Jurnal CyberTech

Vol.3. No.7, Juli 2020, pp. 1290~1296
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Perancangan Keamanan Data Menggunakan Algoritma Data Encyption Standard Pada Penjualan Jasa Tour dan Travel di PT. Bintan Holidays Wisata Tour Medan

Harapan Mendrofa.[*],Puji Sari Ramadhan.[**], Firahmi Rizky.[***]

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

Article Info

Article history:
Received Jul 12th, 2020
Revised Jul 20th, 2020
Accepted Jul 30th, 2020

Keyword:
Ciphertext
Data
Kriptografi
Plaintext
RSA

ABSTRACT

Keamanan dalam penyimpanan suatu data atau informasi adalah hal yang sangat penting dan tidak dapat diabaikan, data yang dulunya berupa data tertulis telah berubah menjadi elektronik atau digital. PT. Bintan Holidays Wisata Tour mengalami pencurian data penjualan, yang mengakibatkan keaman privasi pelanggan diketahui orang yang dikenal. Maka dibutuhkan kemanan data yang kuat dan tidak dapat bobol. Permasalahan tersebut dapat diatasi dengan keilmuan yang cocok digunakan adalah kriptografi. Kriptografi merupakan salah satu ilmu yang membahas masalah keamanan komputer seperti menyembunyikan pesan, kerahasiaan data, keutuhan data dan otentikasi entitas. Dengan enkripsi data tidak dapat terbaca karena teks asli atau plaintext telah diubah ke teks yang tak terbaca atau disebut ciphertext. Algoritma yang digunakan untuk enkripsi dan deskripsi untuk mengamankan data dengan menggunakan RSA. Hasil yang pengujian ini digunakan algoritma RSA dapat membantu PT. Bintan Holidays Wisata Tour Medan dalam melakukan pengamanan data dan data tidak dapat terbaca karena teks asli atau plaintext telah diubah ke teks yang tak terbaca atau disebut ciphertext. Algoritma yang digunakan untuk enkripsi dan deskripsi dengan cepat.

Corresponding Author:
Nama :Harapan Mendrofa
Program Studi : Sistem Informasi
STMIK Triguna Dharma
Email: harapanmendrofa98@gmail.com

1. PENDAHULUAN

Keamanan dalam penyimpanan suatu data atau informasi adalah hal yang sangat penting dan tidak dapat diabaikan, data yang dulunya berupa data tertulis telah berubah menjadi elektronik atau digital [1]. PT. Bintan Holidays Wisata Tour mengalami pencurian data penjualan, yang mengakibatkan keaman privasi pelanggan diketahui orang yang dikenal. Maka dibutuhkan kemanan data yang kuat dan tidak dapat bobol. Dengan masalah tersebut, dibidang keilmuan yang cocok digunakan adalah kriptografi.

Kriptografi merupakan salah satu ilmu yang membahas masalah keamanan komputer seperti menyembunyikan pesan, kerahasiaan data, keutuhan data dan otentikasi entitas[2]. Dalam kriptografi ada dua proses utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses pengamanan suatu informasi atau data dengan membuat informasi atau data tidak dapat dibaca dan dimengerti oleh orang lain. Sedangkan dekripsi adalah kebalikan dari enkripsi yaitu

dapat mengubah kembali bentuk tersamar tersebut menjadi informasi atau data awal, sehingga dapat dibaca dan dimengerti. Dalam algoritma kriptografi, proses enkripsi diterapkan untuk mengamankan data. Dengan enkripsi data tidak dapat terbaca karena *teks* asli atau plaintext telah diubah ke *teks* yang tak terbaca atau disebut *ciphertext*. Algoritma yang digunakan untuk enkripsi dan deskripsi untuk mengamankan data dengan menggunakan RSA.

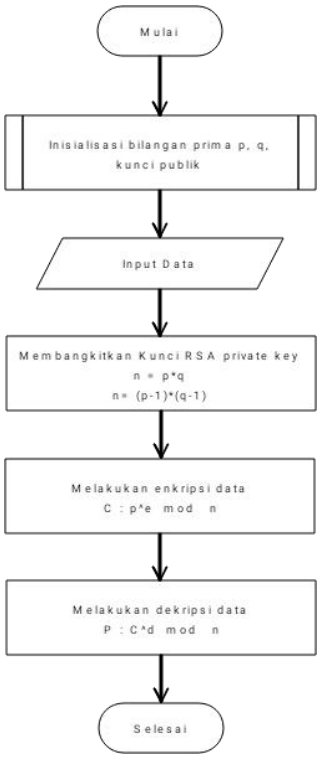
RSA adalah metode yang menggunakan perhitungan matematika yang rumit dan disertai dengan kunci pengaman awal (dengan *private key* maupun dengan *public key*) sehingga amat sulit untuk ditembus oleh *hacker*. Adapun prinsip pengamanan metode ini adalah bagaimana sistem dapat mengamankan proses penyimpanan dan pengiriman dokumen. Mula-mula dokumen dalam bentuk *teks* dienkripsi dengan metode RSA. Sehingga dokumen tidak dapat dibaca oleh siapapun, karena *teks* telah berubah menjadi susunan huruf yang teracak[3]. algoritma RSA dapat membantu PT. Bintan Holidays Wisata Tour Medan dalam melakukan pengamanan data.

2. METODE PENELITIAN

Dalam melakukan sebuah penelitian ada beberapa hal yang dilakukan untuk mencapai tujuan penelitian yang baik dan benar. Konsep metodologi penelitian yang baik dengan cara melakukan pengumpulan data yang benar dan juga memiliki kajian pustaka yang luas. Dengan menggunakan beberapa metode pengumpulan data yang akan dijabarkan pada pembahasan dapat menyelesaikan masalah dan mendapatkan data yang dibutuhkan dalam penelitian.

2.1 Flowchart Metode RSA

Flowchart merupakan penggambaran secara grafik dari langkah-langkah dan urutan prosedur dari suatu program kerja secara keseluruhan menggunakan metode RSA mulai dari awal sampai akhir prosesnya.



Gambar 1. *Flowchart*Metode RSA

2.2 Digital Signature Menggunakan Algoritma RSA

Langkah pertama pengujian dimasukan dengann nama karyawan Novin hutagalung dalam AlgoritmaRSA adalah melakukan inisialisasi terhadap nilai bilang prima p = 29 dan q = 43 yang diambil secara acak. Berikut ini adalah salah satu data tabel 3.1 yang dimana setiap plainteks akan di ubah ke bentuk kode ASCII yaitu sebagai berikut:

Tabel 1. ASCII

No	Plainteks	Kode ASCII
1	N	*78*
2	o	*79*
3	v	*86*
4	i	*73*

5	n	*78*
6	h	*49*
7	u	*79*
8	t	*78*
9	a	*42*
10	g	*40*
11	a	*42*
12	l	*69*
13	u	*79*
14	n	*78*
15	g	*40*

Berikut metode RSA:

1. Pembangkit Kunci Metode RSA
   a. Pilihlah bilangan prima yang sudah di dapat diatas adalah (p)= 29 dan nilai (q)=43.
   b. Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkaliann= p* qn = 29 * 43 = 1247
   c. Hitung (phi) n=(p-1)(q-1) n=28 * 42 =1176
   d. Pilih nilai edengan syarat e> 1 = 1

   Nilai eyang di ambil adalah 53. Bukti:
   (53, 1176)
   1176 *mod* 53 = 10
   53 *mod* 10 = 3
   10 *mod* 3 = 1
   3 *mod* 1 = 0
   Sehingga d*e=1(*mod* 1176) dan d<1176 d*53=1*mod*1176 d*53 *mod*1176 = 1 d = 821
   Bukti:
   821 * 53 *mod* 1176 = 1
   Sehingga pasangan kunci yang di dapat adalah :
   (e,n) = (53, 1247) dan Privatekey(d,n) = (821, 1247)
2. Enkripsi Data
   C1 = 4953 *mod* 1247 = 36
   C2 = 5353 *mod* 1247 = 1176
   C3 = 4953 *mod* 1247 = 3
   C4 = 4953 *mod* 1247 = 36
   C5 = 48 *mod* 1247 = 292
   C6 = 4953 *mod* 1247 = 36

Tabel 2. Hasil Enkripsi

Plaintext	***Hasil Enkripsi***	***Heksa***
49	*36*	*24*
79	*1176*	*498*
78	*36*	*24*
42	*36*	*24*
40	*292*	*124*
49	*36*	*24*

3. Dekripsi Data
   Langkah selanjutnya adalah melakukan dekripsi data dengan rumus
   P= Cd *mod* n.
   P1 = 36821 *mod* 1247 = 49
   P2 = 1176821 *mod* 1247 = 53
   P3 = 36821 *mod* 1247 = 49
   P4 = 36821 *mod* 1247 = 49
   P5 = 292821 *mod* 1247 = 48
   P6 = 36821 *mod* 1247 = 49

Tabel 3. Hasil Dekripsi Data

Chipertext	***Hasil DekripsiData***	***Plaintext***
36	*49*	N

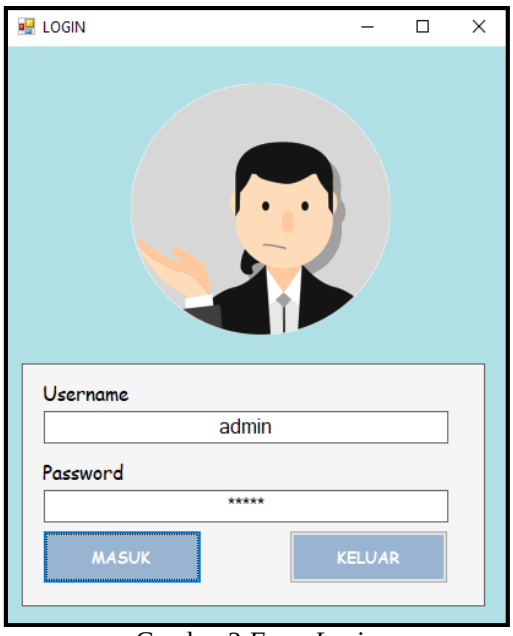
1176	*53*	o
36	*49*	v
36	*49*	i

3. ANALISA DAN HASIL

Implementasi sistem adalah tahapan dimana sistem atau aplikasi siap untuk dioprasikan pada keadaan yang sebenarnya sesuai dari hasil analisis dan perancangan yang dilakukan, sehingga akan diketahui apakah sistem atau aplikasi yang dibangunn dapat menghasilkan suatu tujuan yang dicapa, dan aplikasi Kriptografi ini dilengkapi dengan tampilan yang bertujuan untuk memudahkan penggunanya. Fungsi dari *interface* (antarmuka) ini adalah untuk memberikan *input* dan menampilkan *output* dari aplikasi. Pada aplikasi ini memiliki *interface* yang terdiri dari *Form Login*, *Form* Menu Utama, *Form* Data Karyawan, dan *Form* Metode RSA.

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 2.*Form Login*

Keterangan : Tombol “Masuk” digunakan untuk mem-validasikan *username* dan *password* yang telah kita isi pada kotak teks yang disediakan.

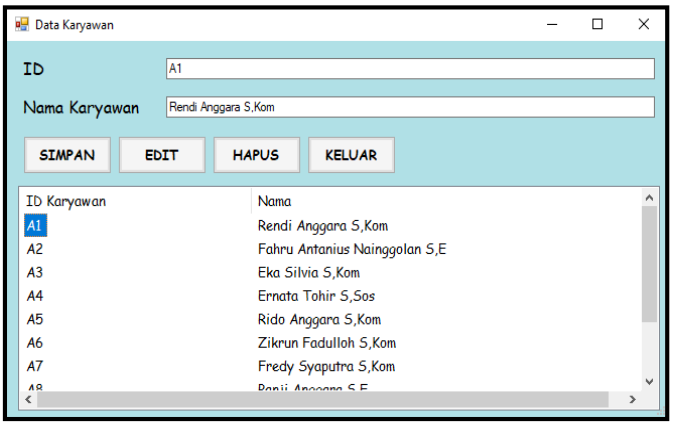
2. *Form* Menu Utama

Form Menu Utama digunakan sebagai penghubung untuk *Form* Data Karyawan, *Form* Metode *RSA* dan ada beberapa *form* lainnya.

Gambar 3.*FormMenu* Utama

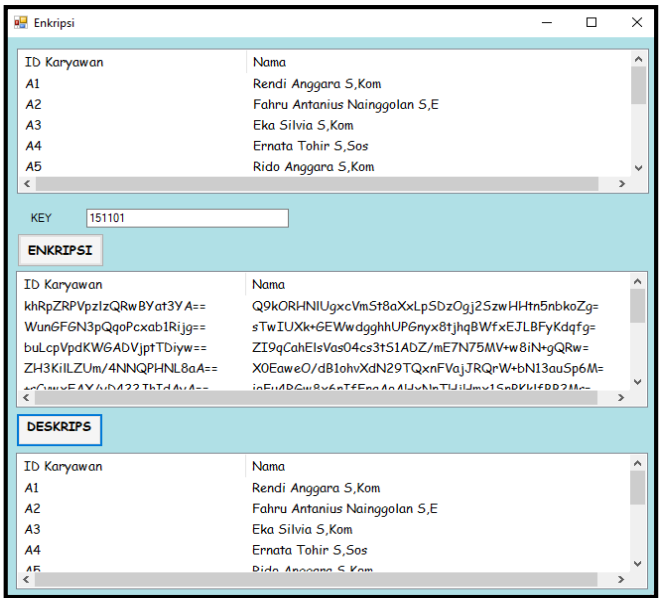
3. *Form* Data Karyawan

Form Data Karyawan adalah *form* pengolahan data karyawan dalam penginputan data, ubah data dan penghapusan data karyawan. Adapun *form* data karyawan adalah sebagai berikut.



Gambar 4.*Form*Data Karyawan

4. *Form* Metode RSA



Gambar 5. *Form* Proses *RSA*

Dalam *Form* RSA dapat mengenkripsikan dan deskripsikan adalah sebagai berikut :

a. Button Proses Enskrips berfungsi untuk memproses mengenkripsikan data karyawan.
b. Button Proses Deskripsi berfungsi untuk memproses mendenkripsikan data karyawan.
c. Button Keluar berfungsi untuk kembali ke *menu* utama.

4. KESIMPULAN

Berdasarkanhasilanalisadaripermasalahan yang terjadidengankasus yang di bahastentangmengamankan data karyawandengan menggunakan algoritma RSAadalahsebagaiberikut:

1. Untukmenganalisapermalahan, maka proses yang dilakukanmelakukankunciplaint text denganmengubahkalimat Ascii dan diamanakandalambentukenkripsi data text.
2. Untukmerancang Kriptografi dalam menentukan mengamankan data karyawandenganmenggunakanbahasapemodelanataupun UML dan membangunsystemdenganmenggunakanbahasapemograman*basic* Visual Studio 2010.

3. Dapatmegimplementasikandenganmenjalankansistem di komputer dan memasukan data alternatif dan bobotcriteriauntukmelakukanmengamankan datakaryawanyang ditampilkandalambentuklaporan yang disajikandalamsistem.

UCAPAN TERIMA KASIH

Terima Kasih diucapkan kepada kedua orang tuaserta keluarga yang selalu memberi motivasi, Doa dan dukungan moral maupun materi, serta pihak-pihak yang telah mendukung dalam proses pembuatan jurnal ini yang tidak dapat disebutkan satu persatu. Kiranya jurnal ini bisa memberi manfaat bagi pembaca dan dapat meningkatkan kualitas jurnal selanjutnya.

REFERENSI

[1] T. Raharjo, "Pengelolaan Dan Pengembangan Usaha Penyewaan Alat Berat Pada Pt. Sepakat Bersama Jaya Di Samarinda," *Agora*, Vol. 1, No. 3, Pp. 1006–1014, 2013.

[2] L. Hakim And A. Fauzy, "Menggunakan Metode Association Rules," *Univ. Res. Colloq.*, Pp. 73–81, 2015.

[3] Yuda Pratama Wibawa, "Implementasi Data Mining Menentukan Merek Celana Dalam Abstract : Sales Of Apparel Products , Especially Clothing Pants In Both Men And Women Is Increasing Every Month , The Products Offered Are A Variety Of Brands , Brands That Have Influenced People To," Pp. 57–62, 2016.

[4] F. A. Sianturi, "Penerapan Algoritma Apriori Untuk Penentuan Tingkat Pesanan," *Mantik Penusa*, Vol. 2, No. 1, Pp. 50–57, 2018.

[5] J. A. Kantor, "Kepuasan Kerja Pengawas Produksi Berpengaruh Terhadap Kinerja Operator Alat Berat Pada Usaha Jasa Kontraktor Pertambangan Mineral Dan Batubara," Pp. 33–42, 2018.

[6] A. Maddeppungeng, "Analisis Produktivitas Alat Berat Pada Proyek Pembangunan Pabrik Dwi Novi Setiawati Begitu Pula Proyek Pembangunan Pabrik," Pp. 91–103.

BIBLIOGRAFI PENULIS

	**Nama Lengkap** : **Harapan Mendrofa** **NIRM** : **2017020922** **Tempat/Tgl.Lahir** : **Padang,11 Desember 1998** **Jenis Kelamin** : **Laki - Laki** **Alamat** : **Jln.Flamboyan Raya No 58 Tanjung Sari Medan Selayang** **No/Hp** : **08232146668** **Email** : **harapanmendrofa98@gmail.com** **Program Keahlian** : **Pemograman Berbasis Web**
	**Nama Lengkap** : **Puji Sari Ramadhan, S.Kom., M.Kom.** **NIDN** :**0126039201** **Tempat/Tgl.Lahir** : **-** **Jenis Kelamin** : **Laki-Laki** **No/Hp** : **08116332227** **Email** : **pujisariramadhan@gmail.com** **Pendidikan** : **- D3 – STMIK Triguna Dharma** **- S2 – STMIK Triguna Dharma** **- S2 – Universitas Putra Indonesia Yptk Padang** **Bidang Keahlian** : **Ilmu Kecerdasan Buatan, Sistem Pakar, Pengolahan Citra dll**
	**Nama Lengkap** : **Firahmi Rizky, S.Kom., M.Kom.** **NIDN** :**0116079201** **Tempat/Tgl.Lahir** : **-** **Jenis Kelamin** : **Perempuan** **No/Hp** : **085262060416** **Email** :**firahmirizky@gmail.com** **Pendidikan** : **- S1 – STMIK Triguna Dharma** **- S2 – Universitas Putra Indonesia (YPTK) Padang** **Bidang Keahlian** : **Aljabar Linier, SPK, Statistika dll**