Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Oct 2022, V (3): 664 – 670 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

PENGAMANAN DATA PENJUALAN DENGAN KRIPTOGRAFI ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) PAD A TOKO BAJU FAMILY

Karina Andriani[1], B.Herawan Hayadi[2]
Universitas Potensi Utama, Medan
e-mail: andrianikarina@gmail.com[1] , b.herawan.hayadi @gmail.com[2]

Abstract: *The development of computer technology at this time has a major impact in the delivery of information, while data security is one of the most important aspects in today's information systems. The family clothing store uses computer technology to process sales transactions so that every transaction made is stored in the form of sales data. In the problems discussed, by implementing Data Security Application Design, one of them is by using the RSA (Rivest Shamir Adleman) algorithm in securing sales data. By securing sales data, it aims to assist employees in securing their sales data. The result of the research is the creation of a Data Security application with the RSA Algorithm (Rivest Shamir Adleman) which can assist employees in securing sales data at the Family Clothing Store.*

Keywords: *Cryptography, RSA (Rivest Shamir Adleman).*

Abstrak: Perkembangan teknologi komputer pada saat ini memberikan dampak yang besar dalam penyampaian informasi, sedangkan keamanan data menjadi salah satu apek yang sangat penting dalam sistem informasi saat ini. Toko baju family menggunakan teknologi komputer dalam melakukan proses transaksi penjualan sehingga setiap transaksi yang dilakukan tersimpan dalam bentuk data penjualan.
Pada permasalahan yang dibahas, dengan menerapkan Perancangan Aplikasi Keamanan Data salah satunya dengan menggunakan algoritma RSA (Rivest Shamir Adleman) dalam mengamankan data penjualan. Dengan mengamankan data penjualan bertujuan untuk membantu pegawai dalam mengamankan data penjualannya. Hasil penelitian merupakan terciptanya sebuah aplikasi Pengamanan Data dengan Algoritma RSA (Rivest Shamir Adleman) yang dapat membantu pegawai dalam mengamankan data penjualan yang berada pada Toko Baju Family.

Kata kunci: Kriptografi, RSA (Rivest Shamir Adleman)

PENDAHULUAN

Penjualan adalah suatu tindakan untuk menukar barang atau jasa dengan uang dengan cara mempengaruhi orang lain agar mau memiliki barang yang ditawarkan sehingga kedua belah pihak mendapatkan keuntungan dan kepuasan.

Data penjualan merupakan informasi yang didapat dari kegiatan transaksi penjualan pada suatu perusahaan melalui proses pemasaran. Data ataupun informasi adalah aset yang begitu penting bagi suatu perusahaan ataupun individu dan tidak terlepas dari adanya ancaman pencurian atau penyalahgunaan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Penyimpanan data menggunakan komputer sebagai upaya pengamanan data, sehingga data-data atau informasi yang berharga dapat terjamin ke rahasiaannya.

Dalam hal ini toko baju family belum memiliki sistem keamanan pada data penjualan sehingga data penjualan tersebut rentan terhadap pencurian dan manipulasi data. Maka untuk itu perlu diperlukannya pengamanan data yang kuat dengan menggunakan algoritma kriptografi.

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Oct 2022, V (3): 664 – 670 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

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. Proses penyamaran dari plaintext ke ciphertext disebut enkripsi (encryption), dan proses pengembalian dari ciphertext menjadi plaintext kembali disebut dekripsi (decryption) . Untuk melakukan proses enkripsi dan dekripsi dengan menggunakan metode algoritma Rivest Shamir Adleman (RSA).

Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci public. Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (signing) dan untuk enkripsi salah satu penemuan besar pertama dalam kriptografi kunci public.

METODE

Metode pengembangan sistem secara umum diartikan sebagai urutan langkah- langkah yang terstruktur untuk mengembangkan sebuah sistem informasi berbasis komputer. Metode pengembangan sistem juga dapat berarti menyusun suatu sistem yang baru untuk menggantikan sistem yang lama secara keseluruhan atau mengembangkan sistem yang telah ada. Berikut beberapa langkah yang dilakukan dalam penelitian:

ObservasiMelakukan observasi langsung di Toko Baju Family untuk mencari masalah yang dialami di took tersebut untuk mengatasi pemgamanan pada data penjualan. Masalah tersebut akan diselesaikan dalam penelitian ini.

Wawancara dilakukan kepada pihak yang menangani bagian data penjualan. Adapun data yang didapatkan dari hasil observasi dan wawancara sebagai berikut:

Tabel. Data Penjualan Toko Baju Family Bulan Februari

Data Penjualan Toko Baju Family Bulan Januari						
No	Tanggal	Kode	Nama Barang	Jumlah	Harga Satuan	Total
1	01/01/21	B01	Baju Gamis	30	135,000	4,050,000
2	02/01/21	B04	Baju Koko	15	65,000	975,000
3	03/01/21	B03	Baju Kemeja	22	115,000	2,530,000
4	04/01/21	B02	Baju anak	36	80,000	2,880,000
5	05/01/21	B07	Kaos	28	100,000	2,800,000
6	07/01/21	B05	Jaket	10	150,000	1.500.000
7	09/01/21	B08	Celana	20	90,000	1,800,000
8	10/01/21	B09	Sepatu	8	50,000	400,000
9	11/01/21	B10	Kaos Kaki	14	15,000	210,000
10	12/01/21	B06	Pakaian Bekas	25	20,000	500,000
						26.420.000

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Oct 2022, V (3): 664 – 670 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Tabel. Data Penjualan Toko Baju Family Bulan Februari

Data Penjualan Toko Baju Family Bulan Februari						
No	Tanggal	Kode	Nama Barang	Jumlah	Harga Satuan	Total
1	01/02/21	B01	Baju Gamis	8	135.000	1.080.000
2	02/02/21	B04	Baju Koko	10	65.000	650.000
3	03/02/21	B03	Baju Kemeja	17	115.000	1.955.000
4	04/02/21	B02	Baju Anak	20	80.000	1.600.000
5	06/02/21	B07	Kaos	15	100.000	1.500.000
6	09/02/21	B05	Jaket	0	150.000	0
7	10/02/21	B08	Celana	2	90.000	180.000
8	11/02/21	B09	Sepatu	0	50.000	0
9	03/02/21	B10	Kaos Kaki	0	15.000	0
10	04/02/21	B06	Pakaian Bekas	5	20.000	100.000
						7.065.000

Tabel. Data Penjualan Toko Baju Family Bulan April

Data Penjualan Toko Baju Family Bulan April						
No	Tanggal	Kode	Nama Barang	Jumlah	Harga Satuan	Total
1	01/04/21	B01	Baju Gamis	6	135.000	810.000
2	02/04/21	B04	Baju Koko	8	65.000	520.000
3	03/04/21	B03	Baju Kemeja	19	115.000	2.185.000
4	05/04/21	B02	Baju Anak	3	80.000	240.000
5	06/04/21	B07	Kaos	8	100.000	800.000
6	07/04/21	B05	Jaket	0	150.000	0
7	08/04/21	B08	Celana	9	90.000	810.000
8	10/04/21	B09	Sepatu	0	50.000	0
9	10/04/21	B10	Kaos Kaki	2	15.000	30.000
10	11/04/21	B06	Pakaian Bekas	4	20.000	80.000
						5.475.000

Tabel. Data Penjualan Toko Baju Family Bulan Maret

Data Penjualan Toko Baju Family Bulan Maret						
No	Tanggal	Kode	Nama Barang	Jumlah	Harga Satuan	Total
1	04/03/21	B01	Baju Gamis	17	135.000	2.295.000
2	06/03/21	B04	Baju Koko	4	65.000	260.000
3	07/03/21	B03	Baju Kemeja	8	115.000	920.000
4	08/03/21	B02	Baju Anak	10	80.000	800.000
5	09/03/21	B07	Kaos	5	100.000	500.000
6	09/03/21	B05	Jaket	3	150.000	450.000
7	10/03/21	B08	Celana	13	90.000	1.170.000
8	09/03/21	B09	Sepatu	1	50.000	50.000
9	12/03/21	B10	Kaos Kaki	3	15.000	45.000
10	12/03/21	B06	Pakaian Bekas	15	20.000	300.000
						7.195.000

Tabel. Data Penjualan Toko Baju Family Bulan Mei

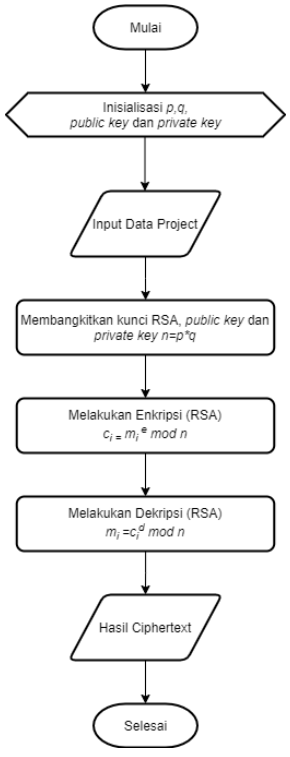
Data Penjualan Toko Baju Family Bulan Mei						
No	Tanggal	Kode	Nama Barang	Jumlah	Harga Satuan	Total
1	01/05/21	B01	Baju Gamis	30	135.000	4.050.000
2	02/05/21	B04	Baju Koko	45	65.000	2.925.000
3	03/05/21	B03	Baju Kemeja	30	115.000	3.450.000
4	04/05/21	B02	Baju Anak	42	80.000	3.360.000
5	06/05/21	B07	Kaos	21	100.000	2.100.000
6	08/05/21	B05	Jaket	12	150.000	1.800.000
7	08/05/21	B08	Celana	30	90.000	2.700.000
8	09/05/21	B09	Sepatu	25	50.000	1.250.000
9	10/05/21	B10	Kaos Kaki	2	15.000	30.000
10	12/05/21	B06	Pakaian Bekas	22	20.000	440.000
						22.105.000

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Oct 2022, V (3): 664 – 670 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Tabel. Data Penjualan Toko Baju Family Bulan Juni

Data Penjualan Toko Baju Family Bulan Juni						
No	Tanggal	Kode	Nama Barang	Jumlah	Harga Satuan	Total
1	01/06/21	B01	Baju Gamis	10	135.000	1.350.000
2	02/06/21	B04	Baju Koko	11	65.000	715.000
3	03/06/21	B03	Baju Kemeja	9	115.000	1.035.000
4	04/06/21	B02	Baju Anak	15	80.000	1.200.000
5	05/06/21	B07	Kaos	30	100.000	3.000.000
6	06/06/21	B05	Jaket	2	150.000	1.500.000
7	07/06/21	B08	Celana	10	90.000	300.000
8	08/06/21	B09	Sepatu	1	50.000	50.000
9	09/06/21	B10	Kaos Kaki	0	15.000	0
10	12/06/21	B06	Pakaian Bekas	15	20.000	300.000
						9.450.000

Flowchart Algoritma Rivest Shamir Adleman (RSA) Dibawah ini adalah *flowchart* proses enkripsi dan dekripsi dari algoritma *Rivest Shamir Adleman* (RSA) sebagai berikut:



Gambar .*Flowchart* Sistem Algoritma RSA

Perhitungan Metode RSA Perhitungan Metode RSA ini merupakan langkah-langkah penyelesaian masalah keamanan data penjualan pada Toko Baju Family:
Proses pembangkit Kunci Proses enkripsi algoritma Rivest Shamir Adleman (RSA) adalah sebagaiberikut:
Pilih dua bilangan prima sembarang p dan , p G q.
Nilai (p) = 19 dan nilai (q) = 7.
Hitung $n = p * q$. Bilangan n disebut *parameter.*
p * q = n
*19 * 7 = 108*
Hitung Hitung $\varphi(n) = (p - 1)(q - 1)$.
$(p - 1)(q - 1) = \varphi(n)$
(19-10)(7-1)= $\varphi(n)$
(18)(6)=108
Pilih nilai e dengan syarat $e > 1$ dan *greatest comman divisior* (e,*108*) = 1Nilai e yang di ambil adalah 7.
Hitung d hingga d,$e \equiv 1$ (mod 108) dan $d < 108$
$d * 7 = 1 \; mod \; 108$
$d * 7 \; mod \; 108 = 1$
$d = 31$
jadi, $31 * 7 \; mod \; 108 = 1$
Sehingga pasangan kunci yang didapat adalah:
Kunci enkripsi (*public key*) (e,n) = (7,133) dan Kunci *dekripsi (private key)* (d,n) = (31, 133).

Proses *Enkripsi* Pertama yang harus dilakukan adalah merubah plaintext menjadi format ASCII, Berikut ini adalah penyelesaiannya:

Plaintext	B	a	j	u	Spasi	G	a	m	i	
ASCII	66	97	106	117	32	71	97	109	105	

Kemudian *m* dipecah menjadi tiap karakter *plaintext.* Berikut ini adalah tabel:

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Oct 2022, V (3): 664 – 670 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Tabel. Karakter *mi* dan kode ASCII untuk *plaintext* baju gamis

Mi	Keterangan	Kode ASCII (desimal)
m1	B	66
m2	a	97
m3	j	106
m4	u	117
m5	Spasi	32
m6	G	71
m7	a	97
m8	m	109
m9	i	105
m10	s	115

Selanjutnya di*enkripsi* dengan $ci = m_i^e \bmod n$, yaitu sebagai berikut:

$Ci = mi^e \bmod n$

$c1 = 66^7 \bmod 133 = 80$
$c2 = 97^7 \bmod 133 = 90$
$c3 = 106^7 \bmod 133 = 106$
$c4 = 117^7 \bmod 133 = 40$
$c5 = 32^7 \bmod 133 = 67$
$c6 = 71^7 \bmod 133 = 22$
$c7 = 97^7 \bmod 133 = 90$
$c8 = 109^7 \bmod 133 = 60$
$c9 = 105^7 \bmod 133 = 91$
$c10 = 115^7 \bmod 133 = 115$

Tabel. Karakter *Ci* dan Kode untuk *Plaintext* Baju Gamis yang telah di*enkripsi*dengan algoritma *Rivest Shamir Adleman* (RSA)

Ci	Kode ASCII (decimal)	Kode ASCII (Hexadesimal)
c1	80	50
c2	90	5a
c3	106	6a
c4	40	28
c5	67	43
c6	22	16
c7	90	5a
c8	60	3c
c9	91	5b
c10	115	73

Maka, dari kata "Baju Gamis" menjadi deret karakter Hexadesimal 505a6a2843165a3c5b73.

Proses Dekripsi Selanjutnya yang harus dilakukan adalah merubah ciphertext menjadi format ASCII, Berikut ini adalah penyelesaiannya:

ciphertext	50	5a	6a	28	43	16	5a	3c	5b	73
ASCII	80	90	106	40	67	22	90	60	91	115

Kemudian *ciphertext* dipecah dalam dua karakter Hexadesimal.

Tabel. Karakter ci dan kode ASCII untuk ciphertext 505a6a2843165a3c5b73.

Ci	Kode ASCII (Heksadesinal)	Kode ASCII (Desimal)
c1	50	80
c2	5a	90
c3	6a	106
c4	28	40
c5	43	67
c6	16	22
c7	5a	90
c8	3c	60
c9	5b	91
c10	73	115

Kemudian didekripsikan kembali menggunakan algoritma Rivest Shamir Adleman (RSA) dengan rumus $m_i = c^d \bmod n$, yaitu sebagai berikut:

$m1 = 80^{31} \bmod 133 = 66$
$m2 = 90^{31} \bmod 133 = 97$
$m3 = 106^{31} \bmod 133 = 106$

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Oct 2022, V (3): 664 – 670 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

$m4 = 40^{31} \mod 133 = 117$
$m5 = 67^{31} \mod 133 = 32$
$m6 = 22^{31} \mod 133 = 71$
$m7 = 90^{31} \mod 133 = 97$
$m8 = 60^{31} \mod 133 = 109$
$m9 = 91^{31} \mod 133 = 105$
$m10 = 115^{31} \mod 133 = 115$

Maka, didapat hasil dari dekripsi yaitu: 66, 97, 106, 117, 32, 71, 97, 109, 105,115 dalam karakter ASCII adalah:

ASCII	66	97	106	117	32	71	97	109	105	115
Plaintext	B	a	j	u	Spasi	G	a	m	i	s

HASIL DAN PEMBAHASAN

Dalam sistem pengamanan data penjualan ini di lengkapi dengan tampilan yang bertujuan untuk memudahkan penggunannya. Fungsi dari antarmuka (*interface)* ini adalah untuk memberikan input dan menampilkan output dari aplikasi. Pada aplikasi ini memiliko *interface* yang terdiri dari Menu Utama, Enkripsi dan Dekripsi.

Tampilan *Form Login*

Sebelum masuk dan mengakses

aplikasi, *user* harus melakukan *login* terlebih dahulu dengan cara meng-*input user name* dan *password* dengan benar sesuai dengan sistem *database* dan akan masuk ke menu utama, namun jika tidak maka harus mengulangi untuk meng-*input user name* dan *password* dengan benar. Dibawah ini merupakan tampilan *form login* adalah sebagai berikut:

Gambar. *Form Login* Form Menu Utama

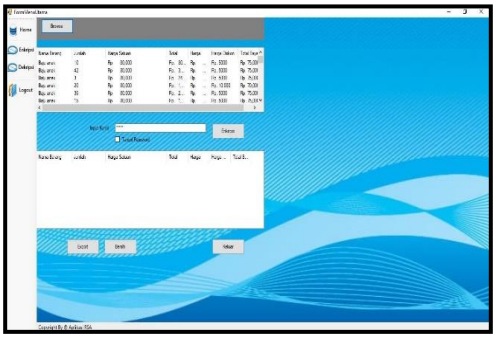
Menu utama merupakan *form* yang akan menampilkan menu pada sistem. Menu utama terdiri dari beberapa tombol yaitu Menu Enkripsi dan Dekripsi.

Berikut adalah tampilan Menu Utama:

Gambar .*Form* Menu Utama

Form Enkripsi

Form enkripsi digunakan untuk melakukan proses penyandian pada data. Berikut tampilan dari *form* enkripsi:



Gambar Form Menu Enkripsi

Form Dekripsi

Form Deksripsi digunakan untuk melakukan proses penyandian pada data. Berikut tampilan dari *form* dekripsi:

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Oct 2022, V (3): 664 – 670 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Gambar Form Menu Dekripsi

SIMPULAN

Berdasarkan Penelitian yang telah dilakukan dalam tahap perancangan dan evaluasi implementasi metode Rivest Shamir Adleman (RSA) untuk pengamanan data penjualan pada Toko Baju Family, maka dapat disimpulkan bahwa :

Berdasarkan hasil peneltian yang dilakukan sebelumnya dengan Algoritma RSA (Rivest Shamir Adleman) maka diterapkan kedalam sebuah sistem agar dapat mengenkripsi dan mendekripsi data penjualan untuk memperoleh keamanan data penjualan pada Toko Baju Family.

Berdasarkan hasil rancangan aplikasi pengamanan data penjualan dengan Algoritma RSA (Rivest Shamir Adleman) dirancang dengan pemodelan UML (Unified Modeling Language), yaitu aplikasi yang digambarkan pada Use Case Diagram, Activity Diagram dan Class Diagram. Kemudian dilakukan pengcodingan dengan perancangan berbasis dekstop.

Berdasarkan hasil pengujian ini maka pengamanan data penjualan dengan menerapkan Algoritma RSA (Rivest Shamir Adleman) diuji dengan cara mengenkripsi dan mendekripsi data penjualan sehingga sistem ini mampu membantu pegawai dalam mengamankan data penjualan Toko Baju Family

DAFTAR PUSTAKA

Wijaya and R. Irawan, “Prosedur Administrasi Penjualan Pada Usaha Jaya Teknika Jakarta Barat,” *Perspektif*, vol. 16, no. 1, pp. 26–30, 2018.

S. Setti, I. Gunawan, B. E. Damanik, S. Sumarno, and I. O. Kirana, “Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 182, 2020, doi: 10.30865/jurikom.v7i1.1960.

F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, “Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard,” *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

I. Gunawan, “Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks,” *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 2, no. 2, pp. 124–129, 2018, doi: 10.30743/infotekjar.v2i2.266.

A. P. N. Nurdin, “Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia,” *Jesik*, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com.

Wulandari and S. Aprilia, “Jurnal TAM (Technology Acceptance Model) Volume 4 Juli 2015,” *Technol. Accept. Model*, vol. 4, pp. 1–7, 2015.