A Symmetric Double Encryption Cryptography Algorithm using Complete Bipartite graphs

Ann Mary George[1], Savitha K.S[2]
[1,2] *Post Graduate and Reseach Department of Mathematics, St. Paul's College, Kalamassery, Cochin, India*
[1]ann397mary@gmail.com, [2]savitha@stpauls.ac.in

Abstract

Graph theory is a branch of Mathematics that focuses on the study of graphs. It is widely used in fields like Computer Science, Engineering and Economics also. One of the key intersections between graph theory and cryptography is in the analysis of graph-theoretic stuctures that can be used for secure cryptographic protocols. A cryptography algorithm in which ciphertext elements can be sent in any order is discussed in [1]. In [6], a unique graph based cryptosystem using bipartite graphs is proposed to guarantee data integrity during user-to-user communication. A new symmetric encryption block cipher that proceeds by representing plaintext messages using disjoint Hamiltonian circuits and then dealing with them as an adjacency matrix in a pre-encryption phase is proposed in [5]. Graph theory helps to represent and analyze complex communication networks, encryption processes, and security protocols in a clear and structured way. By trasforming plaintext and keys into graph structures, it is possible to create encryption schemes that are highly resistant to traditional cryptanalysis. The proposed algorithm uses the concepts from graph theory such as Complete bipartite graphs, their fusion and lexicographic product operation for encryption and decryption processes using matrix-based approaches.

Every integer $n > 1$ can be uniquely written as a product of prime numbers, except for the order of the factors [2]. A pair of vertices a, b in a graph are said to be fused (merged or identified) if the two vertices are replaced by a single new vertex such that every edge that was incident on either a or b or on both is incident on the new vertex [3]. A complete bipartite graph is a special bipartite graph where the vertex set is partitioned into two disjoint sets, U and V, and every vertex in U is adjacent to every vertex in V. It is denoted as $K_{m,n}$, where m and n are the number of vertices in each set [3]. This is an important graph class for network design and modeling relationships.

We define a kind of fusion operation in complete bipartite graphs for the encryption process in this paper, which will make fusion operation reversible.

Let G and H be two graphs. The lexicographic product of the graphs G and H denoted by $G \circ H$ or $G[H]$ is a graph with vertex set containing ordered pairs (u, v) where u is a vertex from G and v is a vertex from H. An edge exists between (u_1, v_1) and (u_2, v_2) if one of the following conditions hold:
a)u_1 is adjacent to u_2 in G.
b)$u_1 = u_2$ and v_1 is adjacent to v_2 in H [4].
From the definition, we get the lexicographic product of graphs with loops and parallel edges also. This product graph is actively researched and has high significance in network analysis and data mining.

In this paper, we use a symmetric algorithm in which each element of plain text is converted to matrices after a series of operations using graphs and matrices. The resulting matrices will be of order at most 6. We use paired keys (k_1, k_2) for double encryption, which provides increased security where each key is a matrix. Even if one key is compromised, the data is still protected. We can encrypt each of the ASCII codes from 0 to 127 is an advantage of this system. Using this algorithm, we can send each ciphertext element in any order since position number is also included while encryption. Brute force attack is not possible in this system because of double encryption and large key space.

References

[1] Binoy Joseph, Bindhu K Thomas. *A new cryptographic method irrespective of code order using graph theory.* Malaya J. Math. (2021)

[2] David M. Burton. *Elementary Number Theory, 6th edition.* Tata McGraw-Hill (2007)

[3] Deo, Narsingh. *Graph Theory with Applications to Engineering and Computer Science.* Dover (2016)

[4] Hausdorff, F. *Grundzüge der Mengenlehre*, Leipzig (1914)

[5] Khalid Bekkaoui, Soumia Ziti, Fouzia Omary. *Data Security: A New Symmetric Cryptosystem based on Graph Theory.* IJACSA (2021)

[6] V.Harsha Shastri, C. Pragathi. *Data Security using Crypto Bipartite Graph Theory with Modified Diffie-Hellman Algorithm.* Springer (2024)