Volume 2, No. 7, July 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

MULTILEVEL CRYPTOGRAPHY TECHNIQUE USING GRACEFUL CODES

Prof K.Govinda[1*], Dr.E.Sathiyamoorth

[1]School of Computer science & Engg. VIT University, Vellore, India
kgovinda@vit.ac.in
[2]School of Information Technology & Engg.,VIT University, Vellore, India.
esathiyamoorthy@vit.ac.in

***Abstract*:** Once an application steps out of the bounds of a single-computer box, its external communication is immediately exposed to a multitude of outside observers with various intentions, good or bad. In order to protect sensitive data while these are en route, applications invoke different methods. In today's world, most of the means of secure data and code storage and distribution rely on using cryptographic schemes, such as certificates or encryption keys. Thus, cryptography mechanisms form a foundation upon which many important aspects of a solid security system are built. Cryptography is the science of writing in secret code and is an ancient art. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. This paper describes multilevel cryptography technique for data encryption-decryption using graceful codes.

***Keywords*:** Cryptography, DES, RSA, Graceful Codes, Symmetric, Asymmetric

INTRODUCTION

Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of Cryptography. The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals. [1] "Cryptography" derives from the Greek word *kruptos*, meaning "hidden". The key to hiding data is to devise a hiding (encryption) mechanism that is very difficult to reverse (i.e., to find the original data) without using the decryption key. [2] Usually, the harder it is to discover the key, the more secure the mechanism. In symmetric (also called "secret-key" and, unfortunately, "private key") encryption, the same key (or another key fairly easily computed from the first) is used for both encryption and decryption. In asymmetric (also called "public-key") encryption, one key is used for encryption and another for decryption. More specifically this paper deals with multilevel Symmetric Key cryptography technique using graceful codes which is based on graph theory. A new Symmetric Key cryptographic algorithm has been propsed in this paper with its advantages and disadvantages.

BRIEF HISTORY OF CRYPTOGRAPHY

Cryptography, the science of encrypting and decrypting information, dates as far back as 1900 BC when a scribe in Egypt first used a derivation of the standard hieroglyphics of the day to communicate.[3] There are many notable personalities who participated in the evolution of Cryptography. For example, "Julius Caesar (100-44 BC) used a simple substitution with the normal alphabet (just shifting the letters by 3 positions) in government communications", [3] and later, Sir Francis Bacon in 1623, who described a cipher is known today as a 5-bit binary encoding. He advanced it as a steganographic device by using variation in type face to carry each bit of the encoding". For all the historical personalities involved in the evolution of cryptography, it is William Frederick Friedman, founder of Riverbank Laboratories, cryptanalyst for the US government, and lead code-breaker of Japan's World War II Purple Machine, who is "honored as the father of US cryptanalysis". In 1918 Friedman authored The Index of Coincidence and Its Applications in Cryptography, which is still considered by many in this field as the premiere work on cryptography written this century. During the late 1920s and into the early 1930s, the US Federal Bureau of Investigation (FBI) established an office designed to deal with the increasing use of cryptography by criminals. At that time the criminal threat involved the importation of liquor.

According to a report written in the mid-1930s by Mrs. Elizabeth Friedman, a cryptanalyst employed by the US government like her husband, William F. Friedman, the cryptography employed by bootleggers. Although cryptography was employed during World War I, two of the more notable machines were employed during World War II: the Germans' Enigma machine, developed by Arthur Scherbius, and the Japanese Purple Machine, developed using techniques first discovered by Herbert O. Yardley. In the 1970s, Dr. Horst Feistel established the precursor to today's Data Encryption Standard (DES) with his 'family' of ciphers, the 'Feistel ciphers', while working at IBM's Watson Research Laboratory. In 1976, The National Security Agency (NSA) worked with the Feistel ciphers to establish FIPS PUB-46, known today as DES. Today, triple-DES is the security standard used by U.S. financial institututions. Also in 1976, two contemporaries of Feistel, Whitfield Diffie and Martin Hellman first introduced the idea of public key cryptography in a publication entitled "New Directions in Cryptography". Public key cryptography is what PGP, today's industry standard, uses in its software.In the September, 1977 issue of The Scientific American, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman introduced to the world their RSA cipher, applicable to public key cryptography and digital signatures. The authors offered to send their full report to anyone who sent them self-addressed stamped envelopes, and the ensuing international response was so overwhelming the NSA balked at the idea of such widespread distribution of cryptography source code. In the mid-1980s ROT13 was employed by USENET groups to prevent the viewing of "objectionable material [by] innocent eyes", and soon thereafter, a 1990 discovery by Xuejia Lai and James Massey proposed a new, stronger, 128-bit key cipher designed to replace the aging DES standard named International Data Encryption Algorithm (IDEA). This algorithm was designed to work more efficiently with "general purpose" computers used by everyday households and businesses. Concerned by the proliferation of cryptography, the FBI renewed its effort to gain access to plaintext messages of US citizens. In response, Phil Zimmerman released his first version of Pretty Good Privacy (PGP) in 1991 as a freeware product, which uses the IDEA algorithm. PGP, a free program providing military-grade algorithm to the internet community, has evolved into a cryptographic standard because of such widespread use. The initial versions of PGP were geared towards the more computer literate individual, but to the individual nonetheless. Phil Zimmerman could be compared to Henry Ford in his efforts to provide PGP to every home by making it free, and therefore, affordable. Today, PGP's updated version is offered free to the public. In 1994, Professor Ron Rivest, co-developer of RSA cryptography, published a new algorithm, RC5, on the Internet. It had been claimed that RC5 is stronger than DES. [3] the rest of the paper is organized as follows Chapter III describes the purpose of cryptography, Chapter IV describes about types of cryptography techniques, Chapter V describes the proposed method and architecture in Chapter VI, Chapter VII describes the implementation, Chapter VIII describes the results followed by conclusion.

THE PURPOSE OF CRYPTOGRAPHY

In a typical situation where cryptography is used, two parties (X and Y) communicate over an insecure channel. X and Y want to ensure that their communication remains incomprehensible by anyone who might be listening. Furthermore, because X and Y are in remote locations, X must be sure that the information she receives from Y has not been modified by anyone during transmission. In addition, she must be sure that the information really does originate from Y and not someone impersonating Y. Cryptography is used to achieve the following goals:

***Confidentiality*:** To ensure data remains private. Confidentiality is usually achieved using encryption. Encryption algorithms (that use encryption keys) are used to convert plain text into cipher text and the equivalent decryption algorithm is used to convert the cipher text back to plain text. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use a public/private key pair. [4]

***Data integrity*:** To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication codes or hashes. A hash value is a fixed length numeric value derived from a sequence of data. Hash values are used to verify the integrity of data sent through insecure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered. [4]

***Authentication*:** To assure that data originates from a particular party. Digital certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent. [4]

TYPES OF CRYPTOGRAPHY

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into ciphertext (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms. The most common types are i) Secret Key Cryptography which is also known as Symmetric Key Cryptography and ii) Public Key Cryptography which is also known as Asymmetric Key Cryptography. [2]

Secret Key Cryptography

In secret key cryptography, a single key is used for both encryption and decryption. As shown in Fig. 1, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is

the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

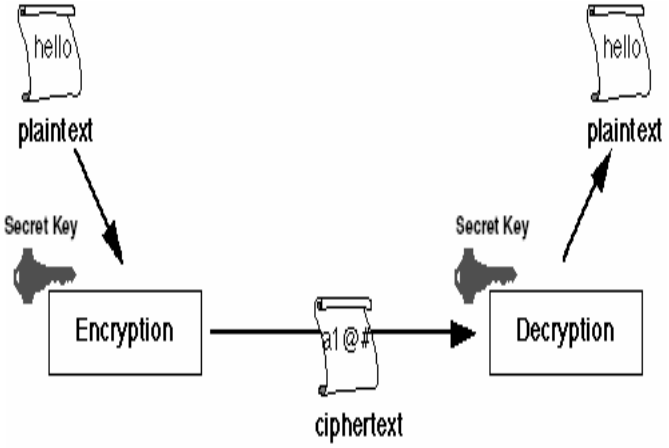

Figure.1 Secret Key Cryptography

Public Key Cryptography

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement. Fig. 2 describes the Public Key cryptography.[8]

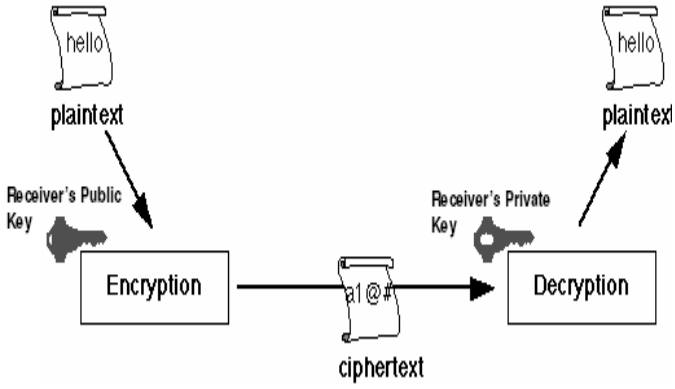

Figure.2 Public Key Cryptography

Many different cryptographic algorithms have been developed in recent past, some of which are worth mentioning like the R.S.A or the D.E.S, which are looked upon as very safer for secure communication. But one thing common to all is the repetition of data values in the cipher coded text, or which in a different language might be called as patterns. An intelligent intruder might easily recognize these patterns and thus can generalize the coding algorithm after a deep analysis. This might pose a serious threat to data communication.

PROPOSED METHOD

In this approach, we define an algorithm, that is much more safer and secure then the rest as it goes into multiple levels of encryption with giving flexibility to the user to choose the depth of security. Moreover, all the data vales, that appears in the final cipher text are unique in that data set. These data sets are in turn unique and different for any value or text in the universal space. By 'levels' of security, we mean we can go up to two, three or 'n' levels based upon user's choice and by 'depth' of security, we mean the number of data values in the final cipher text. This data value can either be chosen by the user or can be taken automatically by the computer randomly, different for each data item.

Example:
For example, if the original data/text is:

LET THE CODING BEGIN.

Thus, with this multilevel cryptographic algorithm, the encryption would be like this:

AMSGEASBDUWXSVEFZAHRCCDKAINHX
NUWDXBWXNWXNXIHXID

Here, it is very difficult for an intruder to figure out that how many characters represents the first letter 'L' and how many for 'E' and so on. Moreover these cipher data sets are unique for each character and inside the set, each value is unique as well in order to eliminate all the patterns (if any).[6]

First of all, all the white spaces are removed from the original string. Now we have a contiguous collection of characters. Each character now is mapped into its equivalent ASCII value. This ASCII values is then encrypted into a set of random numbers, by an algorithm called as the graceful code algorithm, what we call technically as G-codes. This G-code set is unique for all the characters and the number of data values in it is also different for all. This data values are then converted into their equivalent ASCII. But the data values inside a particular set might repeat. For example: for character 'L', the first level encrypted data set might contain: 'ADDAVDS', which has 'A' and 'D' repeated. Although this set as a whole is unique, but the encrypted data set has values repeating, which might create a possibility for an intruder to hack it. Thus in order to eliminate this repeating pattern(s), we move on by digging deeper to a second level of encryption, which converts this G-code into their unique and non-recurring permutations.

Second Level of Encryption

As the original data stream when mapped to an initial (first) level of security had some of the data values repeating, this data stream of repeating values is again encrypted to a second level of security, which had all the data values inside a set as unique with differentiating patterns from other data sets as well. This second level of encryption is technically called as 'permutations', for it map's each and every character into a set of unique values, which differentiates from other sets as well.

This process of encrypting the encrypted form into a deeper level of ciphers is termed as multilevel graceful code cryptography.

ARCHITECTURE

The architecture consists of four major components that forms the whole encryption-decryption process are:

- **Number To Graceful code**
- **Graceful Code To Permutation**
- **Permutation To Graceful Code**
- **Graceful Code To Number**

The first two processes corresponds to the encryption process where in, the first process mappes the original data into the first level of security, but might have repeated data values in the set and the second process encrypts the already encrypted first level values into unique data sets without any reflecting patterns. The other two, thirds and fourth are the reverse of the above two, and forms the decryption cycle as shown in Fig3 depicts the whole secured data communication process.

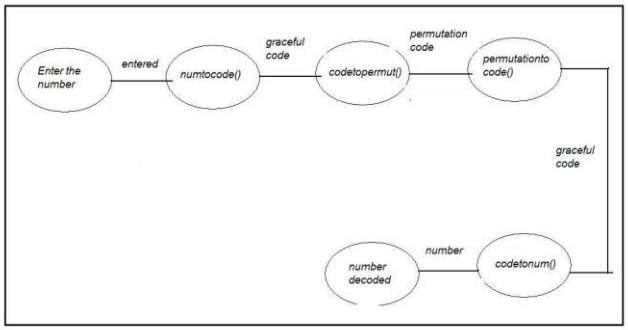

Figure.3 Architecture

IMPLEMENTATION

Practically, the first level of encryption can be represented by a graph as shown in Fig4, with each vertex numbered uniquely like the one shown below. Here, the graceful code (0,4,1,0,1,0) represents the first level of security and is obtained by:
For the below graph V(G) = {0, 1, 4, 6 }

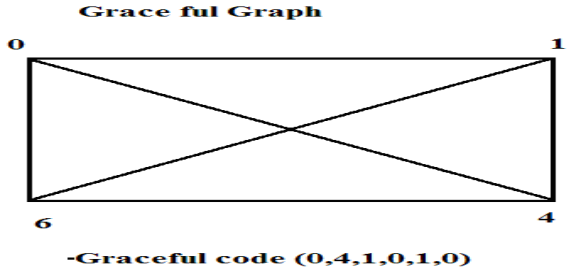

Figure.4 Graceful Graph

Code for this graceful graph will be of the form (a_1, a_2, a_3, a_4, a_5, a_6) where

a_1=min{ e_1=(0,1)} =0

a_2=min{ e_2=(4,6)} =4

a_3=min{ e_3=(1,4)} =1

a_4=min{ e_4=(0,4)} =0

a_5=min{ e_5=(1,6)} =1

a_6=min{ e_6=(0,6)} =0

Thus the graceful code turns out to be:
[0,4,1,0,1,0].

But this set has some of the values repeating like '0' and '1' thus exposing a certain possibility to the eaves-dropper to find the pattern and hack it. Thus, there is an immediate need to dig deeper to a second level of coding, which gives all the values as unique, which can be represented by the same graph.[6]
Here, each unique value can be obtained by subtracting any two edges. Example:

1 => (1-0)
2 => (6-4)
3 => (4-1)
4 => (4-0) and so on as shown in Fig5.

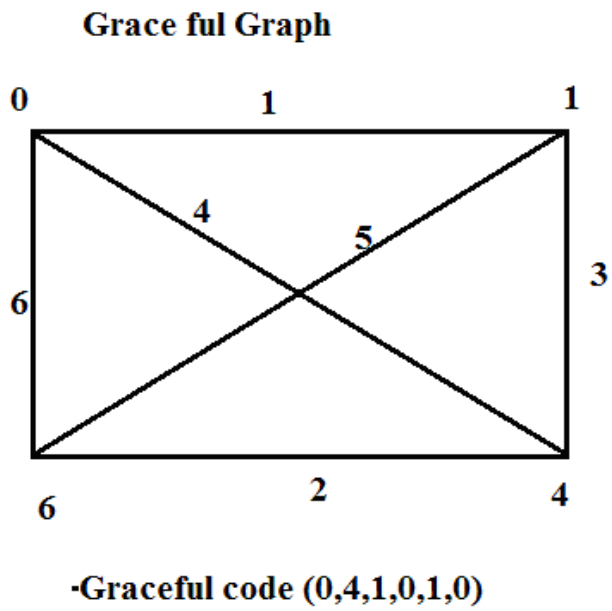

Figure.5 Graceful Graph with unique edge label

These values are unique for all the data sets and has independent unique values inside the set as well. In practical terms, when we are applying this algorithm for securing data privacy over a LAN (say), then these values (1,2,3,4…) would be sufficiently larger so as to map them into their equivalent ASCII into characters.

RESULTS

Here, I present a basic experimental result of the work implemented.

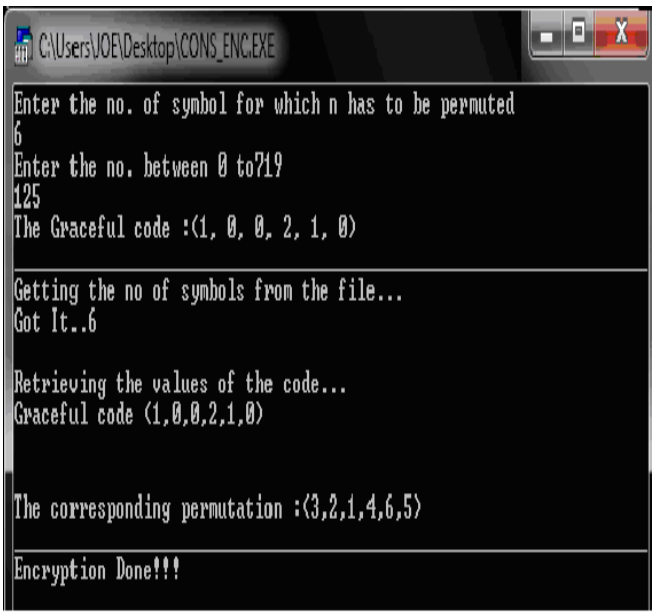

Figure.6 Encryption Process

The above Fig6 shows the encryption process. the first set is the graceful code, which has some of its data values repeating while the second level of encryption shows the permutation values, that has all the values being unique.

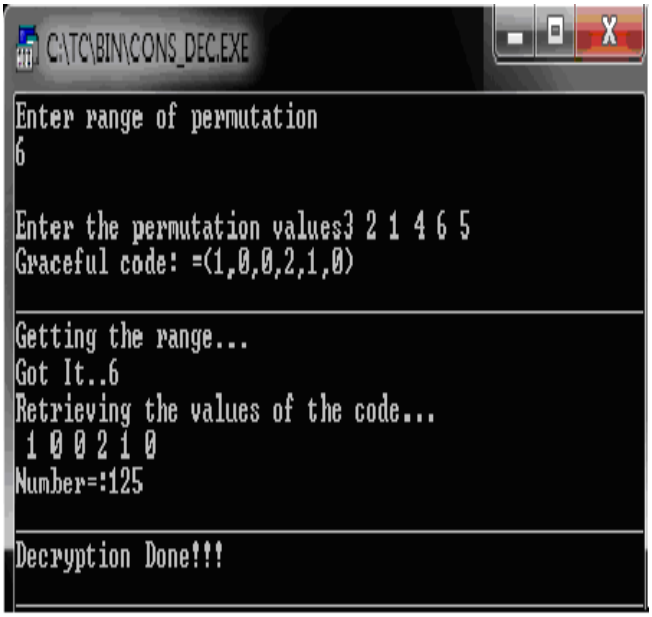

Figure.7 Decryption Process

The above Fig7 shows the opposite of the whole encryption process, decrypting it to give out the original number entered. This is just one representational model of graceful graph cryptography. [9] It is graceful in the sense that it is elegantly and ingeniously simple and ciphers the data to two levels of encryption.

CONCLUSION

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the data which has sent to the receiver from the sender. Now, in order to achieve these goals various cryptographic algorithms are developed by various people. It has been found that the algorithms which are available at this moment are easy to decrypt using some pattern or less complex in nature. Because those algorithms are used to maintain high level of security against any kind of forgeries. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. The aim of this work was to design and implement a multilevel algorithm to address this issue. The same can be extended to texts and large data values. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but of-course not sacrificing the security issues.

REFERENCES

[1] S. William, *Cryptography and Network Security: Principles and Practice*, 2nd edition, Prentice-Hall, Inc.,1999. pp 23-50.

[2] "Basic Cryptographic Algorithms",an article available atwww.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.htm#Algorithms

[3] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html.

[4] K. Gary, *"An Overview of Cryptography"*, an article available at www.garykessler.net/library/crypto.html..

[5] J.A. Bondy and U.S.R Murty ,"Graph Theory with Application", Macmillan Press Ltd, First Edition 1976.

[6] K. Balasubramanium , N.Chandramowliswaran, N. Ramachandran , S Arun , Pawan Kumar ,Mathematical properties of trees generation code and "Algorithm to generate all free code for given number of edge ", Kyoto Interat conf. on Computational Geometry and Graph Theory**.**

[7] Neal Koblitz, "A course in Number theory and Cryptography", Second Edition, Springer.

[8] International William Stalling , "Cryptographic and Network Security- Principles and Practices", Prentice

[9] S.Arun , "Project Report on Graceful Labelings", November 2006, Dept Of Computer Science and Engineering , SCSVMV (Deemed University) Kanchipuram

