

Pengamanan Short Message Service (SMS) Menggunakan Algoritma Vibranium Cipher

Nifeyani Gulo^{1*}

¹Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: ^{1*}nifeyani_gulo@gmail.com

Abstrak—Pengamanan SMS (Short Message Service) merupakan salah satu kegiatan yang dilakukan agar SMS dari sebuah informasi yang dirahasiakan tidak dapat diketahui oleh orang lain kecuali orang-orang yang diberi hak untuk itu. Terdapat beberapa pendekatan teknik pengamanan SMS hingga saat ini masih digunakan oleh sejumlah kalangan diantaranya dengan menerapkan teknik kriptografi, teknik steganografi, watermark dan teknik lainnya. Sebuah pesan yang tidak di sandikan atau dienkripsi disebut plaintext, Sedangkan pesan yang telah disandikan dengan sebuah algoritma kriptografi disebut ciphertext. Kriptografi merupakan suatu teknik mengamankan pesan dengan melakukan enkripsi terhadap isi pesan tersebut agar aman, sedangkan short message service merupakan layanan yang disediakan oleh telepon seluler ataupun android untuk mengirim dan menerima pesan. Terjadinya penyadapan pada jalur komunikasi, maka teks SMS akan sangat mudah di baca oleh penyadap, Dalam enkripsi data khususnya yang dibahas yaitu SMS, terdapat berbagai algoritma yang dapat digunakan untuk mengamankan data, salah satunya algoritma vibranium cipher yang menggunakan blok dengan ukuran 128 bit yang dapat membantu pengguna untuk mengirim pesan singkat dengan aman, cepat dan mudah

Kata Kunci: Kriptografi, Short Message Service (SMS), Plaintext, Ciphertext.

Abstract—Security of SMS (Short Message Service) is one of the activities carried out so that SMS from an undisclosed information cannot be known by other people except those who are given the right to do so. There are several approaches to SMS security techniques that are still used by a number of people today, including by applying cryptographic techniques, steganographic techniques, watermarks and other techniques. A message that is not encoded or encrypted is called plaintext, while a message that has been encoded with a cryptographic algorithm is called ciphertext. . Cryptography is a technique of securing messages by encrypting the contents of the message so that it is safe, while the short message service is a service provided by cellular or Android phones to send and receive messages. The tapping occurs on the communication line, so the SMS text will be very easy to read by tapping, in data encryption, especially the one discussed, namely SMS, there are various algorithms that can be used to secure data, one of which is the vibranium cipher algorithm which uses blocks with a size of 128 bits which can help users to send short messages safely, quickly and easily

Keywords: Cryptography, Short Message Service (SMS), Plaintext, Ciphertext.

1. PENDAHULUAN

Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (cryptology). Kriptografi bertujuan untuk menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah [1].

SMS (Short Message Service) merupakan layanan yang banyak diaplikasikan pada sistem komunikasi tanpa kabel (nir kabel). Pesan pertama yang dikirim menggunakan SMS dilakukan pada bulan Desember 1992, dikirim dari sebuah Personal Computer (PC) ke telepon mobile dalam jaringan GSM milik Vodafone Inggris. Layanan yang disediakan oleh telepon seluler untuk mengirim dan menerima pesan singkat, sangat praktis dan murah serta sangat efisien. Namun SMS (Short Message Service) yang masuk di perangkat pengguna merupakan salah satu privasi bagi dirinya [2]

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting didalam pengiriman atau penerimaan sms. Salah satu masalahnya terjadi penyadapan sehingga keamanan rahasia pribadinya dapat terbongkar. Disisi lain dengan fasilitas SMS yang ada, maka timbul pertanyaan bagaimana keamanan informasi jika seseorang mengirimkan suatu informasi rahasia melalui fasilitas sms. Pengirim tentu saja menginginkan pesan dapat dikirim secara aman, yaitu ia yakin bahwa pihak lain tidak dapat membaca isi pesan yang ia kirim. Hal yang sudah biasa dilakukan untuk mengirim pesan dengan aman yaitu dengan cara menghapus Sms secara otomatis segera setelah 40 detik pesan di baca atau di kenal dengan nama self-destruct text message. Ada juga pengamanan sms dengan menggunakan kriptografi sms yang memanfaatkan kunci untuk mendeskripsikan SMS yang telah di enkripsi.

Penelitian ini akan mencoba menguraikan proses yang dilakukan untuk mengkombinasikan teknik kriptografi dalam mengamankan sms. Teknik kriptografi digunakan untuk melakukan penyandian Sms rahasia berdasarkan algoritma vibranium cipher yang melakukan enkripsi dan dekripsi kepada sebuah pesan dengan cara membagi pesan-pesan tersebut ke dalam beberapa blok., pergeseran bit, dan operasi XOR dan juga cipher ini dapat menggunakan tabel s- box untuk meningkatkan kompleksitas ini akan menggunakan prinsip jaringan feistel untuk memperkuat algoritma sehingga sulit untuk dipecahkan. [3]

Dalam penelitian sebelumnya Algoritma Vibranium Cipher diterapkan oleh Ade Dermawan, Eriq Muhammad Adams Jonemaro, & Tri Afianto di Jurnal Ilmu Teknik Teknologi Vol.3 No.5, Mei 2017 ISSN:2337-5779 dan E-ISSN:2338-5502. Algoritma cipher ini merupakan salah satu cara kriptografi yang membagi plaintext yang diubah menjadi blok-blok pesan dengan ukuran tertentu yang besarnya telah di tentukan sebelumnya. Algoritma ini telah memenuhi prinsip Diffusion dan confusion Shannon, karena dengan perubahan satu karakter yang signifikan pada ciphertext dan mempunyai kompleksitas yang baik disebabkan kesulitan dalam melakukan bruteforce terhadap ciphertext. [3]

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi merupakan ilmu yang mempelajari untuk menyembunyikan suatu pesan. Kriptografi (*cryptography*) berasal dari bahasa Yunani, yaitu *cryptos* (penulisan) dan *graphia* yang berarti (rahasia) dari dua kata tersebut dapat didefinisikan yaitu sebuah teknik penulis yang dirahasiakan. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi dalam pengertian modern adalah ilmu yang berdasarkan dengan teknik matematika yang berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data, dan otentikasi entitas. [6]

2.2 SMS (Short Message Service)

SMS adalah kemampuan untuk mengirim dan menerima pesan singkat dalam bentuk singkat dalam bentuk teks dari sebuah perangkat nirkabel, yaitu perangkat telekomunikasi telepon seluler, dalam hal ini perangkat nirkabel yang digunakan adalah telepon seluler. Teks tersebut bisa berupa kata-kata atau nomor ataupun kombinasi alfanumerik [5].

Pendapat lain mengenai pengertian SMS diutarakan oleh Romzi Imron yang mengungkapkan tentang pengertian SMS adalah layanan yang banyak diaplikasikan pada jaringan komunikasi tanpa kabel yang memungkinkan dilakukannya pengiriman pesan dalam bentuk alfanumerik antar terminal pelanggan (ponsel) atau antara terminal pelanggan dengan sistem eksternal seperti e-mail, paging, voice mail, dan sebagainya. Aplikasi SMS merupakan aplikasi yang memiliki banyak peminat dan pengguna saat ini walaupun banyak digantikan oleh aplikasi berbasis mobile seperti WhatsApp, BlackBerry Messenger, Facebook Messenger, Line dan lain-lain.

2.3 Algoritma Vibranium Cipher

Sebuah algoritma blok cipher baru, bernama Vibranium Cipher. Cipher ini mengandalkan berbagai operasi matematika seperti, pergeseran bit, dan operasi XOR. Selain itu, cipher ini juga menggunakan tabel permutasi dan tabel S-Box untuk meningkatkan kompleksitas. Kriptografi merupakan ilmu mengamankan pesan, sehingga pesan tidak dibaca/diakses oleh yang tidak berkepentingan. Ilmu ini telah digunakan sejak zaman Julius Caesar. Dengan berkembangnya ilmu pengetahuan, maka ilmu kriptografi juga semakin berkembang [8].

Block Cipher merupakan salah satu algoritma kriptografi, dimana setiap plaintext dibagi menjadi blok-blok. Kemudian pengoperasian akan dilakukan berdasarkan blok-blok tersebut. Dalam paper ini, penulis ingin mengajukan sebuah algoritma blok cipher yang baru, yang dinamakan Vibranium Cipher. Kami mengajukan algoritma ini karena kami ingin adanya suatu algoritma blok cipher yang mudah diimplementasikan serta sederhana.

Blok cipher adalah suatu metode pengenkripsian yang beroperasi berdasarkan blok. Cara kerjanya adalah dengan cara membagi plaintext menjadi blok-blok yang besarnya telah ditentukan sebelumnya.

Terdapat 5 mode pengoperasian dalam Block Cipher:

1. Electronic Code Book (ECB)
Plaintext dibagi menjadi blok-blok, dan lakukan enkripsi pada setiap blok tersebut secara terpisah.
2. Cipher Block Chaining (CBC)
Setiap blok plaintext di-XOR-kan dengan ciphertext sebelumnya sebelum melakukan enkripsi
3. Cipher Feedback (CFB)
Pada mode ini, membuat block cipher menjadi stream cipher. Mode ini sangat mirip dengan mode CBC, dimana ciphertext sebelumnya dienkripsi terlebih dahulu, kemudian di-XOR-kan dengan plaintext.
4. Output Feedback (OFB)
Mode ini juga membuat block cipher menjadi stream cipher. Ciphertext didapatkan dari hasil operasi XOR antara plaintext dan hasil enkripsi dari tahap sebelumnya. Pada round pertama, digunakan initialization Vector (IV).
5. Mode counter
Dalam mode ini, setiap pengirim dan penerima harus dapat mengakses sebuah counter yang reliable, di mana nilai dari counter tersebut akan diakses setiap ciphertext blok dipertukarkan. Nilai counter ini tidak harus rahasia.

Diffusion dan confusion merupakan salah satu cara kriptografer untuk memperkuat kriptografi sehingga tidak dapat melakukan analisis frekuensi dan memberikan perbedaan besar pada ciphertext hanya dengan sedikit perubahan pada plaintext. Diffusion adalah metode untuk menyebarkan pengaruh perubahan dari suatu karakter atau bagian pada input dapat mengubah banyak atau seluruh bagian output. Metode yang dapat digunakan untuk melakukan hal ini adalah menggunakan permutasi. Dengan difusi ini, pola-pola yang ada seharusnya hilang atau tersebar. Sedangkan confusion adalah metode untuk menghilangkan bentuk statistik yang dapat muncul pada sebuah bahasa atau kata-kata yang beraturan, hal ini dapat dilakukan dengan cara melakukan substitusi sehingga mengubah input secara drastis ketika menjadi output.

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Analisa merupakan proses penguraian konsep kedalam bagian-bagian yang lebih sederhana, sedemikian rupa sehingga struktur logisnya menjadi jelas. Kegiatan penguraian dari suatu sistem yang utuh kedalam bagian komponennya dengan

maksud untuk mengidentifikasi dan mengevaluasi permasalahan-permasalahan, hambatan yang terjadi dan kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan.

Permasalahan yang di analisa pada penelitian ini di fokuskan pada poin-poin masalah yang telah dirumuskan pada bagian pendahuluan yaitu peningkatan pengamanan SMS dengan menerapkan kombinasi teknik kriptografi dengan tujuan agar dapat meminimalisir pencurian dan penyalahgunaan SMS yang sifatnya rahasia.

Masalah keamanan SMS hingga saat ini menjadi salah satu hal yang dianggap sangat penting dalam menjaga kerahasiaan terhadap tindakan-tindakan pencurian, penyalahgunaan, yang dapat saja dilakukan oleh pihak-pihak yang tidak memiliki hak akses. Namun tidak diherankan juga bahwa tindakan tersebut dapat merugikan pihak-pihak pemilik pesan maupun pihak penerima pesan yang sebenarnya.

Teknik kriptografi dengan algoritma yang digunakan mampu merubah seluruh katakter SMS asli menjadi karakter-karakter yang justru tidak memiliki makna yang berkoresponden lagi dengan pesan aslinya. Hal inilah yang disebut penyandian SMS (proses enkripsi). Semakin rumit algoritma dan kunci yang digunakan, maka hasil sandi yang dihasilkan lebih sulit terpecahkan. Masing –masing pihak yang menggunakan teknik kriptografi (baik pengirim maupun penerima SMS) harus menyepakati algoritma dan kunci yang digunakan dalam proses enkripsi SMS yang didistribusikan.

SMS yang akan didistribusikan akan disandikan terlebih dahulu oleh pihak pengirim berdasarkan algoritma kriptografi yang telah disepakati sebelumnya kemudian dikirimkan kepada penerima yang sah. Apabila suatu saat pesan itu diambil atau diketahui oleh pihak lain maka sudah tentu mereka tidak dapat mengetahui pesan sebenarnya apa, karena yang dikirimkan adalah karakter-karakter hasil sandi dari SMS asli.

3.1.1 Penerapan Metode Vibranium Cipher

Vibranium Cipher adalah algoritma kriptografi jenis block. Vibranium cipher menggunakan blok dengan ukuran 128 bit. Dimana blok intinya diubah dengan menggunakan jaringan feistel. Setiap byte ganjil pada blok akan dipertukarkan dengan byte yang berada kanannya. Selanjutnya blok akan di XOR dengan kunci, dan kemudian hasil XOR akan digeser ke kanan sebesar satu blok. Setelah byte-byte pada blok digeser, blok akan disubstitusikan dengan menggunakan S-Box dan kemudian di XOR kan kembali dengan kunci. Secara umum, algoritma ini menggunakan jaringan feistel yang diulang sebanyak 16 kali. Besar blok pesan yang digunakan adalah sebesar 128 bit yang kemudian dibagi menjadi dua bagian, 64 bit untuk pesan bagian kiri dan 64 bit untuk pesan bagian kanan. Kunci internal akan digenerate sebanyak 16 kali, satu kunci untuk setiap perulangan jaringan feistel. Panjang kunci yang dimasukkan pengguna minimal 64 bit. Apabila pengguna memasukkan kunci dengan panjang lebih dari 64 bit, yang terpakai hanya 64 bit.

Ddata yang digunakan untuk melakukan perhitungan terhadap algoritma vibranium cipher, dengan menggunakan SMS (Short Message Service). Adapun isi pesan SMS yang akan dienkripsi:

Pesan = Selamat Pagi!

Kunci = Nifeyani Gulo

Langkah 1 : Konversi Karakter Pesan dan Kunci ke dalam Nilai Hexadecimal

Melakukan konversi karakter ke nilai hexadecimal penulis menggunakan tabel bantu ASCII dan juga aplikasi konversi online dengan link <http://www.convertstring.com>, berikut hasil konversi yang dilakukan

Pesan = 53 65 6C 61 6D 61 74 20 50 61 67 69 21

Kunci = 4E 69 66 65 79 61 6E 69 20 47 75 6C 6F

Langkah 2 : Membagi Pesan Menjadi Dua Blok, Blok Kanan dan Blok Kiri masing-masing berjumlah 64 bit.

Pesan (L) = 53 65 6C 61 6D 61 74 20

Pesan (R) = 50 61 67 69 21 00 00 00

Keterangan:

L = Left (Kiri)

R = Right (Kanan)

Langkah 3 : Lakukan Proses Round Function terhadap Pesan (R)

Pesan (R) = 50 61 67 69 21 00 00 00

PUTARAN 1 :

1. Pertukaran Byte (R')

Lakukan perpindahan posisi byte disetiap bilangan hexadecimal dengan cara, bilangan hexadecimal yang berposisi di kiri di pindahkan ke kanan, dan demikian sebaliknya, hal ini dilakukan mulai dari pinggir sisi kiri blok Pesan (R). Lebih jelasnya dapat dilihat pada penerapan berikut.

Pesan (R) = 50 61 67 69 21 00 00 00

Pesan (R') = 61 50 69 67 00 21 00 00

2. Lakukan XOR antara blok dengan kunci

Kunci internal akan digenerate sebanyak 16 kali, satu kunci untuk setiap perulangan jaringan feistel. Panjang kunci yang dimasukkan pengguna minimal 64 bit. Apabila pengguna memasukkan kunci dengan panjang lebih dari 64 bit, yang terpakai hanya 64 bit. Hal ini karena pada algoritma ini ukuran blok tetap. Kunci internal dilakukan dengan menggeserkan byte kunci ke kanan sebanyak perputaran jaringan feistel. Jika jaringan feistel berada pada perputaran pertama, maka kunci yang akan digunakan adalah kunci hasil pergeseran ke kanan sebanyak satu pergeseran, jika jaringan feistel berada pada putaran ke dua, maka kunci yang digunakan adalah kunci hasil pergeseran ke kanan sebanyak 2 pergeseran. Hal yang sama dilakukan juga pada putaran berikutnya. Dari nilai kunci

Dari nilai hexadecimal Kunci awal 4E69666579616E692047756C6F Maka nilai hexadecimal kunci yang digunakan adalah Kunci = 4E69666579616E69

Lakukan proses XOR terhadap pesan dan kunci:

Pesan (R') = 61 50 69 67 00 21 00 00

Kunci = 4E 69 66 65 79 61 6E 69

Pesan = 01100001 01010000 01101001 01100111 00000000 00100001 00000000 00000000

Kunci = 01001110 01101001 01100110 01100101 01110001 01100001 01101110 01101001

Maka generate kunci proses putaran 1 yaitu melakukan pergeseran 1 bit kekanan, berikut hasilnya

K1 = 10011100 11010010 11001100 11001010 11110010 11000010 11011100 11010010

R0 = 01100001 01010000 01101001 01100111 00000000 00100001 00000000 00000000

K1 = 10011100 11010010 11001100 11001010 11110010 11000010 11011100 11010010

11111101 10000010 10110101 10101101 11110010 11100011 11011100 11010010

3. Rotasi Blok

R = 11010010 11111101 10000010 10110101 1010110 11110010 11100011 11011100

R = D2 FD 82 B5 CD F2 E3 DC

4. Substitusi S-BOX

R = D2 FD 82 B5 CD F2 E3 DC

R = F4 C5 32 4C C3 B7 8B 7A

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L0 = 53 65 6C 61 6D 61 74 20

R1 = F4 C5 32 4C C3 67 8B 7A +

A7 A0 5E 2D AE D6 FF 54

PUTARAN 2 :

L = R (Putaran 1)

= A7 A0 5E 2D AE D6 FF 54

1. Pertukaran Byte (R')

Pesan (R) = A7 A0 5E 2D AE D6 FF 54

Pesan (R') = A0 A7 2D 5E D6 AE 54 FF

Kunci awal = 01001110 01101001 01100110 01100101 01110001 01100001 01101110 01101001

Maka generate kunci proses putaran 2 yaitu melakukan pergeseran 2 bit kekanan, berikut hasilnya

K2 = 00111001 10100101 10011001 10010101 11100101 10000101 10111001 10100101

2. XOR Blok Kunci

R1 = 10100000 10100111 00101101 01011110 11010110 10101110 01010100 1111111

K2 = 00111001 10100101 10011001 10010101 11100101 10000101 10111001 10100101

= 10011001 10000010 10111100 11001011 00110011 00101011 11101101 01011010

3. Rotasi Blok

R = 01011010 10011001 10000010 10111100 11001011 00110011 00101011 11101101

R = 5A 99 82 BC CB 33 2B ED

4. Substitusi S-BOX

R = 5A 99 82 BC CB 33 2B ED

R = 5B FF 32 01 B9 9A 58 AB

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L1 = 50 61 67 69 21 00 00 00

R2 = 5B FF 32 01 B9 9A 58 AB +

0B 9E 55 68 98 9A 58 AB

PUTARAN 3 :

L = R (Putaran 2)

= 0B 9E 55 68 98 9A 58 AB

1. Pertukaran Byte (R')

Pesan (R) = 0B 9E 55 68 98 9A 58 AB

Pesan (R') = 9E 0B 68 55 9A 98 AB 58

Kunci awal = 01001110 01101001 01100110 01100101 01110001 01100001 01101110 01101001

Maka generate kunci proses putaran 3 yaitu melakukan pergeseran 3 bit kekanan, berikut hasilnya

K3 = 01110011 01001011 00110011 00101011 11001011 00001011 01110011 01001010

2. XOR Blok Kunci

R2 = 10011110 00001011 01101000 01010101 10011010 10011000 10101011 01011000

K3 = 01110011 01001011 00110011 00101011 11001011 00001011 01110011 01001010

11101101 00000000 01011011 01111110 01010001 10010011 11011000 00010010

1. Rotasi Blok

R = 00010010 11101101 00000000 01011011 01111110 01010001 10010011 11011000

R = 12 ED 00 5B 7E 51 93 D8

2. Substitusi S-BOX

R = 12 ED 00 5B 7E 51 93 D8

R = 81 AB 0C 34 78 D2 84 A9

3. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L2 = 0B 9E 55 68 98 9A 58 AB

R3 = 81 AB 0C 34 78 D2 84 A9 +
8A 35 59 5C E0 48 DC 02

PUTARAN 4 :

L= R (Putaran 3)

= 8A 35 59 5C E0 48 DC 02

1. Pertukaran Byte (R')

Pesan (R) = 8A 35 59 5C E0 48 DC 02

Pesan (R') = 35 8A 5C 59 48 E0 48 02

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001

Maka generate kunci proses putaran 4 yaitu melakukan pergeseran 4 bit kekanan, berikut hasilnya

K4 = 11100110 10010110 01100110 01010111 10010110 00010110 11100110 10010100

2. XOR Blok Kunci

R3 = 00110101 10001010 01011100 01011001 01001000 11100000 01001000 00000010

K4 = 11100110 10010110 01100110 01010111 10010110 00010110 11100110 10010100
11010001 00011100 00111010 00001110 11011010 11110110 10101011 10010110

3. Rotasi Blok

R = 10010110 11010001 00011100 00111010 00001110 11011010 11110110 10101011

R = 96 D1 1C 3A 0E DA F6 AB

4. Substitusi S-BOX

R = 96 D1 1C 3A 0E DA F6 AB

R = 85 C6 0A CE 02 80 31 12

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L3 = 8A 35 59 5C E0 48 DC 02

R4 = 85 C6 0A CE 02 80 31 12 +
0F F3 53 92 E2 C8 ED 10

PUTARAN 5 :

L= R (Putaran 4)

= 0F F3 53 92 E2 C8 ED 10

1. Pertukaran Byte (R')

Pesan (R) = 0F F3 53 92 E2 C8 ED 10

Pesan (R') = F3 0F 92 53 C8 E2 10 ED

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001

Maka generate kunci proses putaran 5 yaitu melakukan pergeseran 5 bit kekanan, berikut hasilnya

K5 = 11001101 00101100 11001100 10101111 00101100 00101101 11001101 00101001

2. XOR Blok Kunci

R4 = 11110011 00001111 10010010 01010011 11001000 11100010 00010000 11101101

K5 = 11001101 00101100 11001100 10101111 00101100 00101101 11001101 00101001
= 00111110 01100011 01011110 10111100 11100100 11001111 11011101 11000100

3. Rotasi Blok

R = 11000100 00111110 01100011 01011110 10111100 11100100 11001111 11011101

R = C4 3E 63 5E BC E4 CF DD

4. Substitusi S-BOX

R = C4 3E 63 5E BC E4 CF DD

R = 7E 79 3E F7 01 62 55 93

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L4 = 0F F3 53 92 E2 C8 ED 10

R5 = 7E 79 3E F7 01 62 55 93 +
71 8A 6D 65 E3 AA B8 83

PUTARAN 6 :

L= R (Putaran 5)

= 71 8A 6D 65 E3 AA B8 83

1. Pertukaran Byte (R')

Pesan (R) = 71 8A 6D 65 E3 AA B8 83

Pesan (R') = 8A 71 65 6D AA E3 B8 83

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001
01101110 01101001

Maka generate kunci proses putaran 6 yaitu melakukan pergeseran 6 bit kekanan, berikut hasilnya

K5 = 10011010 01011001 10011001 01011110 01011000 01011011 10011010 01010011

2. XOR Blok Kunci

R4 = 10001010 01110001 01100101 01101101 10101010 11100011 11001000 10000011

K5 = 10011010 01011001 10011001 01011110 01011000 01011011 10011010 01010011
00010000 00101000 00101100 00110011 01111010 10111000 00110010 11010000

3. Rotasi Blok

R = 11010000 00010000 00101000 00101100 00110011 01111010 10111000 00110010

R = D0 10 28 3C 33 7A B8 32

4. Substitusi S-BOX

R = D0 10 28 3C 33 7A B8 32

R = BF 86 3A B3 9A 57 96 E4

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L5 = 71 8A 6D 65 E3 AA B8 83

R6 = BF 86 3A B3 9A 57 96 E4 +
CE 0C 57 D6 79 FD 2E 67

PUTARAN 7 :

L = R (Putaran 6)

= CE 0C 57 D6 79 FD 2E 67

1. Pertukaran Byte (R')

Pesan (R) = CE 0C 57 D6 79 FD 2E 67

Pesan (R') = 0C CE D6 57 FD 79 67 2E

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001

Maka generate kunci proses putaran 7 yaitu melakukan pergeseran 7 bit kekanan, berikut hasilnya

K6 = 00110100 10110011 00110010 10111100 10110000 10110111 00110100 10100111

2. XOR Blok Kunci

R5 = 00001100 11001110 11010110 01010111 11111101 01111001 01100111 00101110

K6 = 00110100 10110011 00110010 10111100 10110000 10110111 00110100 10100111
00111000 01111100 11100100 10001011 01001101 01001010 11010011 10001001

3. Rotasi Blok

R = 10001001 00111000 01111100 11100100 10001011 01001101 01001010 11010011

R = 89 38 7C D4 8B 4B 4A D3

4. Substitusi S-BOX

R = 89 38 7C D4 8B 4B 4A D3

R = 89 6D 09 0B 99 5F A2 69

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L6 = CE 0C 57 D6 79 FD 2E 67

R7 = 89 6D 09 0B 99 5F A2 69 +
47 61 5E DD E0 A2 8C 0E

PUTARAN 8 :

L = R (Putaran 7)

= 47 61 5E DD E0 A2 8C 0E

1. Pertukaran Byte (R')

Pesan (R) = 47 61 5E DD E0 A2 8C 0E

Pesan (R') = 61 47 DD 5E A2 E0 0E 8C

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001

Maka generate kunci proses putaran 8 yaitu melakukan pergeseran 8 bit kekanan, berikut hasilnya

Hasil Kunci = 01101001 01100110 01100101 01111001 01100001 01101110 01101001 01001110

2. XOR Blok Kunci

R7 = 01100001 01000111 11011101 01011110 10100010 11100000 00001110 10001100

K8 = 01101001 01100110 01100101 01111001 01100001 01101110 01101001 01001110
= 10001000 00100001 10111000 00100111 11000011 10000110 01100111 01000010

3. Rotasi Blok

R = 01000010 10001000 00100001 10111000 00100111 11000011 10000110 01100111

R = 42 88 21 B8 27 C3 86 67

4. Substitusi S-BOX
 $R = 42\ 88\ 21\ B8\ 27\ C3\ 86\ 67$
 $R = B8\ 28\ A6\ 96\ ED\ 43\ 60\ 65$
5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)
 $L7 = 47\ 61\ 5E\ DD\ E0\ A2\ 8C\ 0E$
 $R8 = \underline{B8\ 28\ A6\ 96\ ED\ 43\ 60\ 65} +$
 $\quad FF\ 49\ F8\ 4B\ 0D\ E1\ EC\ 6B$

PUTARAN 9 :

L= R (Putaran 8)

= FF 49 F8 4B 0D E1 EC 6B

1. Pertukaran Byte (R')
 Pesan (R) = FF 49 F8 4B 0D E1 EC 6B
 Pesan (R') = 49 FF 4B F8 E1 0D 6B EC
 Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001
 Maka generate kunci proses putaran 9 yaitu melakukan pergeseran 9 bit kekanan, berikut hasilnya
 $K9 = 11010010\ 11001100\ 11001010\ 11110010\ 11000010\ 11011100\ 0\ 11010010\ 10011100$
2. XOR Blok Kunci
 $R8 = 01001001\ 11111111\ 01001011\ 11111000\ 11100001\ 00001101\ 01101101\ 11101100$
 $K9 = \underline{11010010\ 11001100\ 11001010\ 11110010\ 11000010\ 11011100\ 11010010\ 10011100}$
 $= 10011011\ 00110011\ 10000001\ 00001010\ 00100011\ 11010001\ 10111111\ 01110000$
3. Rotasi Blok
 $R = 01110000\ 10011011\ 00110011\ 10000001\ 00001010\ 00100011\ 11010001\ 10111111$
 $R = 70\ 9B\ 33\ 81\ 0A\ 23\ D1\ BF$
4. Substitusi S-BOX
 $R = 70\ 9B\ 33\ 81\ 0A\ 23\ D1\ BF$
 $R = EC\ 75\ 9A\ F0\ 90\ 17\ C6\ EF$
5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)
 $L8 = FF\ 49\ F8\ 4B\ 0D\ E1\ EC\ 6B$
 $R9 = \underline{EC\ 75\ 9A\ F0\ 90\ 17\ C6\ EF} +$
 $\quad 13\ 3C\ 62\ BB\ 9D\ F6\ 2A\ 84$

PUTARAN 10 :

L= R (Putaran 9)

= 13 3C 62 BB 9D F6 2A 84

1. Pertukaran Byte (R')
 Pesan (R) = 13 3C 62 BB 9D F6 2A 84
 Pesan (R') = 3C 13 BB 62 F6 9D 84 2A
 Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001
 Maka generate kunci proses putaran 10 yaitu melakukan pergeseran 10 bit kekanan, berikut hasilnya
 $K10 = 10100101\ 10011001\ 10010101\ 11100101\ 10000101\ 10111001\ 10100101\ 00111001$
2. XOR Blok Kunci
 $R9 = 00111011\ 00010011\ 10111011\ 01100010\ 11110110\ 10011101\ 10000100\ 00101010$
 $K10 = \underline{10100101\ 10011001\ 10010101\ 11100101\ 10000101\ 10111001\ 10100101\ 00111001}$
 $\quad 10011110\ 10101010\ 00101110\ 10010111\ 01010011\ 00100100\ 00100001\ 00010011$
3. Rotasi Blok
 $R = 00010011\ 10011110\ 10101010\ 00101110\ 10010111\ 01010011\ 00100100\ 00100001$
 $R = 13\ 9E\ AA\ 2E\ 97\ 53\ 24\ 21$
4. Substitusi S-BOX
 $R = 13\ 9E\ AA\ 2E\ 97\ 53\ 24\ 21$
 $R = 3B\ 8F\ 8E\ A4\ 72\ A1\ 45\ A6$
5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)
 $L9 = 13\ 3C\ 62\ BB\ 9D\ F6\ 2A\ 84$
 $R10 = \underline{3B\ 8F\ 8E\ A4\ 72\ A1\ 45\ A6} +$
 $\quad 28\ B3\ EC\ 1F\ EF\ 57\ 6F\ 22$

PUTARAN 11 :

L= R (Putaran 10)

= 28 B3 EC 1F EF 57 6F 22

1. Pertukaran Byte (R')
 Pesan (R) = 28 B3 EC 1F EF 57 6F 22
 Pesan (R') = B3 28 1F EC 57 EF 22 6F

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001
 Maka generate kunci proses putaran 11 yaitu melakukan pergeseran 11 bit kekanan, berikut hasilnya
 K11 = 01001011 00110011 00101011 11001011 00001011 01110011 01001010 01110011

2. XOR Blok Kunci

R10=10110011 00101000 00011111 11101100 01010111 11101111 00100010 01101111
 K11=01001011 00110011 00101011 11001011 00001011 01110011 01001010 01110011
 = 10011000 00011011 00110100 00100101 01011100 10010100 01101000 00011100

3. Rotasi Blok

R = 00011100 10011000 00011011 00110100 00100101 01011100 10010100 01101000
 R = 1C 98 1B 34 25 5C 94 68

4. Substitusi S-BOX

R = 1C 98 1B 34 25 5C 94 68
 R = 0A AC 91 78 76 21 33 8D

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L10 = 28 B3 EC 1F EF 57 6F 22
 R11 = 0A AC 91 78 76 21 33 8D +
 22 1F 7D 67 99 76 5C AF

PUTARAN 12 :

L= R (Putaran 11)

= 22 1F 7D 67 99 76 5C AF

1. Pertukaran Byte (R')

Pesan (R) = 22 1F 7D 67 99 76 5C AF
 Pesan (R') = 1F 22 67 7D 76 99 AF 5C

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001
 Maka generate kunci proses putaran 12 yaitu melakukan pergeseran 12 bit kekanan, berikut hasilnya
 K12 = 10010110 01100110 01010111 10010110 00010110 11100110 10010100 11100110

2. XOR Blok Kunci

R11=00011111 00100010 01100111 01111101 01110110 10011001 10101111 01011100
 K12=10010110 01100110 01010111 10010110 00010110 11100110 10010100 11100110
 = 10001001 01000100 00110000 00101011 01100000 01111111 00111011 10111010

3. Rotasi Blok

R = 10111010 10001001 01000100 00110000 00101011 01100000 01111111 00111011
 R = BA 89 44 30 2B 60 7F 3B

4. Substitusi S-BOX

R = BA 89 44 30 2B 60 7F 3B
 R = 3F 89 AA D4 58 24 11 DC

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L11 = 53 65 6C 61 6D 61 74 20
 R12 = 3F 89 AA D4 58 24 11 DC +
 6C EC C6 B5 35 45 65 FC

PUTARAN 13 :

L= R (Putaran 12)

= 6C EC C6 B5 35 45 65 FC

1. Pertukaran Byte (R')

Pesan (R) = 6C EC C6 B5 35 45 65 FC
 Pesan (R') = EC 6C B5 C6 45 35 FC 65

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001
 Maka generate kunci proses putaran 13 yaitu melakukan pergeseran 13 bit kekanan, berikut hasilnya
 K13 = 00101100 11001100 10101111 00101100 00101101 1100110 1 00101001 11001101

2. XOR Blok Kunci

R12=11101100 01101100 10110101 11000110 01000101 00110101 11111100 01100101
 K13=00101100 11001100 10101111 00101100 00101101 11001101 00101001 11001101
 = 11000000 10100000 00011010 11101010 10101000 11011000 11010101 10101000

3. Rotasi Blok

R = 10101000 11000000 10100000 00011010 11101010 10101000 11011000 11010101
 R = A8 B0 A0 1A EA A8 B8 B5

4. Substitusi S-BOX

R = A8 B0 A0 1A EA A8 B8 B5
 R = 1A B2 39 26 BD 1A 96 4C

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L12 = 6C EC C6 B5 35 45 65 FC

R13 = 1A B2 39 26 BD 1A 96 4C +
76 5E FF 93 88 5F F3 B0**PUTARAN 14 :**

L= R (Putaran 13)

= 76 5E FF 93 88 5F F3 B0

1. Pertukaran Byte (R')

Pesan (R) = 76 5E FF 93 88 5F F3 B0

Pesan (R') = 5E 76 93 FF 5F 88 B0 F3

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001

Maka generate kunci proses putaran 14 yaitu melakukan pergeseran 14 bit kekanan, berikut hasilnya

K14 = 01011001 10011001 01011110 01011000 01011011 10011010 01010011 10011010

2. XOR Blok Kunci

R13=01011110 01110110 10010011 11111111 01011111 10001000 10110000 11110011

K14=01011001 10011001 01011110 01011000 01011011 10011010 01010011 10011010

= 00000111 11101111 11001100 10100111 10000100 00010010 00100101 01101001

3. Rotasi Blok

R = 01101001 00000111 11101111 11001100 10100111 10000100 00010010 00100101

R = 69 07 0F CC A7 84 12 25

4. Substitusi S-BOX

R = 69 07 0F CC A7 84 12 25

R = 59 B4 40 D6 F8 B0 81 76

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L13 = 76 5E FF 93 88 5F F3 B0

R14 = 59 B4 40 D6 F8 B0 81 76 +
2F EA BF 45 70 EF 72 C6**PUTARAN 15 :**

L= R (Putaran 14)

= 2F EA BF 45 70 EF 72 C6

1. Pertukaran Byte (R')

Pesan (R) = 2F EA BF 45 70 EF 72 C6

Pesan (R') = EA 2F 45 BF EF 70 C6 72

K15 = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001

Maka generate kunci proses putaran 15 yaitu melakukan pergeseran 15 bit kekanan, berikut hasilnya

K14 = 10110011 00111001 10111100 10110000 10110111 00110100 01001110 00110100

2. XOR Blok Kunci

R14=11101010 00101111 01000101 10111111 11101111 01110000 11000110 01110010

K15=10110011 00111001 10111100 10110000 10110111 00110100 01001110 00110100

= 01011000 00010110 10001001 00000111 01001000 01000100 10101000 01000110

3. Rotasi Blok

R = 01000110 01011000 00010110 10001001 00000111 01001000 01000100 10101000

R = 43 58 16 89 07 48 44 A8

4. Substitusi S-BOX

R = 43 58 16 89 07 48 44 A8

R = 1D 77 95 89 B4 9F AA 1A

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L14 = 53 65 6C 61 6D 61 74 20

R15 = 1D 77 95 89 B4 9F AA 1A +
4E 12 F9 E8 D9 FE DE 3A**PUTARAN 16 :**

L= R (Putaran 15)

= 4E 12 F9 E8 D9 FE DE 3A

1. Pertukaran Byte (R')

Pesan (R) = 4E 12 F9 E8 D9 FE DE 3A

Pesan (R') = 12 4E E8 F9 FE D9 3A DE

Kunci awal = 01001110 01101001 01100110 01100101 01111001 01100001 01101110 01101001

Maka generate kunci proses putaran 15 yaitu melakukan pergeseran 15 bit kekanan, berikut hasilnya

K16 = 01100110 01110011 01111001 01100001 01101110 01101000 10011100 01101001

2. XOR Blok Kunci

R15=00010010 01001110 11101000 11111001 11111110 11011001 00111010 11011110

K16=01100110 01110011 01111001 01100001 01101110 01101000 10011100 01101001

= 11110100 00111101 10010001 10011000 10010000 10110001 10100010 10010111

3. Rotasi Blok

R = 10010111 11110100 00111101 10010001 10011000 10010000 10110001 10100010

R = 97 F4 3D 91 98 90 B1 A2

4. Substitusi S-BOX

R = 97 F4 3D 91 98 90 B1 A2

R = 72 CD 2E 66 AC 0C A8 DE

5. Perubahan Posisi Blok Kiri (L) dan Kanan (R)

L15 = 4E 12 F9 E8 D9 FE DE 3A

R16 = 72 CD 2E 66 AC 0C A8 DE +

3C DF D7 8E 75 F2 76 E4

Setelah putaran sebanyak 16 kali maka hasilnya, adalah

Hasil L = 4E 12 F9 E8 D9 FE DE 3A

Hasil R = R3 DF D7 8E 75 F2 76 E4

Maka hasil akhirnya: 4E12F9E8D9FEDE3AR3CDFD78E75F276E4

3.2. Implementasi

Pengguna komputer sebagai alat pengolah data terdiri beberapa fasilitas pendukung yang harus memenuhi syarat. Implementasi sistem adalah prosedur yang dilakukan untuk menyelesaikan peancangan sistem. Perangkat keras adalah komponen-komponen peralatan yang membentuk suatu sistem komputer sehingga dapat melaksanakan tugasnya. Perangkat keras yang digunakan sebagai pendukung untuk membuat program aplikasi pada pembuatan skripsi ini mempunyai spesifikasi sebagai berikut:

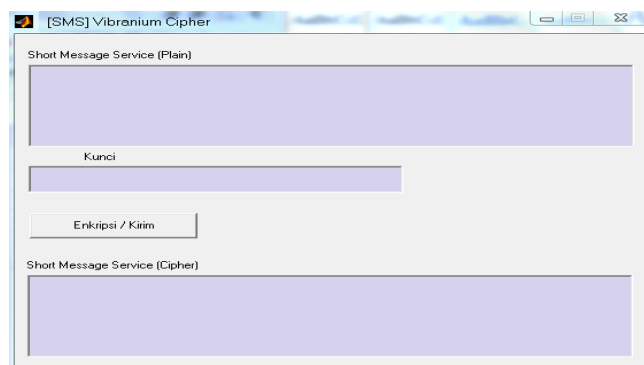
1. Processor Intel(R) core(TM) i3-3217U CPU @ 1.80GHz
2. Harddisk 500 GB
3. Monitor dengan resolusi 1336 x 768
4. Memory RAM yang digunakan 4 GB
5. Keyboard dan Touch Screen

Perangkat lunak adalah sekumpulan instruksi yang telah di program terlebih dahulu untuk mengendalikan dan mengkoordinasi elemen-elemen perangkat keras komputer di dalam sebuah sistem informasi. Perangkat lunak yang dibutuhkan untuk menunjang aktivitas berjalannya program aplikasi adalah:

1. sistem operasi windows 7
2. MATLAB

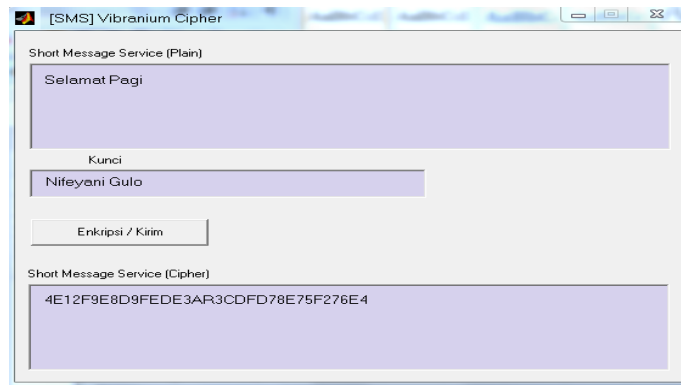
Tahapan implementasi dilakukan dengan cara melakukan proses pengujian terhadap algoritma vibranium cipher untuk mengamankan SMS dengan menggunakan aplikasi yang telah di bangun menggunakan matlab. Proses penerapannya diperanin dua operator yaitu pengirim dan penerima. Pengirim melakukan proses pengiriman SMS yang telah dienkripsi sebelumnya yang kemudian dikirim kepada penerima pesan. Kunci yang digunakan telah disepakati bersama antara pengirim dan penerima. Operator penerima akan melakukan proses deskripsi terhadap SMS terenkripsi sehingga isi pesan dapat dibaca dan dipahami oleh sipenerima.

Proses enkripsi pesan dilakukan oleh pengirim sebelum melakukan proses pengiriman SMS, berikut proses penggunaan aplikasi pengamanan SMS:



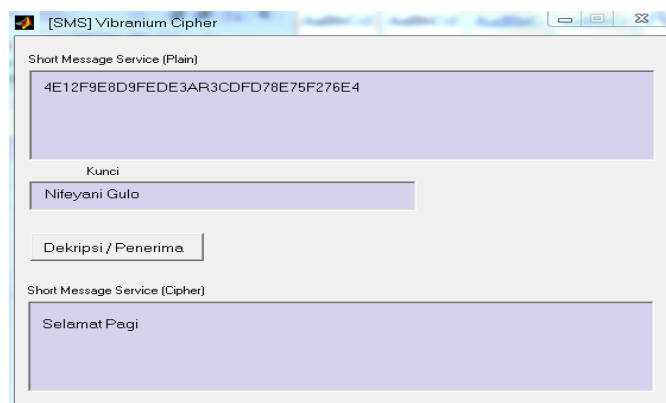
Gambar 1. Tampilan Awal Form

Selanjutnya melakukan proses pengetikan SMS kemudian dilakukan proses enkripsi dan pengiriman. Berikut tampilan form:



Gambar 2. Form Proses Pengiriman dan Enkripsi SMS

Setelah SMS dikirimkan oleh pengirim selanjutnya pihak penerima SMS melakukan proses dekripsi, berikut tampilan form dekripsi SMS



Gambar 3. From Proses Menerima dan Dekripsi SMS

4. KESIMPULAN

Dari penjelasan yang sudah diperoleh pada bab-bab sebelumnya, dapat ditarik kesimpulan bahwa Melakukan penyandian pengubahan karakter informasi dari teks yang dapat dibaca (plaintext) menjadi teks yang tidak dapat dibaca (cipher text), sehingga membuat kerahasiaan informasi pada SMS menjadi terjaga. Teknik Penerapan algoritma vibranium cipher sangat mudah mengingat proses enkripsinya menggunakan model jaringan feistel sehingga perputaran nilai cipher menghasilkan nilai cipher yang bervariasi. Setelah dilakukan proses pengujian terhadap algoritma vibranium cipher, algoritma ini memberikan hasil yang samar sehingga sulit untuk mengetahui kunci yang digunakan.

REFERENCES

- [1] Emy Setyaningsih, S.Si., M.Kom Kriptografi & Implementasi Menggunakan MATLAB, Nikodemus WK, Ed. Yogyakarta, 2015.
- [2] faisal taufik iqbal kamil siregar, "perancangan aplikasi sms alert berbasis web," JIMP-jurnal informatika merdeka pasuruan, p. 2, 2017.
- [3] Eriq Muhammad Adams Jonemaro, Tri Afirianto Ade Dermawan, "Analisis Penerapan Algoritma Vibranium Cipher," Jurnal Ilmu Teknik Dan Teknologi, vol. 3, p. 2, mei 2017.
- [4] Kamus Besar Bahasa Indonesia. (2019, 4 Juli) KBBI Online. [Online]. <http://apaati.com/arti kata pengamanan.html>
- [5] Okky Dwi Nurhayati, Eko Didik Widiyanto Muhammad Ridwan Asad, "Sistem Pengamanan Pintu Rumah Otomatis Via SMS Berbasis Mikrokontroller ATmega328P," Jurnal Teknologi Dan Sistem Komputer, vol. 3, p. 2, Januari 2015.
- [6] S.Si., M.Kom. Emy Setyaningsih, Kriptografi & Implementasinya Menggunakan MATLAB, Nikodemus WK, Ed. Yogyakarta: ANDI, Indonesia, 2015.
- [7] Rinaldi Munir, Kriptografi, 1st ed. Bandung, Inonesia: Informatika Bandung, 2006.
- [8] Eriq Muhammad Adams Jonemaro, Tri Afirianto Ade Dermawan, "Analisis Penerapan Algoritma Vibranium Cipher," Jurnal Ilmu Teknik Dan Teknologi, vol. 3, p. 2, Mei 2017.
- [9] Rosa A. S. and Muhammad Shalahuddin, Rekayasa Perangkat Lunak. Bandung, Indonesia: Penerbit Modula, 2011.
- [10] Ph.D Marwan, S.T., M.Eng.Sc., Belajar Mudah MATLAB Beserta Aplikasinya, Yeskha M.M, Ed. Yogyakarta :ANDI, Indonesia, 2017.