International Journal of Mathematics Trends and Technology
ISSN: 2231-5373/ https://doi.org/10.14445/22315373/IJMTT-V68I6P524
Volume 68 Issue 6, 190-194, June 2022
© 2022 Seventh Sense Research Group®

Original Article

Super-Encryption Method using Affine Transform Via Trees

Beena Kittur[1], D. Chaya Kumari[2], Sneha G. Kulkarni[3], Manjula K M[4]

[1,2,3,4]*Department of Mathematics, AMC Engineering College, Bangalore, India.*

Received: 24 May 2022 Revised: 03 July 2022 Accepted: 06 July 2022 Published: 09 July 2022

Abstract *- In this paper, a new technique of super encryption is established with Affine transformation by exploring the features of trees in Graph theory.*

Keywords *- Affine transformation, Graph, Tree.*

1. Introduction

To visualize the discrete objects and the relations between them, graphs are of great help. Graphs basically contain objects represented as vertices or nodes and relation between them as lines (edges) connecting the nodes.

In recent years Graph theory concepts such as spanning tree, Euler graph, complete graph and molecular graphs are being utilized in cryptography ([8]-[19]). In [4] and [6], Chayakumari et.al. have considered super and multiple encryption method using Fibonacci and Lucas transformation.

The unique property of tree helps to solve many traversal problems like BFS, DFS in Data structure, optimal prefix codes in cryptography, sorting etc. Huffman's code gives an efficient way to compress the text message by always giving optimal tree with leaves as letters in the messages. To enhance the network security of encrypted message we have proposed a method of constructing a type of cryptosystem using the idea of trees.

In this paper, we propose a super-encryption method by exploring the idea of optimal prefix codes by constructing an optimal tree from the numerical equivalents of the plain text and Affine transformations.

2. Basic Definitions

Graph: Graph is a mathematical representation of a network and it describes the relationship between discrete objects.
Simple Graph: A graph without loops and parallel edges is called a simple graph.
Directed Graph: It is a graph in which the edges have a direction. This is usually indicated with an arrow on the edge.
Un-directed Graph: It is a graph where the vertices or nodes that are connected together, where all the edges are bidirectional.
Connected Graph: A graph is said to be a connected graph if there is a path between every pair of vertex.
Disconnected Graph: A graph is said to be a disconnected graph if it has two or more components.
Complete Graph: A simple graph with 'n' mutual vertices is called a complete graph and it is denoted by K_n.
Bi-partite Graph: It is a graph whose vertices can be divided into two disjoint and independent sets U and V i.e., every edge connects a vertex in U to one in V.
Complete Bi-partite Graph: It is a graph whose vertices can be partitioned into two subsets V_1 and V_2 such that no edge has both end points in the same subset and every vertex of V_1 is incident on every vertex of V_2.
Tree: If there is a graph which has no cycles but there exist a unique path between any 2 vertices is referred to as a tree.
Classification of trees: A normal tree has no restriction on the number of leaves each node can have.
Binary tree: A rooted tree is called a binary tree if every vertex is of out-degree less than or equal to two.
Complete Binary tree: A rooted tree is said to be complete binary tree if every internal vertex is of out-degree two.
Full Binary tree: A complete binary tree where every leaf is at the same level is length of path from root to leaf is same
Weighted tree: A tree in which each leaf/edge is assigned a positive integer is called a weighted tree
Optimal tree: For a given set of weights, there can be many weighted trees. A tree in this set which carries the minimum weight is called an optimal tree.
Code: A code is a binary sequence of 0's and 1's which are assigned to each letter in the message.
Prefix code: A set P of binary sequence is such that any binary sequence in P does not appear in the beginning of the binary sequence of any other code then P is a prefix code
E.g.: P= {11,101,001}

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Optimal prefix code: An optimal prefix code with minimal average length. Huffman code is a particular type of optimal prefix code that is commonly used for lossless data compression.
Cryptography: Cryptography is the technique of sending messages by preserving the secrecy.
Plain text: Plain text refers to the information or message that is to be sent by the sender to the receiver.
Cipher text: Cipher text refers to the encoded or encrypted message that contains the plain text in an unreadable format.
There are two types of cryptography

a) **Symmetric/private key cryptography:** In symmetric key cryptography, we use the same key for both encryption and decryption.
b) **Asymmetric/public key cryptography:** In asymmetric key cryptography, we employ different keys for both encryption and decryption.

Affine transformation: Affine Transformation is a kind of a symmetric key crypto-system given by $c = ax + b(mod\ 27)$ and its inverse affine transformation is $x = a^{-1}(c - b)\ (\text{mod } 27)$ (including space).

3. Proposed Encryption Algorithm

Step-1: Consider the plain text 'm' and write its numerical equivalent.
Step-2: Draw an optimal tree by using Huffman's procedure with the above numerical equivalents.
Step-3: Prefix codes of the letters obtained as leaves in the optimal tree converted to decimal equivalents.
Step-4: Add level of each leaf to the decimal equivalent obtained in step-3 and sender sends this cipher text to the receiver keeping the level as secret key.
Step-5: Sender again encrypts the cipher text obtained in step-4 by using affine transformation.

4. Proposed Decryption Algorithm

Step-1: Receiver receives the cipher text from the sender and decrypts with inverse affine transformation as first level of decryption.
Step-2: Receiver again decrypts the cipher text and applies secret (private key-level) to the cipher text as second level of decryption.
Step-3: Subtract the levels of optimal tree from the numerical equivalents of decrypted text.
Step-4: Now, the receiver constructs his own optimal tree with the private key sent by the sender. Finally, the plain text will be retrieved.

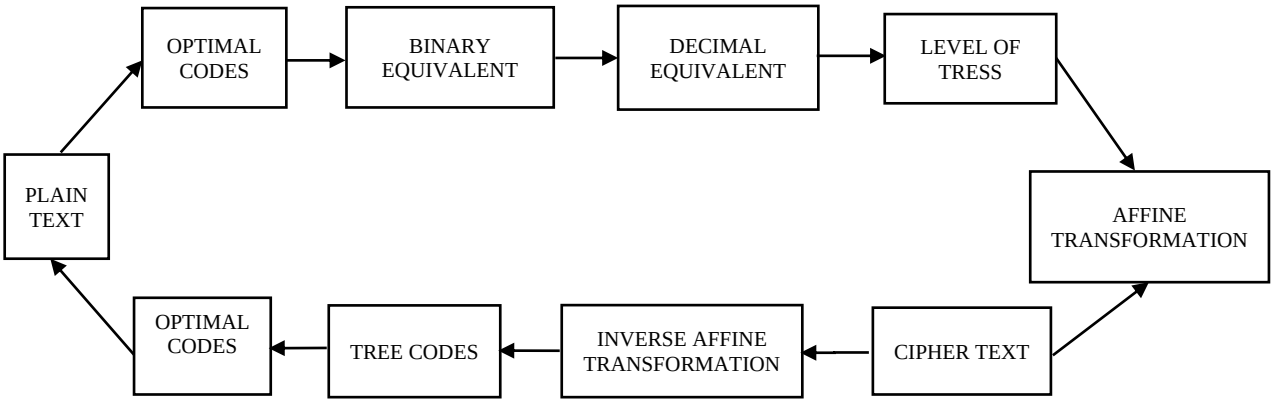

Fig. 1 Flow chart for encryption decryption scheme

Example:
Encryption: Take the sentence "GOD_IS_GREAT" and write its numerical equivalents as weights and construct an optimal tree.

Table 1. The numerical equivalents of the alphabets

Alphabets	A	B	C	D	…	L	…	W	X	Y	Z	_
Numerical value	0	1	2	3	…	11	…	22	23	24	25	26

Write the alphabets in the ascending order of their numerical equivalent.

Alphabets	A	D	E	G	G	I	O	R	S	T	_	_
Numerical value	0	3	4	6	6	8	14	17	18	19	26	26

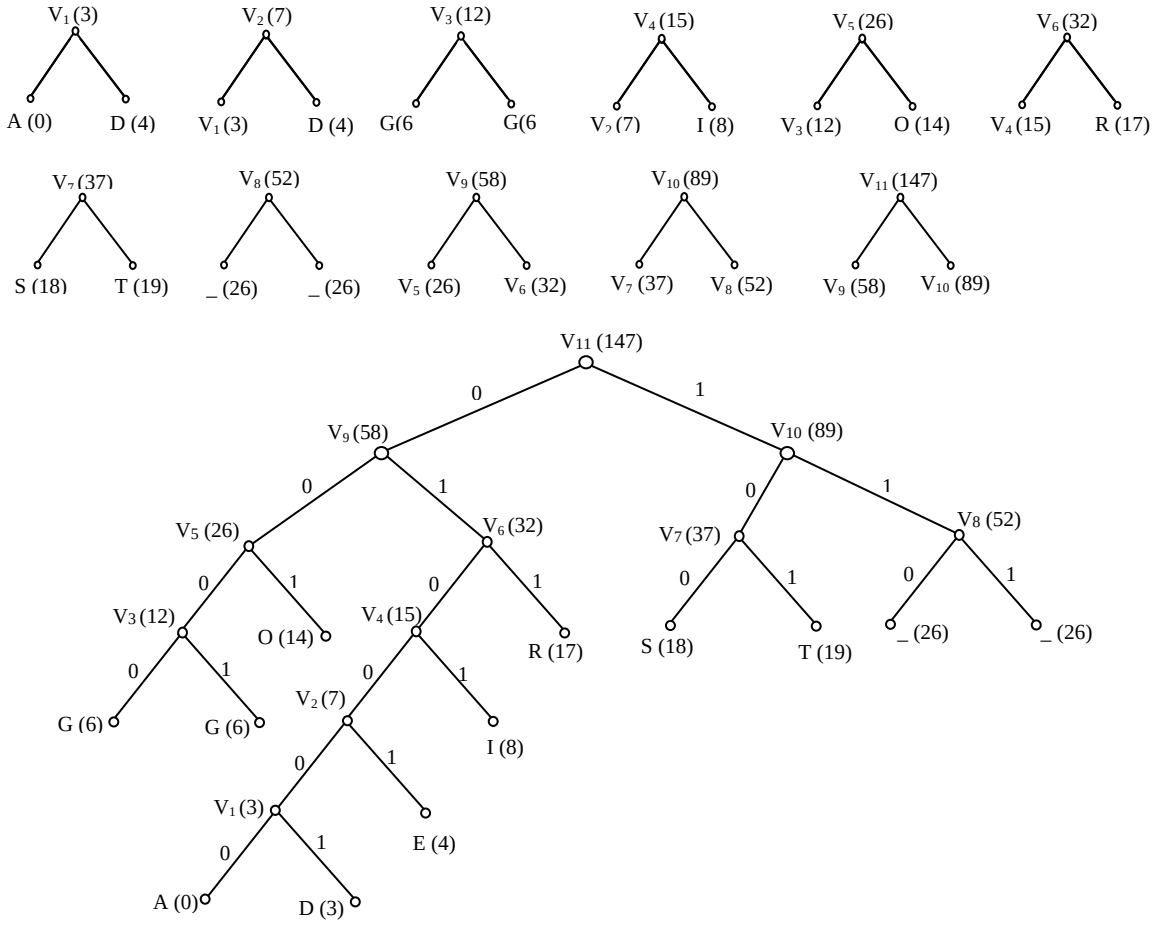

Fig. 2 Construction of optimal tree

Table 2. First level encryption

Alphabets	G	O	D	_	I	S	_	G	R	E	A	T
Binary equivalent	0000	001	010001	110	0101	100	111	0001	011	01001	010000	101
Decimal equivalent	0	1	17	6	5	4	7	1	3	9	16	5
Level	4	3	6	3	4	3	3	4	3	5	6	3
Decimal equivalent + Level	4	4	23	9	9	7	10	5	6	14	22	8
Cipher text	E	E	X	J	J	H	K	F	G	O	W	I

Then “GOD_IS_GREAT” is encrypted as EEXJJHKFGOWI as first level of encryption. Now, affine transformation is employed to the cipher text obtained in the first level.

Table 3. Second level of encryption

Cipher text	Numerical equivalent	Affine transformation C=5x+7	5x+7 (mod 27)	First level Cipher text
E	4	27	0	A
E	4	27	0	A
X	23	122	14	O
J	9	52	25	Z
J	9	52	25	Z
H	7	42	15	P
K	10	57	3	D
F	5	32	5	F
G	6	37	10	K
O	14	77	23	X
W	22	117	9	J
I	8	47	20	U

Decryption:

By taking the cipher text obtained in the second level AAOZZPDFKXJU and decrypting with inverse affine transformation x=11(c-7).

Table 4. First level of decryption

Final Cipher text	Numerical equivalent	Inverse Affine transformation x=11(c-7) (mod 27)	Final Cipher text
A	0	4	E
A	0	4	E
O	14	23	X
Z	25	9	J
Z	25	9	J
P	15	7	H
D	3	10	K
F	5	5	F
K	10	6	G
X	23	14	O
J	9	22	W
U	20	8	I

Now, subtract the levels of optimal tree from the numerical equivalent of decrypted text. Then, the receiver constructs his own optimal tree with the private key sent by the sender.

5. Conclusion

The constructed cryptosystem is more secure than symmetric key cryptosystem with polynomial running time. This can be extended to public key cryptosystem.

References

[1] J.Buchman, "Introduction to Cryptography," *Springer-Verlag*, 2001.

[2] Neal Koblitz, "A Course in Number Theory and Cryptography".

[3] K.H.Rosen, "Elementary Number Theory and Its Applications," Third edition., *AddsonWesly*.

[4] Dr.D.ChayaKumari, Dr.S.Ashok Kumar, D.Triveni, "Super-Encryption Method of Laplace Transformations using Fibonacci Numbers," *Journal of Huazhong University of Science and Technology*, vol. 50, no. 7.

[5] A.ChandraSekhar, D. ChayaKumari, S. Ashok Kumar, "Symmetric Key Cryptosystem for Multiple Encryptions," *International Journal of Mathematics Trends and Technology*, vol. 29, no. 2, 2016.

[6] A.ChandraSekhar, D. ChayaKumari, Ch.Pragathi, S. Ashok Kumar, "Multiple Encryptions of Fibonacci Lucas Transformations," *International Organization of Scientific Research* (IOST), vol. 12, no. 2, pp. 66-72, 2016. Doi: 10.9790/5728-1202026672.

[7] A.ChandraSekhar, D. ChayaKumari, Ch.Pragathi, S. Ashok Kumar, "Triple Encryption Scheme Using two Independent Keys," *International Journal of Engineering Science and Technology*, vol. 8, No. 4, 2016.

[8] Uma Dixit, "Cryptography A Graph Theory Approach," *International Journal of Advance Research in Science and Engineering*, vol. 6 no. 1, 2017.

[9] Rishi Pal Singh, Vandana, "Application of Graph Theory in Computer Science and Engineering," *International Journal of Computer Applications*, vol. 104, no. 1, 2014.
[10] P. Amudha, A.C. Charles Sagayaraj, A.C.ShanthaSheela, "An Application of Graph Theory in Cryptography," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 13, pp. 375-383, 2018.
[11] Nandhini R, Maheswari V and Balaji V, "A Graph Theory Approach on Cryptography," *Journal of Computational Mathematica*.
[12] Wael Mahmoud Al Etaiwi, "Encryption Algorithm Using Graph Theory," Journal of Scientific Research and Reports, vol. 3, no. 19, pp. 2519-2527, 2014.
[13] P.A.S.D.Perera, G.S.Wijesiri, "Encryption and Decryption Algorithms in Symmetric Key Cryptography Using Graph Theory," *Psychology and Education*, vol. 58, no. 1, pp. 3420-3427, 2021.
[14] Dharmendra Kumar Gurjar and AuparajitaKrishnaa, "Lexicographic Labeled Graphs in Cryptography," *Advances and Applications in Discrete Mathematics*, vol. 27, no. 2, pp. 209-232, 2021.
[15] W. Mahmoud Al Etaiwi, "Encryption Algorithm Using Graph Theory," *Journal of Scientific Research and Reports*, vol. 3, no. 19, pp. 2519-2527, 2014.
[16] H. K. Krishnappa, N. K. Srinath and S. Manjunath, "Vertex Magic Total Labeling of Complete Graphs and Their Application for Public-Key Cryptosystem," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 2, 2013.
[17] J. Dharani, V. Maheswari and V. Balaji, "Encryption Approach on Graph Theory," *Journal of Computational Mathematica*, vol. 2, no. 1, 2018.
[18] Dharmendra Kumar Gurjar, AuparajitaKrishnaa, "Complete Graph and Hamiltonian Cycle in Encryption and Decryption," *International Journal of Mathematics Trends and Technology*, vol. 67, no. 12, pp. 62-71, 2021.
[19] A. Krishnaa, "Some Applications of Labelled Graphs," *International Journal of Mathematics Trends and Technology (IJMTT)*, vol. 37, no. 3, pp. 209-213, 2016.
[20] SafaaHraiz and WaelEtaiwi, "Symmetric Encryption Algorithm Using Graph Representation," *in 2017 8th International Conference on Information Technology (ICIT)*, IEEE, pp. 501-506, 2017.
[21] G.Ashok, S.Ashok Kumar, D.ChayaKumari, "A New Kind of Cryptosystem Using Polynomials and Fibonacci Numbers," *presented at the International Conference on Computational Sciences – Modelling, Computing and Soft Computing (CSMCS-2022)*, through online, Department of Mathematics, Manipal Institute of Technology, Manipal, India, 2022.
[22] L Shobana, J BhaskarBabujee, Ismail NaciCangul, "A New Cryptographic Method by Means of Molecular Graph," *Proceedings of the Jangjeon Mathematical Society*, vol. 23, no. 4, pp. 503-507, 2020.
[23] "Connections between Graph Theory And Cryptography, Natalia Tokareva G2C2: Graphs and Groups, Cycles and Coverings," Novosibirsk, Russia, 2426, 2014.
[24] Abdullah K, "Comparison between the RSA Cryptosystem and Elliptic Curve Cryptography," *The University of Waikato, Hamilton, New Zealand*.
[25] "Cryptography: A very Short Introduction," by Fred Piper and Sean Murthy. E.H.Lock Wood, *A single-light on Pascal's triangle, Math, Gazette*, vol. 51, pp. 243-244, 1967.