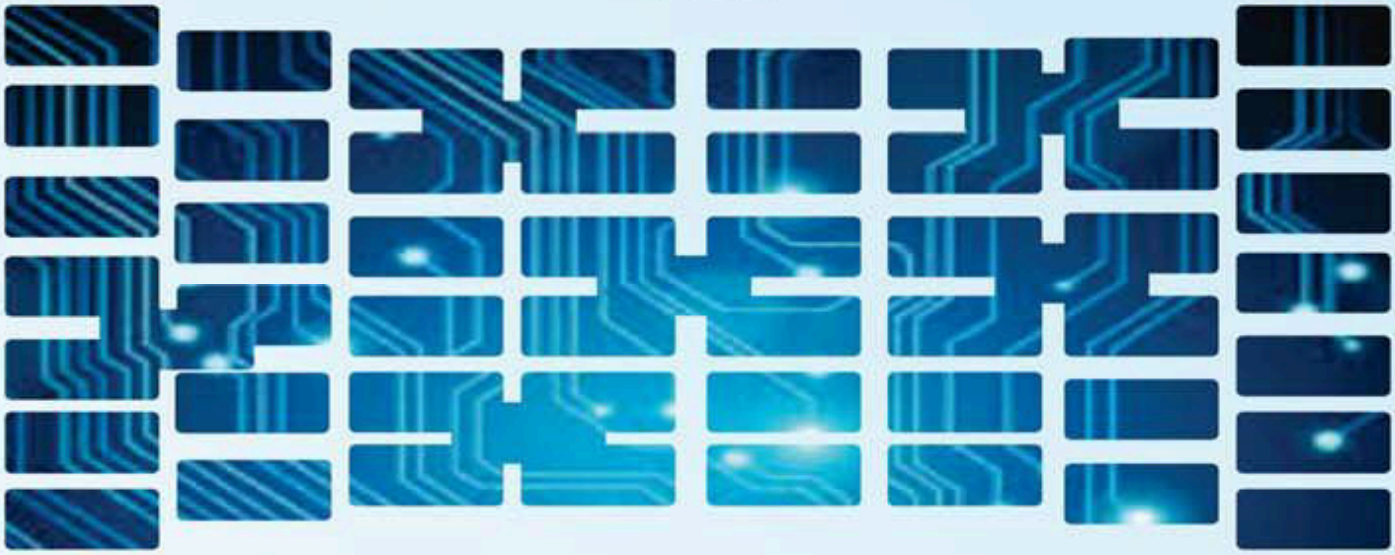
ISBN: 978-602-71550-0-8

PROSIDING

Gedung D4 FMIPA Unnes

11 Oktober 2014

SEMINAR NASIONAL ILMU KOMPUTER 2014



Trusted Digital Identity and Intelligent System

http://ilkom.unnes.ac.id/snik/2014/prosiding

Jurusan Ilmu Komputer

FMIPA UNNES

Susunan Editorial

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas terselenggaranya Seminar Nasional Ilmu Komputer 2014 dengan tema: *"Trusted Digital Identity and Intelligent System"*. Seminar ini merupakan agenda tahunan dari Jurusan Ilmu Komputer FMIPA Universitas Negeri Semarang.

Peserta dalam seminar ini terdiri dari: mahasiswa, guru, dosen dan praktisi pendidikan dari jenjang pendidikan dasar hingga perguruan tinggi dari berbagai propinsi di Indonesia. Dua narasumber utama yang hadir dalam seminar nasional ini, yaitu: Prof. Dr. Ir. R. Eko Indrajit, M.Sc., MBA., Mphil., MA., dan Nurul Hidayat, S.Pt., M.Kom. Selain itu, pemakalah pendamping yang akan mempresentasikan artikel hasil penelitian dan konseptual tentang perkembangan ilmu komputer dalam berbagai bidang. Seminar Nasional Ilmu Komputer ini ditujukan sebagai sarana mengkomunikasikan dan memfasilitasi pertukaran informasi antara peserta seminar dengan narasumber yang kompeten.

Panitia mengucapkan terimakasih pada berbagai pihak yang telah membantu penyelenggaraan seminar, yaitu:

1. Prof. Dr. Wiyanto, M.Si. (Dekan FMIPA Unnes),
2. Narasumber utama yang telah berkenan hadir,
3. Bank Mandiri, BTN, dan BNI atas sponsorshipnya,
4. Peserta dan pemakalah pendamping atas partisipasinya,
5. Segenap rekan panitia yang telah bekerja keras hingga terselenggaranya seminar.

Kumpulan artikel yang telah diseminarkan, telah disusun dalam prosiding, mudah-mudahan dapat bermanfaat bagi pemakalah dan pembaca.

Semarang, Oktober 2014

Panitia SNIK 2014

SAMBUTAN KETUA PANITIA

Oleh: Riza Arifudin, S.Pd., M.Cs.

Assalamualaikum Wr. Wb.

Yth. Bapak Dekan FMIPA Universitas Negeri Semarang
Ibu Ketua Jurusan Ilmu Komputer FMIPA Universitas Negeri Semarang
Narasumber Utama:
Bapak Prof. Dr. Ir. R. Eko Indrajit, M.Sc., MBA., Mphil., MA.
Bapak Nurul Hidayat, S.Pt., M.Kom.
Bapak/Ibu Pimpinan Jurusan dan Prodi di FMIPA Unnes
Peserta Seminar, Pemakalah Pendamping dan Bapak/Ibu tamu undangan

Hadirin yang berbahagia,

Puji syukur ke hadirat Allah SWT atas rahmat dan hidayah-Nya sehingga pada saat ini kita dapat hadir dalam kegiatan Seminar Nasional Ilmu Komputer 2014 dengan tema *"Trusted Digital Identity and Intelligent System"*. Perkembangan *Intelligent System* untuk mendukung *Trusted Digital Identity* pada saat ini sudah merupakan bagian integral dalam perencanaan strategis Sistem Informasi/Teknologi Informasi (SI/TI) suatu organisasi/perusahaan, misalnya dalam pada *e-government*, *e-commerce*.

Banyak Negara telah memberikan perhatian yang besar kepada system keotentikan *Digital Identity* untuk mendorong global dan regional e-commerce. Hal ini terkait isu tentang *privacy* dan *cyber security.* Proyek-proyek *Digital Identity* saat ini sudah diterapkan oleh pemerintah kita, misalnya seperti e-KTP. Tantangan yang dihadapi oleh penggunanya terletak pada wilayah keamanan datanya.

Dalam rangka mengkomunikasikan dan memfasilitasi pertukaran informasi berkaitan *"Trusted Digital Identity and Intelligent System"*, maka Jurusan Ilmu Komputer FMIPA Unnes akan menyelenggarakan Seminar Nasional Ilmu Komputer 2014 sebagai wahana interaksi profesional antar komunitas bidang ilmu komputer di Indonesia untuk saling bertukar pikiran, pengetahuan, pengalaman, dan gagasan, untuk mengakselerasi pengembangan penelitian di bidang ilmu komputer.

Bapak Dekan dan hadirin yang terhormat,

Penyenggaraan kegiatan seminar nasional ini merupakan seminar pertama Jurusan Ilmu Komputer FMIPA Unnes. Selain itu, banyaknya para akademisi, praktisi, dan mahasiswa telah banyak melakukan penelitian dan perlu difasilitasi untuk mengkomunikasikan berbagai hasil yang telah diperoleh. Selanjutnya pada kesempatan ini kami laporkan bahwa berdasarkan data peserta dari kegiatan seminar ini, jumlah peserta dan pemakalah pendamping yang hadir sekitar 150 orang.

Bapak Dekan dan peserta seminar yang terhormat,

Kegiatan seminar ini mengundang dua narasumber utama yaitu: Bapak Prof. Dr. Ir. R. Eko Indrajit, M.Sc., MBA., Mphil., MA., dan Bapak Nurul Hidayat, S.Pt., M.Kom.. Ucapan terimakasih dan penghargaan yang setinggi-tingginya atas kehadiran beliau berdua di Kampus Unnes Konservasi.

Akhirnya kami mohon Bapak Dekan untuk memberikan sambutan dan sekaligus membuka kegiatan seminar ini. Pada kesempatan ini, kami selaku panitia menyampaikan ucapan terima kasih pada semua pihak atas kerjasamanya sehingga acara seminar hari ini dapat terlaksana.

Wassalamu'alaikum Wr. Wb.

Semarang, 11 Oktober 2014
Ketua Panitia

Riza Arifudin, S.Pd., M.Cs.

DAFTAR ISI
PROSIDING SEMINAR NASIONAL ILMU KOMPUTER 2014
"Trusted Digital Identity and Intelligent System"

KRIPTOGRAFI PADA APLIKASI KOMUNIKASI DATA DENGAN ALGORITMA AES 256

K. I. Santoso[1] dan R. Habibi[2]
[1]Jurusan Sistem Informasi, [2]Jurusan Teknik Informatika, STMIK Bina Patria
Jl. Raden Saleh No.2 Magelang 56116
E-mail : kartikaimams@gmail.com[1], robeth.steve@gmail.com[2]

ABSTRAK

Teknologi dalam bidang komunikasi berkembang dengan pesat, tetapi ada pihak yang berusaha untuk melakukan penyadapan demi mendapatkan apa yang diinginkan dan kemudian disalahgunakan. Keamanan dari suatu data sangat penting dan jika data yang kita miliki telah disalahgunakan oleh pihak lain, maka itu akan sangat merugikan, sehingga dapat digunakan teknik kriptografi sebagai cara untuk melakukan pengaman data. Algoritma AES 256 adalah salah satu algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat proses enkripsi dan dekripsi. Data berupa pesan dalam bentuk plaintext yang akan dienkripsi dengan algoritma AES 256, dan dengan kunci yang dihasilkan dari fungsi hash MD5 (username pengirim dan penerima) menghasilkan pesan dalam bentuk chipertext. Komunikasi data yang terjadi adalah mengirimkan pesan dalam bentuk chipertext, kemudian pada saat sampai pada tujuan akan didekripsi dengan algoritma AES 256 dan kunci yang sama saat proses enkripsi sehingga pesan akan kembali dalam bentuk plaintext dan dapat dibaca oleh penerimanya. Jika terjadi penyadapan saat komunikasi data berlangsung, maka yang akan didapatkan adalah pesan chipertext yang dihasilkan dari proses enkripsi. Dengan demikian, pesan tersebut dalam kondisi aman dan dibutuhkan waktu sangat lama untuk dapat mendekripsi secara paksa chipertext dari hasil enkripsi algoritma AES 256.

Kata Kunci: AES 256, Komunikasi data, Kriptografi, MD5.

I. PENDAHULUAN

Di jaman sekarang, teknologi dalam bidang komunikasi untuk pesan sudah sangat canggih, lebih efektif, dan efisien untuk digunakan. Misalnya dengan teknologi SMS (Short Message System), Email, Chat orang bisa melakukan komunikasi dengan orang lain kapanpun, dimanapun, dengan siapapun tanpa harus bertemu selama terhubung dalam suatu sistem jaringan. Teknologi tersebut bahkan digunakan untuk aktifitas komunikasi yang penting atau rahasia. Namun keamanan komunikasi tersebut belum bisa sepenuhnya terjamin, karena masih banyak teknologi komunikasi data pesan yang belum memperhatikan bagaimana pengamanan dari data pesan tersebut. Sehingga menimbulkan aktifitas kejahatan dari pihak-pihak yang ingin mengetahui isi pesan dan kemudian bisa disalahgunakan.

Seperti yang tertulis pada www.nasional.kontan.co.id bahwa data di internet sangat rentan terjadi aksi pencurian. Ada peralatan canggih yang bisa mengambil data pribadi milik pengguna internet disediakan oleh berbagai vendor di dunia yaitu teknologi surveilance milik Gamma International yang berbasis di Munich, Jerman, yang terpasang di beberapa perusahaan jasa internet. Teknologi penyadapan ini bisa mengeluarkan data, mengambil data di dalam e-mail, percakapan pesan instan (instant messaging), komunikasi Voice over Internet Protocol (VoIP), dan memata-matai pengguna melalui webcam dan mikropon. Informasi yang didapat kemudian mereka kirim ke server penyadapan. Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) melaporkan pada tahun 2012 rata-rata serangan untuk mengambil data atau informasi secara ilegal melalui lalu lintas internet Indonesia mencapai 40.000 per hari. Di 2011, jumlahnya tiga juta serangan terhadap situs-situs pemerintah "go.id".

Penerapan kriptografi sangat dibutuhkan dalam pengamanan data dan menjaga kerahasiaan suatu data pada sistem komunikasi data. Kriptografi adalah ilmu untuk menjaga kerahasiaan informasi dari aspek-aspek yang dapat mengancam keamanan suatu informasi dengan metode dan teknik matematika tertentu. Salah satu algoritma kriptografi yang memiliki tingkat ketahanan dalam menjaga kerahasiaan data adalah algoritma AES 256.

Tujuan penelitian ini adalah:

1. Dapat mengetahui faktor-faktor apa saja yang mempengaruhi pada pengamanan data dengan teknik kriptografi.
2. Merancang dan membangun suatu sistem pengamanan data pada pesan yang berupa text.
3. Dapat menerapkan Algoritma AES 256 untuk pengamanan data berupa text.

II. METODOLOGI PENELITIAN

1. Landasan Teori

a. Komunikasi data

Data berarti informasi yang disajikan oleh isyarat digital biner. Transmisi data berarti pengiriman data antara dua komputer atau antara sebuah komputer dengan terminal. CCITT (Consultative Committee International Telephony and Telegraphy), yang sekarang dikenal sebagai ITU-T (International Telecommunications Union – Telephony) menyebut terminal sebagai piranti terminal data (Data Terminal Equipment = DTE). Jenis komputer dalam suatu jaringan data terdiri dari satu atau lebih komputer mainframe, atau host computer, komputer-komputer mini, dan komputer mikro, atau komputer pribadi. Terminal-terminal yang paling sering dipakai antara lain adalah disc drive, pencetak, plotter, layar tampilan, dan papan ketik. Selain harus dapat berkomunikasi dengan terminal-terminal lokal atau piranti peripheral, komputer harus mampu berkomunikasi dengan komputer lain dan/ atau terminal-terminal yang terpisah cukup jauh [1].

b. Keamanan komputer

Sistem keamanan komputer digunakan untuk menjamin agar sumber daya tidak digunakan atau dimodifikasi orang yang tidak diotorisasi. Pengamanan termasuk masalah teknis, manajerial, legalitas dan politis. Keamanan sistem terbagi menjadi tiga yaitu:

a) Keamanan eksternal adalah pengamanan yang berhubungan dengan fasilitas komputer dari penyusup dan bencana, misalnya bencana alam.
b) Keamanan interface pemakai berkaitan dengan identifikasi pemakai sebelum diijinkan mengakses program dan data yang tersimpan didalam sistem.
c) Keamanan internal berkaitan dengan beragam pengamanan yang dibangun pada perangkat keras dan sistem operasi untuk menjamin operasi yang handal dan untuk menjaga keutuhan program serta data.

Keamanan komputer meliputi beberapa aspek diantaranya:

a) Authentication: agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi. Dengan kata lain, informasi tersebut benar-benar dari orang yang dikehendaki.
b) Integrity: keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
c) Nonrepudiation: merupakan hal yang bersangkutan dengan si pengirim. Si pengirim tidak bisa mengelak bahwa dialah yang mengirimkan informasi tersebut.
d) Authority: Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
e) Confidentialit: merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Confidentiality biasanya berhubungan dengan informasi yang diberikan kepada pihak lain.
f) Privacy: merupakan lebih ke arah data-data yang sifatnya private (pribadi).
g) Availability: aspek Availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau yang dijebol dapat menghambat atau meniadakan akses ke informasi.
h) Access control: aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal itu biasanya berhubungan dengan masalah authentication dan juga privacy. Access control seringkali dilakukan menggunakan kombinasi user id dan password atau dengan menggunakan mekanisme lainnya [2].

c. Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani : “cryptos” artinya “secret” (rahasia), sedangkan “graphein” artinya “writing” (tulisan). Jadi, kriptografi berarti “secret writing” (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu dimana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun, saat ini kriptografi lebih dari sekedar privacy tetapi juga untuk tujuan data integrity, authentication, dan non-repudiation. Kriptografi bertujuan untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan) sebagai berikut:

a) Kerahasiaan (confidentiality), adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapt dibaca oleh pihak-pihak yang tidak berhak. Di dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi chiperteks.
b) Integritas data (data integrity), adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: " Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi) ?". Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubstitusian data ke dalam pesan yang sebenarnya.
c) Otentikasi (authentication), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication atau entry 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.
d) Nirpenyangkalan (non-repudiation), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. Sebagai contoh misalkan pengirim pesan memberi otoritas kepada penerima pesan untuk melakukan pembelian, namun kemudian ia menyangkal telah memberikan otoritas tersebut [3].

d. AES (Advanced Encryption Standard) 256 / RIJNDAEL

Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu.

Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun Rijndael mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Berikut adalah perbandingan jumlah proses yang harus dilalui untuk masing-masing masukan. (lihat Tabel 1)

Tabel 1. Jumlah Putaran Pengoperasian AES

Tipe	Panjang Kunci	Panjang Block Input	Jumlah Putaran
AES-128	128 bit	128 bit	10
AES-192	192 bit	128 bit	12
AES-256	256 bit	128 bit	14

Blok-blok data masukan dan kunci dioperasikan dalam bentuk array. Setiap anggota array sebelum menghasilkan keluaran ciphertext dinamakan dengan state. Setiap state akan mengalami proses yang secara garis besar terdiri dari empat tahap yaitu, AddRoundKey, SubBytes, ShiftRows, dan MixColumns. Kecuali tahap MixColumns, ketiga tahap lainnya akan diulang pada setiap proses sedangkan tahap MixColumns tidak akan dilakukan pada tahap terakhir. Proses enkripsi adalah kebalikkan dari dekripsi.

Dalam proses enkripsi terjadi beberapa tahap, maka diperlukan subkey-subkey yang akan dipakai pada tiap tahap. Pengembangan jumlah kunci yang akan dipakai diperlukan karena kebutuhan subkey-subkey yang akan dipakai dapat mencapai ribuan bit, sedangkan kunci yang disediakan secara default hanya 128-256 bit. Jumlah total kunci yang diperlukan sebagai subkey adalah sebanyak Nb(Nr+1), dimana Nb adalah besarnya blok data dalam satuan word. Sedangkan Nr adalah jumlah tahapan yang harus dilalui dalam satuan word [4].

Ada empat macam operasi yang dilakukan setiap putaran:

a) Transformasi Subtitusi Byte

Dalam operasi ini, setiap byte yang akan dienkripsi disubtitusikan dengan nilai byte lain dengan menggunakan S-box. S-box dibuat dari multiplicative inverse dari angka yang diberikan dalam Rijndael's finite field yang kemudian ditransformasikan dengan affine transformation seperti yang ditunjukan pada Gambar 1.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Gambar 1. Affine Transformation

Hasilnya kemudian di-xor dengan 9910 atau 0x6316 atau 11000112. Operasi matriks dengan xor ini ekuivalen dengan persamaan:

$$b'_i = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus c_i \quad (1)$$

dengan b', b, dan c adalah array 8 bit dan nilai c adalah 01100011. Proses tersebut menghasilkan masing-masing nilai dari elemen tabel S-box pada Tabel 2. Seperti yang telah diketahui sebelumnya, AES merupakan algoritma simetri, yang berarti tabel subtitusi yang dibutuhkan untuk mengenkripsi berbeda dengan untuk mendekripsi. Untuk acuan tersebut, digunakanlah tabel S-box inversi seperti pada Tabel 3.

Tabel 2. S-box

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Tabel 3. S-box Inversi

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Sebagai contoh, input yang akan dienkripsikan adalah

95 95 08 19
4f 6b 5c 6e
c8 89 80 26
fc 75 4e 6c

Dengan menggunakan S-box, hasil dari operasi ini adalah

2a 2a 30 d4
84 7f 4a 9f
e8 a7 cd f7
b0 9d 2f 50

Jika hasil tersebut ingin dikembalikan ke nilai semula sebelum operasi, nilai nilainya dapat disubtitusikan dengan menggunakan tabel S-box inversi. Operasi transformasi subtitusi byte pada proses

enkripsi dan dekripsi tidak dilakukan pada putaran pertama. Operasi ini hanya dilakukan pada putaran kedua hingga terakhir.

b) Transformasi Pergeseran Baris

Pada operasi ini, byte-byte pada setiap baris digeser secara memutar dengan pergeseran yang berbeda dari tiap-tiap baris. Setiap baris digeser dengan aturan tertentu untuk jenis panjang blok yang berbeda. Baris pertama blok untuk semua jenis panjang blok (128, 196, dan 256 bit) tidak digeser. Baris kedua untuk semua jenis panjang blok digeser 1 ke kiri. Pergeseran baris ketiga dan keempat untuk panjang blok 128 dan 196 bit berbeda dengan 256 bit. Pada panjang blok 128 dan 196 bit, baris ketiga digeser ke kiri sebanyak dua kali dan baris keempat digeser ke kiri sebanyak tiga kali. Pada panjang blok 256 bit, baris ketiga digeser ke kiri sebanyak tiga kali dan baris keempat digeser ke kiri sebanyak empat kali. Untuk lebih jelasnya, proses tersebut dapat dilihat pada Gambar 2.

S

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$	$S_{0,4}$	$S_{0,5}$	$S_{0,6}$	$S_{0,7}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,4}$	$S_{1,5}$	$S_{1,6}$	$S_{1,7}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$	$S_{2,4}$	$S_{2,5}$	$S_{2,6}$	$S_{2,7}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$	$S_{3,4}$	$S_{3,5}$	$S_{3,6}$	$S_{3,7}$

↓

S'

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$	$S_{0,4}$	$S_{0,5}$	$S_{0,6}$	$S_{0,7}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,4}$	$S_{1,5}$	$S_{1,6}$	$S_{1,7}$	$S_{1,0}$
$S_{2,3}$	$S_{2,4}$	$S_{2,5}$	$S_{2,6}$	$S_{2,7}$	$S_{2,0}$	$S_{2,1}$	$S_{2,2}$
$S_{3,4}$	$S_{3,5}$	$S_{3,6}$	$S_{3,7}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Gambar 2. Operasi pada Blok 256 bit

Sebagai contoh, hasil operasi ini terhadap input yang nilainya adalah output dari hasil operasi subtitusi byte sebelumnya adalah sebagai berikut:

2a 2a 30 d4
7f 4a 9f 84
cd f7 e8 a7
50 b0 9d 2f

c) Transformasi Percampuran Kolom

Transformasi ini mengoperasikan blok pada masing masing kolomnya. Setiap kolom diperlakukan sebagai four-term polynomial dengan cara Galois Field (GF) (28) dan dimodulokan dengan x tetap a(x), yaitu a(x) = {03}x3 + {01}x2 + {01}x + {02} Hal ini dapat dituliskan sebagai perkalian matriks sebagai berikut:

$$s'(x) = a(x) \otimes s(x)$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad (2)$$

dengan c adalah letak kolom, sehingga hasilnya

$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c} \quad (3)$$

$$s'_{0,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c} \quad (4)$$

$$s'_{0,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c}) \quad (5)$$

$$s'_{0,c} = (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c}) \quad (6)$$

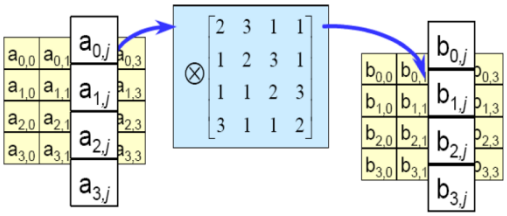
Jika hasil perkalian memiliki lebih dari 8 bit, bit yang lebih tidak begitu saja dibuang. Hasil tersebut di dengan 1000110112. Sebagai contoh, perkalian 11001010 dengan 11 dengan GF(28) akan berlangsung sebagai berikut:

```
11001010
        11
-------------- *
11001010
 11001010
---------------- xor
101011110
100011011
---------------- xor
   1000101
```

Nilai 1000101 merupakan hasil dari perkalian tersebut. Misalnya, jika dalam transfomasi ini input yang dipakai adalah hasil dari operasi pergeseran baris sebelumnya, hasil yang diperoleh adalah sebagai berikut:

48	cd	af	ac
c8	0c	ab	1a
24	5e	d8	74
6c	b8	06	fa

Transformasi ini dapat diilustrasikan seperti Gambar 3.



Gambar 3. Ilustrasi Transformasi Percampuran Kolom

Operasi transformasi ini tidak digunakan dalam putaran terakhir, baik untuk enkripsi maupun dekripsi.

d) Transformasi Penambahan Kunci

Dalam operasi transformasi ini, digunakanlah upakunci untuk masing-masing putaran yang berasal dari kunci utama dengan menggunakan jadwal kunci Rijndael (Rijndael's key schedule) yang ukuran upakunci tersebut sama dengan ukuran blok yang akan diproses. Upakunci tersebut kemudian di-xor dengan blok input sehingga diperoleh hasilnya. Sebagai contoh adalah:

jika inputnya:

a3	c5	08	08
78	a4	ff	d3
00	ff	36	36
28	5f	01	02

dan diperoleh upakunci:

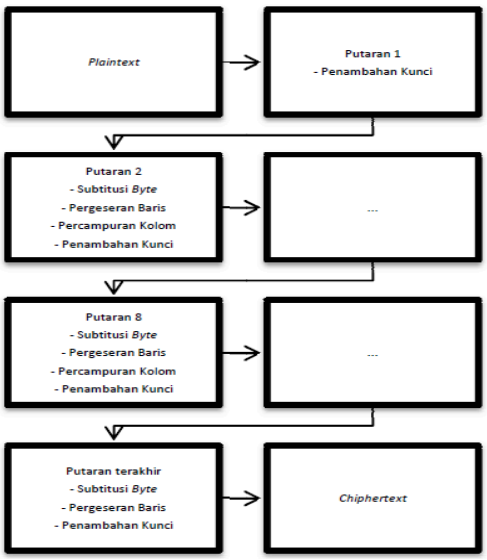
36	8a	c0	f4
ed	cf	76	a6
08	a3	b6	78
31	31	27	6e

Maka, hasilnya adalah:

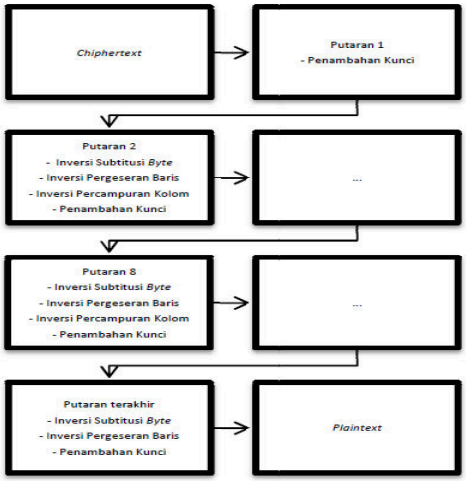
a6	34	1a	00
24	dd	f1	0e
62	a8	73	cf
48	b9	5d	61

e) Putaran

Seperti yang telah diketahui sebelumnya, jumlah putaran pengoperasian blok input untuk setiap macam panjang blok berbeda-beda. Akan tetapi jumlah putaran untuk proses enkripsi dan dekripsi tetap sama. Proses enkripsi bisa dilihat pada Gambar 4 dan proses dekripsi bisa dilihat pada Gambar 5.



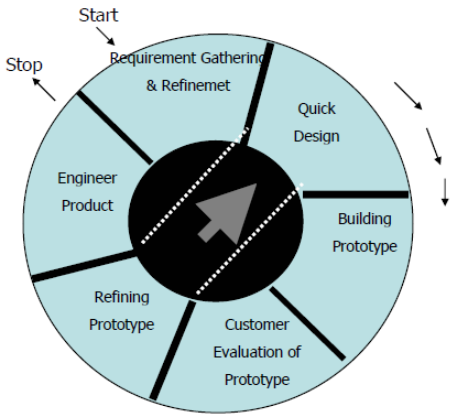
Gambar 4. Diagram Proses Enkripsi



Gambar 5. Diagram Proses Dekripsi

e. Model proses

Model Proses yang digunakan untuk membangun sistem aplikasi ini adalah Model Prototyping. Model Perancangan Prototyping dapat di lihat pada Gambar 6.



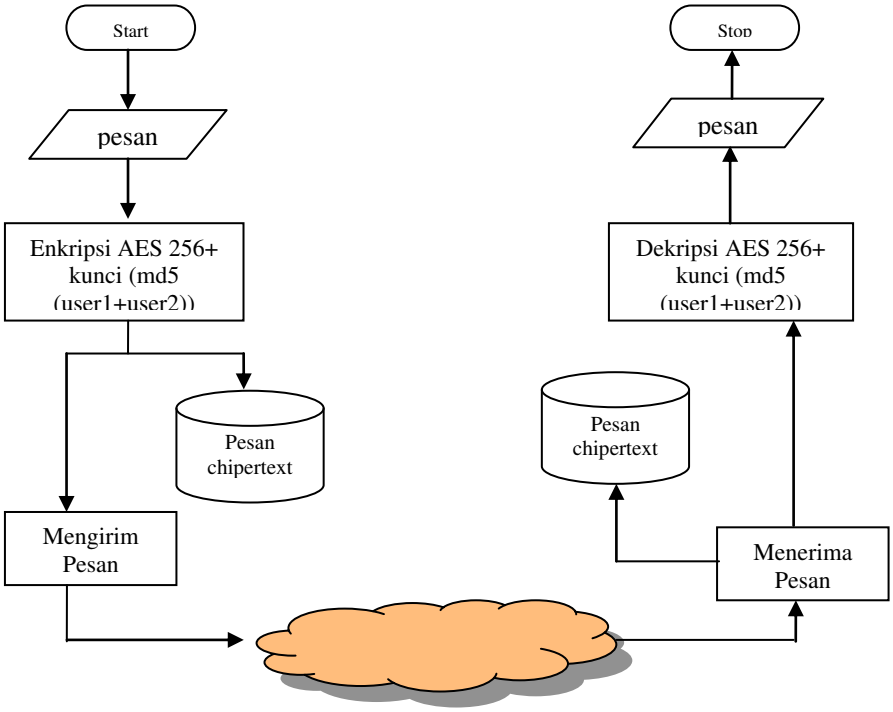
Gambar 6. Model Perancangan Prototyping

Prototyping paradigma dimulai dengan pengumpulan kebutuhan. Pengembang dan pengguna bertemu dan mendefinisikan obyektif keseluruhan dari perangkat lunak, mengidentifikasi segala kebutuhan yang diketahui, dan area garis besar dimana definisi lebih jauh merupakan keharusan kemudian dilakukan "perancangan kilat".

Perancangan kilat berfokus pada penyajian dari aspek-aspek perangkat lunak tersebut yang akan nampak bagi pelanggan/ pemakai (contohnya pendekatan input dan format output). Perancangan kilat membawa kepada kontruksi sebuah prototipe. Prototipe tersebut dievaluasi oleh pelanggan/ pemakai dan dipakai untuk menyaring kebutuhan pengembangan perangkat lunak. Iterasi terjadi pada saat prototipe disetel untuk memenuhi kebutuhan pelanggan dan pada saat yang sama memungkinkan pengembang untuk lebih baik memahami apa yang harus dilakukan [5].

III. HASIL DAN PEMBAHASAN

Hasil penelitian adalah sebuah sistem prototipe kriptografi pada komunikasi data dengan algoritma AES 256. Gambar alur dari sistem tersebut dapat dilihat pada Gambar 7.

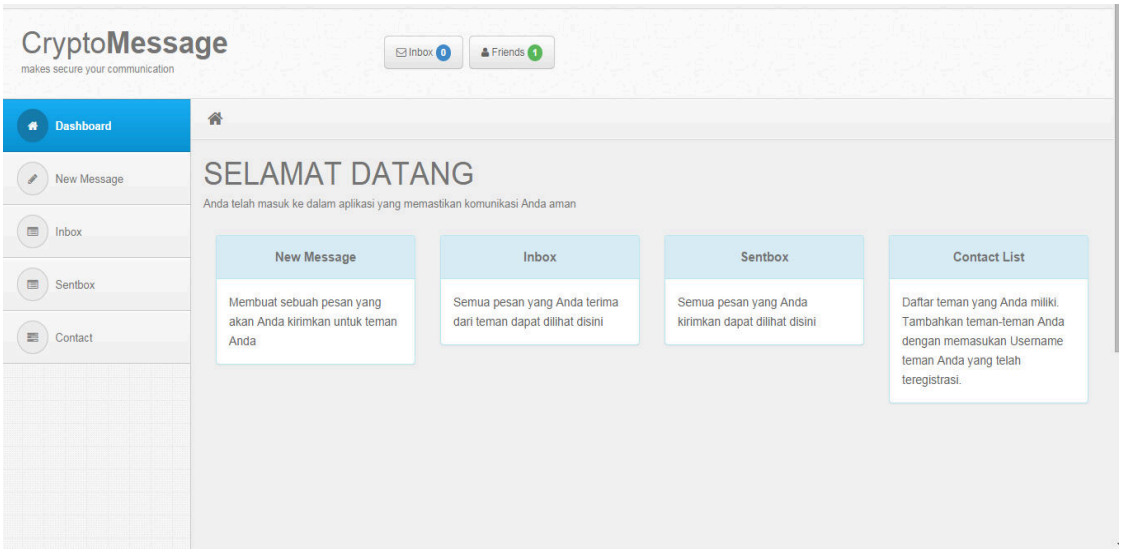


Gambar 7. Alur system

User membuat pesan baru dalam bentuk plaintext yang akan dikirimkan ke user lain sebagai penerima. Pesan plaintext akan dienkripsi dengan algoritma AES 256 dengan kunci yang dibangkitkan dari fungsi hash MD5 username pengirim dan username penerima. Pesan hasil enkripsi yang berupa chipertext akan disimpan di database lokal komputer pengirim serta akan dikirimkan ke penerima melalui jaringan internet.

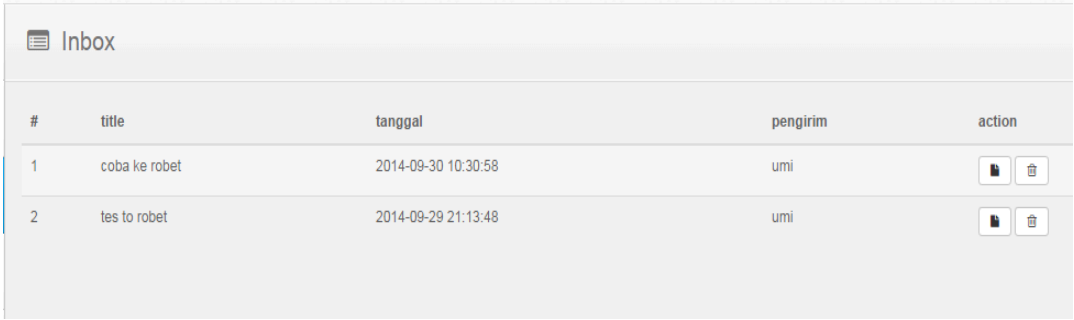
Pesan yang telah dikirim oleh pengirim, akan diterima oleh penerima sesuai dengan username yang dituju berupa pesan chipertext. Pesan tersebut akan disimpan di database lokal komputer penerima serta akan didekripsi dengan algoritma AES 256 dengan kunci yang dibangkitkan dari fungsi hash MD5 username pengirim dan username penerima. Pesan hasil dekripsi berupa pesan plaintext sesuai dengan pesan yang dikirimkan oleh pengirim, kemudian penerima dapat membaca pesan tersebut.

Hasil interface dari sistem yang telah dibangun, antara lain Halaman Utama pada Gambar 8, Form untuk memasukkan pesan (Form New Message) yang akan dikirmkan bisa dilihat pada Gambar 9, halaman pesan masuk (inbox) bisa dilihat pada Gambar 10, serta halaman isi pesan (Detail inbox message) bisa dilihat pada Gambar 11.

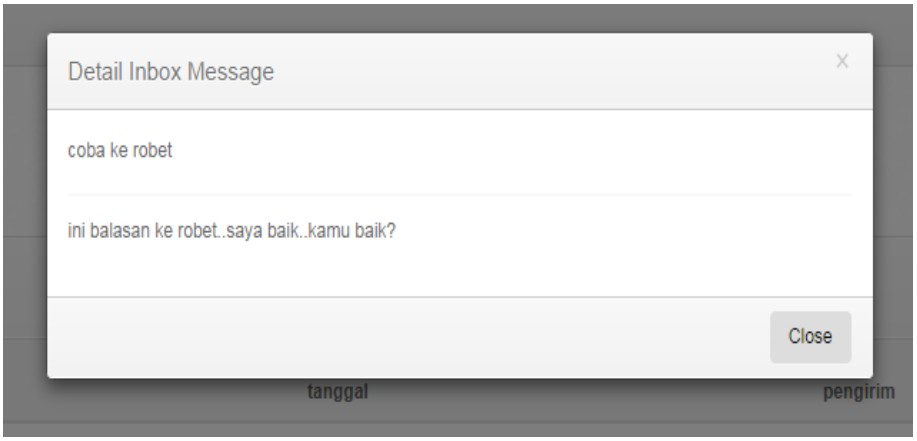


Gambar 8. Halaman Utama

Gambar 9. Form New Message



Gambar 10. Halaman Inbox



Gambar 11. Detail Inbox Message

1. Analisa Brute Force Attack

Untuk membuktikan bahwa pengamanan data dengan algoritma AES 256 dan dengan kunci yang dibangkitkan dari MD5 (pengirim + penerima) memiliki tingkat keamanan yang kuat, maka penulis akan melakukan analisis dengan metode Brute Force Attack. Dengan cara menghitung perkiraan waktu yang dibutuhkan untuk melakukan peretasan pada MD5 dan AES 256.

Jika diasumsikan spesifikasi komputer yang digunakan untuk melakukan brute force attack adalah supercomputer dengan spesifikasi yang dapat dilihat pada Tabel 2.

Tabel 2. Spesifikasi Supercomputer

Cores:	705.024
Linpack Performance (Rmax)	10.510 TFlop/s
Power:	12.659,89 kW
Memory:	1.410.048 GB
Processor:	SPARC64 VIIIfx 8C 2GHz
Operating System:	Linux

Dari data spesifikasi tersebut, diketahui komputer tersebut memiliki kemampuan melakukan pencarian acak yaitu 10.51 x 10^{15} per detik dan pengecekan kombinasi sebanyak 1000 kali per detik, maka berikut perhitungannya:

Jumlah pengecekan kombinasi per detik
(10.51 x 10^{15}) / 1000 = 10.51 x 10^{12}
Jumlah detik selama 1 tahun
365 x 24 x 60 x 60 = 31536000 detik

Waktu yang dibutuhkan untuk melakukan crack pada AES 256 dengan jumlah kemungkinan kunci 1.1 x 10^{77}:

= (1.1 x 10^{77}) / [(10.51 x 10^{12} / detik) x (31536000 detik / tahun)]
= (1.1 x 10^{59}) / 331.44336
= 3.3188 x 10^{56} tahun

Dari hasil perhitungan yang diperoleh diatas, butuh waktu begitu lama untuk dapat melakukan crack terhadap algoritma MD5 dan AES 256 yang digunakan pada sistem ini. Sehingga algoritma tersebut dapat dikatakan mempunyai tingkat keamanan yang kuat.

IV. SIMPULAN

Kriptografi dengan algoritma AES 256 telah dapat mengamankan data berupa pesan pada komunikasi data. Faktor-faktor yang mempengaruhi keamanan dari suatu pesan, yaitu algoritma kriptografi yang digunakan, kunci yang digunakan untuk proses enkripsi dan dekripsi. Algoritma AES 256 yang digunakan untuk pengamanan data pesan temasuk aman, karena kemungkinan untuk membobol sebuah data pesan adalah 3.3188 x 10^{56} tahun.

V. REFERENSI

[1] Santosa I. (1995). Komunikasi Data / DC Green. Yogyakarta: Penerbit Andi.
[2] Ariyus D. (2006). Computer Security. Yogyakarta: Penerbit Andi.
[3] Munir, R. (2006). Kriptografi. Bandung: Penerbit Informatika.
[4] Dharmawan EA. (2013). Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael. Jurnal EECCIS, 7(1): 77-84.
[5] Pressman RS. (1997). *Software Engineering : A Practitioner's Approach.* New York: The McGraw-Hill Companies.