Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

Perancangan Aplikasi Keamanan Data Customer Pada Online Shop Dengan Menggunakan Metode Kriptografi RSA (Rivest, Shamir, Adleman) Dan Caesar Cipher

M Jimi Hendra[*], Azanuddin[**], Sri Murniyanti[**]
[*] Program Studi Sistem Informasi, STMIK Triguna Dharma
[**] Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info
Article history:

Keyword:
Sistem Pendukung Keputusan, Weighted Product, Golongan Perumahan.

ABSTRACT

Online Shop merupakan proses pembelian barang/jasa oleh konsumen ke penjual realtime, tanpa pelayan, dan melalui internet (Ollie, 2008). Jual beli online di artikan sebagai jual beli barang dan jasa melalui media elektronik, khususnya melalui internet atau secara online.

Pada permasalahan yang dibahas, dapat menerapkan Perancangan Aplikasi Keamanan Data salah satunya ialah menggunakan algoritma Rivest Shamir Adleman(RSA) dan Caesar Chiper dalam mengamankan data customer olshop.

Hasil penelitian merupakan terciptanya sebuah aplikasi Pengamanan Data dengan Algoritma Rivest Shamir Adleman(RSA) dan Caesar Cipher yang dapat membantu owner dalam mengamankan data customernya yang membeli ke toko Jeje Olshop.

First Author
Nama : M Jimi Hendra
Program Studi : Sistem Informasi STMIK Triguna Dharma
Email : jimihendra11@gmail.com

1. PENDAHULUAN

Online Shop merupakan proses pembelian barang/jasa oleh konsumen ke penjual *realtime*, tanpa pelayan, dan melalui *internet* (Ollie, 2008). Jual beli *online* di artikan sebagai jual beli barang dan jasa melalui media elektronik, khususnya melalui *internet* atau secara *online* [1]. Penjual *online shop* dalam media sosial instagram memiliki register yang ditemui pada kolom komentar atau *caption* setiap mengunggah foto, Salah satu contoh adalah penjualan produk/barang secara online melalui internet seperti yang dilakukan *Lazada, Tokopedia, Buka Lapak, Blibli, Elevania, Shopee dll* [2].

Keunggulan belanja *online* dari pada belanja secara *offline* yaitu. Mudah karena dapat dilakukan dimana saja & kapan saja, melalui perangkat *computer* dimana saja yang terkoneksi dengan *internet*, termasuk dari perangkat *mobile* pribadi. Mudah karena tinggal masuk ke web, pilih produk, baca deskripsi produk, klik beli, pilih cara pembayaran, dan tunggu barang diantar, Murah alasan lain adalah belanja lewat *online* lebih murah [3].

Kriptografi adalah suatu teknik matematika yang berhubungan dengan aspek-aspek pengamanan informasi seperti data *confidentiality*, data *integrity* dan data *authentication*. *Cryptographic algorithm* adalah fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Terdapat dua fungsi yang saling berhubungan yaitu satu untuk enkripsi dan satu lagi untuk dekripsi.

Algoritma kriptografi Rivest Shamir Adleman (RSA) adalah algoritma untuk enkripsi kunci publik (*public-key encryption*). Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandatangani (*signing*) dan untuk enkripsi (*encryption*) dan salah satu penemuan besar pertama dalam kriptografi kunci publik [4]

Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

Berdasarkan masalah yang dihadapi, maka penulis mengangkat judul sebagai inti pembahasan dalam penelitian yaitu **"Perancangan Aplikasi Keamanan Data Customer Pada Online Shop Dengan Menggunakan Metode Kriptografi RSA(Rivest, Shamir, Adleman) Dan Caesar Cipher"**

2. KAJIAN PUSTAKA

2.1 Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi. Contoh algoritma kriptografi yang dapat dihandalkan adalah RSA, dimana RSA merupakan proses penyandian kunci asimetrik (*asymmetric key*). Proses perumusan RSA didasarkan pada *Teorema Euler*, sedemikian sehingga menghasilkan kunci umum dan kunci pribadi yang saling berkaitan [5].

2.2 Rivest Shamir Adleman Dan Caesar Cipher

Pada tahun 1977, Rivest, Shamir, dan Adleman merumuskan algoritma praktis yang menginplementasikan sistem kriptografi kunci publik disebut dengan sistem kriptografi RSA, (Rivesetal., 1983 dalam Sadikin, 2012:249). Meskipun pada tahun 1997 badan sandi Inggris mempublikasikan bahwa *Clifford Cock* telah merumuskan sistem algoritma RSA 3 tahun lebih dulu dari pada Rivest, Shamir dan Adleman.

Caesar Cipher adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet (Haryanto, Apriani and Sefyanto 2012). Pada *Caesar Cipher*, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah pergeseran huruf [6].

2.3 Algoritma Rivest Shamir Adleman Dan Caesar Cipher

Adapun algoritma penyelesaian metode RSA dan Caesar Cipher yaitu sebagai berikut:

1. Langkah Pertama : Menginput Plaintext.
   Menginputkan Kunci Publik dimana kunci tersebut nantinya akan diproses dan hasilnya akan menjadi cipherteks.

2. Langkah Kedua : Merubah cipherteks kembali menjadi Plaintext awal.

Algoritma Pembangkit Kunci RSA:

$n = p \times q$
$\phi(n) = (p-1) \times (q-1)$
$e \xleftarrow{R} Z_{\phi(n)}$ dengan $\gcd(e,\phi(n)) = 1$
$d = e^{-1}$ pada $Z_{\phi(n)}$
$K_{Publik} = (e,n)$, $K_{Privat} = d$

Keterangan:

p, q	: Adalah bilangan prima
n	: Adalah modulus yang digunakan
e	: Adalah eksponen public atau eksponen enkripsi
d	: Adalah eksponen pribadi atau eksponen dekripsi

Algoritma Kunci Caesar Cipher:

Pergeseran mungkin dalam jumlah berapa pun, sehingga algoritma Caesar umum adalah:

$C = E(k, p) = (p + k) \bmod 26$ (2)

Di mana k mengambil nilai dalam rentang 1 hingga 26. Untuk perhitungan Algoritma dekripsi sebagai berikut:

$p = D(k, C) = (C - k) \bmod 26$ (3)

3. METODOLOGI PENELITIAN

Untuk mempermudah penelitian ini dalam penentuan metodologi adalah hal terpenting, karena metode penelitian merupakan prosedur atau langkah-langkah dalam mendapatkan pengetahuan yang digunakan seseorang dalam melakukan kegiatan penelitian, jadi metode penelitian merupakan cara sistematis untuk menyusun ilmu pengetahuan dalam memecahkan masalah penelitian dan dapat dipahami sebagai ilmu yang mempelajari bagaimana penelitian dilakukan secara ilmiah.

Didalam metode penelitian ini terdapat beberapa langkah yaitu *data collecting* atau pengumpulan data dan *studi literatur*. Penjelasannya adalah sebagai berikut:

1. *Data Collecting*

Dalam teknik pengumpulan data terdapat beberapa hal yang harus dilakukan di antaranya yaitu sebagai berikut:

a. Observasi

Observasi merupakan teknik pengumpulan data, metode ini dipakai untuk mengumpulkan keterangan atau data dengan cara mengamati dan mencatat fenomena-fenomena yang terjadi pada sasaran pengamatan.

b. Wawancara

Wawancara merupakan metode pengumpulan data, dilakukan dengan cara interaksi dengan komunikasi interpersonal yang melibatkan dua orang atau lebih dalam sebuah percakapan yang berbentuk tanya jawab.

2. *Studi Literatur*

Dalam *studi literartur*, tahap ini dilakukan cara pengumpulan data mengunakan jurnal-jurnal baik jurnal internasional, jurnal nasional, jurnal lokal maupun buku sebagai sumber referensi.

3.1 Metode Perancangan Sistem

Metode penelitian yang diterapkan pada penelitian ini adalah dengan pengembangan metode *waterfall*. Metode *waterfall* merupakan model pengembang sistem informasi yang menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau terurut dimulai dari analisis, desain, pengodean, pengujian, dan tahap pendukung (*support*). Berikut ini adalah fase yang dilakukan dalam penelitian ini yaitu:

1. Analisis Kebutuhan Perangkat Lunak.
2. Desain.
3. Pembuat Kode Program.
4. Pengujian.
5. Pendukung (*support*) atau pemeliharaan (*maintenance*).

3.2 Algoritma Sistem

Algoritma Algoritma Sistem adalah sebuah prosedur yang melakukan proses pengamanan dalam mengamankan data *online shop* sesuai dengan data customer. Adapun algoritma sistem dalam permasalahan ini menggunakan metode Rivest Shamir Adleman dan Caesar Cipher, berikut ini adalah langkah-langkah penyelesaian metode Rivest Shamir Adleman dan Caesar Cipher:

1. Menginput Plaintext.
2. Menginput Kunci Publik.
3. Memilih Data cutomer.
4. Menginput Kunci Private.
5. Mendekripsi data customer.

3.2.1 Penyelesaian

Berikut ini adalah data *customer* yang didapat dari Jeje Olshop Medan, yang akan diamankan. Dalam pengujiannya, sebagai contoh data yang digunakan sebagai sampel dalam penelitian ini yaitu sebagai berikut:

Tabel 3.2 Sampel Data *Customer* di Jeje Olshop Medan

No	Id	Nama	Alamat	Email	No-Telp	Nama Barang	Harga
1	101	Nazmi mayy sarah	Asrto 2000 SM. Raja	Sarahnazmi22@gmail.com	816020384430	Mouza 2, Daster kerut 1	Rp.345.000

3.3.3 Penyelesaian Masalah Dengan Algoritma RSA Dan Caesar Cipher

Sesuai dengan referensi yang telah dipaparkan pada bab sebelumnya, berikut ini adalah langkah-langkah penyelesaiannya yaitu:

3.3.3.1 Proses Enkripsi Algoritma Rivest Shamir Adleman (RSA)

Proses enkripsi algoritma Rivest Shamir Adleman (RSA), yaitu sebagai berikut:

4. Pilihlah bilangan prima dengan sembarang, dalam pemilihan ini, di pilih nilai prima (p) = 13 dan nilai (q) = 17.
5. Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkalian $n = p * q$

$n = 13 * 17 = 221$

6. Hitung (*phi*) $n = (p-1)$ (q-1)

*n= 12 * 16 = 192*

7. Pilih nilai *e* dengan syarat *e* > 1 dan *greatest comman divisior* (*e,192*) = 1
   Nilai *e* yang di ambil adalah 5.
8. Sehingga *de = 1* (mod 192) dan *d* < 192

*d * 5 = 1 mod 192*
*d * 5 mod 192 =1*
d = 77
Bukti:
77 * 5 mod 192 = 1
Sehingga pasangan kunci yang didapat adalah :
Kunci enkripsi (*public key*) (*e,n*) = (5, 221) dan
Kunci dekripsi (*private key*) (*d,n*) = (77, 221)

Pertama yang harus dilakukan adalah merubah *plaintext* menjadi format ASCII, berikut ini adalah penyelesaiannya:

Plaintext : A u t o 2 0 0 0 S M . R a j a
ASCII : 65 117 116 111 32 50 48 48 48 32 83 77 46 32 83 97 106 97

Kemudian *p* dipecah menjadi tiap karakter *plaintext*. Berikut ini adalah tebel *Pi*:

Tabel 3.3 Karakter *Pi* dan Kode ASCII untuk *Plaintext* Auto 2000 SM. Raja

Pi	Keterangan	Kode ASCII
P1	A	65
P2	U	117
P3	T	116
P4	O	111
P5	Spasi	32
P6	2	50
P7	0	48
P8	0	48
P9	0	48
P10	spasi	32
P11	S	83
P12	M	77
P13	.	46
P14	Spasi	32
P15	R	83
P16	A	97

Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

Pi	Keterangan	Kode ASCII
P17	J	106
P18	A	97

Setelah dibagi perkarakater, selanjutnya dienkripsi dengan rumus *Ci = Pi^e mod n*, yaitu sebagai berikut:

C1 = 65^5 mod 221 = 182
C2 = 117^5 mod 221= 104
C3 =116^5 mod 221 = 12
C4 = 111^5 mod 221= 76
C5 = 32^5 mod 221 = 2
C6 = 50^5 mod 221 = 33
C7 = 48^5 mod 221 = 29
C8 = 48^5 mod 221 = 29
C9 = 48^5 mod 221 = 29
C10 = 32^5 mod 221 = 2
C11 = 83^5 mod 221 = 70
C12 = 77^5 mod 221 = 25
C13 = 46^5 mod 221 = 37
C14 = 32^5 mod 221 = 2
C15 = 83^5 mod 221 = 114
C16 = 97^5 mod 221 = 54
C17 = 106^5 mod 221= 123
C18 = 97^5 mod 221 = 54

Tabel 3.4 Karakter *Ci* dan Kode untuk *Plaintext* Auto 2000 SM. Raja yang telah dienkripsi dengan algoritma Rivest Shamir Adleman (RSA)

Ci	Kode
C1	182
C2	104
C3	12
C4	76
C5	2
C6	33
C7	29
C8	29
C9	29
C10	2
C11	70

Ci	Kode
C12	25
C13	37
C14	2
C15	114
C16	54
C17	123
C18	54

Maka, setelah dienkripsi hasilnya yaitu, 182, 104, 12, 76, 2, 33, 29, 29, 29, 2, 70, 25, 37, 2, 114, 54, 123, 54.

3.3.3.2 Proses Enkripsi Algoritma Caesar Cipher

Untuk mengenkripsi dangan Caesar Cipher cukup dengan penjumlahan dan modulus seperti berikut.

Ci = (Ci+k) mod n

Setelah dienkripsi dengan algoritma RSA, selanjutnya di enkripsi menggunakan rumus Caesar Cipher Ci = (Ci+k) mod n dengan k =10, yaitu sebagai berikut:

C1 = 182+10 mod 221 = 192
C2 = 104+10 mod 221 = 114
C3 =12+10 mod 221 = 22
C4 = 76+10 mod 221 = 86
C5 = 2+10 mod 221 = 12
C6 = 33+10 mod 221 = 43
C7 = 29+10 mod 221 = 39
C8 = 29+10 mod 221 = 39
C9 = 29+10 mod 221 = 39
C10 = 2+10 mod 221 = 12
C11 = 70+10 mod 221 = 80
C12 = 25+10 mod 221 = 35
C13 = 37+10 mod 221 = 47
C14 = 2+10 mod 221 = 12
C15 = 114+10 mod 221 = 124
C16 = 54+10 mod 221 = 64
C17 = 123+10 mod 221 = 133
C18 = 54+10 mod 221 = 65

Tabel 3.5 Karakter *Ci* dan Kode untuk *Plaintext* Auto 2000 SM. Raja yang telah dienkripsi dengan algoritma Caesar Cipher

Ci	Kode	*Char*
C1	192	À
C2	114	r
C3	22	

Ci	Kode	*Char*
C4	86	V
C5	12	‡
C6	43	+
C7	39	‘
C8	39	‘
C9	39	‘
C10	12	‡
C11	80	p
C12	35	#
C13	47	/
C14	12	‡
C15	124	|
C16	64	@
C17	133	...
C18	64	@

Maka, setelah dienkripsi hasilnya yaitu, 192, 114, 22, 86, 12, 43, 39, 39, 39, 12, 80, 35, 47, 12, 124, 64, 133, 64.

3.3.3.3 Proses Dekripsi Algoritma Caesar Cipher

Proses dekripsi adalah proses untuk mengembalikan ke bentuk semula (*plaintext*), setelah *chipertext* dari kata Auto 2000 SM. Raja didapat. Untuk merubah kembali menjadi *plaintext* awalnya kita akan melakukan dekripsi menggunakan algoritma Caesar Cipher dengan rumus *Ci*= (*Ci-k*) mod *n* , dimana k = 10. Berikut ini adalah penyelesaiannya:

C1 = 192-10 mod 221 = 182
C2 = 114-10 mod 221 = 104
C3 =22-10 mod 221 = 12
C4 = 86-10 mod 221 = 76
C5 = 12-10 mod 221 = 2
C6 = 43-10 mod 221 = 33
C7 = 39-10 mod 221 = 29
C8 = 39-10 mod 221 = 29
C9 = 39-10 mod 221 = 29
C10 = 12-10 mod 221 = 2
C11 = 80-10 mod 221 = 70
C12 = 35-10 mod 221 = 25
C13 = 47 -10 mod 221 = 37
C14 = 12-10 mod 221 = 2
C15 = 124-10 mod 221 = 114

C16 = 64-10 mod 221 = 54
C17 = 133-10 mod 221 = 123
C18 = 64-10 mod 221 = 54

Maka, setelah didekripsi hasilnya yaitu, 182, 104, 12, 76, 2, 33, 29, 29, 29, 2, 70, 25, 37, 2, 114, 54, 123, 54.

3.3.3.4 Proses Dekripsi Algoritma Rivest Shamir Adleman (RSA)

Setelah didekripsi dengan algoritma Caesar Cipher, selanjutnya didekripsi kembali menggunakan algoritma Rivest Shamir Adleman (RSA) dengan rumus Pi = *Ci^d* mod n, yaitu sebagai berikut:

P1 = 182^77 mod 221 = 65
P2 = 104^77 mod 221 = 117
P3 = 12^77 mod 221 = 116
P4 = 76^77 mod 221 = 111
P5 = 2^77 mod 221 = 32
P6 = 33^77 mod 221 = 50
P7 = 29^77 mod 221 = 48
P8 = 29^77 mod 221 = 48
P9 = 29^77 mod 221 = 48
P10 = 2^77 mod 221 = 32
P11 = 70^77 mod 221 = 83
P12 = 25^77 mod 221 = 77
P13 = *37*^77 mod 221 = 46
P14 = 2^77 mod 221 = 32
P15 = 114^77 mod 221 = 83
P16 = 54^77 mod 221 = 97
P17 = 123^77 mod 221 = 106
P18 = 54^77 mod 221 = 97

Maka, setelah didekripsi hasilnya yaitu, 65, 117, 116, 111, 32, 50, 48, 48, 48, 32, 83, 77, 46, 32, 83, 97, 106, 97 dalam karakter ASCII adalah:

ASCII : 65 117 116 111 32 50 48 48 48 32 83 77 46 32 83 97 106 97
Karakter : A u t o 2 0 0 0 S M . R a j a

4. PEMODELAN SISTEM DAN PERANCANGAN

Pemodelan merupakan suatu rencana atau rancangan yang menjelaskan mengenai suatu objek yang akan dibuat. Sedangkan sistem adalah suatu jaringan kerja yang saling berhubungan satu dengan yang lainnya dalam melakukan kegiatan untuk mencapai suatu tujuan. Dari kedua defenisi tersebut dapat disimpulkan bahwa pemodelan sistem merupakan suatu rancangan dalam membangun objek atau pola dari suatu sistem secara menyeluruh agar memudahkan pemahaman dari informasi yang dibutuhkan.

Berikut ini adalah penjelasan mengenai beberapa rancangan yang terdapat pada sistem berupa *use case diagram, activity diagram, dan class diagram*.

1. *Use Case Diagram*
   Use case diagram adalah pemodelan yang menggambarkan peranan pengguna pada sebuah sistem.
2. *Activity Diagram*
   Activity diagram merupakan gambaran aliran kerja dari menu menu yang terdapat pada sebuah sistem.
3. *Class Diagram*
   Class diagram merupakan gambaran aliran kerja pada struktur – struktur dalam membangun sebuah sistem.

5. PENGUJIAN DAN IMPLEMENTASI

Pengujian sistem merupakan kegiatan akhir dari penerapan sistem, dimana sistem akan mengoperasikan secara menyeluruh menggunakan metode *Weighted Product.* Sebelum sistem digunakan, sistem harus diuji terlebih dahulu agar tidak adanya kendala yang muncul pada saat digunakan. Dalam pengujian program sistem pendukung keputusan untuk menentukan golongan perumahan membutuhkan 2 (dua) buah perangkat yaitu perangkat lunak (*Software*) dan perangkat keras (*Hardware*). Adapun perangkat lunak software dan perangkat keras hardware yang dibutuhkan yaitu sebagai berikut:

1. Perangkat Lunak (*Software)*

Perangkat Lunak (*Software*) yaitu merupakan program yang berisikan instruksi dalam pengoperasian komputer. Adapun perangkat Lunak yang dibutuhkan adalah sebagai berikut:

a. Sistem Operasi *Windows 7, Windows 8, Windows 10* atau sejenisnya.
b. *Microsoft Visual Studio* 2010.

c. *Microsoft Acces* 2007.
d. *Crystal Report 8.5*
2. Perangkat Keras (*Hardware)*

Sistem yang terkomputerisasi ini dapat dijalankan apabila telah dilakukan beberapa hal yaitu proses instalasi sudah dilakukan serta *hardware* yang mendukung dalam menjalankan program ini telah dipersiapkan. Spesifikasi *hardware* yang digunakan untuk mengimplementasikan sistem agar berjalan dengan baik adalah sebagai berikut:

a. *Processor* Minimal *Intel Dual Core Processor.*
b. RAM *(Random Access Memory)* minimal 1 Gb.
c. *Keyboard.*
d. *Mouse.*
e. *Harddisk* minimal 100 Gb.

5.1 Implementasi Sistem

1. *Form Login*

Form Login digunakan untuk mengamankan sistem dari *user-user* yang tidak bertanggung jawab sebelum masuk ke Menu Utama. Berikut adalah tampilan *Form Login* :

Gambar 1 *Form Login*

Berikut keterangan pada gambar 1 *Form Login* :

a. Tombol login digunakan untuk mem-validasikan *username* dan *password* yang telah kita isi pada kotak teks yang disediakan.
b. Tombol Batal digunakan ketika kita batal melakukan *login* dan akan keluar dari sistem.
c. Link masuk sebagai pengunjung digunakan apa bila pengunjung ingin mencari rekomendasi terbaik untuknya.

2. *Form* Menu Utama

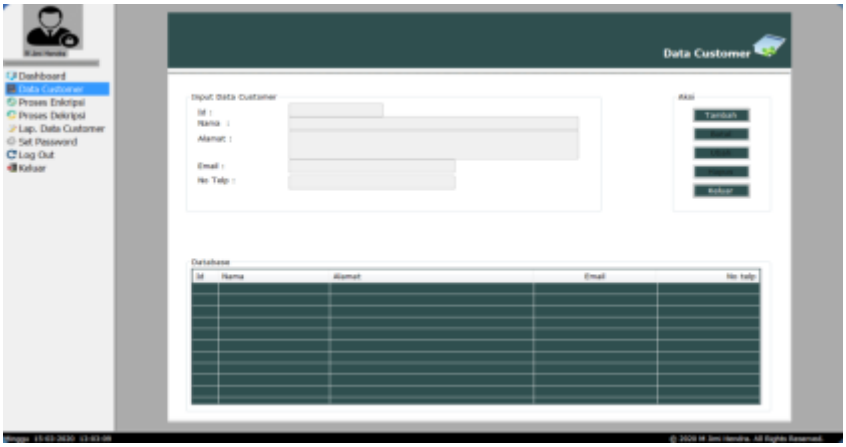
Form Menu Utama digunakan sebagai penghubung untuk *Form* Data *Customer*, *Form* Proses *Enkripsi*, *Form Dekripsi*, dan *Form* Laporan. Selain itu, ada beberapa menu lainnya salah satunya ada menu *Keluar* bertujuan untuk mengakhiri program secara keseluruhan.

Gambar.2 *Form* Menu Utama

3. *Form* Data *Customer*

Form Data *Customer* adalah *form* yang berfungsi untuk mengelola data Alternatif tentang *Smartphone* dan akan diolah dengan Metode Rivest Shamir Adleman dan Caesar Cipher. Berikut adalah tampilan hasil dari form data *Customer*.

Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475



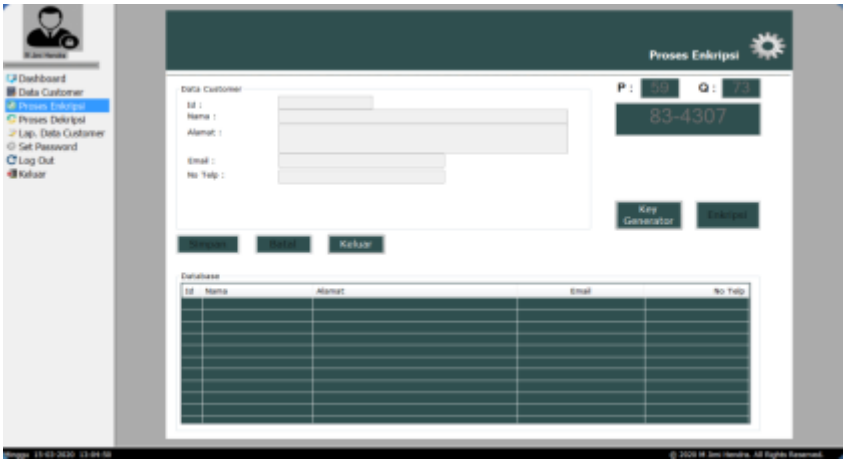
Gambar 3 *Form* Data *Customer*

Berikut keterangan pada gambar 3 *form* Data *Customer*:

a. Tombol simpan digunakan ketika seluruh kotak teks telah terisi dan data dari kotak teks tersebut akan disimpan.
b. Tombol ubah digunakan untuk mengubah data yang telah tersimpan sebelumnya.
c. Tombol hapus digunakan untuk menghapus data yang terpilih pada daftar data yang ada.
d. Tombol keluar digunakan untuk keluar dari form.

4. *Form* Enkripsi

Form Enkripsi adalah *Form* yang digunakan untuk Mengamankan data customer. Berikut adalah tampilan form Enkripsi:



Gambar 4 *Form* Enkripsi

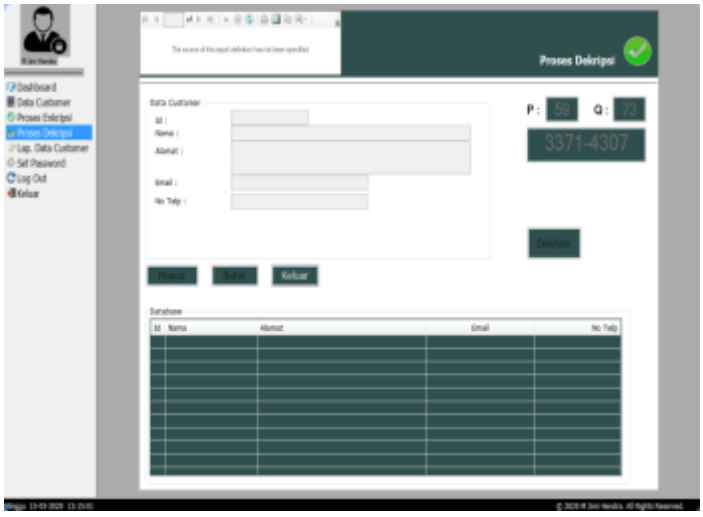
Berikut keterangan pada gambar 4 *form* Enkripsi:

a. Tombol Enkripsi digunakan untuk mengamankan data *customer* yang ada dengan menggunakan Algoritma Rivest Shamir Adleman dan Caesar Cipher.
b. Tombol key generator untuk mencari generator kunci yang lain.
c. Tombol Cetak laporan digunakan untuk menampilkan laporan hasil enkripsi

5. *Form* Dekripsi

Form Dekripsi adalah *Form* yang digunakan untuk Mengubah data customer kembali seperti semula. Berikut adalah tampilan form Dekripsi:

Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475



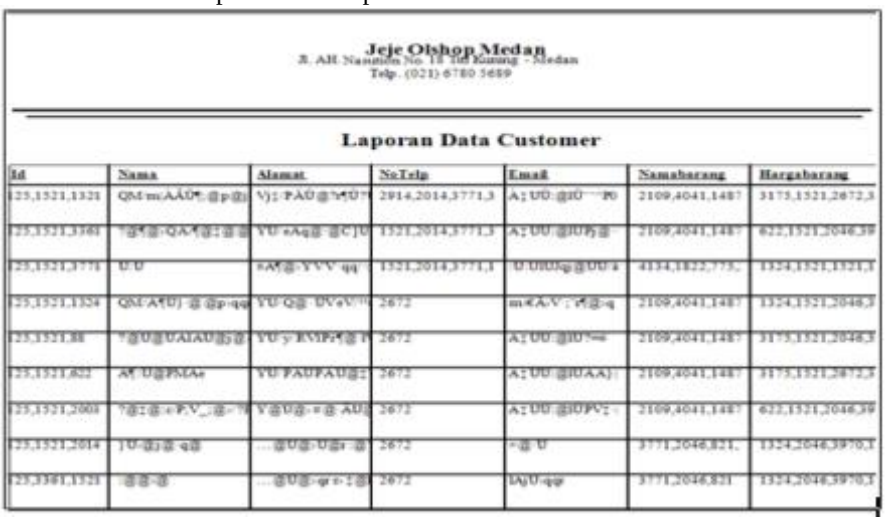
Gambar 5 *Form* Dekripsi

Berikut keterangan pada gambar 5 *form* Enkripsi:

a. Tombol Dekripsi digunakan untuk mengamankan data *customer* yang ada dengan menggunakan Algoritma Rivest Shamir Adleman dan Caesar Cipher.
b. Tombol key generator untuk mencari generator kunci yang lain.
c. Tombol Cetak laporan digunakan untuk menampilkan laporan hasil dekripsi

6. *Form* Laporan

Form Laporan adalah *Form* yang digunakan untuk menampilkan hasil Enkripsi Data berdasarkan metode Rivest Shamir Adleman. Berikut adalah tampilan form Laporan:



Gambar 6 *Form* Laporan

5.2 Kelebihan dan Kelemahan Sistem

Setelah melakukan proses penerapan dan pengujian terhadap sistem, algoritma Rivest Shamir Adleman dan Caesar Cipher ini mempunyai beberapa kelebihan dan kelemahan terhadap sistemnya, dimana sistem ini masih memerlukan pengembangan secara bertahap. Berikut kelebihan dan kelemahan dari sistem ini adalah :

a. Kelebihan Sistem
   a. Dapat mengamankan data dalam database dengan sistem pengamanan data yang cukup rumit.
   b. Proses pengamanan data yang rumit, dapat diubah menjadi sederhana dan spesifik.
   c. Aplikasi pengamanan data ini dapat membantu pengguna atau pihak Jeje Olshop untuk lebih mudah dalam mengamankan data *customer* olshop.
   d. Aplikasi yang telah dibangun ini dapat digunakan pada perusahaan lain karena fungsinya untuk mengamankan *database* yang penting.

1. Kelemahan Sistem
   a. Aplikasi pengamanan data yang telah dibangun ini hanyalah membahas tentang pengamanan data pada *database*.

b. Pada sistem ini belum memiliki fasilitas *backup* data, apabila data hilang atau terhapus maka datanya tidak dapat dikembalikan kedalam bentuk semula.
c. Dalam proses pengamanan data masih berbasis desktop sehingga dalam proses mengakses data cukup sulit untuk diakses pihak jeje olshop.

6. KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan penelitian yang telah dilalui dalam tahap perancangan dan evaluasi kriptografi dalam mengamankan data *customer* pada Jeje Olshop dengan menggunakan algoritma Rivest Shamir Adleman dan Caesar Cipher maka dapat disimpulkan bahwa:

1. Untuk mengamankan data *customer* Jeje Olshop medan yang bersifat rahasia akan diamankan menggunakan algoritma kriptografi Rivest Shamir Adleman dan Caesar Cipher.
2. Algoritma Rivest Shamir Adleman(RSA) dan Caesar Cipher digunakan sebagai sistem dalam pengamanan data yang merupakan algoritma yang cukup rumit dalam perhitungannya untuk mengamankan data yang cukup banyak sehingga dapat mengurangi resiko dalam penyalahgunaan data *customer* dan dapat mengoptimalkan dalam pengamanan data untuk mengamankan data *customer* pada Jeje Olshop.
3. Dengan cara merancang sistem aplikasi yang dapat digunakan dalam mengamankan data *customer* olshop dan mengenkripsi data menjadi karakter sehingga dapat mengamankan data dengan maksimal dan baik.

6.2 Saran

Adapun saran-saran yang dapat disampaikan kepada pembaca dan kepada seluruh pihak yang berkaitan dengan perancangan sistem ini, yaitu:

1. Diharapkan dalam penelitian yang selanjutnya dapat dikembangkan dengan menggabungkan algoritma yang lain sehingga dapat meningkatkan kinerja sistem.
2. Kepada *owner* Jeje Olshop yang akan menggunakan sistem ini harus diberikan pelatihan untuk pengoperasiannya. Hal ini disampaikan agar penggunaan sistem ini dapat lebih maksimal dan menghindari kesalahan yang tidak diinginkan.
3. Sistem ini masih dibuat hanya untuk Jeje Olshop, disarankan agar sistem ini juga dapat di gunakan untuk perusahaan lainnya.

UCAPAN TERIMA KASIH

Pada kesempatan ini saya ucapkan terimakasih kepada Bapak, Ibu dan keluarga saya atas segala doa, semangat dan motivasinya. Selain itu, terimakasih sebesar-besarnya kepada semua pihak yang telah membantu untuk menyelesaikan penulisan skripsi ini, yaitu :

1. Bapak Rudi Gunawan, SE, M.Si, Selaku Ketua STMIK Triguna Dharma Medan.
2. Bapak Dr. Zulfian Azmi, ST, M.Kom Selaku Wakil Ketua I Bidang Akademik STMIK Triguna Dharma Medan.
3. Bapak Marsono. S.Kom, M.Kom, Selaku Ketua Program Studi Sistem Informasi STMIK Triguna Dharma Medan.
4. Bapak Azanuddin, S.Kom, M.Kom selaku Dosen Pembimbing I yang membimbing dan menyediakan waktu selama ini.
5. Ibu Sri Murniyanti, SS., MM selaku Dosen Pembimbing II yang membimbing dan menyediakan waktu selama ini.
6. Seluruh Dosen, Staff dan Pegawai STMIK Triguna Dharma.
7. Terimakasi juga disampaikan kepada Jeje Olshop Medan yang telah mengizinkan melakukan penelitian dan memberikan data yang benar sehingga skripsi ini dapat terselesaikan dengan baik.

Akhir kata saya ucapkan rasa terima kasih kepada semua pihak yang terlibat dalam penyelesaian skripsi ini Skripsi ini masih sangat jauh dari sempurna. Oleh karena itu, diharapkan saran dan kritik yang sifatnya membangun dari para pembaca demi kesempurnaan skripsi ini.

REFERENSI

[1] "Analisis Faktor-Faktor Yang Mempengaruhi Keputusan Membeli Di Online Shop Mahasiswa Jurusan Pendidikan Ekonomi Angkatan Tahun 2012," vol. 9, 2017.

[2] "Bisnis Jual Beli Online (Online Shop) Dalam Hukum Islam Dan Hukum Negara," *Tira Nur Fitria*, vol. 3, p. 4, Maret 2017.

[3] "Analisis Faktor-Faktor Yang Mempengaruhi Keputusan Membeli Di Online Shop Mahasiswa Jurusan Pendidikan Ekonomi Angkatan Tahun 2012," vol. 9, 2017.

[4] "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," Yusuf Anshori, vol. 18, Mei 2019.

[5] "Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma Rsa Dengan Metode Waterfall Berbasis Java," *Rudi Firmansyah*, vol. 4, p. 1, 2019.

[6] "Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher Dan Advance Encryption Standard (Aes) Untuk File Teks," Aji Fitrah Marisman, vol. 19, p. 1, Desember 2015.

Data Diri

Nama	: M Jimi Hendra
Tempat/Tanggal Lahir	: Medan, 14 November 1997
Jenis Kelamin	: Laki Laki
Agama	: Islam
Status	: Belum Menikah
Pendidikan Terakhir	: Sekolah Menengah Kejuruan
Kewarganegaraan	: Indonesia
E-mail	: jimihendra11@gmail.com

Pendidikan Formal

1. Tahun 2004 - 2010	: SD Swasta Pembangunan Tg. Morawa
2. Tahun 2010 -2013	: SMP Swasta Bersubsidi Tg. Morawa
Tahun 2013 -2016	: SMK Dwi Tunggal Tg. Morawa

Azanuddin, S.Kom., M.Kom
Beliau merupakan dosen pengajar tetap di STMIK Triguna Dharma.

Sri Murniyanti, SS., MM
Beliau merupakan dosen pengajar tetap di STMIK Triguna Dharma.