IMPLEMENTASI KRIPTOGRAFI DENGAN MENGGUNAKAN METODE RC4 DAN BASE64 UNTUK MENGAMANKAN DATABASE SEKOLAH PADA SDN GROGOL UTARA 10

Abdul Kodir[1)], **Wahyu Pramusinto**[2)]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : khodir.abduel@gmail.com[1)], wahyu.pramusinto@budiluhur.ac.id[2)]

Abstrak

Pesatnya perkembangan teknologi dan juga komunikasi dizaman saat ini dapat membawa pengaruh bebas terutama dibagian keamanan data ataupun informasi yang penting. Namun kemudahan dalam mengakses media komunikasi oleh siapapun, membawa dampak yang buruk bagi keamanan informasi data. Data menjadi sangat mudah untuk dicuri, dirusak dan juga diubah oleh orang yang tidak bertanggung jawab. Hal ini membuat para guru-guru SDN Grogol Utara 10 khawatir jika akan menggunakan aplikasi sekolah untuk menyimpan kedalam database, karena data dan informasi yang penting dan juga rahasia yang masih rentan terhadap pencurian dan juga penyalahgunaan oleh pihak tertentu bahkan dapat menimbulkan kerugian yang cukup besar. Dari masalah tersebut maka yang dibutuhkan adalah suatu metode yang dapat melindungi data dan informasi. Oleh karena itu, dibuatlah suatu aplikasi sekolah yang bisa melindungi dan mengamankan data dan informasi. Didalam perancangan aplikasi ini, penulis ingin membuat suatu metode dengan cara proses enkripsi. Penulis akan menggunakan 2 (dua) algoritma kriptografi yaitu RC4 dan BASE 64. Aplikasi yang dibuat ini menggunakan bahasa pemprograman PHP. Dengan aplikasi kriptografi dengan menggunakan metode RC4 dan BASE64 ini diharapkan informasi data yang disimpan kedalam aplikasi sekolah SDN Grogol Utara 10 akan aman dan tidak bocor kepada penyadap ataupun pihak yang tidak bertanggung jawab. Pada aplikasi ini, informasi yang di enkripsi adalah data siswa, data guru, mata pelajaran dan nilai. Berdasarkan implementasi ataupun pengujian program, dapat disimpulkan bahwa aplikasi ini mudah digunakan dan juga dapat melindungi kerahasiaan data ataupun informasi. Serta bermanfaat untuk guru sekolah SDN Grogol Utara 10 dalam menjalankan tugas pokok dan fungsi.

Kata Kunci : *Kriptografi, Keamanan Data, RC4, Base 64, SDN Grogol Utara*

1.1 PENDAHULUAN .

SDN GROGOL UTARA 10 beralamat di Jl. Kemandoran 1 rt.004/005 Grogol Utara, Kebayoran Lama, Jakarta Selatan. SDN GROGOL UTARA 10 mempunyai data siswa, guru dan penilaian siswa yang penting untuk disimpan ke dalam database sistem informasi sekolah. Jika data dan informasi tersebut disimpan tanpa ada satupun pengamanan yang baik, data dan informasi tersebut akan rentan terhadap pencurian atau pengubahan data oleh orang yang ingin mencuri atau mengubah data tesebut. Karena itu agar tidak ada orang asing dapat mengubah data yang sudah disimpan ataupun mencuri data yang ada, dibutuhkan sebuah metode yang dapat melindungi data dalam *record database*. Penerapan kriptografi dalam tugas akhir ini akan difokuskan bagaimana kriptografi bisa mengamankan data yang disimpan melalui sistem *database* menjadi aman sampai dengan data dibuka oleh orang yang berkepentingan.

Banyak teknik yang bisa digunakan untuk melindungi data-data tersebut diantaranya adalah steganografi dan juga kriptografi. Kedua teknik tersebut memiliki keuntungan masing-masing, kriptografi bertujuan untuk mengubah suatu pesan (*plaintext*) menjadi suatu pesan yang sulit dimengerti (*chipertext*). Namun kriptografi dapat menimbulkan kecurigaan pada orang yang membaca data terenkripsi, kecurigaan ini dapat memicu orang untuk memecahkan enkripsi tersebut.

Berkaitan dengan masalah tersebut penulis berkeinginan untuk membuat sebuah implementasi terhadap pengamanan data atau informasi ke *database*. Kriptografi yang digunakan adalah metode *RC4 dan BASE64*. Teknik algoritma ini dipilih karena sangat mudah digunakan. Algoritma *RC4 dan BASE64* yang dibangun ini dapat meng*enkripsi* dokumen (*plaintext*) dalam bentuk *record database*. Enkripsi yang dilakukan dengan cara menggunakan kunci tertentu, sehingga menghasilkan chipertext yang tidak dapat dimengerti ataupun sulit diingat. Ciphertext tersebut juga bisa dikembalikan seperti semula.

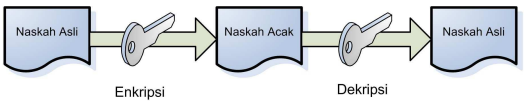
2.1 LANDASAN TEORI

2.2.1 Keamanan Komputer

Keaman komputer merupakan tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab (*John D. Howard*). Banyak yang belum mengetahui bahwa keamanan *(security)* merupakan sebuah komponen yang sangat penting. Bagi perancang dan pengelola sistem informasi, masalah kemanan sering menjadi masalah. Kriptografi juga sangat berperan dalam berkomunikasi, untuk melakukan enkripsi (pengacakan) data, lalu ditransaksikan dari awal ke akhir bahkan bisa melakukan dekripsi data yang diacak tersebut.

2.2.2 Kriptografi

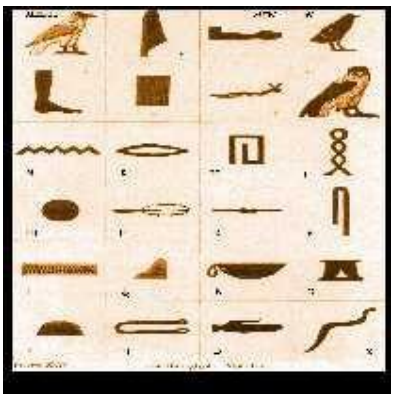
Kriptografi ialah ilmu yang mempunyai teknik enkripsi dimana "text asli" (plaintext) diacak menggunakan kunci enkripsi menjadi "text acak jadi sulit dibaca" (ciphertext) oleh orang yang tidak mempunyai kunci dekripsi. Dekripsi yang menggunakan kunci dekripsi bisa mendapatkan data asli, seperti yang ditunjukkan pada gambar 1.



Gambar 1: proses Enkripsi Dekripsi

2.2.3 Sejarah Kriptografi

Kriptografi berasal dari bahasa Yunani, "kryptós" artinya tersembunyi dan "gráphein" artinya tulisan. Julius Caesar telah menggunakan Kriptografi sejak zaman Romawi Kuno. Teknik ini juga disebut Caesar cipher untuk mengirim sebuah informasi secara rahasia, adapun teknik yang digunakan ini sangat tidak memadai untuk masa kini. Casanova menggunakan pengetahuan daripada kriptografi untuk mengelabui Madame d'Urfe (Casanova mengatakan ke Madame d'Urfe bahwa jin memberi tahukan kunci rahasia Madame d'Urfe pada Casanova, padahal Casanova sendiri yang berhasil memecahkan kunci rahasia didasarkan pengetahuan terhadap kriptografi), sehingga Casanova berhasil mengontrol kehidupan Madame d'Urfe.



Gambar 2: Hieroglyph

Pada tahun 4000 tahun lalu kriptografi telah dikenal oleh orang-orang Mesir lewat hieroglyph walaupun bukan dalam bentuk tulisan standard. Pada zaman Rumawi Kuno, Julius Caesar mengirimkan pesan rahasia kepada panglima perang di medan perang dengan mengubah semua susunan huruf alfabet dari: a b c d e f g h i j k l m n o p q r s t u v w x y z, menjadi : d e f g h i j k l m n o p q r s t u v w x y z a b c.

2.2.4 Kriptografi Modern

Kriptografi modern adalah suatu perbaikan daripada kriptografi klasik. Pada kriptogarfi modern ini juga terdapat macam-macam algoritma yang telah dimasukan untuk melindungi informasi yang telah dikirim melalui jaringan komputer.

2.3 RC4

2.3 Pengenalan Algoritma RC4

Menurut Dony Ariyus. RC4 juga merupakan jenis aliran kode yang berarti operasi enkripsinya dilakukan per huruf ataupun angka 1 byte untuk sekali operasi. Pada Algoritma kriptografi RC4 ini merupakan algoritma kunci simetris yang diciptakan oleh RSA Data Security Inc (RSADSI) yang merupakan bentuk dari stream chipper. Algoritma ini ditemukan tahun 1987 oleh Ronald Rivest dan juga menjadikannya simbol dari keamanan RSA.

2.4 BASE64

2.4 Cara Kerja Algoritma BASE64

Cara Kerja Algoritma Base 64 adalah Carilah kode ASCII dari masing-masing teks lalu cari bilangan biner 8 bit dari kode ASCII yang ada dan gabungkan 8 bit tadi menjadi 24 bit Kemudian, pecah 24 bit tadi menjadi 6 bit maka akan menghasilkan 4 pecahan masing-masing pecahan diubah diubah kedalam nilai decimal terakhir, jadikan nilai – nilai decimal yang akan menjadi indeks untuk memilih karakter penyusun daripada base64 dan juga maksimal adalah 63 atau indeks ke 64 ternyata didalam proses encoding juga terdapat sisa pembagi, maka tambahkan menjadi penggenap sisa karakter tersebut '='. Maka sering kali pada base64 akan muncul satu atau dua karakter '='.

2.5 Tinjauan Studi

Dibawah ini adalah penelitian yang telah dilakukan sebelumnya dengan topik mengenai enkripsi:

a. Penulis : (Hayati, Budiman & Sharif, 2019)
   Judul : Implementasi Algoritma RC4 dan MD5 untuk Menjamin *Confidentiality* dan *Integrity* pada *File* Teks
   Bentuk : Jurnal / ISSN : 2541 – 2019
   Terbitan : Teknik Informatika, Universitas Sumatera Utara.
b. Penulis : (Arintamy, Cahyani, & Mulyana, 2014)
   Judul: Analisa Algoritma RC4 Sebagai Metode Enkripsi WPA-SPK Pada Sistem Keamanan Jaringan Wireless LAN
   Bentuk : Jurnal / ISSN : 2355 - 9365 (2014)
   Terbitan : Fakultas Teknik Elektro, Universitas Telkom Bandung
c. Penulis : (Hakim, Khairil & Utama, 2014)
   Judul : Aplikasi Enkripsi Dan Dekripsi Data Menggunakan Algoritma RC4 Dengan Menggunakan Bahasa Pemograman PHP
   Bentuk : Jurnal / ISSN : 1858 - 2680
   Terbitan : Fakultas Ilmu Komputer, Universitas Daerhasen Bengkulu
d. Penulis : (Nugroho, Azmi & Arif, 2016)
   Judul : Aplikasi Keamanan Email Menggunakan Algoritma RC4
   Bentuk : Jurnal / ISSN : 1978-6603
   Terbitan : Jurusan Sistem Informasi, STMIK Triguna Dharma.

e. Penulis : (Dermawan & Alamsyah, 2014)
Judul : Penerapan Algoritma RC4 untuk Enkripsi dan Dekripsi SMS Berbasis Android
Bentuk : Jurnal / ISSN : 2407-1102
Terbitan : Fakultas Ilmu Komputer, SPHP-ILKOM

f. Penulis : (Indra Yatini B & Femi Dwi Astuti, 2015)
Judul : Analisis Performansi Kriptografi Menggunakan Algoritma Affine Cipher, Vigenere Cipher dan Base64
Bentuk : Jurnal / ISSN 2088 - 3676
Terbitan : Jurusan Teknik informatika, STMIK AKAKOM Yogyakarta.

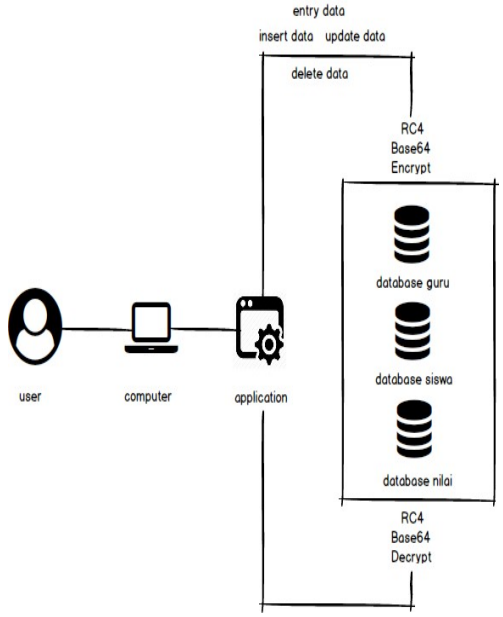
g. Penulis : (Siswanto, M. Anif & Windu Gata, 2018)
Judul : Penerapan Algoritma Kriptografi Tea dan Base64 Untuk Mengamankan Email
Bentuk : Jurnal / ISSN 2598-3245
Terbitan: Jurnal ELTIKOM

h. Penulis: (Mgs.Deny Ramadhan, Wiwik Andriani, Shinta Puspasari & Eka Puji Widiyanto, 2015)
Judul : Rancang Bangun Bangun Sistem Keamanan Data Dengan Menerapkan Modifikasi Penggabungan Algoritma
Bentuk : Jurnal / ISSN: 1978-1520
Terbitan : Program Studi Informatika, STMIK GI MDP, Palembang

3. ANALISIS MASALAH DAN PERANCANGAN SOLUSI

3.1 Arsitektur Sistem Aplikasi

Pada arsitektur sistem aplikasi kriptografi database di SDN Grogol Utara 10 ada beberapa tahap yaitu input data, lalu data dienkripsi ke database. Lalu proses dekripsi data yaitu di dekripsi sebelum proses output. dapat dilihat pada gambar 4.

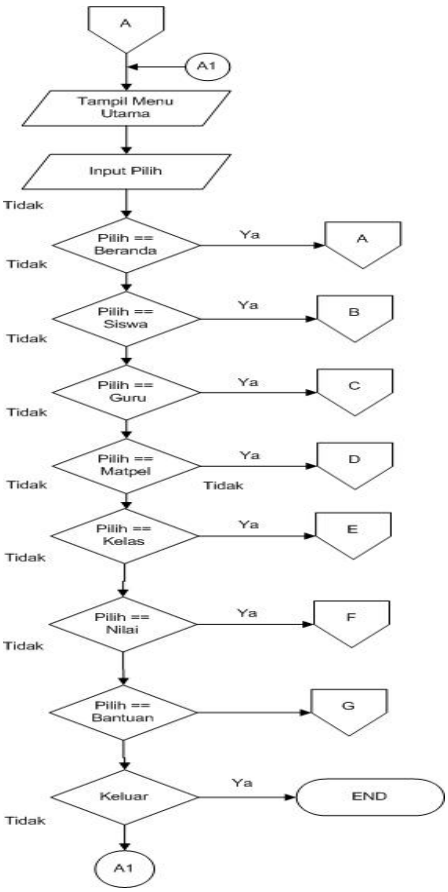


Gambar 4. Arsitektur Sistem Aplikasi

3.2 *Flowchart* Menu Utama

Gambar 5 merupakan *flowchart* menu utama ini terdapat lima menu diantaranya Beranda, Siswa, Guru, Mata Pelajaran, Nilai, Kelas, Bantuan, dan *Logout*.

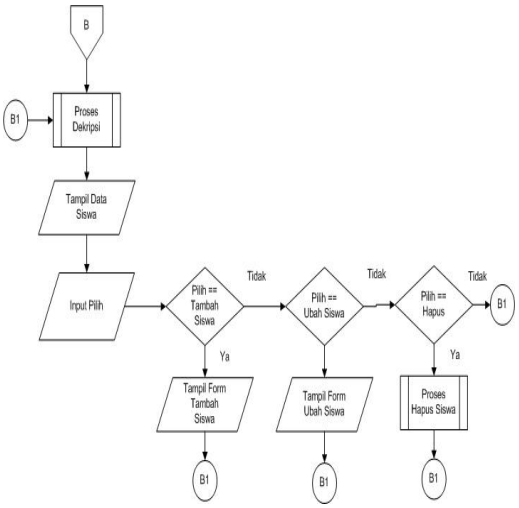
.



Gambar 5. Flowchart Menu Utama

3.3 *Flowchart* Siswa

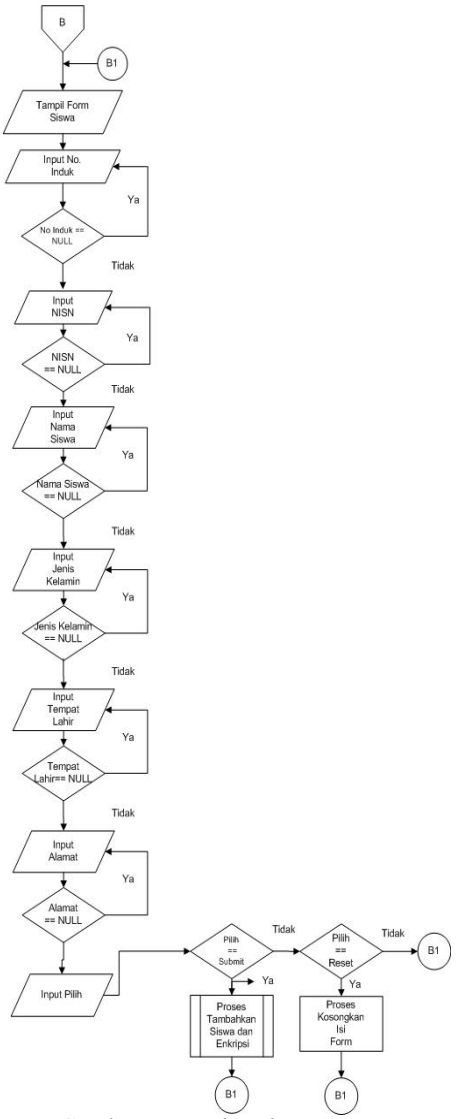
Gambar 6 merupakan *flowchart* siswa menjelaskan proses tampil siswa yang sudah didekripsi dari *database* untuk ditampilkan kedalam table data siswa.



Gambar 6. Flowchart Tampil Data Siswa

3.4 *Flowchart* Tambah Data Siswa

Gambar 7 menunjukkan flowchart tambah siswa

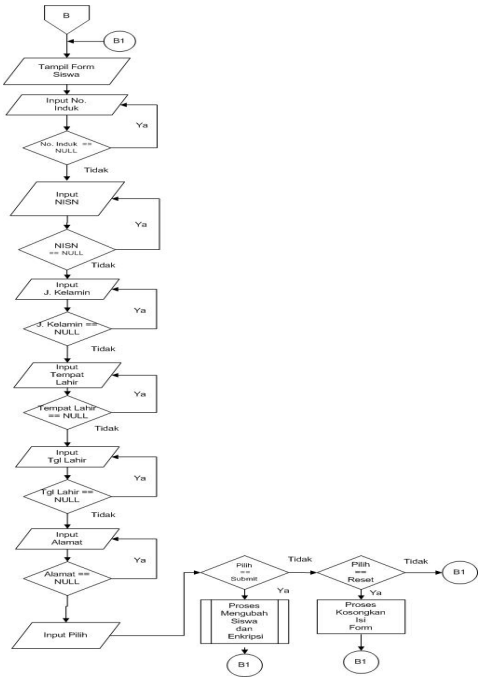


Gambar. 7 Flowchart Form Tambah Siswa

Flowchart Tambah Siswa ini merupakan alur jalannya proses dimana *admin user* menambahkan data Siswa kedalam database yang ingin di*enkrip*. Setelah admin *user* menklik tombol *submit,* terlebih dahulu *admin user* memasukan semua proses input agar bisa terjaga rahasianya.

3.5 *Flowchart* Ubah Data Siswa

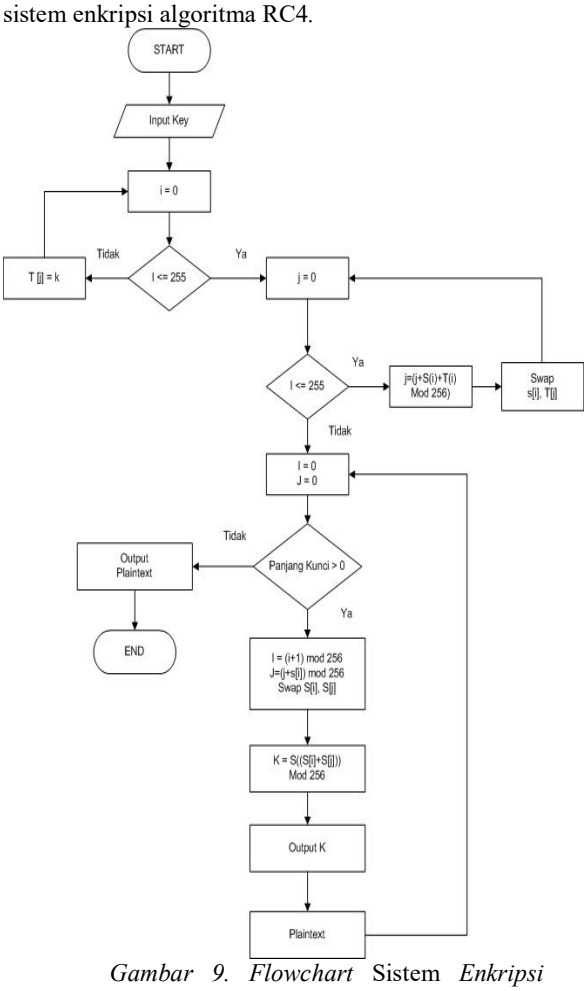
Flowchart Ubah Siswa ini merupakan alur jalannya proses dimana *admin user* mengubah data siswa kedalam database dan data siswa akan di*enkrip* kembali. Setelah admin *user* menklik tombol *submit,* data siswa akan masuk kedalam *database*. *Flowchart Form* siswa dapat dilihat pada Gambar dibawah ini.



Gambar 8. Flowchart Tampil Ubah Siswa

3.6 *Flowchart* Sistem *Enkripsi* Algoritma *RC4*

Pada gambar ini menjelaskan bagaimana proses sistem enkripsi algoritma RC4.

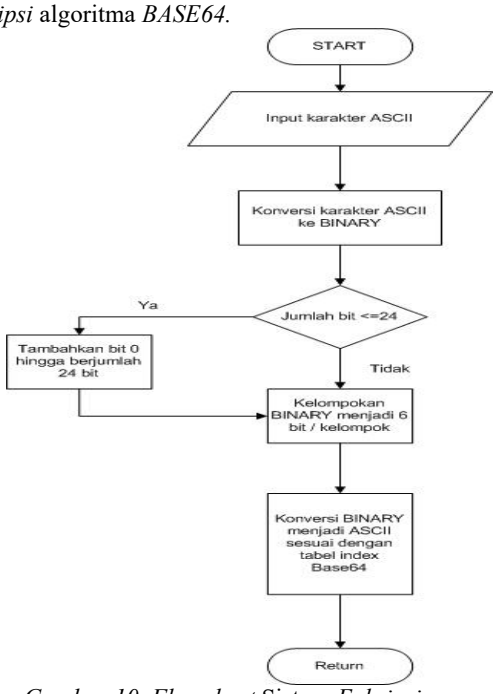


Gambar 9. Flowchart Sistem *Enkripsi*

Algoritma *RC4*

3.7 *Flowchart* Sistem *Enkripsi* Algoritma *BASE64*

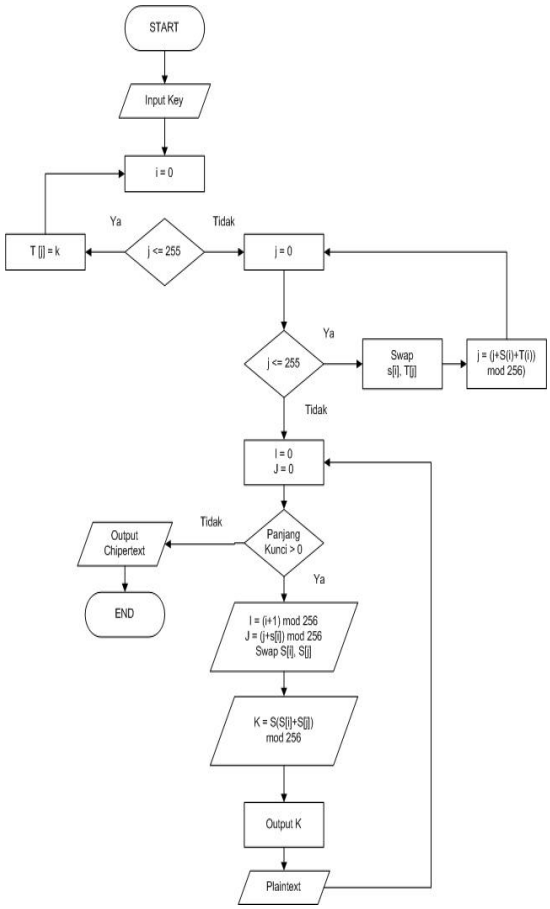
Flowchart ini menjelaskan bagaimana proses sistem *enkripsi* algoritma *BASE64.*



Gambar 10. Flowchart Sistem *Enkripsi* Algoritma *BASE64*

3.8 *Flowchart Dekripsi* Algoritma *RC4*

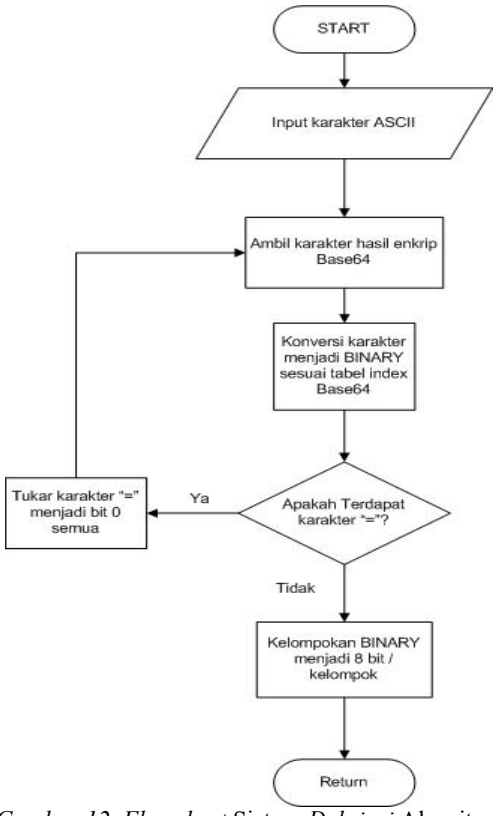
Pada gambar dibawah ini menjelaskan bagaimana proses *dekripsi* algoritma *RC4.*



Gambar 11. Flowchart Sistem *Dekripsi* Algoritma *RC4*

3.9 *Flowchart* Sistem *Dekripsi* Algoritma *BASE64*

Flowchart ini menjelaskan bagaimana proses sistem *dekripsi* algoritma *BASE64* .



Gambar 12. Flowchart Sistem *Dekripsi* Algoritma *BASE64*

4. IMPLEMENTASI DAN UJI COBA SOLUSI

4.4.1 Black Box

Pengujian metode black box adalah pengujian dari sisi fungsionalitas input/output pada suatu perangkat lunak.

Modul untuk Testing yang akan dilakukan dengan menguji : login, data siswa, data siswa, kelas, nilai.

Tabel. 1 : Metode Testing Black Box

No	Rancangan Proses	Hal yang di harapkan	Hasil	Keterangan
1	Mengisi Form Login	Masuk ke Halaman Utama	Sesuai	Jika di Input Benar
2	Klik Menu Siswa	Masuk ke Halaman List Data Siswa	Sesuai	Jika ke Halaman List Data Siswa
3	Klik Button Tambah Siswa	Masuk ke Halaman Form Tambah Data Siswa	Sesuai	Jika ke Halaman Form Tambah Data Siswa
4	Mengisi Form Tambah Siswa	Data Siswa Terenkripsi ke dalam Database	Sesuai	Jika di Input Benar
5	Klik Link Edit	Masuk ke Halaman Form Edit Data Siswa	Sesuai	Jika ke Halaman Form Edit Data Siswa
6	Mengisi Form Edit Siswa	Data Siswa dapat di Ubah dan Terenkripsi kembali ke Database	Sesuai	Jika di Input Benar
7	Klik Link Hapus	Data setelah di klik akan terhapus	Sesuai	Jika di Klik
8	Klik Menu Guru	Masuk ke Halaman List Data Guru	Sesuai	Jika ke Halaman List Data Guru
9	Klik Button Tambah Guru	Masuk ke Halaman Form Tambah Data Guru	Sesuai	Jika ke Halaman Form Tambah Data Guru
10	Mengisi Form Tambah Guru	Data Guru Terenkripsi ke dalam Database	Sesuai	Jika di Input Benar
11	Klik Link Edit	Masuk ke Halaman Form Edit Data Guru	Sesuai	Jika ke Halaman Form Edit Data Guru
12	Mengisi Form Edit Guru	Data Guru dapat di Ubah dan Terenkripsi kembali ke Database	Sesuai	Jika di Input Benar
13	Klik Link Hapus	Data setelah di klik akan terhapus	Sesuai	Jika di Klik
14	Klik Menu Kelas	Masuk ke Halaman List Data Kelas	Sesuai	Jika ke Halaman List Data Kelas
15	Klik Button Tambah Kelas	Masuk ke Halaman Form Tambah Data Kelas	Sesuai	Jika ke Halaman Form Tambah Data Kelas
16	Mengisi Form Tambah	Data Kelas Terenkripsi	Sesuai	Jika di Input Benar

4.4.2 Tabel Enkripsi

Tabel enkripsi ini, akan membahas proses enkripsi dari data siswa. Pengujiannya adalah data asli siswa sebelum di enkripsi.

Nama Siswa *(Plaintext)*	*Key Base 64* (Kunci Caesar Cipher)	Key RC4	Nama Siswa *(Ciphertext)*
Daffa Aditya	*bin2hex (Budi Luhur)*	htjls	mnwtN0hH9qIfhHUuZVUmoAl
Dafa Adriano	*bin2hex (Budi Luhur)*	xuzst	kT6y2VOqj4/xmtTDyhIeP94avpP
Arina Rachel Ayu Cherika	*bin2hex (Budi Luhur)*	dbgzv	z5b6Q68gbNkXtUE13J2FEixmkg=
Arif Prasetyo	*bin2hex (Budi Luhur)*	utdno	8tjsH6pm5NHfYqtfcyJMkL6xzJDWig==
Aqila Khairiyan	*bin2hex (Budi Luhur)*	jpffo	6z034rcBDgoqKdCrxnAKgfClig==
Alyia Siti Nutyiana	*bin2hex (Budi Luhur)*	syqst	sBAkHOXII1kMuIVWBj8
Almira Zaida Wulandari	*bin2hex (Budi Luhur)*	pdzej	IGZoNzFpujs3QcubNg==
Azila Auffania Nazwa	*bin2hex (Budi Luhur)*	pvsbk	UM4DCgktQ8wGV+ODWgnv8PcMZNe6tnhR
Ahmad Afriyan Saputra	*bin2hex (Budi Luhur)*	sbtel	OGyqnoMmoJ2ZyYk5

Tabel 2 : Tabel Hasil Enkripsi Data Siswa

4.4.2 Tabel Dekripsi

Didalam pengujian, akan dilakukan proses dekripsi. Pengujian tersebut yaitu data siswa setelah di*enkripsi* yang pada saatnya akan di*dekripsi* seperti nama siswa, *key*, menjadi data asli setelah dilakukan *dekripsi*.

Nama Siswa (*Ciphertext*)	*Key Base 64* (Kunci Caesar Cipher)	Key RC4	Nama Siswa (*Plaintext*)
mnwtN0hH9qIftiHUuZV UmoAl	*bin2hex (Budi Luhur)*	htjls	Daffa Aditya
kT6y2VOqj4/xmtTDyhI eP94avpP	*bin2hex (Budi Luhur)*	xurst	Dafa Adriano
z5b6Q68gbNkXtUE13J2 FEixmkg=	*bin2hex (Budi Luhur)*	dbgzv	Arina Rachel Ayu Cherika
8tjsH6pm5NHfYqtfcyJM kL6xrJDWig==	*bin2hex (Budi Luhur)*	utdno	Arif Prasetyo
6z034rcBDgoqKdCrxnA KgfCIg==	*bin2hex (Budi Luhur)*	jpffo	Aqila Khairiyan
sBAk1tOXI11kMuIVWB j8	*bin2hex (Budi Luhur)*	syqat	Alyia Siti Nutyiana
1GZoNzFpujs3QcubNg= =	*bin2hex (Budi Luhur)*	pdzej	Almira Zaida Wulandari
UM4DCgktQ8wGV+OD Wgnv8PcMZNe6tnhR	*bin2hex (Budi Luhur)*	pysbk	Azila Auffania Nazwa
OGyqnoMmoJ2ZyYk5	*bin2hex (Budi Luhur)*	sbtel	Ahmad Afriyan Saputra
gSIOS+SVJgTQreD2	*bin2hex (Budi Luhur)*	lmchd	Adira Putri Silvia

Tabel 4.3 : Tabel Hasil Dekripsi Data Siswa

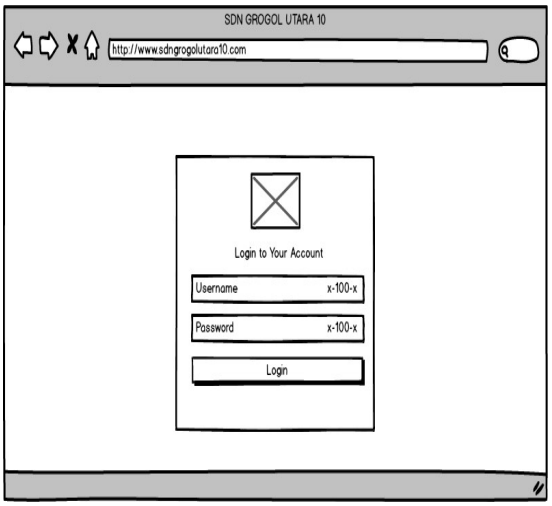
4.4.3 Rancangan Layar

Perancangan layar bertujuan untuk memberikan gambaran tentang aplikasi yang akan dibangun. Sehingga akan mempermudah dalam mengimplementasikan aplikasi serta akan memudahkan pembuatan aplikasi yang *user friendly.*

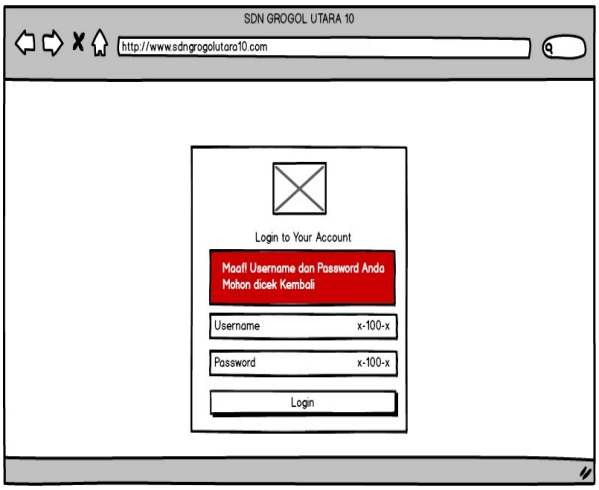
4.4.4 Rancangan Layar *Form* Login

Sebelum masuk ke halaman utama, maka sebaiknya login dengan mengetik username dan juga password dengan benar. Kalau login berhasil maka dapat masuk ke halaman utama. Jika tidak berhasil maka akan muncul pesan error.

.



Gambar 13. Rancangan Layar *Form* Login



Gambar 13. Rancamgan Layar *Form* Login salah

5. KESIMPULAN

Kesimpulan dari penelitian ini adalah :

a. Dengan adanya aplikasi sistem sekolah kriptografi database ini, data penting yang dimiliki oleh SDN GROGOL UTARA 10 dapat terjamin keamanan dan kerahasiannya.
b. Aplikasi yang telah di implementasikan agar bisa dipahami oleh *user*.
c. Aplikasi memiliki isi data sistem informasi siswa, guru, mata pelajaran, dan nilai kedalam *database* tersebut maka data tersebut otomatis telah terenkripsi.
d. Diimplementasikan menggunakan bahasa pemograman *PHP* dengan menggunakan algoritma *RC4* dan *Base 64* untuk *enkripsi* dan *dekripsi*

DAFTAR PUSTAKA

[1] Busran, M. P. (2012). Pengertian RC4. Padang: Jurnal Teknologi dan Informasi Pendidikan Vol. 5, No. 1 Maret 2012: 32-45.

[2] Hayati, B. &. (2015). Implementasi Algoritma RC4 dan MD5 untuk Menjamin Confidentiality dan Integrity pada File Teks, *Jurnal Teknik Informatika*.

[3] Kromodimoeljo. (2009). Proses Enkripsi dan Dekripsi, Depok.

[4] Kurniawan. (2014). Algoritma Simetris, Surabaya.

[5] Munir. (2009). Kriptografi Klasik. Penerbit Informatika, Bandung.

[6] Siregar, H. &. (2016). Pengertian Database. *Sekolah Tinggi Manajemen Informatika dan Ilmu Komputer Elrahma Yogyakarta*.

[7] Nugroho, A. &. (2016). Aplikasi Keamanan Email Menggunakan Algoritma RC4. *Jurnal Jurusan Sistem Informasi, STMIK Triguna Dharma*.

[8] Silalahi. (2015). *Scytale*. Retrieved from http://desijugul.blogspot.com/2015/04/algoritma-kriptografi-klasik.html, diakses tanggal 7 Februari 2019.

[9] Siswanto, M. A. (2018). Penerapan Algoritma Kriptografi Tea dan Base64 Untuk Mengamankan Email. *Jurnal ELTIKOM*.