Jurnal Nasional Informatika dan Teknologi Jaringan
E-ISSN : 2540-7600
P-ISSN : 2540-7597

PENERAPAN KOMBINASI ALGORITMA BASE64 DAN ROT47 UNTUK ENKRIPSI DATABASE PASIEN RUMAH SAKIT JIWA PROF. DR. MUHAMMAD ILDREM

Rachmat Aulia [1], Ahmad Zakir [2], Dian Agung Purwanto[3]

[13]*Prodi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer*
[2]*Prodi Sistem Informasi, Fakultas Teknik dan Ilmu Komputer*
Universitas Harapan Medan, Jl. HM Jhoni No. 70 Medan, Indonesia
jackm4t@gmail.com[1], suratzakir@gmail.com[2], dian.agungp@gmail.com[3]

***Abstrak*--Pada suatu perusahaan, data merupakan hal yang sangat penting untuk dilindungi sehingga masalah keamanan data merupakan hal yang sangat di perhatikan. Hal yang dapat dilakukan untuk melindungi data agar tidak dapat disalah gunakan oleh orang lain ialah dengan menggunakan teknik kriptografi. Kriptografi terdiri dari seperangkat algoritma dan teknik untuk mengubah data menjadi bentuk lain sehingga isinya tidak terbaca dan tidak dapat dijelaskan oleh siapa saja yang tidak memiliki kewenangan untuk membaca atau menulis data yang telah di ubah. Dalam tugas akhir ini membahas metode enkripsi menggunakan algoritma ROT47 yang digunakan untuk mengenkripsi data dimana data yang ada posisinya akan dirubah sesuai dengan jumlah rotasi yang ada, kemudian data kembali dienkripsi menggunakan algoritma Base64 yang merupakan skema pengkodean data biner menjadi rangkaian kode ASCII sesuai index pada Base64. Dengan demikian menggunakan kedua metode perlindungan tersebut secara bersama-sama akan meningkatkan keamanan untuk melindungi data.**

Kata Kunci--Kriptografi, Base64, ROT47, Data, Algoritma, ASCII.

Abstract--In a company, the data is very important to be protected so that the data security problem is a matter of great concern. The thing that can be done to protect data so that can't be misused by others is by using cryptography technique. Cryptography consists of a set of algorithms and techniques for converting data into other forms so that the content is unreadable and can't be explained by anyone who has no authority to read or write data that has been changed. In this final project discusses the encryption method using ROT47 algorithm that is used to encrypt data where the existing data position will be changed according to the number of existing rotation, then the data is re-encrypted using Base64 algorithm which is a binary data encoding scheme into ASCII code sequence according to index on Base64. Thus using both methods of protection together will increase security to protect data.

***Keywords*--Cryptography, Base64, ROT47, Data, Algorithm, ASCII.**

I. PENDAHULUAN

Teknologi komputer sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi). Kelompok (organisasi) tersebut sangat membutuhkan adanya komputerisasi dalam setiap kegiatannya. Dari hal penggunaan komputerisasi tersebut, maka dibuatlah sebuah sistem keamanan bagi seluruh aset-asetnya, terutama informasi dan data penting demi menjaga kerahasiaan informasi data tersebut.

Keamanan merupakan aspek penting dari suatu data atau informasi, dimana pengiriman data atau informasi membutuhkan keamanan yang tinggi [6]. Ada beberapa cara melakukan pengamanan data ataupun pesan, diantaranya adalah dengan menggunakan teknik penyamaran data yang disebut dengan kriptografi. Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal [5].

Pada saat ini rumah sakit jiwa Prof. Dr. Muhammad Ildrem masih menggunakan aplikasi pengolah data pasien yang dimana data pada aplikasi tersebut dapat dilihat oleh orang lain yang tidak

memiliki tanggung jawab terhadap data yang ada tersebut. Data yang ada dapat dilihat, digandakan, dan juga dimanipulasi, hal tersebut tentunya dapat menimbulkan masalah apabila data pribadi pasien yang ada disalah gunakan oleh orang yang tidak bertanggung jawab tersebut dengan tindak kejahatan seperti penipuan.

Pengamanan data yang akan digunakan untuk menjaga data yang ada yaitu dengan menggunakan kombinasi Algoritma ROT47 dan Algortima Base64 untuk mengenkripsi data pasien yang ada, dimana dengan mengkombinasi kedua algoritma tersebut dapat menjadi salah satu teknik enkripsi yang cukup rumit dikarenakan apabila ada orang yang ingin melihat teks asli harus mengetaui kunci dan jenis kombinasi algoritma yang digunakan untuk mengenkripsi data yang ada.

Ada beberapa referensi yang diambil sebagai bahan pertimbangan untuk penelitian yang dilakukan, referensi tersebut diambil dari beberapa penelitian yang dilakukan sebelumnya yang membahas tentang permasalahan yang hampir sama, antara lain :

1. Penelitian yang dilakukan oleh Basri, ia melakukan suatu analisis dalam perspektif keamanan data dan kompleksitas komputasi menggunakan dua jenis metode kriptografi Asimetri untuk implementasinya [3].
2. Egar Dika Santosa, ia merancang mengimplementasikan algoritma caesar cipher dan hill cipher pada database sistem inventori TB Mita Jepara [4].
3. Komarudin, ia merancang sistem keamanan web menggunakan kriptografi MD5 pada koperasi Mitra Sejahtera Bandung dan dirancang menggunakan pendekatan metode *Object Oriented Development Life Cycle (OODLC)*[5].

Dalam pelaksanaan penelitian ini, masalah yang dibahas, dan diselesaikan adalah:

1. Bagaimana menerapkan algoritma ROT47 dan algoritma Base64 untuk enkripsi data pasiendi rumah sakit jiwa Prof. Dr. Muhammad Ildrem ?
2. Apakah dengan aplikasi ini dapat membantu pihak rumah sakit jiwa Prof. Dr. Muhammad Ildrem untuk mengamankan data pasien yang ada.

Tujuan dari penelitian ini, antara lain :

1. Membangun dan menerapkan sebuah aplikasi yang dapat mengamankan data pribadi pasien dengan mengkombinasikan algoritma ROT47 dan algoritma Base64.
2. Membantu pihak rumah sakit jiwa Prof. Dr. Muhammad Ildrem untuk mengamankan data pasien agar tidak dapat di salah gunakan oleh orang yang tidak bertanggung jawab.

Kriptografi berasal dan bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dan suatu tempat ke tempa lain.

Kriptografi adalah ilmu untuk menjaga isi data atau pesan agar tetap aman. Aman di sini berarti tidak bisa atau sulit diakses oleh orang lain yang tidak berhak. Kata “hak” di sini bukan hak dalam artian legal hukum atau di ijinkan atas nama hukum, tetapi seseorang yang memang diijinkan oleh pengirimnya atau si empunya data untuk mengakses data tersebut.

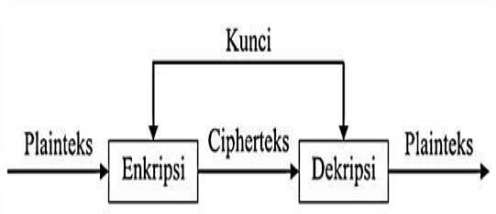
Algoritma*Base64* merupakan salah satu algoritma untuk *Encoding* dan *Decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang digunakan untuk melakukan encoding (penyandian) terhadap data binary [7]. Algorimtainibanyak digunakan di dunia *Internet* sebagai media data format untuk mengirimkan data, penggunaan tersebut dikarenakan hasil dan *encode base64* berupa *plaintext*, maka data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa *binary*. Skema Base64 biasanya digunakan ketika ada kebutuhan untuk menyandikan data biner yang perlu disimpan dan ditransfer melalui media yang dirancang untuk menangani data tekstual.

Algoritma *Base64* menggunakan kode ASCII dan kode *index base64* dalam melakukan proses enkripsi ataupun dekripsinya. Dalam melakukan enkripsi pada URL *website*, kode *index base64* perlu dimodifikasi. Simbol “+“ dimodifikasi menjadi “-“ dan simbol simbol *“/”* menjadi”_” [17].

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	W
1	B	17	R	33	h	49	X
2	C	18	S	34	i	50	Y
3	D	19	T	35	j	51	Z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	T	61	9
14	O	30	e	46	U	62	+
15	P	31	f	47	V	63	/

Gbr. 1 Index algoritma Base64
Sumber :[1]

Algoritma kriptografi Base64 ini sebenarnya menggunakan algoritma kunci simetris atau disebut juga algoritma kriptografi konvensional, yaitu algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi.



Gbr. 2 Algoritma simetris

Adapun tahapan - tahapan enkripsi menggunakan Algoritma Base64 adalah sebagai berikut :

1. Mengkonversi karakter ke biner.
2. Perhatikan dan pastikan bahwa ada 24 bit.
3. Mengkonversi 24 bit dari tiga kelompok 8 bit ke empat kelompok 6 bit.
4. Convert masing-masing empat kelompok 6 bit ke desimal.
5. Gunakan masing-masing desimal untuk mencari kode karakter pada index Base64.

Adapun tahapan - tahapan dekripsi menggunakan Algoritma Base64 adalah sebagai berikut :

1. Mengkonversi karakter Base64 ke biner dengan menggunakan 6 bit.
2. Konversi 24 bit dari empat kelompok 6 bit ke tiga kelompok 8 bit.
3. Konversi masing-masing tiga kelompok 8 bit ke desimal.
4. Gunakan masing-masing tiga desimal untuk mencari karakter ASCII untuk nilai yang ada.

ROT47 merupakan algoritma yang menggantikan karakter dalam rentang ASCII dengan karakter 47 karakter setelah itu (rotasi) dalam tabel ASCII.Ini adalah algoritma dibalik yaitu menerapkan algoritma yang sama untuk memasukkan dua kali akan mendapatkan teks asal. ROT47 merupakan pengembangan dari jenis varian ROT13, dimana ROT47 dapat dikatakan lebih unggul dikarenakan ROT47 yang menambah angka dan simbol-simbol di samping alfabet dasar.

$$s = \mathrm{ROT}_{47}(\mathrm{ROT}_{47}(s))$$

Gbr. 3 Rumus ROT47

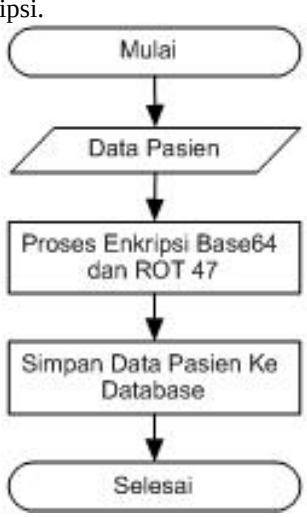
Dimana :
S= subtitusi

Algoritma ROT47 adalah turunan dari ROT13. ROT47 memperkenalkan huruf dan simbol campuran, oleh karena itu, teks yang dikodekan terlihat lebih jelas bahwa teks telah dienkripsikan. ROT47 juga dapat dengan mudah diimplementasikan oleh bahasa pemrograman modern dengan banyak cara. Cara kerja Algortma ROT47 yaitu bekerja berdasarkan nilai ASCII dengan rentang nilai 33 - 126 dan melihat nilai dimiliki oleh setiap karakter, contoh huruf "a" bernilai "97" maka dengan melakukan pergeseran sebanyak 47 langkah akan menjadi angka "2" dengan nilai "50"

Basis data adalah kumpulan data yang saling berelasi. Data sendiri merupakan fakta mengenai obyek,orang,dan lain-lain. Data dinyatakan dengan nilai (angka, deretan karakter, atau simbol). Menurut James Martin (1975), basis Data adalah kumpulan dari data yang saling terhubung (*interrelated*data) yang disimpan secara bersama-sama pada suatumedia, tanpa ada kerusakan atau kerangkapan data,sehingga proses penambahan, pengambilan dan modifikasi data dapat dilakukan dengan mudah dan terkontrol[2].

2. Perancangan Sistem

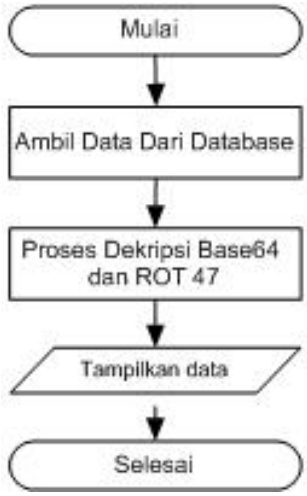
Proses perancangan *flowchart* terdiri dari dua proses yaitu perancangan *flowchart* enkripsi dan *flowchart* dekripsi.



Gbr. 4 *Flowchart* skema proses enkripsi dari aplikasi

Proses enkripsi yang akan di terapkan kepada aplikasi yang akan di rancang, adapun prosesnya yaitu :

1. Database pasien akan proses dan dienkripsi menggunakan algoritma ROT47 dan Base64.
2. Data yang telah diproses dan dienkripsi menggunakan algoritma ROT47 dan Base64 selanjutnya akan disimpan kedalam *database*.

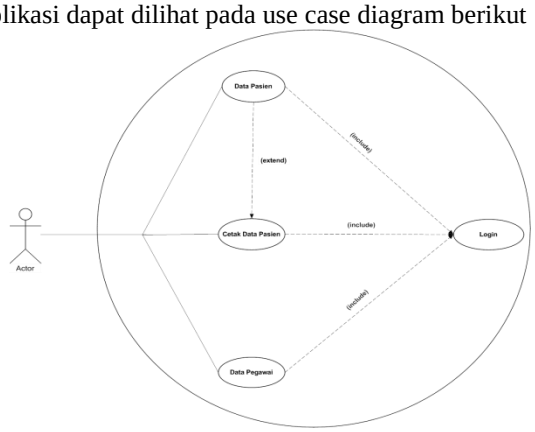


Gbr. 5 *Flowchart* skema proses dekripsi dari aplikasi

Proses dekripsi yang akan di terapkan kepada aplikasi yang akan di rancang, adapun prosesya itu :

1. Database pasien akan diambil dari *database*.
2. Data diproses dan didekripsi menggunakan algoritma ROT47 dan Base64.
3. Data yang telah diproses akan di tampilkan pada aplikasi.

Langkah-langkah yang dilakukan pengguna aplikasi dapat dilihat pada use case diagram berikut :



Gbr. 6 *Usecase diagram* pengguna aplikasi

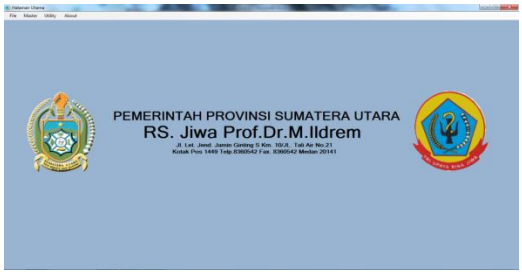
Pada *usecase diagram* pengguna aplikasiterdapat *actor* didalam sistem yang dirancang yaitu sebagai pegawai. Pegawai berperan untuk menambahkan, mengubah, menghapus data pasien dan data pegawai, dan hanya pegawai yang bisa mencetak data pasien yang ada.

3. Hasil dan Pembahasan

Pada bagian ini, diuraikan hasil perancangan aplikasi dan pembahasan dari metode yang telah diuraikan diatas.

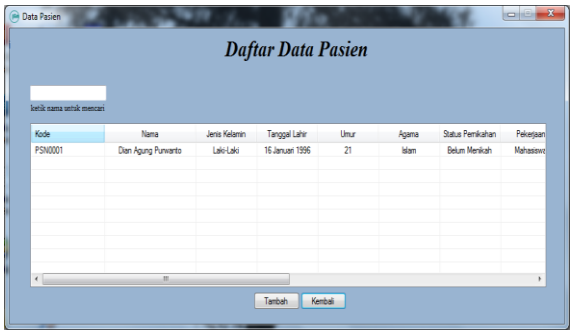
Gbr. 7 Menu login

Menu *login* merupakan tampilan yang digunakan pegawai untuk masuk ke menu utama dengan memasukkan *username*dan *password*. Pegawai yang sudah memiliki akun akan memasukkan *username* dan *password* dan selanjutnya system melakukan validasi.



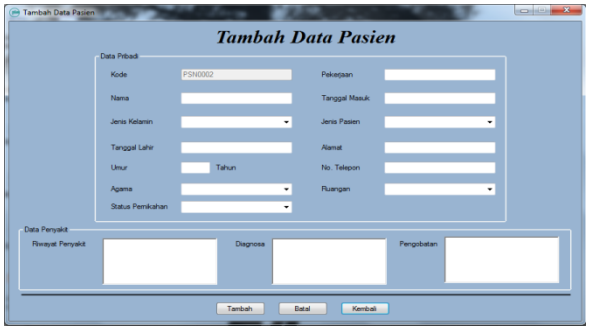
Gbr. 8 Menu utama

Menu utama pegawai merupakan tampilan utama yang di gunakan oleh pegawai untuk masuk ke beberapa menu.



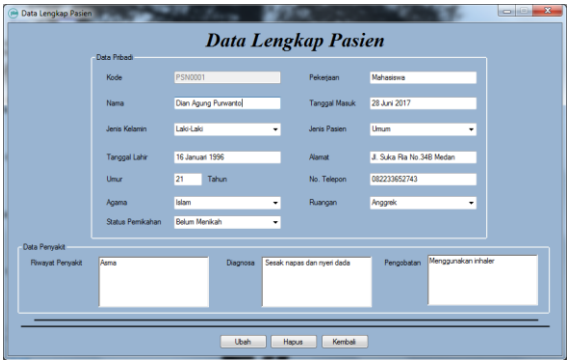
Gbr. 9 Menu daftar data pasien

Menu data pasien merupakan tampilan menu untuk melihat data pasien, di dalam menu ini terdapat informasi terkait data pribadi pasien.



Gbr. 10 Menu tambah data pasien

Pada menu tambah, pegawai bisa menambah identitas pasien baru dan apabila data pada *listview* di klik maka akan menampilkan menu ubah data pasien.

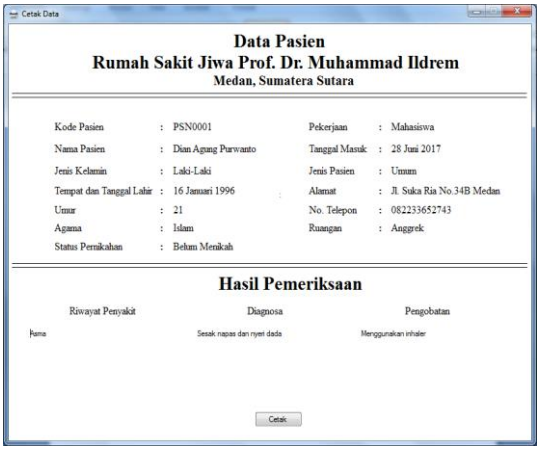


Gbr. 11 Menu ubah data pasien

Pada gambar diatas terlihat beberapa data seperti nama, jenis kelamin, dan tanggal lahir. Jika data pada salah satu *textbox*di ubah, maka data tidak akan tersimpan. Pada gambar juga terlihat tombol hapus yang digunakan untuk menghapus data pasien terpilih.

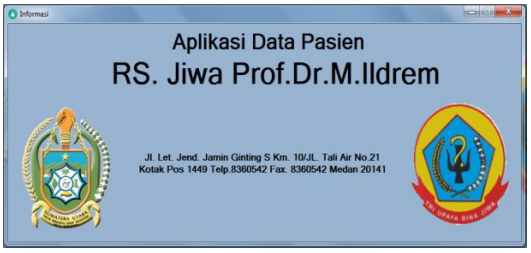
Gbr. 12 Menu pilih data pasien untuk di cetak

Menu cetak data pasien merupakan tampilan menu untuk melihat dan mencetak data pasien pada rumah sakit jiwa Prof. Dr. Muhammad Ildrem



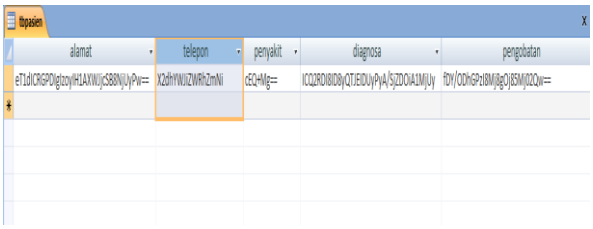
Gbr. 13 Hasil cetak data pasien

Pada gambar 4.10 diatas terlihat beberapa informasi mengenai pasien seperti nama, agama, alamat, dll.



Gbr. 14 Menu informasi.

Menu Informasi merupakan tampilan menu untuk melihat informasi mengenai aplikasi yang telah dirancang.



Gbr. 15 Data Enkripsi

Berdasarkan gambar diatas terlihat beberapa data yang telah terenkripsi pada *database*. Adapun data yang terenkripsi adalah data pada *field* alamat, *field* telepon, *field* penyakit, *field* diagnose, dan *field* pengobatan.

4. Kesimpulan dan Saran

Berdasarkan dari uraian yang telah dibahas sebelumnya melalui implementasi dan pengujian sistem, maka penulis dapat mengambil kesimpulan sebagai berikut :

1. Aplikasi ini dirancang dengan menggunakan Microsoft Visual Studio 2015 dengan tujuan untuk mengamankan database pasien pada rumah sakit jiwa Prof. Dr. M. Ildrem.

2. Kombinasi algoritma ROT47 dan Base64 dapat menjadi sebuah algoritma dengan keamanan yang memadai dan dapat digunakan untuk mengamankan database pasien pada rumah sakit jiwa Prof. Dr. M. Ildrem.
3. Kombinasi algoritma ROT47 dan Base64 dapat di imlementasikan ke dalam sistem enkripsi database pasien dengan baik.

Dengan dirancangnya sistem ini diharapkan dapat menjadi sarana bagi perkembangan sistem yang lebih lanjut, agar dapat meningkatkan kinerja sistem yang lebih baik. Berikut adalah saran penulis yaitu :

1. Diharapkan pada perkembangan selanjutnya, desain aplikasi dapat lebih diperbaiki agar terlihat lebih menarik.
2. Menambah algoritma lain pada aplikasi dimasa mendatang agar dapat memperkuat keamanan pada *database.*
3. Menambah fitur/fasilitas pada aplikasi dimasa mendatang agar dapat memenuhi kebutuhan dari aplikasi, dan juga berfungsi untuk kenyaman pengguna.

REFERENSI

[1] Ahmad , Mohammad A. 2012. Protection of the Texts Using Base64 and MD5. Maret 2012. University Malaysia, Malaysia

[2] Aulia, Rachmat. 2013. *Pemanfaatan Website Sebagai Saranan Managing Data Dalam Suatu Organisai (Studi Kasis : Pertemuan Ilmian Nasional (PIN) Perhimpunan Dokter Spesialis Saraf Indonesia (Perdossi) 2013 Medan.* September 2016. Vol. 1. No. 1. Medan. Universitas Islam Sumatera Utara (UISU).

[3] Basri. 2016. Kriptografi SimetrisDan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi. September 2016. Vol. 2, No. 2. Sulawesi Barat. Universitas Al Asyariah Mandar .

[4] Dika Santosa, Egar. 2015. Ilmplementasi Algoritma Caesar Cipher Dan Hill Cipher Pada *Database* Sistem *Inventory* TB Mitra Jepara. Universitas Dian Nuswantoro.

[5] Komarudin. 2013. Sistem Keamanan Web Dengan Menggunakan Kriptografi Message Digest 5/Md5 Pada Koperasi Mitra Sejahtera Bandung. Juni 2013. Vol. 7, No. 1. STMIK Mardira Indonesia.

[6] Pradipta, Anjar. 2016. *Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi*. Agustus 2016. *Volume 5 No 3.* Yogyakarta. STMIK AMIKOM Yogyakarta.

[7] Wahyu C, Febrian. 2012. *Penerapan Algoritma Gabungan RC4 dan Base64 Pada Sistem Keamanan E-Commerce*.Juni 2012. Universitas Kristen Satya Wacana.