A cryptographic method to send a secret route or map to a receiver using concepts in graph theory and number theory

S.A.S. Sureni Wickramasooriya, Thisal M. Weerasekara, G.H. Jayantha Lanel, T.P. de Silva, N.C. Ganegoda

Abstract— **Even though new solutions for problematic situations arising from security norms are developing day by day, possibly there are some issues remaining on our hand yet to be tackled. Among those one of the major problem for almost every country might experience is routing and mapping secrecy. In detail, when sending someone's route of some places or sending a map of protectorate places, its secrecy is the most important factor to be considered. In this study a system is developed which could be used to send a route of a particular person or a map of some specific secret place in a secret manner. Concepts in graph theory and number theory together with some cryptographic algorithms are used to develop this system. In brief, the route or map is transformed into a graph which might be directed or non-directed. Then it simplified in to a numerical value which could be encrypted by applying particular encrypting algorithm. Thereafter, encrypted numerical code is sent to the receiver. Once receiver receives that unreadable code then he/she applies decrypting algorithm on that to obtain the original numerical value. Finally, the graph can be derived from that numerical value and it could be regarded as the map or route that has been sent. However different methods are followed to send the map or route due to the directivity of the graph. Although there are some restrictions and assumptions which have been made during the process, there may be possibilities to further improve this system.**

Index Terms— **Cipher text, Decryption, Directed graph, Encryption, Non-directed graph.**

I. INTRODUCTION

Cryptography has played an enormous role in the shaping and development of many societies and cultures. Cryptography probably began in or around 2000 B.C. in Egypt, where hieroglyphics were used to decorate tombs of deceased rulers and kings which represents the story of the life of the king and proclaimed the great acts of his life. Cryptography is the science that has been used for many years to translate messages into secret format and getting the real message from the secret format. Though cryptography has begun with very small techniques such as symbols, with the rise of the information age, computers have bought it to a whole new level. In 1553, Giovan Batista Belaso came up with idea of the password. In world war II, mechanical and electromechanical cipher machines were widely used.

S.A.S. Sureni Wickramasooriya, Department of Mathematcs, Faculty of Engineering, University of Moratuwa, Sri Lanka, +94716961356.
Thisal M. Weerasekara, Department of Mathematcs, Faculty of Applied Sciences, University of Sri Jayewardenepura, Sri Lanka, +94714480113**G.H. Jayantha Lanel**, Department of Mathematcs, Faculty of Applied Sciences, University of Sri Jayewardenepura, Sri Lanka, +94112758384
T.P. de Silva, Department of Mathematcs, Faculty of Applied Sciences, University of Sri Jayewardenepura, Sri Lanka, +94112758377
N.C. Ganegoda, Department of Mathematcs, Faculty of Applied Sciences, University of Sri Jayewardenepura, Sri Lanka, +94112758380

In some situations, one's route should be very critical and secret. As an example, when the leader of a country is in an official visit to the part of his own country or to another country, that visit should be very secret. If his route is disclosed by enemy there may arise many security and confidential problems. Therefore this emphasizes the necessity of possessing a route in a secret way for an imperative person.

The protection of routes in a plan of protector places such as military camps is very essential. Therefore the other application is based on sending a secret map to a recipient in a secure manner. If there is no any proper method of sending the map in a secret way there will be malignant attacks. The combination of cryptographic algorithms and graph theoretical concepts can be used to solve these problematic situations up to some extent. In brief, the objective of this research is to convert a graph or map into an encrypted numerical value which can be easily sent to a receiver without any hesitation. Furthermore this contains the process of building up the secret map or route by the receiver. More importantly software with MATLAB which could implement this procedure by generating the numerical value from the graph and decrypting it to generate the graph back is developed to give more reliable solution.

II. METHODOLOGY

The first step is converting the map or route in to a graph. Here the roads are represented by edges and junctions or cities or countries can be represented by vertices. Map is represented by a non-directed graph while the route is represented by a directed graph. Then the constructed graph is transformed into adjacency matrix. A new procedure is followed to calculate the numerical value from the adjacency matrix. Calculation part varies according to the directivity (a map or route) of the graph.

Sending a secret map and reconstructing back

Let takes the adjacency matrix of the graph as, $A = \{a_{ij}\}$ where $a_{ij} \in \{0,1\}$ with $a_{ii} = 0$ for $i, j = 1,2, \ldots, n$

In this approach, the graph related to map is symmetric. Due to the symmetric attribute of non-directed graph, the upper triangular matrix is equal to the transpose of lower triangular matrix.
Generally, the adjacency matrix can be represented as follows.

$$A = \begin{pmatrix} 0 & a_{12} & \ldots\ldots\ldots & a_{1n} \\ a_{12} & 0 & \ldots\ldots\ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ a_{1(n-1)} & a_{2(n-1)} & \vdots & a_{(n-1)2} \\ a_{1n} & a_{2n} & \vdots & 0 \end{pmatrix}$$