

ICETAR

THE 1st INTERNATIONAL CONFERENCE ON EDUCATIONAL THEORIES,
PRACTICES AND RESEARCH
TARBIYAH AND TEACHER TRAINING FACULTY, STATE ISLAMIC
UNIVERSITY SYEKH ALI HASAN AHMAD ADDARY
PADANGSIDIMPUAN ON 4TH - 5TH JULY, 2023
"Development of Post Pandemic Education to Face the Social Era 5.0"

Application of Integer Theory in Cryptography

Irma Rizki Aulia Efendi¹, Nur Fauziah Siregar,²

State Islamic University Syekh Ali Hasan Ahmad Addary Padangsidimpuan,
Indonesia

e-mail:¹ irmarizki@gmail.com, ² fauziahsrg@uinsyahada.ac.id

Abstract With the development of the times, science and mathematics also developed. The rapid development of mathematics is closely related to the world of information and communication. Where mathematics is also used as a scientific foundation. One of them is in the science of cryptography which uses integer theory as the basis of its knowledge. In this discussion, we will discuss the theory of integers in cryptography and how they relate
Keywords: Integer theory, mathematics, cryptography.

INTRODUCTION

Mathematics is a science that has been studied starting from elementary school to college which helps us solve many problems in everyday life. In higher education, especially in mathematics education study programs, mathematics is not a foreign thing because in college it is certain to study mathematics starting from the most basic to the complex.

Along with the development of the current era has changed everything both in terms of social science, culture, economics and science. As is the case in the field of mathematics which is closely related to engineering or often called engineering mathematics. In this discussion, we will touch on mathematics with information

engineering related to cryptography and algorithms. Where cryptography is closely related to integer theory (Setiawan et al, 2021).

Cryptography is the study of mathematical techniques related to aspects of information security, such as data confidentiality, data validity, data integrity, and data authentication (Rochmat, 2018). Its function is to secure the content of data or maintain the confidentiality of information from people who are not entitled to know the contents of the data. In this paper, we discuss what cryptography is, how to use it and its relationship with algorithms.

METHOD

This research uses a qualitative method using a library approach (library search), which uses literature review as the object of research. Qualitative research is a type of research by collecting data in the form of words used as data sources. The literature selected and used are articles relevant to the theory of integers in cryptography using Google Scholar search. The instrument in this research uses a human instrument, namely the researcher himself who acts as a research instrument. Then the research sample uses purposive technique because the sample taken is in accordance with the research theme. Data analysis in this research is descriptive qualitative.

RESULT AND DISCUSSION

A. Euclidean Algorithm

The Euclidean algorithm is one of the most effective methods in finding the Greatest Common Divisor (PBB) (Anwar et al, 2019). This method was known centuries ago. Euclid, the originator of the Euclidean Algorithm is a Greek mathematician scholar who wrote down his algorithm in his famous book entitled Element.

Formally, the Euclidean algorithm is formulated as follows.

Suppose m and n are non-negative integers with $m \geq n$. Suppose r_0 and $r_1 = n$, perform successive divisions as below.

$$r_0 = r_1q_1 + r_2 \quad 0 \leq r_2 \leq r_1$$

$$r_1 = r_2q_2 + r_3 \quad 0 \leq r_3 \leq r_2$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \quad 0 \leq r_n \leq r_{n-1}$$

$$r_{n-1} = r_nq_n + 0$$

Then the PBB of m and n (PBB(m,n)) is the last remainder of the division.

In short, the Euclidean algorithm is written as follows.

Euclidean Algorithm

1. If $n = 0$, then m is PBB(m,n); stop occurs if $n \neq 0$.
2. Divide m by n and let r be the remainder.
3. Replace the value of m with the value of n and the value of n with r, then go back to step 1.

Note: if $m \leq n$, then exchange the values of m and n.

B. Modulo Arithmetic

Modular Arithmetic or modulo arithmetic has an important role in integer computing, especially in cryptographic applications. The operator used in modulo arithmetic is mod (Endaryono, 2020). The mod operator, when used in integer division, gives the remainder of the division as the return. For example $53 \text{ mod } 5$ gives the result = 10 and remainder = 3. Then $53 \text{ mod } 5 = 3$. The definition of the mod operator is as follows.

Suppose a is an integer and m is an integer > 0 , the operation $a \text{ mod } m$ gives the remainder if a is divided by m. In other words $a \text{ mod } m = r$, such that $a = mq + r$, with $0 \leq r \leq m$.

1. Congruent

Sometimes two integers a and b, have the same remainder when divided by a positive integer m. We say that a and b are congruent modulo m and denoted as

$$a \equiv b \pmod{m}$$

If a is not congruent to b in modulo m, then it is written:

$$a \not\equiv b \pmod{m}$$

For example $53 \text{ mod } 5 = 3$ and $13 \text{ mod } 5 = 3$, then $53 \equiv 13 \pmod{5}$.

The formal definition of congruence is stated as follows.

Suppose a and b are integers and m is a number > 0 , then $a \equiv b \pmod{m}$ if m completely divides $a-b$.

The calculation properties of modulo arithmetics, especially with respect to multiplication and addition operations, are stated as follows.

Suppose m is a positive integer

1. If $a \equiv b \pmod{m}$ and c is any integer, then

$$\text{i. } (a+c) \equiv (b+c) \pmod{m}$$

$$\text{ii. } ac \equiv bc \pmod{m}$$

$$\text{iii. } a^p \equiv b^p \pmod{m} \text{ for } p \text{ integers } > 0$$

2. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\text{i. } (a+c) \equiv (b+d) \pmod{m}$$

$$\text{ii. } ac \equiv bd \pmod{m}$$

C. Prime Numbers

Prime numbers are positive integers that have important applications in computer science and mathematics. A prime number is a positive integer number greater than 1 that is only divisible by 1 and itself (Yusfrizal, 2019). Formally, the definition of prime numbers is as follows.

A positive integer p ($p > 1$) is called prime if the only numbers divisible by it are 1 and p . An example is the number 13. The number 13 is only divisible by 1 and 13. Then 13 is a prime number. Numbers other than prime are composite numbers. For example, 12 is a number that is divisible by 1, 2, 4, 6, 12.

An important theorem concerning prime numbers is stated by a well-known theorem in number theory, the fundamental theorem of arithmetic which contains the following. Every positive integer greater than or equal to 2 can be expressed as the product of one or more primes or composite numbers, both of which can be expressed as the product of one or more prime factors. For example,

$$9 = 3 \times 3 \quad (2 \text{ prime factors})$$

$$100 = 2 \times 2 \times 5 \times 5 \quad (4 \text{ prime factors})$$

$$13 = 13 \quad (1 \text{ prime factor})$$

$$12 = 2 \times 2 \times 3 \quad (3 \text{ prime factors})$$

D. Cryptography

Modulo arithmetic and prime numbers have many applications in computer science, one of the most important applications is cryptography. Cryptography comes from the Greek language: "cryptos" means "secret", while "graphein" means "writing". So, cryptography is secret writing. There are several definitions of cryptography that have been presented in various literatures. The definition used in older books (before the 1980s) states that cryptography is the science and art of keeping messages secret by encoding them into a form that is no longer understandable (Suhandinata et al, 2019). This definition may have been appropriate in the past when cryptography was used to secure important communications such as those between the military, diplomats and spies. However, today cryptography is more than just privacy, but also for the purposes of data integrity, authentication, and non-repudiation.

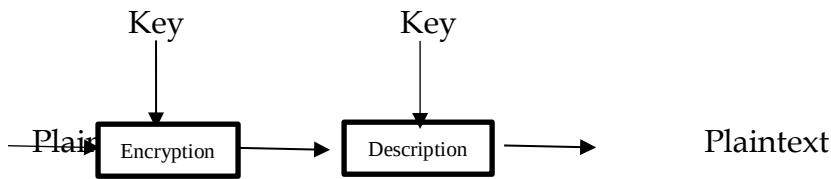
For comparison, in addition to this definition, there is also a definition put forward in :

Cryptography is the study of mathematical techniques that deal with aspects of information security such as confidentiality, data integrity, and authentication.

The word "art" in the definition comes from the historical fact that in the early days of cryptography, everyone had a unique way of keeping messages secret. These unique ways may have been different for each person using cryptography so that each way of writing a secret message had its own aesthetic value and cryptography evolved into an art of keeping messages secret. We will look at examples of cryptographic techniques from ancient times to the present day so that we can understand that cryptography can be viewed as an art of keeping messages secret. Later on, cryptography developed into its own discipline because cryptographic techniques can be mathematically formulated into a formal method.

There are several specialized terms in cryptography. The secret message is called the plaintext (clear and understandable text), while the obfuscated message is called the ciphertext (encrypted text). The process of transforming from plaintext to ciphertext is called encryption and the process of reversing from ciphertext to plaintext is called decryption. Encryption and decryption in a message masking

process has its own key. And only the right person knows the key. The figure below shows a diagram of the two processes in question.



Although the ciphertext is no longer secret, its content is unclear and its meaning cannot be understood. Only the right person can restore the obscure message to its original state using a key.

Cryptography can also be written in mathematical notation. If C stands for ciphertext and P stands for plaintext, then the encryption function E maps P to C, written as follows.

$$E(P) = C$$

In the reverse process, the description process, the function D maps C to P, written as follows.

$$D(C) = P$$

The process of encryption and then description returns the message to the original message, so the following equality must be true.

$$D(E(P)) = P$$

E. Relationship between Integer Theory and Cryptography

As explained earlier, cryptography is very relevant to mathematics, especially functions and integer theory which contains : 1) Integer and division properties, 2) Euclidean algorithm, 3) modulo arithmetic, and 4) prime numbers. It is very close because today's modern cryptography no longer bases the strength of cryptography on its algorithms. Instead, today's cryptography bases its cryptographic strength on the key. Before talking further, it would be nice to explain the strength of cryptography based on algorithms and keys as follows.

A cryptographic algorithm or chipper is a mathematical function used for encryption and description. The strength of a cryptographic algorithm is measured by the amount of work required to resolve the ciphertext data into its plaintext

(Putri et al, 2019). The more work required, the stronger the cryptographic algorithm, which means the safer it is to use to encode messages.

If the strength of the cryptography is determined by keeping the algorithm secret, then the cryptographic algorithm is called a restricted algorithm. Suppose a group of people agree to encode every message with the same algorithm, the algorithm is to exchange each word's first character with the second character, the third character with the fourth character and so on.

To describe the message, the same algorithm is used again. Unfortunately, the restricted algorithm is not suitable nowadays. If one person leaves the group, then the message encoding algorithm must be changed again as the confidentiality can no longer be relied upon. Modern cryptography no longer bases its strength on its algorithms. So the algorithm is no longer secret and can be known by the public. The strength of cryptography lies in the key which is a string of characters or a string of integers, kept secret. Only people who know the key can perform encryption and description. Keys are analogous in function to passwords on computer systems, PINs on ATMs or credit cards. The difference is that the password aims too

CONCLUSION

Through this explanation, it can be concluded that mathematics is closely related to engineering, especially in information engineering, namely cryptography. Where this cryptography is related to integer theory as explained above. Currently, cryptography has a strong relationship with digital computer systems in data and information security.

REFERENCES

- Anwar, Badrul, Nurcahyo Budi Nugroho, Jaka Prayudha, and Azanuddin Azanuddin. "Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam." *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)* 18, no. 1 (2019): 30.
- Dwi Putri, Yuningrat, Rosihan Rosihan, and Salkin Lutfi. "Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance." *JIKO (Jurnal*

- Informatika dan Komputer*) 2, no. 2 (2019): 87–94.
- Endaryono, Endaryono. “Perancangan Simulasi Metode Caesar Cipher Menggunakan Microsoft Excel – Alternatif Media Pembelajaran Kriptografi.” *SAP (Susunan Artikel Pendidikan)* 4, no. 3 (2020).
- Handbook of Applied Cryptography, <http://www.cacr.math.uwaterloo.ca/hac/> Diakses tanggal 18 Desember 2022
- Munir, Rinaldi. (2004). Diktat Kuliah IF2153 Matematika Diskrit, Edisi Keempat, Departemen Teknik Informasi, Institut Teknologi Bandung. 2022.
- Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informasi, Institut Teknologi Bandung.
- Nasrul, Kukuh. (2006). Penerapan Teori Bilangan Bulat dalam Kriptografi dan Aplikasinya dalam Kehidupan Sehari-hari. 2022
- Nur Rochmat, R.Rizal Isnanto. “Perancangan Aplikasi Data Daftar Pemilih Tetap (DPT) Untuk Panitia Pemungutan Suara (PPS)” 1, no. 2 (2018): 14–20.
- Setiawan, Erwan, Guntur Maulana Muhammad, and Muhamad Soeleman. “Analisis Kemampuan Pemecahan Masalah Mahasiswa Pada Mata Kuliah Teori Bilangan.” *Mosharafa: Jurnal Pendidikan Matematika* 10, no. 1 (2021): 61–72.
- Suhandinata, Sebastian, Reyhan Achmad Rizal, Dedy Ongky Wijaya, Prabhu Warren, and Srinjiwi Srinjiwi. “Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa.” *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)* 6, no. 1 (2019): 1–10.
- Yusfrizal. “Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android.” *Jurnal Teknik Informatika Kaputama (JTIK)* 3, no. 2 (2019): 29–37