International Journal of Educational Research Excellence (IJERE)
https://ejournal.ipinternasional.com/index.php/ijere

Volume 03, Issue 01, January-June 2024
e-ISSN: 2830-7933
DOI: 10.55299/ijere.v3i1.733

Application of Number Theory in Cryptography

Andreas Perdamenta Peranginangin*
Universitas Prima Indonesia
*)Corresponding Author: pprestasigemilang@gmail.com

Article history: received December 25, 2023; revised January 11, 2024; accepted January 15, 2024

Abstract. Life has changed in this era of technology. With technology, information can be searched easily and quickly, starting from the difficulty of finding information. Besides, people can easily store information in software or on the Internet. But you don't want this information to get out to anyone who doesn't want it. Therefore, data security is needed, which is applied using the science of cryptography, which uses material from number theory. This research will look at various cryptographic algorithms and processes for encrypting and decrypting data. This study uses library research or (library research). Library research involves gathering detailed information from numerous sources including literature, books, notes, journals, and other sources.

Keywords: cryptography, theory, application

I. INTRODUCTION

Information is crucial in our lives as it guides our decision-making. It can be obtained through personal experimentation, communication with others, or sources such as letters and news. It is important to note that subjective evaluations should be clearly marked as such. In today's technological era, obtaining information has become easier through software. Information can be easily and quickly accessed through the internet, videos, and other sources.

Technology also facilitates the storage of large, difficult-to-remember, or highly important information in software. However, it is crucial to process confidential information to prevent unauthorized access. It is imperative to ensure that confidential information stored in storage or on the internet is not exposed to unknown individuals.

Technology developers are searching for ways to secure stored information or data. This search continues until a method is found to process or manipulate data, which is called cryptography. Cryptography utilizes a material called Number Theory.

The author proposes to write a paper titled 'Application of Number Theory in Cryptography for Data Security.' The paper will provide examples of how number theory can be applied in cryptography to ensure data security.

Mathematics is a crucial field in human life, and number theory is one of its fundamental topics. This branch of mathematics finds a wide range of applications in various aspects of human life. Mathematics is a crucial field in human life, and number theory is one of its fundamental topics. Although technology is advancing rapidly, it can have both positive and negative effects.

While we tend to focus on the positive aspects, it is important to acknowledge the negative effects of technology as well. Technology is intended to simplify and speed up human affairs. However, if technology is used for malicious purposes, it can have negative consequences. Cybercrime is a common form of crime in the world of technology, especiallyin the field of information technology. Hacking of important information and data is becoming increasingly prevalent, causing discomfort for information technology users. A system was created to address this issue.

Cryptography is a solution to reduce cybercrime. It uses specific algorithms to transform information or data into random codes that are difficult for unauthorized individuals to read.

Volume 03, Issue 01, January-June 2024
e-ISSN: 2830-7933
DOI: 10.55299/ijere.v3i1.733

Number theory is utilized in cryptography to develop these algorithms. This paper discusses several applications of number theory in cryptography.

II. METHOD

Bibliographic research is a widely used method for gathering in-depth information. It involves gathering information from various sources such as literature, books, journals, and other relevant sources. Researchers can obtain information from books, journals, and dissertations that are relevant to the problem being studied. To collect data, researchers use three techniques: edit, organize, and find.

Editing involves checking the data for completeness and clarity.Organization involves putting the data into a framework, while analysis involves further examining the organized results using given rules, theories, and methods.The resulting answers are solutions to the problem at hand.Researchers commonly use three techniques to analyze data.Data reduction involves summarizing and selecting the main points that fit the theme or pattern.Data presentation can take the form of charts, brief descriptions, relationships between categories, flow diagrams, and other similar methods.The process of data analysis involves three main steps: data reduction, data presentation, and data interpretation. However, if strong, valid, and consistent evidence is found, the conclusion will become credible.

III. RESULT & DISCUSSION

Number theory is a branch of pure mathematics that focuses on the study of integers or integer-valued functions. Whole numbers, also known as integers, do not have decimal fractions. Examples of whole numbers include 8, 21, -5, and 0. Real numbers, on the other hand, have decimal points, such as 8.0, 6.7, and 1.9.

Integer division has a specific property. For instance, if a and b are integers, where a is not equal to 0, this property holds true. In number theory, a divides b if there exists an integer c such that $b = ac$. This division is denoted by $a \mid b$ if $b = ac$, $c \in \boldsymbol{Z}$, and $a \neq 0$. Euclidean theorems are also included in number theory. The Euclidean Theorem assumes that m and n are integers.

The nature of the division is denoted as $a \mid b$ if $b = ac$, where c is an integer and $a \neq 0$. Number theory also includes Euclidean theorems. The Euclidean theorem assumes that m and n are integers, where n is greater than 0. If m is divided by n, the result is q (quotient) and r (remainder), such that

$$m = nq + r$$

With $0 \leq r \leq n$.

The Greatest Common Divisor (GCD) is a concept in number theory. Given two non-zero integers, a and b, the GCD is the largest integer d that divides both a and b. If d is the GCD of a and b, it can be denoted as GCD(a,b) = d.

When two integers a and b have a GCD of 1, they are said to be relatively prime. For example, GCD(20,3) = 1, which means that 20 and 3 are relatively prime. If this is related to a linear combination, then a and b are relatively prime. So, integers m and n are

$$ma + nb = 1$$

GCD(a,b) can be expressed as a linear combination of a and b, where the coefficients are integers m and n. If a and b are positive integers, then this holds true.

$$\text{GCD}(a,b) = ma + nb.$$

Modulo arithmetic is a fundamental concept in number theory. The value m is called modulo, and the arithmetic result modulo m is always an element of the set {0, 1, 2, ..., m - 1}. Given integers a and m, where m is greater than 0, the operation $a \ mod \ m$ (pronounced "a $modulo \ m$") returns the remainder when a is divided by m.

Specifically, $a \ mod \ m = r$ where $a = mq + r$ and $0 \leq r < m$. The value m is referred to as the modulus or modulo, and the arithmetic result modulo m is always an element of the set {0, 1, 2, ..., $m - 1$}.

Congruency is a concept in number theory. If a and b are integers and $m > 0$, then $a \equiv b$ $(mod \ m)$ if and only if $m \mid (a - b)$. If a is not congruent to b in terms of modulus m, then it is written

$$a \not\equiv b \ (mod \ m).$$

Let m be a positive integer.

1) If $a \equiv b \ (mod \ m)$ and c is any integer then
- $(a + c) \equiv (b + c)(mod \ m)$
- $ac \equiv bc \ (mod \ m)$
- $ap \equiv bp \ (mod \ m)$, p non-negative integer

2) If $a \equiv b \ (mod \ m)$ and $c \equiv d \ (mod \ m)$, then
- $(a + c) \equiv (b + d)(mod \ m)$
- $ac \equiv bd \ (mod \ m)$

In real number arithmetic, the inverse of a non-zero number is a fraction such that the product of the two is equal to 1. If a is a non-zero number, then its inverse is $1/a$, such that $a \times 1 = 1$. The inverse of a is denoted by $a{-}1$. In modulo arithmetic, calculating the inverse modulo of an integer is more difficult. Given an integer a (mod m), if a and m are relatively prime and $m > 1$, then the inverse of a (mod m) exists. The inverse of a (mod m) is an integer x such that

$$xa \equiv 1 \ (mod \ m)$$

In other notation it can be written as

$$a^{-1}(mod \ m) = x$$

The combination of congruence and linear combination is linear congruence. Shaped linear congruence

$$ax \equiv b \ (mod \ m)$$

($m > 0$, a and b are any integers, and x is an integer variable).

The variable k is an integer that rounds x numbers.

The Euclidean algorithm is a well-known algorithm for finding the greatest common divisor of two integers. It was invented by Euclid, a Greek mathematician, and is based on the repeated application of the division algorithm.

Euclidean Algorithm Searching UN. Given two non-negative integers m and n (m ≥ n), then using the theorems explained previously, we can find the UN using the following steps:

1. If n = 0 then m is GCD(m, n); but if n □ 0, go to step 2.
2. Divide m by n and let r be the remainder.
3. Replace the m value with the n value and the n value with the r value, then go back to step 1.

Here's an illustration, for example $r0$ = m and $r1$ = n

$$r0 = r1 \ . \ q1 + r2 \ , \quad 0 \leq r2 < r1$$

$$r1 = r2 \ . \ q2 + r3 \ , \quad 0 \leq r3 < r2$$
$$\vdots$$
$$rn\text{-}1 = rn\text{-}1 \ . \ qn\text{-}1 + rn \ , \qquad 0 \leq rn < rn\text{-}1$$
$$rn = rn \ . \ qn + 0$$

So you get:

GCD(m, n) = GCD($r0, r1$) = GCD($r1, r2$) = …GCD(rn-1, rn) = GCD(rn, 0) = rn

Example : m = 76, n = 16 dan dipenuhi syarat m □ n

76 = 4□16 + 12
16 = 1□12 + 4
12 = 3□4 + 0

So you get:

GCD(76,16) = GCD(16,12) = GCD(12,4) =GCD(4,0) = 4

The Euclidean algorithm is a well-known algorithm. It was named after Euclid, a Greek mathematician who described it in his book, Elements.

Cryptography is a fundamental aspect of securing information. The term cryptography is derived from the Greek words cryptos and graphein, meaning secret and writing, respectively. Cryptography is a scientific field that studies mathematical techniques related to securing information, including confidentiality, integrity, and authentication. According to Schneier, cryptography is the science and art of maintaining message security. This includes maintaining confidentiality, ensuring data integrity, proving the sender's identity, and preventing the sender's deniability.

The field of cryptography includes several technical terms. Below is a list of common terminology used in cryptography:

1. Information that is presented in a way that is accessible to both visual and auditory senses..
2. The individual or entity transmitting the message..
3. The message recipient is the party who receives the message..
4. Ciphertext or messages are encoded to prevent unauthorized parties from reading them..
5. The process of encryption or encoding transforms plaintext into ciphertext..
6. During the decryption or restoration process, the ciphertext is transformed back into the original plaintext..
7. Cipher or encryption and decryption algorithm..
8. Keys or parameters used in encryption and decryption..
9. During the transmission process of messages, there may be eavesdroppers or individuals/machines attempting to intercept them..
10. Cryptoanalysis or the science and art of breaking ciphertext into plaintext without knowing the key used. The perpetrator of cryptanalysis is a cryptanalyst. Cryptoanalysis was first proposed by an Arab scientist in the 9th century named Abu Yusuf Yaqub Ibnu Ishaq Ibn As-Sabbah Ibnu 'Omran Ibnu Ismail Al-Kindi or better known as Al-Kindi.
11. Cryptology (cryptology) or the study of cryptology and cryptanalysis.

For thousands of years, cryptography has been a part of human life. Cryptography has a long history dating back to ancient times, despite its modern sophistication. For instance, cryptography was used in Ancient Egypt around 4000 years ago, where unusual hieroglyphs were employed to write messages on the walls of pyramids.

Volume 03, Issue 01, January-June 2024
e-ISSN: 2830-7933
DOI: 10.55299/ijere.v3i1.733

Ancient civilizations such as Egypt, Greece, Rome, and India used cryptography. The Greeks used the scytale 400 years before Christ. The Arab Origins of Cryptology book series, published by the King Faisal Center for Research and Islamic Studies in Saudi Arabia, documents the Arab history of cryptography.

It was used as a means of secret communication. Advice for women on how to understand writing using ciphers is given in the book Kama Sutra. Two types of ciphers are described: Kautiliyam and Mulavediy. Cryptography was also in use in Europe during the Renaissance, particularly in the 15th and 16th centuries. Many codes became popular during the Middle Ages:

1. The Vigenere Cipher is a cryptographic method that was first published by the French diplomat Blaise de Vigenere in 1586.
2. The Playfair Cipher is a cryptographic technique that was promoted by a British diplomat named Lord Playfair. It was originally invented by Charles Wheatstone in 1854.

Cryptography also had a tragic consequence. During the 17th century, Queen Mary of Scotland was captured after her encrypted message, containing a plan to assassinate Queen Elizabeth I, was successfully deciphered by Thomas Phelippes, a code breaker, while she was imprisoned. During World War II, cryptography was also used. The German Nazi government created an encryption machine called Enigma, which was successfully solved by the Allies. The success of solving Enigma is often considered a contributing factor to the relatively short duration of World War II.

Cryptography applies algorithms based on number theory. Various cryptographic algorithms exist, including the RSA, Elgamal, Diffie-Hellman key exchange, and knapsack cryptographic algorithms. Also cryptographic algorithms can be classified into three types: Symmetric Key Cryptography, Asymmetric Key Cryptography, and Hash Function.

Symmetric Key Cryptography, also known as Private or Secret Key Cryptography, is an algorithm that uses the same key for both encryption and decryption.This classic algorithm has been in use for over 4000 years. In order to decrypt a message sent with this algorithm, the recipient must have access to the key. The security of messages using this algorithm is entirely dependent on the key. Someone can encrypt and decrypt the message if they know the key.

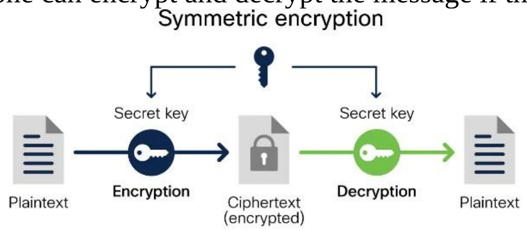

Figure 1. Symmetric Key Cryptography Concept

Algorithms that use symmetric keys include:

- RC2, RC4, RC5, RC 6
- *On Time Pad* (OTP)
- *Data Encryption Standard* (DES)
- *Advanced Encryption Standard* (AES)
- *International Data Encryption Algorithm* (IDEA)
- A5, dan lain sebagainya.

Asymmetric key cryptography uses different keys for encryption and decryption, also known as public key cryptography. This algorithm divides the key into two parts, namely:

1. Public key, a key that everyone is allowed to know (published).
2. Secret key (private key), a key that is kept secret (only known to one person).

These keys are related to each other. A public key can be used to encrypt messages, but it cannot be used to decrypt them. Only the person who possesses the secret key can decrypt the message. Asymmetric algorithms provide greater security for sending messages than symmetric algorithms.

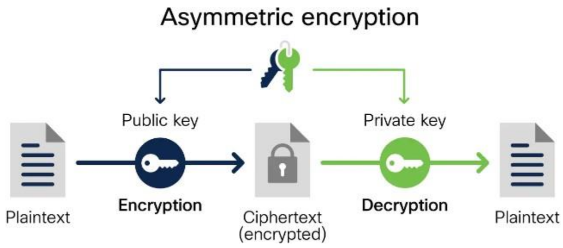

Figure 2. Asymmetric Key Cryptography Concept

Algorithms that use public keys include:

- *Digital Signature Algorithm* (DSA)
- *RSA*
- *Diffle-Hellman* (DH)\
- *Elliptic Curve Cryptography* (ECC)
- Quantum *Cryptography*

Hash function is a mathematical function that takes a variable-length input and converts it to a fixed-length binary sequence, often referred to as a one-way function, message digest, compression function, or message authentication code (MAC). The Hash function is commonly used to create a fingerprint of a message. Fingerprinting is a way to verify a message's authenticity and ensure it has not been tampered with.

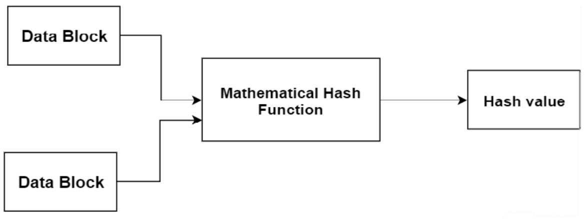

Figure 3. Asymmetric Key Cryptography Concept

Commonly used hash functions include:

- MD5
- SHA-1, SHA-2, SHA-3
- MAC

RSA is a widely used public-key algorithm that has many uses. It was discovered by Ronald Rivest, Adi Shamir, and Len Adleman, three researchers at the Massachusetts Institute of Technology, in 1976. The name RSA is derived from the initials of their last names. The challenge of factoring large integers into prime factors is the basis for the security of the RSA algorithm.

RSA's security is based on the difficulty of factoring the integer n into its prime factors (p and q), where $n = p \times q$. After factoring n in p and q, $(n) = (p\text{-}1) \times (q\text{-}1)$ can be computed. If the encryption key e is not kept secret, the decryption key d can be computed from the congruence $ed \equiv 1\ (mod(n))$.

According to the creator of the RSA algorithm, the values of p and q are recommended to exceed 100 digits, thus ensuring that the product $n = p$ x q exceeds 200 digits. It is important to note that the fastest factoring algorithms currently available are of high complexity.

For an integer n of b-bit length, no algorithm for factoring large integers in polynomial time has been found, making the RSA algorithm still considered safe at this time. The longer the integer, the more time it takes to factor it.

Volume 03, Issue 01, January-June 2024
e-ISSN: 2830-7933
DOI: 10.55299/ijere.v3i1.733

Although the RSA algorithm has several weaknesses, it is still widely used. It is slower than symmetric-key cryptographic algorithms such as DES and AES. The RSA algorithm is not used to encrypt messages, but rather to encrypt the symmetric key (session key) with the public key of the message recipient. The messages themselves are encrypted using a symmetric algorithm, such as DES or AES. Both the message and the symmetric key are sent simultaneously using the RSA algorithm. The receiver then decrypts the symmetric key using their private key and subsequently decrypts the message using the symmetric key.

The Elgamal algorithm was created by Taher Elgamal in 1985 and was first presented in a paper entitled It was first presented in a paper entitled "A public key cryptosystem and a signature scheme based on discrete logarithms". The difficulty of computing discrete logarithms is the basis of its security. This problem arises when p is a prime and g and y are arbitrary integers, and x is found to look

$$g^x \equiv y \ (mod\ p)$$

The encryption procedure for the Elgamal algorithm is as follows:

1. Arrange the plaintext into blocks
2. Choose a random number k, which satisfies $1 \leq k \leq p - 2$
3. Each block is encrypted with a formula

$$a = g^k \ mod\ p$$
$$b = y^k m \ mod\ p$$

The pair a and b is the ciphertext for the message block. So, the size of the ciphertext is 2 times the size of the plaintext. Apart from that, there is also a decryption procedure. The decryption procedure includes the following

1. Use private key x to calculate $(a^x)^{-1} \equiv a^{p-1-x}$.
2. Calculate plaintext with the following equation

$$m = \frac{b}{a^x} mod\ p = b(a^x)^{-1} mod\ p$$

Whitfield Diffie and Martin Hellman are the creators of the Diffie-Hellman key exchange algorithm. This algorithm enables two communicating entities to share the same secret key, which is then which is then used to encrypt messages using symmetric key cryptographic algorithms such as DES and AES. The difficulty of computing discrete logarithms makes the algorithm secure.

The Knapsack cryptographic algorithm, also known as the Merkle-Hellman algorithm, was discovered by Ralph Merkle and Martin Hellman in 1978. It is an early public key cryptographic algorithm. It is based on the Knapsack problem. The knapsack problem is a well-known NP-complete problem in algorithm theory, which means it cannot be solved in polynomial time.The knapsack cryptographic algorithm utilizes this problem by encoding messages as a series of solutions. In this algorithm, each weight (wi) in the knapsack problem serves as a secret key, while the plaintext bits represent bi.

The AES algorithm is a symmetric encryption and decryption algorithm that uses the same key. It has three key options: AES-128, AES-192, and AES-256, each with a different internal key called the round key for each round process. The AES-128 encryption process consists of 10 rounds, which are carried out as follows:

1. AddRoundKey
2. In each round, the following processes are carried out nine times: SubstituteBytes, ShiftRows, MixColumns, and AddRoundKey.
3. The final round involves the SubBytes, ShiftRows, and AddRoundKey processes.

During the AES-128 decryption process, the rotation process is also repeated 10 times. Specifically, it is carried out as follows:

1. AddRoundKey
2. In each of the 9 rounds, the following processes are carried out: InverseShiftRows, InverseSubstituteBytes, AddRoundKey, and InverseMixColumns.
3. The final round involves the InverseShiftRows, InverseSubBytes, and AddRoundKey processes.

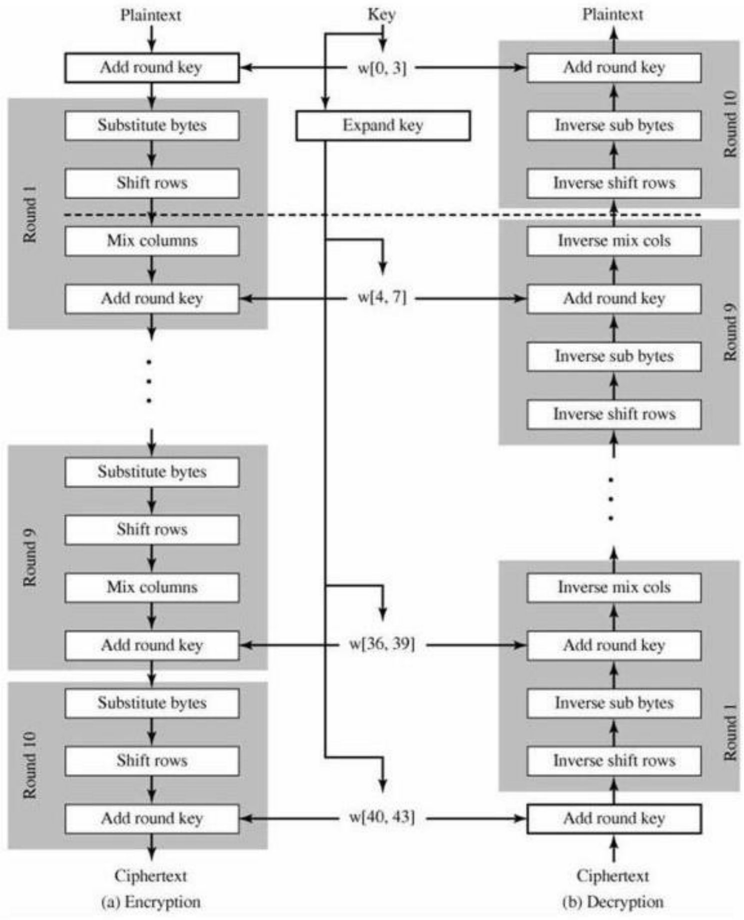

Figure 3. Concept of AES-128 Encryption and Decryption

IV. CONCLUSION

Number theory is a branch of mathematics with numerous applications, including algorithms in cryptography. Cryptography is the science of transforming meaningful information into meaningless information and vice versa.It is used to keep messages secret by utilizing specific algorithms or functions for encryption. Cryptography plays a crucial role in technology by enhancing security and preventing unauthorized data or information disclosure. Cryptographic algorithms based on number theory, such as the RSA, Elgamal, Diffie-Hellman key exchange, and knapsack cryptographic algorithms, are widely used. Cryptography is a valuable tool in technology as it aims to enhance security and prevent unauthorized data or information disclosure. There are various algorithms available for cryptography, and the selection of the most suitable algorithm depends on its intended use.

Volume 03, Issue 01, January-June 2024
e-ISSN: 2830-7933
DOI: 10.55299/ijere.v3i1.733

REFERENCES

A. Prayitno and N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," *J. Elektron. Sist. Inf. dan Komput.*, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com

AES -Advanced Encryption Standard-. http://studyinformatics.blogspot.com/2012/07/aes-advanced-encryption- standard.html. Diakses pada 12 Desember 2022

Algoritma RSA. https://komputerkata.com/algoritma-rsa/. Diakses pada 12 Desember 2022

Ariyus D, 2006. *Kriptografi: Keamanan Data dan Komunikasi*. Graha Ilmu. Yogyakarta.

Arrijal, I. M. A., Efendi, R., & Susilo, B. (2016). Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. Jurnal Pseudocode, 3(1), 69-82.). https://doi.org/10.33369/pseudocode.3.1.69-82

B. Solihin Hasugian, "Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019, doi: https://doi.org/10.46576/wdw.v0i53.269.

Endaryono; Dwitiyanti, Nurfidah; Setiawan, Heri Satria. 2021. *Aplikasi Operasi Matriks pada Perancangan Simulasi Metode Hill Cipher Menggunakan Microsft Excel.* STRING, Vol.6 No.1 Agustus 2021. http://dx.doi.org/10.30998/string.v6i1.8603

F. Aryani and Yulianis, 2018, "Trace Matriks Berbentuk Khusus 2 x 2 Berpangkat Bilangan Bulat Negatif," *J. Sains Mat. dan Stat.*, vol. 4, no. 2, pp. 105–113. http://dx.doi.org/10.24014/jsms.v4i2.5474

Ginting, Dahlia Br. 2010. *Peranan Aritmetika Modulo dan Bilangan Prima pada Algoritma Kriptografi RSA.* Media Informatika Vol.9 No.2 (2010).

Ibrahim. (2012). *Pembelajaran Matematika dengan ICT Sebagai Sarana Pengembangan Kecerdasan Emosional Siswa Menuju Pembangunan Karakter Bangsa*. Jurnal Fourier, *1*(2), 47–51. https://doi.org/10.14421/fourier.2012.12.47-51

Khabibah, 2001, "Suatu Alternatif Pembelajaran Matematika SD" *Makalah* disampaikan dalam seminar Nasional PMRI Tanggal 21 November 2001.

Kriptografi #2 (Macam-macam Algoritma Kriptografi). http://gilang-kurniawan.blogspot.com/2012/05/kriptografi-2-macam-macam- algoritma.html. Diakses pada 10 Desember 2022

Lismareni, N., Somakim., Kesumawati, N. (2014). Pengembangan Bahan Ajar Materi Aritmetika Sosial Menggunakan Konteks Bahan Bakar Minyak Dengan Pendekatan Pendidikan Matematika Realistik Indonesia Di SMP. *Jurnal Pendidikan Matematika UNSRI*, *1*, 1–12. http://dx.doi.org/10.22342/jpm.9.1.2186.48%20-%2058

Munir, Rinaldi, 2020. "Teori Bilangan (Bagian 1)". https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian1.pdf. Diakses pada 08 Desember 2022

Munir, Rinaldi, 2020. "Teori Bilangan (Bagian 3)". https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf. Diakses 08 Desember 2022

Musrikah. 2016. *Model Pembelajaran Matematika Realistik Sebagai Optimalisasi Kecerdasan Logika Matematika pada Siswa SD/MI.* TA'ALLUM, Vol.04., No.01, Juni 2016.

Puspita, K., &Wayahdi, M. R. (2015, February). Analisis Kombinasi Metode Caesar Cipher, Vernam Cipher, Dan Hill Cipher Dalam Proses Kriptografi. In Jurnal Seminar Nasional Teknologi Informasidan Multimedia).

Rebu, Marselinus Junardi. 2015. *Kriptografi Klasik.* Yogyakarta: Universitas Sanata Dharma

Volume 03, Issue 01, January-June 2024
e-ISSN: 2830-7933
DOI: 10.55299/ijere.v3i1.733

Schneier B, 1996. *Applied Cryptography: Protocols, Algorithms and Source Code in C 2nd Ed*. John Wiley & Sons, Inc. New Jersey.

T, A. M., Konseling, B., Pendidikan, F. I., & Surabaya, U. N. (2018). Studi Kepustakaan Mengenai Landasan Teori Dan Praktik Konseling Expressive Writing. *Jurnal BK UNESA*, *8*, 1–8. https://ejournal.unesa.ac.id/index.php/jurnal-bk-unesa/article/view/22037

What is Cryptography : Types, Tools and Its Algorithms. https://www.elprocus.com/cryptography-and-its-concepts/. Diakses pada 11 Desember 2022

What Is Encryption?. https://www.cisco.com/c/en/us/products/security/encryption-explained.html. Diakses pada 11 Desember 2022

Widaya, Wayan. 2018. *Modul Penyusunan Soal Keterampilan Berpikir Tingkat Tinggi (Higher Order Thingking Skills) Matematika.* Jakarta: Direktorat Pembinaan Sekolah Menengah Atas.

Yanti, Ili. 2022. *Analisis Kemampuan Literasi Matematika Siswa dalam Menyelesaikan Soal Higher Order Thingking Skill (HOTS) pada Materi Matriks di Sekolah Menengah Atas Al-Azhar Jambi.* Skripsi UIN Sulthan Thaha Saifuddin Jambi. Dipublikasikan. http://dx.doi.org/10.24127/ajpm.v11i3.5442