Volume 2, Issue 3, March 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multilevel Encryption System using Graceful Codes

G. Usha Devi , Ipsita Rana, Sutanu Nandi

School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India
ushadevi.g@vit.ac.in

***Abstract*— Information security is important for many systems like net-banking, defense systems, Satellite control systems, e-business etc. where small change of data can lead to major problems. Hence there is a need for a stronger encryption which is very hard to break. So, to achieve better results and improve security, information has to pass through several levels of encryption. This paper proposes a multi level of encryption system using graceful codes to increase the security of the algorithm.**

Keywords- Cryptography, Encryption, confidentiality, RSA, Graceful Codes, Asymmetric key cryptography.

I. INTRODUCTION

To ensure the security and confidentially the plain text is converted to unintelligent format, known as cipher text and this process is called as encryption. The way of encryption should not be vulnerable to attacks. Caesar's cipher method, poly alphabetic substitution method, bit-level encryptions like substitution box, permutation box, encoding, and rotation are some of the conventional encryption methods [5]. These methods are easy to implement but can be broken easily with the modern technologies and by various cryptanalysis. The objective of this project is to develop multi-level encryption system using graceful code that can be used to encrypt top-secret files and confidential messages in such a way that no clue is given to the attacker by eliminating all kinds of patterns and the time complexity is low compared to other cryptographic algorithms.

II. RELATED WORKS

There are various cryptanalysis techniques available to break most of the encryption algorithms at one point of time like linear cryptanalysis, n-gram analysis, brute force attack, Man in the middle attack etc. [4]. Besides this in recent past some famous algorithms have been developed like RSA, DES or the AES. These algorithms look safer. But these algorithms cannot eliminate the repetition of data values in the cipher text which is called as patterns [1]. Besides these some multilevel encryption system have been developed using the existing cryptographic algorithms to provide more security [2]. But the disadvantage of this kind of multilevel system is that it is relatively slow compared to other cryptographic algorithms because of multiple levels and multiple algorithms. In recent past some multilevel encryptions using graceful code have also been developed. They eliminate the patterns [1] but the disadvantage is that one character is encrypted into fixed number of data values [2]. So they can be vulnerable to the attackers. Besides these, in some paper, the biometric multilevel encryption is proposed [3]. But this technique is costly and not platform independent.

III. PROPOSED METHOD

It is proposed that the multilevel encryption system using graceful codes which is different and efficient from the existing systems and overcomes all the disadvantages as follows,

1. The system is platform independent. It can be used in any system.
2. It is developed through multilevel encryption to provide more security so that it cannot be broken using any type of the cryptanalysis.
3. It eliminates any type of pattern in the cipher text. All the data values for corresponding characters in the cipher text are unique.
   For example, if the original data/text is:
   i love india.
   Thus, with this multilevel encryption algorithm, the cipher text would be like this: ***doucdndfmteclIwemghijkfksvedjrchiuelgchdgqb***.
   Here, it is very difficult for an attacker to guess that how many characters represents the first letter i and how many for l and so on. So it is almost impossible for the attacker to guess any pattern in the cipher text.
4. One character is encrypted into variable number data values. It is kept secret and automatically determined by the encryption system itself.

The proposed multilevel encryption system is faster than the existing encryption systems such as rsa or the existing multilevel encryption system which is based on the existing cryptographic algorithms.

IV. SOLUTION METHODOLOGY

In this paper, a multilevel encryption system has been proposed with the help of graceful codes. Here in this multilevel encryption system, the concept of graceful graphs are used. The concept of graceful graph is discussed as follows:

A. *Graceful graph*

A labeled graph which can be "gracefully numbered" is called a graceful graph [5].

Generation

1. Label the nodes with distinct nonnegative integers.
2. Then label the graph edges with the absolute differences between node values. If the graph edge numbers then run from 1 to e, where e is the number of edges in the graph, then the graph is gracefully numbered.
3. In order for a graph to be graceful, it must be without loops or multiple edges.

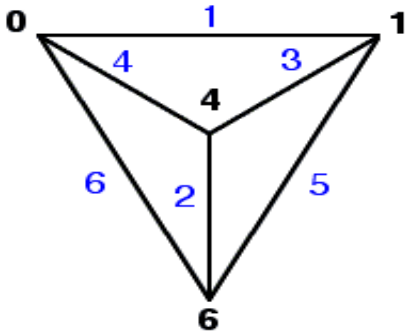

Figure 1. Graceful graph

V. IMPLEMENTATION

To implement a relatively fast and secured multilevel encryption system, the concept of graceful graph is used. Here, two level of encryption is used to eliminate any patterns in the cipher text.

A. *First level encryption*

Firstly, all the blank spaces are removed from the original message. Now we have a contiguous collection of characters. Each character now is mapped into its corresponding ASCII value. This ASCII value is then encrypted into a set of random prime numbers using the prime factors. But this set of random prime numbers may contain repetition of data values, which may create a possibility for an attacker to break it. So we go for another level to eliminate this pattern.

B. *Second level encryption*

Thus in order to eliminate this repeating pattern, we move on to a second level of encryption, which converts this random prime factors into the Graceful code what we call technically as G-codes by mapping them into a Graceful tree in such way that it satisfies all the conditions of the Graceful graph. This G-code set is unique for all the characters, data values are not repeating inside the G-code set for each character and also the number of data values in it is also different for all. Hence, the cipher text is almost impossible to break.

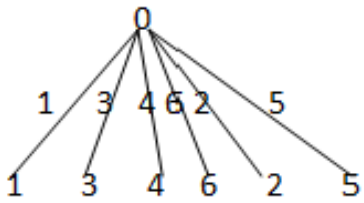

Figure 2. Graceful Tree

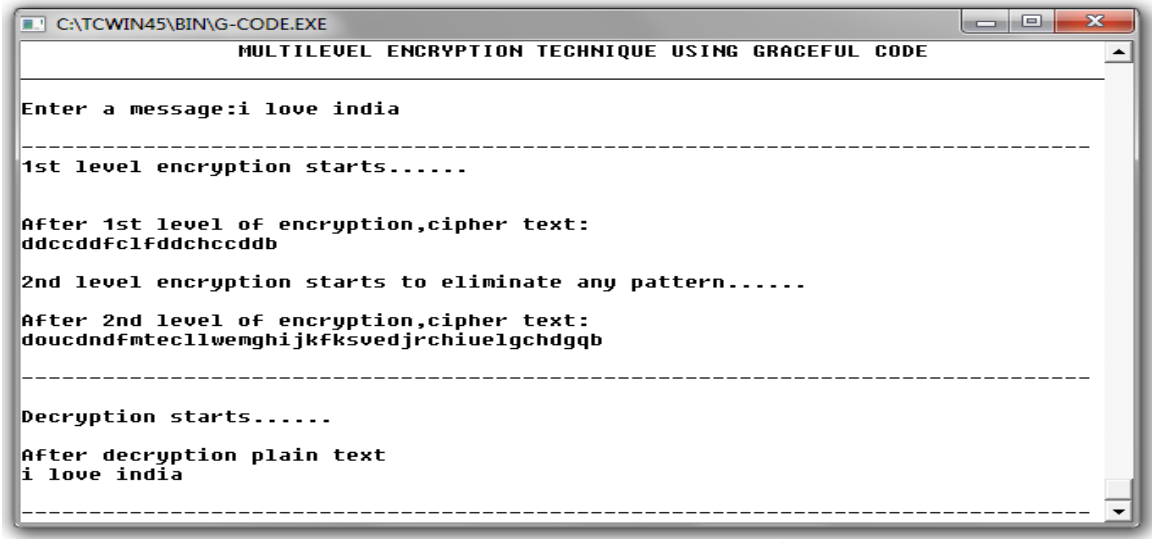

Figure 3. Encryption and Decryption using Graceful code

VI. RESULTS

Basic experiment has been conducted and the result of the work is described here. In the figure 3, we can see that the data value is repeated within the set of prime numbers after the first level of encryption. After the second level of encryption, we get a set of G-code in which all the data values are unique. So there is no pattern in the final cipher text. So it is almost impossible for the attacker to guess any pattern from the cipher text. After that, final cipher text is passed to the receiver and is successfully decrypted to get the plain text.

VII. PERFORMANCE ANALYSIS

After the completion of the development phase, the performance of the multilevel encryption system using graceful code is analyzed against the RSA cryptosystem to provide the security because RSA is the most widely used public key cryptosystem. We have compared with the most widely used public key cryptosystem because in our proposed multilevel encryption scheme same key is not used for encryption and decryption unlike the private key cryptosystem. Encryption is done using the prime factors of the ASCII value of the corresponding character and decryption is done using the counter of the prime factors and the public key and private key is different. So our proposed multilevel encryption system is a public key cryptosystem.

A. Platform

Using the following platform, the performance of the multilevel encryption system is analyzed

Processor: Intel Core 2 Duo processor @ 2.2 GHz
Memory: 3GB RAM
OS: Windows 7 Ultimate (32 bit)
Programming Language: C

Here the execution time and the CPU Utilization of the encryption and decryption are analyzed.

B. Comparison table

The comparison table for this analysis is given below:

TABLE 1. COMPARISON OF EXECUTION TIME

Algorithms	Execution time	CPU Utilization
Multilevel encryption system using Graceful Code	5.36 sec	52%
RSA Cryptosystem	10.43 sec	55%

C. Comparison chart

The data from the table 1 is plotted and figure 4 shows the comparison chart. From the table 1 and figure 4, it is clear that our proposed multilevel encryption system using Graceful code takes much less time for encryption and decryption process than RSA cryptosystem and also it uses less resource in terms of CPU utilization compared to RSA cryptosystem. Besides these RSA needs a longer key size i.e. 1024 bit long but our proposed multilevel encryption system is keyless. Hence, our proposed multilevel encryption system using Graceful code performs much better than the RSA cryptosystem.

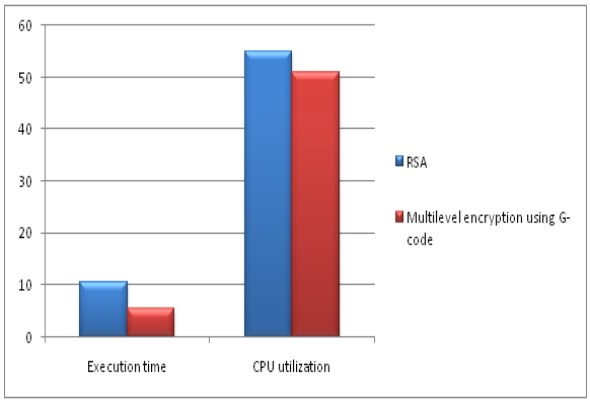

Figure 4. Comparison chart

VIII. CONCLUSION

The above analysis suggests that our proposed multilevel encryption system outperforms the RSA cryptosystem in every prospect. Firstly, it takes less execution time than the RSA; secondly, it uses less CPU than the RSA cryptosystem; thirdly, RSA uses large key size (1024 bit); fourthly, it eliminates any pattern in the cipher text unlike the RSA cryptosystem. Hence, our proposed multilevel encryption system using Graceful code provides the authenticity, privacy, integrity and non-repudiation to ensure better security.

REFERENCES

[1] G.Usha Devi and R.S.D. Wahida Banu, "Secure Multilevel Encryption Using Graceful Codes", International Conference on Network Communication and Computer – ICNCC 2011, Page-530
[2] Sairam Natarajan, Manikandan Ganesan, Krishnan Ganesan, "A Novel Approach for Data Security Enhancement Using Multi Level Encryption Scheme", International Journal of Computer Science and Information Technologies, Vol. 2 (1), 2011, 469-473
[3] Alexander Wong, William Bishop, "Backwards compatible, Multi-level regions-of-Interest (ROI) Image Ecryption Architecture with Biometric Authentication", 2007
[4] Behrouz A. Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", Tata McGraw-Hill © 2010 by McGraw-Hill Companies.
[5] http://mathworld.wolfram.com/GracefulGraph.html

