degree from Acharya Nagarjuna University, Guntur, Andhra Pradesh, India and pursing M.tech degree in computer networks and security in KL University, Guntur. He is doing dissertation work under the esteemed guidance of Dr.V.Srikanth professor and Head, department of computer science, KL University, India.

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

Dr.V.Srikanth obtained his B.E., M.E. and PhD from the University of Madras and Acharya Nagarjuna University respectively. He is a prolific researcher with experience of 13 years and worked under various capacities in KL University. Presently he is working as Head of the Computer Science and Engineering department in KL University. He has more than 25 publications in the area of MAC issues and Routing aspects in Wireless Sensor, Ad-hoc and under Water Acoustic Networks.

Mr. Bobba Veeramallu obtained his B.E., M.Tech. from the University of Madras and Jawaharlal Nehru Technological University respectively. He is a prolific researcher with experience of 14 years and worked under various capacities in KL University. Presently he is doing his Phd in KL University, India.

Mr.S.Satish Kumar received B.Tech degree from Jawaharlal Nehru Technological University Hyderabad, Andhra Pradesh, India and pursuing M.Tech degree in computer networks and security in KL University Guntur. He is doing dissertation work under the guidance of Dr.P.V.R.D. Prasad, Assoc professor computer science department, KL University, India.

Mr.K.Srinivas Achari received B.Tech degree from Jawaharlal Nehru Technological University, Anathapur, Andhra Pradesh, India and pursuing M.Tech degree in computer networks and security in KL University Guntur. He is doing dissertation work under the guidance of Dr.Khalim Amjad Meerja, professor, computer science department, KL University, India

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE