Secure Multilevel Cryptography Using Graceful Codes

Usha Devi G. and R. S. D. Wahida Banu

***Abstract*—Security plays an important role in most of the applications 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. In order to achieve better results and improve security, information has to pass through several levels of encryption. A multilevel encryption-decryption of original text into cipher data with each character encoded uniquely into its corresponding cipher and eliminating the possibility of any pattern(s) is proposed in this paper. It is graceful that elegantly and ingeniously simple and ciphers the data to two levels of encryption. The analysis shows that there is an improvement in the efficiency compared to conventional schemes.**

***Index Terms*—Multilevel encryption, graceful code, cryptography, security.**

I. Introduction

Many different cryptographic algorithms [1] have been developed in recent past, some of which are worth mentioning like the RSA or the DES, 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.

Secured multilevel cryptography [2] is a new data encryption-decryption technique that focuses on coding the original data into ciphers. It provides more than one level of security so as to eliminate all kinds of patterns that might originate in other cryptographic algorithms. It encodes each character or integer into a set of integer values that is unique for it without any value repeated. Thus any eaves dropper would have no idea about how many integers together form a cipher for a particular character. The value would be random and also there isn't any pattern(s) repeated in the cipher code that would make almost impossible for an intruder to decode.

II. Literature Survey

There are various cryptanalytic 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. [1]. Besides this in recent past some famous algorithms have been developed like RSA[3], 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 [4]. Besides these some multilevel encryption system have been developed using the existing cryptographic algorithms to provide more security [5]. 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 [2] have also been developed. They eliminate the patterns but the disadvantage is that one character is encrypted into fixed number of data values. So they can be vulnerable to the attackers. Besides these, in some paper, the biometric multilevel encryption is proposed [6]. But this technique is costly and not platform independent.

III. Secure Multilevel Cryptography

In the proposed approach, an algorithm defined is much safer and secure than 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 values that appear 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, it can go up to two, three or 'n' levels based upon user's choice and by 'depth' of security, it means 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.

The multilevel encryption system [7], [8] using graceful codes which is different and efficient from the existing systems and overcomes some of 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.
4) For example, if the original data/text is 'LET THE CODING BEGIN', thus, with this multilevel cryptographic algorithm, the encryption would be 'Amsgeasbduwxsvefzahrccdkainhxnuwdxbwxnwx nxihxid'. 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

Manuscript received on May 17, 2012; revised June 12, 2012.

Usha Devi G is with Vellore Institute of Technology University, Tamil Nadu, India (e-mail: ushaadevi_g@yahoo.co.in).

R. S. D. Wahida Banu is with Government college of Engineering, Salem, Tamil Nadu, India.

and inside the set; each value is unique as well in order to eliminate all the patterns.

5) 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. Implementation

A. First Level of Security

First step is that, all the white spaces are removed from the original string and the result becomes a contiguous collection of characters. Each character is mapped into its equivalent ASCII value and then encrypted into a set of random numbers, by an algorithm called as the graceful code [6] algorithm (technically as G-codes). This G-code set is unique for all the characters and the number of data values in it. 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), it is necessary to do a second level of encryption, which converts this G-code into their unique and non-recurring permutations.

B. Second Level of Security

As the original data stream when mapped to an initial (first) level of security had some of the data values repeating. It 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 mapped 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.

C. Encryption-Decryption Cycle

The four major steps that form the whole encryption-decryption process are:

Number To Graceful code
Code To Permutation
Permutation To Code
Code To Number

The first two steps responds to the encryption process where in, the first process maps 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 last two steps are the reverse of the first two and forms the decryption cycle. Fig.2 depicts the whole secured data communication process.

V. Practical Implications

A. Graceful Graph

It is a part of graph theory [9] which uses computational theory. A labeled graph [10] which can be "gracefully numbered" is called a graceful graph [2]. The generation procedure of graph is as follows.

1) Label the nodes with distinct nonnegative integers.
2) 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.

Practically, the first level of encryption can be represented by a graph, with each vertex numbered uniquely as shown in the Fig.1.

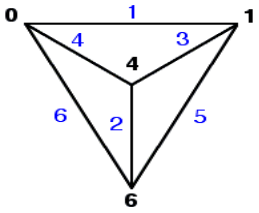

Fig. 1. Graceful graph

The graceful code (0,4,1,0,1,0) represents the first level of security and is obtained for the Fig.1 graph that has vertices V(G)={0,1,4,6}. Code for this graceful graph [11] 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' that expose 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 and that can be represented by the same graph. Here, each unique value can be obtained by subtracting any two edges. For example, (1-0) => 1; (6-4) => 2; (4-1) => 3; (4-0) => 4 and so on. These values are unique for all the data sets and have independent unique values inside the set as well.

In practical terms, when applying this algorithm for securing data privacy over a LAN, these values 1, 2, 3, 4… would be sufficiently larger so as to map them into their equivalent ASCII into characters.

VI. Experimental Results

The basic experimental model has been conducted with 720 numbers. The graceful graph with 6 vertices is assumed to calculate the graceful code which is used in the encryption process. Fig. 3 shows the result of multilevel encryption process. The first set is the graceful code with redundant patterns so that the second level of encryption is done and that has all the values being unique.

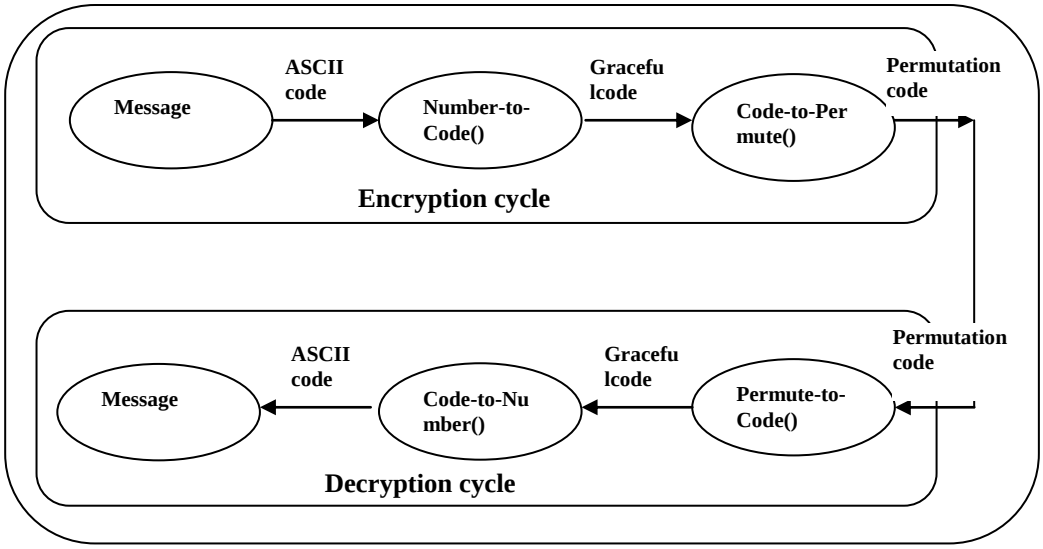

Fig. 2. Multilevel encryption-decryption cycle

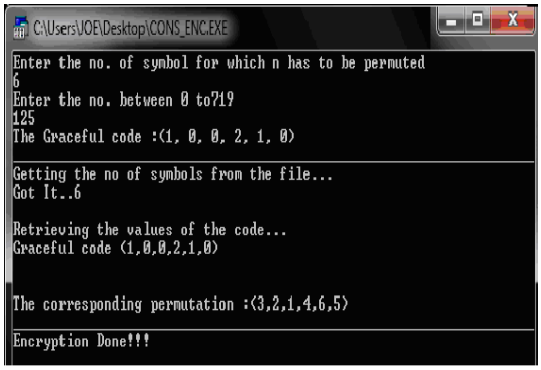

Fig. 3. Snapshot of multilevel encryption process

Fig. 4 shows the reverse of the multilevel encryption process called multilevel decryption which gives out the original data entered.

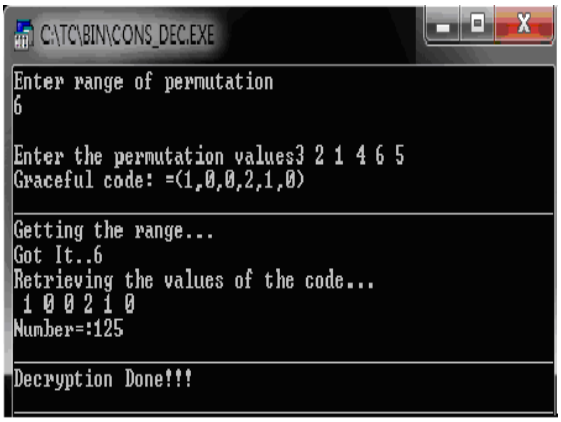

Fig. 4. Snapshot of multilevel decryption process

This is just one representational model of graceful graph cryptography; the same can be extended to texts and large data values. The result confirms more secured communication because of multilevel encryption. If two consecutive characters are same, the encryption algorithm will encrypt them separately to generate different patterns thus eliminating every possibility of pattern recognition by any eavesdropper. Secret key can also be taken from the user and is also encrypted for providing higher level of security. Mapping table does all the index related operations thus giving a sense of a separate tie for each process. Number of permutations generated for each character would be different and random for safer communication. It differentiates between the capital and a small character along with the white spaces. It reduces the time complexity by encrypting the whole string into two parts and then encrypting it simultaneously. It can generate a customized secret key for each individual user. But the space complexity is a bit high.

After the completion of the implementation phase, the performance of the multilevel encryption system using graceful code is analyzed against the RSA cryptosystem to provide the security because RSA is most widely used public key cryptosystem. It is compared with the most widely used public key cryptosystem with its execution time and CPU utilization parameters and the results are shown in the Table I.

TABLE I: COMPARISON WITH EXISTING APPROACH

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

From the Fig. 5, it is clear that the 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 for the encryption process compared to RSA cryptosystem. Besides these RSA needs a longer key size such as 1024 bit but the proposed system uses less size. Hence, the proposed multilevel encryption system using Graceful code performs much better than the RSA cryptosystem.

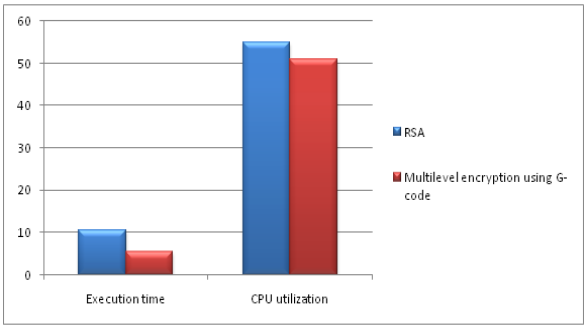

Fig. 5. Comparison chart

VII. Conclusion

Secure Multilevel Cryptography uses features and capabilities of Graceful codes and to deny unauthorized network access and helps to prevent unknown hosts from gaining access to your intranet and privacy.

The proposed multilevel encryption system outperforms the RSA cryptosystem in several aspects. Confidentiality can be ensured since multilevel encryption can be done using Graceful codes. It takes less execution time and less CPU utilization than the RSA cryptosystem. It eliminates any pattern in the cipher text unlike the RSA cryptosystem. Finally, it uses less key size than RSA. Hence, the proposed multilevel cryptography system using Graceful code provides the authenticity, privacy, integrity and non-repudiation to ensure better security.

References

[1] W. Stallings, "Cryptographic and Network Security- Principles and Practices," *Prentice Hall*, 1999.

[2] G .U. Devi and R. S. D. W. Banu, "Secure Multilevel Encryption Using Graceful Codes," *International Conference on Network Communication and Computer – ICNCC* 2011, pp. 530-532, 2011.

[3] B. A. Forouzan and D. Mukhopadhyay, "Cryptography and Network Security," Tata McGraw-Hill, 2010.

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

[5] K. Balasubramanium, N. Chandramowliswaran, N. Ramachandran, S. Arun, and P. Kumar, "Mathematical properties of trees generation code and Algorithm to generate all free code for given number of edge," *Kyoto International conference on Computational Geometry and Graph Theory*, 2007

[6] N. Koblitz, "A course in Number theory and Cryptography," *Second Edition*, Springer, Second edition, 1994.

[7] S. Natarajan, M. Ganesan, and K. Ganesan, "A Novel Approach for Data Security Enhancement Using Multi Level Encryption Scheme," *International Journal of Computer Science and Information Technologies*, vol. 2, no. 1, 2011, pp. 469-473

[8] A. Wong and W. Bishop, "Backwards compatible, Multi-level Regions-of-Interest (ROI) Image encryption architecture with biometric authentication," in press.

[9] Computational Geometry and Graph theory, Springer, 2008

[10] J. A. Gallian, "A dynamic survey of graph labeling," *Electronic Journal of Combinatorics* (DS6), October 2006.

[11] Wolfram. [Online]. Available: http://mathworld.wolfram.com/GracefulGraph.html

Usha Devi G is an Assistant professor – Senior Grade in the School of Information technology and Engineering, Vellore Institute of Technology University, Vellore, Tamil Nadu, India. She received her Bachelor of Engineering degree in Computer Science and Engineering from University of Madras and Master of Engineering in Computer science and Engineering from Anna University, Chennai. Her research interests include Secure Group Communication, Wireless and Ad-hoc networks, Network Security and Multicast communications.