Indonesian Journal of Ethnomathematics
Volume 1, No. 2, 2022, pp. 131-144
ISSN 2775-8001

The Application of Cryptography in Mathematics Education: A Study on Modulo

Dwi Atmi Yuliarni, Sekar Arum Hayasi

Mathematics Education Department, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
E-mail: sekar2100006057@webmail.uad.ac.id

Abstract

Cryptography has significant potential to enrich mathematics education. Besides its direct relation to mathematics, cryptography can also be used as a novel method for teaching mathematics at the school level. The cryptographic method offers a fresh perspective on mathematics lessons and can change students' views of mathematics more positively. The Caesar Cipher cryptography is one of the most straightforward and well-known cryptographic techniques for encrypting and decrypting text. This research aims to implement cryptography in mathematics learning based on Realistic Mathematics Education (RME) for the modulo material. The type of research used is library research. The research data were collected from several books on cryptography and several journals on cryptography and mathematics education. The results of this study indicate the implementation of mathematics learning in the form of modulo concepts in Caesar ciphers at the Sandi Museum in Yogyakarta. These mathematical concepts can be utilized to introduce and understand interesting and realistic mathematical concepts.

Keywords: Caesar Cipher, Cryptography, Modulo, Library Research, Realistic Mathematics Education

How to Cite: Yuliarni, D. A., & Hayasi, S. A. (2022). The Application of Cryptography in Mathematics Education: A Study on Modul. *Indonesian Journal of Ethnomathematics, 1*(2), 131-144. http://doi.org/10.48135/ije.v1i2.131-144

Introduction

Mathematics has played a crucial role in human civilization, from its origins in Babylon and Egypt to its development through the 19th and 20th centuries (Howson, 1974; Geiges, 2000; Alisherovich, 2023). Mathematics involves logical reasoning that starts from agreed-upon definitions and leads to definite implications (Durand-Guerrier, 2003; Priest, 2023). Therefore, the inability to understand mathematics can result in losing disciplined thinking when faced with real-world problems (Abdullah et al., 2012; Schoenfeld, 2016; Sinaga et al., 2023). However, mathematics education faces significant challenges (Stephan et al., 2015; Rosyada & Retnawati, 2021; Suryanti et al., 2023). One of these challenges is transforming the approach to teaching mathematics from a deductive and doctrinaire method to an approach that allows students to discover mathematical concepts realistically (Gee et al., 2018). In other words, mathematics teaching in schools should only focus on memorizing formulas and understanding their origins. Instead, mathematics teaching in schools should be directed toward learning mathematical concepts related to realistic problems (Sumirattana et al., 2017; Hang & Thanh, 2021; Caraan et al., 2023).

Freudenthal introduced the Realistic Mathematics Education (RME) approach to help teachers design mathematics learning that engages students more, allowing them to understand the concepts taught easily (Traffers, 1993; Webb et al., 2011; Loc & Tien, 2020). The RME approach emphasizes using

real-world contexts relevant to students' daily lives (Gravemeijer & Doorman, 1999; Negara et al., 2021). Additionally, RME uses realistic problems as a starting point for understanding mathematical concepts (Sitorus, 2016; Octaria et al., 2023). These realistic problems can increase students' motivation and interest in mathematics (Ardiansah et al., 2019; Prahmana et al., 2020). Consequently, students can see that mathematics is related to their daily activities, making the knowledge gained more meaningful. According to Gravemeijer (1994), RME is based on three main principles: guided reinvention and progressive mathematization, didactical phenomenology, and self-developed models. In progressive mathematics, students can work with mathematics according to their experiences. Didactical phenomenology involves providing problems that lead students to understand mathematical concepts.

Gravemeijer (1994) also identified five characteristics of RME: (1) The Use of Context; (2) Use of Models, Bridging by Vertical Instruments; (3) Student Contribution; (4) Interactivity; and (5) Intertwining with Other Topics. Students are expected to solve real-world problems informally. Self-developed models are used to connect informal knowledge with formal knowledge. According to Treffers and Goffree (in Erman, 2003), contextual problems in RME have four main functions: (1) helping students form mathematical concepts, (2) forming basic mathematical models that support students' mathematical thinking, (3) utilizing reality as a source and domain of mathematical application, and (4) training students' ability to apply mathematics to real situations. The reality referred to here is a relevant context.

RME is based on three main principles: guided reinvention and progressive mathematization, didactical phenomenology, and self-developed models. One mathematical topic that encompasses various advanced mathematical theories is cryptography (Silverman et al., 2008; Budaghyan et al., 2019). Cryptography is the science and art of keeping messages or data secret (Silverman et al., 2008). In everyday life, cryptography is closely related to using passwords, banking data security, and national security data protection.

Therefore, cryptography meets one of the essential requirements for applying RME-based learning: the alignment between mathematical concepts and accurate and relevant situations in daily life. However, cryptography is only partially suitable for teaching at the secondary school level. The highly advanced mathematical concepts in cryptography do not align with the secondary education curriculum. Additionally, cryptography requires high-specification computers and sophisticated cryptographic machines, which are difficult to present in the learning process. Therefore, the authors attempt to address this challenge by exploring the modulo concept in RME-based mathematics learning.

Methods

The type of research used in this study is library research. Library research collects necessary data

from books, journals, or previous research results (Mirzaqon & Purwoko, 2018). This study selected several books on cryptography and several journals on cryptography and mathematics education. Furthermore, Paar and Pelzl (2010) was the primary reference for studying cryptography materials. Several articles and journals on cryptography, modulo, matrices, and realistic mathematics were selected. Nisak (2015) served as the primary reference for understanding Caesar Cipher and Hill Cipher cryptography. On the other hand, Mubarak's research (2019) was used as a reference for examining realistic mathematics education. Finally, Ginting's exploration (2010) was used to understand modulo material. Other journals related to the title of this research were also used.

Results and Discussions

Several researchers have documented their findings, demonstrating the effectiveness of Realistic Mathematics Education (RME) in mathematics teaching (Fitri et al., 2023). Research by Laurens et al. (2017) indicates that teachers must empower students' intellectual abilities through RME and games to achieve meaningful and contextual learning. Additionally, Widodo et al. (2023) show that the RME approach significantly enhances mathematical problem-solving skills at the elementary school level. Furthermore, findings by Muhtarom et al. (2019) suggest that the multi-representation abilities of students who receive RME are better than those of students who receive conventional learning.

These research results highlight the potential impact of the RME approach in improving mathematics learning outcomes while also reinforcing the core of education, which is students' character formation. This paper focuses on implementing cryptographic algorithms within RME-based learning to understand the concept of modulo. The discussion will be divided into three sub-discussions: the basics of cryptography, the implementation of cryptography in RME-based learning, and understanding the concept of modulo.

The Basics of Cryptography

These research results highlight the potential impact of the RME approach in improving mathematics learning outcomes while also reinforcing the core of education, which is students' character formation. This paper focuses on implementing cryptographic algorithms within RME-based learning to understand the concept of modulo. The discussion word cryptography consists of two parts derived from Greek: "crypto" and "graphia," where "crypto" can be translated as secret, and "graphia" as writing. Linguistically, cryptography originates from Greek, composed of two words: "cryptos," meaning secret, and "graphene," meaning writing (Schneier, 2007). Terminologically, cryptography can be defined as the science of writing secret messages to hide the meaning of the messages (Paar & Pelzl, 2010). According

to its terminology, cryptography is the science and art of securing messages when sending them from one place to another (Bryant, 2006). be divided into three sub-discussions: the basics of cryptography, the implementation of cryptography in RME-based learning, and understanding the concept of modulo.

Cryptography is a science that analyzes mathematical techniques related to data security, such as data hiding, data validity, data integrity, and data authenticity (Schneier, 1996). Cryptography is the science and art of protecting messages to remain secure. The purpose of cryptography is to create something obscure in the form of secret messages like text, audio, images, and video (Seftyanto et al., 2012). Generally, cryptography is the science and art of maintaining the confidentiality of messages.

One practical application of cryptography is in sending secret messages. Two parties communicating secretly or sending messages containing confidential information require cryptography to maintain the secrecy of the message. This is done to prevent unauthorized third parties from understanding the meaning of the secret message. In secret message transmission, cryptography plays a role in encoding the original readable message (plaintext) into an unreadable coded message (ciphertext) and converting the ciphertext back into plaintext (Dafid, 2006). The goal of cryptography is to provide security services (Nasution et al., 2019) which include:

a. Confidentiality

Confidentiality is a service that keeps information content hidden from anyone except those with the authority or the secret key to decrypt the information. Data confidentiality is achieved by hiding data from unauthorized individuals.

b. Integrity

Data integrity relates to protecting data from unauthorized modifications. To maintain data integrity, the system must be able to detect data manipulation by unauthorized parties, such as insertion, deletion, and substitution of data. Data should remain unchanged until it reaches the recipient during the transmission process.

c. Message Authentication

Authentication relates to identification, both of the system and the information itself. Two communicating parties must mutually identify themselves. Information sent through the channel must be authenticated for its authenticity, data content, transmission time, etc. Clear identity of all related entities and data source authentication is necessary.

d. Non-repudiation

Non-repudiation is the effort to prevent the denial of sending or creating information by the sender or creator. Each related entity cannot deny or refute the sent or received data.

Several critical aspects of cryptography to be aware of include (Nasution et al., 2019):

a. Sender and Receiver

The sender is the entity that sends the message to the receiver securely without interference from eavesdroppers. The receiver is the entity that receives the message from the sender.

b. Plaintext dan Ciphertext

In cryptography, the pure message is called plaintext, while the obscured message is called ciphertext.

c. Encryption and Decryption

The process of converting plaintext to ciphertext is called encryption, and the process of converting ciphertext back to plaintext is called decryption.

d. Cryptographers, Cryptanalysts, and Cryptologists

A cryptographer studies and uses cryptographic methods to protect messages. Conversely, the methods used to attack cryptographic techniques using computational mathematics are called cryptanalysis, and those involved in cryptanalysis are called cryptanalysts. The discipline of studying both cryptography and cryptanalysis is known as cryptology, and those who study it are called cryptologists.

e. Ciphers

An encryption algorithm is a mathematical function used for encryption and decryption. To solve encryption problems, a unit called a key is required, which has a tremendous numerical value. The size of this value is called the critical range. Some encryption algorithms use different keys for encryption and decryption.

f. Eavesdropper

An eavesdropper is a person who wants to gather as much information as possible about the transmitted message and decipher the ciphertext from the encryption system. The eavesdropper intercepts the communication between the sender and the receiver.

The Caesar cipher, or shift cipher, is a straightforward and popular encryption method in cryptography. This code substitutes each letter in the original text (plaintext) with another letter a certain number of positions down the alphabet. In the Caesar cipher, letters are shifted by a fixed number of positions in the alphabet.

Implementation of Cryptography in RME Mathematics Learning for Understanding Modulo Concepts

In cryptography, the Caesar cipher, or the shift cipher, is a straightforward and widely used encryption method. This code involves substituting each letter in the plaintext with another letter that is a fixed number of positions away in the alphabet. In the Caesar cipher, letters are shifted to the following

letter in the alphabet by a specified amount. The Caesar cipher, also known as the shift cipher or Caesar shift, is one of the most basic, straightforward, and well-known encryption techniques. This cipher involves shifting letters by a certain number of positions. The result of this shift is the Caesar cipher text. For example, if n=3, the phrase *"Aku ingin mandi"* becomes "Dnx lqjlq pdqgl." The process of the Caesar Cipher is:

1. Determine the number of character positions to shift to create the ciphertext from the plaintext.
2. Substitute the position of the plaintext characters with the ciphertext characters based on the previously determined shift. For example, with a shift of 3, the letter A becomes D, B becomes E, and so on. As shown in the following image

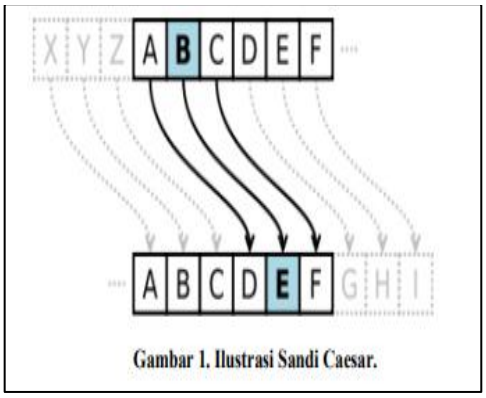

Figure 1. Caesar Cipher Illustration

The steps of Caesar encryption are often included as part of more complex encryptions, such as the Vigenère cipher. Due to its use of a single alphabet substitution in encryption, the Caesar cipher can be easily broken. In practice, it provides less assurance of confidentiality and security in communication. The Caesar cipher uses a shift of three letters. As shown in Table 1 and Table 2

Table 1: Caesar Cipher Plain

Plain																								
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Table 2: Caesar Cipher Ciphertext

Cipher																								
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

To create ciphertext, you must match the letters between the plaintext and ciphertext alphabet. To determine the plaintext, perform the reverse process.

→ Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

→ Ciphertext: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

Encryption can also be represented using modular arithmetic by first transforming letters into numbers. A=0, B=1, ..., Z=25. Encrypting a letter x with a shift n can be mathematically described as:

$E_n(x)=(x+n) \bmod 26$

The representation for decryption is not much different, which is:

$D_n(x)=(x-n) \bmod 26$

The decryption process uses the following equation:

Cp= (Pt + k) modulo 26…….(1)

Where 26 is the number of letters in the alphabet. Equation 1 is used in the encryption process. The decryption process uses the following equation (Equation 2):

Pt= (Cp-k) modulo 26 ……(2)

The Caesar cipher is a type of substitution cipher where the cipher is created by substituting characters from the plaintext with characters from the ciphertext. This method is known as a single-character password cipher.

The steps to create plaintext using the Caesar cipher are as follows:

a. Determine the number of character shifts used to transform the word into ciphertext.

b. Convert the characters of the word based on the shift. For example, with a shift of 3, the letter A becomes D, B becomes E, and so on. The alphabet format after shifting 3 letters is shown in the following substitution table:

Table 4. Substitution Table for ROT 3

Index	0	1	2	3	4	5	6	7	8	9	10	12	13
P	A	B	C	D	E	F	G	H	I	J	K	L	M
C	D	E	F	G	H	I	J	K	L	M	N	O	P
Index	13	14	15	16	17	18	19	20	21	22	23	24	25
P	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

In the first case, the cipher can be solved using techniques similar to simple substitution ciphers, such as frequency analysis or word patterns. While solving, the decoder will recognize the regularity of the solution and conclude that the algorithm used in the code is the Caesar cipher.

In the second example, decoding the code is more straightforward. Since it is already known that the code is the result of Caesar cipher encryption and there are only a limited number of possible shifts

(26), the code can be tested randomly using what is known as a brute force attack. This involves writing ciphertext segments in a table of possibilities for all possible shifts—a technique known as "completing the components." For example, given the ciphertext "EXXEGOEXSRGI," it can be seen that the possible plaintext is "ATTACKATONCE," where the letter shift is 4. As shown in Figure 2.

Decryption shift	Candidate plaintext
0	exxegoexsrgi
1	dwwdfndwrqfh
2	cvvcemcvqpeg
3	buubdlbupodf
4	attackatonce
5	zsszbjzsnmbd
6	yrryaiyrmlac
...	
23	haahjrhavujl
24	gzzgiqgzutik
25	fyyfhpfytshj

Figure 2. Illustration of Caesar Cipher Shift

Another random method is to match the frequency distribution of letters. In English, the distribution of letters in sample texts has a specific and predictable shape. The Caesar shift rotates this distribution, and it is quite possible to determine the shift by examining the results from the frequency graph. One can quickly determine the letter shift by analyzing the graph by plotting the frequency graph of letter occurrences in the ciphertext and comparing it with the expected distribution of letters in the original plaintext language. This method is known as frequency analysis. For example, in English, the frequency of the letters E and T (which usually appear most frequently) and Q and Z (which usually appear least frequently) is very characteristic. Computers can also measure how well the actual frequency distribution matches the expected distribution, for example, using chi-square distribution (statistics).

There is usually only one reasonable decryption possibility for plaintext in a common language, although very short plaintexts may have more candidates. For example, the ciphertext MPQY (in English) could be decrypted as “Aden” or “know”; similarly, “ALIIP” could be “dolls” or “wheel,” and “AFCCP” could be “jolly” or “cheer.”

Calculating Caesar Cipher

The first step is for the teacher to divide the students into two groups, for example, Group A and Group B. The teacher sends a hidden message to Group A. For instance, the message could be "the

world of mathematics." Group A is asked to convert the message into a secret code through the encryption process as follows:

Encryption Process:

a. The teacher asks the students to convert the message from letters to numbers as follows:

Table 5: Caesar Cipher Calculation

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Given Message : **PENDIDIKAN MATEMATIKA**
Encoded as *plaintext* P :**15 4 13 3 8 3 8 10 0 13 12 0 19 4 12 0 19 8 10 0**

In the second step, the teacher provides a key, for example, 10. The students are instructed to add 10 to each number in P. If the resulting number exceeds 25, the teacher asks them to subtract 26 from the result. Mathematically, the encryption process in the Caesar Cipher is carried out as follows:

$$C=(K+P) \bmod 26$$

C = Cyphertext
K = Key
P = Plaintext
Key: 10

C_1= (K+P_1) mod 26=(10+15)mod 26=25 mod 26=25=Z
C_2= (10+4) mod 26=14 mod 26=14=O
C_3= (10+13) mod 26=23 mod 26=23=X
C_4= (10+3) mod 26=13 mod 26=13=N
C_5= (10+8) mod 26=18 mod 26=18=S
C_6= (10+3) mod 26=13 mod 26=13=N
C_7=(10+8) mod 26=18 mod 26=18=S
C_8=(10+10) mod 26=20 mod 26=20=U
C_9=(10+0) mod 26=10 mod 26=10=K
C_{10}=(10+13) mod 26=23 mod 26=23=X
C_{11}=(10+12) mod 26=22 mod 26=22=W
C_{12}=(10+0) mod 26=10 mod 26=10=K
C_{13}=(10+19) mod 26=29 mod 26=3=D
C_{14}=(10+4) mod 26=14 mod 26=14=O
C_{15}=(10+12) mod 26=22 mod 26=22=W
C_{16}=(10+0) mod 26=10 mod 26=10=K

C_{17}=(10+19) mod 26=29 mod 26=3=D
C_{18}=(10+8) mod 26=18 mod 26=18=S
C_{19}=(10+10) mod 26=20 mod 26=20=U
C_{20}=(10+0) mod 26=10 mod 26=10=K

The message= PENDIDIKAN MATEMATIKA in encrypted into C= ZOXNSNSUKXWKDOWKDSUK
Decryption Process:
After Group A completes the encryption process, the teacher asks Group B to interpret the contents of the secret message. The steps taken are:

a. First, convert the ciphertext back into numbers, as in the initial encryption process.

   $C =$ **ZOXNSNSUKXWKDOWKDSUK**

   Translates to: $C =$ **25 14 23 13 18 13 18 20 10 23 22 10 3 14 22 10 3 18 20 10**

b. Then, the teacher informs the students that the key is 10. The students should subtract ten from each number. If the result is a negative number, they should add 26 or its multiples to the result. Mathematically, the decryption process in the Caesar Cipher is as follows:

$$P = (C - K)\ mod\ 26$$

   C = Cyphertext
   K = Key
   P = Plaintext
   Key: 10

$P_1 = (C_1 - K) mod\ 26 = (25 - 10) mod 26 = 15\ mod\ 26 = 15 = P$
$P_2 = (14 - 10) mod\ 26 = 4\ mod\ 26 = 4 = E$
$P_3 = (23 - 10) mod\ 26 = 13\ mod\ 26 = 13 = N$
$P_4 = (13 - 10) mod\ 26 = 3\ mod\ 26 = 3 = D$
$P_5 = (18 - 10) mod\ 26 = 8\ mod\ 26 = 8 = I$
$P_6 = (13 - 10) mod\ 26 = 3\ mod\ 26 = 3 = D$
$P_7 = (18 - 10) mod\ 26 = 8\ mod\ 26 = 8 = I$
$P_8 = (20 - 10) mod\ 26 = 10\ mod\ 26 = 10 = K$
$P_9 = (10 - 10) mod\ 26 = 0\ mod\ 26 = 0 = A$
$P_{10} = (23 - 10) mod\ 26 = 13\ mod\ 26 = 13 = N$
$P_{11} = (22 - 10) mod\ 26 = 12\ mod\ 26 = 12 = M$
$P_{12} = (10 - 10) mod\ 26 = 0\ mod\ 26 = 0 = A$
$P_{13} = (3 - 10) mod\ 26 = -7 mod\ 26 = 19 = T$
$P_{14} = (14 - 10) mod\ 26 = 4\ mod\ 26 = 4 = E$
$P_{15} = (22 - 10) mod\ 26 = 12\ mod\ 26 = 12 = M$
$P_{16} = (10 - 10) mod\ 26 = 0\ mod\ 26 = 0 = A$

$$P_{17} = (3 - 10) mod\ 26 = -7 mod\ 26 = 19 = T$$
$$P_{18} = (18 - 10) mod\ 26 = 8\ mod\ 26 = 8 = I$$
$$P_{19} = (20 - 10) mod\ 26 = 10\ mod\ 26 = 10 = K$$
$$P_{20} = (10 - 10) mod\ 26 = 0\ mod\ 26 = 0 = A$$

Based on the above description, the result is returned to the original message: PENDIDIKAN MATEMATIKA. Based on this result, the teacher explained to the students that what was done involved the concept of modulo. The teacher then guides the students in understanding the concept of modulo.

Conclusion

Cryptography can be used in mathematics education in schools. As a new method, besides providing a fresh approach to teaching, cryptography also offers other positive impacts, such as teaching students to think more critically when solving problems. The Caesar Cipher cryptographic algorithm can be applied to modulo concepts by sending secret messages between students in a classroom. Activities that present messages in role-playing games are one of the learning programs that bring mathematics to life. Cryptographic media is not limited to modulo concepts and is used for educational purposes. Other materials that can be explored with cryptography include data collection and analysis related to function composition and inverse composition.

Acknowledgments

The authors express their gratitude to the anonymous reviewers for their constructive feedback, which significantly improved the manuscript. They also extend their thanks to mathematics education department, Universitas Ahmad Dahlan for supporting this research.

References

Abdullah, N., Zakaria, E., & Halim, L. (2012). The effect of a thinking strategy approach through visual representation on achievement and conceptual understanding in solving mathematical word problems. *Asian Social Science, 8*(16), 30. https://doi.org/10.5539/ASS.V8N16P30.

Alisherovich, Y. J. (2023). The importance of mathematics in the prosperity of society. *American Journal of Applied Science and Technology, 3*(10), 20-24.

Ardiansah, D., Yusmianti, M., & Firdaus, A. R. (2019). Mathematical learning motivation of submission and reduction of participants in primary school using Realistic Mathematics Education (RME). *PrimaryEdu: Journal of Primary Education, 3*(1), 27-34. https://doi.org/10.22460/PEJ.V3I1.1223.

Bryant, L. (2006). Caesar Ciphers: An Introduction to Cryptography.

Budaghyan, L., Li, C., & Parker, M. G. (2019). Special issue on mathematical methods for cryptography. *Cryptography and Communications, 11*, 363-365. https://doi.org/10.1007/s12095-019-00356-8.

Caraan, D. R., Dinglasan, J. K., & Ching, D. (2023). Effectiveness of realistic mathematics education approach on problem-solving skills of students. I*nternational Journal of Educational Management and Development Studies, 4*(2), 64-87. https://doi.org/10.53378/352980.

Dafid, D. (2006). Symmetric Key Cryptography Using the Crypton Algorithm. *goritma, 2*(3), 20-27.

Durand-Guerrier, V. (2003). Which notion of implication is the right one? From logical considerations to a didactic perspective. *Educational Studies in mathematics, 53*, 5-34.

Erman, S. (2003). Contemporary Strategies for Mathematics Education. Bandung: Universitas Pendidikan Indonesia.

Fitri, A., Pakpahan, H., & Matondang, N. (2023). The Effect of RME application on mathematics learning outcomes. *International Journal of Educational and Psychological Sciences, 1*(23), 313-320. https://doi.org/10.59890/ijeps.v1i4.916.

Gee, E., Fauzan, A., & Atmazaki, A. (2018). Designing learning trajectory for teaching sequence and series using RME approach to improve students' problem solving abilities. *In Journal of Physics: Conference Series, 1088*(1), 012096. IOP Publishing. https://doi.org/10.1088/1742-6596/1088/1/012096.

Geiges, H. (2000). Facets of the cultural history of mathematics. *European Review, 8*(4), 487-497. https://doi.org/10.1017/S1062798700005044.

Ginting, D. B. (2010). The Role of Modular Arithmetic and Prime Numbers in the RSA Cryptographic Algorithm. Media inform. sekol. tinggi manaj. inform. dan Komput. *LIKMI, 9*(2), 48-57.

Gravemeijer, K. P. E. (1994). *Developing realistic mathematics education*.

Gravemeijer, K., & Doorman, M. (1999). Context problems in realistic mathematics education: A calculus course as an example. *Educational studies in mathematics, 39*(1), 111-129. https://doi.org/10.1023/A:1003749919816.

Hang, N., Quyet, V., & Thanh, L. (2021). Designing realistic mathematics problems for the last grade of secondary school. *Vinh University Journal of Science. 50*(1), 36-45 https://doi.org/10.56824/vujs.2021ed15.

Howson, A. G. (1974). Mathematical thought from ancient to modern times, by Morris Kline. Pp xvii, 1238. 12. 1973 (Oxford University Press). *The Mathematical Gazette, 58*(403), 58-59. https://doi.org/10.2307/3615488.

Laurens, T., Batlolona, F. A., Batlolona, J. R., & Leasa, M. (2017). How does realistic mathematics education (RME) improve students' mathematics cognitive achievement?. *Eurasia Journal of Mathematics, Science and Technology Education, 14*(2), 569-578. https://doi.org/10.12973/EJMSTE/76959.

Loc, N. P., & Tien, N. T. T. (2020). Approach to realistic mathematics education in teaching mathematics: A case of cosine theorem–Geometry 10. *International Journal of Scientific and Technology Research, 9*(4), 1173-1178.

Mirzaqon, A., & Purwoko, B. (2018). Literature Review on the Theoretical Foundations and Practice of Expressive Writing Counseling. *Jurnal BK Unesa, 1*, 1-8.

Mubarok, N. (2019). Implementation of the modified enigma cryptographic algorithm as a PMRI-based mathematics learning medium for function composition and inverse function materials. Journal of Mathematics Education*, 7*(1), 65-80.

Muhtarom, M., Nizaruddin, N., Nursyahidah, F., & Happy, N. (2019). The effectiveness of realistic mathematics education to improve students'multi-representation ability. *Infinity Journal, 8*(1), 21-30. https://doi.org/10.22460/INFINITY.V8I1.P21-30.

Nasution, A. B. (2019). Implementation of Data Security Using the Caesar Cipher Algorithm and Transposition Cipher*. (JurTI) Jurnal Teknologi Informasi, 3*(1), 1-6.

Negara, H. R. P., Ibrahim, M., Kurniawati, K. R. A., Firdaus, A., Maulidina, R., & Saifudin, M. (2021). The effect of the realistic mathematic education (rme) learning model on students' mathematical problem solving abilities: A Meta-Analysis. *Justek: Jurnal Sains Dan Teknologi, 4*(1), 40-51.

Nisak, K. (2015). Cryptographic Encoding Methods Using Hill Cipher and Caesar Cipher with AppInventor (Doctoral dissertation, Universitas Islam Negeri Maulana Malik Ibrahim). http://etheses.uin-malang.ac.id/id/eprint/6275

Octaria, D., Zulkardi, Z., & Putri, R. I. I. (2023). Systematic Literature Review: How students learn linear programming with realistic mathematics education?. *International Journal of Trends in Mathematics Education Research, 6*(1), 41-46. https://doi.org/10.33122/ijtmer.v6i1.174.

Paar, C., & Pelzl, J. (2010). *Understanding cryptography* (Vol. 1). Springer-Verlag Berlin Heidelberg.

Prahmana, R. C. I., Sagita, L., Hidayat, W., & Utami, N. W. (2020). Two decades of realistic mathematics education research in Indonesia: A survey. *Infinity Journal, 9*(2), 223-246. https://doi.org/10.22460/infinity.v9i2.p223-246

Priest, G. (2023). Logic as applied mathematics–with particular application to the notion of logical form. *Logic and Logical Philosophy, 32*(3), 443-457. https://doi.org/10.12775/llp.2023.003.

Rosyada, M. N., & Retnawati, H. (2021). Challenges of mathematics learning with heuristic strategies. *Al-Jabar: Jurnal Pendidikan Matematika, 12*(1), 161-173. https://doi.org/10.24042/AJPM.V12I1.8730.

Schneier, B. (1996). Applied Cryptography: protocols, algorithms, and source code in c. Canada: John Wiley & Sons, Inc.

Schneier, B. (2007). Applied cryptography: protocols, algorithms, and source code in C.

Schoenfeld, A. H. (2016). Learning to think mathematically: Problem solving, metacognition, and sense making in mathematics (Reprint). *Journal of education, 196*(2), 1-38. https://doi.org/10.1177/002205741619600202.

Silverman, J. H., Pipher, J., & Hoffstein, J. (2008). *An introduction to mathematical cryptography* (Vol. 1). Springer New York. https://doi.org/10.5860/choice.46-3906.

Sinaga, B., Sitorus, J., & Situmeang, T. (2023). The influence of students' problem-solving understanding and results of students' mathematics learning. *In Frontiers in Education 8*,1088556. Frontiers Media SA. https://doi.org/10.3389/feduc.2023.1088556.

Sitorus, J. (2016). Students' creative thinking process stages: Implementation of realistic mathematics education. *Thinking Skills and Creativity, 22*, 111-120. https://doi.org/10.1016/J.TSC.2016.09.007.

Stephan, M. L., Chval, K. B., Wanko, J. J., Civil, M., Fish, M. C., Herbel-Eisenmann, B., ... & Wilkerson, T. L. (2015). Grand challenges and opportunities in mathematics education research. *Journal for research in mathematics education, 46*(2), 134-146. https://doi.org/10.5951/JRESEMATHEDUC.46.2.0134.

Sumirattana, S., Makanong, A., & Thipkong, S. (2017). Using realistic mathematics education and the DAPIC problem-solving process to enhance secondary school students' mathematical literacy. *Kasetsart Journal of Social Sciences, 38*(3), 307-315. https://doi.org/10.1016/J.KJSS.2016.06.001.

Suryanti, S., Nusantara, T., Parta, I. N., & Irawati, S. (2023). Problem-Based Tasks in Mathematics Learning: Opportunities and Challenges for Teachers. *JTAM (Jurnal Teori dan Aplikasi Matematika), 7*(2), 372-383. https://doi.org/10.31764/jtam.v7i2.12864.

Treffers, A. (1993). Wiskobas and Freudenthal realistic mathematics education. *Educational Studies in Mathematics, 25*(1), 89-108. https://doi.org/10.1007/978-94-017-3377-9_6.

Webb, D. C., Van der Kooij, H., & Geist, M. R. (2011). Design research in the Netherlands: Introducing logarithms using realistic mathematics education. *Journal of Mathematics Education at Teachers College, 2*(1) 47-52. https://doi.org/10.7916/JMETC.V2I1.708.

Widodo, S., Santia, I., Katminingsih, Y., & Handayani, A. D. (2023). Increasing Students' Mathematical Problem Solving Ability Through Realistic Mathematics Education (RME). *International Journal of Research and Review, 10*(1), 68-76. https://doi.org/10.52403/ijrr.20230109.