Hindawi
Journal of Mathematics
Volume 2021, Article ID 6614172, 8 pages
https://doi.org/10.1155/2021/6614172

Research Article

Some Graph-Based Encryption Schemes

Baizhu Ni,[1] Rabiha Qazi,[2] Shafiq Ur Rehman ,[2] and Ghulam Farid [2]

[1]*Mathematics Science Department, Normal University of Mudanjiang, Mudanjiang, Heilongjiang, China*
[2]*Department of Mathematics, COMSATS University, Islamabad, Attock Campus, Pakistan*

Correspondence should be addressed to Shafiq Ur Rehman; shafiq@cuiatk.edu.pk

Received 9 November 2020; Revised 21 December 2020; Accepted 28 December 2020; Published 19 February 2021

Academic Editor: Ghulam Mustafa

In today's technological world, confidentiality is an important issue to deal with, and it is carried out through different proficiencies. Cryptography is a scientific technique of securing a communication from unauthenticated approach. There exist many encryption algorithms in cryptography for data security. The need of new nonstandard encryption algorithms has been raised to prevent the communication from traditional attacks. This paper proposes some new encryption algorithms for secure transmission of messages using some special corona graphs and bipartite graph along with some algebraic properties. These proposed encryption schemes will lead to more secure communication of secret messages.

1. Introduction

Secret communications have been needed by military officers and diplomats since ancient times. In today's advanced age, where the internet, mobile phones, and computer technology are widely used in almost every sphere of life, the need to keep important information secure and confidential is also increasing day by day. Overtime, as data security continues to evolve, new ways to break the confidential communication are being discovered.

Cryptography is the science of transforming the secret data into coded information with the goal that it can safely reach its end without leakage. It was basically utilized for war time plans. Classical cryptography goes back over two thousand years. Modern cryptography was established by Shannon in 1949 [1]. After the development of digital communications, new forms of cryptography have come. It addresses the problems of secrecy, privacy, authentication, passwords, digital signatures, identification, and digital money. It is now an integral part of a modern society.

The process to transform the original message into a code format is called the encryption, and the reverse process is known as decryption [2]. Encryption prevents the original contents from interception. Uncovered message is known as plaintext. In any encryption scheme, the information which is referred as plaintext is encoded or encrypted to generate a cipher text with the help of a specified key. This cipher text is then converted into readable message through decryption. Key is such a piece of information that is used to put the original data in code shape and then decrypt to get real text. Through a provided key, the authorized recipient can open up the hidden message with full ease, but it is not possible for an interceptor. Mainly, three types of schemes are used in modern cryptography, i.e., symmetric key cryptography, public key cryptograph, and hash functions [3]. Symmetric key cryptography uses one key for both encryption and decryption, while the public key cryptography uses one key for encryption and another key for decryption. The hash functions use a transformation to irreversibly encrypt information.

We are interested in developing encryption by using graph theory and some algebraic concepts. Firstly, some useful concepts of graph theory are recalled [4]. A graph $G = G(V, E)$ consists of two sets: the set of vertices $V(G)$ and the set of edges $E(G)$. If the vertex set $V(G)$ can be partitioned into two disjoint nonempty subsets such that each edge has one vertex in each partition, then the graph G is said to be a bipartite graph. A bipartite graph is said to be complete-bipartite if every vertex in one partition is joined to all vertices of other partition. A complete-bipartite graph, in

which only one vertex is in one partition while all other vertices are in second partition, is termed as star graph. A vertex of degree one is named a pendent vertex, and the edge incident to it is pendent edge. The corona of two graphs G and H is the graph $G \odot H$ formed by one copy of G and $|V(G)|$ copies of H, where the ith vertex of G is joined to each vertex in the ith copy of H. This product is an important operation between graphs, introduced by Frucht and Harary [5]. The star graph S_{n+1} on $n+1$ vertices can be seen as a corona graph $K_1 \odot \overline{K_n}$. The corona graph of the cycle C_n with K_1, i.e., $C_n \odot K_1$, is a graph on $2n$ vertices obtained by attaching n pendant edges in a cycle graph C_n.

Graphs can be used for designing different encryption algorithms. The interaction between graph theory and cryptography is quite interesting. For applications of graph theory in cryptography, refer to [6–9]. The recent past has seen a growing interest in exploring graphs as a tool to propose new methodologies in different areas of cryptography (see [10–20]). In [10], Selvakumar and Gupta proposed an innovative algorithm for encryption and decryption using connected graphs. In [11], Kedia and Agrawal discussed a new encryption algorithm, in which data are secured through numeric representation and letters, using basic concepts of mathematics like Venn diagram. In [12], the authors have proposed a graph-based algorithm for encryption in which fundamental circuits are chosen with respect to corresponding weights of edges. In [13], Yamuna and Karthika describe a unique method of transferring data by using bipartite graph. They constructed a numeric table for the representation of alphabets. In [14], Al Etaiwi presented a new symmetric encryption algorithm using cycle graph, complete graph, and minimum spanning tree. It is reflected in paper [15] that the authors highlight some vast applications of bipartite graph in computation. In [16], the authors presented a scheme for securing a data by giving a new concept of line sigraph. Sigraph consists of graphs with sign of edges and belongs to $\{-1, +1\}$ as their labeled number. In [17], the authors proposed a novel bipartite graph-based propagation approach to overcome fraud detection in large advertising system. In [18], Razaq et al. used coset diagram for the action of $\mathrm{PSL}(2, \mathbb{Z})$ on projective line over the finite field $\mathbb{F}_{2^9}$ to construct proposed substitution box (S-box). The strong S-box is an important area of research in cryptography. In [19], Razaq et al. generated a strong S-box using orbits of coset graphs and the action of the symmetric group S_{256}. In [20], Selim G. Akl described an algorithm for encrypting a graph for its secure transmission from a sender to a receiver.

Our aim in this work is to describe new encryption algorithms based on some types of graphs, particularly, the corona graph $C_n \odot K_1$, $K_1 \odot \overline{K_n}$ (also called star graph), and the bipartite graph. The proposed algorithms send and receive secure messages consisting of words of any length by using graphs and certain algebraic properties. After applying prescribed algorithmic steps, data could be fully protected. The recipient then gets the labeled graph and eventually approaches to the original message.

In Section 2, an encryption scheme is described by using the corona graph $C_n \odot K_1$. Afterwards, an algorithm of this scheme is formulated. Application of this algorithm is studied through an example. However, in Section 3, bipartite graphs are used to construct a secure encryption scheme with described algorithm. This scheme is applicable on important information, shown by an example. In Section 4, a secured encryption scheme is described by using a special corona graph $K_1 \odot \overline{K_n}$, also named as a star graph. Its algorithm is mentioned, and application is viewed through an example.

2. Secure Data Transfer Using Corona Graph $C_n \odot K_1$

To initiate the described algorithm, the first step is to take a simple text which is to be transferred and is to be encrypted before sending. Every letter in data has its unique numeric representation, mentioned in encoding table, which is used to encode each alphabetic character. Then, each digit is transmuted up to n-place, through shift type of cipher. Now, new numeric values a_i are obtained. Randomly, some positive integers b_i are selected which are relatively prime with a_i. By taking inverse of that a_i in the modulus of b_i, corona graph $C_n \odot K_1$ is considered according to length of simple text with specified outward vertices and allocates the resulting inverses to suspended outward vertices, while main vertices are labeled with b_i. The final labeled corona graph $C_n \odot K_1$ is the encrypted data, in which the recipient receives to get required information. Figure 1 replicates the schematic diagram of the proposed algorithm.

Algorithm for encryption is as follows:

Give a plain-text word of length n.

Give the numerical values to the alphabets of plain-text word and apply shift cipher; $e_n(x) = x + n \pmod{26}$, to each numerical value obtained before and get new numerical values, say $a_1, a_2, a_3, \ldots, a_n$.

Find a sequence; $b_1, b_2, b_3, \ldots, b_n$ of positive integers in increasing order such that $\gcd(b_i, a_i) = 1$ and $b_i > 26$.

Consider a corona graph $C_n \odot K_1$ with $2n$ vertices and allot weights $b_1, b_2, b_3, \ldots, b_n$ to the vertices, adjacent to pendent vertices randomly.

Find the inverse of $a_i \pmod{b_i}$ for all i and denote them by c_i, i.e., $c_i = (a_i)^{-1} \pmod{b_i} \forall i$.

Give numeric values $c_1, c_2, c_3, \ldots, c_n$ to pendent vertices.

Send this corona graph $C_n \odot K_1$ to the receiver.

Algorithm for decryption is as follows.

The receiver receives the graph, and following steps are applied to transform the information and get original data:

Arrange those vertices which are adjacent to the pendent vertices, in increasing order as $b_1 < b_2 < b_3 < \cdots < b_n$.

Find the inverse of the weights of pendent vertices c_i modulus their adjacent vertices b_i and denote them by a_i for each i.

Compute $w_i = a_i - (\text{order of graph}/2) \bmod 26, \forall i$.

Convert the numeric values w_i for each i, to relate specific alphabets.

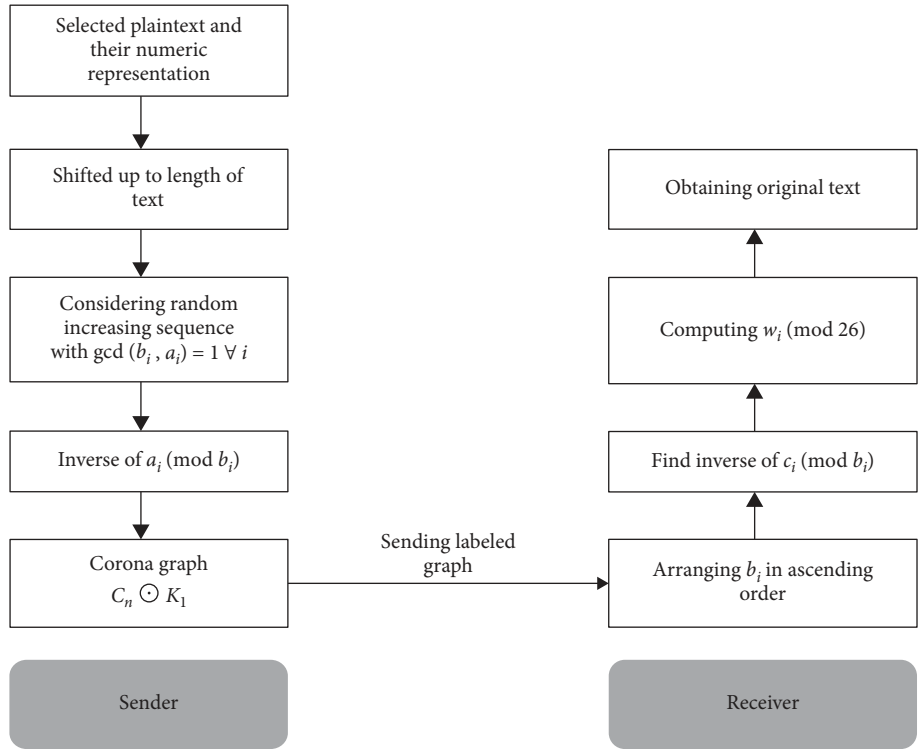

Figure 1: Schematic diagram.

Example 1. Let us suppose we have to transfer information, i.e., EDGE, encrypting it and then sending it to the recipient.

The starting point is to convert the alphabetic letters into numbers of their respective positions through the encoding table, as shown in Figure 2:

$$\begin{matrix} E & D & G & E \\ 5 & 4 & 7 & 5 \end{matrix}. \tag{1}$$

Here, length of word is $n = 4$. Applying shift cipher $e_n = x + n(\mathrm{mod}26)$, we get

$$\begin{aligned} 5 + 4 &= 9 = a_1, \\ 4 + 4 &= 8 = a_2, \\ 7 + 4 &= 11 = a_3, \\ 5 + 4 &= 9 = a_4. \end{aligned} \tag{2}$$

Given word is encrypted in the form

$$I \quad H \quad K \quad I. \tag{3}$$

Selecting random increasing integers b_i such that value of $b_i > 26$:

$$\begin{aligned} \gcd(b_1, a_1) &= \gcd(28, 9) = 1, \\ \gcd(b_2, a_2) &= \gcd(31, 8) = 1, \\ \gcd(b_3, a_3) &= \gcd(35, 11) = 1, \\ \gcd(b_4, a_4) &= \gcd(47, 9) = 1. \end{aligned} \tag{4}$$

Construct corona graph $C_n \odot K_1$ and put value of b_i to main vertices randomly, as shown in Figure 3.

Now, through the below-mentioned step,

$$c_i = (a_i)^{-1} (\mathrm{mod} b_i), \tag{5}$$

we get

$$\begin{aligned} c_1 &= (a_1)^{-1} (\mathrm{mod} b_1) = (9)^{-1} (\mathrm{mod} 28) = 25, \\ c_2 &= (a_2)^{-1} (\mathrm{mod} b_2) = (8)^{-1} (\mathrm{mod} 31) = 4, \\ c_3 &= (a_3)^{-1} (\mathrm{mod} b_3) = (11)^{-1} (\mathrm{mod} 35) = 16, \\ c_4 &= (a_4)^{-1} (\mathrm{mod} b_4) = (9)^{-1} (\mathrm{mod} 47) = 21. \end{aligned} \tag{6}$$

These inverse values are given to the adjacent pendant vertices of Figure 3, as shown in Figure 4.

Send this labeled graph (Figure 4) to the receiver.

The recipient, after receiving that labeled graph, arranges the main vertices in ascending order such that

$$28 < 31 < 35 < 47, \tag{7}$$

and considers these numbers as values of *bi* such that

$$b_1 < b_2 < b_3 < b_4. \tag{8}$$

Taking inverses of corresponding pendent vertices with respect to the value of each b_i, as shown in Figure 4, we get

$$\begin{aligned} 25^{-1} (\mathrm{mod} 28) &= 9 = a_1, \\ 4^{-1} (\mathrm{mod} 31) &= 8 = a_2, \\ 16^{-1} (\mathrm{mod} 35) &= 11 = a_3, \\ 21^{-1} (\mathrm{mod} 47) &= 9 = a_4. \end{aligned} \tag{9}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Figure 2: Numeric representation.

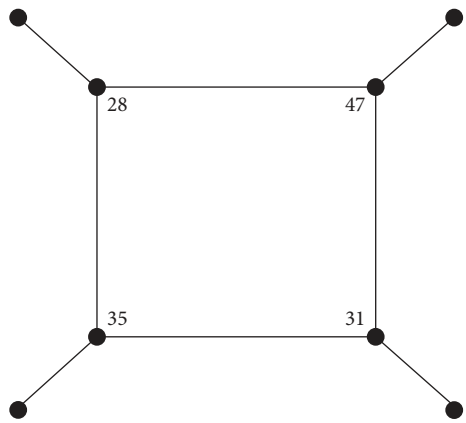

Figure 3

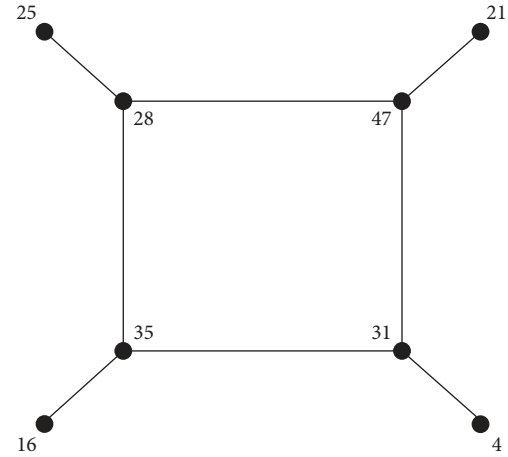

Figure 4

Now, for w_i,

$$w_i = a_i - \left(\frac{2n}{2}\right) \text{mod} 26. \tag{10}$$

Find values of a_1, a_2, a_3, and a_4:

$$\begin{aligned} w_1 &= a_1 - \left[\frac{2(4)}{2}\right] \text{mod} 26 = 5 = E, \\ w_2 &= a_2 - \left[\frac{2(4)}{2}\right] \text{mod} 26 = 4 = D, \\ w_3 &= a_3 - \left[\frac{2(4)}{2}\right] \text{mod} 26 = 7 = G, \\ w_4 &= a_4 - \left[\frac{2(4)}{2}\right] \text{mod} 26 = 5 = E. \end{aligned} \tag{11}$$

Finally, we get the original text.

3. Secure Data Transfer Using Bipartite Graphs

In this section, we propose an encryption algorithm for the secure and confidential communication of messages between two communicating parties. The construction of this encryption algorithm is based on bipartite graph and the concept of unique factorization domain (UFD). The following are the steps of algorithm.

Algorithm for encryption is as follows:

Take a UFD with infinite primes. For example, $\mathbb{Z}$.

Take a set P_n of first "n" primes, where $n = \lceil (26/k) + k \rceil$, $2 < k < 13$, and $k =$ key (which is fixed according to length of a word).

Consider a message, for encryption with length S.

Then, make a table $(n - k) \times k$ such that the first value shows number of rows and second value shows the number of columns.

After that, alphabets are partitioned as

1 st, 2 nd, 3 rd, . . . , k th position primes. (horizontally)

while;

$(k + 1)$th, $(k + 2)$th, $(k + 3)$th, . . ., nth position primes. (vertically)

Now, label the alphabets with the integers $r_i c_i$; r_i = row position, c_i = column position.

Label the entry ij with $r_i c_i$, where $k + 1 \le i \le n$, $1 \le j \le k$

Forming each number as vertex of path graph (according to sequence of letters).

Multiplying $i.j$ and then label each vertex with that number (say, a_p where $1 \le p \le k$). Keeping in view that, one place digits are not taken in column position. In other words, we say that column position has just 2-digit primes.

Construct a path graph by giving consecutive i, j numbers to each vertex.

Separate the graph labels as row and column numbers;

V_1 = {first place numbers from i}

V_2 = {second place numbers from j}

Edge set of G becomes (r_1, c_1), (r_2, c_2), ..., (r_n, c_n).

Now construct a bipartite graph with mentioned edge set. Edges move from r_i to c_i.

Assign random numbers to the edges as weight in increasing order.

Send that labeled graph.

Algorithm for decryption is as follows.
The recipient receives the labeled bipartite graph.

Arrange the weight of edges in increasing order.

Then, arrange edges with respect to weights in a set of order pair such that number of rows at first and number of columns at second position.

Construct path graph with the help of order pair information.

Find prime factorization of each vertex label.

Resultantly, required alphabets are taken through factorization, by using table (described).

Example 2. For defining the scheme, we have to explain an example. Take a word, **G R A P H**. Numerically, corresponding digits are 7, 18, 1, 16, and 8, respectively. Here, length of word is $k = 5$.

Step 1: take a UFD with infinite primes, i.e., $\mathbb{Z}$.

Step 2: in this example, $n = \lceil (26/5) + 5 \rceil$; $2 < k < 13$. So, $n = 11$. Take a set P_{11} of first 11 primes. As, $P_{11} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$.

Step 3: Figure 5 shows a table. For making a table, $(n - k) \times k = 6 \times 5$. First value, i.e., 6 shows the number of rows and 5 the number of columns.

Step 4: message becomes $G = 173$, $R = 235$, $A = 132$, $P = 232$, $H = 175$; $6 \le i \le 11$, $1 \le j \le 5$.

Step 5: corresponding values are

$$\begin{aligned} a_1 &= 17 \times 3 = 51, \\ a_2 &= 23 \times 5 = 115, \\ a_3 &= 13 \times 2 = 26, \\ a_4 &= 23 \times 2 = 46, \\ a_5 &= 17 \times 5 = 85. \end{aligned} \tag{12}$$

Next, we construct a path graph by labelling the vertices, as shown in Figure 6

Here, $V_1 = \{5, 11, 2, 4, 8\}$ and $V_2 = \{1, 5, 6\}$.

The vertex set of bipartite graph becomes

$$G(V_1, V_2) = \{(5, 1), (11, 5), (2, 6), (4, 6), (8, 5)\}. \tag{13}$$

Graph is obtained as shown in Figure 7.

Now, apply arbitrary weights to the adjacent edges of the bipartite graph in Figure 7, as shown in Figure 8.

Send the labeled graph in Figure 8 to the receiving authority. Then, apply the steps for decryption:

	2	3	5	7	11
13	*A*	*B*	*C*	*D*	*E*
17	*F*	*G*	*H*	*I*	*J*
19	*K*	*L*	*M*	*N*	*O*
23	*P*	*Q*	*R*	*S*	*T*
29	*U*	*V*	*W*	*X*	*Y*
31	*Z*				

Figure 5

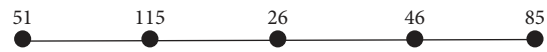

Figure 6

Step 1: at first, arrange the weight of the edges in ascending order:

$$W = \{10, 18, 21, 36, 41\}. \tag{14}$$

Step 2: now, arrange edges {(5,1), (11,5), (2,6), (4,6), (8,5)}.

The corresponding path graph is shown in Figure 9.

Step 3: prime factorization of each vertex label. As, $51 = 3 \times 17$, ..., $85 = 5 \times 17$. Numerical values are 173, 235, 132, 232, and 175, respectively.

Step 4: we finally get the alphabets **G R A P H** according to values in the described table. Keep in view that one place digits are not in column position.

The examples prove the security of described algorithm. This tells a simple bipartite graph can make secrecy of information very strong, that is, the major output of any encryption scheme.

4. Secure Data Transfer Using Star Graphs

Many schemes are introduced to protect data. The mentioned scheme is based on star graphs. Information is transferred with full secrecy of main idea. These steps are followed to encrypt data and then decrypt it by applying decryption steps.

Algorithm for encryption is as follows:

Let M be the message which is to be encrypted. Length is l(say).

Here, we have to use shift cipher with formulation:

$$e_k(x) = x + k (\text{mod} 26). \tag{15}$$

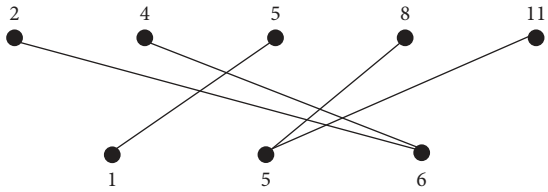

Figure 7

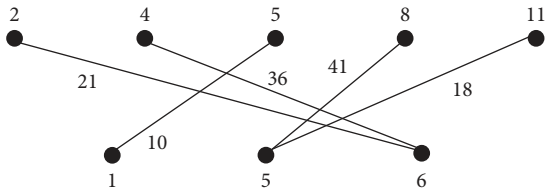

Figure 8

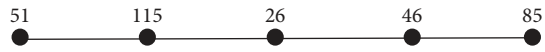

Figure 9

Keeping $k = l$ (fixed).

Converting the plaintext message to a sequence of integers by adding k into every value, by reducing every sum into modulo 26.

Now, take a star graph $S_{n+1} = K_1 \odot \overline{K_n}$, corresponding to the length of message, by fixing center vertex with the numeric value zero, such that number of vertices of star graph = 1 + number of alphabetic characters in the text.

Representing data as vertices of a graph, each vertex is represented by a letter. However, all adjacent vertices of a graph will be represented as adjacent letters.

Now label each vertex with respect to their numeric representation in shift cipher.

Next, give weights $w_1, w_2, w_3, \ldots, w_n$ to each edge $e_1, e_2, e_3, \ldots, e_n$ in such a way that

$$w_1(e_1) < w_2(e_2) < w_3(e_3) < \cdots < w_n(e_n). \tag{16}$$

Method for finding weights of edges.

Subtract increasing power of 10 from each vertex label, adjacently with respect to edges, such that

$$V_1 - 10, V_2 - 10^2, V_3 - 10^3, \ldots, V_n - 10^n, \tag{17}$$

where $V_i \in$ vertex tex $i = \{1, 2, 3, \ldots, n\}$.

These resulting values become weight of corresponding edges e_i.

Now, the final graph is the star graph with edge's weights (hiding the vertex label).

Send this graph to the receiver.

After explaining the encryption procedure, we have to explain the decryption scheme as well.

Algorithm for decryption is as follows:

Arrange the weight of edges in ascending order.

Now add up the increasing power of 10, respectively.

Apply the decryption formulation for shift cipher in the resulting number.

Decode the characters from encoding table, and eventually, we get the required text.

Example 3. For explaining the described scheme, we have to take an example for satisfying the steps. Let us take a word **CODE**. We have to send this word by encrypting it with the help of such scheme.

Replace the alphabetic characters with their numeric representation. Length of message is $k = 4$:

$$\begin{matrix} C & O & D & E \\ 3 & 15 & 4 & 5 \end{matrix}. \tag{18}$$

Now, consider a star graph $S_5 = K_1 \odot \overline{K_4}$, such that the number of its corner vertices is equal to the length of message. Figure 10 shows the respective star graph in such a way that edges are labeled as e_1, e_2, e_3, and e_4.

Apply the shift type of cipher as shifting up to the length k of the message. In this example, translated through formula,

$$e_4(x) = x + 4 (\text{mod} 6). \tag{19}$$

New shifted numeric values are 7, 19, 8, and 9, respectively. The related graph becomes as shown in Figure 11.

After that, apply weights $w_i, \forall i \in \{1, 2, 3, 4\}$ to the corresponding edges of the vertices:

$$w_1(7) < w_2(19) < w_3(8) < w_4(9). \tag{20}$$

Weights are given by subtracting the increasing power of 10 from each adjacent numeric value in Figure 11:

$$\begin{aligned} &\text{weight of edge } e_1 = w_1 = 7 - 10, \\ &\text{weight of edge } e_2 = w_2 = 19 - 10^2, \\ &\text{weight of edge } e_3 = w_3 = 8 - 10^3, \\ &\text{weight of edge } e_4 = w_4 = 9 - 10^4. \end{aligned} \tag{21}$$

Resulting star graph is shown in Figure 12.

This is the final labeled graph, which is to be send to the second authority. Now, describe the decryption process. Firstly, the recipient receives the labeled graph, as shown in Figure 12.

The initial step is arranging the weights of edges (Figure 13) in ascending order of mod values, i.e.,

$$|-3| < |-81| < |-992| < |-9991|. \tag{22}$$

Add the increasing power of 10 to each adjacent value such that

$$|-3 + 10| < |-81 + 100| < |-992 + 1000| < |-9991 + 10000|. \tag{23}$$

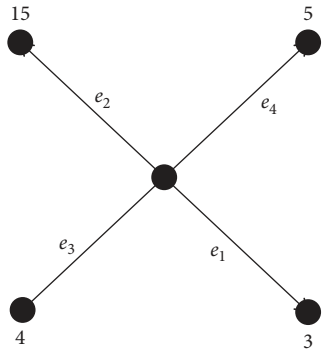

Figure 10

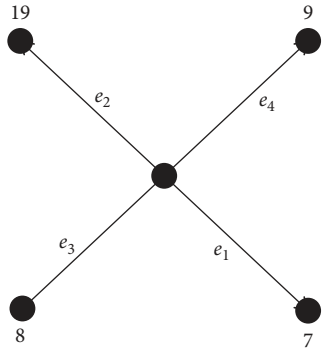

Figure 11

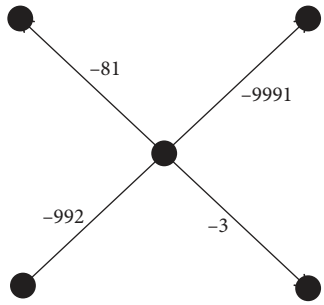

Figure 12

Through this mod operation, we get the values:

$$7, 19, 8, 9. \tag{24}$$

Apply inverse shifting by guessing the number of edges of the star graph, which is 4. So, the values become as follows:

$$\begin{aligned} 7 - 4 &= 3, \\ 19 - 4 &= 15, \\ 8 - 4 &= 4, \\ 9 - 4 &= 5. \end{aligned} \tag{25}$$

Finally, we get the values $3, 15, 4, 5$. Through the encoding table, we get their respective letters as **C O D E**. Get the required hidden text.

This example explains that any type of data is hidden and is kept secure until it approaches to the receiver. The algorithm depends on star graphs. Labeled graphs are sent to the recipient. It is a best possible way to secure the data.

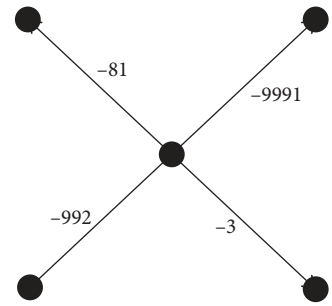

Figure 13

5. Conclusion

This work presents graph theoretic-based schemes to improve encryption quality. Three new encryption algorithms are proposed which are very helpful for secure communication of secret messages. In the first algorithm, encryption and decryption is performed by using a specific corona graph $C_n \odot K_1$ along with some basic algebraic properties. The second algorithm is based on encoding table, bipartite graph, and the concept of unique factorization domain (UFD). In third algorithm, we used a certain labeling of vertices and edges of the star graph $K_1 \odot \overline{K_n}$. These symmetric algorithms use the concept of shared key that must be predefined and shared between two communicating parties. We can modify the proposed algorithms, to be applicable for the communication of sentences or the set of sentences. Furthermore, for more complexity, these algorithms could be improved by using the public key cryptography. Moreover, we can try to implement these algorithms using any programming language like C++, JAVA, or Microsoft.Net.

Data Availability

There are no additional data required.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

The study was supported by the Heilongjiang Education Department Project (project number: 1355MSYQN001) and Research Project of Mudanjiang Normal University (project number: QN2020008). Also, the authors are thankful to the referees for many useful suggestions.

References

[1] C. E. Shannon, "Communication theory of secrecy systems*," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] K. H. Rosen, *Elementary Number Theory and its Applications*, Addison-Wesley, Boston, MA, USA, 5th edition, 2005.

[3] D. R. Stinson, *Cryptography: Theory and Practice*, Chapman and Hall/CRC, Boca Raton, FL, USA, 4th edition, 2018.
[4] D. B. West, *Introduction to Graph Theory*, Pearson, London, UK, 2nd edition, 2001.
[5] R. Frucht and F. Harary, "On the corona of two graphs," *Aequationes Math*, vol. 4, pp. 322–325, 1970.
[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[7] V. A. Ustimenko, "On graph-based cryptography and symbolic computations," *Serdica Journal of Computing*, vol. 1, pp. 131–156, 2007.
[8] D. X. Charles, K. E. Lauter, and E. Z. Goren, "Cryptographic hash functions from expander graphs," *Journal of Cryptology*, vol. 22, no. 1, pp. 93–113, 2009.
[9] P. L. K. Priyadarsini, "A survey on some applications of graph theory in cryptography," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, no. 3, pp. 209–217, 2015.
[10] R. Selvakumar and N. Gupta, "Fundamental circuits and cutsets used in cryptography," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 15, no. 4-5, pp. 287–301, 2012.
[11] P. Kedia and S. Agrawal, "Encryption using Venn-diagrams and graph," *International Journal of Advanced Computer Technology*, vol. 4, no. 01, pp. 94–99, 2015.
[12] M. Yamuna and A. Elakkiya, "Data transfer using fundamental circuits," *International Journal of Computer and Modern Technology*, vol. 2, no. 01, 2015.
[13] M. Yamuna and K. Karthika, "Data transfer using bipartite graphs," *International Journal of Advance Research in Science and Engineering*, vol. 4, no. 02, pp. 128–131, 2015.
[14] W. Mahmoud and A. Etaiwi, "Encryption algorithm using graph theory," *Journal of Scientific Research and Reports*, vol. 3, no. 19, pp. 2519–2527, 2014.
[15] B. R. Arunkumar, "Applications of Bipartite Graph in diverse fields including cloud computing," *International Journal of Modern Engineering Research*, vol. 5, no. 7, p. 7, 2015.
[16] D. Sinha and A. Sethi, "Encryption using network and matrices through signed graphs," *International Journal of Computer Applications (0975-8887)*, vol. 138, no. 4, pp. 6–13, 2016.
[17] J. Hu, J. Liang, and S. Dong, "A bipartite graph propagation approach for mobile advertising fraud detection," *Mobile Information Systems*, vol. 2017, p. 12, Article ID 6412521, 2017.
[18] A. Razaq, M. Awais Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, "A novel construction of substitution box involving coset diagram and a bijective map," *Security and Communication Networks*, vol. 2017, p. 16, Article ID 5101934, 2017.
[19] A. Razaq, H. Alolaiyan, M. Ahmad et al., "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," *IEEE Access*, vol. 8, pp. 75473–75490, 2020.
[20] G. A. Selim, "How to encrypt a graph," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 35, no. 6, pp. 668–681, 2020.