Pi International Journal of Mathematical Sciences
© PIJMS | Volume 1 | Issue 3 | December 2025 | ISSN: 3107-9830 (Online)
Available online at: https://pijms.com/
DOI: https://doi.org/10.59828/pijms.v1i3.11

Graph Theory and its Cryptography Applications: A Novel Approach

Hemant Gena[1], Dr. Subhash Yadav[2], Dr. Binny Gupta[3]
[1]Scholar, Department of Mathematics Sri Khushal Das University, Pilibanga, Hanumangarh
[2]Professor, Department of Mathematics, SBRM Govt. College, Nagaur
[3]Assistant Professor, Department of Mathematics, Sri Khushal Das University, Pilibanga, Hanumangarh
Email: binnykakkar29@gmail.com[3]

Received: 17 November 2025 | **Accepted:** 21 December 2025 | **Published:** 25 December 2025

ABSTRACT

In our modern society werely extensively on digital technology, which plays a critical role in various sectors, including banking, e-commerce transactions and cybersecurity such as managing computer passwords. This extensive integration emphasizes the critical role of reliable and secure digital infrastructure in our day-to-day activities. Therefore, it is more important to secure information during storage and transformation. Cryptography is the process of safeguarding information by converting it in a protected form, making it accessible only to authorized users. The process employs encryption algorithms to turn simple data, or "plaintext," into a coded version, referred to as "ciphertext," making it unreadable without proper authorization. Cryptography benefits from graph theory, as it enables the seamless conversion of graphs into matrices for cryptographic operations. In numerous disciplines, Graph Theory is indispensable, especially in encryption, due to its numerous properties and its ease of implementation as a matrix in computational systems. This paper introduces a novel approach that combines graph theory with symmetric cryptography, presenting an innovative method to enhance data security and protect against unauthorized access.

Keywords: Cryptography, Decryption.

1. Introduction

Cryptography is mainly have two branches: cryptanalysis and cryptography [5]. Cryptography is the study and practice of developing secure communication systems, focusing on techniques like encryption, digital signatures, hashing functions. Cryptanalysis, on the other hand, is the discipline of breaking cryptographic systems by analyzing encryption methods to identify vulnerabilities that could allow unauthorized access to encrypted data or compromise the system's security. Cryptanalysts frequently try to compromise cryptographic systems by identifying patterns or leveraging mathematical vulnerabilities. Essentially, cryptography aims to protect communication, whereas cryptanalysis seeks to undermine that protection. Together, these disciplines contribute to enhancing the robustness and dependability of cryptographic systems.

In mathematics, cryptology encompasses and draws upon various fields. The study of cryptographic security often involves theoretical computer science, particularly complexity theory. The practical aspects, such as implementing cryptosystems and performing detailed security analyses for specific systems, belong to the domains of applied computer science.

Adjacency matrix: A graph with no parallel edges. Then the nth adjacency matrix which is a symmetric and elements of matrix x_{ij} are given by

$$x_{ij} = \begin{cases} 1 & , if\ v_i v_j \in E \\ 0 & , otherwise \end{cases}$$

XOR

In cryptography, the XOR code is a simplest form of encryption. It relies on the principles of the XOR (exclusive OR) operation, denoted by ⊕, which works as follows

$$(1)\ u \oplus u = 0$$

$$(2)\ u \oplus 0 = u$$

Proposed Methodology for encoding:

1.Convert every alphabet into its equivalent numerical values using encoding table.

A	0	N	13	a	26	n	39
B	1	O	14	b	27	o	40
C	2	P	15	c	28	p	41
D	3	Q	16	d	29	q	42
E	4	R	17	e	30	r	43
F	5	S	18	f	31	s	44
G	6	T	19	g	32	t	45
H	7	U	20	h	33	u	46
I	8	V	21	i	34	v	47
J	9	W	22	j	35	w	48
K	10	X	23	k	36	x	49
L	11	Y	24	l	37	y	50
M	12	Z	25	m	38	z	51

Table(a):- Encoding table

(2) Take values of q and r such that they satisfies the condition

$$gcd(q, m) = 1 \text{ and } 0 < q, r < m \text{ where } m=52.$$

(3) Change every alphabet in numerical form using above table.

(4) We get the alphabets (y), corresponding to the value $(qx + r) mod\ m$, by using encoding table (Table-a) again.

(5) Convert each values into their corresponding ASCII value.

(6) Then get binary value.

(7) Then get $\text{XOR}^{ed.}$ Value using personal key 0100000.

(8) Put these values in array.

(9) Form an adjacency matrix of order equal to number of one in XOR.

(10) Then these matrices summaries into array form in which sum of all digits in array is equal to 7, because length of XOR^{ed} binary string is 7. And total number of elements in array equal to order of corresponding matrix(n).

Proposed Methodology for decoding:

(1) Received array will be converted into a temporary adjacency matrix.

(2) We will focus on the leading diagonal, elements of the adjacency matrix.

(3) Next, we generate the binary stream using the elements of the temporary adjacency matrix.

(4) Finally, all operations applied during the encoding process are reversed to recover the original message.

EXAMPLE:

Let our message is "NeED bacKup"

Let $q=17, r=31$ and binary key is "0100000"

Alphabet	**x**	**(17x+31)mod52**	**y**	**ASCII code**	**Binary form**	**XOR^{ed}form**
N	13	44	s	115	1110011	1010011
e	30	21	V	86	1010110	1110110
E	4	47	v	118	1110110	1010110
D	3	30	e	101	1100101	1000101
b	27	22	W	87	1010111	1110111
a	26	5	F	70	1000110	1100110
c	28	39	n	110	1101110	1001110
K	10	45	t	116	1110100	1010100
u	46	33	h	104	1101000	1001000
p	41	0	A	65	1000001	1100001

Table(b):- Encryption table

In this table we converted alphabets of our message into digits using encoding table then using (qx+r)mod m we get "y" alphabets again by encoding table(a). Then we changed decimal digits into binary form and then into XOR^{er} form.

By using encryption method and graph, we got symmetric matrix corresponding to every alphabet of our message. They are given as:-

$$N=\begin{bmatrix}0&2&0&0\\2&0&3&0\\0&3&0&1\\0&0&1&0\end{bmatrix}\quad e=\begin{bmatrix}0&2&0&0\\2&0&2&0\\0&2&0&1\\0&0&1&0\end{bmatrix}E=\begin{bmatrix}0&1&0&0&0\\1&0&1&0&0\\0&1&0&2&0\\0&0&2&0&1\\0&0&0&1&0\end{bmatrix}$$

$$D=\begin{bmatrix}0&4&0\\4&0&2\\0&2&0\end{bmatrix}\quad b=\begin{bmatrix}0&1&0&0&0&0\\1&0&1&0&0&0\\0&1&0&2&0&0\\0&0&2&0&1&0\\0&0&0&1&0&1\\0&0&0&0&1&0\end{bmatrix}a=\begin{bmatrix}0&1&0&0\\1&0&3&0\\0&3&0&1\\0&0&1&0\end{bmatrix}$$

$$c=\begin{bmatrix}0&3&0&0\\3&0&1&0\\0&1&0&1\\0&0&1&0\end{bmatrix}K=\begin{bmatrix}0&2&0\\2&0&2\\0&2&0\end{bmatrix}u=\begin{bmatrix}0&3\\3&0\end{bmatrix}p=\begin{bmatrix}0&1&0\\1&0&5\\0&5&0\end{bmatrix}$$

for each alphabet receiver will receives these array

For “N” [2,3,1,1]

For “e” [2,2,1,2]

For “E” [1,1,2,1,2]

For “D” [4,2,1]

For “b” [1,1,2,1,1,1]

For “a” [1,3,1,2]

For “c” [3,1,1,2]

For “K” [2,2,3]

For “u” [3,4]

For “p” [1,5,1]

By using these arrays receiver will get actual message shown in given table below

data from array	XOR^{ed}form	Binary form	Decimal values	ASCII code	Numerical values(x)	(x-1612)mod52 /884mod52	Alphabet
2,3,1,1	1010011	1110011	115	s	44	13	N
2,2,1,2	1110110	1010110	86	V	21	30	e
1,1,2,1,2	1010110	1110110	118	v	47	4	E
4,2,1	1000101	1100101	101	e	30	3	D
1,1,2,1,1,1	1110111	1010111	87	W	22	27	b
1,3,1,2	1100110	1000110	70	F	5	26	a
3,1,1,2	1001110	1101110	110	n	39	28	c
2,2,3	1010100	1110100	116	t	45	10	K
3,4	1001000	1101000	104	h	33	46	u
1,5,1	1100001	1000001	65	A	0	41	p

Table(c):- Decryption table

After these calculations receiver will get the actual message “NeEDbacKup”

CONCLUSION:

Symmetric key cryptography employs the one key for both process encryption and decryption, by high efficiency and speed. However, its effectiveness relies on securely sharing the key between the sender and receiver, as the confidentiality of the key is crucial for maintaining communication security. This challenge of secure key distribution is a significant limitation of symmetric encryption.

To address this issue, this paper introduces a novel approach utilizing graph theory to enhance the security and practicality of key sharing in symmetric key cryptography. Cryptography is a method used to ensure safe communication.

This cryptographic approach significantly increases the complexity and uncertainty of decrypting and interpreting the original message, as each graph corresponds to a single character of the data. The algorithm provides robust data security, ensuring that the information remains protected against unauthorized access.

REFERENCES:

[1]. P. Amudha, A.C. Charles Sagayaraj, and A.C. Shantha Sheela. An application of graph theory in cryptography. International journal of Pure and Applied Mathematics, 119(13):375-383.

[2]. Manisha Kumari and V.B. Kirubanad. Data encryption and decryption using graph plotting. International Journal of Civil Engineering and Technology (IJCIET) Volume, 9:36-46, 2018.

[3]. Mahantesh Gawannavar, Payal Mandulkar, R. Thandeeswaran, N. Jeyanthi, Office in cloud: Approach to Authentication and Authorization, Recent Advances in Communications and Networking Technology, Bentham sciences, Vol.4, No.1, 2015, pp.49-55.

[4]. N. Jeyanthi, R. Thandeeswaran, J. Vinithra, 2014, RQA Based Approach to Detect and Prevent DDoS Attacks in VoIP Networks, Cybernetics and Information Technologies, Vol.14, No.1, pp. 11-24.

[5]. C. Vasudev. Graph theory with applications. New Age International, 2006.

[6]. Srilekha Chowdhury, Promita Ghosh, Mayurakshi Jana, An Approach of Graph Theory for Solving Cryptographic Problem, BKGC SCHOLARS July -December 2020, Vol. 1 Issue. 2, PP. 64 – 68.

[7]. Amrutha, R. Thandeeswaran, N. Jeyanthi, 2014, Cloud based VoIP Application in Aircraft Data Networks, International Journal of Grid Distribution Computing, Vol.7, No.6 (2014) December, pp.11-18.

Cite this Article:

Hemant Gena, Dr. Subhash Yadav, Dr. Binny Gupta, "Graph Theory and its Cryptography Applications: A Novel Approach", ***Pi International Journal of Mathematical Sciences, ISSN:*** *3107-9830 (Online), Volume 1, Issue 3, pp. 01-05, December 2025.*

Journal URL: *https://pijms.com/*

DOI: *https://doi.org/10.59828/pijms.v1i3.11*