Alifmatika: Jurnal Pendidikan dan Pembelajaran Matematika
Volume 6, Issue 1, 90-103, June 2024
e-ISSN: 2715-6109 | p-ISSN: 2715-6095
https://journal.ibrahimy.ac.id/index.php/Alifmatika

Polyalphabetic cipher cryptosystem application *in making anti-hacker* passwords learning management systems in junior high schools

Muhlisatul Mahmudah[1*], Tri Novita Irawati[2], Friska B. Nur Aini[3]

[1*,2,3]Mathematics Education, Jember Islamic University, East Java 68121, Indonesia
[1*]maxlisa742@gmail.com, [2]tri.novitairawati@gmail.com, [3]afifzainmiss@gmail.com

Received: March 6, 2024 | Revised: April 23, 2024 | Accepted: June 25, 2024 | Published: June 30, 2024
*Corresponding author

***Abstract*:**
Research on developing an anti-hacker network security system for the learning management system was conducted at SMP Plus Darus Salam. Learning activities at SMP Plus Darus Salam use LMS as a media, which is a program to maximize learning activities at school. its also has risks, it is related to the security of students data work, so network security is needed. Network security used within computer networks to facilitate secure communication in different network entities based on predefined security protocols. On the other hand, the Learning Management System (LMS) is a software platform designed for online educational activities, e-learning programs, and educational resources, simplifying student engagement in learning processes. This study employs applied research methodology, focusing on a single tribune graph, and involves a labeling process for vertices and edges to construct a graph tree, resulting in the generation of ciphertext. This research aims to develop anti-hacker passwords in the SMP Plus Darusalam LMS using a polyalphabetic cipher cryptosystem. The research utilizes a data set comprising 24 LMS account samples. Data collection techniques encompass observation, interviews, distribution of questionnaires, and documentation, while data analysis involves tabulation and the generation of ciphertext codes in the form of usernames and passwords. Based on the results, it shows a total score of 2,096 with an average of 91.13 or a security percentage of 91.13%, which shows that it is successful and useful in the SMP Plus Darus Salam learning management system (LMS) account. Thus, it can be concluded that the secjar (network security) network security efforts made were successful and provided significant benefits in securing learning management system (LMS) accounts at SMP Plus Darus Salam. Therefore, the researcher suggests to the readers to conduct research on the development of anti-hacker network security using Tribun graphs with $d = 1$ and $d = 2$.

Keywords: Anti-Hacker; Ciphertext; Network Security; Polyalphabetic; Learning Management System; Tribune Graph.

How to Cite: Mahmudah; M., Irawati., T. N., & Aini, F. B. N. (2024). Polyalphabetic cipher cryptosystem application in making anti-hacker passwords learning management systems in junior high schools. *Alifmatika: Jurnal Pendidikan dan Pembelajaran Matematika*, 6(1), 90-103. https://doi.org/10.35316/alifmatika.2024.v6i1.90-103

Introduction

The concept of mathematics is classified because it is the science of numbers and space, the science of magnitude (quantity) and breadth, the knowledge of relationships between objects, the science of non-concrete structures, and a scientific discipline oriented towards deduction. In mathematics has a graph principle or graph theory ((Siagian, 2016)*graph theory*) which is the current branch of science with science.

According to research in the book graph theory by (Daniel & Prida. N. L, 2019), the concept of graph theory first appeared in 1736 through the work of Leonhard Euler, a Swiss mathematician. Graphs are visually represented with objects depicted as dots or vertices, while relationships between objects are represented by lines or edges. Mathematically, a graph can be defined as an unordered pair consisting of a set of vertices and a set of edges (Mahmudah, 2016) (u, v) of two you and v on V, a graph with points (u) and (v) sides denoted with uv (Fauzia, 2017).

The subjects studied involve graph structures typically represented by vertices and edges, as well as subsets of vertices known as labels (Jamil, 2014). According to (Firmansah et al., 2016), the concept of graph labeling was introduced by Sedláček in 1964, and until 2015 there has been a significant development in graph labeling research that Gallian has constantly updated. Gallian has compiled about 2000 journals from researchers around the world and invented about 200 new classes of graphs and how they are labeled (Gallian, 2018). Applications of graph labeling are widespread in many fields of science, including coding, radar, circuit design, database management, secret message sharing, and cryptography.

Many analysts and software developers have endeavored to create secure information systems, but users often abandon these systems (Purwanto, 2020). This happens because system development typically emphasizes the manufacturer's needs, resulting in systems that are difficult to use, less user-friendly, lack interactivity, and do not provide a pleasant user experience. In addition, user confusion with the system often occurs because the user interface does not pay attention to user behavior habits, the layout and menus of the system difficult to understand. Users also perceive limitations in the system, as it enforces standard procedures, making it feel rigid and less flexible. Consequently, the security of the information systems developed is often questioned (Siahaan et al., 2018).

According to the results of research that has been conducted by (Mahmudah, 2014), the discussion on the labeling of total super (a,d)-side antimagic on the grandstand graph, and also the labeling of total super (a,d)-side antimagic on the semi-parachute graph SP 2n-1, as presented in the study by (Rizqy Aprilia et al., 2014). Cryptography systems are important in enhancing information system security (Purwanto, 2020), just like LMS. The application of graphs is certainly also needed in the world of education, one of which is in this study by providing security for passwords ((Afrilian, 2017)*passwords* and usernames) on accounts owned by schools so that their authenticity is maintained. However, in practice not all schools have an information system due to limited facilities, resulting in a lack of updates in the implementation of the system.

A similar situation occurred at SMP Plus Darus Salam, where the existing information system has not been fully utilized. In addition, there is a lack of school facilities. Educators involved with information systems are also absent, resulting in students being unfamiliar with technology use, particularly in utilizing school

information systems such as learning management systems (LMS), Google Classroom, online quizzes, and similar platforms.

These problems can be overcome through the use of information systems that can increase the ease in the learning process, for example through the use of Learning Management Systems (LMS). LMS is a software platform for online learning activities, e-learning programs, and educational content (Wibowo et al., 2014) that has various features (sources) including, namely special content management (subjects), ongoing learning management, chatting, and interaction between students in one class (Larasati & Andani, 2019). LMS helps teachers and students see the results of student work and see material or modules provided through a system without fear of data lost or erased (Listiawan, 2016).

However, systems often have vulnerabilities in their design, such as weak passwords or passwords that are too easily guessed, making them susceptible to unauthorized access. This can also happen through an information system that is useful for education such as the LMS provided by this school, the account used by the unauthorized party can change its authenticity both in the form of assignment collection data and the personal information of the account owner due to weak passwords created. The security of an information system is very important in the world of information technology, because a number of findings regarding crimes committed in the (Sutabri, 2012) world of information technology such as hacking, cracking, spyware, phreaking, cyberpunk, and so on, aim to seize information without the owner's permission, with the aim of changing, modifying, deleting, or even falsifying information (Purnama, 2014). One of the efforts to protect information is the provision of network security (secjar) in the form of passure (*password* and *username*). In this case, coding knowledge is needed to keep a message secret in the form of passwords and *usernames* (Mahmudah et al., 2020).

Network security refers to (Indarta et al., 2022)computer network systems that allow various parts of the network space to communicate with each other in accordance with predefined security policies. Its purpose is to protect the network from potentially harmful access. In this context, the use of cryptography ensures that the same letters in plain text (plaintext) will be encrypted into different text (ciphertext) (Muktyas & Sugeng, 2014)increasing the level of data confidentiality (Dwi & Sudaryanto, 2017).

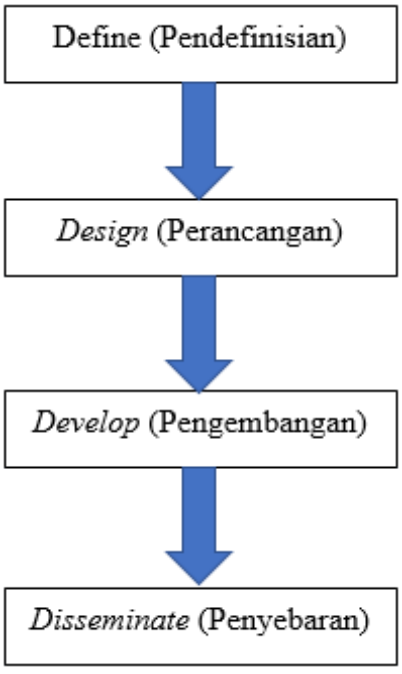
According to research findings on the significance of cryptography in safeguarding information systems, it has been concluded that cryptography is an effective and dependable method for maintaining security and ensuring protection. This technology can be extensively applied across various business and technological domains, utilizing methods such as ID identification and one-time passwords (Purwanto, 2021). This highlights the critical importance of graphs, particularly in the field of cryptography. A study on the utilization of graphs in database system privileges demonstrated that the relationship between graphs and granting privileges to database devices is closely intertwined. In this context, database users are depicted as nodes in the graph and cannot access the database unless they have a path to the server. Studies conducted by (Fikri, 2015) and (Mahmudah et al., 2020) on the use of polyalphabetic cipher cryptosystems emphasize that employing this method enhances the confidentiality level of created messages, making them challenging for unauthorized parties to crack or penetrate.

Based on the findings of the study and the problems faced in the school environment related to information system security, the author proposes a solution by conducting research on labeling total super (a,d)-antimagic side on tribune ($\mathfrak{T}_n$graphs) using tree graphs *H*. Tree graphs *H* are simple finite graphs, especially grandstand graphs with no double vertices (loops) or double sides (parallel). In the use of ciphertext, only 26 letters are used, namely from the alphabet *a* to *z*, , which can be upper or lowercase, a combination of punctuation marks as many as 15 marks, and combined with 1 number from the numbers 0-9; accounts used in the *d* = 0 *Learning Management System* are up to 24 accounts. Research success is measured based on a positive response of at least 70% to the implementation of secjar (network security). This research aims to develop anti-hacker passwords in the SMP Plus Darusalam LMS using a polyalphabetic cipher cryptosystem.

Research Methods

This research employs the Research and Development (R&D) method, which encompasses research and development stages to solve a problem (Sugiyono, 2019). The objective was to develop anti-hacker network security software within the LMS at SMP Plus Darus Salam, conducted from March 1st to 15th, 2023. In the book "Introduction to Educational Research" by Gall and Borg, it discusses an educational development approach that integrates industrial system concepts to design new procedures and products through innovative research.

The research method applied in this study is the 4-D Research Design method developed by Thiagarajani. This approach comprises four stages: definition, design, development, and dissemination. The details of these stages can be outlined in the following diagram (Picture 1).



Picture 1. 4-D Research Stages

a. Definition Stage

The initial steps in the definition stage include five main activities: conducting a preliminary analysis, analyzing the learners, performing a concept analysis, carrying out a task analysis, and determining the instructional objective. The implementation involves identifying the existing problem among learners, namely the vulnerability of LMS account security being known to other learners.

b. Design Stage

After identifying the problem during the definition stage, the next step is to proceed to the design stage. The implementation involves utilizing the super edge antimagic total labeling (a,d)-side method on the single Tribune graph $\mathfrak{T}_n$ with $d = 0$, inspired by previous studies on super edge antimagic total labeling on Tribune graphs by (Mahmudah, 2014).

c. Development Stage

In this research, the next step is to develop ciphertext through the T_n Tribune tree graph with d = 0 on the secret message consisting of passures (password and username) for securing the LMS accounts at SMP Plus Darus Salam.

d. Dissemination Stage

After conducting limited testing and revising the instruments used, the next step is the dissemination stage. The aim of this stage is to disseminate information about the created security network. In this research, dissemination is carried out in a limited manner by providing passwords to a select number of students and teachers at SMP Plus Darus Salam.

The research procedure was performed on a single Tribune graph where super (a,d)-side antimagic total labeling was applied and followed by pattern recognition on the tree structure of the Tribune graph with $\mathfrak{T}_n$ $d = 0$. Some of the research steps carried out are as follows:

1) Markers the structure of a single grandstand graph using the SEATL ($\mathfrak{T}_n$ $d = 0$ (*Super Edge Antimagic Total Labeling*) method or super(a,d)-side antimagic total labeling by taking into account possible d-side difference values.
2) Identify the bijective function of super total labeling (a,d)-side antimagic on a single Tribune graph with $\mathfrak{T}_n$ $d = 0$.
3) Create ciphertext tailored to the needs of the message, where the structure *of the ciphertext* depends on the marking given to each graph.

In this study, various antimagic sides super marking patterns, including initial and different values, will be explored and obtained through the results of Lemma 2.1.1 as presented in the research. This study can be interpreted as an effort to apply the super total marking (a,d)-side of antimagic to the a d (Mahmudah, 2014) Tribune graph $\mathfrak{T}_n$ using a sample of 24 learning management system accounts of SMP Plus Darus Salam students, which will be secured using secjar in the form of ciphertext. The sample is selected based on the number of accounts available at this institution.

a. Observation

Observation, as described by (Mania, 2017) is a data collection technique that involves structured and systematic observation and recording of the object being observed. Observations in the context of this study were made during the learning

process in the classroom, especially in the implementation of technology that has been used in schools.

b. Interview

This study involved two types of interviews: Interviews with learners, these interviews were conducted to ask questions related to the technology used by the institution. The aim was to gather information about the students' knowledge of security and the types of learning programs used, making it easier for researchers to conduct their study.

Interviews with teachers were conducted to ask teachers about the technology used by the school, focusing on both security and learning programs during the research period. The information gathered will help improve the secjar. A voice recorder on the researcher's Android device was used to avoid mistakes and to understand any differences in perspective between the researcher and the teachers.

c. Questionnaire

According to the basic book of research methodology, questionnaires or questionnaires are a method of collecting data in the form of sheets that are given a number of written questions according to research needs. The questionnaire aims to obtain a piece of information from teachers and students related to security made by researchers, (Sitoyo & Sodik, 2015) in the form of *passure* (*password* and *username*). In this study, researchers used a checklist questionnaire. A checklist questionnaire is a research tool that allows respondents to select answers or responses by marking the answer boxes provided by researchers on the creation of an anti-hacker secjar for LMS at this institution.

d. Documentation

The method of data collection in the form of documentation involves gathering information through images related to securing school accounts. This process includes observations, interviews, and questionnaires.

The data analysis method used in this study is tabulation, and providing code (*ciphertext*) in relation to the application of the *learning management system* (LMS). The steps and processes in detail as below:

1. Tabula

In this tabulation, researchers analyzed the results of user response questionnaires adopted from *mobile learning* media books on mathematics. Here are the results of the score for the level of network security implemented in the LMS:

Table 1. Acquisition of Network Security Level Score created on LMS

Category	Average Score Limit	Scurity Percentage
Very good/safe	> 95 Score	(≥ 75%)
Good/reasonably safe	> 82 – 95 Score	(≥ 64 – 73%)
Adequate/less scure	> 68 – 81 Score	(≥ 53 – 63%)
Less/unsafe	> 54 – 67 Score	(≥ 42 – 52%)
At risk/high risk	> 54 Score	(≤ 41%)

Source: Peltier in (Fathul, 2021)

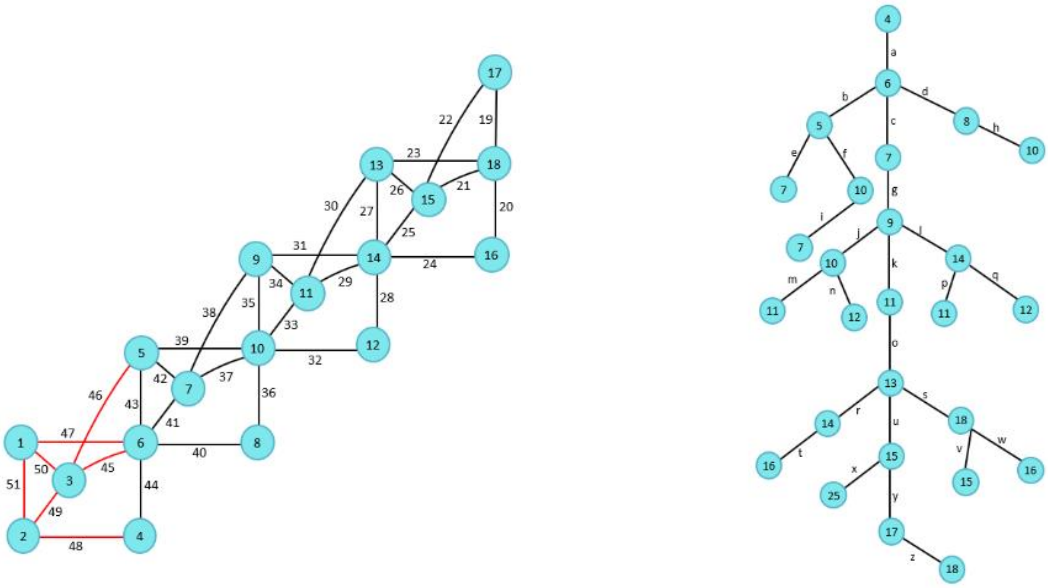
2. Provide code (*ciphertext*) in the application relationship to the *learning management system* (LMS) information system

In this stage, researchers provide code in the form of ciphertext that will be implemented in the learning management system (LMS). This code can then serve as a password to log into the learner's individual LMS account.

Results and Discussion

In this ciphertext, the *SEATL* Tribune graph $\mathfrak{T}_4$is utilized. The secret message, comprising 24 passwords for logging into the students' LMS accounts, will be encoded. The first step involves creating a Tribune graph $\mathfrak{T}_4$ with a label of $d = 0$. The point and side labels in figure 4.1 are numbered from 1 to 51, before the letters are inserted into the tree diagram, the repeating branches will be removed. The initial step of this omission involved the sum of the Tribune graphs $\mathfrak{T}_4$ $d = 0$ by the total letters in the alphabet. The number of dots in figure 4.1 is 18 and the number of letters in the alphabet is 26, so the total sum is 44. Branches or side labels that have a value greater than the number of points of the Tribune graph $\mathfrak{T}_4$ $d = 0$ and the number of letters in the alphabet are removed. Therefore, the removed side labels are 45, 46, 47, 48, 49, 50, 51. After the elimination of the sides marked in red, the next step is to create a tree diagram with roots in label 44 and include side labels as in figure 4.2 (Removed side labels are not included in the Tribune graph tree diagram $\mathfrak{T}_4$ $d = 0$).

The next step is to place all the letters from a to z on each branch of the tree diagram. The placement of these letters should be sequential from left to right and start from the first layer as described in chapter 2. The placement of letters is carried out as in figure 4.3, and then a modulo calculation of each branch or side label is carried out according to the position of the letters.



Picture 2. $d = 0$ Examples of Tribune Graphs $\mathfrak{T}_4$ and Alphabet Placement on the Tribune Graph Tree Diagram $\mathfrak{T}_4$ $d = 0$

Secret messages are encrypted using cryptographic methods by applying modulo 26 operations to each letter of the alphabet, and the results are presented in the following Table 2, which describes the Modulo 26 technique for ciphertext on the Super(a,d)-side of Total Antimagic on Tribune Graphs $\mathfrak{T}_4$ with parameters $d = 0$.

Table 2. Application of modulo method 26 to create ciphertext on the super-side of Antimagic Total on a tribune graph $(a, d)\ \mathfrak{T}_4$ with parameter $d = 0$

Abjad	Side Labels	Module 26	Ciphertext	Abjad	Side Labels	Module 26	Ciphertext
A/a	44	18	S/s	N/n	32	6	G/g
B/b	43	17	R/r	O/O	30	4	E/e
C/c	41	15	P/p	P/P	29	3	D/d
D/d	40	14	O/o	Q/ q	28	2	C/c
E/e	42	16	Q/ q	R/R	27	1	B/b
F/f	39	13	N/n	S / s	23	23	X/x
G/g	38	12	M/m	T/t	24	24	Y/y
H/h	36	10	K/k	U/u	26	0	A/a
I/I	37	11	L/L	V/ v	21	21	V/v
J/j	35	9	J/d	W/w	20	20	U/u
K/k	34	8	I/I	X/x	25	25	Z/z
L/L	31	5	F/f	Y/y	22	22	W/w
M/m	33	7	H/h	Z/z	19	19	T/t

The process continues with the sequential placement of numbers and punctuation marks on each branch of the tree diagram, with numbers using the operation modulo 10 and symbols using modulo 15. This step generates the ciphertext, which is represented in the table below.

Table 3. Application of modulo 10 method to create ciphertext on super-side of total antimagic on tribune graphs $(a, d)\ \mathfrak{T}_4$ with parameter $d = 0$

Number	Side Labels	Module 10	Ciphertext	Number	Side Labels	Module 10	Ciphertext
0	28	8	8	5	23	3	3
1	27	7	7	6	22	2	2
2	25	5	5	7	20	0	0
3	23	4	4	8	18	9	9
4	26	6	6	9	21	1	10

Table 4. Application of modulo 15 method to create Ciphertext on Super-side Total Antimagic on Tribune Graphs $(a, d)\ \mathfrak{T}_4$ with parameter $d = 0$.

Punctuation	Side Labels	Mod 15	Ciphertext	Punctuation	Side Labels	Mod 15	Ciphertext
.	33	3	( )	_	27	12	...
,	32	2	!	:	24	9	__
( )	30	0	‘	;	26	15	;
“	29	14	/	...	22	7	?
“ ”	28	13	[ ]	[ ]	21	6	!
!	23	8	-	/	20	5	“ ”
?	31	1	.	‘	19	4	“
-	25	10	:				

Next, the message is encrypted into ciphertext by replacing characters using alphabetical characters (upper and lower case) accompanied by a combination of numbers, punctuation marks and no spaces.

This study aims to develop anti-hacker network security (secjar) on the learning management system (LMS) in the form of passwords and usernames. Furthermore, the graph used in encryption is a Tribun graph with parameter $d = 0$. Based on the research results from a sample of 24 accounts at SMP Plus Darus Salam, passwords are obtained by substituting ciphertext using alphabetic characters (both uppercase and lowercase), combined with numbers, punctuation combinations, and no spaces from the message "Faruk001., zuL04,ini, devIr44-, Evi64Fah-, 7inA.saad, Umar84gtg!, rofl,5ati, “1Silvish”.

Table 5. Techniques for converting *plaintext* into ciphertext

No.	User	Name	Plaintext	Ciphertext
1.	0443	AF	Faruk001	(Nsbai887)
2.	0444	AZ	zuL04,ini	taF86!gl
3.	0445	DYRS	Dev1r44-	oqbvLb66:
4.	0446	EV	Evi64Fah-	Qvi26Nsk:
5,	0447	IS	7inA.saad	7lgS.xsso
6.	0448	MUF	Umar84gtg!	Ahsb96mym-
7.	0450	SR	Rofl,5ati	benL,3syl
8.	0451	SSH	“1Silvish”	[1Xlflxk]
9.	0453	AH	haLimb03!	ksFlhr84-
10.	0454	AO	4A; ofikgns	6s; anlimgx
11.	0455	DR	ratNa/5ari	bsyGs/5sbl
12.	0456	MA	?akbaR004	.sirsB886
13.	0457	NS	(bIIasho65)	‘rLfsxke23
14.	0458	SHM	8’sAfira’	9/xSnlbs
15.	0459	FA	F3la_flla	N3fs... nLfs
16.	0460	HK	Hel3n60	Kqf3g28_
17.	0461	MDF	dErik1; 61	oQblif; 27
18.	0462	SS	sA2... Fira	xS5?nlbs
19.	0463	L	Lutfi/na3	“Fayngs4”

No.	User	Name	Plaintext	Ciphertext
20.	0464	MAA	fiaN04'sip	'nisG86xld'
21.	0465	MDRFF	faTon1l65	nsYegf723
22.	0466	QFI	0Qfah6m!	8Cnsk6h-
23.	0467	WMI	Wlma70zHq	Ufhs08tKc
24	2052	Admin	Smp.darsa01	Xhd.osbxs01

Based on Table 5 above, it shows that haLimb03!, 4A;ofikgns, ratNa/5ari, ?akbaR004, (bIlasho65), 8'sAfira', F3la_fIla, Hel3n60:, dErik1;61, sA2...fira, Lutfi/na3, fiaN04'sip, faTon1l65, 0Qfah6m!, wlma70zHq, Smp.darsa01" to "(Nsbai887), taF86!lgl, oqbvLb66:, Qvi26Nsk:, 7lgS.xsso, Ahsb96mym-, benL,3syl, [1Xlflxk], ksFlhr84-, 6S;enlimgx, bsyGs/5sbl, .sirsB886, 'rLfsxke23, 9/xSnlbs, N3fs...nLfs, Kqf3g28_, oQblif;27, xS5?nlbs, "Fayngs4", 'nisG86xld', nsYegf723, 8Cnsk6h-, Ufhs08tKc, Xhd.osbxs01". In previous research (Mahmudah, 2016), ciphertext was limited to only 26 letters, from a-z, while in this study, passwords are created with various combinations, making it difficult for unauthorized parties to know, which is an advantage of this study. However, the limitation of this research is that the passwords created are only for one LMS account and cannot be more unless the admin can view the activities of other accounts.

In this study, user response questionnaires were used to support the development of secjar. Researchers distributed questionnaires to students at SMP Plus Darus Salam, obtaining 24 respondents who answered 20 questions. Based on the interviews conducted, it is evident that teachers expressed a need for solutions regarding security on student LMS accounts. This necessity prompted researchers to develop secjar, a security system tailored to address these concerns. The development of secjar was further substantiated by the positive responses received from both teachers and students through questionnaires. The cumulative score of 2,096 and an average score of 91.13%, indicating a high level of security, reaffirm the effectiveness of the implemented measures.

Table 6. Secjar security (*network security*)

Variable	Statement	Symbol
Security (X1)	Do you agree that security from unauthorized parties in The LMS is anough?	X1.1
	Do you agree that security protection against external attacks on the LMS is sufficient?	X1.2
	Do you agree that data protection measures in LMS are effective?	X1.3
	Do you agree with the existence of *network security* in the LMS?	X1.4
	Do you agree with the existence of *network security* makes it easier for students to log into the LMS	X1.5
	Do you agree that this *network security* does not provide opportunities for students to log in to other students' LMS accounts	X1.6
	Do you agree with the existence of this *network security*,	X1.7

Variable	Statement	Symbol
	the work you make is safe and cannot be seen by other students?	
	Do you agree that the security of LMS accounts is better maintained with network *security*?	X1.8
	Do you agree with the existence of *network security* makes the LMS guaranteed security?	X1.10
	Do you agree with the existence of *network security* do not worry in use?	X1.16
	Do you agree if the existence of *network security* in the use of LMS is more systematic?	X1.19
User (Y1)	Do you agree if users combine combinations based on numbers, letters, and special characters to make *the password* more secure?	Y1.1
	Do you agree if the *password* is used on the LMS account for the long term?	Y1.2
	Do you agree if long-term *passwords* make it easy to *login*?	Y1.3
	Do you agree if the *password* created is difficult for other students to know?	Y1.4
	Do you agree with the existence of *network security passwords* are easy to remember?	Y1.5
	Do you agree with long-term passwords making it easy to *login* on other devices?	Y1.6
	Do you agree with the *new passwords* login faster?	Y1.7
	Do you agree if in LMS *network security* is very helpful?	Y1.8
	Do you agree that *network security* is necessary in the long run?	Y1.9

Upon closer examination of the score table, it becomes apparent that the network security measures implemented have yielded successful outcomes, proving to be beneficial for schools. The results suggest that the security measures implemented are robust enough to withstand potential breaches, ensuring the safeguarding of each student's LMS account. In-depth discussions surrounding the development and implementation of secjar may include an analysis of the specific security protocols employed, the integration of encryption techniques, and the feasibility of scalability to accommodate future growth and technological advancements. Additionally, considerations regarding user access management, regular security audits, and ongoing updates to mitigate emerging threats can contribute to sustaining the effectiveness of the implemented security measures over time.

Conclusions and Suggestions

Based on the previously conducted analysis, it can be concluded that the development of anti-hacker network security in the learning management system, utilizing Tribune graphs with parameter $d = 0$ devoid of *loop* or double sides (parallel), and the substitution process into ciphertext using alphanumeric characters (both upper

and lower case), combined with numbers and punctuation, without spaces, has been successfully implemented. This process begins with labeling the Tribune graph $\mathfrak{T}_n$ with SEATL and determining its bijective function. The subsequent step involves labeling the points and sides with numbers from 1 to 51, followed by the removal of duplicate branches. The initial phase of eliminating the Tribune graph $\mathfrak{T}_4$ involves adding dots, alphabetic characters, numbers, and punctuation marks, then substituting side labels into sequential graph trees from left to right. This is followed by calculations of modulo 26 (for alphabets), modulo 10 (for numbers), and modulo 15 (for punctuation) from each branch or corresponding side label to generate its ciphertext, which has been successfully achieved. Therefore, it can be concluded that the efforts made in securing the learning management system (LMS) accounts at SMP Plus Darus Salam through secjar (network security) were successful and yielded significant benefits. Hence, the researcher recommends that readers pursue further research on the development of anti-hacker network security using Tribune graphs with $d = 1$ and $d = 2$.

References

Afrilian, A. (2017). Pemanfaatan Teknologi Informasi sebagai Sumber Belajar Siswa Kelas XI IPS SMA Negeri 1 Tengaran [Utilization of Information Technology as a Learning Resource for Class XI IPS Students at SMA Negeri 1 Tengaran.]. Doctoral dissertation, Program Studi Pendidikan Ekonomi FKIP-UKSW. https://repository.uksw.edu/handle/123456789/14142

Daniel, F. T., & Prida. N. L. (2019). *Teori Graf [Graph Theory]*(T. Yulianti, Ed.; 1st ed.). CV Budi Utama.

Dwi, O. :, & Sudaryanto, H. (2017). *Merancang Pengaman (Security) Jaringan Komputer [Designing Computer Network Security]*. *07*(1), 64-73. http://ejurnal.ppsdmmigas.esdm.go.id/sp/index.php/swarapatra/article/view/168

Fathul, A. (2021). *Analisis tingkat keamanan sistem informasi akademik (Siakad) UIN Ar-Raniry menggunakan standar ISO 2700;2013 dengan klausul 11 dan 14 [Analysis of the security level of UIN Ar-Raniry's academic information system (Siakad) using the ISO 2700;2013 standard with clauses 11 and 14]*. Repository Ar-Raniry.

Fauziah, D. A. (2017). *Penerapan rainbow 2-connected pada graf khusus dan graf hasil operasi korona dan kartesian [Application of rainbow 2-connected to special graphs and graphs resulting from corona and Cartesian operations]*. Repository Universitas Jember.

Fikri, R. N. (2015). *Penerapan graf pada database system privilege [Application of graphs to database system privileges]*. Program Studi Teknik Informatika Institut Teknologi Bandung.

Firmansah, F., Wahid, M., Prodi, S., & Matematika, P. (2016). *Pelabelan harmonis ganjil pada graf kincir angin double quadrilateral [Odd harmonic labeling in double quadrilateral windmill graphs]*. *Unwidha Repository*. http://repository.unwidha.ac.id:880/2637/

Gallian, J. A. (2018). A dynamic survey of graph labeling. *Electronic Journal of Combinatorics*, *1*((DynamicSurveys), [#DS6]). https://experts.umn.edu/en/publications/a-dynamic-survey-of-graph-labeling-3

Indarta, Y., Ranuharja, F., Ashari, I. F., Sihotang, J. I., Simarmata, J., Harmayani, Algifari, M. H., Muslihi, M. T., Jamaluddin, Mahmudi, A. A., Fatkhudin, A., Gustiana, Z., Subowo, E., & Idris, M. (2022). *Keamanan siber tantangan di era revolusi industri 4.0 [Cybersecurity challenges in the era of industrial revolution 4.0]* (R. Watrianthos, Ed.; 1st ed.). Yayasan Kita Menulis.

Jamil, N. A. (2014). Super (a,d)-H antimagic total covering pada graf triangular ladder. *Prosiding Seminar Matematika Dan Pendidikan Matematik*, *1*(1), 110-118. https://jurnal.unej.ac.id/index.php/psmp/article/view/915

Larasati, N. A., & Andayani, S. (2019). Pengaruh penggunaan learning management system (LMS) terhadap tingkat kepuasan mahasiswa menggunakan metode DeLone and McLean [The effect of using a learning management system (LMS) on student satisfaction levels using the DeLone and McLean method]. *Jurnal Teknik Informatika Unika Santo Thomas*, *4*(1), 13-20. https://doi.org/10.17605/jti.v4i1.506

Listiawan, T. (2016). Pengembangan learning management system (LMS) di program studi pendidikan matematika STKIP PGRI Tulungagung [Development of a learning management system (LMS) in the STKIP PGRI Tulungagung mathematics education study program]. *Jurnal Ilmiah Pendidikan Informatika)*, *1*(1), 14–22. https://doi.org/10.29100/jipi.v1i01.13

Mahmudah, M. (2014). *Pelabelan total super (a;d)-sisi antimagic pada graf tribun [Antimagic super(a;d)-edge total labeling of tribune graphs]*. Repository Universitas Jember.

Mahmudah, M. (2016). *Analisis keterkaitan seatl graf konektif dan diskonektif serta aplikasi dalam pengembangan kriptosistem polyalphabetic cipher [Analysis of the connection between connective and disconnective Seatl graphs and application in the development of polyalphabetic cipher cryptosystems]*. Repository Universitas Jember.

Mahmudah, M., Novita Irawati, T., & Islam Jember, U. (2020). Cryptosystem Polyalphabetic Cipher Application. *AXIOMA Jurnal Program Studi Pendidikan Matematika Universitas Islam Jember*, *5*(1), 11-19. https://doi.org/10.36835/axi.v5i1.539

Mania, S. (2017). Observasi sebagai alat evaluasi dalam dunia pendidikan dan pengajaran [Observation as an evaluation tool in the world of education and teaching]. *Jurnal Ilmu Tarbiyah Dan Keguruan*, *11*(DESEMBER), 220–233. https://doi.org/https://doi.org/10.24252/lp.2008v11n2a7

Muktyas, I. B., & Sugeng, K. (2014). Pemanfaatan pelabelan graceful pada symmetric tree untuk kriptografi polyalphabetic [Utilization of graceful labeling in symmetric trees for polyalphabetic cryptography]. Gramedia Pustaka Utama.

Purnama, B. (2014). Pengamanan pesan rahasia melalui kriptografi vigenere cipher dengan kunci berlapis [Securing secret messages through vigenere cipher

cryptography with layered keys]. *Jurnal Ilmiah Media Processor*, *9*(3), 264-269. https://ejournal.unama.ac.id/index.php/processor/article/view/243

Purwanto, D. (2020). Peranan kriptografi dalam peningkatan pengamanan sistem informasi [The role of cryptography in increasing information system security]. *Seminar of Social Sciences Engineering & Humaniora, 1*(1), 188-193. https://jurnal.pancabudi.ac.id/index.php/scenario/article/view/1177

Rizqy Aprilia, K., Hesti, I. A., & Dafik. (2014). Pelabelan total super (a,d)-sisi antimagic pada graf semi parasut SP 2n−1 [Antimagic total labeling of super (a,d)-edges on SP 2n−1 semi-parachute graphs]. *Prosiding Seminar Matematika Dan Pendidikan Matematik*, *1*(5), 88-96. https://jurnal.unej.ac.id/index.php/psmp/article/view/912

Siagian, M. D. (2016). Kemampuan koneksi matematik dalam pembelajaran matematika [Mathematical connection abilities in mathematics learning]. *MES: Journal of Mathematics Education and Science, 2*(1), 58-67. https://doi.org/10.30743/mes.v2i1.117.

Siahaan, A. P. U., Aryza, S., Hariyanto, E., Hasudungan Lubis, A., Ikhwan, A., & Len Eh Kan, P. (2018). Combination of levenshtein distance and rabin-karp to improve the accuracy of document equivalence level. *International Journal of Engineering & Technology, 7*(2.27), 17-21. https://doi.org/10.14419/ijet.v7i2.27.12084

Sitoyo, S., & Sodik, M. A. (2015). *Dasar metodologi penelitian [Basic research methodology]* (Ayup, Ed.; 1st ed.). Literasi Media Publishing.

Sugiyono, P. D. (2019). *Metode penelitian pendidikan (kuantitatif, kualitatif, kombinasi, R&D dan penelitian tindakan) [Educational research methods (quantitative, qualitative, combination, R&D and action research)]*. Bumi Aksara.

Sutabri, T. (2012). *Analisis sistem informasi [Information systems analysis]* (C. Putri, Ed.). CV Andi Offset.

Wibowo, A. T., Akhlis, I., & Nugroho, S. E. (2014). Pengembangan LMS (learning management system) berbasis web untuk mengukur pemahaman konsep dan karakter siswa [Development of a web-based LMS (learning management system) to measure student understanding of concepts and character]. Scientific Journal of Informatics, 1(2), 127-137. https://doi.org/10.15294/sji.v1i2.4019