J-SISKO TECH
Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
P:ISSN : 2621-8976 E-ISSN : 2615-5133 ■ 96
Vol.3, No.1, Januari 2020, pp.96-102

Aplikasi Pengamanan Dokumen Penjualan Tiket Pesawat Di Pt. Benua Raya Jaya Tour And Travel Menggunakan Metode Advanced Encryption Standard (AES)

***Badrul Anwar, Azanuddin, Nurcahyo Budi Nugroho, Rahmadani Siregar**
Program Studi Sistem Informasi, STMIK Triguna Dharma
Jl. A.H Nasution No.73 Medan, Sumatera Utara, 20142
E-mail: badrul_anwar@trigunadharma.ac.id

Abstrak

Hal yang sangat penting dalam komunikasi menggunakan computer dan jaringan computer adalah keamanan dokumen, data ataupun informasi dalam proses pertukaran data. Hal ini disebabkan karena kemajuan di bidang jaringan komputer dengan konsep open system-nya sehingga memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Sistem-sistem vital yang membutuhkan pengamanan data saat ini seperti pengamanan dokumen penjualan tiket pesawat sangat diperlukan, sehingga kecurangan ataupun perubahan yang dilakukan oleh pihak yang tidak berkepentingan dan tidak bertanggung jawab di PT.Benua Raya Jaya Tour and Travel bisa diatasi, apabila perubahan dokumen penjualan tiket pesawat tersebut terjadi, maka akan menjadi suatu masalah bagi direktur dan bagian keuangan untuk mempertanggung jawabkan hasil penjualantiketpesawat. Hal ini mengakibatkan kurang efektif dan efisien dalam proses pengolahan dokumen penjualan tiket pesawat. Oleh karena itu diperlukan adanya sistem pengamanan dokumen penjualan tiket pesawat dengan menggunakan algoritma Advanced Encryption Standart (AES) Dengan adanya sistem tersebut diharapkan kinerja dan waktu dalam pengolahan dokumen penjualan tiket pesawat menjadi lebih efektif dan efisien baik dari segi kecepatan dan keamanan data dalam penyimpanannya.
Hasil program ini menunjukkan bahwa sistem yang dibangun dengan berbasis web dapat mempermudah direktur dalam melakukan penyimpanan dokumen penjualan tiket pesawat di database dan juga dapat membantu bagian keuangan dalam pembuatan laporan penjualan tiket pesawat, dengan sistem ini pimpinan pada PT. Benua Raya Jaya Tour and Travel dapat meminimalisir kebocoran dokumen penjualan tiket pesawat, dengan sistem ini bagian keuangan dapat membuat report dokumen penjualan tiket pesawat dengan cepat dan efisien dan juga mempermudah kepala Perusahaan untuk melihat laporan penjualan tiket pesawat, dan dengan mengimplementasikan sistem pengamananan dokumen penjualan tiket pesawat menggunakan metode AES akan mempermudah dan mempercepat dalam pembuatan dokumen penjualan tiket pesawat dan juga memberikan keamanananya.

Kata Kunci :Algoritma Kriptografi AES, Penjualan Tiket Pesawat, PT. Benua Raya Jaya Tour and Travel.

Abstract

The most important thing in communication using computers and computer networks is the security of documents, data or information in the data exchange process. This is due to advances in the field of computer networks with its open system concept making it easier for

someone to enter the network. Vital systems that require data security today such as securing flight ticket sales documents are indispensable, so fraud or changes made by unauthorized and irresponsible parties at PT. Benua Raya Jaya Tour and Travel can be overcome, if changes in sales documents If the plane ticket occurs, it will be a problem for the director and the finance department to account for the sales results of the aircraft. This resulted in less effective and efficient processing of aircraft ticket sales documents. Therefore we need a system to secure aircraft ticket sales documents using the Advanced Encryption Standard (AES) algorithm. With this system, it is expected that the performance and time in processing flight ticket sales documents will be more effective and efficient both in terms of speed and security of data in storage.The results of this program show that the web-based system can facilitate the director in storing flight ticket sales documents in the database and can also assist the financial department in making flight ticket sales reports, with this system the leadership of PT. Benua Raya Jaya Tour and Travel can minimize leakage of airline ticket sales documents, with this system the finance department can make flight ticket sales document reports quickly and efficiently and also makes it easier for the head of the Company to view flight ticket sales reports, and by implementing a system for securing ticket sales documents aircraft using the AES method will simplify and speed up the production of flight ticket sales documents and also provide safety.

Keywords: AES Cryptographic Algorithm, Airplane Ticket Sales, PT. Benua Raya Jaya Tour and Travel.

I. PENDAHULUAN

Tiket pesawat adalah dokumen yang dikeluarkan oleh sebuah maskapai penerbangan atau agen perjalanan, untuk mengkonfirmasikan bahwa seseorang telah membeli kursi penerbangan di pesawat terbang. Hal yang sangat penting dalam komunikasi menggunakan komputer adalah keamanan dokumen, data ataupun informasi dalam proses pertukaran data. Teknik penyandian ini disebut Teknik Kriptografi dimana suatu dokumen, data, informasi dan pesan disembunyikan dengan sekumpulan teknik yang menyediakan keamanan informasi. Dalam kriptografi terdapat dua konsep utama penyandian yaitu enkripsi dan dekripsi. Kriptografi dapat dibedakan menjadi kriptografi kunci simetris dan asimetris. Pada kriptografi kunci simetris, kunci untuk proses enkripsi sama dengan kunci pada proses dekripsi.

Pengamanan dokumen penjualan tiket pesawat di PT. Benua Raya Jaya Tour and Travel sangat perlu, agar terhindar dari kecurangan ataupun adanya perubahan yang dilakukan oleh pihak yang tidak berkepentingan dan tidak bertanggung jawab. Dan masalah ini bisa diatasi dengan menggunakan salah satu metode dari kriptografi yaitu Advanced Encryption Standard (AES).

Meode Advanced Encryption Standard (AES) merupakan blok chipetextt simetrikyang dapat mengenkripsikan dan mendekripsikan dokumen menggunakan kunci kriptografi 128, 192 dan 256 bit untuk mengenkripsi dan dekripsi data pada blok 128 bit. AES mempunyai keunggulan dalam keamanan, kecepatan dan karakteristik algoritma beserta implementasinya.

II. METODE PENELITIAN

1. Kriptografi

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata kriptografi dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. (Ariyus, 2006 : 77)

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik metematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. (Sadikin, 2012 : 9)

2. Advanced Encryption Standard (AES)

Menurut Ibrahim (2017 : 54) “Advanced Encryption Standard (AES) merupakan blok chipertext simetrik yang dapat mengenkripsikan (encipher) dan dekripsi (decipher) informasi. Yang menggunakan kunci 128, 192, dan 256 bit untuk mengenkrip dan dekripsi data”

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan kedalam state akan mengalami transformasi byte AddRoundKey.setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut dengan round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns.

Garis besar algoritma AES Rijndael yang beroprasi pada blok 128 bit dengan kunci 128 bit (diluar proses pebangkitan roundkey) adalah sebagai berikut:

a. .AddRounKey, melakuan XOR antara awal (plaintext) dengan cipher key.
b. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah:
    - SubBytes adalah subsitusi byte menggunakan table substitusi (S-Box).
    - ShifRows adalah pergeseran baris-baris array state secara wrapping.
    - MixColumns adalah mengacak data di masing-masing kolom array state.
    - AddRoundKey adalah melakukan XOR antara state sekarang round key.
c. Final Round, proses untuk putaran terakhir:
    - SubBytes
    - ShiftRow
    - AddRounKey

3. Penjualan Tiket Pesawat

Istilah penjualan mempunyai pengertian dalam arti mikro dan makro. Penjualan dalam arti mikro yaitu penyelenggaraan kegiatan yang berusaha mencapai tujuan organisasi, dengan cara memperkirakan kebutuhan langganan dan mengarahkan suatu arus barang dan jasa untuk memenuhi kebutuhan dari produsen ke konsumen. Sedangkan dalam penjualan makro yaitu proses sosial yang mengarahkan arus barang-barang dan jasa-jasa dari suatu perekonomian dari produsen ke konsumen, dengan cara yang selektif menyesuaikan penawaran dan permintaan untuk mencapai tujuan yang diinginkan masyarakat.

Menurut Isnandi & Wardani (2014 : 20) “Penjualan merupakan kegiatan manusia yang bertujuan untuk memuaskan kebutuhan dan keinginan langganan, melalui proses pertukaran dan pihak-pihak yang berkepentingan dengan perusahaan”.

Menurut Umar dkk (2016 : 4) “Tiket pesawat adalah dokumen yang dikeluarkan oleh sebuah maskapai penerbangan atau agen penjualan, untuk mengkonfirmasi bahwa seseorang telah membeli kursi penerbangan dipesawat terbang”.

Jadi penjualan tiket pesawat terbang adalah kegiatan manusia untuk memuaskan kebutuhan dan keinginan pelanggan dengan cara, sebuah maskapai penerbangan atau agen penjualan dapat mengeluarkan dokumen pembelian kursi penerbangan.

III. ANALISIS DAN HASIL

Algoritma yang diterapkan dalam pengamanan dokumen penjualan tiket pesawat adalah algoritma Advanced Encryption Standard (AES). Advanced Encryption Standard menggunakan 4 transformasi yaitu SubBytes, ShiftRows, MixColumns dan AddRounKey. Penyandiannya menggunakan proses berulang yang disebut ronde. Jumlah ronde yang digunakan yaitu 10 karena panjang kunci yang digunakan 128 bit. Plaintext yang akan di enkripsi, diurutkan dan dimasukkan kedalam state 4 x 4. Plaintext yang telah dimasukkan ke dalam state akan mengalami 4 transformasi di atas dan di XOR-kan dengan masig-masing dengan kunci yang berbeda setiap rondenya (roun key).

1. Ekspansi Kunci

Kunci ronde round key diperlukan untuk proses enkripsi dan dekripsi Advanced Encryption Standard. Maximal panjang kunci adalah sebnayak 10 digit dan jumlah kunci ronde yang dibutuhkan yaitu 10 kunci yang akan diperoleh dari proses ekspansi kunci. Pada kasus ini, kunci yang akan digunakan yaitu “DATAPENJUALANTKT”. Berikut ini adalah proses ekspansi kunci pada algoritma Advanced Encryption Standard.

D	A	T	A	P	E	N	J	U	A	L	A	N	T	K	T
44	41	54	41	50	45	4E	4A	55	41	4C	41	4E	54	4B	54

$$\begin{bmatrix} 65 & 35 & 60 & 2E \\ F2 & B7 & F6 & A2 \\ 74 & 34 & 76 & 3D \\ 6E & 2A & 65 & 31 \end{bmatrix} \quad \begin{bmatrix} 5D & 68 & 08 & 26 \\ D5 & 62 & 94 & 36 \\ B3 & 89 & FF & C2 \\ 5F & 7B & 1E & 2F \end{bmatrix} \quad \begin{bmatrix} 5C & 34 & 3C & 1A \\ F0 & 92 & 06 & 30 \\ A6 & 2F & D0 & 12 \\ A8 & D3 & CD & F2 \end{bmatrix}$$

Kunci Ronde Ke-1 Kunci Ronde Ke-2 Kunci Ronde Ke-3

$$\begin{bmatrix} 50 & 64 & 58 & 42 \\ 39 & AB & AD & 9D \\ 3E & 11 & C1 & D3 \\ 0A & D9 & 14 & F6 \end{bmatrix} \quad \begin{bmatrix} 1E & 7A & 22 & 60 \\ 5F & F4 & 59 & C4 \\ 7C & 6D & AC & 7F \\ 26 & FF & EB & 1D \end{bmatrix} \quad \begin{bmatrix} 22 & 58 & 7A & 1A \\ 8D & 79 & 20 & E4 \\ D8 & B5 & 19 & 66 \\ F6 & 09 & E2 & FF \end{bmatrix}$$

Kunci Ronde Ke-4 Kunci Ronde Ke-5 Kunci Ronde Ke-6

$$\begin{bmatrix} 0B & 53 & 29 & 33 \\ BE & C7 & E7 & 03 \\ CE & 7B & 62 & 04 \\ 54 & 5D & BF & 40 \end{bmatrix} \quad \begin{bmatrix} F0 & A3 & 8A & B9 \\ 4C & 8B & 6C & 6F \\ C7 & BC & DE & DA \\ 97 & CA & 75 & 35 \end{bmatrix} \quad \begin{bmatrix} 43 & E0 & 6A & D3 \\ 1B & 90 & FC & 93 \\ 51 & ED & 33 & E9 \\ C1 & 0B & 7E & 4B \end{bmatrix}$$

Kunci Ronde Ke-7 Kunci Ronde Ke-8 Kunci Ronde Ke-9

$$\begin{bmatrix} A3 & 43 & 29 & FA \\ 05 & 95 & 69 & FA \\ E2 & 0F & 3C & D5 \\ A7 & AC & D2 & 99 \end{bmatrix}$$

Kunci Ronde Ke-10

2. Enkripsi

Penjelasan mengenai proses enkripsi berupa dokumen penjualan tiket pesawat pada PT. Benua Raya Jaya Tour and Travel. Adapun contoh penjualan tiket pesawat yaitu “PT.BENUARAYAJAYA”. Berikut ini adalah proses enkripsi dari plaintext tersebut:

P	T	.	B	E	N	U	A	R	A	Y	A	J	A	Y	A
50	54	2E	42	45	4E	55	41	52	41	59	41	4A	41	59	41

Hasil dari proses AddRoundKey pada ronde ke-10 merupakan hasil akhir proses enkripsi yaitu : 9260E417784B8B0AEBA9D579D0ACDA3B.

3. Dekripsi

Proses transformasi pada dekripsi dalam metode Advanced Encryption Standard yaitu InvSubBytes, InvShiftRows, InvMixColumn dan AddRoundKey. AddRoundaKey merupakan transformasi yang bersifat self-invers. Kunci yang digunakan sama dengan yang digunakan pada proses enkripsi. Berikut adalah proses dekripsi dari hasil ciphertext yang telah diperoleh dari sebelumnya.

Setelah proses ronde ke-10 selesai, hasil dari *InvSubBytes* ronde ke-10 di-*XOR*-kan dengan *cipherkey* atau kunci ronde ke-0.

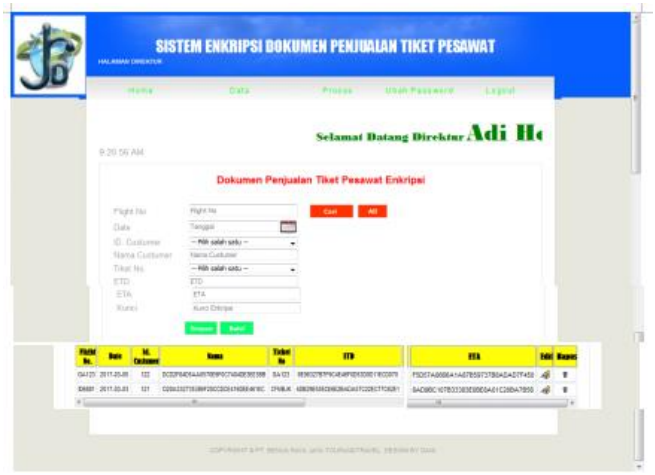
14	15	07	04		44	41	54	41		50	54	2E	42
15	0B	00	15	⊕	50	45	4E	4A	=	45	4E	55	41
7A	1B	15	12		55	41	4C	41		52	41	59	41
03	0B	00	15		4E	54	4B	54		4A	41	59	41

Langkah selanjutnya adalah mengubah hasil dari *InvSubBytes* ronde ke-10 di-*XOR*-kan dengan *cipherkey* ke dalam bentuk bilangan desimal kemudian diubah lagi ke dalam bentuk text berdasarkan kode ASCII.

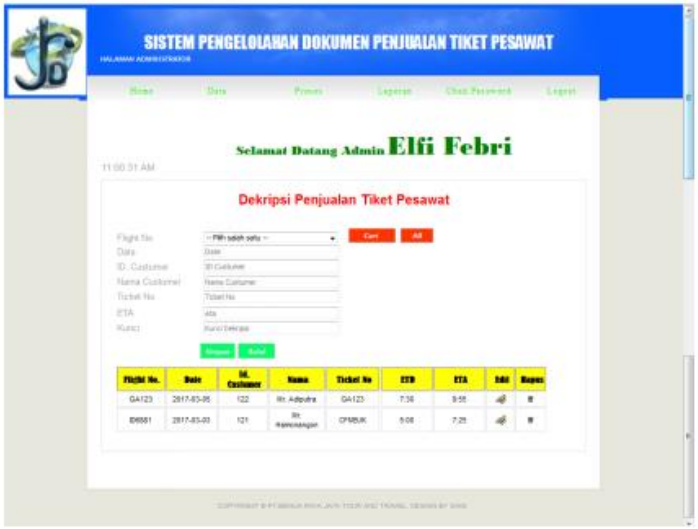
50	54	2E	42	45	4E	55	41	52	41	59	41	4A	41	59	41

PlainText

P	T	.	B	E	N	U	A	R	A	Y	A	J	A	Y	A



Gambar 1 Form Enkripsi Penjualan Tiket Pesawat



Gambar 2 Form Dekripsi Penjualan Tiket Pesawat

IV. Kesimpulan

Setelah menyelesaikan tahapan-tahapan dalam perancangan sistem pengamanan dokumen penjualan tiket pesawat menggunakan metode Advanced Encryption Standart Pada PT. Benua Raya Jaya Tour and Travel. Maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Dengan menganalisa permasalahan dan kebutuhan perancangan sistem pengamanan dokumen penjualan tiket pesawat maka dapat diketahui alur kerja dokumen penjualan tiket pesawat, permasalahan dokumen penjualan tiket pesawat dan kebutuhan yang diperlukan untuk sistem pengamanan dokumen penjualan tiket pesawat
2. Dengan merancang sistem pengamanan dokumen penjualan tiket pesawat menggunakan metode Advanced Encryption Standart Pada PT. Benua Raya Jaya Tour and Travel berbasis web, dapat mempermudah direktur dalam melakukan pengamanan dokumen penjualan tiket pesawat dan juga dapat membantu bagian keuangan dalam pembuatan laporan penjualan tiket pesawat.
3. Dengan mengimplementasikan sistem pengamanan dokumen penjualan tiket pesawat menggunakan metode Advanced Encryption Standart Pada PT. Benua Raya Jaya Tour and Travel dapat mempermudah dan mempercepat dalam pembuatan dokumen penjualan tiket pesawat dan juga memberikan keamanan dalam hal penyimpanan dokumen penjualan tiket pesawat di database

DAFTAR PUSTAKA

Anton Wasid Nugroho dkk. 2015. Aplikasi Runnimg Text Dengan Update Informasi Via Sms. Jurnal Coding Sistem Komputer Untan, 03(2), 23-32.

Ami, A. I. 2017. Perancangan Pengamanan Data Menggunakan Algoritma AES

(Advanced Encryption Standard). Jurnal Teknik Informatika STMIK Antar Bangsa, III(1), 53-60.

Basri. 2016. Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi. Jurnal Ilmiah Ilmu Komputer, 2(2),

17-23.

Christianus Sigit Sulistya. 2013. Adobe Dreamweaver CS6. Yogyakarta, Andi.

Dony Ariyus. 2006. Computer Security. Yogyakarta, Andi.

Isnandi & Indah Uly Wardati. 2014. Sistem Informasi Penjualan Tiket Pada Al Fath Tours Dan Travel Pacitan. Speed Journal Sentra Egineering Dan

Edukasi, 11(2), 19-23.

Janner Simarmata & Imam Paryudi. 2006-2010. Basis Data. Yogyakarta, Andi.

Mahmud Hidayatulloh & Entik Insannudin. 2016. Enkripsi dan Dekripsi Menggunakan Vigenere Cipher ASCII Java. Jurnal Teknik Informatika

UIN Bandung, II, 01-05.

Priyanto Hidayatullah. 2014. Pemrograman Web. Bandung, Informatika Bandung.

Rifki Sadikin. 2012. Kriptografi Untuk Keamanan Jaringan. Yogyakarta, Andi.

Rosa A. S. & M. Shalahuddin. 2014. Rekayasa Perangkat Lunak. Bandung, Informatika Bandung.

Sudirman Hi Umar dkk. 2016. Pengaruh Strategi Pemasaran B2B (Business To Business) Dan B2C (Business To Costumer) Terhadap Cara Pembelian

Tiket Pesawat Di Lingkungan Mahasiswa. Jurnal Flight Attendant Kedirgantaraan, 3(2), 1-12.