Graph-Based Cryptosystem

Riset Internasional ITB

Rinovia Simanjuntak [1], Sanming Zhou [2], Hilda Assiyatun [1], Aleams Barra [1], Finny Oktariani [1]

[1] Faculty of Mathematics and Natural Science, Institut Teknologi Bandung
[2] School of Mathematics and Statistics, University of Melbourne

Abstract

In the digital era where data has become the "new oil," data security has become one of the critical issues in information technology, computer science, and the mathematics that underpins them. Without adequate protection, the risks arising from data being accessed by unauthorized parties can have far-reaching impacts, from the individual level to the global level.

In recent years, cryptographic schemes based on graph labeling have been extensively studied by researchers. The method used involves transforming data into a complex graph structure in which each vertex and edge is assigned a special label, so that the encryption and decryption of data can be carried out by exploiting the special properties of the graph under study.

We introduce two new antimagic labelings in oriented graphs and propose a cryptosystem scheme based on such labelings.

Keyword: graph labelling, antimagic labelling, graph based cryptosystem

Introduction

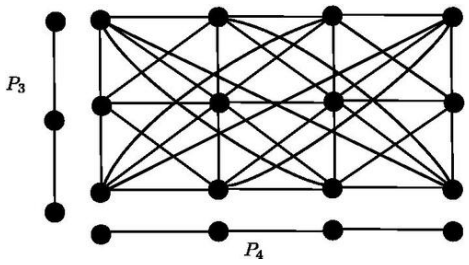
In the digital era where data has become the "new oil," data security has become one of the critical issues in information technology, computer science, and the mathematics that underpins them. Without adequate protection, the risks arising from data being accessed by unauthorized parties can have far-reaching impacts, from the individual level to the global level. Some examples of risks that have occurred in Indonesia include: the BPJS Kesehatan (National Health Insurance) data breach (2021), which affected 279 million citizen records, and the cyberattack on Tokopedia (2020), which exposed 91 million user records.

In recent years, cryptographic schemes based on graph labeling have been extensively studied by researchers. The method used involves transforming data into a complex graph structure in which each vertex and edge is assigned a special label, so that the encryption and decryption of data can be carried out by exploiting the special properties of the graph under study. This will naturally make it difficult for unauthorized parties to decrypt the data without the correct key.

In this research, we collaborate with a partner from the University of Melbourne, Prof. Sanming Zhou. Additionally, this research is also part of the dissertation work of three of our doctoral students, Risma Yulina Wulandari, M.Si, Hassan Pervaiz, M.Sc., and Ahmad Muchlas Abrar, M.Si.

Research Method

We construct a cryptographic scheme based on D-antimagic labeling, a variant of antimagic labeling, which we introduced in 2021. This research is divided into two parts. In the first part, we conduct a theoretical study on the construction of D-antimagic labeling and D-antimagic group labeling, on both undirected and directed (oriented) graphs. In the second part, we will apply the labelings obtained in the first part to construct cryptographic schemes.



Picture 1. Lexicographic product of two paths

The research has the following objectives:

1. Constructing D-antimagic labeling on Cayley graphs,
2. Introducing A-D-antimagic labeling on oriented graphs,
3. Designing encryption and decryption schemes based on the labelings in 1 and 2,
4. Designing encryption and decryption algorithms based on the schemes in 3, and
5. Implementing the algorithms in 4 and comparing the performance of the scheme with previously studied data security schemes based on graph labeling.

To demonstrate the existence of D-antimagic labeling for Cayley graphs (Objective 1), we use two non-constructive methods: the probabilistic method introduced by Erdős [3,4] and the polynomial method (Combinatorial Nullstellensatz) introduced by Alon [2]. In applying these methods, we weaken the labeling to an injection and conduct a study on the minimum largest label used in that injection.

As for the encryption scheme we propose in Objective 3, it consists of two stages:

1. Encryption-1, using D-antimagic labeling on the graph representing the plaintext to obtain ciphertext-1, followed by
2. Encryption-2, using the Vigenère Cipher on ciphertext-1 to obtain ciphertext-2.

We perform both stages because ciphertext-1 undergoes a character reduction compared to the plaintext, thereby providing fewer clues for decryption. In this way, we apply a double filtering on the plaintext, which is expected to make cryptanalysis extremely difficult to perform.

Discussion and Results

Some advantages of using graph labeling-based data security are in terms of:

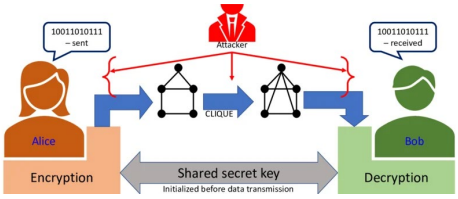
Complexity: The complex structure of a graph with many edges and labeling possibilities makes brute-force attacks extremely difficult.

Key management: The encryption key is a labeling scheme, which, in addition to being asymmetric, can also be managed more efficiently compared to commonly used symmetric keys.

Flexibility: Various graph labelings can be used based on the data type and encryption requirements.

The results of this research are:

1. Two new antimagic labelings for oriented graphs and the study of the properties of those labelings,
2. The study of sharp bounds for outer multiset dimension of joint and lexicographic products of arbitrary graphs with a complete graph and its complement,
3. A proposed cryptosystem scheme based on antimagic labelings.



Picture 2. Proposed cryptosystem scheme

Publication

1. “Outer multiset dimensions of (extended) corona product graphs”, *Electronic Journal of Graph Theory and Applications* **14** (2) (2026), 485–505 (Q2)
2. "D-Antimagic and D-Magic Arc Labelings of Oriented Graphs“, submitted to *Electronic Journal of Graph Theory and Applications* (Q2)
3. "Outer Multiset Dimension of Lexicographic Product Graphs“, submitted to *Proceedings - Mathematical Sciences* (Q2)
4. “Antimagic Labelings via Probabilistic Method”, draft, to be submitted to *Lecture Notes in Computer Science* (Q2)
5. “D-magic and antimagic labelings of hypercubes”, draft, to be submitted to *SIAM Journal of Discrete Mathematics* (Q1)