J.Natn.Sci.Foundation Sri Lanka 2024 52 (4): 435- 440
DOI: http://dx.doi.org/10.4038/jnsfsr.v52i4.12196

RESEARCH ARTICLE

Cryptography

Symmetric encryption using snake graphs and supermagic covering

PGRS Ranasinghe*, RMVV Bandara and AMSLK Athapaththu
Department of Mathematics, Faculty of Science, University of Peradeniya, Peradeniya, Sri Lanka.

Submitted: 18 May 2024; Revised: 17 September 2024; Accepted: 26 September 2024

Abstract: Cryptography involves the exploration of methods for safeguarding sensitive information. In this pursuit, graph-theoretic approaches play a significant role. Graph labeling, a key aspect of this, assigns labels or values to vertices and edges within a graph, serving as a means to encode information. It is instrumental in designing cryptographic protocols centered around graph-based structures. The sheer variety of labeling methods makes it challenging to discern the specific technique employed and distinguish between the graphs used for encryption. Notably, in 2020, Giridaran utilized super magic labeling as an encryption technique. Building upon this foundation, our present cryptographic scheme leverages graphs with snake vertex labeling to symmetrically encrypt plaintext. This encryption process harnesses the inherent randomness within super magic covering wheel graphs of odd order, in tandem with an advanced shift cipher. In this scheme, both the sender and receiver possess a secret key pair (k,l), carefully selected for the task at hand. The encryption process employs an odd number k, representing the sides of a cyclic graph (polygon), while l is chosen to preserve the symmetries of consecutive snake graphs. The use of graph labeling proves to be an effective tool in the creation of flexible, efficient, and secure cryptographic protocols. Our protocol, tailored for encryption, ensures a high level of security by capitalizing on the intrinsic structure and the stochastic nature of graph labeling. Through the careful selection of the labeling scheme, we have devised a protocol that remains resilient against a range of potential attacks, including impersonation and replay attacks.

Keywords: Shift cipher, snake vertex labeling, supermagic covering, wheel graph.

INTRODUCTION

Today, information security stands as a paramount concern, encompassing a spectrum of tools and methodologies designed to safeguard sensitive data. Cryptography, the field dedicated to the development of techniques for ensuring information security, plays a pivotal role in this endeavor. Among the mathematical tools used in implementing cryptographic schemes, graph theoretical concepts get their prominence.

To state a couple of related results in literature, in 2014, Al Etaiwi (2014) presented an encryption algorithm using spanning trees and in 2020, Giridaran (2020) used super magic labeling in encryption which is the base for the present study.

In the present cryptographic scheme, we use graphs with snake vertex labeling to encrypt a plaintext symmetrically (symmetric encryption means using one key to encrypt and decrypt the message) using the randomness of the distribution of super magic covering of wheel graphs of odd order. The sender and the receiver hold the secret key pair (k,l) which has been chosen appropriately; k is the number of sides of a cyclic graph (polygon) and l is chosen to preserve the symmetries of numbers labeled on vertices of consecutive snake graphs.

* Corresponding author (rajithamath@sci.pdn.ac.lk; https://orcid.org/0009-0008-4973-8299)

METHODOLOGY

First, we shall provide some graph theoretic terminologies in relation to our cryptographic scheme.

Definition 1. A *snake graph* $C_{k,q}^{m}$ is the fusion of m number of k-cycles, C_k, such that, for $2 \leq i \leq m$, a shared vertex called the vertebrae, denoted v_i, results from the fusion where a minimal path of length q joins v_{i-1} and v_i.

The points of fusion, denoted v_i, are the internal vertebrae of the snake, $2 \leq i \leq m$. Additionally, the vertebra v_1 is a vertex in the first cycle that has a path of q edges between it and v_2, while the vertebra v_{m+1} is a vertex in the m^{th} cycle that has a path of q edges between it and v_m.

A minimal path of length qm from v_1 to v_{m+1} is called the spine. The vertices along the spine which are not shared between two cycles are referred to as s_l^i, where i refers to the cycle to which the spine vertex belongs and l refers to the distance between s_l^i and v_i. For all snakes, $1 \leq i \leq m$ and $1 \leq l \leq q-1$.

The path of $(k-q)m$ edges from v_1 to v_{m+1} that does not contain any vertices on the spine is called the belly of the snake graph. The vertices along the belly not shared between two cycles are referred to as b_j^i, where i refers to the cycle to which the belly vertex belongs and j specifies the distance between b_j^i and v_i. For all snakes, $1 \leq i \leq m$ and $1 \leq j \leq k-q-1$.

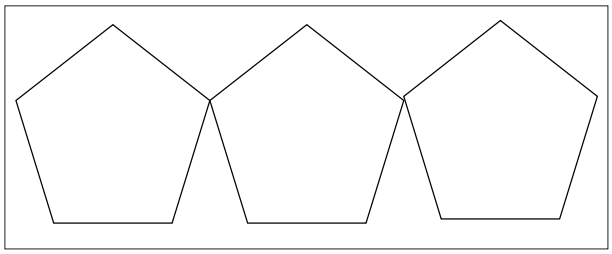

Figure 1: A snake graph with 3 cyclic graphs of 5 vertices

Definition 2. The assignment of integers to the vertices, edges, or both based on some condition is known as graph labeling.

Definition 3. A cyclic snake labeling is defined by the following bijective mapping $f(x): V(C_{k,q}^{m}) \to \{1,2,\ldots,m\}$. For any vertex x in $C_{k,q}^{m}$ such that $1 \leq i \leq m+1$, $1 \leq j \leq k-q-1$, and $1 \leq l \leq q-1$,

$$f(x) = \begin{cases} ik-i-k+2 & \text{if } x = v_i, \\ ik-i+1-q+l & \text{if } x = s_l^i, \\ ik-i-k+j+2 & \text{if } x = b_j^i. \end{cases}$$

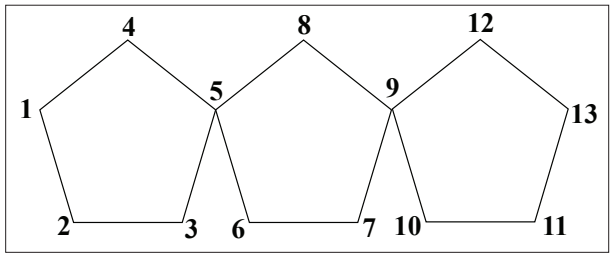

Figure 2: Cyclic snake labeling of a snake graph.

Definition 4. A wheel graph W_n of order n is a graph that contains a cycle of order $n-1$ and for which every graph vertex in the cycle is connected to one other graph vertex.

Definition 5. The process of assigning labels to the edges of G such that the sum over the edges incident with any vertex is the same, independent of the choice of vertex is known as magic labeling.

In magic labeling, if the labels assigned are the first q positive integers, where q is the number of edges in the graph, then such a labelling is called supermagic labeling.

Definition 6. Let $G = (V, E)$ be a finite simple graph. An edge-covering of G is a family of subgraphs $H_1, \ldots, H_k$ such that each edge of E belongs to at least one of the subgraphs H_i, $1 \leq i \leq k$. Then it is said that G admits an $(H_1, \ldots, H_k)$ (edge) covering. If every H_i is isomorphic to a given graph H, then G admits an H-covering.

Suppose that $G = (V, E)$ admits an H-covering. A bijective function $f: V \cup E \to \{1,2,\ldots,|V|+|E|\}$, is an H-magic labeling of G whenever, for every subgraph $H' = (V', E')$ of G isomorphic to H, $F(H') = \sum_{v \in V'} f(v) + \sum_{e \in E'} f(e)$ is constant. In this case, we say that the graph G is H-*magic*. If $F(V) = \{1,2,\ldots,|V|\}$, then G is said to be H-supermagic. The constant value that every copy of H takes under the labeling f is denoted by $m(f)$ in the magic case and by $s(f)$ in the super magic case [2].

In the present cryptographic scheme, we use graphs with snake vertex labeling to encrypt a plaintext symmetrically using the randomness of the distribution of super magic labeling of wheel graphs of odd order. Both the sender and the receiver hold the secret key k, where k is the number of sides of a cyclic graph (polygon) and l is chosen to preserve the symmetries of consecutive snake graphs.

RESULTS AND DISCUSSION

Encryption and decryption algorithms are stated below along with an example.

Encryption algorithm with an illustration

For example, suppose we want to encrypt the plaintext $M = \text{mathematics}$, with $r = 11$ number of characters.

Step 1. The secret key pair (k, l) is chosen appropriately. We choose positive integers $p = 3, s = 2 (< k = 5)$ such that $pk - (p-1) = r + s = 13$, thus, we get $k = (r + s + p - 1)/p = (11 + 2 + 3 - 1)/3 = 5$. We can construct a snake graph with $p = 3$ cyclic graphs of $k = 5$ vertices.

Step 2. We convert each character of M into 3-digit ASCII representations and s is the number of dummy characters that are attached to the original message (such as spaces). Thus, we get $r + s = 11 + 2 = 13$, 3-digit ASCII representations.

Step 3. We assign each ASCII representation to each vertex according to the snake graph labeling. ASCII representations of each letter in 'mathematics' are $[109, 097, 116, 104, 101, 109, 097, 116, 105, 099, 115]$.

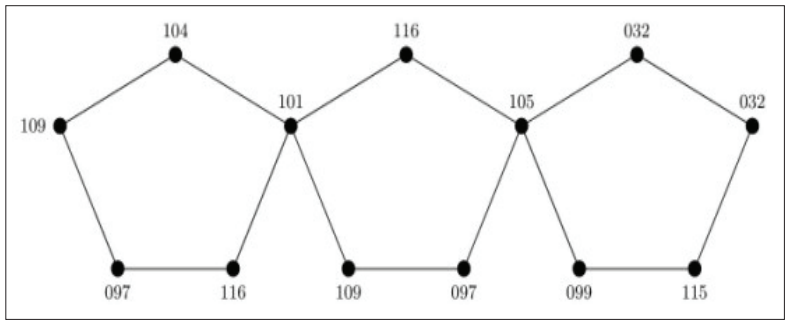

Figure 3: Snake graph with vertices labeled using ASCII representations

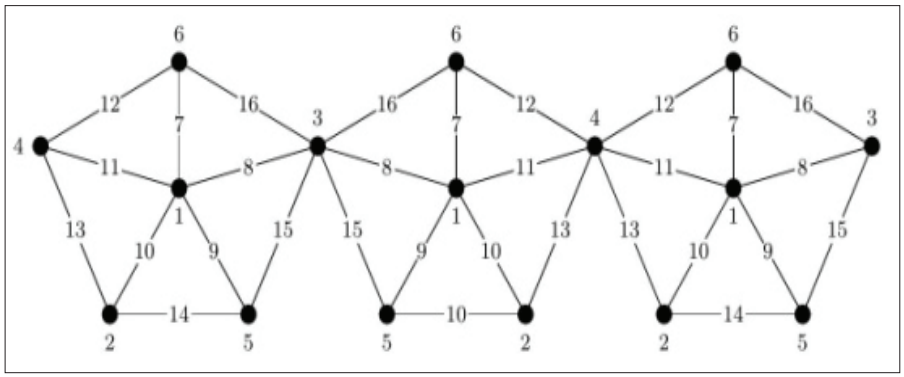

Figure 4: Wheel snake graph labeled using supermagic labeling

Step 4. We construct a similar cyclic graph, modify it into a wheel graph, and label it with C_3-supermagic labeling. In this step we assign the value $l = 3$ to the connecting vertex of the first cycle of the snake graph and the next cycle is constructed as the mirror graph of the previous one.

Step 5. We consider the two snake graphs in steps 3 and 4. Each assigned ASCII value is multiplied by the corresponding vertex label value and the value assigned to an edge between consecutive vertices is added to that. The final value (mod 128) is replaced with the original vertex in the graph of step 3.

For example, consider the first letter 'm' of the plaintext. ASCII representation of 'm' is 109, the corresponding vertex label value is 4 and the edge label value of the edge between the vertex and the consecutive vertex is 13. Therefore, we have to multiply 109 by 4 and add 13 under modulo 128. $(109 \times 4) + 13 = 449 \equiv 65 \pmod{128}$. So, we get 065 as the new vertex label value.

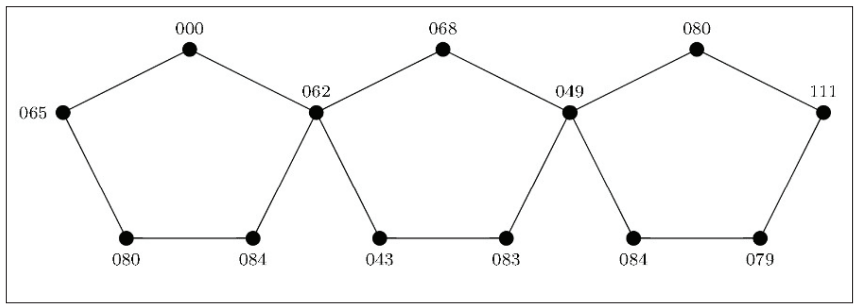

Figure 5: Snake graph labeled with newly assigned vertex labels

Step 6. We obtain the characters represented by ASCII values as the encrypted message $[A, P, T, NUL, >, +, S, D, I, T, O, P, o]$.

Decryption algorithm with an illustration

Now, suppose we want to decrypt the encrypted message, using the shared secret key pair $(k, l); k = 5$ is the odd number of sides of a cyclic graph, and $l = 3$ is the number we consider for symmetries of snake cycle graphs.

Step 1. First, we count the number of characters in the encrypted message, and it is the value of $r + s = 13$. Since we know the value for $k = 5$, we use the equation $pk - (p - 1) = r + s$ to calculate p (number of cycles in the snake graph).$(p \times 5) - (p - 1) = 13 \Rightarrow p = 3$.

Step 2. Next, we can construct a snake graph with $p = 3$ cyclic graphs of $k = 5$ vertices and assign ASCII representations of each character in the encrypted message consecutively. Let those values be m_i.

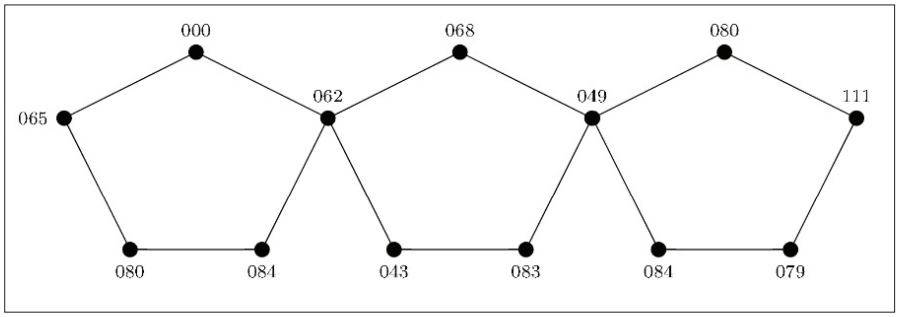

Figure 6: Snake graph labeled using the encrypted message

Step 3. We construct a similar cyclic graph into a wheel graph and label it with supermagic covering. In this step we assign the value $l = 3$ to the connecting vertex of the first cycle of the snake graph and the next cycle is constructed as the mirror graph of the previous one.

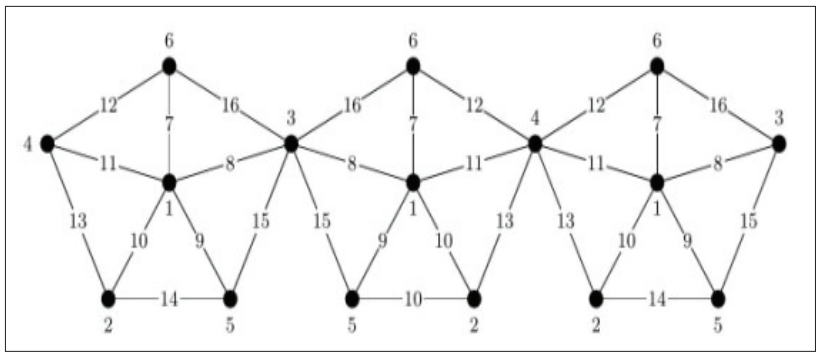

Figure 7: Wheel snake graph with supermagic labeling

Step 4. We consider the two snake graphs in steps 2 and 3. We denote each ASCII value in the encrypted snake graph as d_i in the snake cyclic graph of step 2 and the snake wheel graph of step 3, the edge value between two consecutive vertices is e_i and the previous vertex value be l_i. To decrypt the encrypted message, we find solutions (m_i) for the system of congruences; $l_i m_i + e_i \equiv d_i \pmod{128}$. Here the largest solution for $m_i \pmod{128}$ is the ASCII value corresponding to each character of the original message.

For example, consider the letter 'A' of the encrypted message. Here, $l_i = 4, e_i = 13$ and $d_i = 65$. Solving $4m_i + 13 = 65 \pmod{128}$ we get $m_i \equiv 13, 45, 77,$ and 109 modulo 128. Since 109 is the largest value, it is the ASCII value corresponding to the first character of the original message.

Step 5. Finally, using the ASCII table we can obtain characters represented by ASCII values(m_i) as the original message $M = \text{'mathematics'}$.

CONCLUSION

The wheel W_k for $k \geq 5$ odd, is C_3-supermagic [2]. Hence for every odd number k, we can choose the appropriate key pair (k, l). The uniqueness of the labeling of the snake wheel graph is preserved by defining a total labeling f of W_n as follows. Set $f(v) = 1$, $f(v_n v_1) = 2n + 2$ and for $1 \leq i < n$, $f(v_i v_{i+1}) = 3n + 2 - i$, where v is the center vertex of a wheel.

Error handling is essential in cryptographic protocols to ensure reliability and security. Our scheme implements input validation to prevent processing errors, robust key management for secure key generation and renewal, and error detection codes to verify data integrity during transmission. Additionally, the system is designed for graceful degradation, providing informative error messages while safeguarding sensitive information.

The key parameters in our cryptographic scheme are chosen with careful consideration to enhance security and performance. An odd number of sides in cyclic graphs promotes randomness in labeling, complicating pattern recognition for attackers. Snake graphs are utilized for their complex interconnections, while super magic labeling ensures uniformity and randomness. The shift cipher approach offers efficiency and an added layer of security through modular arithmetic.

Given the wide array of graph labeling methods found in literature, the utilization of graphs in cryptography is considered secure, primarily due to the challenge of identifying the specific labeling technique and distinguishing between encrypted graphs. In our study, we harnessed the randomness of the supermagic covering and a sophisticated shift cipher approach for the encryption and decryption of confidential messages. As a future direction, we aim to explore the application of diverse graph-theoretic techniques to further enhance the security of our cryptographic scheme. Some potential extensions include investigating other graph labeling methods and incorporating additional graph structures.

REFERENCES

Etaiwi, W. (2014). Encryption algorithm using graph theory. *Journal of Scientific Research and Reports*, *3*(19), 2519-2527. https://doi.org/10.9734/jsrr/2014/11804

Giridaran, M. (2020). Application of super magic labeling in cryptography. *International Journal of Innovative Research in Science, Engineering and Technology, 9*(6): 4816-4822. https://doi.org/10.15680/IJIRSET.2020.0906003

Lladó, A., & Moragas, J. (2007). Cycle-magic graphs. *Discrete Mathematics*, *307*(23), 2925-2933. https://doi.org/10.1016/j.disc.2007.03.007