International Journal of Linguistics and Computational Applications (IJLCA)
Volume 8, Issue 1, January – March 2021
ISSN 2394-6385 (Print)
ISSN 2394-6393 (Online)

Applying Graph Theory to Secure Data by Cryptography

Dr. Gurusharan Kaur[1], Dr. Namrata Tripathi[2]

Assistant Professor, Dept. of Computer Science/ Mathematics, Career College, Bhopal, Madhya Pradesh, India
Assistant Professor, Department of Mathematics, Govt. PG. College, Rajgarh, Madhya Pradesh, India

Abstract— Graph Theory is one of the significant and important areas in Mathematics, which is used in Network Security. Cryptography is art of science to achieving security by encoding message to make it non-readable (secretive) to unintended users. Many techniques are presents to encrypt plain text and convert it to the cipher text [2]. Any cryptographic scheme is secure if and only if it is unbreakable in reasonable time, using feasible resources in spite of the intruder's being aware of the encryption and decryption algorithm and size of the key. In the proposed algorithm, adjacent matrix of graph can be used to obtain key for encryption and decryption which is safer compared to other keys.

Keywords *— Cryptography; Substitution; Transposition; Adjacent Matrix; Sparse; Symmetric; Asymmetric.*

1. Introduction

The main objective of Data Security is to secure data transmission over unreliable network. Data Security is a challenging issue of data communications today, which touches many areas including secure Communication channels, Strong Data Encryption Technique and trusted third party to maintain the database secure, is the prime concern of the research paper. The art of Sciences and Computer Science with Graph Theory creating non readable data, so that only the intended person is able to read text with the help of Cryptography. Encryption is a process by which we convert our data to cipher text or non-readable form. Decryption is the reverse process of Encryption. Hence, it is very important and crucial to apply effective encryption/decryption methods to enhance data security. Encryption is the only conventional methods to maintain the data security. The information could be accessed by the unauthorized user for mischievous purposes.

Cryptography is a process to safeguard network and data transmission over wireless networks. Data Security is the main concept to secure data transmission over unreliable networks. Data Security is a challenging and risky task of data communications today that touches varied areas including secure communication channels, strong data encryption techniques and trusted third party to maintain the database. The rapid progress and development in information technology, the secure transmission of confidential (secretive) data hereby gets a great deal of attention. The adjacent matrix that we are using in network security plays a vital role to transmit the secure keys.

2. Definitions

- *Cryptography* - The processing of transforming a plain message into cipher text (non-readable), and then re-transforming that message back to its original form is called Cryptography.
- *Plaintext* - In cryptography, the original message or simple text which is in readable form that has to be encrypted and makes it a non-readable form.
- Cipher-text - In cryptography the transformed message which we received after applying key on plain text.
- *Key* - Some non-readable cipher text, known only sender & receiver, a key is a variable that is useful using an algorithm to produce encrypted text, or to decrypt encrypted text.
- *Encipher (encode) and Decipher (decode)* - The process of converting plaintext (readable text) to cipher-text (unreadable text). The process of converting cipher-text (unreadable text) back into plaintext (readable text).
- *Encryption and Decryption* - A process of encoding a message using some key or method so that it's meaning is not easily understandable. The reverse process of encryption method of converting cipher text into plain text is Decryption.
- *Brute Force Attack* - A brute force attack is a hit and trial process used to obtain information from the authenticate users.

2.1 Adjacency Matrix

- This is the matrix representation of Graph. It is used in computer processing.
- The advantage of using adjacency matrix representation is that many results of matrix algebra can be willingly applied to study the structural properties of graphs.
- An adjacency list represents a graph (with no multiple edges) by specifying the vertices that are adjacent to each vertex. This matrix is based on ordering chosen for the vertices.
- This matrix can be representing both directed and undirected graphs**.**

DOI: **10.30726/ijlca/v8.i1.2020.81001**

2.2 Incidence Matrix

The incidence matrix G is n × m matrix (b_{ij}) where n and m are the numbers of vertices and edges respectively, such that matrix $b_{ij}=1$ if the vertex v_i and edge e_j are incident and 0 otherwise.

3. Main Result

Proposed Algorithm: Use the proposed algorithm to encrypt and decrypt data. (Send key_2 in the form of graph)

3.1 Encryption

This algorithm is used to convert plain text to cipher text.

- First we take a message or plain text from user which have to encrypt
- Use key_1 to shift character.
- Encrypt the message by replacing each letter by decided key $_1$.
- Write encrypted message in the form of matrix.(where (n-1) x n where n=number of digits in key_2) which is decided by sender and receiver.
- Read off the message row by row and permute the order of column.
- The output of step 5 , write in matrix form again and read row by row.
- After reading row by row , we get our cipher text.

3.2 Decryption

This algorithm is used to convert cipher text to plain text.

- It take the cipher text and use key $_2$ to write cipher text in the form of matrix.
- (where, (n-1) x n where n=number of digits in key_2) which is decided by sender and receiver.
- Arrange the cipher in matrix form column by column using key $_2$.
- Read message row by row.
- Again arrange the cipher of step 3 in matrix form column by column using key $_2$.
- Now decrypt the message with key_1.
- Finally we get plain text.

3.3 Example :- (Encryption)

- First take a message or plain text from user which we have to encrypt. For ex. THIS IS AN EXAM
- Use key_1 to shift character.
- Suppose key $_1$ = +3
- Encrypt the message by replacing each letter by decided key 1.
- XLMWMWERIBEQ
- Write encrypted message in the form of matrix(where (n-1) x n where n=number of digits in key_2) which is decided by sender and receiver.

$cKey_2$ is shared in the form of adjacent graph, sender and receiver have to calculate key_2 from the given graph.

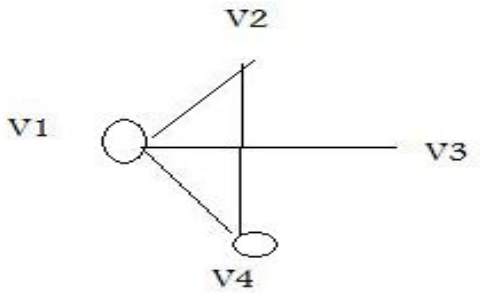

Fig.1: Graph for the calculation of key_2

Convert the above graph into adjacent matrix which is used as key $_2$

Table 1: Adjacent matrix of key_2

	V1	V2	V3	V4
V1	1	1	1	1
V2	1	0	0	1
V3	1	0	0	0
V4	1	1	0	1

Now the key_2 is **4 2 1 3**

Table 2(a): Message creation from key_2

4	2	1	3
X	L	M	W
M	W	E	R
I	B	E	Q

- Read off the message row by row and permute the order of column MEELWBWRQXMI
- The output of step 5 , write in matrix form again and read row by row.

Table 2(a): Message creation from key_2

4	2	1	3
M	E	E	L
W	B	W	R
Q	X	M	I

DOI: **10.30726/ijlca/v8.i1.2020.81001**

- After reading row by row, we get our cipher text. EWMEBXLRIMWQ (cipher text to be sent).

4. Decryption

- It take the cipher text and use key $_2$ to write cipher text in the form of matrix (where (n-1) x n, where n=number of digits in key$_2$) which is decided by sender and receiver.
  Received cipher text is: - EWMEBXLRIMWQ
- Arrange the cipher in matrix form column by column using key$_2$.

Table 3(a): Cipher text in matrix form

4	2	1	3
M	E	E	L
W	B	W	R
Q	X	M	I

- Read message row by row. MEELWBWRQXMI
- Again arrange the cipher of step 3 in matrix form column by column using key $_2$.

Table 3(b): Cipher text in matrix form

4	2	1	3
X	L	M	W
M	W	E	R
I	B	E	Q

Received cipher text is: - XLMWMWERIBEQ

- Now decrypt the message with key$_1$. Key$_1$=(-3)
- Finally we get plain text.
  Result: This is an exam

5. Conclusion

This algorithm is secured by "Double Transposition column" method with graph as key has various advantages over simple algorithm. It is more difficult to cryptanalyst. Due to use of graph for developing of key$_2$, the result (plaintext) cannot be cracked and hence security is enhanced. Brute force attack is not possible. Through this proposed algorithm maximum limitation of Caesar Cipher are overcome. New application can be easily updated. Generate several keys for other applications: banking, electronic commerce, electronic voting, etc. It's difficult to implement as simple Caesar cipher. Due to implementation of graph theory in security sometimes it takes more space in memory.

Future Enhancements

This algorithm is based on the concept of taking alphabet as plaintext, which can also be extended in future with alpha numeric data.

References

[1] Atul Kahate (2009)Cryptography and Network security, 2nd Edition , McGraw Hill
[2] "Enhancing security of caesar cipher by Double columnar transposition method" by Vinod Saroha, Suman Mor and Anurage Dagar, International journal of advanced research in computer science and software engineering, vol. 2, issue 10, Oct. 2012.
[3] Stalling. W (1999), Cryptography and Network security, 2nd Edition, Prentice Hall
[4] William stalling "Network security Essentials (Application and standards)", Pearson Education, 2004
[5] www.securnet.biz/Ebooks/Network_Security.pdf , Accessed on 2nd October 2020.

DOI: **10.30726/ijlca/v8.i1.2020.81001**