PROSIDING
Seminar Nasional MIPA 2016
Naskah diseminarkan pada 5 November 2016 dan dipublikasikan pada
http://conf.unnes.ac.id/index.php/mipa/mipa2016/schedConf/presentations

Penerapan Jam Analog dalam Proses Seni Penyandian Menggunakan Algoritma Pembagian

Muhammad Rafid Fadil[1], Linda Permata Sari[2], Fitriyani[3], Nikken Prima P[4]
Departemen Matematika Fakultas FSM Universitas Diponegoro
mrfadil.25@gmail.com[1], linda.permata9@gmail.com[2], fitriyaniaja1@gmail.com[3], nikkenprima@yahoo.com[4]

Abstrak

Kriptografi adalah seni untuk menyembunyikan pesan, dalam prosesnya diperlukan algoritma untuk melakukan proses enkripsi dan deskripsi. Enkripsi dilakukan dengan cara mengkonversikan plainteks kedalam bilangan desimal sesuai Tabel ASCII, sedangkan untuk kuncinya digunakan aplikasi jam analog yang dikonversikan kedalam bentuk desimal. Proses enkripsi dimulai dengan menjumlahkan bilangan desimal pada plainteks dengan kunci yang telah dibuat dengan modulo 144. Bilangan desimal yang diperoleh diubah kedalam bentuk jam dengan bagian menit dikalikan bilangan desimal 5. Kemudian kelompokkan bentuknya menjadi 2 blok, blok pertama untuk bilangan yang menunjukkan jam dan blok kedua untuk bilangan yang menunjukkan menit. Selanjutnya seluruh blok diubah kedalam bentuk biner dengan panjang pada blok pertama 4 bit dan blok kedua 6 bit. Keseluruhan biner dikelompokkan menjadi 5 bit lalu dikonversikan kedalam bentuk desimal dan dijumlahkan 32. Hasilnya dikonversikan kedalam Tabel ASCII sehingga diperoleh chipperteksnya. Algoritma untuk proses deskripsi sejalan dengan proses enkripsi.

Kata kunci: Jam analog; deskripsi; enkripsi; Tabel ASCII

Abstract

Cryptography is the art hiding messages, in process required to make algorithms for encryption process and descriptions. Encryption is done by converting plaintext into decimal number corresponding ASCII table, whereas for the key used analog clock application that converted into decimal. Encryption begins by summing decimals in plaintext with key that made with modulo-144. Decimal numbers obtained is converted into form of hours with section minutes multiplied by decimal number 5. then the shape into two blocks, the first block of numbers that show hours and second block of numbers that indicate minutes. Subsequently, the whole block is converted into binary form with a length of 4-bits in the first block and the second block of 6-bits. entire binary grouped into 5-bit and converted into decimal form and summed-32. The result is converted into ASCII table for obtain chipperteks. algorithm for the description process in line with the encryption process.

Keywords*: analog clock; description; encryption; ASCII table*

PENDAHULUAN

Keamanan dalam berkomunikasi merupakan salah satu aspek terpenting dari kehidupan bersosialisasi. Seseorang memberikan informasi hanya kepada pihak yang berhak menerima informasi tersebut. Ketika suatu pesan akan dikirim dari pengirim ke penerima pesan, isi pesan dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan tersebut, maka pesan dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain. Cara untuk merahasiakan suatu pesan adalah dengan cara penyandian yang disebut kriptografi.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data,

integritas data, dan autentikasi data [3]. Dalam kriptografi terdapat istilah proses enkripsi dan dekripsi. Proses enkripsi adalah perubahan plainteks menjadi cipherteks atau pesan yang disembunyikan. Sedangkan proses dekripsi merupakan proses perubahan chiperteks menjadi plainteks atau pesan asli [5].

Berbagai macam algoritma digunakan dalam kriptografi. Variasi-variasi algoritma kriptografi telah banyak digunakan agar proses pengamanan pesan menjadi lebih aman. Salah satunya adalah penerapan jam analog dalam proses enkripsi dan dekripsi pada algoritma kriptografi. Jam analog merupakan jam yang menunjukkan waktu dengan jarum panjang menunjukkan menit *(minute hand)*, dan jarum pendek menunjukkan jam *(hour hand)*. Algoritma pembagian pada jam analog adalah algoritma hasil modifikasi dari algoritma kriptografi klasik. Algoritma ini bekerja dengan menggunakan sebuah satuan waktu baik sebagai model pada plainteks maupun kunci yang dikonversikan ke dalam bilangan desimal, begitu pula sebaliknya. Dalam hal ini, terdapat q merupakan karakter angka desimal yang akan dikonversikan menjadi satuan waktu, p merupakan karakter angka desimal 12, r merupakan karakter desimal yang mengacu pada jarum pendek pada jam analog (satuan jam), dan s merupakan karakter desimal yang mengacu pada jarum panjang pada jam analog (satuan menit). Algoritma ini juga digunakan untuk melakukan konversi pada kunci (karakter yang digunakan kunci adalah karakter satuan waktu) menjadi karakter angka desimal agar kunci tersebut dapat digunakan untuk melakukan enkripsi. Berdasarkan hal di atas, maka diharapkan kerahasiaan pesan menjadi lebih aman dan terjaga sehingga tidak mudah ditebak oleh pihak lain selain pengirim dan penerima pesan.

HASIL DAN PEMBAHASAN

1. Pemanfaatan Algoritma Pembagian

Pesan yang dibuat oleh penulis pesan maupun yang akan dibaca oleh penerima pesan terdiri dari karakter-karakter yang sesuai dengan tabel ASCII. Dalam hal ini, digunakan jam analog sebagai media untuk melakukan proses enkripsi dan dekripsi pesan. Dalam proses akan terdapat karakter yang menggunakan satuan waktu (misalkan pukul 08.15).

Algoritma utama yang digunakan untuk mendukung proses enkripsi dan dekripsi ini adalah algoritma pembagian [2]. Dengan algoritma ini sebagai berikut:

Jika p, q merupakan bilangan bulat dan $p > 0$, maka terdapat bilangan r dan s merupakan bilangan bulat tunggal, sehingga memenuhi

$q = r.\ p + s$, dengan $0 \leq s < p$.

Dari pernyataan diatas, maka r disebut hasil bagi (*quotient*), s disebut sisa (*remainder*), q disebut yang dibagi (*dividend*), dan p disebut pembagi (*divider*).

Algoritma pembagian dapat diterapkan pada jam analog, dimana algoritma ini digunakan untuk mengubah karakter angka desimal menjadi karakter satuan waktu, begitu pula sebaliknya. Dalam hal ini, dapat dikatakan q merupakan karakter angka desimal yang akan dikonversikan menjadi satuan waktu, p merupakan karakter angka desimal 12, r merupakan karakter desimal yang mengacu pada jarum pendek pada jam analog (satuan jam), dan s merupakan karakter desimal yang mengacu pada jarum panjang pada jam analog (satuan menit). Sehingga untuk selanjutnya q dapat dituliskan dalam satuan waktu sebagai berikut:

$q \rightarrow r.\ (5 \times s)$ (satuan waktu; dibaca pukul r lewat (5 x s) menit)

Dikatakan (5 x s) karena jika jarum panjang menunjukkan ke arah s (s merupakan suatu bilangan bulat) pada jam analog, maka jarum panjang itu pasti menunjukkan (5 x s) menit.

Ditetapkan nilai dari karakter angka desimal p adalah 12 karena dalam jam analog terdiri dari 12 angka, sehingga jika perhitungan algoritma pembagian diterapkan kepada jam analog maka nilai s tidak boleh melebihi angka 12 (dalam jam analog, jarum panjang menunjukkan angka 12 berarti menunjukkan 0 menit).

Algoritma pembagian ini juga digunakan untuk melakukan konversi pada kunci (karakter yang digunakan kunci adalah karakter satuan waktu) menjadi karakter angka desimal agar kunci tersebut dapat digunakan untuk melakukan enkripsi.

2. Algoritma Enkripsi

Proses enkripsi diperlukan pembuat pesan untuk mengubah pesan yang berupa plainteks menjadi cipherteks. Proses enkripsi dilakukan sebagai berikut:

1. Menentukan plainteks yang akan dienkripsi.
2. Menentukan kata kunci yang akan digunakan untuk proses enkripsi dan dekripsi. (Kata kunci berupa satuan waktu, yang selanjutnya akan dikonversikan menjadi angka desimal)
3. Melakukan konversi pada setiap karakter plainteks menjadi angka desimal sesuai dengan tabel ASCII.
4. Melakukan proses enkripsi yang pertama, dengan langkah sebagai berikut:
   $x_i = p_i + x_{i-1} + K \pmod{144}$, dengan i = 1, 2, ... , n dan $x_0 = 0$.
   Dimana:
   x_i = Karakter ke-i hasil proses enkripsi pertama
   p_i = Karakter ke-i plainteks yang telah dikonversi menjadi angka desimal
   K = Kata kunci yang telah dikonversi menjadi angka desimal
   n = Jumlah karakter plainteks
   Proses enkripsi yang pertama selesai [4].
5. Melakukan proses enkripsi yang kedua, dimana dalam proses ini menggunakan algoritma pembagian, dengan langkah sebagai berikut:
   $x_i = q_i \cdot 12 + r_i$
   dengan i = 1, 2, ... , n , $0 \leq r_i < 12$, q_i dan r_i merupakan bilangan bulat.
6. Perhatikan nilai dari karakter q_i dan r_i. Untuk selanjutnya nilai karakter q_i mengacu pada jarum pendek pada jam analog, sedangkan nilai karakter r_i mengacu pada jarum panjang pada jam analog, sehingga diperoleh nilai dari karakter x_i yang dikonversikan ke dalam satuan waktu, atau dapat ditulis:
   $x_i \longrightarrow q_i.5r_i$ (satuan waktu ; dibaca pukul q_i lebih $5r_i$ menit)
   dengan i = 1, 2, ... , n.
   Proses enkripsi yang kedua selesai.
7. Mengelompokkan nilai dari karakter q_i dan $5r_i$ menjadi dua bagian yang dapat dituliskan sebagai berikut:
   $q_1q_2q_3...q_n(5r_1)(5r_2)(5r_3)...(5r_n)$
8. Melakukan proses enkripsi yang ketiga, dimana untuk q_i , i = 1, 2, ... , n , dikonversikan ke dalam karakter bilangan biner dengan panjang 4 bit setiap blok, sedangkan untuk r_i , i = 1, 2, ... , n , dikonversikan ke dalam karakter bilangan biner dengan panjang 6 bit setiap blok.
9. Keseluruhan bilangan biner dikelompokkan menjadi 5 bit tiap blok, kemudian dikonversikan ke dalam karakter angka desimal dan tambahkan 32.
   Proses enkripsi yang ketiga selesai.
10. Melakukan konversi tiap karakter angka desimal ke dalam karakter cipherteks sesuai dengan tabel ASCII, sehingga diperoleh cipherteks tersebut. Dengan ini proses enkripsi selesai.

3. Algoritma Dekripsi

Kemudian proses dekripsi juga diperlukan bagi penerima pesan untuk menerjemahkan pesan yang berupa cipherteks menjadi plainteks. Dalam hal ini, pembuat pesan dan penerima pesan harus menyepakati algoritma enkripsi dan dekripsi yang digunakan agar penerima pesan dapat menerjemahkan pesan yang disampaikan oleh pembuat pesan. Proses dekripsi dilakukan dengan langkah sebagai berikut:

1. Melakukan konversi pada setiap karakter cipherteks menjadi angka desimal sesuai dengan tabel ASCII, lalu kurangkan setiap karakter yang telah dikonversi dengan angka desimal 32.
2. Melakukan proses dekripsi yang pertama, dimana setiap karakter dikonversikan ke dalam karakter biner dengan panjang 5 bit setiap blok.
3. Jika banyaknya karakter cipher teks adalah sebanyak 2xn karakter, maka karakter biner diatas dibagi menjadi dua bagian. Untuk bagian pertama karakter bilangan biner dikelompokkan menjadi 4 bit setiap bloknya sebanyak n blok, kemudian untuk bagian kedua karakter bilangan biner dikelompokkan menjadi 6 bit setiap bloknya sebanyak n blok.
4. Setiap blok dikonversikan ke dalam karakter angka desimal yang dapat di tuliskan sebagai berikut:
   $q_1q_2q_3...q_nr_1r_2r_3...r_n$
   Dimana:
   q_i = Karakter desimal ke-i yang merupakan hasil konversi dari karakter bilangan biner dengan panjang 4 bit
   r_i = Karakter desimal ke-i yang merupakan hasil konversi dari karakter bilangan biner dengan panjang 6 bit
   Proses dekripsi yang pertama selesai.
5. Mengambil setiap karakter q_i dan r_i selanjutnya digabung menjadi sebuah karakter dengan satuan waktu (nilai dari karakter q_i mengacu pada jarum pendek pada jam analog, sedangkan nilai dari karakter r_i mengacu pada jarum panjang pada jam analog) yang akan disebut sebagai x_i. Dengan kata lain:
   $x_i \longrightarrow q_i.r_i$ (satuan waktu ; dibaca pukul q_i lebih r_i menit)
   Catatan: Nilai dari karakter r_i pasti habis dibagi 5.
6. Melakukan proses dekripsi yang kedua, dimana dalam proses ini karakter x_i yang berupa satuan waktu akan dikonversikan menjadi karakter angka desimal. Proses ini menggunakan algoritma pembagian, dengan langkah sebagai berikut:
   $x_i = q_i \,.\, 12 + (r_i / 5)$
   dengan i = 1, 2, ... , n , $0 \leq (r_i / 5) < 12$, q_i dan $(r_i / 5)$ merupakan bilangan bulat.
   Proses deskripsi yang kedua selesai.
7. Melakukan proses dekripsi yang ketiga, dimana setiap karakter x_i akan dikonversikan ke dalam karakter desimal p_i dengan bantuan kunci, dengan langkah sebagai berikut:
   $p_i = x_i - x_{i-1} - K \pmod{144}$, dengan i = 1, 2, ... , n dan $x_0 = 0$.
   Dimana:
   x_i = Karakter angka desimal ke-i hasil proses deskripsi kedua
   p_i = Karakter angka desimal ke-i hasil proses dekripsi ketiga
   K = Kata kunci yang telah dikonversi menjadi angka desimal
   n = Jumlah karakter plainteks
   Proses deskripsi yang ketiga selesai [4].
8. Melakukan konversi tiap karakter angka desimal p_i ke dalam karakter plainteks sesuai dengan tabel ASCII, sehingga diperoleh plainteks tersebut. Dengan ini proses dekripsi selesai.

4. Algoritma Kunci

Setiap pesan pasti mempunyai kunci yang dapat membantu melakukan proses enkripsi dan dekripsi pesan. Kunci yang digunakan pada algoritma ini merupakan satuan waktu. Dengan kata lain:

$K \longrightarrow q.r$ (satuan waktu ; dibaca pukul q lebih r menit)

Dengan K adalah kunci dari sebuah pesan yang masih berupa satuan waktu.

Ada beberapa ketentuan mengenai kunci yang akan digunakan untuk proses enkripsi dan dekripsi yaitu sebagai berikut:

- Kunci tersebut merupakan satuan waktu yang menggunakan sistem 12 jam (Apabila kunci yang digunakan adalah 15.30, maka akan sama dengan 03.30)
- Apabila bagian menit pada kunci tersebut bukan kelipatan 5, maka dilakukan pembulatan ke atas hingga ke kelipatan 5 terdekat (Misalkan 05.23 dibulatkan menjadi 05.25, dan 10.56 dibulatkan menjadi 11.00)

Kunci tersebut akan dikonversikan menjadi karakter angka desimal dengan menggunakan algoritma pembagian [1], dengan langkah sebagai berikut:

$$K = q \cdot 12 + r$$

dengan $i = 1, 2, \ldots, n$, $0 \leq r_i < 12$, q_i dan r_i merupakan bilangan bulat.
Sehingga diperoleh kunci yang berupa karakter angka desimal.

5. Penerapan Algoritma Kunci

Algoritma kunci diperlukan agar kunci dapat dikonversikan menjadi karakter angka desimal yang selanjutnya dapat digunakan untuk melakukan proses enkripsi dan dekripsi. Agar lebih jelas, diberikan contoh sebagai berikut:

Kunci yang akan digunakan adalah 02.30.

Dari kunci diatas, diketahui bahwa dalam jam analog, kunci tersebut menunjukkan angka 2 sebagai satuan jam dan menunjukkan angka 6 sebagai satuan menit. Maka kunci tersebut akan dikonversikan menjadi karakter angka desimal dengan menggunakan algoritma pembagian, sehingga:

$$K = 02.30 \rightarrow 2 \cdot 12 + 6 = 30$$

Maka diperoleh kunci yang telah dikonversi dari satuan waktu yaitu K = 30.

6. Penerapan Algoritma Enkripsi

Agar lebih jelas, diberikan contoh pesan yang akan dienkripsikan menjadi cipherteks yaitu sebagai berikut:

Plainteks : KRIPTOGRAFI (11 Karakter)

Misalkan pembuat pesan menentukan jam (kunci) yang digunakan adalah 02.30.

Maka dapat dilakukan proses enkripsi sebagai berikut:

K	R	I	P	T		O	G	R	A	F	I
↓	↓	↓	↓	↓	(i)	↓	↓	↓	↓	↓	↓
75	82	73	80	84		79	71	82	65	70	73
↓	↓	↓	↓	↓	(ii)	↓	↓	↓	↓	↓	↓
105	73	32	142	112		77	34	2	97	53	12

Langkah (i) : Melakukan konversi ke dalam karakter angka desimal (Sesuai tabel ASCII)
Langkah (ii) : Melakukan proses enkripsi pertama

Kemudian dilakukan proses enkripsi yang kedua dengan menggunakan algoritma pembagian [2], diperoleh:

$105 = 8 \cdot 12 + 9 \rightarrow 08.45$
$73 = 6 \cdot 12 + 1 \rightarrow 06.05$
$32 = 2 \cdot 12 + 8 \rightarrow 02.40$
$142 = 11 \cdot 12 + 10 \rightarrow 11.50$
$112 = 9 \cdot 12 + 4 \rightarrow 09.20$
$77 = 6 \cdot 12 + 5 \rightarrow 06.25$
$34 = 2 \cdot 12 + 10 \rightarrow 02.50$
$2 = 0 \cdot 12 + 2 \rightarrow 00.10$

97 = 8 . 12 + 1 → 08.05
53 = 4 . 12 + 5 → 04.25
12 = 1 . 12 + 0 → 01.00
Kemudian setiap karakter yang berupa satuan jam dikelompokkan menjadi dua bagian, yaitu bagian pertama yang memuat semua karakter yang berupa satuan jam, dan bagian kedua yang memuat semua karakter satuan menit. Sehingga menjadi:
08 06 02 11 09 06 02 00 08 04 01 45 05 40 50 20 25 50 10 05 25 00
Bagian Pertama Bagian Kedua
Kemudian dilakukan proses enkripsi yang ketiga, dimana bagian pertama dikonversikan menjadi karakter bilangan biner dengan panjang 4 bit dan bagian kedua dikonversikan menjadi karakter bilangan biner dengan panjang 6 bit. Sehingga diperoleh:
1000 0110 0010 1011 1001 0110 0010 0000 1000 0100 0001 101101 000101 101000 110010 010100 011001 110010 001010 000101 011001 000000
Kemudian semua karakter bilangan biner dikelompokkan menjadi 5 bit sehingga menjadi:
10000 11000 10101 11001 01100 01000 00100 00100 00011 01101 00010 11010 00110 01001 01000 11001 11001 00010 10000 10101 10010 00000
Konversikan karakter bilangan biner diatas ke dalam karakter angka desimal sehingga diperoleh:
16 24 21 25 12 08 04 04 03 13 02 26 06 09 08 25 25 02 16 21 18 00
Kemudian setiap karakter ditambahkan dengan 32 sehingga diperoleh:
48 56 53 57 44 40 36 36 35 45 34 58 38 41 40 57 57 34 48 53 50 32
Lalu dilakukan konversi ke dalam karakter cipher teks (sesuai tabel ASCII), sehingga diperoleh:
0 8 5 9 , ($ $ # – " : &) (9 9 " 0 5 2 Spasi
Cipherteks yang dihasilkan : 0859,($$#–":&)(99"052 (22 Karakter)

7. Penerapan Algoritma Dekripsi

Agar lebih jelas, diberikan contoh cipherteks yang telah diperoleh dari hasil enkripsi untuk didekripsikan kembali menjadi plainteks yaitu sebagai berikut:
Cipherteks : 0859,($$#–":&)(99"052 (22 Karakter)
Misalkan pembuat pesan menentukan jam (kunci) yang digunakan adalah 02.30.
Maka dapat dilakukan proses dekripsi sebagai berikut:
0 8 5 9 , ($ $ # – " : &) (9 9 " 0 5 2 Spasi
Kemudian melakukan konversi ke karakter desimal sesuai tabel ASCII, sehingga diperoleh:
48 56 53 57 44 40 36 36 35 45 34 58 38 41 40 57 57 34 48 53 50 32
Lalu, setiap karakter dikurangkan dengan 32 sehingga diperoleh:
16 24 21 25 12 08 04 04 03 13 02 26 06 09 08 25 25 02 16 21 18 00
Setelah itu, dilakukan proses dekripsi pertama, dimana setiap karakter dikonversikan ke dalam karakter bilangan biner sehingga menjadi:
10000 11000 10101 11001 01100 01000 00100 00100 00011 01101 00010 11010 00110 01001 01000 11001 11001 00010 10000 10101 10010 00000
Kemudian karena banyaknya karakter ada 22, maka karakter bilangan biner diatas dibagi menjadi dua bagian, dimana bagian pertama karakter bilangan biner dikelompokkan menjadi 4 bit sebanyak 11 blok, bagian kedua karakter bilangan biner dikelompokkan menjadi 6 bit sebanyak 11 blok.
1000 0110 0010 1011 1001 0110 0010 0000 1000 0100 0001 (Bagian pertama)
101101 000101 101000 110010 010100 011001 110010 001010 000101 011001 000000 (Bagian kedua)
Setiap karakter bilangan biner diatas dikonversikan ke dalam karakter angka desimal sehingga menjadi:

08 06 02 11 09 06 02 00 08 04 01 | 45 05 40 50 20 25 50 10 05 25 00

Bagian Pertama Bagian Kedua

Ambil karakter pertama pada bagian pertama dan karakter pertama pada bagian kedua, lalu gabungkan untuk menjadi karakter dengan satuan waktu, dan seterusnya. Kemudian dilakukan proses dekripsi yang kedua, sehingga menjadi:

08.45 → 8 . 12 + 9 = 105
06.05 → 6 . 12 + 1 = 73
02.40 → 2 . 12 + 8 = 32
11.50 → 11 . 12 + 10 = 142
09.20 → 9 . 12 + 4 = 112
06.25 → 6 . 12 + 5 = 77
02.50 → 2 . 12 + 10 = 34
00.10 → 0 . 12 + 2 = 2
08.05 → 8 . 12 + 1 = 97
04.25 → 4 . 12 + 5 = 53
01.00 → 1 . 12 + 0 = 1

Kemudian dari karakter diatas, dilakukan proses dekripsi yang ketiga sehingga diperoleh:

105	73	32	142	112	77	34	2	97	53	12
↓	↓	↓	↓	↓	(i) ↓	↓	↓	↓	↓	↓
75	82	73	80	84	79	71	82	65	70	73
↓	↓	↓	↓	↓	(ii) ↓	↓	↓	↓	↓	↓
K	R	I	P	T	O	G	R	A	F	I

Langkah (i) : Melakukan proses dekripsi ketiga
Langkah (ii) : Melakukan konversi ke dalam karakter plainteks (Sesuai tabel ASCII)
Plainteks yang dihasilkan: KRIPTOGRAFI (11 Karakter)

KESIMPULAN

Pemanfaatan jam analog ini termasuk kedalam salah satu contoh dari kriptografi klasik. Pada proses enkripsi dan proses deskripsi dilakukan secara manual dari proses pengiriman pesan dan penerimaan pesan. Dalam prosesnya dibutuhkan ketelitian dalam penggunaan table, perubahan dari chipperteks ke plainteks, dan sebaliknya agar yang dihasilkan dapat dibaca oleh penerima dengan kunci rahasia yang hanya diketahui oleh pihak pengirim dan pihak penerima saja.

DAFTAR PUSTAKA

[1] Hoffstein, J. (2000). *An Introduction to Mathematical Cryptography*. Network.
[2] Muhsetyo, Gatot. (2014). *Teori Bilangan Edisi 1*. Tangerang Selatan: Universitas Terbuka.
[3] Munir, Rinaldi. (2004). *Pengantar Kriptografi*. Bandung: Informatika.
[4] Munir, Rinaldi. (2014). *Matematika Diskrit (Edisi Revisi Kelima)*. Bandung: Informatika.
[5] Schneier, Bruce. (1996). *Applied Cryptography, Second Edition: Protocol, Algorithms, and Source Code in C (cloth)*. John Wiley & Sons, Inc.