IMPLEMENTASI ENKRIPSI DAN DESKRIPSI DATA SIAK (SISTEM INFORMASI ADMINISTRASI KEPENDUDUKAN) MENGGUNAKAN ALGORITMA DES, AES DAN MD5

Putra Adi Wijaya[1], Meilani Damanik[2], Puspita Hartati[3], Indra Gunawan[4]
Program Studi Sistem Informasi
STIKOM Tunas Bangsa Pematangsiantar
Putraadiwijaya265@gmail.com [1]

Abstrak

Abstrak— Perkembangan teknologi yang semakin berkembang pesat setiap saatnya mengakibatkan terbukanya cela bagi oknum oknum yang tidak betanggung jawab untuk masuk kedalam suatu program atau data,guna untuk mengetahui suatu data /program yang bersifat rahasia. Dari sekian banyak manfaat atau dampak positif yang di timbulkan oleh perkembangang teknologi, Banyak Juga Dampak-Dampak negatif yang di timbulkan oleh perkembangan teknologi tersebut. Yang di antaranya adalah tentang keamanan yang semakin mudah di retas oleh setiap orang di karenakan akses untuk masuk ke suatu program atau data seseorang semakin muda, karna adanya dukungan akses internet dan teknologi lainnya. Oleh sebab itu kita harus mengantisipasi secara tepat agar tidak menjadi masala yang berkesinambungan di masa yang akan datang. Pada penelitian ini dilakukan pengamanan data siak menggunakam 3 metode yang berbeda yaitu metode DES (*data encryption standart),* AES *(advanced encryption standart), MD5(Message Digest 5)*. ketiga metode ini berguna untuk meng enkripsi data. DES Lebih dulu di perkenalkan di dunia komputer, sementara AES adalah metode yang di ciptakan guna untuk meminimalisir kekurangan yang terdapat di dalam algoritma des Sementara MD5 adalah algoritma yang di buat guna untuk mempermuda dalam enkripsian data.

Kata Kunci : computer, des, aes, md5

DOI: https://doi.org/10.29103/techsi.v12i1.1302

Abstract

Abstract— The development of technology that is growing rapidly every time results in the opening of reproach for unscrupulous individuals who are not responsible for entering into a program or data, in order to find out a data / program that is confidential. Of the many benefits or positive impacts caused by the development of technology, there are also many negative impacts caused by the development of these technologies. Which of them is about security that is increasingly easy to crack by everyone because access to enter a program or data is getting younger, because of the support of internet access and other technologies. Therefore we must anticipate precisely so as not to become a sustainable problem in the future. In this research, siak data security is done using 3 different methods, namely DES (data encryption standard) method, AES (advanced standard encryption), MD5 (Message Digest 5). These three methods are useful for encrypting data. DES First introduced in the world of computers, while AES is a method created to minimize the deficiencies contained in the des algorithm. While MD5 is an algorithm that is made to make it easier in data encryption.

Keywords: computer, des, aes, md5

1. Pendahuluan

Pada dasarnya sistem administrasi kependudukan merupakan sub sistem dari sistem administrasi Negara, yang mempunyai peranan penting dalam pemerintahan dan pembangunan penyelenggaraan administrasi kependudukan.rahasia yang terdapat di dalam data tersebut bersifat rahasia, oleh karna itu perlu pengamanan yang khusus, guna untuk mengamankan data tersebut agar tidak di ketahui oleh oknum-oknum yang tidak betanggung jawab.

Pengamanan data ini kami lakukan guna untuk memperkecil tingkat kejahatan yang memanfaatkan data diri penduduk, yang merupakan suatu data yang tidak seharusnya di ketahui oleh banyak orang. Kurangnya penanggulangan untuk menanggulangi

DOI: https://doi.org/10.29103/techsi.v12i1.1302

masala ini,mengakibatkan semakin banyaknya data kependudukan yang di salah gunakan,contohnya sebagai data palsu untuk orang yang bukan prmilik data tersebut untuk menjalankan niat dan tujuannya.

Dengan menggunakan 3 algoritma yang berbeda yaitu Algoritma DES (data encryption standart),AES (advanced encryption standart) dan MD5(Message Digest 5) data siak yang bersifat rahasi tersebut dapat teramankan secara efisien.

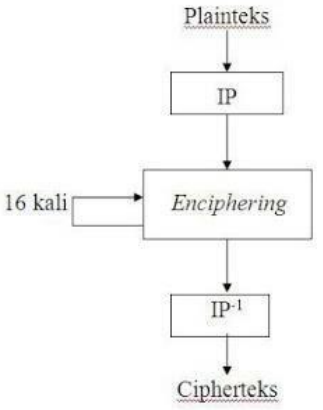
2. Metode Penelitian

Data Encryption Standard (DES) adalah salah satu algoritma kriptografi simetris, artinya kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi. Algoritma DES ini juga merupakan algoritma enkripsi block-chiperdengan panjang blok 64 bit dan dengan panjang kunci 56 bit yang bersifat rahasia yang dibagi (shared secret). Shared secret sendiri merupakan sepenggal data yang hanya diketahui oleh pihak - pihak yang melakukan komunikasi, dalam hal ini yaitu pengirim pesan dan penerima pesan. Yang dimaksud sepenggal data di sini dapat berupa kata sandi (password), passphrase, atau kunci pada algoritma enkripsi. Saat ini DES sudah hampir tidak digunakan lagi karena panjang kunci yang hanya 56 bit itu amat dengan mudah dibongkar dengan serangan Brute Force. Menggunakan prosesor tercepat saat tulisan ini dibuat, DES dapat dibongkar hanya dalam waktu beberapa menit. Algoritma lain yang dianggap sebagai ganti dari algoritma DES ialah algoritma AES (Advanced Encryption Standard).

Data Encryption Standard

Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti/dibaca manusia (plainteks) ke bentuk lain yang tidak dapat dimengerti/dibaca oleh manusia (cipherteks). Proses transformasi plainteks menjadi chiperteks diistilahkan dengan enkripsi.

DOI: https://doi.org/10.29103/techsi.v12i1.1302



Gambar 1. Cara Kerja Data Enkripsi

Advance Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext.

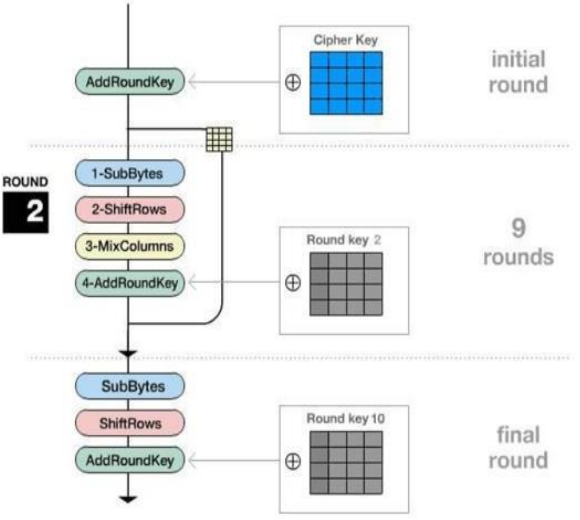
AES (Advanced Encryption Standard) adalah lanjutan dari algoritma enkripsi standar DES (Data Encryption Standard) yang masa berlakunya dianggap telah usai karena faktor keamanan. Kecepatan komputer yang sangat pesat dianggap sangat membahayakan DES, sehingga pada tanggal 2 Maret tahun 2001 ditetapkanlah algoritma baru Rijndael sebagai AES.

AES memiliki ukuran block yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. Berdasarkan ukuran block yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Sedangkan **Rijndael** sendiri

DOI: https://doi.org/10.29103/techsi.v12i1.1302

dapat mempunyai ukuran matriks yang lebih dari itu dengan menambahkan kolom sebanyak yang diperlukan.

Blok chiper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak. Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok-blok tersebut dalam bentuk heksadesimal. Barulah kemudian blok itu akan diproses dengan metode yang akan dijelaskan. Secara umum metode yang digunakan dalam pemrosesan enkripsi dalam algoritma ini dapat dilihat melalui gambar berikut:



Gambar 2. Cara Kerja *AES Method*

DOI: https://doi.org/10.29103/techsi.v12i1.1302

3. Hasil dan Pembahasan

Sampel Data SIAK
(Sistem Informasi Administrasi Kependudukan)

DATA SIAK (SISTEM INFORMASI ADMINISTRASI KEPENDUDUKAN)						
NO		NO KK	NAMA	NIK	JENIS KELAMIN	TANGGAL LAHIR
1	1	1208021402080713	PAIDI	1208020704650001	LAKI-LAKI	4-Jul-1965
	2		ROMINAH	1208027112660055	PEREMPUAN	31-12-1966
	3		DARA ELZA PUTRI	1208026701080002	PEREMPUAN	27-01-2008
	4		SUKILAH	1208027112380008	PEREMPUAN	31-12-1938
2	5	1208021402080666	WAKIDI	1208021202520001	LAKI-LAKI	2-Dec-1952
	6		MESINEM	1208024911690001	PEREMPUAN	11-Sep-1969
	7		ERWIN GUNAWAN	1208021912000001	LAKI-LAKI	19-12-2000
3	8	1208023008160003	ANDI FARIKO	1208022306900001	LAKI-LAKI	23-06-1990
	9		TIKA SILPIYA	1208217006950004	PEREMPUAN	30-06-1995
	10		ANDRIAN ANUGRAH RAMADHAN	1208020307160002	LAKI-LAKI	3/7/2016
4	11	1208021602170004	BILLY AZHAR ZEIN	1208021807890002	LAKI-LAKI	18-07-1989
	12		RIA ANJELA	1208025708970003	PEREMPUAN	17-08-1997
	13		REYFALDI AZHAR	1208020602160002	LAKI-LAKI	2-Jun-2016
5	14	1208022507130001	MARIA	1208027112690034	PEREMPUAN	31-12-1969
6	15	1208021210110004	JUNI AGUSTINA	1208026608770003	PEREMPUAN	26-06-1977

DOI: https://doi.org/10.29103/techsi.v12i1.1302

	16		YELSY PUIGA UTARI	1208026408980003	PEREMPUAN	24-08-1998
7	17	1208021402080633	JUMINA	1208027112590005	PEREMPUAN	31-12-1959
8	18	1208022912140006	SUMINEM	1208025512370001	PEREMPUAN	16-12-1937
9	19	1208021501150010	ERNI JULIANA	1208024411900001	PEREMPUAN	11-Apr-1990
	20		MUHAMMAD ADITYA	1208020904140004	LAKI-LAKI	4-Sep-2014
10	21	1208020607170005	WAGINI	1208027006710001	PEREMPUAN	30-06-1971
	22		WIDIA PIRAMITA	1208024509010001	PEREMPUAN	9-May-2001
	23		MUZAKI PRASETYO	1208022101060002	LAKI-LAKI	21-01-2006
	24		HASRIRA KHAIFANI	1208025701100002	PEREMPUAN	17-01-2010
11	25	1208021602160004	YANTI	1208027112660054	PEREMPUAN	31-12-1966
	26		RANI	1208026401970002	PEREMPUAN	24-01-1997
12	27	1208022008100018	BERTA TAMBUNAN	1208027112470014	PEREMPUAN	31-12-1947
	28		ADELIA PUTRI NAIPOSPOS	1208025710900001	PEREMPUAN	17-10-1990

Proses Enkripsi menggunakan Algoritma DES, AES, dan MD5

Login	
User id	Password
admin	Admin
computer	1334 57799BBCDFF1
teknik	**74 65 6b 6e 69 6b**

DOI: https://doi.org/10.29103/techsi.v12i1.1302

Dari table di atas kami akan mencoba mengambil bebarapa contoh untuk meng enkripsi data untuk login agar keamanan data kependudukan yang kita amankan terjamin dan tidak dapat di ketahui oleh banyak orang melainkan hanyalah orang-orang yang berhak mengetahuinya saja.

Data yang berwarna kuning adalah data yang akan kami coba enkripsi menggunakan ketiga metode di atas, di mana ini bertujuan untuk mengamankan dan memperkecil celah untuk masuk yaitu orang-orang yang tidak bertanggung jawab dan ingin menggunakan data penduduk guna untuk melaksanakan niat yang ingin dia wujudkan.

4. Kesimpulan

Berdasarkan hasil penelitian, pengujian, implementasi serta pembahasan mengenai Algoritma *Advanced Encryption Standard,* Algoritma data encryption standard dan Algoritma *Message Digest 5* dalam enkripsi dokumen SIAK:

1. File yang dihasilkan oleh proses enkripsi bisa menjadi 2 kali lipat bahkan lebih dari ukuran dan jumlah karakter file aslinya ini dikarenakan hasil enkripsi dibuat dalam hex. Satu karakter diwakili dua karakter hex, misalkan karakter "U" dalam hex menjadi "75" begitu juga karakter simbol dan spasi juga ada hex-nya. Jadi file hasil enkripsi bisa 2 kali bahkan lebih dari ukuran dan jumlah karakter file aslinya.
2. Dari hasil penelitian, telah dibuktikan bahwa ukuran file hasil enkripsi dan kebutuhan waktu proses dipengaruhi oleh ukuran file asli, namun tidak dipengaruhi oleh jenis format file. Semakin besar ukuran file asli maka semakin besar pula ukuran file hasil enkripsi dan kebutuhan waktu prosesnya.
3. Untuk Menjaga data siak (Sistem Informasi Administrasi kependudukan) Dapat Di Gunakan berbagai macam metode yang di antaranya adalah ketiga metode di atas.

Daftar Pustaka

Jurnal Rekursif, Vol. 4 No. 3 September 2016, ISSN 2303 0755.

Kurniawan,Ivan.2012.http://studyinformatics.blogspot.co.id/202 /07/des-data-encryption- standard.html. *Practical Approach to Design, Implementation and Management*". 1998.

D.a. Rijmen, "AES submission document on Rijndael," 1998.

E. Asliana, "The Procurement of Government Goods and Services in Indonesia," 2012.

F.Widyaningrum, "Implementasi dan Analisis Aplikasi Transfer File Antar PC Menggunakan Algoritma RC4 128 BIT dan AES 128 BIT," 2008.

Inayatullah, "Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password," 2009.

Jogiyanto, H. "*Analisis dan Perancangan Sistem Informasi*". 2001.

L.UNIB,"http://lpse.unib.ac.id/eproc/tentang kami : diakses pada tanggal 05 Desember 2015."

Pender, T. A. (2002). *UML Weekend Crash Course.* Canada: Wiley Publishing, Inc.

Rosa & Shalahuddin, "Metode Pengembangan Sistem," 2011.

S.Bahri, "Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5," 2012.

T.T. N. Duc H. Nguyen, Tan N. Duong, Phong H. Pham, "Cryptanalysis of MD5 on GPU Cluster," 2008.

V.Luisiana, "Implementasi Kriptografi Pada Fle Dokumen Menggunakan Algoritma AES-128," 2001.

V.Yuniati, "Enkripsi Dan Dekripsi Dengan Algoritma AES 256 Untuk Semua Jenis File," 2009.