Contemporary Mathematics
https://ojs.wiserpub.com/index.php/CM/

Research Article

An ASCII Value Based Data Encryption Using Coloring Tripartite Graph

Gomathi D[1], Sivakumar Nagarajan[2*]

[1] Department of Mathematics, School of Advanced Sciences, Vellore Institute of Technology, Vellore, 632014, Tamil Nadu, India
[2] School of Computer Science and Engineering,Vellore Institute of Technology, Vellore, 632014, Tamil Nadu, India
E-mail: nsivakumar@vit.ac.in

Received: 8 October 2024; **Revised:** 10 January 2025; **Accepted:** 4 March 2025

Abstract: In current network systems, cryptography plays a vital role in ensuring a secure data transfer. Robust encryption is essential to safeguard data during transmission, making it a top priority. Encryption transforms readable data into an unreadable format and is commonly used for data protection. Modern cryptography incorporates graph theory principles to enhance the security of information-sharing over networks. This study introduces an ASCII-based data encryption system that utilizes a Coloring Tripartite Graph (CTG) as a confidential key to facilitate secure data exchange. In addition to detailing the security protocols, the recipient receives encrypted data in the form of CTG. The adoption of this encryption technology significantly enhances the security of data transmissions.

***Keywords*:** graph theory, encryption, decryption, coloring tripartite graph

MSC: 05C90, 68P25, 94A60, 05C15

1. Introduction

Global information sharing has become simpler and international society has become more integrated because of the growth of the Internet and advanced networking technologies. Network security has become crucial because of the need to protect precious intellectual property that has become accessible over the internet. The following elements have been carefully considered when establishing a secure network. Access: Only authorized users have been able to communicate with a network. Privacy Protection: Ensuring that data on the network remain private. Verification: Ensuring the uniqueness of persons connected to the network. Data Integrity: Ensuring that messages are not distorted during transmission. Accountability: Keeping users from taking back action on the internet.

A comprehensive network security strategy includes essential security levels, possible attackers, security threats, and vulnerabilities that may affect network attacks. A range of security procedures such as intrusion detection, firewalls, encryption, security management, and authentication methods have been implemented to enhance the protection of computers and networks. Companies worldwide have used a combination of these tools to safeguard their systems. Intranets linked to the internet have been fortified against potential risks. Understanding Internet security challenges is vital for creating effective defenses against online network threats [1]. Data security includes transforming a client's information into a format that is unreadable and requires a specific key for decryption before sharing. Although this

DOI: https://doi.org/10.37256/cm.6220255856

approach is relatively effective, robust encryption has been compromised in the past. To keep up with evolving hacking techniques, encryption methods must be updated frequently. Additionally, sending encrypted data requires a secure network to avoid the accumulation of unwanted messages and protect against unauthorized access [2]. Encryption techniques have frequently been employed to conceal information by first transforming plain text into cipher text through encryption, and then back to plain text through decryption. These methods depend on a secret key that is only accessible to authorized users [3]. Algorithms used in cryptography are divided into two categories: symmetric and asymmetric algorithms. In asymmetric key encryption, two separate keys are used: the sender's private key for encryption and the receiver's public key for decryption. In symmetric-key encryption, both the sender and recipient use the same key for encryption and decryption [4]. In the past few years, there has been growing interest in using graph theory methods for encryption. Graph theory, a specific area of mathematics, studies the properties of graphs, which are the essential elements of discrete mathematics. A graph usually represents the connections between entities through a set of vertices linked by edges. Graphs are used in various domains including electrical networks, transportation systems, and astronomical structures. They offer an organized approach to solving different problems and have served as the foundation for numerous software applications that enhance communication and facilitate complex technical processes [5]. A colored graph K contains vertices that are colored such that no two adjacent vertices share the same color. The chromatic number, denoted by $x(K)$, indicates the total number of colors required for coloring. If the chromatic number $x(K)$ equals k, the graph is called k-chromatic [6]. A tripartite graph has edges connecting each pair of vertices from different sets, and its vertices can be partitioned into three independent sets. The entire vertex set was split into three levels using a tripartite graph. There can be any number of vertices at level [7].

The principal aim is to enhance encryption techniques by utilizing a tripartite graph. In this study, a novel encryption method for safe data transit was developed by combining coloring with the concept of a tripartite graph. After generating a shared secret key using a Colored Tripartite Graph (CTG), the encrypted communication is sent to the receiver in the CTG format. Preserving data privacy is the primary focus. The present paper is divided into six sections: Section 2 surveys the existing literature, Section 3 provides an encryption algorithm and different Observations, Section 4 presents a security analysis, Section 5 presents a Discussion and Section 6 concludes the paper.

2. Related work

Our research was guided by the existing body of literature concerning data protection, particularly on cryptographic algorithms and their associated security characteristics. We thoroughly reviewed the relevant studies to guide our methodology. Ni and Qasi designed sophisticated encryption methods to enhance secure communication. They achieved this by combining different algebraic characteristics with distinctive corona, bipartite, and star graphs. These encryption techniques depend on a shared key that both parties must agree upon and exchange during the message-encoding process [8]. A method for encoding and decoding data based on ASCII character values was developed by Mathur and Akanksha Using these numbers and a secret key, the encryption process changes the data so that plain text can be converted for both encryption and decryption. Because the same key is used for both operations, this method employs symmetric encryption. The data length must match the size of the user-supplied key to ensure that the algorithm operates appropriately [9]. To address data security challenges, Khalaf and colleagues developed an enhanced triple-hill cipher technique. They showcased their application in encrypting binary data, such as images, audio, and video files on the Field-Programmable Gate Array (FPGA). The three stages of the method enhance the strength and ensure strong security for binary data. Each phase incorporates a block cipher with a block size of 128 bits and a key range of 256 bits. Following these three stages, binary data are encrypted using keys generated randomly by a random number generator [10]. Kumari and Kirubanad [11] formulated a new method for encryption and decryption using graph plotting. The upgraded affine cipher algorithm programmed a confidential message by converting it into an ASCII value. Additionally, to aid comprehension, encrypted information is visually depicted on a graph. The data points on the graph were sheltered from unauthorized sightings and alterations by transforming them into images. To enhance cipher security beyond conservative methods, Naik and Tungare [12] developed a novel cryptographic replacement method. Inspired by the Play Color Cipher algorithm, their

method involved replacing special symbols, numerals, and characters with colored blocks. Sensarma and Samanta [13] emphasized how graph theory ideas can be applied to network monitoring, particularly when determining a router's significance through traffic analysis. Two graph-based encryption techniques, intended to safeguard private data, have been introduced. Whereas the second method uses visual codes, the first method uses matrix attributes. Yamuna and Karthika [14] demonstrated how to use a bipartite graph to demonstrate data, and constructed a number table to represent letters.

Kedia and Agrawal [15] researched a novel encryption method that used both letters and numbers to increase data security. In this way, they fuse concepts as basic as Venn diagrams with concepts as sophisticated as graph theory. Selvakumar and Gupta [16] developed a unique encryption and decryption technique that uses interconnected graphs. The spanning tree of the graph is used to encrypt a message. Kumar and Krishnaa [17] explored the use of bipartite trees in conjunction with various graph labeling approaches, such as harmonic, graceful, sequential, and felicitous labelling, for encryption and decryption. They found that in a balanced bipartite tree, the numbers of vertices in the left and right partite sets were equal. Based on the adjacency matrix of a graph, Kaur and Namrata [18] developed a novel encryption and decryption technique. Comparing this method with simpler algorithms, the "double-transposition column" approach has a few advantages. Cryptoanalysts have faced difficulties owing to the algorithm's use of a graph as its key. Regretfully, only texts sorted alphabetically can be processed by the algorithm. Uniyal and Agarwal [19] created an effective encryption method that employs a prime-weighted graph, marking its introduction to cryptography. In their approach, they arbitrarily preferred the number of edges and vertices when constructing the prime-weighted graph. This arbitrariness adds a significant level of unpredictability, making it challenging for outsiders to anticipate chosen vertices or their connections. Consequently, the proposed algorithm serves as an essential tool for ensuring secure communication.

Ajeena and Abdullatif [20] designed a symmetric encryption method that uses a colored bipartite graph as the secret key. The encrypted message, specifically designed for alphabetic characters in the original text, is conveyed to the recipient as a bipartite graph that can be colored. However, this approach cannot encrypt alphanumeric data. Beaula and Venugopal [21] presented a novel symmetric encryption method that uses a shared key to produce encrypted text. This technique uses several computational principles, path graphs, and double-vertex graphs. An approach to symmetric encryption using a triple-vertex path (TVP) graph was presented by Shathir et al. [22] This method sends recipient cipher texts that match the plaintexts in the TVP graph format. By taking advantage of the unique properties of the TVP graph, this approach aims to increase the security of previous encryption techniques.

3. Proposed methodology

3.1 *Encryption algorithm*

This algorithm is used to convert plain text to cipher text. First, we take a message $M = \{m_1, m_2, \ldots, m_n\}$ (plain text) from the user that has to be encrypted. Convert M into decimal values based on ASCII values with modulo 127. Using ASCII the number of the allowed letters chosen is 127. The binary expressions of these numbers are calculated. Let K (Key) be a coloring tripartite graph (CTG) as shown in Figure 1, and let the user can generate the formula.

$$K \equiv (x \cdot first\ color + y \cdot second\ color + z \cdot third\ color)(\mathrm{mod}\ 127). \tag{1}$$

where x, y and z are the numbers of vertices in an independent set of CTG. Each independent set has a unique color. The letters corresponding to the colors are represented in decimal expression based on their ASCII values, which are subsequently converted into binary strings.

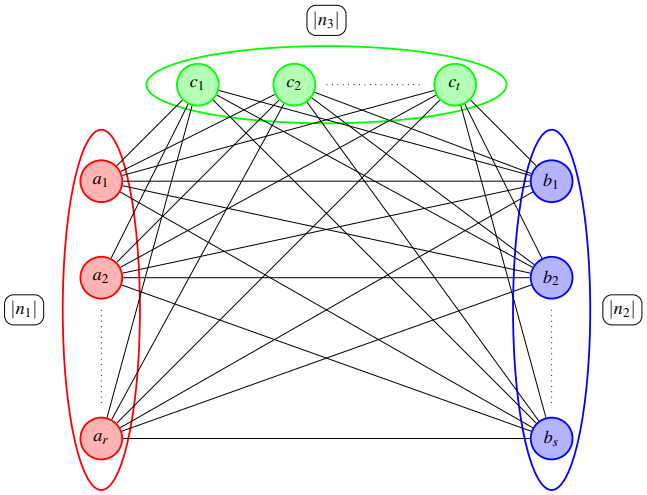

Figure 1. Coloring tripartite graph to generate the shared secret key

Ciphertext C corresponding to message M is generated through the following computation,

$$C \equiv (M+K)(\bmod 2). \tag{2}$$

Specifically,

$$c_i \equiv (m_i+k_i)(\bmod 2),\ i=1,\ 2,\ 3,\ \ldots,\ n. \tag{3}$$

Consequently, the cipher text $C=\{c_1,\ c_2,\ \ldots,\ c_n\}$ is represented as a CTG that is subsequently communicated to the intended recipient, as demonstrated in the accompanying (Figure 2).

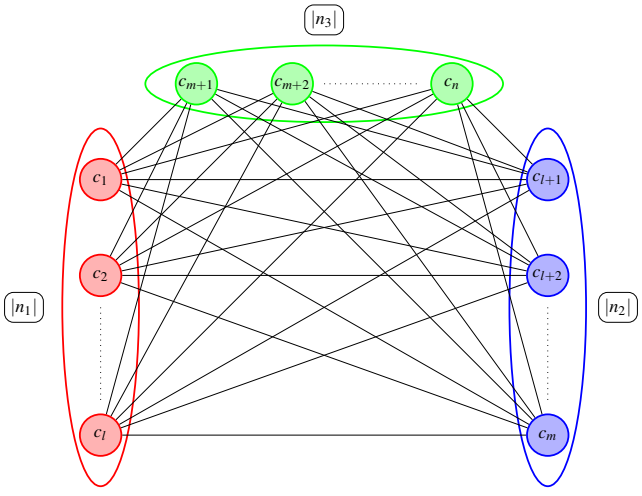

Figure 2. A CTG of a ciphertext

3.2 *Decryption algorithm*

This algorithm is designed to transform ciphertext into plaintext. The recipient receives the ciphertext, referred to as the Coloring Tripartite Graph (CTG). The recipient can decipher the information using colored tripartite graphs. The ciphertext is represented as $C = \{c_1, c_2, \ldots c_n\}$, which is then converted into decimal values based on ASCII encoding followed by conversion into binary expressions of these decimal values. From the CTG, the recipient can derive the secret key K. Given that the CTG employs three distinct colors and the number of vertices in each independent set is denoted as x, y, and z, the secret key is computed using the equation (1). The original plaintext is subsequently calculated using the equation

$$M \equiv (C - K)(\bmod 2) \tag{4}$$

More generally, this can be expressed as

$$m_i \equiv (c_i - k_i)(\bmod 2),\ i = 1,\ 2,\ 3,\ \ldots,\ n. \tag{5}$$

Consequently, the original plaintext is represented as $M = \{m_1, m_2, \ldots m_n\}$. The entire process as shown in the flow chart (Figure 3).

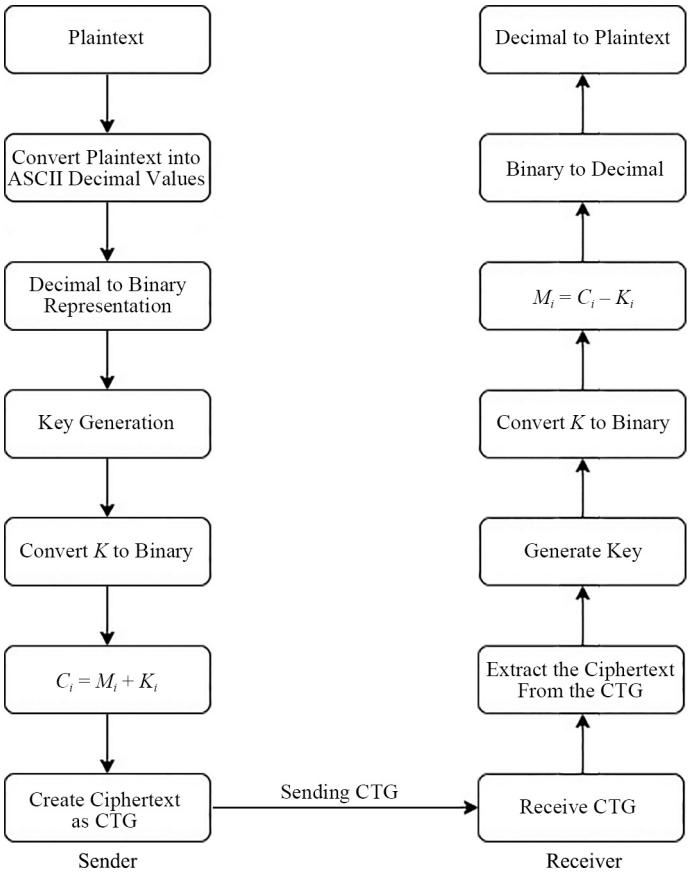

Figure 3. Work flow diagram

Observation 1: $|n_1| = |n_2| = |n_3|$.
If $|n_1| = |n_2| = |n_3| = 3$, then the graph becomes (Figure 4):

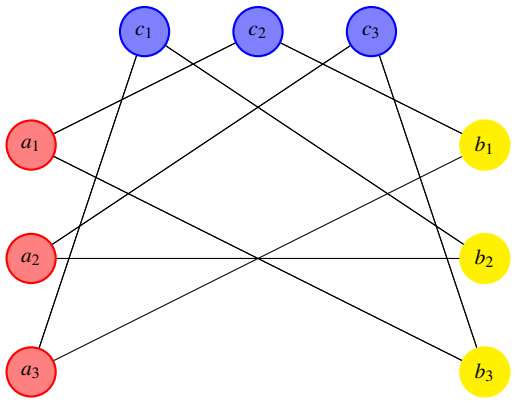

Figure 4. A CTG of a shared secret key

Encryption: Let M be a plaintext from the user that we have to encrypt. For example, let $M = \{C, r, y, p, t, t, e, x, t\}$. The letters of M are converted into numbers by using ASCII values as follows $M = \{67, 114, 121, 112, 116, 116, 101, 120, 116\}$. The numerical values that correspond to the plaintext have the following binary representations $67 \to 1000011$, $114 \to 1110010$, $121 \to 1111001$, $112 \to 1110000$, $116 \to 1110100$, $116 \to 1110100$, $101 \to 1100101$, $120 \to 1111000$, $116 \to 111010$. The chromatic number of the CTG has been determined to be 3. Through a comprehensive analysis of the graph, we identified the secret key by replacing the first color Red, the second color Yellow, and the third color Blue in equation (1) as follows:

$$K \equiv (x \cdot Red + y \cdot Yellow + z \cdot Blue)(\bmod 127)$$
$$\equiv (3 \cdot \{82, 101, 100\} + 3 \cdot \{89, 101, 108, 108, 111, 119\} + 3 \cdot \{66, 108, 117, 101\})(\bmod 127)$$
$$\equiv (\{246, 303, 300\} + \{267, 303, 324, 324, , 333, 357\} + \{198, 324, 351, 303\}(\bmod 127)),$$
$$K \equiv \{76, 41, 86, 119, 79, 103\}(\bmod 127).$$

The binary expressions of the numbers $\{76, 41, 86, 119, 79, 103\}$ are determined by $76 \to 1001100$, $41 \to 0101001$, $86 \to 1010110$, $119 \to 1110111$, $79 \to 1001111$, $103 \to 1100111$. The ciphertext C corresponding to the message M is calculated using equation (3) as follows:

$c_1 \equiv (1000011 + 1001100)(\bmod 2) = 0001111 \to 15 \to SI$
$c_2 \equiv (1110010 + 0101001)(\bmod 2) = 1011011 \to 91 \to [$
$c_3 \equiv (1111001 + 1010110)(\bmod 2) = 0101111 \to 47 \to /$
$c_4 \equiv (1110000 + 1110111)(\bmod 2) = 0000111 \to 7 \to BEL$
$c_5 \equiv (1110100 + 1001111)(\bmod 2) = 0111011 \to 59 \to :$
$c_6 \equiv (1110100 + 1100111)(\bmod 2) = 0010011 \to 19 \to DC3$
$c_7 \equiv (1100101 + 1001100)(\bmod 2) = 0101001 \to 49 \to 1$
$c_8 \equiv (1111000 + 0101001)(\bmod 2) = 1010001 \to 81 \to Q$
$c_9 \equiv (1110100 + 1010110)(\bmod 2) = 0100010 \to 34 \to "$
$\therefore C = \{SI, [, /, BEL, :, DC3, 1, Q, "\}$.

The cipher text is sent as a tripartite coloring graph by the sender to the receiver, as shown in the Figure 5.

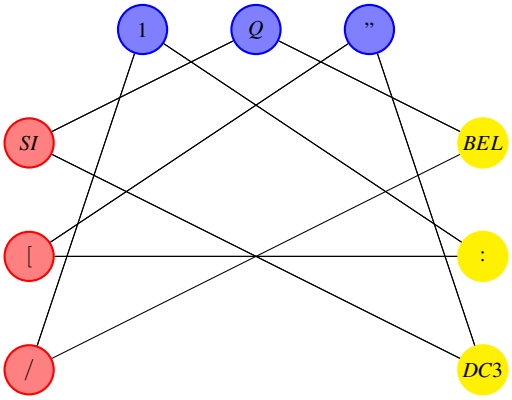

Figure 5. A CTG of a ciphertext

Decryption: The recipient receives the ciphertext shown in the above graph and performs the following steps. $C = \{SI,\ [,\ /\ ,\ BEL,\ :,\ DC3,\ 1,\ Q,"\}$. The alphanumeric numbers in ciphertext C are transformed into numbers according to their ASCII values in the following manner. $SI \to 15$, $[\to 91$, $/ \to 47$, $BEL \to 7$, $:\to 59$, $DC3 \to 19$, $1 \to 49$, $Q \to 81$, $" \to 34$. The binary expressions of these numbers are determined by $15 \to 0001111,\ 91 \to 1011011,\ 47 \to 0101111,\ 7 \to 0000111,\ 59 \to 0111011,\ 19 \to 0010011,\ 49 \to 0101001,\ 81 \to 1010001,\ 34 \to 0100010$. The colored vertices in the CTG are Red, Yellow, and Blue, and the vertices are 3, 3, and 3, respectively. Therefore, the secret key K is determined as:

$$K \equiv (x \cdot Red + y \cdot Yellow + z \cdot Blue)(\bmod 127)$$
$$\equiv (3 \cdot \{82,\ 101,\ 100\} + 3 \cdot \{89,\ 101,\ 108,\ 108,\ 111,\ 119\} + 3 \cdot \{66,\ 108,\ 117,\ 101\})(\bmod 127)$$
$$\equiv (\{246,\ 303,\ 300\} + \{267,\ 303,\ 324,\ 324,\ ,\ 333,\ 357\} + \{198,\ 324,\ 351,\ 303\}(\bmod 127).$$
$$K \equiv \{76,\ 41,\ 86,\ 119,\ 79,\ 103\}(\bmod 127).$$

The binary expressions of the numbers $\{76,\ 41,\ 86,\ 119,\ 79,\ 103\}$ are calculated by $76 \to 1001100,\ 41 \to 0101001,\ 86 \to 1010110,\ 119 \to 1110111,\ 79 \to 1001111,\ 103 \to 1100111$.

The original unencrypted message is obtained by substituting ciphertext c_i and secret key k_i into equation (5) as follows:

$$m_1 \equiv (0001111 - 1001100)(\bmod 2) = 1000011 \to 67 \to C$$
$$m_2 \equiv (1011011 - 0101001)(\bmod 2) = 1110010 \to 114 \to r$$
$$m_3 \equiv (0101111 - 1010110)(\bmod 2) = 1111001 \to 121 \to y$$
$$m_4 \equiv (0000111 - 1110111)(\bmod 2) = 1110000 \to 112 \to p$$
$$m_5 \equiv (0111011 - 1001111)(\bmod 2) = 1110100 \to 116 \to t$$
$$m_6 \equiv (0010011 - 1100111)(\bmod 2) = 1110100 \to 116 \to t$$
$$m_7 \equiv (0101001 - 1001100)(\bmod 2) = 1100101 \to 101 \to e$$
$$m_8 \equiv (1010001 - 0101001)(\bmod 2) = 1111000 \to 120 \to x$$
$$m_9 \equiv (0100010 - 1010110)(\bmod 2) = 1110100 \to 116 \to t.$$

Therefore the original unencrypted message is $\{C,\ r,\ y,\ p,\ t,\ t,\ e,\ x,\ t\} = Crypttext$.

Observation 2: $|n_1| < |n_2| < |n_3|$. If $|n_1| = 1,\ |n_2| = 3,\ |n_3| = 4$, then the graph becomes (Figure 6):

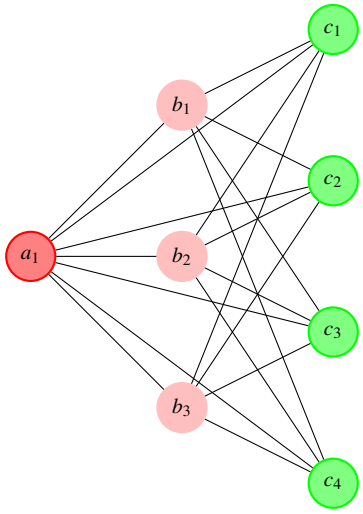

Figure 6. A CTG of a shared secret key

Encryption: Let M be a plaintext from the user that we have to encrypt. For example, let $M = Welcome\# = \{W,\ e,\ l,\ c,\ o,\ m,\ e,\ \#\}$. The letters of M are converted into numbers by using ASCII values as follows $M = \{87,\ 101,\ 108,\ 99,\ 111,\ 109,\ 101,\ 35\}$. The binary expressions of the numbers in the original text are $87 \to 1010111,\ 101 \to 1100101,\ 108 \to 1101100,\ 99 \to 1100011,\ 111 \to 1101111,\ 109 \to 1101101,\ 101 \to 1100101,\ 35 \to 0100011$. The chromatic number of CTG is 3. We determined the secret key from the graph by:

$$\begin{aligned} K &\equiv (x \cdot Red + y \cdot Pink + z \cdot Green)(\bmod 127) \\ &\equiv (1 \cdot \{82,\ 101,\ 100\} + 3 \cdot \{80,\ 105,\ 110,\ 107\} + 4 \cdot \{71,\ 114,\ 101,\ 101,\ 110\})(\bmod 127) \\ &\equiv (\{82,\ 101,\ 100\} + \{240,\ 315,\ 330,\ 321\} + \{284,\ 456,\ 404,\ 404,\ 440\}(\bmod 127) \\ &\equiv \{606,\ 872,\ 834,\ 725,\ 440\}(\bmod 127), \\ K &\equiv \{98,\ 110,\ 72,\ 90,\ 59\}(\bmod 127). \end{aligned}$$

The binary expressions of the numbers $\{98, 110, 72, 90, 59\}$ are determined by $98 \to 1100010,\ 110 \to 1101110,\ 72 \to 1001000,\ 90 \to 1011010,\ 59 \to 0111011$. The ciphertext C corresponding to message M is calculated using equation (3) as follows:

$$\begin{aligned} c_1 &\equiv (1010111 + 1100010)(\bmod 2) = 0110101 \to 53 \to 5 \\ c_2 &\equiv (1100101 + 1101110)(\bmod 2) = 0001011 \to 11 \to VT \\ c_3 &\equiv (1101100 + 1001000)(\bmod 2) = 0100100 \to 36 \to \$ \\ c_4 &\equiv (1100011 + 1011010)(\bmod 2) = 0111001 \to 57 \to 9 \\ c_5 &\equiv (1101111 + 0111011)(\bmod 2) = 1010100 \to 84 \to T \\ c_6 &\equiv (1101101 + 1100010)(\bmod 2) = 0001111 \to 15 \to SI \\ c_7 &\equiv (1100101 + 1101110)(\bmod 2) = 0001011 \to 11 \to VT \\ c_8 &\equiv (0100011 + 1001000)(\bmod 2) = 1101011 \to 107 \to k \\ \therefore C &= \{5,\ VT,\ \$,\ 9,\ T,\ SI,\ VT,\ k\}. \end{aligned}$$

The cipher text is sent as a coloring tripartite graph by the sender to the receiver, as shown in the Figure 7.

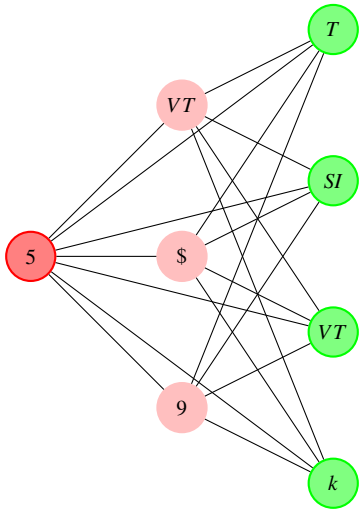

Figure 7. A CTG of a ciphertext

Decryption: The recipient receives the ciphertext shown in the above graph and performs the following steps. $C = \{5,\ VT,\ \$,\ 9,\ T,\ SI,\ VT,\ k\}$. The alphanumeric numbers in ciphertext C are transformed into numbers according to their ASCII values in the following manner. $5 \to 53,\ VT \to 11,\ \$ \to 36,\ 9 \to 57,\ T \to 84,\ SI \to 15,\ VT \to 11,\ K \to 107$. The binary expressions of these numbers are determined by $53 \to 0110101,\ 11 \to 0001011,\ 36 \to 100100,\ 57 \to 0111001,\ 84 \to 1010100,\ 15 \to 0001111,\ 11 \to 0001011,\ 107 \to 1101011$. The colored vertices in the CTG are Red, Pink, and Green, and the number of vertices is 1, 3 and 4, respectively. Therefore, the secret key is determined by:

$K \equiv (x \cdot Red + y \cdot Pink + z \cdot Green)(\bmod 127)$

$\equiv (1 \cdot \{82,\ 101,\ 100\} + 3 \cdot \{80,\ 105,\ 110,\ 107\} + 4 \cdot \{71,\ 114,\ 101,\ 101,\ 110\})(\bmod 127)$

$\equiv (\{82,\ 101,\ 100\} + \{240,\ 315,\ 330,\ 321\} + \{284,\ 456,\ 404,\ 404,\ 440\}(\bmod 127)$

$\equiv \{606,\ 872,\ 834,\ 725,\ 440\}(\bmod 127)$,

$K \equiv \{98,\ 110,\ 72,\ 90,\ 59\}(\bmod 127)$.

The binary expressions of the numbers $\{98, 110, 72, 90, 59\}$ are calculated by

$98 \to 1100010,\ 110 \to 1101110,\ 72 \to 1001000,\ 90 \to 1011010,\ 59 \to 0111011$.

The original unencrypted message is obtained by substituting ciphertext c_i and secret key k_i into equation (5) as follows:

$m_1 \equiv (0110101 - 1100010)(\bmod 2) = 1010111 \to 87 \to W$

$m_2 \equiv (0001011 - 1101110)(\bmod 2) = 1100101 \to 101 \to e$

$m_3 \equiv (0100100 - 1001000)(\bmod 2) = 1101100 \to 108 \to l$

$m_4 \equiv (0111001 - 1011010)(\bmod 2) = 1100011 \to 99 \to c$

$m_5 \equiv (1010100 - 0111011)(\bmod 2) = 1101111 \to 111 \to o$

$m_6 \equiv (0001111 - 1100010)(\bmod 2) = 1101101 \to 109 \to$

$m_7 \equiv (0001011 - 1101110)(\bmod 2) = 1100101 \to 101 \to e$

$m_8 \equiv (1101011 - 1001000)(\bmod 2) = 100011 \to 35 \to \#$.

Therefore, the original unencrypted message is $\{W,\ e,\ l,\ c,\ o,\ m,\ e,\ \#\} = Welcome\#$.

Observation 3: $|n_1| = |n_2| > |n_3|$.

If $|n_1| = |n_2| = 4,\ |n_3| = 2$, then the graph becomes (Figure 8):

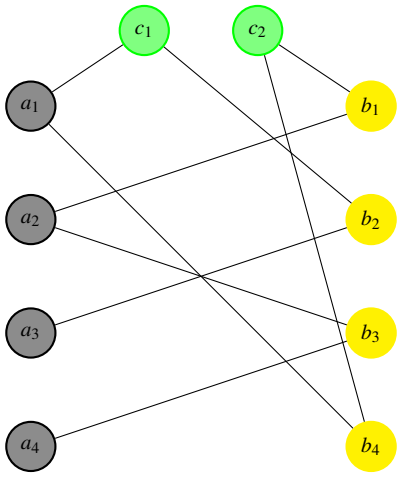

Figure 8. A CTG of a shared secret key

Encryption Let M be a plaintext from the user that we have to encrypt. For example, let $M = Encryption = \{E,\ n,\ c,\ r,\ y,\ p,\ t,\ i,\ o,\ n\}$. The letters of M are converted into numbers by using ASCII values as follows. $M = \{69,\ 110,\ 99,\ 114,\ 121,\ 112,\ 116,\ 105,\ 111,\ 110\}$. The binary expressions of the numbers in the original text are $69 \to 1000101$, $110 \to 1101110$, $99 \to 1100011$, $114 \to 1110010$, $121 \to 1111001$, $112 \to 1110000$, $116 \to 1110100$, $105 \to 1101001$, $111 \to 1101111$, $110 \to 1101110$. The chromatic number of the CTG is 3. We determined the secret key from the graph by:

$$\begin{aligned} K &\equiv (x \cdot Black + y \cdot Yellow + z \cdot Green) (\bmod 127) \\ &\equiv (4 \cdot \{66,\ 108,\ 97,\ 99,\ 107\} + 4 \cdot \{89,\ 101,\ 108,\ 108,\ 111,\ 119\} + 2 \cdot \{71,\ 114,\ 101,\ 101,\ 110\}) (\bmod 127) \\ &\equiv (\{264,\ 432,\ 388,\ 396,\ 428\} + \{356,\ 404,\ 432,\ 432,\ 444,\ 476\} + \{142,\ 228,\ 202,\ 202,\ 220\} (\bmod 127) \\ &\equiv \{762,\ 1064,\ 1022,\ 1030,\ 1092,\ 476\} (\bmod 127), \end{aligned}$$

$K \equiv \{0,\ 48,\ 6,\ 14,\ 76,\ 95\} (\bmod 127)$.

The binary expressions of the numbers $\{0, 48, 6, 14, 76, 95\}$ are calculated by $0 \to 0000000$, $48 \to 0110000$, $6 \to 0000110$, $14 \to 0001110$, $76 \to 1001100$, $95 \to 1011111$. The ciphertext C corresponding to message M is calculated using equation (3) as follows:

$$\begin{aligned} c_1 &\equiv (1000101 + 0000000) (\bmod 2) = 1000101 \to 69 \to E \\ c_2 &\equiv (1101110 + 110000) (\bmod 2) = 1011110 \to 94 \to \hat{} \\ c_3 &\equiv (1100011 + 0000110) (\bmod 2) = 1100101 \to 101 \to e \\ c_4 &\equiv (1110010 + 0001110) (\bmod 2) = 1111100 \to 124 \to | \\ c_5 &\equiv (1111001 + 1001100) (\bmod 2) = 0110101 \to 53 \to 5 \\ c_6 &\equiv (1110000 + 1011111) (\bmod 2) = 0101111 \to 47 \to / \\ c_7 &\equiv (1110100 + 0000000) (\bmod 2) = 1110100 \to 116 \to t \\ c_8 &\equiv (1101001 + 0110000) (\bmod 2) = 1011001 \to 89 \to Y \\ c_9 &\equiv (1101111 + 0000110) (\bmod 2) = 1101001 \to 105 \to i \\ c_{10} &\equiv (1101110 + 0001110) (\bmod 2) = 1011001 \to 96 \to ' \end{aligned}$$

$\therefore C = \{E, \hat{}, e, |, 5, /, t, Y, i, '\}$.

The cipher text is sent as a CTG by the sender into the receiver, as shown in the Figure 9.

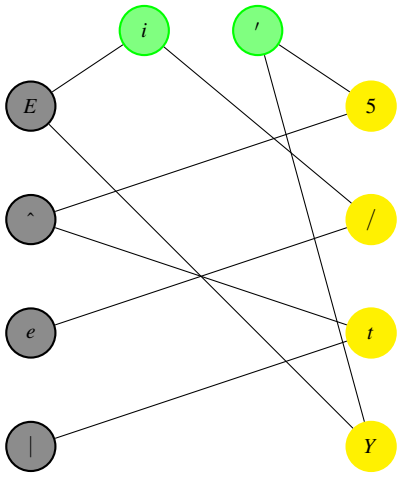

Figure 9. A CTG of a ciphertext

Decryption: The recipient receives the ciphertext shown in the above graph and performs the following steps. $C = \{E, \hat{}, e, |, 5, /, t, Y, i, '\}$. The alphanumeric numbers in ciphertext C are transformed into numbers according to their ASCII values in the following manner. $E \to 69, \hat{} \to 94, e \to 101, | \to 124, 5 \to 53, / \to 47, t \to 116, Y \to 89, i \to 105, ' \to 96$. The binary expressions of these numbers are determined by $69 \to 1000101$, $94 \to 1011110$, $101 \to 1100101$, $124 \to 1111100$, $53 \to 0110101$, $47 \to 0101111$, $116 \to 1110100$, $89 \to 1011001$, $105 \to 1101001$, $96 \to 1100000$. The colored vertices in the CTG are Black, Yellow, and Green, and the number of vertices are 4, 4 and 2, respectively. Therefore, the secret key is determined by:

$$\begin{aligned} K &\equiv (x \cdot Black + y \cdot Yellow + z \cdot Green) (\bmod 127) \\ &\equiv (4 \cdot \{66, 108, 97, 99, 107\} + 4 \cdot \{89, 101, 108, 108, 111, 119\} + 2 \cdot \{71, 114, 101, 101, 110\}) (\bmod 127) \\ &\equiv (\{264, 432, 388, 396, 428\} + \{356, 404, 432, 432, 444, 476\} + \{142, 228, 202, 202, 220\} (\bmod 127) \\ &\equiv \{762, 1064, 1022, 1030, 1092, 476\} (\bmod 127), \\ K &\equiv \{0, 48, 6, 14, 76, 95\} (\bmod 127). \end{aligned}$$

The binary expressions of the numbers $\{0, 48, 6, 14, 76, 95\}$ are calculated by $0 \to 0000000$, $48 \to 0110000$, $6 \to 0000110$, $14 \to 0001110$, $76 \to 1001100$, $95 \to 1011111$.

The original unencrypted message is obtained by substituting ciphertext c_i and secret key k_i into equation (5) as follows:

$$\begin{aligned} m_1 &\equiv (1000101 - 0000000) (\bmod 2) = 1000101 \to 69 \to E \\ m_2 &\equiv (1011110 - 0110000) (\bmod 2) = 1101110 \to 110 \to n \\ m_3 &\equiv (1100101 - 0000110) (\bmod 2) = 1100011 \to 99 \to c \\ m_4 &\equiv (1111100 - 0001110) (\bmod 2) = 1110010 \to 114 \to r \\ m_5 &\equiv (0110101 - 1001100) (\bmod 2) = 1111001 \to 121 \to y \\ m_6 &\equiv (0101111 - 1011111) (\bmod 2) = 1110000 \to 112 \to p \\ m_7 &\equiv (1110100 - 0000000) (\bmod 2) = 1110100 \to 116 \to t \\ m_8 &\equiv (1011001 - 0110000) (\bmod 2) = 1101001 \to 105 \to i \\ m_9 &\equiv (1101001 - 0000110) (\bmod 2) = 1101111 \to 111 \to o \\ m_{10} &\equiv (1100000 - 0001110) (\bmod 2) = 1101110 \to 110 \to n. \end{aligned}$$

Therefore, the original unencrypted message is $\{E, n, c, r, y, p, t, i, o, n\} = Encryption$.

Observation 4: $|n_1| = |n_2| < |n_3|$.

If $|n_1| = |n_2| = 2$, $|n_3| = 4$, then the graph becomes (Figure 10):

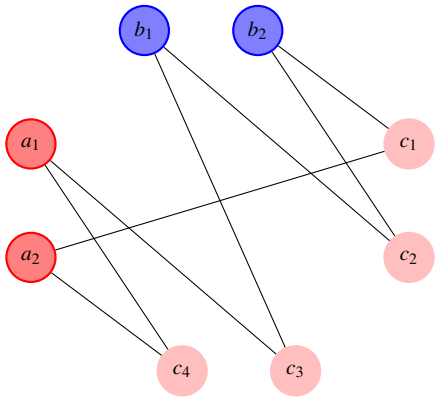

Figure 10. A CTG of the shared secret key

Encryption: Let M be a plaintext from the user that we have to encrypt. For example, let $M = Crypt\ 100 = \{C,\ r,\ y,\ p,\ t,\ 1,\ 0,\ 0\}$. The letters of M are transformed into numerical values using their ASCII representations in the following manner. $M = \{67,\ 114,\ 121,\ 112,\ 116,\ 49,\ 48,\ 48\}$. The binary expressions of the numbers in the plaintext are $67 \to 1000011,\ 114 \to 1110010,\ 121 \to 1111001,\ 112 \to 1110000,\ 116 \to 1110100,\ 49 \to 110001,\ 48 \to 110000,\ 48 \to 110000$. The chromatic number of the CTG is 3. Using the graph, we identified the secret key by:

$$\begin{aligned} K &\equiv (x \cdot Red + y \cdot Blue + z \cdot Pink)(\bmod 127) \\ &\equiv (2 \cdot \{82,\ 101,\ 100\} + 2 \cdot \{66,\ 108,\ 117,\ 101\} + 4 \cdot \{80,\ 105,\ 110,\ 107\})(\bmod 127) \\ &\equiv (\{164,\ 202,\ 200\} + \{132,\ 216,\ 234,\ 202\} + \{320,\ 420,\ 440,\ 428\}(\bmod 127) \\ &\equiv \{616,\ 838,\ 874,\ 630\}(\bmod 127), \\ K &\equiv \{108,\ 76,\ 112,\ 122\}(\bmod 127). \end{aligned}$$

The binary expressions of the numbers $\{108, 76, 112, 122\}$ are calculated by $108 \to 1101100,\ 76 \to 1001100,\ 112 \to 1110000,\ 122 \to 1111010$.

The ciphertext C corresponding to message M is calculated using equation (3) as follows:

$$\begin{aligned} c_1 &\equiv (1000011 + 1101100)(\bmod 2) = 0101111 \to 47 \to / \\ c_2 &\equiv (1110010 + 1001100)(\bmod 2) = 0111110 \to 62 \to > \\ c_3 &\equiv (1111001 + 1110000)(\bmod 2) = 0001001 \to 9 \to TAB \\ c_4 &\equiv (1110000 + 1111010)(\bmod 2) = 0001010 \to 10 \to LF \\ c_5 &\equiv (1110100 + 1101100)(\bmod 2) = 0011000 \to 24 \to CAN \\ c_6 &\equiv (0110001 + 1001100)(\bmod 2) = 1111101 \to 125 \to \} \\ c_7 &\equiv (0110000 + 1110000)(\bmod 2) = 1000000 \to 64 \to @ \\ c_8 &\equiv (110000 + 1111010)(\bmod 2) = 1001010 \to 74 \to J \end{aligned}$$

$\therefore C = \{/,\ >,\ TAB,\ LF,\ CAN,\ \},\ @,\ J\}$.

The cipher text is sent as a coloring tripartite graph by the sender into the receiver, as shown in the Figure 11.

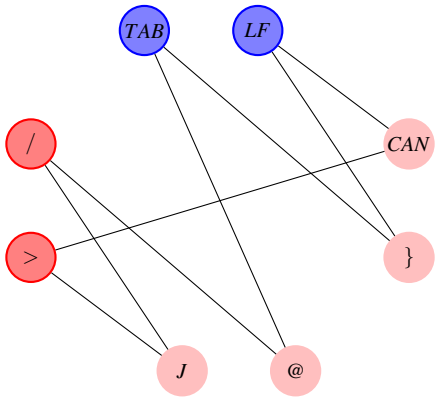

Figure 11. A CTG of a ciphertext

Decryption: The recipient receives the ciphertext shown in the above graph and performs the following steps. $C = \{/,\ >,\ TAB,\ LF,\ CAN,\ \},\ @,\ J\}$. The alphanumeric numbers in ciphertext C are transformed into numbers according to their ASCII values in the following manner. $/ \to 47,\ > \to 62,\ TAB \to 9,\ LF \to 10,\ CAN \to 24,\ \} \to 125,\ @ \to 64,\ J \to 74$. The binary expressions of these numbers are determined by $47 \to 0101111,\ 62 \to 0111110,\ 9 \to 0001001,\ 10 \to 0001010,\ 24 \to 0011000,\ 125 \to 1111101,\ 64 \to 1000000,\ 74 \to 1001010$. The colored vertices in the CTG are Red, Blue, and Pink, and the number of vertices are 2, 2, and 4, respectively. Consequently, the secret key is determined as

$$\begin{aligned} K &\equiv (x \cdot Red + y \cdot Blue + z \cdot Pink)(\bmod 127) \\ &\equiv (2 \cdot \{82,\ 101,\ 100\} + 2 \cdot \{66,\ 108,\ 117,\ 101\} + 4 \cdot \{80,\ 105,\ 110,\ 107\})(\bmod 127) \\ &\equiv (\{164,\ 202,\ 200\} + \{132,\ 216,\ 234,\ 202\} + \{320,\ 420,\ 440,\ 428\}(\bmod 127) \\ &\equiv \{616,\ 838,\ 874,\ 630\}(\bmod 127), \\ K &\equiv \{108,\ 76,\ 112,\ 122\}(\bmod 127). \end{aligned}$$

The binary expressions of the numbers $\{108, 76, 112, 122\}$ are calculated by $108 \to 1101100,\ 76 \to 1001100,\ 112 \to 1110000,\ 122 \to 1111010$.

The original unencrypted message is obtained by substituting ciphertext c_i and secret key k_i into equation (5) as follows:

$$\begin{aligned} m_1 &\equiv (0101111 - 1101100)(\bmod 2) = 1000011 \to 67 \to C \\ m_2 &\equiv (0111110 - 1001100)(\bmod 2) = 1110010 \to 114 \to r \\ m_3 &\equiv (0001001 - 1110000)(\bmod 2) = 1111001 \to 121 \to y \\ m_4 &\equiv (0001010 - 1111010)(\bmod 2) = 1110000 \to 112 \to p \\ m_5 &\equiv (0011000 - 1101100)(\bmod 2) = 1110100 \to 116 \to t \\ m_6 &\equiv (1111101 - 1001100)(\bmod 2) = 0110001 \to 49 \to 1 \\ m_7 &\equiv (1000000 - 1110000)(\bmod 2) = 0110000 \to 48 \to 0 \\ m_8 &\equiv (1001010 - 1111010)(\bmod 2) = 0110000 \to 48 \to 0. \end{aligned}$$

Therefore the original unencrypted message is $\{C,\ r,\ y,\ p,\ t,\ 1,\ 0,\ 0\} = Crypt100$.

Observation 5: $|n_1| < |n_2| < |n_3|$. where $n_1,\ n_2,\ n_3$ are prime numbers.

If $|n_1| = 2,\ |n_2| = 3,\ |n_3| = 5$, then the graph becomes (Figure 12):

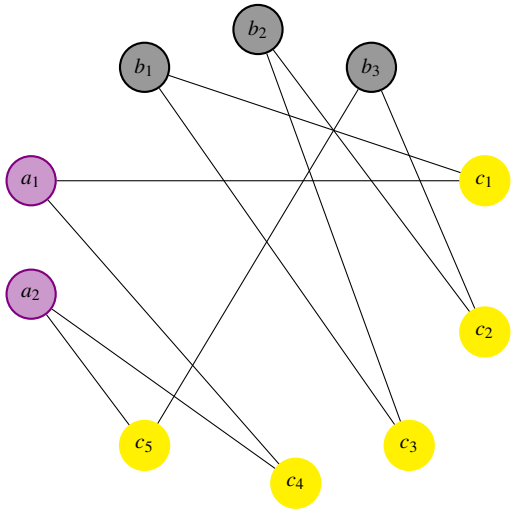

Figure 12. A CTG of a shared secret key

Encryption: Let M be a plaintext from the user that we have to encrypt. For example, let $M = Ciphertext = \{C,\ i,\ p,\ h,\ e,\ r,\ t,\ e,\ x,\ t\}$. The letters of M are transformed into numerical values using their ASCII representations in the following manner. $M = \{67,\ 105,\ 112,\ 104,\ 101,\ 114,\ 116,\ 101,\ 120,\ 116\}$. The binary expressions of the numbers in the plaintext are $67 \to 1000011,\ 105 \to 1101001,\ 112 \to 1110000,\ 104 \to 1101000,\ 101 \to 1100101,\ 114 \to 1110010,\ 116 \to 110100,\ 101 \to 1100101,\ 120 \to 1111000,\ 116 \to 1110100$. The chromatic number of the CTG is 3. From the graph, we identified the secret key by:

$$\begin{aligned} K &\equiv (x \cdot Violet + y \cdot Black + z \cdot Yellow) (\bmod 127) \\ &\equiv (2 \cdot \{86,\ 105,\ 111,\ 108,\ 101,\ 116\} + 3 \cdot \{66,\ 108,\ 97,\ 99,\ 107\} + 5 \cdot \{89,\ 101,\ 108,\ 108,\ 111,\ 119\}) (\bmod 127) \\ &\equiv (\{172,\ 210,\ 222,\ 216,\ 202,\ 232\} + \{198,\ 324,\ 291,\ 297,\ 321\} + \{445,\ 505,\ 540,\ 540,\ 555,\ 595\} (\bmod 127) \\ &\equiv \{815,\ 1039,\ 1054,\ 1053,\ 1078,\ 827\} (\bmod 127), \\ K &\equiv \{53,\ 23,\ 38,\ 37,\ 62,\ 65\} (\bmod 127). \end{aligned}$$

The binary expressions of the numbers $\{53, 23, 38, 37, 62, 65\}$ are determined by $53 \to 110101,\ 23 \to 010111,\ 38 \to 100110,\ 37 \to 100101,\ 62 \to 111110,\ 65 \to 1000001$. The ciphertext C corresponding to message M is calculated using equation (3) as follows:

$$\begin{aligned} c_1 &\equiv (1000011 + 0110101) (\bmod 2) = 1110110 \to 118 \to v \\ c_2 &\equiv (1101001 + 0010111) (\bmod 2) = 1111110 \to 126 \to \sim \\ c_3 &\equiv (1110000 + 0100110) (\bmod 2) = 1010110 \to 86 \to V \\ c_4 &\equiv (1101000 + 0100101) (\bmod 2) = 1001101 \to 77 \to M \\ c_5 &\equiv (1100101 + 111110) (\bmod 2) = 1011011 \to 91 \to [\\ c_6 &\equiv (1110010 + 1000001) (\bmod 2) = 0110011 \to 51 \to 3 \\ c_7 &\equiv (1110100 + 0110101) (\bmod 2) = 1000001 \to 65 \to A \\ c_8 &\equiv (1100101 + 0010111) (\bmod 2) = 1110010 \to 114 \to r \\ c_9 &\equiv (1111000 + 0100110) (\bmod 2) = 1011110 \to 94 \to \hat{} \\ c_{10} &\equiv (1110100 + 0100101) (\bmod 2) = 1010001 \to 81 \to Q \end{aligned}$$

$\therefore C = \{v,\ \sim,\ V,\ M,\ [,\ 3,\ A,\ r, \hat{},\ Q\}$.

The ciphertext is sent as a coloring tripartite graph by the sender into the receiver, as shown in the Figure 13.

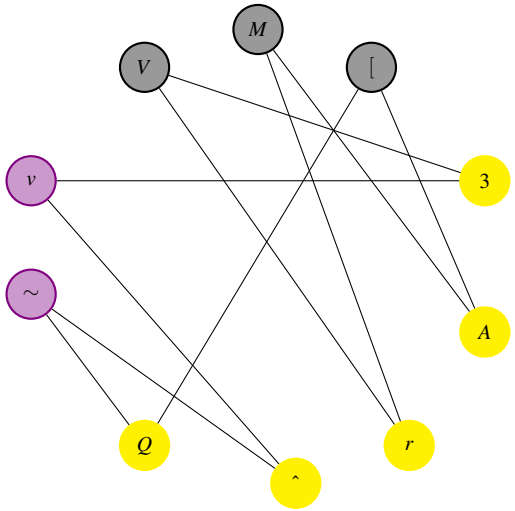

Figure 13. A CTG of a ciphertext

Decryption: The recipient receives the ciphertext shown in the above graph and performs the following steps. $C = \{v,\ \sim,\ V,\ M,\ [,\ 3,\ A,\ r, \hat{},\ Q\}$. The alphanumeric numbers in ciphertext C are transformed into numbers according to their ASCII values in the following manner. $v \to 118,\ \sim \to 126,\ V \to 86,\ M \to 77,\ [\to 91,\ 3 \to 51,\ A \to 65,\ r \to 114, \hat{} \to 94,\ Q \to 81$. The binary expressions of these numbers are determined by: $118 \to 1110110,\ 126 \to 1111110,\ 86 \to 1010110,\ 77 \to 1001101,\ 91 \to 1011011,\ 51 \to 0110011,\ 65 \to 1000001,\ 114 \to 1110010,\ 94 \to 1011110,\ 81 \to 1010001$. The colored vertices in the CTG are Violet, Black, and Yellow, and the number of vertices is 2, 3, and 5, respectively. Therefore the secret key K is determined by

$$\begin{aligned} K &\equiv (x \cdot Violet + y \cdot Black + z \cdot Yellow) (\bmod 127) \\ &\equiv (2 \cdot \{86,\ 105,\ 111,\ 108,\ 101,\ 116\} + 3 \cdot \{66,\ 108,\ 97,\ 99,\ 107\} + 5 \cdot \{89,\ 101,\ 108,\ 108,\ 111,\ 119\}) (\bmod 127) \\ &\equiv (\{172,\ 210,\ 222,\ 216,\ 202,\ 232\} + \{198,\ 324,\ 291,\ 297,\ 321\} + \{445,\ 505,\ 540,\ 540,\ 555,\ 595\} (\bmod 127) \\ &\equiv \{815,\ 1039,\ 1054,\ 1053,\ 1078,\ 827\} (\bmod 127), \end{aligned}$$

$K \equiv \{53,\ 23,\ 38,\ 37,\ 62,\ 65\} (\bmod 127)$.

The binary expressions of the numbers $\{53, 23, 38, 37, 62, 65\}$ are calculated by $53 \to 110101,\ 23 \to 010111,\ 38 \to 100110,\ 37 \to 100101,\ 62 \to 111110,\ 65 \to 1000001$.

The original unencrypted message is obtained by substituting ciphertext c_i and secret key k_i into equation (5) as follows:

$$\begin{aligned} m_1 &\equiv (1110110 - 0110101) (\bmod 2) = 1000011 \to 67 \to C \\ m_2 &\equiv (1111110 - 0010111) (\bmod 2) = 1101001 \to 105 \to i \\ m_3 &\equiv (1010110 - 0100110) (\bmod 2) = 1110000 \to 112 \to p \\ m_4 &\equiv (1001101 - 0100101) (\bmod 2) = 1101000 \to 104 \to h \\ m_5 &\equiv (1011011 - 0111110) (\bmod 2) = 1100101 \to 101 \to e \\ m_6 &\equiv (0110011 - 1000001) (\bmod 2) = 1110010 \to 114 \to r \\ m_7 &\equiv (1000001 - 0110101) (\bmod 2) = 1110100 \to 116 \to t \\ m_8 &\equiv (1110010 - 0010111) (\bmod 2) = 1100101 \to 101 \to e \\ m_9 &\equiv (1011110 - 0100110) (\bmod 2) = 1111000 \to 120 \to x \\ m_{10} &\equiv (1010001 - 0100101) (\bmod 2) = 1110100 \to 116 \to t. \end{aligned}$$

Therefore the original unencrypted message is $\{C,\ i,\ p,\ h,\ e,\ r,\ t,\ e,\ x,\ t\} = Ciphertext$.

4. Security analysis

A reliable approach for generating a shared secret key should be part of the data security plan. Deciphering the shared secret key has proven to be challenging for those attempting to decipher it. Therefore, a greater variety of possibilities must be considered. The total probability can be calculated as

$$nC_r = \frac{n!}{r!(n-r)!}$$

$$127C_a + 127C_b + 127C_c = \frac{127!}{a!(127-a)!} + \frac{127!}{b!(127-b)!} + \frac{127!}{c!(127-c)!}$$

where a, b and c are the numbers of letters in the color vertices of the CTG. Based on the observation (1) example $n = 127$, $n_1 = n_2 = n_3 = 3$, the total probabilities are

$$127C_3 + 127C_3 + 127C_3 = \frac{127!}{3!(127-3)!} + \frac{127!}{3!(127-3)!} + \frac{127!}{3!(127-3)!} = 333375 + 333375 + 333375 = 1000125.$$

Only one of the 1000125 possible variants of the shared secret key that the individuals working in this case need to produce will be accurate. Consequently, the vast array of potential solutions strengthens the security of the decryption of the original plaintext.

5. Discussion

This study investigated the application of random coloring techniques in tripartite graphs, integrating constraints to enhance computational efficiency. The results are promising for tripartite graph cases; however, extending this approach to larger n-partite graphs introduces considerable computational difficulties. As the size of the graph and the number of partitions grow, the challenge of finding a valid coloring solution increases exponentially. This heightened complexity serves as a significant obstacle for adversaries attempting to decipher encrypted communications, as the decoding process is closely linked to the successful determination of the appropriate coloring. To address these scalability issues, future investigations should focus on developing novel graph coloring algorithms tailored specifically for n-partite graph configurations. Alternatively, improving existing, well-established graph coloring algorithms to enhance their performance in n-partite graphs could yield valuable insights. In summary, these advancements have the potential to greatly enhance the security of data storage systems. By introducing a substantial degree of computational complexity, this strategy effectively discourages unauthorized access to sensitive data, thereby strengthening the overall security framework of the system.

6. Conclusion

This paper introduces a novel data encryption algorithm that improves data security and privacy by integrating ASCII values with a novel color-based graph encoding scheme for secret key generation. While previous research has explored the use of ASCII values in encryption, this work distinguishes itself by uniquely combining ASCII values with graph-theoretic concepts involving color assignments. Recognizing the vulnerabilities of data transmission over unreliable networks to exploitation and hacking, this research proposes a unique approach based on a shared secret key represented as a colored tripartite graph (CTG). The original plaintext is converted into ciphertext before being sent

to the intended recipient. By employing this ASCII-based encryption system with CTG, data transmission security is significantly improved. The application of graph theory introduces a new level of complexity, making it more difficult for unauthorized users to break encryption and access the data. A comprehensive security analysis and clear experimental results with small parameter values support the effectiveness of this approach. The CTG symmetric encryption method demonstrates enhanced security compared to previous graph-based approaches. Hackers face significantly increased challenges, requiring them to generate 1,000,125 sequences of the shared secret keys, of which only one is valid, to recover the original plaintext. This method incorporates randomness by allowing the sender to utilize numerous random colors in the shared secret key generation process. As hackers lack knowledge of these color choices, it significantly hinders their ability to compromise the encryption scheme. This technology provides a valuable contribution to secure cryptographic communication. While our current research has yielded promising results, future work will focus on addressing the computational complexity associated with coloring larger n-partite graphs for practical cryptographic applications. Additionally, we plan to explore potential applications of this algorithm in various domains beyond traditional cryptographic communication.

Conflict of interest

The authors declare no competing financial interest.

References

[1] Sanghavi P, Mehta K, Soni S. Network security. *International Journal of Scientific and Research Publications*. 2013; 3(8): 1-5.

[2] Dowd PW, McHenry JT. Network security: It's time to take it seriously. *Computer*. 1998; 31(9): 24-28. Available from: https://doi.org/10.1109/2.708446.

[3] Stallings W. *Cryptography and Network Security*. 5th ed. New Delhi: Pearson Education India; 2011.

[4] Sasikumar K, Sivakumar N. Comprehensive review and analysis of cryptography techniques in cloud computing. *IEEE Access*. 2024; 12: 52325-52351. Available from: https://doi.org/10.1109/ACCESS.2024.3385449.

[5] Bekkaoui K, Ziti S, Omary F. Data security: A new symmetric cryptosystem based on graph theory. *International Journal of Advanced Computer Science and Applications*. 2021; 12(9): 742-750. Available from: https://doi.org/10.14569/IJACSA.2021.0120982.

[6] Gross J, Yellen J, Anderson M. *Graph Theory and Its Applications*. 3rd ed. USA: Chapman and Hall/CRC; 2018.

[7] *Wikipedia. Multipartite graph*. Available from: https://en.wikipedia.org/wiki/Multipartite_graph [Accessed 5th July 2024].

[8] Ni B, Qazi R, Rehman SU, Farid G. Some graph based encryption schemes. *Journal of Mathematics*. 2021; 2021(1): 6614172. Available from: https://doi.org/10.1155/2021/6614172.

[9] Mathur A. A research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms. *International Journal on Computer Science and Engineering*. 2012; 4(9): 1650-1657.

[10] Khalaf AM, Abd El-karim MS, Hamed HFA. A triple hill cipher algorithm proposed to increase the security of encrypted binary data and its implementation using FPGA. In: *Proceedings of the 18th International Conference on Advanced Communication Technology*. PyeongChang, Korea (South): IEEE; 2016. Available from: https://doi.org/10.1109/ICACT.2016.7423615.

[11] Kumari M, Kirubanad VB. Data encryption and decryption using graph plotting. *International Journal of Civil Engineering and Technology*. 2018; 9(2): 36-46.

[12] Naik M, Tungare P, Kamble P, Sabnis S. Color cryptography using substitution method. *International Research Journal of Engineering and Technology*. 2016; 3(3): 941-944.

[13] Sensarma D, Sen Sarma S. Application of graphs in security. *International Journal of Innovative Technology and Exploring Engineering*. 2019; 8(10): 2273-2279.

[14] Yamuna M, Karthika K. Data transfer using bipartite graphs. *International Journal of Advance Research In Science And Engineering*. 2015; 4(2): 128-131.

[15] Kedia P, Agrawal S. Encryption using Venn diagrams and graph. *International Journal of Advanced Computer Technology*. 2015; 4(1): 94-99.

[16] Selvakumar R, Gupta N. Fundamental circuits and cut-sets used in cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*. 2012; 15(4-5): 287-301. Available from: https://doi.org/10.1080/09720529.2012.10698381.

[17] Kumar D, Krishnaa A. Balanced bipartite trees in cryptography. *Indian Journal of Scientific Research*. 2022; 12(2): 35-40. Available from: https://doi.org/10.32606/IJSR.V12.I2.00005.

[18] Kaur G, Tripathi N. Applying graph theory to secure data by cryptography. *International Journal of Linguistics and Computational Applications*. 2021; 8(1): 1-3.

[19] Agarwal S, Uniyal AS. Prime weighted graph in cryptographic system for secure communication. *International Journal of Pure and Applied Mathematics*. 2015; 105(3): 325-338. Available from: https://doi.org/10.12732/ijpam.v105i3.1.

[20] Ajeena RKK, Abdullatif FA. New version of symmetric encryption scheme using the coloring bipartite graph. In: *2023 Fifth International Conference on Electrical, Computer and Communication Technologies*. Erode, India: IEEE; 2023. Available from: https://doi.org/10.1109/ICECCT56650.2023.10179637.

[21] Venugopal P. Encryption using double vertex graph and matrices. *Solid State Technology*. 2021; 64(2): 2486-2493.

[22] Shathir MK, Ajeena RKK, Arif GE. More secure on the symmetric encryption schemes based on triple vertex path graph. *Journal of Discrete Mathematical Sciences and Cryptography*. 2023; 26(4): 1175-1182. Available from: https://doi.org/10.47974/JDMSC-1564.