Design an Algorithm for Data Encryption and Decryption Using Pentaoctagesimal SNS

Debasis Das[1], U. A. Lanjewar[2], S. J. Sharma[3]

[1] *Assistant Professor, VMV Com., JMT Arts & JJP Science College, Nagpur, India*

[2]*Professor, VMV Com., JMT Arts & JJP Science College, Nagpur, India*

[3]*Reader and Head, Department of Electronics and Computer Sc., RTM Nagpur University, Nagpur*

ABSTRACT : *Encryption is the most effective way of computer science concerned with developing schemes and formula to achieve data and information security through the use of codes. Today the privacy is the main issue to sending information from one point to another in data transmission. Encryption is the procedure that allows messages or information to be encoded in such a way that it is extremely difficult to read or understand where decryption is the procedure to transforming encoded text into the original message and information. In this paper we present an algorithm for data encryption and decryption which is based on number theory. In addition, data encryption using strange number system (especially using pentaoctagesimal (SNS) can provide real physical security to data—allowing only authorized users to delete or update data. This algorithm is used pentaoctagesimal strange number system to encrypt data and we propose a better data encryption and decryption strategy, which will offer better security towards all possible ways of attacks while data transmission.*

Keywords - *Encryption; Decryption; Strange Number System (SNS); Data Transmission; Pentaoctagesimal SNS*

I. INTRODUCTION

Cryptography is the study of Secret (crypto-)-Writing (-graphy). It is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form. As the field of cryptography has advanced; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances.

Since times immemorial, security of data to maintain its confidentiality, proper access control, integrity and availability has been a major issue in data communication. Codes, hence, form an important part of our history; starting from the paintings of Da Vinci and Michelangelo to the ancient Roman steganographic practices the necessity of data hiding was obvious. Today in the e-age, the need to protect communications from prying eyes is greater than ever before. Cryptography, the science of encryption plays a central role in mobile phone communication, e-commerce, Pay-TV, sending private e-mails, transmitting financial information and touches on many aspects of daily lives.

In some cryptologic systems, encryption is accomplished, for example, by choosing certain prime numbers and then products of those prime numbers as a basis for further mathematical operations. In addition to developing such mathematical keys, the data itself is divided into blocks of specific and limited length so that the information that can be obtained even from the form of the message is limited. Decryption is usually accomplished by following an elaborate reconstruction process that itself involves unique mathematical operations. In other cases, decryption is accomplished by performing the inverse mathematical operations performed during encryption [1, 2, 3].

Cryptographic systems are generally classified in three different categories [4, 5]:

1. Type of operations used for transforming plain text to cipher text.
2. The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret

key conventional encryption. If the sender and the receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption.

3. The way in which the plaintext is processed: A block cipher processes the input on block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Many different encryption / decryption processes or algorithms exist. In general, the functions of security system are security, authenticity, integrity and non-repudiation. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives when we sign our name to some document and for instance and, as we move to world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication. Cryptography provides mechanisms for such procedures. However, today's cryptography is more than encryption and decryption. It is difficult to keep the algorithm secret because if an algorithm is to be widely used, it is highly likely that determined attackers will manage to learn the algorithm by reverse engineering whatever implementation is distributed, or just because the more people who know something the more likely it is for the information to leak to the wrong places. At present, there are many available data encryption algorithms such as Substitution techniques, RSA encryption and Arithmetic coding etc.

Secure data transmission is done with a technology called encryption. Data encryption using strange number system is the process of converting information into an encrypted form, so that it is intelligible only to someone who knows how to 'decrypt' it to obtain the original text. Data encryption and decryption using pentaoctagesimal SNS is a novel concept to secure the data. This algorithm is based on the concept of base encryption in which a word of text is converted into ASCII number and after that it converted into pentaoctagesimal number. Finally after encryption, result is again an ASCII number; this number is converted into original string and sends to the receiver.

II. SNS AND PENTAOCTAGESIMAL SNS

Number system is used just about everywhere, especially traditional number system (binary, octal, decimal and hexadecimal). People count by decimal number system and machine count by binary number system. But there are countless other ways to count. The numbers in strange number system (SNS) are those numbers which are other than the numbers of traditional number system. Apart from these traditional number systems, the strange number system also plays a significant role in computing. The numbers in strange number system (SNS) are those numbers which poses some extra features than the numbers of traditional number system (TNS) viz. decimal (base 10), binary (base-2), octal (base-8) and hexadecimal (base 16). Some of the strange numbers are unary, ternary, …, Nonary, ..., unodecimal, …, vigesimal… sexagesimal, etc [6, 7].

The revolution of digital technologies has changed the way human beings number representation and application from traditional number system to strange number system. In this day and age, most people tend to use strange number system in the various field of computing to perform a variety of tasks. The invention of ternary computer is the best example of such changes to science and technology.

The number system with base eighty five is known as the pentaoctagesimal number system is a form of binary-to-text encoding developed by Paul E. Rutter for the btoa utility. By using five ASCII characters to represent four bytes of binary data, it is more efficient than uuencode or Base64, which use four characters to represent three bytes of data. The basic need for a binary-to-text encoding comes from a need to communicate arbitrary binary data over preexisting communications protocols that were designed to carry only human-readable text.

In the pentaoctagesimal SNS eighty five symbols are used to represent numbers and these are numerals 0 through 9, capital alphabets A through Z, small alphabets a through z and special symbol !, #, $, %, &, (,), *, +, -, ;, <, =, >, ?, @, ^, _,`, {, |, }, and ~. In pentaoctagesimal number system the leftmost bit is known as most significant bit (MSB) and the right most bit is known as least significant bit (LSB). The following expression shows the position and the power of the base 85 [8]:

$$\mathbf{\ldots\ldots 85^{3}85^{2}85^{1}85^{0}.85^{-1}85^{-2}85^{-3}\ldots\ldots}$$

The arithmetic operations like addition, subtraction, multiplication and division operations of decimal numbers can be also performed on pentaoctagesimal numbers. This number system is used in ASCII 85 encoding system to encode binary data to text format.

III. DATA ENCRYPTION DECRYPTION USING PENTAOCTAGESIMAL SNS

Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, people need to ensure information security and safety. Security of network communications is arguably the most important issue in the world today given the vast amount of valuable information that is passed around in various networks. Encryption using pentaoctagesimal strange number system is a better data encoding and decoding strategy, which will offer better security towards all possible ways of attacks while transmission.

Algorithm

Steps for Encryption:

1. Start
2. Calculate the length of the text and store it into a variable
3. Set count=0
4. Do until (end of the file)
5. Read the text and pick the four characters from the text
6. Calculate the ASCII value of each character and concatenate them and store into a variable b
7. Set count=0
8. Do until (b > 85)
9. Set s = “”
10. Do until (b > 0)
11. r = b % 85
12. Concatenate s and r and store it into s
13. Perform integer division between b and 85 and store the result into b
14. End of the loop
15. count = count + 1
16. End of the loop
17. Convert the value of count into string type and concatenate it with s and store the result into str
18. Calculate the length of str and store it into L
19. Set I = 1
20. Do until (I <= L)
21. Read two digit from str and symbolized them using Base 85 number system
22. I = I + 2
23. End of the loop
24. End of the loop
25. Result file is compressed file
26. End

Steps for Decryption:

1. Start
2. Calculate the length of the compressed text and store it into L
3. Set s=” ”
4. Set I = 1
5. Do until (I<=L)
6. Read one symbol from compressed text and convert them using base 85 and store it into str
7. Concatenate s and str and store the result into s
8. Set n = str
9. I=I+2
10. End of the loop
11. Set k=1
12. s1=s
13. Set S2=0
14. Set t=0
15. Do until (k<=n)
16. Calculate the length of s1 and store it into p
17. Set q=1
18. Do until (q<=p)
19. Read two digit from s and store it into r
20. s2 = s2 + (Math.Pow(85, t)) * r
21. q=q+2
22. t=t+1
23. End of the loop
24. s1=s2
25. k=k+1
26. End of the loop
27. Calculate the length of s1 and store it into p
28. Set m=1
29. Do until (m<=p)
30. Read the digit and converted it into character
31. m=m+1
32. End of the loop
33. Extract will be decompressed file
34. End

Algorithm Illustration

For example consider a text like ‘LOVE IS BLIEND’. Then separate four characters from the beginning of the text are ‘L’, ‘O’, ‘V’, ‘E’ and their ASCII values are 76, 79, 86, 69 respectively. After concatenation these four numbers, we get 76798669. Now convert this number into pentaoctagesimal number system whenever converted number is not less than 85. We converted the above number into pentaoctagesimal number system 9 times to get the number less than 85 i.e., 31. Then symbolize 31 and 9 using pentaoctagesimal number system and the encrypted text is ‘V9’. Now the decryption process converts the encrypted text into pentaoctagesimal number firstly and then converted pentaoctagesimal number into decimal number 9 times, i.e., 76798669. Finally, separate two digits and represent their ASCII values to get back the original text. In such a way encryption and decryption process can be done.

IV. CONCLUSION

This paper provides an excellent data encryption and decryption technique to increases the data security and transfer rate during data communication. The algorithm can be used as an encoding converter in text files. In the present network system, to increase security, every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key. Our proposed technique fulfils all such requirements as this technique use the concept of data encryption and decryption. The most prominent feature of strange number system is its full fleshed Cryptography that provides techniques of encryption and decryption while hiding all the technical details. In conclusion, data Encryption with pentaoctagesimal SNS, a base conversion routine, symbol remapping, and a dynamic algorithm is the only encryption algorithm that is as secure as one-time pad.

REFERENCES

[1] T.SubhamastanRao, M.Soujanya, T.Hemalatha, T.Revathi, Simultaneous Data Compression and Encryption, International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011, 2369-2374.

[2] Dr. V. K. Govindan, B. S. Shajee mohan, An Intelligent Text Data Encryption and Compression for High Speed and Secure Data Transmission over Internet. NIT Calicut, Kerala.

[3] Majdi Al-qdah & Lin Yi Hui, Simple Encryption/Decryption Application, International Journal of Computer Science and Security, Volume (1) : Issue (1).

[4] V.K. Govindan, B.S. Shajee mohan, An Intelligent Text Data Encryption and Compression for High Speed and Secure Data Transmission over Internet, unpublished.

[5] D.R. Stinson, Cryptography Theory and Practice, CRC Press, Inc., 2002.

[6] Debasis Das, Dr U A Lanjewar, Strange Number System: An Enhancing Tool for Data Encryption and Decryption, International Journal of Advanced Research in Computer Science, Volume 3, No. 2, March-April 2012.

[7] Debasis Das, Dr. U A Lanjewar, Realistic Approach of Strange Number System from Unodecimal to Vigesimal, International Journal of Computer Science and Telecommunications, Sysbase Solution Ltd. London, vol. 3, Issue 1, pp. 11–16, January 2012.

[8] Debasis Das, Dr. U A Lanjewar, Exploring Strange Number System: Latent Talent to be used in place of Traditional Number System, International Journal of Advances in Science and Technology, vol. 3, No. 1, pp. 102–150, January 2012.

[9] Mark Johnson, Daniel Schonberg, On Compressing Encrypted Data, IEEE Transactions on Signal Processing, vol. 52, No. 10, pp.2992–3006, October 2004.

[10] Mark Johnson, Prakash Ishwar, Daniel Schonberg, Kannan Ramchandran, On Compressing Encrypted Data, IEEE Transactions on Signal Processing, Vol. 52, No. 10, October 2004.

[11] Ajit Singh, Rimple Gilhotra, Data Security using Private Key Encryption System Based on Arithmetic Coding, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

[12] Debasis Das, Abhishek Ray, A Parallel Encryption Algorithm for Block Ciphers Based on Reversible Programmable Cellular Automata, Journal of Computer Science and Engineering, Volume 1, Issue 1, May 2010.