ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.3, 1221–1227
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.3.47 Spec. Issue on RDESTM-2020

SECURE DATA ENCRYPTION WITH GRAPH THEORY

ANU PIUS[1] AND R. BALAKUMAR

ABSTRACT. The requirement for secure communication of messages is the same old thing. It has been available for a very long time. Security in this day and age is one of the significant difficulties. Ciphers can be changed over into graphs for secret communication. The field of Graph Theory assumes an indispensable role in encryption, because of its different properties and its simple portrayal in PCs as a grid. In the current paper, a scalable cryptographic plan to improve the message security is introduced dependent on limited state machines and the graph structure.

1. INTRODUCTION

Cryptography is the study of secret composition with the goal of hiding the significance of a message. Cryptography has for quite some time been the craft of spies and warriors. These days, it is utilized each day by billions of individuals for making sure about electronic mail and installment exchanges. The study of cryptography addresses numerous different controls, both inside arithmetic and software engineering and in engineering. In science, cryptology uses and addresses, variable based math, number theory, graph and cross section theory, mathematical geometry, and likelihood and measurements. Analysis of cryptographic security prompts utilizing hypothetical software engineering particularly intricacy theory. The real usage of crypto systems and the difficult work

[1] *corresponding author*

Key words and phrases. Cryptography, Encryption, Decryption.

of doing security analysis for explicit crypto systems falls into engineering and pragmatic software engineering and processing.

With every encryption algorithm, however, there comes somebody looking to break it. If an adversary continuously intercepts messages, the encryption can be broken given enough time. The time it takes is prohibitively long for most generic attacks on encryptions, so cleverer and more specific attacks are required to bring the time requirement down to acceptable levels. The study of breaking encryption is known as cryptanalysis, and there is a constant struggle between cryptanalysis and cryptography. When a new encryption technique is developed by cryptologists, cryptanalysts will attempt to break it by brainstorming attacks against it. In response to those attacks, the encryption technique is strengthened or a new encryption technique altogether is invented, which prompts the cryptanalysts to figure out new and better attacks, and so on and so forth.

Valuable references in the field are [1-11].

2. Development of the cipher using graph structure

A graph is a pair of sets (V, E) where:

- V is nonempty conventional elements are called nodes or vertices;
- E is a collection of two element subsets of V called edges.

The vertices relate to the dots in the image, and the edges compare to the lines. In this manner, the dots and lines outline above is a pictorial portrayal of the graph (V,E). or then again a graph is triple G=(V, E, ϕ) where ϕ is a capacity with area E and codomain P2(V). The capacity ϕ is in some cases called the rate capacity of the graph.

Characterize the level of $v \in V$ be the number of $e \in E,$ with the end goal that $v \in \phi$ (e): i.e., e is occurrence on v. assume |V| = n, let $d1, d2, ..., dn,$ where $d1 \leq d2 \leq ...dn$ is the sequence of degrees of the vertices of G , arranged by the size. This sequence is alluded to as the degree sequence of the graph G.

Let G= (V, E, ϕ) be a graph. A graph G'= (V', E', ϕ') is a sub-graph of G if $V' \subseteq V$, $E' \subseteq E$ and ϕ is the restriction of ϕ to E'.

On the off chance that for any two components in V, there is a way between two components then G is called associated graph. A cycle in a graph is Hamiltonian cycle for G if each component of V is a vertex of the cycle. A graph

G (V, E, ϕ) is Hamiltonian on the off chance that it has a sub-graph that is a Hamiltonian cycle for G.

The contiguousness network of an undirected graph is symmetric and in this way has a total arrangement of genuine eigen-values and an orthogonal Eigen vector premise. The arrangement of Eigen estimations of a graph is the range of the graph. Assume two coordinated or undirected graphs G1and G2 with nearness frameworks A1 and A2 are given. G1and G2 isomorphic if and just if there exists a stage lattice P with the end goal that $PA1P-1=A2$. Specifically, A1and A2 are comparative and along these lines has the equivalent negligible polynomial, trademark polynomial, eigenvalues, determinant and follow. These can hence fill in as isomorphism invariants graphs. In any case, two graphs may groups a similar arrangement of Eigenvalues however not isomorphic.

In the event that A is the adjacency matrix of the coordinated or uncoordinated graph G, at that point matrix A (for example the matrix result of n duplicates of A) has a fascinating understanding the section in line I and segment j gives the number of (coordinated or undirected) ways of length n from vertex I to vertex j.

The matrix $I-A$ (where I signify the nxn personality matrix) is invertible if and just if there are no coordinated cycles in the graph G. For this situation, the backwards $(I-A)-1$ has the accompanying translation. The passage in line I and segment j gives the number of guided ways from vertex I to vertex j (which is consistently limited if there are no coordinated cycles). This can be comprehended utilizing the geometric arrangement for frameworks:

$$(I-A)-1=I+A+A2+A3+\dots.$$

Graph G is depicted by the square adjacency matrix $A=[a_{\text{ij}}], i,j=1,2,..m$ The components of A fulfill for $I\neq j$, a_{ij}=1, if $v_1, v_2 \epsilon E$ (where vertices v_1, v_2 are associated by an edge). Let f(G) be a capacity that changes over the graph into a number n and f(n) is the converse of the capacity f(G). An adjacency matrix A decides the graph G. the inverse isn't accurate. By permuting vertices of G an assortment of adjacency grids can be created. Subsequently extra data must be given to implement injective property of the mapping. One of the potential outcomes is to fix request of G's vertices. Consider a graph G with five vertices:

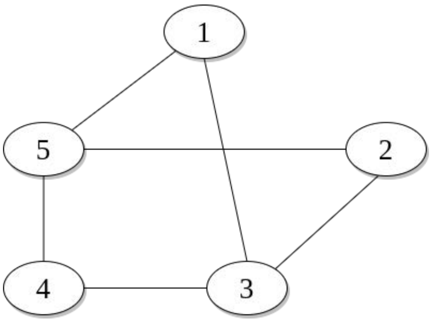

FIGURE 1. Graph

The adjacency matrix for the above graph is as:

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

The adjacency matrix A will be a symmetric matrix, subsequently having all the passages on the principle inclining and all the sections beneath primary corner to corner, one can portray entire matrix (and as the outcome graph G). Thus, it tends to be composed as the sequence $a_{21}a_{31}a_{32}a_{41}a_{42}a_{43}\dots a_{mm}$, $a_{11}a_{22}a_{33}\dots a_{mm}$ where the initial segment ($a_{21}a_{31}a_{32}....a_{m(m-1)}$) compares to all the sections underneath fundamental slanting (graph structure), while the second ($a_{11}a_{22}a_{33}\dots a_{mm}$) to the principle askew itself. Henceforth the proportional code for the adjacency matrix is n=011001110111001 sent as secret key. This portrayal isn't special so it turns out to be exceptionally hard for the eve dropper to break the code even the key is known.

3. ENCRYPTION

Let plain text P be a square matrix of order n.

- Define Mealy/Moor public channel machine.
- Send adjacency matrix as key in binary form to the receiver.

- Define the cipher text at $q(i+1)^{th}$ state [Cipher text at $q(i+1)^{th}$ state is equal to the cipher text at $q(i)^{th} state * (adjacencymatrix)$ output at $q(i+1)^{th}$ state]
- Send the cipher text to the receiver.
- Decrypt the message using the inverse operation on the cipher text to get the original message.

3.1. **Mathematical Work.** Algorithm proposed is a basic utilization of the Hill ciper utilizing adjacency matrix. Number of rounds relies upon the Adjacency matrix (secret key). It is exceptionally hard to break the figure content without appropriate key and the picked limited state machine.

3.2. **Strength of the key.** Strength of the secret key depends on the adjacency matrix.

3.3. **Rounds.** The number of rounds relies upon the secret key utilized and the chosen finite state machine. It is extremely hard to figure the number of rounds and the repeat matrix without an able secret key.

3.4. **Time calculation.** Let the aggregate of the yields of the finite state machine for k bit secret key is r. leave tm alone the time required for every duplication and ta be the time required for every expansion. At that point the all out time required for k bit secret key is:

$$r(n3tm + n(n-1)ta).$$

4. Analysis of Security

To extricate the first data, it is troublesome because of the picked finite state machine. Animal power assault on key is likewise troublesome because of the expansion in key size.

TABLE 1. Security Analysis

S.No.	**Name of the attack**	**Possibility of the attack**	**Remarks**
1.	Known plain text attack	Not Easy	Because of the chosen finite state machine and the activity matrix duplication.
2.	Cipher text attack	Very difficult	Because of the secret key, chosen finite state machine and adjacency matrix.
3.	Adaptive chosen plain text attack	Difficult	On account of the chosen finite state machine and the activity matrix duplication.
4.	Chosen plain text attack	Difficult	Because of the chosen finite state machine and the activity matrix augmentation.
5.	Adaptive chosen cipher text attack	Very Difficult	Because of the secret key, chosen finite state machine and adjacency matrix
6.	Chosen cipher text attack	Very Difficult	Because of the secret key, chosen finite state machine and the adjacency matrix.

5. CONCLUSION

Robust usage of the secure information of the executives is basic to the message change. In the current paper, a scalable cryptographic plan to upgrade the message assurance is introduced dependent on finite state machines and the activity matrix increase Secrecy is kept up at three levels, the secret key, the picked finite state machine, and the request for the vertices in the picked adjacency matrix. The acquired figure content turns out to be very hard to break or to separate the first data regardless of whether the algorithm is known. Along these lines a progressively dependable cryptosystem can be acknowledged with a solitary secret key.

References

[1] N. Deo: *Graph Theory with Applications to Engineering and Computer Science*, Prentice Hall, 2010.

[2] M. Gawannavar, P. Mandulkar, R. Thandeeswaran, N. Jeyanthi: *Office in cloud: Approach to Authentication and Authorization*, Recent Advances in Communications and Networking Technology, Bentham sciences, **4**(1) (2015), 49–55.

[3] K. E. Vengatesan, S. Kumar, S. Yuvaraj, P. S. Tanesh, A. Kumar: *An Approach for Remove Missing Values in Numerical and Categorical Values Using Two Way Table Marginal Joint Probability*, International Journal of Advanced Science and Technology, **29**(5) (2020), 2745–2756.

[4] F. Amounas: *Enhanced Elliptic Curve Encryption Approach of Amazigh alphabet with Braille representation*, International Journal of Computer Science and Network Solutions, **3**(8) (2015), 1–9.

[5] B. Siva Kishore, J. S. Theja Reddy, N.Jeyanthi: *Three Phase Power Management Algorithms for Green Cloud Computing*, International Journal of Applied Engineering Research, **8**(1) (2013), 1725–1736.

[6] N. Jeyanthi, R. Thandeeswaran, J. Vinithra: *RQA Based Approach to Detect and Prevent DDoS Attacks in VoIP Networks*, Cybernetics and Information Technologies, **14**(1) (2014), 11–24.

[7] A. Amrutha, R. Thandeeswaran, N. Jeyanthi: *Cloud based VoIP Application in Aircraft Data Networks*, International Journal of Grid Distribution Computing, **7**(6) (2014), 11–18.

[8] N. Tokareva: *Connections between graph theory and cryptography,* G2C2: Graphs and Groups, Cycles and Coverings, 24–26, 2014, Novosibirsk, Russia.

[9] R. P. Singh, Vandana: *Application of Graph Theory in Computer Science and Engineerin*, International Journal of Computer Applications, **104**(1) (2014), 09758887.

[10] K. R. Sandeep Narayan, M. S. Sunitha: *Connectivity in a Fuzzy Graph and its Complement*, ICRS, **9** (2012), 38–43.

[11] S. Mathew, M. S. Sunitha, N. Anjali: *Some Connectivity Concepts in Bipolar Fuzzy Graphs*, Annals of Pure and Applied Mathematics, **7** (2014), 98–108.

Department of Mathematics
PRIST Deemed to be University
Thanjavur
E-mail address: anupius06@gmail.com

Department of Mathematics
PRIST Deemed to be University
Thanjavur
E-mail address: balaphdmaths@gmail.com