Jurnal CyberTech

Vol.4. No.7, Juli 2021, pp. xx~xx
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Pengamanan Data Penjualan Dengan Kriptografi Algoritma Rivest Shamir Adleman (RSA) Pada Toko Baju Family

Sitti Khoirun Nisa*, Mukhlis Ramadhan, S.E., M.Kom., Devri Suherdi, S.Kom., M.Kom.****

* Program Studi Sistem Informasi, STMIK Triguna Dharma
** Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info

Article history:
Received Jul 12th, 2021
Revised Jul 20th, 2021
Accepted Jul 30th, 2021

Keyword:

Toko Baju Family, Kriptografi, RSA (Rivest Shamir Adleman).

ABSTRACT

Perkembangan teknologi komputer pada saat ini memberikan dampak yang besar dalam penyampaian informasi. Maka keamanan data menjadi salah satu aspek yang sangat penting dalam sistem informasi saat ini. Salah satunya dalam pengamanan data penjualan. Toko Baju Family adalah toko yang bergerak dalam bidang bisnis. Beberapa produk yang ditawarkan pada toko ini yaitu baju, jaket, sepatu, kaus kaki dan masih banyak yang lainnya. Toko Baju Family menggunakan teknologi komputer dalam melakukan proses transaksi penjualan sehingga setiap transaksi yang dilakukan tersimpan dalam bentuk data penjualan. Data penjualan pada Toko Baju Family adalah salah satu data yang bersifat rahasia, sehingga hanya pihak-pihak tertentu saja yang dapat menerima dan membaca data penjualan itu, maka diperlukannya pengamanan pada data penjualan tersebut.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 absensi bulanan karyawan yang berada pada Toko Baju Family.

Corresponding Author
Nama : Sitti Khoirun Nisa
Program Studi Sistem Informasi
STMIK Triguna Dharma
Email: sittikhoirunnisa1@gmail.com

1. 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[1].

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 dan 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 kerahasiaannya[2].

Data penjualan pada Toko Baju Family adalah salah satu data yang bersifat rahasia, sehingga hanya pihak-pihak tertentu saja yang dapat menerima dan membaca data penjualan itu, maka diperlukannya pengamanan pada data penjualan tersebut. 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 diperlukannya pengamanan data yang kuat dengan menggunakan algoritma kriptografi.

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*) [3]. Untuk melakukan proses enkripsi dan dekripsi dengan menggunakan metode algoritma *Rivest Shamir Adleman* (RSA).

Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci publik. Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi dan salah satu penemuan besar pertama dalam kriptografi kunci publik [4]. Penerapan algoritma kriptografi RSA ini diharapkan menjadi solusi yang baik pada sistem penjualan yang akan dibangun Toko Baju Family untuk menjamin kerahasiaan data-data penjualan yang disimpan didalam database, dengan penggunaan algoritma RSA ke dalam sistem penjualan tersebut.

2. METODE PENELITIAN

2.1 Metode Penelitian

Metode penelitian yang digunakan yaitu metode pengembangan sistem. Metode pengembangan sistem secara umum diartikan sebagai urutan langkah-langkah yang terstruktur untuk mengembangkan sebuah sistem informasi berbasis komputer[5].

1. **Data Sampel Penelitian**

Berikut ini merupakan data sampel penelitian yang digunakan dalam pengamanan data penjualan pada bulan Januari :

Data Penjualan Toko Baju Family Bulan Januari						
No	**Tanggal**	**Kode**	**Nama Barang**	**Jumlah**	**Harga Satuan**	**Total**
1	01/01/2021	B01	Baju Gamis	30	Rp. 135,000	Rp. 4,050,000
2	02/01/2021	B04	Baju Koko	15	Rp. 65,000	Rp. 975,000
3	03/01/2021	B03	Baju Kemeja	22	Rp. 115,000	Rp. 2,530,000
4	04/01/2021	B02	Baju anak	36	Rp. 80,000	Rp. 2,880,000
5	05/01/2021	B07	Kaos	28	Rp. 100,000	Rp. 2,800,000
6	07/01/2021	B05	Jaket	10	Rp. 150,000	Rp . 1,500,000
7	09/01/2021	B08	Celana	20	Rp. 90,000	Rp. 1,800,000

Data Sampel (Lanjutan)

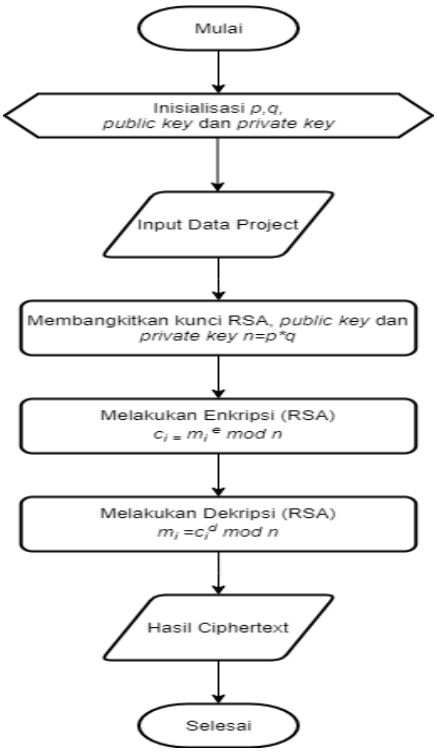
8	10/01/2021	B09	Sepatu	8	Rp. 50,000	Rp. 400,000
9	11/01/2021	B10	Kaos Kaki	14	Rp. 15,000	Rp. 210,000
10	12/01/2021	B06	Pakaian Bekas	25	Rp. 20,000	Rp. 500,000

3.3 Algoritma Sistem

Algoritma sistem adalah langkah-langkah untuk menyelesaikan masalah dalam perancangan sistem keamanan data penjualan menggunakan algoritma RSA(*Rivest Shamir Adleman*) . Hal ini dilakukan untuk meningkatkan keamanan data penjualan tersebut.

3.3.1 Flowchart Algoritma Rivest Shamir Adleman (RSA)

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



Gambar 3.1 *Flowchart* Sistem Algoritma RSA

3.3.2 Dekripsi Data Dari Penelitian

Berikut ini adalah data penjualan yang didapat dari Toko Baju Family yang akan diamankan. Untuk pengujian ini, sebagai contoh data yang diambil sebagai sampel dalam penelitian ini yaitu:

Tabel 3.7 Sampel Data Penjualan Toko Baju Family Bulan Januari

No	Tanggal	Kode	Nama Barang	Jumlah	Harga Satuan	Total
1	01/02/2021	B01	Baju Gamis	30	Rp 135,000	Rp 4,050,000

3.3.3 Penyelesaian Masalah Dengan Algoritma RSA

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

1. Proses Pembangkit Kunci RSA

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

a. Pilih dua bilangan prima sembarang p dan , $p \neq q$.

b. Nilai (p) = 19 dan nilai (q) = 7.

c. Hitung $n = p * q$. Bilangan n disebut *parameter*.

$p * q = n$

*19 * 7 = 108*

d. Hitung Hitung $\varphi(n) = (p - 1)(q - 1)$.

$(p - 1)(q - 1) = \varphi(n)$

(19-1)(7-1) = $\varphi(n)$

(18)(6) = 108

e. Pilih nilai *e* dengan syarat *e* > 1 dan *greatest comman divisior* (*e,108*) = 1

Nilai *e* yang di ambil adalah 7.

f. 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)

2. 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	s
ASCII	66	97	106	117	32	71	97	109	105	115

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

Tabel 3.8 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 rumus $c_i = m_i^e \ mod \ n$, yaitu sebagai berikut:

ci = $mi^e \ mod \ n$

c1 = 66^7 mod 133 = 80

c2 = 97^7 mod 133 = 90

c3 = 106^7 mod 133 = 106

c4 = 117^7 mod 133 = 40

c5 = 32^7 mod 133 = 67

c6 = 71^7 mod 133 = 22

c7 = 97^7 mod 133 = 90

c8 = 109^7 mod 133 = 60

c9 = 105^7 mod 133 = 91

c10 = 115^7 mod 133 = 115

Tabel 3.9 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

Tabel 3.9 Karakter *Ci* dan Kode untuk *Plaintext* Baju Gamis yang telah di*enkripsi* dengan algoritma *Rivest Shamir Adleman* (RSA) (Lanjutan)

c7	90	5a
c8	60	3c
c9	91	5b
c10	115	73

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

3. 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 3.10 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

Tabel 3.10 Karakter *ci* dan Kode ASCII untuk *ciphertext* 505a6a2843165a3c5b73 (Lanjutan)

c5	43	67
c6	16	22
c7	5a	90
c8	3c	60
c9	5b	91
c10	73	115

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

$mi = c_i^d \bmod n$

$m1 = 80^{31} \bmod 133 = 66$

$m2 = 90^{31} \bmod 133 = 97$

$m3 = 106^{31} \bmod 133 = 106$

$m4 = 40^{31} \bmod 133 = 117$

$m5 = 67^{31} \bmod 133 = 32$

$m6 = 22^{31} \bmod 133 = 71$

$m7 = 90^{31} \bmod 133 = 97$

$m8 = 60^{31} \bmod 133 = 109$

$m9 = 91^{31} \bmod 133 = 105$

$m10 = 115^{31} \bmod 133 = 115$

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

3. ANALISA DAN HASIL

Sebelum sistem benar-benar bisa digunakan dengan baik, sistem harus melalui tahap pengujian analisa dan hasil terlebih dahulu yaitu sebagai berikut :

3.1 Tampilan Form Login

Di bawah ini merupakan tampilan *form login* adalah sebagai berikut:

Gambar 5.1 *Form* Login

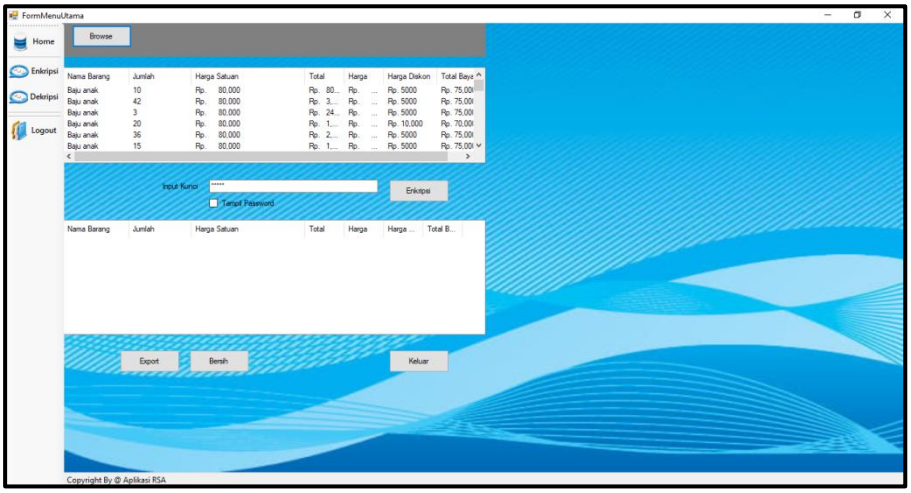
3.2 Tampilan Form Menu Utama

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 5.2 *Form* Menu Utama

3.2 Tampilan Form Enkripsi

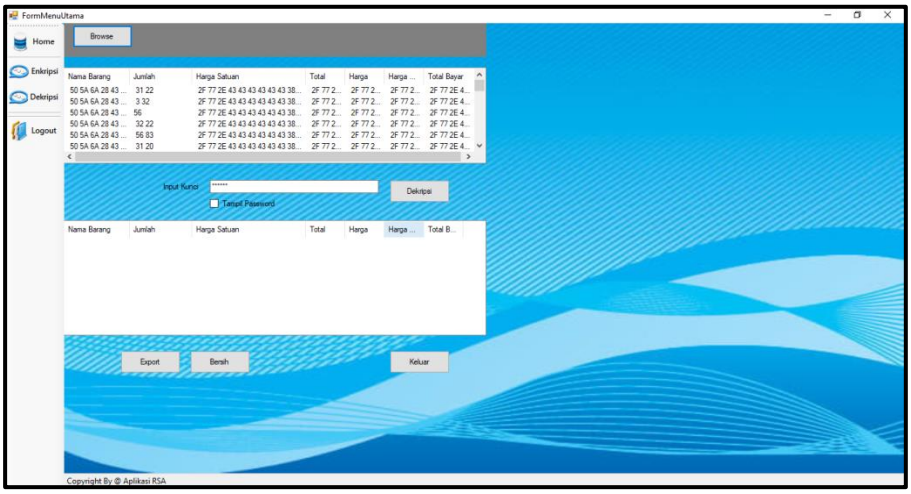
Form enkripsi digunakan untuk melakukan proses penyandian pada data. Berikut tampilan dari *form* enkripsi :



Gambar 5.3 *Form* Enkripsi

3.2 Tampilan Form Dekripsi

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



Gambar 5.3 *Form* Dekripsi

4. KESIMPULAN

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 :

1. 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.

2. 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.
3. 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 .

UCAPAN TERIMA KASIH

Puji syukur kehadirat Allah Swt karena berkat karunia-nya masih memberikan kesehatan dan kesempatan sehingga dapat diselesaikan jurnal ilmiah ini dengan baik. ucapan terima kasih ditujukan kepada kedua Orang tua, atas kesabaran, ketabahan serta ketulusan hati memberikan dorongan moril maupun material serta do'a yang tiada henti-hentinya. Ucapan terimakasih juga ditujukan untuk pihak-pihak yang telah mengambil bagian dalam penyusunan jurnal ilmiah ini.

REFERENSI

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

[2] 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.

[3] 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.

[4] 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.

[5] M. Prof. Dr. Eri Barlian, *Metodologi Penelitian Kualitatif dan Kuantitatif*. Sukabina Press, 2017.

BIBLIOGRAFI PENULIS

Sitti Khoirun Nisa

Wanita kelahiran Medan, 71 Desember 1999 yang saat ini menempuh pendidikan Strata Satu (S-1) di STMIK Triguna Dharma Medan mengambil jurusan Program Studi Sistem Informasi dan tertarik pada desain grafis .

E-Mail : sittikhoirunnisa1@gmail.com

Mukhlis Ramadhan, S.E., M.Kom

Beliau merupakan dosen tetap STMIK Triguna Dharma dengan program studi Sistem Informasi dan Wakil Ketua I Bidang Akademik.
NIDN : 0104107901
Tempat Tanggal Lahir: Medan , 4 Oktober 1979
Jenis Kelamin : Laki – laki
E-mail : mukhlis.ramadhan99@gmail.com
Program Studi : Sistem Informasi

Devri Suherdi, S.Kom., M.Kom

Beliau merupakan dosen tetap STMIK Triguna Dharma serta seorang Praktisi & Kewirausahaan
NIDN : 0124097301
Tempat Tanggal Lahir : PKL. Brandan, 10 Oktober 1987
E-Mail : devrisuherdi10@gmail.com