Indonesian Journal of Combinatorics

www.ijc.or.id

ISSN: 2541-2205

Indonesian Journal of Combinatorics

Indonesian Journal of Combinatorics (IJC) publishes current research articles in any area of combinatorics and graph theory such as graph labelings, optimal network problems, metric dimension, graph coloring, rainbow connection and other related topics.

IJC is published by the Indonesian Combinatorial Society (InaCombS), CGANT Research Group Universitas Jember (UNEJ), and Department of Mathematics Universitas Indonesia (UI).

All papers will be refereed in the normal manner of mathematical journals to maintain the high standards. IJC is an open access journal. Full-text access to all papers is available for free.

This journal is sponsored by Indonesian Mathematical Society (IndoMS) and Faculty of Mathematics and Natural Sciences - Institut Teknologi Bandung (ITB) Indonesia.

Indonesian Journal of Combinatorics (IJC) has been accredited by National Journal Accreditation (ARJUNA) Managed by Ministry of Research, Technology, and Higher Education, Republic Indonesia with Second Grade (Sinta 2) since 2017 to 2022 according to the decree No. 10/E/KPT/2019.

Vol 4, No 1 (2020)

Indonesian Journal of Combinatorics Vol. 4 No. 1 (2020)

Table of Contents

Articles

ISSN: 2541-2205

Indonesian Journal of Combinatorics
www.ijc.or.id

ISSN: 2541-2205

Vol 4, No 1 (2020)

Indonesian Journal of Combinatorics Vol. 4 No. 1 (2020)

Table of Contents

Articles

ISSN: 2541-2205

Indonesian Journal of Combinatorics
www.ijc.or.id

ISSN: 2541-2205

Publication Ethics

Publication Ethics and Malpractice Statement

Indonesian Journal of Combinatorics is a peer-reviewed journal. This statement clarifies the ethical behavior of all parties involved in the act of publishing an article in this journal, including the editorial board, editors, authors, peer reviewers and the publisher (Indonesian Combinatorial Society, CGANT Research Group Universitas Jember, and Department of Mathematics Universitas Indonesia). This statement is based on COPE's best practice guidelines for editors of journals.

Ethical Guideline for Journal Publication

The publication of an article in Indonesian Journal of Combinatorics is an essential element in the development of a coherent and respected network of knowledge. It directly reflects the quality of the work of the authors and the institutions that support them. The peer-reviewed articles support and embody the scientific method. It is therefore important to agree on the ethical behavior standards expected of all parties involved in the publication act: the author, the editor of the journal, the reviewer, the publisher and the society.

Indonesian Combinatorial Society, CGANT Research Group Universitas Jember, and Department of Mathematics Universitas Indonesia as the publishers of Indonesian Journal of Combinatorics takes the supervisory duties on all stages of publishing extremely seriously and we recognize our ethical and other responsibilities. We are committed to ensuring that advertising, reprinting or other commercial revenues have no impact or influence on editorial decisions. In addition, publishers and the editorial board will help to communicate with other journals as well as publishers if it is useful and necessary.

Publication Decisions

The editors of the Indonesian Journal of Combinatorics are responsible for deciding which of the articles submitted to the journal should be published. The validation of the work in question and its importance for researchers and readers must always lead to such decisions. The editors may be guided by the policies of the editorial board of the journal and constrained by the legal requirements that will then apply in respect of defamation, copyright infringement and plagiarism. In making the decision, the editors may confer with other editors or reviewers.

1. *Fair play*

Editors evaluate manuscripts only based on their intellectual content, regardless of race, gender, sexual orientation, religious belief, ethnic origin, citizenship or political philosophy of the authors.

2. *Confidentiality*

The editor and any editorial team shall not disclose any information on a manuscript submitted to anyone other than the authors, reviewers, prospective reviewers, other editorial advisors and the publisher, as the case may be.

3. *Disclosure and conflicts of interest*

Unpublished materials disclosed in a submitted manuscript must not be used in any form of an editor's own research without the written consent of the author.

Duties of Reviewers

1. *Contribution to Editorial Decisions*

The peer review helps the editor make editorial decisions. It can also help the author to improve the paper, through editorial communications with the author.

2. *Promptness*

Any chosen referee who does not feel qualified to review the research reported in a manuscript or knows that he/she would not be able to review on time should inform the editor and apologize for the review process.

3. *Privacy Policy*

All manuscripts received for review should be treated as confidential documents. They must not be presented or discussed with others unless authorized by the editor.

4. *Objectivity*

Reviews must be carried out objectively. The personal criticism of the author is

inappropriate. Referees must clearly articulate their points of view with supporting arguments.

5. *Acknowledgement of Sources*

Reviewers should identify relevant published works that have not been cited by the authors. Any statement containing an observation, derivation, or argument had been previously reported should be presented with the relevant citation. A reviewer should also draw the editor's attention to any substantial similarity or overlap between the manuscript under consideration and any other published document of which they have personal knowledge.

6. *Disclosure and Conflicts of Interest*

Insider information or ideas obtained through peer review should be kept confidential and not used for personal purposes. Reviewers should not consider manuscripts in which they have conflicts of interest arising from competitive, collaborative or other relationships or connections with the authors, corporations, or institutions related to the manuscripts.

Duties of Authors

1. *Reporting Standards*

Authors of original research reports must provide an accurate account of the work done and an objective discussion of its importance. The underlying data must be accurately represented in the manuscript. A manuscript should contain enough details and references to allow others to reproduce the work. Fraudulent or knowingly incorrect statements are unethical and unacceptable.

2. *Data Access and Retention*

The authors should give a public access to raw data (if any) in relation to the editorial review. This data should be retained even for a necessary time after publication.

3. *Originality and Plagiarism*

Authors must guarantee that their works are entirely original and any citations for other works and/or words in the manuscript have been properly done.

4. *Multiple, Redundant or Simultaneous Publication*

An author should generally not publish manuscripts containing essentially the same results in more than one primary journal or publication. Simultaneous submission of the same manuscript to more than one journal is considered unethical and unacceptable.

5. *Recognition of Sources*

Appropriate recognition of the work of others must always be given. Authors must cite publications that have influenced the nature of the work reported.

6. *Authorship*

Authorship should be limited to those who have contributed significantly to the reported research results. All those who have made significant contributions should be listed as co-authors. If there are others involved in some of the substantive aspects of the research project, then they should be acknowledged or listed as contributors. The corresponding author must ensure that all appropriate co-authors are included in the manuscript and that all co-authors have seen and approved the final version of the manuscript and agreed to the submission for publication.

7. *Disclosure and Conflicts of Interest*

All authors must disclose in their manuscripts any financial or other conflicts of interest that could be interpreted as having an influence on the results or interpretation of their manuscript. All sources of financial support for the project should be disclosed.

8. *Fundamental Errors in Published Works*

When an author discovers a significant error or inaccuracy in his/her own published work, it is the author's duty to promptly inform the editor or publisher of the journal and cooperate with the editor to retract or correct the paper.

ISSN: 2541-2205

Indonesian Journal of Combinatorics
www.ijc.or.id

ISSN: 2541-2205

Editorial Team

Honorary Editors

Edy Tri Baskoro, Institut Teknologi Bandung, Indonesia
Martin Baca, Technical University, Kosice, Slovakia

Editors in Chief

S Slamin, Universitas Jember, Indonesia
Kiki A. Sugeng, Universitas Indonesia, Indonesia

Managing Editors

Tita Khalis Maryati, Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta, Indonesia
Anak Agung Gede Ngurah, Universitas Merdeka Malang, Indonesia

Editorial Board

Ali Ahmad, Jazan University, Saudi Arabia
Jose Maria Balmaceda, University of the Philippines - College of Science, Philippines
Sylwia J Cichacz-Przenioslo, AGH University of Science and Technology, Poland
Faqir Muhammad Bhatti, Lahore University of Management Sciences, Pakistan
Nurdin Hinding, Universitas Hasanuddin, Indonesia
Hazrul Iswadi, Universitas Surabaya, Indonesia
Chula Jayawardene, University of Colombo, Sri Lanka
Tri Atmojo Kusmayadi, Universitas Sebelas Maret, Indonesia
Yuqing Lin, The University of Newcastle, Australia
Nacho Lopez, Universidad de Lleida, Spain
P Purwanto, Universitas Negeri Malang, Indonesia
Suhadi Wido Saputro, Institut Teknologi Bandung, Indonesia
Saib Sawilo, Universitas Sumatera Utara, Indonesia
Andrea Semanicova-Fenovcikova, Technical University of Kosice, Slovakia
I Wayan Sudarsana, Universitas Tadulako, Indonesia
Tao-Ming Wang, Tunghai University, Taiwan
Maria Zdimalova, Slovak University of Technology - Bratislava, Slovakia

Layout Editors

Kristiana Wijaya, University of Jember, Indonesia
Ikhsanul Halikin, University of Jember, Indonesia

ISSN: 2541-2205

Indonesian Journal of Combinatorics
www.ijc.or.id

ISSN: 2541-2205

People

Reviewer

A Amrullah, Universitas Mataram, Indonesia

Diari Indriati, Universitas Sebelas Maret Surakarta, Indonesia

Rafiantika Prihandini, University of Jember, Indonesia

Lilik Susilowati, Airlangga University, Indonesia

Novi Bong, University of Delaware, United States

Kristiana Wijaya, University of Jember, Indonesia

Bryan Freyberg, University of Minnesota Duluth, United States

Chula Jayawardene, University of Colombo, Sri Lanka

Roslan Hasni, University Malaysia Terengganu, Malaysia

A. Asmiati, University of Lampung, Indonesia

Anak Agung Gede Ngurah, Universitas Merdeka Malang, Indonesia

Maria Zdimalova, Slovak University of Technology - Bratislava, Slovakia

Tita Khalis Maryati, Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta, Indonesia

I Wayan Sudarsana, Universitas Tadulako, Indonesia

Nurdin Hinding, Universitas Hasanuddin, Indonesia

Yuqing Lin, The University of Newcastle, Australia

D Dafik, University of Jember, Indonesia

Ridho Alfarisi, Universitas Jember, Indonesia

ISSN: 2541-2205

Indonesian Journal of Combinatorics
www.ijc.or.id

ISSN: 2541-2205

PUBLICATION ETHICS
REVIEWERS
STATISTICS
INDEXING

AUTHOR GUIDELINES
ONLINE SUBMISSION
REGISTER
DOWNLOAD TEMPLATE

USER
Username
Password
Remember me
Login

JOURNAL CONTENT
Search
Search Scope
All
Search

Browse
- By Issue
- By Author
- By Title

HOME ABOUT LOGIN REGISTER SEARCH CURRENT ARCHIVES

Home > **Indexed By:**

Indexed By:

ISSN: 2541-2205

Indonesian Journal of Combinatorics
www.ijc.or.id

ISSN: 2541-2205

Randomness of encryption keys generated by super H-antimagic total labeling

Antonius Cahya Prihandoko, Yudha Alif Auliya, Diksy Media Firmansyah, S Slamin

Abstract

SuperH-antimagic total labeling (SHATL) can be utilized to generate encryption keys. The keys are then used to establish the improved block and stream ciphers. In these ciphers, different blocks were encrypted by the different keys, but all block keys were connected one another. These conditions make the developed cryptosystems more secure and require less keys storage capacity compared to the ordinary block and stream cipher. The randomness of the generated keys, however, still need to be tested. The test is necessary to ensure that there is no specific pattern that can be utilized by any intruder to guess the keys. This paper presents the randomness tests applied to all key sequences generated by both the improved block scheme and the stream based scheme.

Keywords

randomness; encryption keys; super H-antimagic total labeling; cryptography; block cipher; stream cipher

Full Text:

PDF

DOI: http://dx.doi.org/10.19184/ijc.2020.4.1.3

References

P.M. Alcover, A. Guillamon, M.C. Ruiz, A New Randomness Test for Bit Sequence, Informatica, 24(3), (2013), 339-356

M. Baca, L. Brankovic, M. Lascsakova, O., Phanalasy, A. Semaniˇcov´a-Feˇnovˇc´ıkov´a, On d-antimagic labelings of plane graphs, Electr. J. Graph Theory Appli., 1(1), (2013), 28-39

Dafik, A.K. Purnapraja, R Hidayat, Cycle-Super Antimagicness of Connected and Disconnected Tensor Product of Graphs, Procedia Computer Science, 74, (2015), 93-99

Dafik, Slamin, D. Tanna, A. Semaniˇcov´a-Feˇnovˇc´ıkov´a, M. Baˇca, Constructions of Hantimagic graphs using smaller edge-antimagic graphs, Ars Combinatoria, 100 (2017), In Press

Dafik, M. Hasan, Y.N. Azizah, I. H. Agustin, A Generalized Shackle of Any Graph H Admits a Super H-Antimagic Total Labeling, Mathematics in Computer Science Journal, (2016). Submitted

P. L'Ecuyer, Testing Random number Generators, Proceedings of the 1992 Winter Simulation Conference, IEEE Press, Dec. (1992), 305-313.

A.C. Prihandoko, Dafik, I.H. Agustin, D. Susanto, A.I. Kristiana, Slamin, The Construction of Encryption Key by Using a Super H-antimagic Total Graph, Program and Abstract the Asian Mathematical Conference, AMC (2016), 408, ISBN 978-602-74668-0-7.

A.C. Prihandoko, Dafik, I.H. Agustin, Implementation of Super H-Antimagic Total Graph on Establishing Stream Cipher, Indonesian Journal of Combinatorics, 3(1), 2019, pp. 14-23.

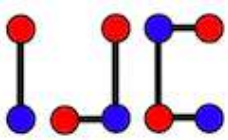
M.E. Whitman, H.J. Mattord, Principles of Information Security, (2012), Boston: Course Technology

Refbacks

- There are currently no refbacks.

ISSN: 2541-2205

Indonesian Journal of Combinatorics **4** (1) (2020), 21–26



INDONESIAN JOURNAL
OF COMBINATORICS

Randomness of encryption keys generated by super H-antimagic total labeling

Antonius Cahya Prihandoko[a], Yudha Alif Auliya[a], Diksy Media Firmansyah[b], Slamin[b]

[a]*Department of Information Technology, Universitas Jember, Jl. Kalimantan 37 Jember, Indonesia*
[b]*Department of Informatics, Universitas Jember, Jl. Kalimantan 37 Jember, Indonesia*

antoniuscp.ilkom@unej.ac.id, yudha.alif@unej.ac.id, diksy@unej.ac.id, slamin@unej.ac.id

Abstract

Super H-antimagic total labeling (SHATL) can be utilized to generate encryption keys. The keys are then used to establish the improved block and stream ciphers. In these ciphers, different blocks were encrypted by the different keys, but all block keys were connected one another. These conditions make the developed cryptosystems more secure and require less keys storage capacity compared to the ordinary block and stream cipher. The randomness of the generated keys, however, still need to be tested. The test is necessary to ensure that there is no specific pattern that can be utilized by any intruder to guess the keys. This paper presents the randomness tests applied to all key sequences generated by both the improved block scheme and the stream based scheme.

Keywords: randomness, encryption keys, super H-antimagic total labeling, crypto-graphy, block cipher, stream cipher
Mathematics Subject Classification: 05C78
DOI: 10.19184/ijc.2020.4.1.3

1. Introduction

A characteristic that is essential in the context of information security is confidentiality. Information is said to be confidential when it is protected from disclosure to unauthorized persons or systems. Cryptography is a popular approach to achieve information confidentiality. In this approach, information is initially encrypted before it is delivered through unsecure channels. The strength of encryption protocols depends on the encryption-decryption keys management: the keys

Received: 31 May 2019, Revised: 14 April 2020, Accepted: 27 May 2020.

have to be kept secret to unauthorized parties. Indeed, keeping the keys from being accessible to unauthorized parties is the major challenge for many cryptographic schemes.

Researches on the encryption-decryption keys management are continuously undertaken and focused to achieve information confidentiality according to the required security level. In previous works [7, 8], encryption keys were generated using super H-antimagic total labeling (SHATL). A bijective function f is called an (a,d)-H-antimagic total labeling of graph G if $f : V(G) \cup E(G) \rightarrow \{1, 2, \ldots, |V(G)| + |E(G)|\}$ such that for all subgraphs of G isomorphic to H, the total H-weights $w(H) = \sum_{v \in V(H)} f(v) + \sum_{e \in E(H)} f(e)$ form an arithmetic sequence $\{a, a+d, a+2d, ..., a+(n-1)d\}$, where a and d are positive integers and n is the number of all subgraphs of G isomorphic to H. Additionally, if $f : V(G) \rightarrow \{1, 2, \ldots, |V(G)|\}$, then the (a,d)-H-antimagic total labeling f is called super.

The encryption keys were constructed from the SHATL of a *generalized shackle* of graph. A *shackle* of graph H, symbolized by $G = shack(H, v, n)$, is a graph G developed by non-trivial graphs $H_1, H_2, \ldots, H_n$, such that for every $1 \leq s, t \leq n$, with $|s - t| \geq 2$, H_s and H_t have no common vertex, but for every $1 \leq i \leq n-1$, H_i and H_{i+1} have precisely one common vertex v, called *connecting vertex*, and all $n-1$ connecting vertices are different. A *generalized shackle* of graph, denoted by $G = gshack(H, K \subset H, n)$, is the graph obtained from $G = shack(H, v, n)$ by substituting the connecting vertex by any subgraph $K \subset H$. The existence of super (a,d)-H antimagic total labeling of *generalized shackle* of graph was proved using an *integer set partition technique* [2, 4]. This proof guarantee that constructing encryption keys using SHATL is feasible.

The constructed keys were utilized to establish the improved block and stream ciphers. The developed cryptosystems have been proved to be more secure and require less keys storage capacity compared to the ordinary block and stream cipher [7, 8]. A randomness test, however, still needs to be applied to the generated keys. This kind of test is needed to ensure that there is no specific pattern that can be utilized by any intruder to guess the key. This paper presents the randomness tests applied to all key sequences generated using SHATL both in the improved block scheme and the stream based scheme.

The rest of this paper is outlined as follows. Section 2 presents the mechanism of constructing encryption keys both in the block scheme and the stream cipher using SHATL. Section 3 describes the randomness of the keys sequences generated by SHATL.

2. Utilizing SHATL to Construct Encryption Keys

In order to simulate the randomness of key sequences generated using SHATL, let us recall the SHATL algorithm for constructing encryption key in a block cipher [7] and the algorithm for generating key stream using SHATL [8]. For the former, assume that the cryptosystem is working on 26 English alphabets. Constructing encryption keys using super $(a,d) - H$ antimagic total labeling of *generalized shackle* of graph is undertaken through the algorithm 1.

Algorithms 1. **SHATL Algorithm for constructing encryption keys**

```
1. Assign f as label of the graph elements
2. If f is bijection, do 3, otherwise back to 1
3. Take a certain d for super (a,d)-HATL
4. Take z = sum of the number of vertices and 26
```

```
5. Draw the layered diagram by ignoring all labels greater than z
6. Place all edge labels in sequence from left to right
   and start from the top to the bottom layer.
7. Use the sequence of labels as the encryption keys
```

Generating a key stream is undertaken by modifying algorithm 1. Assume that the cryptosystem is working on 26 English alphabets. The key stream construction is proceed through the algorithm 2.

Algorithms 2. **Algorithm for generating key stream**

1. Define f for labeling the graph elements
2. If f is bijection, do 3, otherwise back to 1
3. Take a certain d for super (a,d)-HATL
4. Take z = the number of vertices plus 26
5. Draw the layered diagram by ignoring all labels greater than z
6. Place all edge labels in sequence from left to right and start from the top to the bottom layer.
7. Name the sequence by s and let t = length of s
8. Use the sequence s of labels as the source of key stream
9. Determine b = length of block
10. Determine i, such that $1 \leq i \leq t - b$
11. Take $k = s_i, s_{i+1}, s_{i+2}, ..., s_{i+b-1}$ as initial block key
12. Determine stream function $k_{j+b} = g(k_j, k_{j+1}, ..., k_{j+b-1})$

Outputs of algorithm 2 are the initial block key k and the stream function $g(k)$.

3. Randomness of the Constructed Key Sequences

A single SHATL can be used to construct a key sequence in a block cipher and multiple key sequences in a stream cipher. For the simulation, the randomness test is applied to all sequences generated from Super $(a, 12) - H$ ATL of the graph G that was provided in [7]. The labeling is illustrated in Figure 1. It shows that the vertex and edge labels start from 1 to 30 and 31 to 79, respectively.

A layered diagram rooted at label 1 is then drawn by ignoring the labels greater than 56 (Figure 2). The sequence obtained from the diagram is 31, 39, 48, 52, 54, 40, 50, 49, 51, 53, 55, 47, 32, 36, 56, 43, 46, 33, 37, 42, 45, 34, 38, 41, 44, 35, or (in its equivalence modulo 26) 5, 13, 22, 0, 2, 14, 24, 23, 25, 1, 3, 21, 6, 10, 4, 17, 20, 7, 11, 16, 19, 8, 12, 15, 18, 9.

We then use sequence s = 5, 13, 22, 0, 2, 14, 24, 23, 25, 1, 3, 21, 6, 10, 4, 17, 20, 7, 11, 16, 19, 8, 12, 15, 18, 9 as the base sequence. As the randomness test requires a sequence with minimum length is 40, then s can be enlarged by repeating previous components in the context of block cipher key. Therefore, the block cipher key that meet the requirement should be s_b = 5, 13, 22, 0, 2, 14, 24, 23, 25, 1, 3, 21, 6, 10, 4, 17, 20, 7, 11, 16, 19, 8, 12, 15, 18, 9, 5, 13, 22, 0, 2, 14, 24, 23, 25, 1, 3, 21, 6, 10.

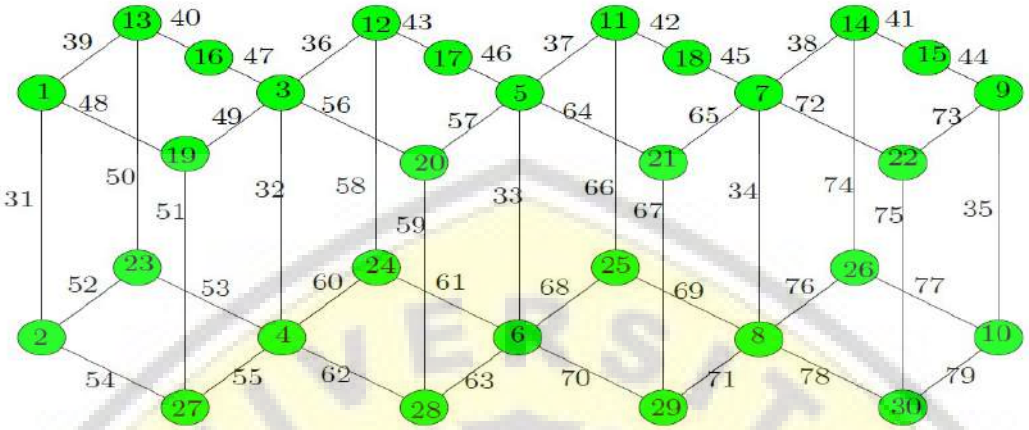


Figure 1. Super $(a, 12) - H$ ATL of a *generalized shackle* of graph

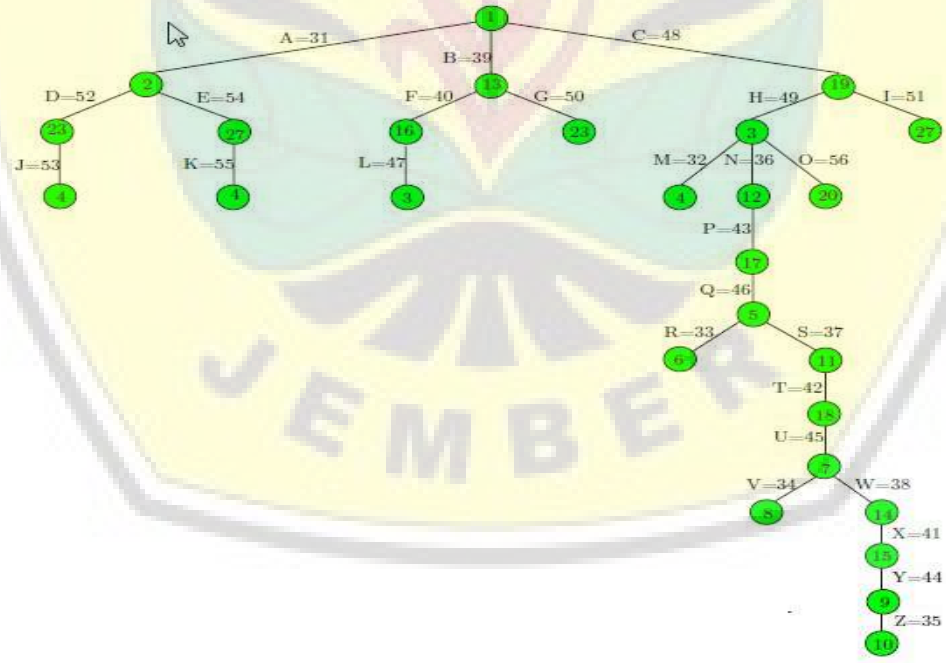


Figure 2. The layered diagram rooted at label 1

In the context of stream cipher key, s_b can generate multiple key streams. For a single key stream construction, the stream function can be executed repeatedly until the required sequence length fulfilled. Suppose $i = 1$, $b = 5$, and the stream function is defined as $k_{j+5} = k_j + k_{j+1} \bmod 26$. We have the initial block key $k = 5, 13, 22, 0, 2$ and, thus the key stream is $st_1 =$ — 5, 13, 22, 0, 2 — 18, 9, 22, 2, 20 — 1, 5, 24, 22, 21 — 6, 3, 20, 17, 1 — 9, 23, 11, 18, 10 — 6, 8, 3, 2, 16 — 14, 11, 5, 18, 6 — 25, 16, 23, 24, 5.

For the same b and stream function, multiple keystreams can be generated. Table 1 presents some keystreams generated from the previously produced base sequence. We then apply the MATLAB function, `runstest`, to these keystreams. The function returns a test decision for the null hypothesis that the values in the keystreams come in random order. Applying `runstest` to these keystreams returns value of $h = 0$. This test results indicate that the `runstest` does not reject the null hypothesis. This means that the values in all generated keystreams are in random order.

Table 1. Some constructed stream keys

i	st_i
1	5, 13, 22, 0, 2, 18, 9, 22, 2, 20, 1, 5, 24, 22, 21, 6, 3, 20, 17, 1, 9, 23, 11, 18, 10, 6, 8, 3, 2, 16, 14, 11, 5, 18, 6, 25, 16, 23, 24, 5
6	14, 24, 23, 25, 1, 12, 21, 22, 0, 13, 7, 17, 22, 13, 20, 24, 13, 9, 7, 18, 11, 22, 16,25, 3, 7, 12, 15, 2, 10, 19, 1, 17, 12, 3, 20, 18, 3, 15, 23
11	3, 21, 6, 10, 4, 24, 1, 16, 14, 2, 25, 17, 4, 16, 1, 16, 21, 20, 17, 17, 11, 15, 11, 8, 2, 0, 0, 19, 10, 2, 0, 19, 3, 12, 2, 19, 22, 15, 14, 21
16	17, 20, 7, 11, 16, 11, 1, 18, 1, 1, 12, 19, 19, 2, 13, 5, 12, 21, 15, 18, 17, 7, 10, 7, 9, 24, 17, 17, 16, 7, 15, 8, 7, 23, 22, 23, 15, 4, 19, 19
21	19, 8, 12, 15, 18, 1, 20, 1, 7, 19, 21, 21, 8, 0, 14, 16, 3, 8, 14, 4, 19, 11, 22, 18, 23, 4, 7, 14, 15, 1, 11, 21, 3, 16, 12, 6, 24, 19, 2, 18
26	9, 5, 13, 22, 0, 14, 18, 9, 22, 14, 6, 1, 5, 10, 20, 7, 6, 15, 4, 1, 13, 21, 19, 5, 14, 8, 14, 24, 19, 22, 22, 12, 17, 15, 18, 8, 3, 6, 7, 0
31	2, 14, 24, 23, 25, 16, 12, 21, 22, 15, 2, 7, 17, 11, 17, 9, 24, 2, 2, 0, 7, 0, 4, 2, 7, 7, 4, 6, 9, 14, 11, 10, 15, 23, 25, 21, 25, 12, 22, 20
36	1, 3, 21, 6, 10, 4, 24, 1, 16, 14, 2, 25, 17, 4, 16, 1, 16, 21, 20, 17, 17, 11, 15, 11, 8, 2, 0, 0, 19, 10, 2, 0, 19, 3, 12, 2, 19, 22, 15, 14

4. Conclusion

This work simulates randomness test to key sequences generated using SHATL. This kind of test is needed to ensure that there is no specific pattern of the key stream that can be utilized by an attacker to guess the key. The results of the randomness test show that the values in the encryption keys generated using SHATL, both in block and stream ciphers, come in random order. This condition indicates that the SHATL based encryption keys are eligible to increase security of the block and stream ciphers protocols.

Acknowledgement

Thanks to all colleagues at the Combinatorics, Graph Theory, and Network Topology (CGANT) research group, the University of Jember, Indonesia, for establishing this collaboration research.

References

[1] P. M. Alcover, A. Guillamon, and M. C. Ruiz, A new randomness test for bit sequence, *Inform.*, **24** (3) (2013), 339–356.

[2] M. Bača, L. Brankovic, M. Lascsáková, O., Phanalasy, and A. Semaničová-Feňovčíková, On d-antimagic labelings of plane graphs, *Electron. J. Graph Theory Appl.*, **1** (1) (2013), 28–39.

[3] Dafik, A. K. Purnapraja, and R. Hidayat, Cycle-super antimagicness of connected and disconnected tensor product of graphs, *Procedia Comput. Sci.*, **74** (2015), 93–99.

[4] Dafik, Slamin, and D. Tanna, A. Semaničová-Feňovčíková, M. Bača, Constructions of H-antimagic graphs using smaller edge-antimagic graphs, *Ars Combin.*, **100** (2017), In Press.

[5] Dafik, M. Hasan, Y. N. Azizah, and I. H. Agustin, A generalized shackle of any graph H admits a super H-antimagic total labeling, *Math. Comput. Sci. J.*, (2016). Submitted.

[6] P. L'Ecuyer, Testing random number generators, *Proc. 1992 Winter Simulation Conf.*, IEEE Press, Dec. (1992), 305–313.

[7] A. C. Prihandoko, Dafik, I. H. Agustin, D. Susanto, A. I. Kristiana, and Slamin, The construction of encryption key by using a super H-antimagic total graph, *Program Abstr. Asian Math. Conf.*, **AMC** (2016), 408, ISBN 978-602-74668-0-7.

[8] A. C. Prihandoko, Dafik, and I. H. Agustin, Implementation of super H-antimagic total graph on establishing stream cipher, *Indones. J. Combin.*, **3** (1) (2019), 14–23.

[9] M. E. Whitman and H. J. Mattord, *Principles Inf. Secur.*, (2012), Boston: Course Technology.