Jurnal CyberTech
Vol.3. No.2, Februari 2020, pp. 393~402
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Implementasi Kriptografi Keamanan Data Anggaran Pada SMP IT AL-IKHWAN Menggunakan Algoritma RC4

Amin Rais S [1], Azanuddin[2], Ahmad Calam[3]

[1] Program Studi Sistem Informasi, STMIK Triguna Dharma
[2,3] Program Studi Sistem Komputer dan Sistem Informasi, STMIK Triguna Dharma

Article Info

Article history:
Received Feb 12th, 2020
Revised Feb 20th, 2020
Accepted Feb 28th, 2020

Keyword:

Kriptografi
Implementasi
Algoritma RC4

ABSTRACT

SMP IT AL–IKHWAN merupakan sekolah swasta yang baru saja berdiri sejak tahun 2015. Sekolah SMP IT AL–IKHWAN mempunyai banyak ekstrakulikuler untuk para murid-murid yang belajar disekolah al-ikhwan, dikarenakan sekolah smp al-ikhwan baru saja berdiri di tahun 2015 maka dana sekolah belum terpenuhi dan para pegawai/guru-guru di smp al-ikhwan sering terjadi pergantian. Agar dana sekolah tersebut bisa terpenuhi dan untuk menganti sepasi dana sekolah aman maka sekolah smp al-ikhwan membutuhkan suatu aplikasi yang bisa mengamankan data anggaran yang akan dimasukan ke dana sekolah .

Untuk mengatasi masalah diatas, maka dibuatlah sebuah program untuk Mengamankan Data Daftar Isian Pelaksanaan Anggaran SMP IT AL – IKHWAN Menggunakan Metode RC4. Metode ini memiliki tingkat keamanan yang cukup sulit untuk di dekripsikan. Sehingga mampu meningkatkan kerahasiaan data Daftar Isian Pelaksanaan Anggaran pada SMP IT AL – IKHWAN.

Hasil yang diharapkan yaitu sebuah program dengan metode Rivest Code 4 ini dapat membantu dalam pengamanan Daftar Isian Pelaksanaan Anggaran SMP IT AL – IKHWAN sehingga dapat mengamankan data tersebut.

.

First Author
Nama : Amin Rais S
Program Studi : Sistem Informasi
Kampus : STMIK Triguna Dharma
Email : raissaragih@gmail.com

1. PENDAHULUAN

Dalam era teknologi informasi saat ini, pengiriman informasi selalu terjadi sehingga unsur keamanan informasi menjadi sangat penting. Benda ini karena penyadapan atau pencurian sering terjadi saat pengiriman informasi yang diberikan oleh pihak yang tidak berwenang. Karena itu dalam pengiriman informasi, pengguna membutuhkan suatu jaminan yang dapat meyakinkan bahwa yang diproleh adalah informasi yang aman dan benar.[1]

Untuk itu sangat diperlukan suatu aplikasi keamanan untuk menjaga kerahasiaan informasi. Salah satu metode untk tujuan ini adalah dengan menggunakan enkripsi informasi yang dikirim, karena tujuan enkripsi adalah untuk menjaga rahasia, integritas, sertifikasi, dan bukti yang tak terbantahkan.

Data anggaran adalah atur secara digital dengan cara yang terencana dan masuk unit moneter yang meliputi seluruh kegiatan Perusahaan, Organisasi, Yayasan dan Sekolah untuk jangka waktu (periode) tertentu di masa yang akan datang. Oleh karena itu rencana yang disiapkan dinyatakan dalam mata uang dan kemudian dalam anggaran biasanya disebut rencana keuangan.[2]

Salah satu kegagalan dari sekolah swasta atau yayasan dapat dilihat dan diukur melalui laporan data anggaran. Laporan data anggaran yang dipegang oleh bendahara sekolah merupakan salah satu sumber informasi mengenai posisi keuangan sekolah, kinerja serta perubahan posisi keuangan sekolah, yang sangat

berguna untuk mendukung pengambilan keputusan yang tepat, data keuangan harus dikonversi menjadi informasi yang berguna dalam pengambilan keputusan ekonmis sekolah. [3]

2. KAJIAN PUSTAKA

2.1 Keamanan Data

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. Secara umum keamanan data ada beberapa aspek, yaitu sebagai berikut :

1. *Privacy/confidentialty*

   Privacy lebih kearah data-data yang sifatnya rahasia, sedangkan *Confidentialty* berhubungan dengan sebuah data yang diberikan kepihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu.
2. *Integrity*

   Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seiizin pemilik informasi. Informasi diterima harus sesuai dan sama persis seperti saaat informasi dikirimkan. Jika terdapat perbedaan antara informasi atau data yang dikirimkan dengan yang diterima maka aspek *integrity* tidak tercapai.
3. Otentikasi (*authentication*)

   adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya.

   Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data. Sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar.

4. Nirpenyangkalan (*non-repudiation*), adalah layanan untuk mencegah terjadinya penyangkalan terhadap pengirim atau terciptanya suatu informasi oleh pengirim pesan.

2.2 Kriptografi

Kriptografi Yaitu Suatu Bidang Pengetahuan Yang Menggunakan Persamaan Matematis Untuk Melakukan Proses Pengamanan Data Dengan Menggunakan Teknik Mengkonversi Data Ke Bentuk Kode-Kode Tertentu Agar Informasi Tidak Dapat Terbaca Oleh Siapapun Kecuali Pihak Yang Berhak. Menurut manezes (1996) kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan seperti kerahasian, integritas data, otentikssi dan anti penyangkalan[4].

2.2.1 Konsep Dasar Kriptografi

Untuk menjamin kerahasian dan keaslian data, maka digunakan teknik kriptografi yang melakukan tranformasi terhadap data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak ketiga[5].

2.2.2 Jenis-Jenis Kriptografi

1. Kriptografi Simetris

Algoritma kriptografi simetris merupakan proses enkripsi dan dekripsi dilakukan dengan memakai 1 key yang sama disebut kunci privat yang terdiri dari metode-metode diantaranya data encryption standart (DES), Rivest Cipher 4 (RC4), On time Pad (OTP), Blowfish, dan sebagainya[8].

2. Kriptografi Asimetris

Kriptografi asimetri adalah kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi dekripsi.

2.3 Algoritma RC4

Algoritma kriptografi Rivest Code 4 (RC4) merupakan salah satu algoritma kunci simetris yang berbentuk stream chipper. Algoritma ini ditemukan pada tahun 1987 oleh Ronal Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu: Rivest Shamir Adleman). RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte[10].

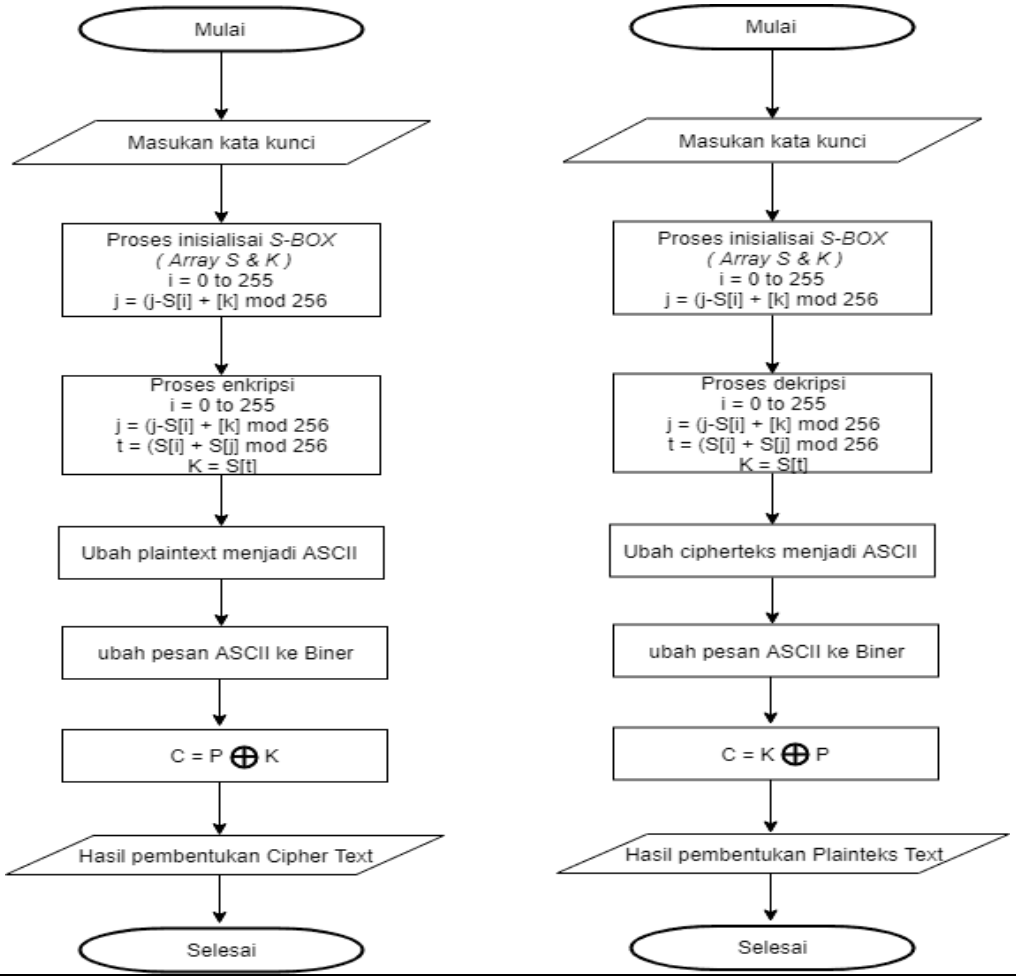
3. Metode Penelitian

3.1 Analisa Permasalahan

Sistem keamanan data anggaran pada SMP Al-IKHWAN masih kurang efektif dimana sekolah smp tersebut belum memiliki system keamanan data anggaran. Dalam mengimplementasikan keamanan data anggaran pada SMP Al-IKHWAN Menggunakan Algoritma RC4 diharapkan dapat membantu mengamankan keamanan data anggaran pada SMP AL-IKHWAN.

3.3.1. Data Kriteria Dari Penelitian

Flowchart algoritma RC4 merupakan keterangan yang lebih rinci tentang bagaimana prosedur sesungguhnya yang dilakukan oleh suatu metode. *Flowchart* ini menggambarkan urutan logika dari suatu prosedur pemecahan masalah Berikut ini adalah *Flowchart* dari *Algoritma Rivest Chiper 4* adalah sebagai berikut :



Gambar 1. Flowchart Sistem Dari Algoritma RC4

3.3.2 Algoritma RC4

Langkah-langkah dari proses algoritma RC4 stream chipper untuk melakukan enkrips – dekripsi yaitu :

1. Proses inisialisasi *S-Box* (*Array* S)
   For i = 0 to 255
   S[i] = i
2. Proses inisialisasi *S-Box* (*Array* K)
   For i = 0 to 255
   S[i] = i
3. Kemudian lakukan langkah pengacakan *S-Box*
   i=0; j=0

   for i= 0 to 255{
   j=(j+S[i]+[K] mod 256
   swap S[i] dan S[j]
   }
4. Membuat *pseudorandom byte*
   i= (i+1) mod 256
   j= (j+S[i]) mod 256
   swap S[i] dan S[j]
   t=(S[i] +S[j]) mod 256
   K=S[t]

Byte K di-XOR-kan dengan *plainteks* untuk menghasilkan *cipherteks* atau di-XOR-kan dengan *cipherteks* untuk menghasilkan *plainteks*.

Berikut adalah implementasi algoritma RC4 dengan mode 256 byte,Untuk mencoba kasus yang akan dibahas dan disimulasikan pembeljaraanya dalam penulisan skripsi ini adalah dengan menyajikan data sebagai berikut:

Plainteks : Saldo

Kunci : Rais

3.3.2 Perhitungan iterasi pertukaran *s-box* (*Swap*)

Hasil yang didapat setelah melakukan seluruh iterasi dari 0 s/d 255 kali iterasi dan melakukan pertukaran *s-box (swap)* adalah sebagai berikut :

Tabel 1. Tabel Hasil Pertukaran *s-box (swap)*

82	180	31	149	235	81	192	58	148	254	113	239	77	187	50	180
22	136	3	137	239	101	228	110	216	82	213	99	209	79	214	104
218	92	231	125	243	121	8	162	28	166	57	215	85	227	122	28
158	48	203	113	247	141	44	214	96	250	157	75	217	119	30	208
98	4	175	101	251	161	80	10	164	78	1	191	93	11	194	132
38	216	147	89	255	181	116	62	232	162	101	51	225	159	102	56
234	172	119	77	3	201	152	114	44	246	201	167	101	51	10	236

174	128	91	65	7	221	188	166	112	74	45	27	233	199	174	160
114	84	63	53	11	241	224	474	117	95	82	80	46	28	19	21
247	233	228	234	208	198	197	207	185	179	182	196	178	176	183	201
187	189	200	222	212	218	233	3	253	7	282	56	54	68	91	125
127	145	172	210	216	238	13	55	65	91	126	172	186	216	255	49
67	101	144	198	220	2	49	107	133	175	226	32	62	108	163	229
7	57	116	186	224	22	85	159	201	3	70	148	194	0	71	153
203	13	88	174	228	42	121	211	13	87	170	8	70	148	235	77
143	225	60	162	232	62	157	7	81	171	14	124	202	40	143	1

3.3.2 Proses Enkripsi dan Dekripsi

Berikutnya adalah proses membuat *pseudorandom byte* :

i= (i+1) mod 256

j=(j+S[i]) mod 256

swap S[i] dan S[j]

t=(S[i] + S[j]) mod 256

K=S[t]

Iterasi ke-1 : Plainteks(S)

i = (i + 1) mod 256

= (0 + 1) mod 256

= 1

j = (j + S[i]) mod 256

= (0 + S[1]) mod 256

= (0 + 180) mod 256 = 180

Swap(S[1],S[180])

t = (S[i] + S[j]) mod 256

= (S[1] + S[180]) mod 256

= (180 + 216) mod 256

= 396 mod 256

= 140

Key[0] = S[140] = 46

Setelah dilakukan perhitungan dari iterasi ke-1 menggunakan plainteks (T), hingga iterasi ke-17 menggunakan plainteks (n) maka diperoleh hasil enkripsi dan dekripsi sebagai berikut

Tabel 2. Hasil Enkripsi Plaintext

Plaintext	Binary	Key (K)	XOR	Chipertext
S	01010011 (83)	00101110 (46)	01111101 (125)	}

Tabel 3. Hasil Dekripsi Plaintext

Plaintext	Binary	Key (K)	XOR	Chipertext
}	01111101 (125)	00101110 (46)	01010011 (83)	S

4.1 Form Login

Berikut ini adalah tampilan *form login* yang digunkan *user* untuk bias masuk kedalam sebuah system dengan menggunankan *username* dan *password* yang telah terdaftar pada *database* yaitu:

Gambar 2. Tampilaln *Form Login*

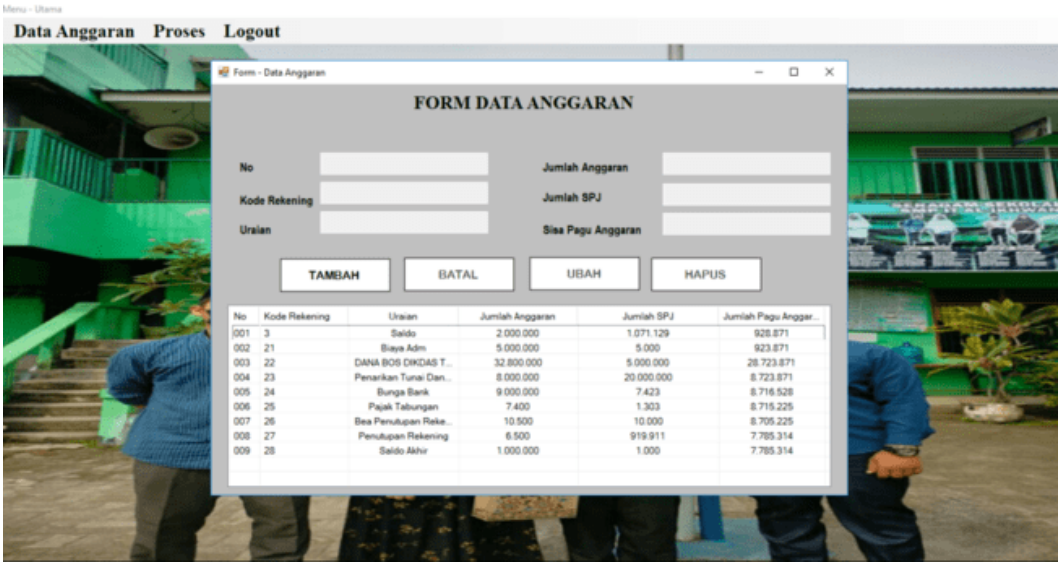
4.2 Form Menu Utama

Halaman ini akan tampil setelah admin berhasil melakukan login kedalam sistem. Pada halaman ini terdapat beberapa menu lain seperti data anggaran proses Enkripsi dan Dekripsi.

Gambar 3. Tampilan *Form* Menu Utama

4.3 Form Input Data Anggaran

Halaman ini berfungsi untuk menambah, mengubah, batal, dan menghapus data anggaran



Gambar 4. Tampilan *Form* Input Data Anggaran

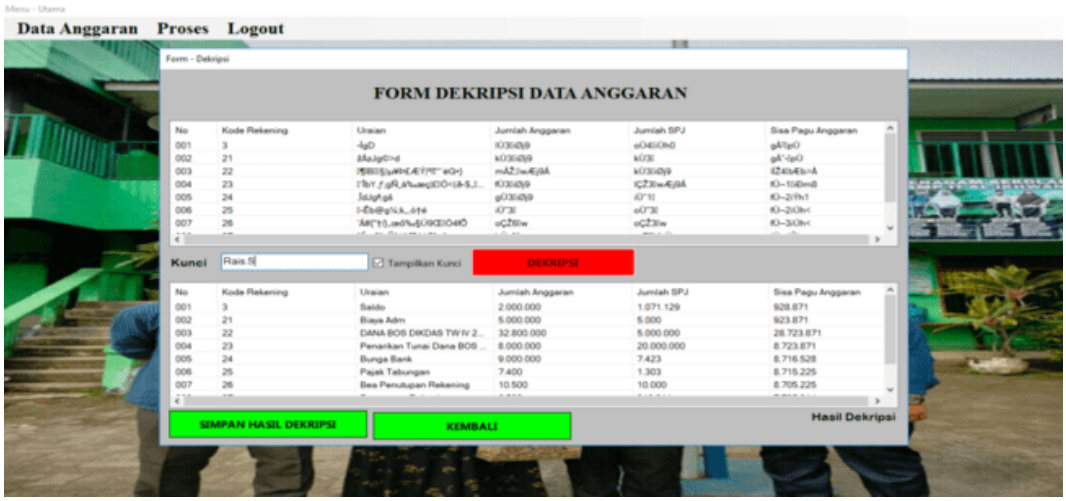
4.4 Form Enkripsi

Halaman ini berfungsi untuk enkripsi data menggunakan algoritma RC4

Gambar 5. Tampilan *Form* Enkripsi

4.5 Form Dekripsi

Halaman ini berfungsi untuk mendekripsi data yang telah di amankan:



Gambar 6. Tampilan *Form* Dekripsi

3. KESIMPULAN

Berdasarkan analisis pembahasan hasil penelitian tentang Implementasi Keamanan Data Anggaran Pada SMP IT AL-IKHWAN Tanjung Morawa Menggunakan Algoritma RC4, maka dapat diambil kesimpulan :

1. Berdasarkan pengujian dan implementasi, pengaruh penerapan sistem keamanan data terhadap keamanan data anggaran pada SMP IT AL-IKHWAN terlihat sangat baik, hal ini dapat dilihat dengan kemudahan dalam proses pengamanan data anggaran tersebut.
2. Dalam menangani masalah keamanan data perlu dirancang aplikasi keamanan data anggaran menggunakan metode RC4, pengguna menginput beberapa data berupa susunan anggaran dan data anggaran.
3. Dalam melakukan pengujian aplikasi keamanan data menggunakan algoritma RC4 adalah sebagai solusi pemecah masalah dalam mengamankan data anggaran agar data anggaran berhasil diterapkan.

UCAPAN TERIMA KASIH

Puji syukur kehadirat Allah SWT atas izin-Nya yang telah melimpahkan rahmat dan karunia-Nya sehingga dapat menyelesaikan jurnal ilmiah ini. Dalam kesempatanini, penulismengucapkan banyak-banyak

terimakasih kepada kedua orang tua Ayahanda tercinta dan ibunda tersayang yang telah melahirkan, membesarkan, membimbing, mendidik dan mendoakan serta senantiasa mendukung hal-hal baik. Penulis juga sangat sadar sepenuhnya skripsi ini tidak terlepas dari bimbingan, semangat, serta dukungan dari banyak pihak, baik bersifat moralmaupun materil, maka dari itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada Bapak Dr. H. Rudi Gunawan, SE, M.Si. selaku Ketua STMIK Triguna Dharma Medan. Bapak Muklis Ramadhan, S.E, M.Kom. Selaku Wakil Ketua I Bidang Akademik STMIK Triguna Dharma Medan. Bapak Puji Sari Ramadhan, S.Kom, M.Kom. Selaku Ketua Program Studi Sistem Informasi (SI) STMIK Triguna Dharma Medan.Bapak Muhammad Iswan, S.Kom., M.Kom. Selaku Dosen Pembimbing I Skripsi yang telah meluangkan waktu untuk membimbing dalam menyelesaikan Sripsi ini.Ibu Sri Murniyanti,SS.,MM. Selaku Dosen Pembimbing II Skripsi yang telah meluangkan waktu untuk membimbing dalam menyelesaikan Skripsi ini.Bapak & Ibu Dosen serta Staff Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Triguna Dharma Medan.

REFERENSI

[1] M. Syahril and H. Jaya, "Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4," *Semin. Nas. Sains Teknol. Inf.*, pp. 505–509, 2019.

[2] R. N. Ibrahim, "PERANGKAT LUNAK KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI SIMETRI TINY ENCRIPTION ALGORITHM (TEA) Data security is one of the most important aspects in information technology . With a high level of security , it is expected that the information pr," vol. 13, no. 1, pp. 1–10, 2019.

[3] M. Diana and T. Zebua, "Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS," no. 1, pp. 12–22, 2018.

[4] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," *J. Format*, vol. 6, no. 1, p. 93, 2017.

[5] B. Setiaji, "Analisis Dan Implementasi Algoritma Kriptografi Kunci Publik Rsa Dan Luc Untuk Penyandian Data," *Data Manaj. dan Teknol. Inf.*, vol. 16, no. 3, p. 27, 2015.

[6] H. Situmorang, "Keamanan Basis Data dengan Teknik Enkripsi," *Mahajana Inf.*, vol. 1, no. 1, pp. 22–27, 2016.

[7] S. Tri, C. Kurniawan, T. Informatika, and S. Informasi, "Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android," vol. 2, no. 2, pp. 102–109, 2017, doi: 10.15575/join.v2i2.113.

[8] A. Lesmana and R. T. Shinta, "Aplikasi Pengamanan EMAIL Berbasis Android dengan Algoritma Kriptografi AES- 128 dan RC4 Pada PT TIRTA INVESTAMA," *Skanika*, vol. 1, no. 2, pp. 534–539, 2018.

BIOGRAFI PENULIS

Nama : Amin Rais S.
Nirm : 2017020896
Program Studi : Sistem Informasi di STMIK Triguna Dharma
Deskripsi : Saya adalah mahasiswa stambuk 2017 pada Program Studi Sistem Informasi yang memiliki minat dan fokus dalam bidang keilmuan Disain dan Multimedia

Nama :Azanuddin, S.Kom., M.Kom.
NIDN :0126068901
Program Studi :Sistem Komputer
Deskripsi :Dosen Tetap STMIK Triguna Dharma yang aktif mengajar dan fokus pada bidang Sistem Jaringan Komputer, Keamanan Komputer dan Jaringan, Komunikasi Data

Nama :Dr.Ahmad Calam, S.Ag. MA
NIDN :0116026802
Program Studi :Sistem Informasi
Deskripsi :Dosen STMIK Triguna Dharma pada Program Studi Sistem Informasi yang aktif mengajar dan fokus pada bidang keilmuan Metopel, Etika Profesi, PPKn