ISSN No. 0976-5697

Volume 3, No. 2, March-April 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Strange Number System: An Enhancing Tool for Data Encryption and Decryption

Debasis Das*
Assistant Professor: MCA Department
VMV Com., JMT Arts & JJP Science College
Nagpur, India
debasis_das2005@rediffmail.com

Dr. U. A. Lanjewar
Professor: MCA Department
VMV Com., JMT Arts & JJP Science College
Nagpur, India
ualanjewar@gmail.com

Abstract: In the electronic age, while information needs to be sent on network with security, it has to be encrypted to protect information from 'prying eyes'. Cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key. Data encryption and decryption using octovicentimal SNS is a novel concept and symbol remapping of cryptography. In this paper we propose a better data encoding and decoding strategy, which will offer better security towards all possible ways of attacks while data transmission.

Keywords: strange number system; octovicentimal; data encryption; data decryption; traditional number system

I. INTRODUCTION

Theoretical research in number theory has a long tradition. Since many centuries, the main goal of these investigations is a better understanding of the abstract theory. Numbers are basic not only for mathematics, but more generally for all sciences; a deeper knowledge of their properties is fundamental for further progress. Remarkable achievements have been obtained, especially recently, as many conjectures have been settled. Yet, a number of old questions still remain open. Among the unexpected features of recent developments in technology are the connections between classical arithmetic on the one hand, and new methods for reaching a better security of data transmission on the other. We will illustrate this aspect of the subject by showing how modern cryptography is related to our knowledge of some properties of strange numbers. As an example, we explain how strange numbers play a key role in the process of data encryption and decryption to secure information during transmission.

Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, people need to ensure information security and safety. **S**ecurity 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. Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet [1].

Data encryption is the process of converting a plaintext message into cipher text which can be decrypted back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. Encryption schemes are based on block or stream ciphers. Data decryption is the process of converting cipher text back to plaintext. Encryption methods can be symmetric in which encryption and decryption keys are the same, or asymmetric in which encryption and decryption keys differ. Public Key methods must be asymmetric, to the extent that the decryption key can not be easily derived from the encryption key. Symmetric keys, however, usually encrypt more efficiently, so they lend themselves to encrypting large amounts of data. Asymmetric encryption is often limited to only encrypting symmetric key and other information that is needed in order to decrypt a data stream, and the remainder of the encrypted data uses the symmetric key method for performance reasons. This does not in any way diminish the security nor the ability to use a public key to encrypt the data, since the symmetric key method is likely to be even more secure than the asymmetric method.

The process of encryption hides data or the contents of a message in such a way that the original information can be recovered through a corresponding decryption process. Encryption and decryption are common techniques in cryptography, the scientific discipline behind secure communications. It is an especially popular and effective technique for maintaining Internet security.

Many different encryption / decryption processes or algorithms exist. It turns out that in cryptography, it's very difficult to keep the logic of an algorithm truly secret. Especially on the Internet, it's generally much easier to use well-known public algorithms, and rely on alternative forms of protection. In computer cryptography, a key is a long sequence of bits used by encryption / decryption algorithms. Some cryptographic algorithms use a single key for both encryption and decryption. Such a key must be kept secret; otherwise, anyone who had knowledge of the key used to send a message could supply that key to the decryption algorithm to read that message. Other algorithms use one key for encryption and a second, different key for decryption. In this case the encryption

key can remain public, because without knowledge of the decryption key, messages cannot be read. In general, keys provide the necessary protection to encrypt and decrypt network communications on the Internet.

Cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances. Almost all cryptographic protocols require the generation and use of secret values that must be unknown to attackers. So, in this paper, we present novel concept of base conversion, symbol remapping, and dynamic algorithms for data encryption and decryption using octovicentimal SNS. It cannot be cracked by brute forced search, which is the main weakness of many current encryption systems.

This paper has two major purposes. The first is to define some of the terms and concepts behind basic cryptographic methods used in today's context, and the second is to provide a better data encoding and decoding strategy. This data encryption and decryption methods uses some mathematical techniques and have been employed by using high level language VB.NET. Our approach is to secure the information using strange number system.

II. BACKGROUND AND RELATED WORKS

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. It is the art of encoding and decoding messages and has existed as long as people have distrusted each other and sought forms of secure communication. The purpose of cryptography is to transmit information such that only the intended recipient receives it.

At present, there are many available data encryption algorithms such as Substitution techniques, RSA encryption, Arithmetic coding, and pipeline data compression and encryption etc.

There are two types of cryptographic schemes: symmetric (private key) cryptography and asymmetric (public key) cryptography. In symmetric key cryptography (also known as private-key cryptography), a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key. For symmetric key ciphers, there are basically two types: BLOCK CIPHERS, in which a fixed length block is encrypted, and STREAM CIPHERS, in which the data is encrypted one 'data unit' (typically 1 byte) at a time, in the same order it was received in. The examples of stream ciphers are RC4 cipher and the one-time pad and of block ciphers are DES and the AES. Public-key cryptography refers to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cyphertext. One of these keys is published or public and the other is kept private. Some examples of popular asymmetric encryption algorithms are RSA, PGP, and DSA etc [2] [3].

Traditionally, several methods can be used to encrypt data streams, all of which can easily be implemented through software, but not so easily decrypted when either the original or its encrypted data stream are unavailable. The best encryption methods have little effect on system performance, and may contain other benefits (such as data compression) built in. The well-known 'PKZIP®' utility offers both compression AND data encryption in this manner [4]. Also DBMS packages have often included some kind of encryption scheme so that a standard 'file copy' cannot be used to read sensitive information that might otherwise require some kind of password to access. They also need 'high performance' methods to encode and decode the data.

A. Existing Systems:

Cryptography is an indispensable tool for protecting information in computer systems. One of the existing system used compression along with encryption using RSA algorithm. This system is basically used for mobile communication. This system provides a solution to this SMS security problem. The approach that is used in this system is to secure the SMS message using Hybrid Compression Encryption (HCE) system. This system compresses the SMS to reduce its length, then encrypts it using RSA algorithm. But this system is using RSA. RSA is a Public Key Encryption method [5]. A disadvantage of using public-key cryptography for encryption is speed. One more exiting system is presented, which provide us a errorless integrated secure transmission of medical information data like Image, Audio, Video etc.

B. Proposed Systems:

The proposed technique 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 octovicentimal number. Finally after encryption, result is again a ASCII number; this number is converted into original string and sends to the receiver.

III. SNS AND ITS IMPORTANCE

Presently in computer science and technology, number system is based on some traditional number system viz. decimal (base 10), binary (base-2), octal (base-8) and hexadecimal (base 16). However, except the traditional number system, there are also some other number systems, those are not as widely known or widely used as traditional number system in computing, but they have charms all their own having a genuine mathematical distinction in its favour. 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].

As we have seen that, not only traditional numbers are used in digital world, but there are some strange numbers, which are also very common and frequently used in most of the digital technologies and devices. Due to the benefits of strange number representation, which include greater speed of arithmetic operations realization, greater density of memorized information, better usage of transmission paths and decreasing of pin number of integrated circuits, this paper concludes that strange number system even though they are not yet more

commercially available, remain a viable field for research, and have a promising future as a replacement for traditional number system.

Today, the complexity of traditional number system is steadily increasing in computing. Due to this fact, strange number system is investigated for efficiently describing and implementing in digital systems. Purpose to review those research papers are to understand the strange number system in depth and their awareness and detailed explanation is necessary for understanding various digital aspects. A basic motivation of this paper is to implement various applications using strange number system in the field of Computer Science and technology.

Although many researcher and knowledge seeker know only the traditional number system such as decimal, binary, octal and hexadecimal and are very comfortable with performing operations using this system, it is important for them to understand that traditional number system is not the only system. By studying other number system such as quadrovigesimal (base-24), hexavigesimal (base-26), heptovigesimal (base-27), trigesimal (base-30), duotrigesimal (base-32), hexatrigesimal (base-36), quadragesimal (base-40), pentagesimal (base-50), sexagesimal (base-60), duosexagesimal (base-62), quadrosexagesimal (base-60), pentaoctagesimal (base-85) and octovicentimal (base-128), researcher will gain a better understanding of how strange number systems work in general.

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.

Since last few decades strange number system has been possible alternative to binary logic. Unfortunately, the development of strange number system was not keeping up with the speed of the binary counterparts. But the strange number system (SNS) does have a genuine mathematical distinction in its favor. By one plausible measure, it is the most efficient of all integer bases; it offers the most economical way of representing numbers. The potential advantages of strange number system distinguish them from the traditional number system and make them worth an extra look; some of these features include [7]:

a. Greater speed of arithmetic operations realization
b. Greater density of memorized information
c. Better usage of transmission paths
d. Decreasing of interconnections complexity and interconnections area
e. Decreasing of pin number of integrated circuits and printed boards
f. Avoid sign problem and zero redundancy problem

The modern digital computer normally deals with the traditional number (i.e. binary, octal, decimal and hexadecimal) as per as computer science and information technology is concern. Apart from these traditional number systems, the strange number system also plays a significant role in computing. The strange number system poses some extra features which distinguish them from the traditional number systems and make them worth an extra look. In this paper, we mainly focused to develop a novel concept for data encoding and decoding using strange number system.

A. Octovicentimal SNS:

Binary numbers are difficult to work with because they require three or four times as many digits as their decimal equivalent. However, digital computers use binary numbers and it is sometimes necessary for the human operator or user to communicate directly with the machine by means of binary numbers. A number system using base 128 (one hundred twenty eight) is known as the octovicentimal number system. It is the largest number which cannot be expressed as the sum of any number of distinct squares. In this system one hundred twenty eight symbols are used to represent numbers and these are numerals 0 through 9, capital alphabets A through Z, small alphabets a through z and some special symbols. It is also a positional number system that each bit position corresponds to a power of 128. It has two parts the integral part or integers and the fractional part or fractions, set a part by radix point. For example (4z8.l3)128

In octovicentimal 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 128 [8]:

$$\ldots..128^3128^2128^1128^0.128^{-1}128^{-2}128^{-3}\ldots..$$

The arithmetic operations like addition, subtraction, multiplication and division operations of decimal numbers can be also performed on octovicentimal numbers. This number system is used to represent in mathematics and military system. This is used to represent bar code and IPv6. Base 128 is also used to develop various applications in computing.

IV. ENCRYPTION AND DECRYPTION USING OCTOVICENTIMAL SNS

Data encryption 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. It is used, while information needs to be sent on network with security. Data encryption and decryption using octovicentimal SNS avoids the major problem (Low Speed, More processing time, More Cost) existing with the current encryption and decryption methods [9].

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances and faster computing technology require these solutions to be continually adapted.

A. Methodology:

Almost all encryption algorithms these days rely mostly on a subset of ASCII (mostly characters and numbers and some punctuation) to represent the plaintext and the cyphertext. There is usually a routine to convert the plaintext into n-bit

sized chunks to feed through the cypherblock. This is often done by literally taking the ASCII bytes of the message and combining enough of them to make n-bit chunks.

Data encryption and decryption using octovicentimal SNS is a novel concept and symbol remapping of cryptography. All the current modern encryption algorithms utilize a limited number of symbols to represent the characters, numbers, and punctuations. Almost all the encryption algorithms rely on a predefined keyspace and length for the encryption/decryption keys, and it is usually fixed (number of bits). It cannot be cracked by brute forced search, which is the main weakness of many current encryption systems.

The data encryption and decryption using octovicentimal SNS 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 octovicentimal number. Finally after encryption, result is again an ASCII number; this number is converted into original string and sends to the receiver.

As an example, we take a string as an input and encoded it as follows-

Unencoded	ASCII	Binary	Encoded
D	68	01000100	)
E	69	01000101	*
B	66	01000010	&
A	65	01000001	%
S	83	01010011	}
I	73	01001001	<
S	83	01010011	}

For the words: "DEBASIS" it is encoded as ")*&%}<}"

B. Algorithm for Data Encryption:

Step-1: Calculate length of the main text and store it into L
Step-2: Initialize C=1
Step-3: While C! = L
- a. Read a single character from the main text
- b. Calculate it's ASCII value and assign it to D
- c. While D>0
  - a) Divide D by 128 and calculate the remainder
  - b) Put the proper symbol of the remainder value and concatenate it with the previous encoded text
  - c) Perform integer division between the value of D and 128 and assign the quotient value into the D variable
- d. End (While)

Step-4: Increment C by 1
Step-5: Return S

C. Algorithm for Data Decryption:

Step-1: Calculate length of the encoded text and store it into L
Step-2: Initialize C=1 and i=0
Step-3: While C! = L
- e. Read a single character from the encoded text
- f. Converted it's Base128 value and assign it to D
- g. While D>0
  - a) Calculate power of 128 depends upon the value of i and add with value of S to get the ASCII value
  - b) Increment i by 1
- h. End (While)

Step-4: Increment C by 1
Step-5: Converted ASCII to Cha and concatenate it with str
Step-6: Reverse str
Step-7: Return str

D. Implementation with Example:

As an example, a section of the poem "It was a Lover and his Lass" of the William Shakespeare looks like this in the original text:

> IT was a lover and his lass,
> With a hey, and a ho, and a hey nonino,
> That o'er the green corn-field did pass,
> In the spring time, the only pretty ring time,
> When birds do sing, hey ding a ding, ding;
> Sweet lovers love the spring.

Running the text through our software yields the following text

It is clear from the above sample data that the encoded text provides a better encryption and a stiff challenge to the hacker. An attacker can decode the encoded text only if he knows the symbols which are used to represent the octovicentimal number system.

V. ADVANTAGES OF DATA ENCRYPTION USING OCTOVICENTIMAL SNS

Base128 data encryption has the following advantages over base64 and base85 data encoding-

- a. Base128 data encoding occupies less space when compared with base64 data encoding
- b. When data is being transmitted by base128 encoding it makes the data transfer easier as only fewer amounts of data needs to be transmitted when compared with base64

VI. USE OF DATA ENCRYPTION IN TODAY'S CONTEXT

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 [10] [11]. Encryption is increasingly used to protect digital information, from personal details held on a computer to financial details transmitted over the Internet. Data encryption plays a very central role in ensuring customers that paying for anything online is secure. Data encryption and decryption are widely used to secure [12] [13]:

- a. Stored data, from single files to entire hard disks;
- b. Computer code such as computer operating systems;
- c. Information transmitted over the Internet, including emails and internet telephony (Voice over Internet Protocol or VoIP);
- d. Entire communications infrastructures, such as wireless networks (including mobile telephony).

VII. 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. In conclusion, data Encryption with octovicentimal SNS, a base conversion routines, symbol remapping, and dynamic algorithms is the only encryption algorithm that is as secure as one-time pad (may be even more so, because even in one-time pad you know the symbol space). All the encryption algorithms these days are fixed in one way or another, and whenever you have anything that is fixed, it can be cracked using brute force techniques in a given time period.

VIII.ACKNOWLEDGMENT

The author wishes to thank Dr. U A Lanjewar, Professor VMV Commerce, JMT Arts & JJP Science College, Wardhaman Nagar, Nagpur for his guidance, support and valuable instructions.

<~WϐιϋWιWτχώμϊWιφλWπρϋWτιϋϋi
[ρόπWιWπμϒiWιφλWιWπχiWιφλWιWπμϒWφχφρφχi
~πιόWχdμϊWόπμWξϊμμφWκχϊφjνρμτλWλρλWψιϋϋi
<φWόπμWϋψϊρφξWόρυμiWόπμWχφτϒWψϊμόόϒWϊρφ
ξWόρυμi
[πμφWɘρϊλϋWλχWϋρφξiWπμϒWλρφξWιWλρφξiWλρφ
ξx
}ϐμμόWτχώμϊϋWτχώμWόπμWϋψϊρφξk

IX. REFERENCES

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

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

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

[4] Ajit Singh, Rimple Gilhotra, "Data Security using Private key Encryption System based on Arithmetic Coding," International Journal of Network Security & Its Applications, Vol. 3, No. 3, pp. 58-67, May 2011.

[5] H. Kruse and A. Mukherjee. "Data Compression Using Text Encryption", Proc. Data Compression Conference, IEEE Computer Society Press, pp. 447, 1997.

[6] 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.

[7] Debasis Das, Dr. U A Lanjewar, "Realistic Approach of Strange Number System from Unary to Decimal," International Journal of Computer Technology and Applications, vol. 3(1), pp. 235–241, 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] Tarek M Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed & Ahmed M Mahfouz, "Hybrid Compression Encryption Technique for Securing SMS" International Journal of Computer Science and Security, Vol. 3, Issue 6, pp. 473-481.

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

[11] Douglas, R. Stinson, "Cryptography – Theory and Practice", CRC Press, 1995.

[12] Kahate A., CRYPTOGRAPHY AND NETWORK SECURITY, Tata-McGraw-Hill, 2nd ed., 2008.

[13] Mohammad Ali Jabraeil Jamali, Ahmad Khademzadeh, Hasan Asil, and Amir Asil, "Encoding and Compressing Data for Decreasing Number of Switches in Base Line Networks," World Academy of Science, Engineering and Technology 54, pp. 35-39, 2009.