Volume 5 Nomor 2, Oktober 2022
e-ISSN : 2621-234X

Implementasi Kriptogrfi Algoritma Elgamal dalam Pengamanan Dokumen Surat

Muhammad Hendri[1], Raudhah[2], Fitri Fatimah[3], Sri Ramadhany[4]

Address: STMIK Logika, Prodi Teknik Informatika, Indonesia[1], STMIK Logika, Program Studi Sistem Informasi, Indonesia[2], STMIK Logika, Prodi Manajemen Informatika, Indonesia [3, 4]

Email: mhendri69@gmail.com[1], adek.raudhah@gmail.com[2], v3fatimah@gmal.com[3], sriramadhany82@gmail.com[4]*

Abstrak

Ada beberapa aspek dalam keamanan jaringan, yaitu keaslian sumber atau objek, kendali akses terhadap sumber daya, kerahasiaan data, keutuhan data, non-repudiation (menghindari penolakan atas penerimaan/pengiriman data yang terkirim) dan ketersediaan layanan. Aspek kerahasiaan merupakan upaya untuk menjaga kerahasiaan dari informasi yang bersifat rahasia atau pribadi agar tidak diketahui orang lain yang tidak memiliki hak akses. Komputer yang sudah terhubung ke jaringan internet rentan terhadap pencurian data ataupun informasi. Adapun tujuan dari penelitian ini adalah bagaimana teknik atau cara melindungi data dari pencurian ataupun perubahan isi. Oleh itu dibutuhkan suatu pengamanan menggunakan metode kriptografi. Disini digunakan ElGamal karena metode ini cukup sulit dipecahkan, karena nilai kunci terpisah antara kunci private maupun kunci public. Berdasarkan hasil penelitian didapat bahwa proses pembangkitan kunci merupakan inti dari proses pengelolaan manajemen keamanan dari ElGamal.

Kata Kunci : *Kendali,* Akses, Kriptografi, Algoritma, ElGamal

Abstract

There are several aspects of network security, namely the authenticity of source or object, control of access to resources, data confidentiality, data integrity, non-repudiation (avoiding storage of received/sent data) and service availability. The confidentiality aspect is an effort to maintain the confidentiality of confidential or private information so that it is not known to other people who do not have access rights. Computers that are connected to the internet are vulnerable to data or information theft. The purpose of this research is how to technique or how to protect data from theft or changes in content. Therefore we need a security using cryptography. Here we use ElGamal this method is quite difficult to solve, because the key value is separate between the private key and the public key. Based on the results of the study, it was found that the key generation process is the core of the security management process from ElGamal.

Keywords *Control, Access, Cryptography, Algorithm, ElGamal*

1. Latar Belakang

Menjaga keamanan dan kerahasiaan data merupakan hal yang sangat penting untuk melakukan sebuah proses pengiriman data, baik itu data teks dan video melalui jaringan internet yang sudah terkoneksi dengan sangat luas. [1] Masalah keamanan data merupakan aspek penting dalam pengiriman informasi baik berupa teks maupun non teks. Maka dari itu dibutuhkan suatu sistem keamanan data yang dapat menjaga kerahasiaan informasi baik berupa data teks maupun non teks. [2]

Pengiriman file pada masa sekarang ini dilakukan secara online melalui *email*. Oleh karena itu diperlukan aspek keamanan yang ketat walaupun data akses menggunakan *password*. Mesekipun aspek keamanan telah digunakan masih ada beberapa orang yang melakukan teknik untuk mendapatkan data dengan cara melakukan pengelabuan seakan-akan dia adalah orang yang dituju dalam pengiriman data. Bila teknik ini berhasil dilakukan, maka sudah bisa dipastikan bahwa data akan jatuh ke tangan orang yang tidak berkepentingan dan dengan mudah dapat dibaca. [3]

Agar dapat mencegah pencurian informasi (data) maka dilakukan beberapa teknik penyamaran data yang biasa disebut dengan istilah kriptografi sementara teknik untuk menyembunyikan data disebut dengan istlah steganografi. [4] Kriptografi adalah ilmu yang mempelajari bagaimana menjaga keamananan suatu pesan (*plaintext*). Tugas utama kriptografi adalah untuk menjaga agar pesan atau kunci ataupun keduanya tetap terjaga kerahasiaannya dari penyadap (*attacker*). Penyadap pesan diasumsikan mempunyai akses yang lengkap dalam saluran komunikasi antara pengirim pesan dan penerima pesan. [5]

Dalam proses ini digunakan sebuah algoritma Asmetris Elgamal. Algoritma elgamal memiliki dua buah kunci yang disebut dengan kunci *public* untuk melakukan proses enkripsi dan kunci *private* untuk proses dekripsi. Kedua kunci tersebut diperoleh dengan menetukan satu bilangan prima dan dua bilangan acak. Algoritma ini merupakan cipher box dan melakukan proses enkrip pada blok – blok *plaintext* dan menghasilkan sebuah box *ciphertext* dan hasil dari dekrip ini digabungkan.[6]

Berdasarkan latar belakang tersebut, maka penulis melakukan penelitian pengamanan dokumen surat dengan menggunakan algoritma elgamal.

2. Metode

Agar penelitian ini dapat terlaksana dan berjalan sesuai dengan langkah-langkah dan prosedur penelitian, maka penulis merancang suatu proses/alur tahapan penelitian yaitu:

a) Tahapan perencanaan penelitian
   Tahapan yang penulis lakukan adalah mendefinisikan masalah, menentukan tujuan dan melakukan perbandingan dengan penelitian yang sudah ada.
b) Tahapan Analisis
   Melakukan kegiatan analisis terhada data yang terkumpul dengan masalah yang akan diteliti.
c) Tahapan Perancangan
   Merupakan kegiatan yang penulis lakukan sebelum penulis membuat pemrograman.
d) Tahapan Pengujian
   Tahap melakukan pengujian validitas data yang dikumpulkan dengan data yang diinginkan oleh instansi.
e) Tahapan Pembuatan Laporan
   Tahapan penulis merancang dokumentasi berupa laporan.

Adapun teknik pengumpulan data yang digunakan dalam penulisan laporan ini, adalah :

a. Observasi (*Observation*)
   Adalah pengamatan objek yang dilakukan secara langsung atau tidak langsung dengan menggunakan instrument dokumentasi baik yang memuat garis-garis besar atau kategori yang akan dicari datanya, maupun check-list yang memuat daftar variabel yang akan dikumpulkan datanya..[7]
b. Wawancara langsung (*Interview*) atau konsultasi Merupakan cara untuk mendapatkan informasi dengan cara bertanya langsung atau tak langsung kepada responden. [8]
c. Penelitian Kepustakaan (*Library Research*)
   Ternyata kepustakaan tidak hanya mengumpulkan, membaca dan mencatat literatur /buku-buku yang difahami banyak orang, tetapi jauh dari itu, penelitian kepustakaan harus memperhatikan langkah-langkah dalam meneliti kepustakaan, harus memperhatikan metode penelitian dalam rangka mengumpulkan data, membaca dan mengolah bahan pustaka serta peralatan yang harus dipersiapkan dalam penelitian tersebut, kegunaannya mempermudah peneliti dalam mendapatkan data.

Proses Pengolahan Algoritma ElGamal

Sebelum mengimplementasikan kepada sistem maka algoritma elgamal akan dilakukan perhitungan secara manual. Adapun proses perhitungan algoritma elgamal adalah sebagai berikut :

a. Perhitungan pembentukan kunci

Langkh pertama adalah menentukan nilai p, g dan x agar dapat menentukan kunci private dan kunci public pada algoritma elgamal.

p = 179
g = 5
x = 7

Kemudian p, g, x digunakan untuk menghitung y :

y = g^x mod p.....*(1)*
y = 5^7 mod 179
y = 81

Jadi kunci public A (p,g,y) adalah (179,5,81)
dan kunci private A (p,x) adalah (179,7)

b. Proses Enkripsi

Pada kasus ini diumpamakan seorang ingin mengirim teks berupa kata “DOKUMEN” kepada orang lain. Pada awal proses enkripsi yang dilakukan adalah mengubah teks yang akan dienkripsi kedalam kode ASCII. Maka diperoleh konversi teks sebagai berikut :

Plainteks ASCII
D = 68
O = 79
K = 75
U = 85
M = 77
E = 69
N = 78

Kemudian nilai ASCII tersebut dimasukkan kedalam blok-blok nilai m secara berurutan, sehingga menjadi:

m1 = 68, m2 = 79, m3 = 75, m4 =85, m5 = 77, m6 = 69, m7 = 78.

Kemudian sipengirim pesan memilih bilangan acak kunci untuk masing-masing nilai m dimana nilai ki ini bernilai 0 < k < p -1. Sehingga diambil nilai acak k untuk masing-masing nilai m sebagai berikut :

Tabel 1. Nilai Kunci

Mi	Nilai	Ki
m1	68	15
m2	79	7
m3	75	29
m4	85	31
m5	77	42
m6	69	18
m7	78	11

Maka dari itu perhitungan enkrisi adalah :

Perhitungan a :

a = g^ki mod p ..... *(2)*

maka nilai m1 :
a1 = g^k1 mod p
a1 = 5^15 mod 179
a1 = 75
Nilai m2 :
a2 = g^k2 mod p
a2 = 5^7 mod 179
a2 = 81
Nilai m3 :
a3 = g^k3 mod p
a3 = 5^29 mod 179
a3 = 67
Nilai m4 :
a4 = g^k4 mod p
a4 = 5^31 mod 179
a4 = 64
Nilai m5 :
a5 = g^k5 mod p
a5 = 5^42 mod 179
a5 = 100
Nilai m6 :
a6 = g^k6 mod p
a6 = 5^18 mod 179
a6 = 93
Nilai m7 :
a7 = g^k7 mod p
a7 = 5^11 mod 179
a7 = 147

Sedangkan Perhitungan bi :

bi = y^ki. mi mod p ..... *(3)*

Nilai m1 :
b1 = y^k1*m1 mod p
b1 = 81^15*68 mod 179
b1 = 165
Nilai m2 :
b2 = y^k2*m2 mod p
b2 = 81^7*79 mod 179
b2 = 154
Nilai m3 :
b3 = y^k3*m3 mod p
b3 = 81^29*75 mod 179
b3 = 51
Nilai m4 :
b4 = y^k4*m4 mod p
b4 = 81^31*85 mod 179
b4 = 68
Nilai m5 :
b5 = y^k5*m5 mod p
b5 = 81^42*77 mod 179
b5 = 56
Nilai m6 :
b6 = y^k6*m6 mod p
b6 = 81^18*69 mod 179
b6 = 154
Nilai m7 :
b7 = y^k7*m7 mod p
b7 = 81^11*78 mod 179
b7 = 136

Setelah mendapatkan nilai a dan b, maka hasil tersebut dapat kita susun menjadi : a1, b1, a2, b2, a3, b3, a4, b4, a5, b5, a6, b6, a7, b7.

Sehingga membentuk *chiperteks*: 75, 165, 81, 154, 67, 51, 64, 68, 100, 56, 93, 154, 147, 136.

c. Proses Dekripsi

Sipenerima pesan dapat mengubah *chipertext* menjadi *plainteks* dengan melakukan perhitungan dengan rumus sebagai berikut :

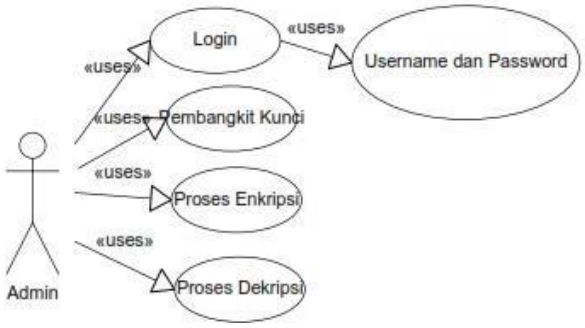
mi = bi.ai^p-1-x mod p..... *(4)*

Nilai m1 :
m1 = b1.a1^p-1-x mod p
m1 = 165*75^179 1-7 mod 179
m1 = 68
Nilai m2 :
m2 = b2.a2^p-1-x mod p
m2 = 154*81^179 1-7 mod 179
m2 = 79
Nilai m3 :
m3 = b3.a3^p-1-x mod p
m3 = 51*67^179 1-7 mod 179
m3 = 75
Nilai m4 :
m4 = b4.a4^p-1-x mod p
m4 = 68*64^179 1-7 mod 179
m4 = 85
Nilai m5 :
m5 = b5.a5^p-1-x mod p
m5 = 56*100^179 1-7 mod 179
m5 = 77

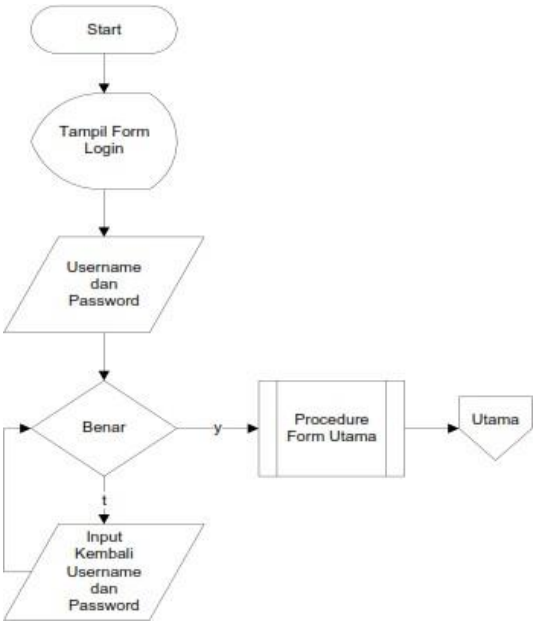
Nilai m6 :
m6 = b6.a6^p-1-x mod p
m6 = 154*93^179-1-7 mod 179
m6 = 69
Nilai m7 :
m7 = b7.a7^p-1-x mod p
m7 = 136*147^179-1-7 mod 179
m7 = 78
Setelah mendapatkan nilai mi dengan perhitungan diatas, maka diperoleh nilai m adalah:
68, 79, 75, 85, 77, 69, dan 78
Setelah itu nilai tersebut harus dikonversikan dengan menggunakan kode ASCII kembali : 68 = D, 79 = O, 75 = K, 85 = U, 77 = M, 69 = E, 78 = N.
Hasil akhir setelah konversi adalah teks "DOKUMEN", sama dengan *plainteks* sebelum di enkripsi.

3. Hasil

Sistem dibangun dengan menggunakan program *java netbeans* dengan desain sistem menggunakan UML. *Unified Modelling Language* (UML) adalah sebuah pemodelan visual yang mendeskipsikan, menggambarkan, membangun serta mendokumentasikan pengembangan sistem informasi yang memiliki paradigma berorientasi objek. [9]
Use case merupakan salah satu alat bantu yang digunakan dalam perancangan berorientasi objek berbasiskan UML. *Use case* adalah rangkaian atau uraian sekelompok yang saling terkait dan membentuk sistem secara teratur yang dilakukan atau diawasi oleh sebuah actor. [10]

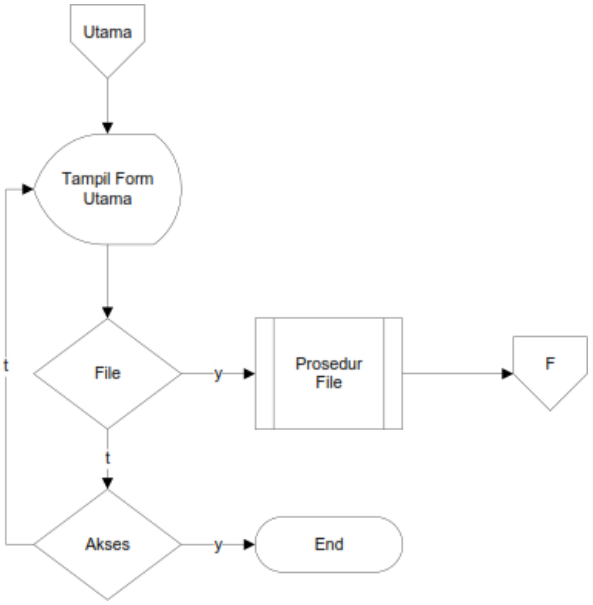


Gambar 1. Use Case diagram program
Sementara algoritma program digambarkan dengan *flowchart*. *Flowchart* atau sering disebut dengan diagram alir merupakan suatu jenis diagram yang merepresentasikan algoritma atau langkah-langkah instruksi yang berurutan dalam sistem. [11]



Gambar 2. *Flowchart* menu *login* program

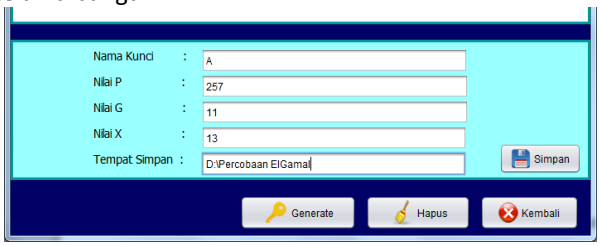
Program ini menggunakan form *login* untuk masuk ke sistem. *Flowchart* diatas adalah *flowchart* untuk masuk ke sistem.
Smentara *flowchart* untuk menu utama sistem terlihat pada gambar dibawah ini :



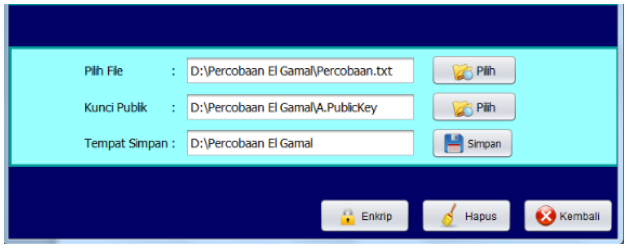
Gambar 3. *Flowchart* menu utama sistem
Hasil tampilan sistem yang dibangun dengan menggunakan program java netbeans adalah sebagai berikut :

Gambar 4. Tampilan menu *login*

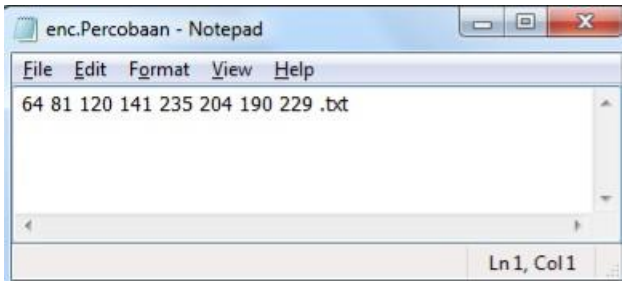
Form diatas merupakan *form login* pada sistem yang telah dibangun.



Gambar 5. Tampilan *form* pembangkit kunci



Gambar 6. *Form* enkripsi



Gambar 7. Hasil proses enkripsi di dokumen teks

Gambar 8. *Form* dekripsi

Adapun proses ujicoba yang dilakukan adalah sesuai dengan tabel dibawah ini :

Tabel 2 Pengujian

No.	Nama File	Durasi Waktu Proses (menit)		Durasi Waktu Rata-Rata (menit)
		Enkripsi	Dekripsi	
1	File 1	5,50	4,58	5.04
2	File 2	5.55	4.52	5.03
3	File 3	5.45	5.02	5.24
4	File 4	5.30	4.50	4.90
5	File 5	5.45	4.58	5.02
6	File 6	5.55	4.50	5.03
7	File 7	5.35	5.00	5.18
8	File 8	5.57	4.58	5.08
9	File 9	5.49	4.48	4.99
10	File 10	5.50	4.78	5.14
11	File 11	5.58	5.01	5.30
12	File 12	5.78	4.98	5.38
13	File 13	5.76	4.78	5.27
14	File 14	5.68	4.87	5.28
15	File 15	5.67	4.55	5.11
16	File 16	5.67	4.65	5.16
17	File 17	5.55	4.63	5.09
18	File 18	5.43	4.52	4.98
19	File 19	5.59	4.51	5.05
20	File 20	5.57	4.57	5.07
21	File 21	5.54	4.58	5.06
22	File 22	5.67	4.59	5.13
23	File 23	5.54	4.85	5.20
24	File 24	5.45	4.75	5.10
25	File 25	5.35	4.79	5.07
26	File 26	5.52	4.78	5.15
27	File 27	5.51	4.71	5.11
28	File 28	5.36	4.51	4.94
29	File 29	5.39	4.53	4.96
30	File 30	5.48	4.52	5.00
31	File 31	5.47	4.51	4.99
32	File 32	5.49	4.56	5.03
33	File 33	5.68	4.58	5.13
34	File 34	5.81	4.59	5.20
35	File 35	5.82	4.57	5.20
36	File 36	5.74	4.59	5.17
37	File 37	5.52	4.57	5.05
38	File 38	5.54	4.58	5.06
39	File 39	5.55	4.62	5.09
40	File 40	5.59	4.56	5.08
41	File 41	5.82	4.63	5.23
42	File 42	5.81	4.71	5.26
43	File 43	5.61	4.70	5.16
44	File 44	5.52	4.60	5.06
45	File 45	5.53	4.52	5.03
46	File 46	5.64	4.50	5.07
47	File 47	5.48	4.81	5.15
48	File 48	5.49	4.52	5.01
49	File 49	5.54	4.57	5.06
50	File 50	5.51	4.52	5.02

Waktu poses rata-rata	5.10

Dari hasil tabel ujicoba 50 file yang dienkripsi dan didekripsi maka dapat terlihat bahwa durasi waktu rata-rata proses enkripsi adalah 5.56 menit sementara rata-rata waktu dekripsi adalah 4.64 menit. Sementara waktu yang digunakan program untuk melakukan proses enkripsi dan dekripsi adalah 5.10 menit.

4. Kesimpulan

Proses pembangkitan kunci merupakan inti dari algoritma ElGamal, karena dengan proses ini dapat dibentuk kunci private dan public. Dimana untuk proses enkripsi digunakan kunci public, dan untuk proses dekripsi menggunakan kunci private.

Proses enkripsi isi file dokumen dapat dilakukan dengan algoritma ElGamal sehingga file dokumen tersimpan di dalam media penyimpanan maupun file dokumen yang dikirim dan diterima tidak bisa dibaca atau dipahami pihak lain kecuali penerima yang sebenarnya.

References

[1] I. Gunawan, "Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, p. 57, 2018, doi: 10.30645/j-sakti.v2i1.48.

[2] Y. Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[3] L. Benny, "Analisis Dan Perancangan Aplikasi Kriptografi Keamanan File Berbasis Teks Dengan Menggunakan Metode Rsa," *Ris. dan E-Jurnal Manaj. Inform. Komput.*, vol. 1, no. April P-ISSN : 2541-1322, pp. 15–23, 2017, [Online]. Available: http://jurnal.polgan.ac.id/index.php/remik/article/view/10116

[4] A. Indriani and Sinawati, "Analisa Pengamanan Teks Menggunakan Teknik Character Cipher Dan Block Cipher," no. 2006, pp. 1–6, 2018.

[5] M. K. Harahap and N. Khairina, "Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks," *J. Penelit. Tek. Inform.*, vol. 1, no. April 2017, pp. 58–62, 2018.

[6] I. K. Dewi, "Implementasi Algoritma Kriptografi Asimetris Elgamal dalam Proses Enkripsi dan Dekripsi File Teks untuk Meningkatkan Keamanan Data," no. January, 2021.

[7] T. A. dan B. Anufia, "Instrumen Pengumpulan Data," pp. 1–20, 1386.

[8] S. T. I. Herdayati, S.Pd., M.Pd1 dan Syahrial, "DESAIN PENELITIAN DAN TEKNIK PENGUMPULAN DATA DALAM PENELITIAN."

[9] T. S. W. Nasution, "PENGEMBANGAN KEAMANAN WEB LOGIN PORTAL DOSEN MENGGUNAKAN UNIFIED MODELLING LANGUANGE (UML)," vol. 3, no. 1, pp. 34–40, 2018.

[10] M. Tabrani and I. Rezqy Aghniya, "Implementasi Metode Waterfall Pada Program Simpan Pinjam Koperasi Subur Jaya Mandiri Subang," *J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 14, no. 1, pp. 44–53, 2020, doi: 10.35969/interkom.v14i1.65.

[11] R. Rosaly and A. Prasetyo, "Pengertian Flowchart Beserta Fungsi dan Simbol-simbol Flowchart yang Paling Umum Digunakan," *Https://Www.Nesabamedia.Com*, vol. 2, p. 2, 2019, [Online]. Available: https://www.nesabamedia.com/pengertian-flowchart/https://www.nesabamedia.com/pengertian-flowchart/

Muhammad Hendri lahir dikota Medan pada tanggal 11 Juli 1969. Menyelesaikan program sarjana di dua jurusan yaitu sarjana teknik Universitas Sumatera utara apad tahun 1995, sarjana computer di STMIK Logika pada tahun 2006. Sedangkan untuk pendidikan Magister diselesaikan pada dua jurusan juga yaitu Magister Manajemen di Universitas Terbuka pada tahun 2007 dan Magister Komputer di UPI YPTK Padang pada tahun 2009. Hobi membaca

Raudhah lahir di Medan pada 01 Januari 1980. Menyelesaikan sarjana ekonomi di UMSU pada tahun 2002, juga mendapat gelar sarjana computer dari STMIK Logika pada tahun 2006. Pendidikan Magister Komputer diraih pada tahun 2011 di UPI YPTK Padang.Hobi membaca dan komputasi.

Volume 5 Nomor 2, Oktober 2022
e-ISSN : 2621-234X

Fitri Fatimah lahir di Medan pada 15 September 1977. Menyelesaikan program Sarjana Sastra Inggris di STBA Harapan pada tahun 2001, serta menyelesaikan program sarjana computer di STMIK Logika pada tahun 2006. Magister computer diperoleh dari UPI YPTK Padang pada tahun 2014.Hobi membaca dan kumpul keluarga

Sri Ramadhany, Lahir di Labuhan deli tanggal 29 Juni 1982. Lulus S1 STMIK Logika tahun 2013 dan lulus Magister computer dari UPI YPTK Padang pada tahun 2014. Hobi belanja dan membaca.