JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi] E-ISSN : 2723-6129
Vol.3 No.3, September-Maret 2021, pp 197-201

Perancangan Aplikasi Penyandian Teks Menggunakan Algoritma Triple DES

Maria Siahaan[1], Jonson Manurung[2]
[1]Jl. Iskandar Muda No.1 Medan
[2]Jl. Iskandar Muda No.1 Medan
[1]mariasiti210396@gmail.com, [2] Johnson.geo@gmail.com

INFORMASI ARTIKEL

KataKunci:
Keamanan ,
Kriptografi,
Algoritma Triple DES

ABSTRAK

Pada perkembangan teknologi saat ini, penting untuk kita menjaga keamanan dari keaslian data kita . Karena perkembangan ilmu teknologi tidak hanya dimanfaatkan orang untuk hal positif, melainkan banyak yang menyalahgunakannya secara negatif bahkan merusak data untuk kepentigan pribadinya. Salah satu pengamanan data yang berupa teks dalam kriptografi adalah algoritma *Triple DES.* Algoritna *Triple DES (Data Encryption Standard)* merupakan salah satu algoritma kriptografi *cipher block* dengan ukuran bloknya 64 bit serta ukuran kuncinya 56 bit. Proses yang terdapat dalam algoritma *Triple DES* adalah proses *Enkripsi* dan *Deksripsi.* Dimana proses enkripsi merupakan pengubahan pesan asli menjadi pesan yang tidak dapat dimengerti. Sedangkan proses dekripsi merupakan proses pengembalian pesan menjadi pesan asli. Dalam pembuatan aplilasi pada algoritma *Triple DES* ini, plainteks dan password harus terdiri dari 8 bit. Program yang di buat terdiri dari tiga kunci yang masing-masing kunci juga terdiri dari 8 bit. Sehingga pada saat dilakukan proses, maka hasil enkrispsi dan deskripsi dapat tampil dengan baik. Kebutuhan yang digunakan oleh algoritma ini adalah kebutuhan perangkat lunak yang terdiri dari bahasa pemograman dan kebutuhan perangkat keras yang terdiri dari *system manufacture,* sistem operasi, dan ram dalam laptop yang digunakan. Untuk dapat masuk kedalam program , pertama memasukkan *username* dan *password* kita. Setelah itu masuk ke form login. Setelah itu masukkan kunci yang digunakan. Setelah kunci sudah diisi, maka klik proses *enkripsi* atau *deksripsi* sesuai yang kita butuhkan. Program ini memiliki tingkat keamanan yang kuat karena terdiri dari tiga kunci yang memiliki panjang 8 sampai 128 digit

Keywords:
Security,
cryptography,
algorithm triple des

ABSTRACT

In today's technological developments, it is important for us to maintain the security of the authenticity of our data. Because the development of technology is not only used by people for positive things, but many people abuse it negatively and even destroy data for their personal interests. Onte of the data security in the form of text in cryptography is the triple Des algoritm. The triple Des (Data Encryption Standard) algorithm is a cipher block cryptographic algorithm with a block size of 64 bits and a key size of 56 bits. The process contained in the triple Des algotithm is the Encryption and Description process. Where the encryption process is changing the original message into an incomprehensible message. Meanwhile, the decryption process in the process of returning the message to the original message. In making applications for the Triple Des algorithm, plaintext and password must consist of 8 bits. The program that is made consists of three keys, each key also consisting of 8 bits. So that when the process in carried out, the result of the description and can appear well. The needs used by this algorithm are software requirements consisting of a programming language and hardware requirements consisting of the manufacturing system, operating system, and ram in the laptop used. To be able to enter the program, first enter our username and password. After that go to the login form. After that enter the key used. After the key has been filled, then click the encryption or description process as we need. This programs has a strong level of security it consists of three keys that have a length of 8 to 128 digits.

I. Pendahuluan

Di Era Globalisasi saat ini, teknologi computer dan *Internet* merupakan teknologi yang sangat penting dan sangat banyak digunakan manusia untuk membantu pekerjaannya. Setiap sistem yang digunakan akan menyediakan fasilitas keamanan data dimana seorang *user* harus memiliki *password* yang dapat digunakan untuk mengakses sistem tersebut.

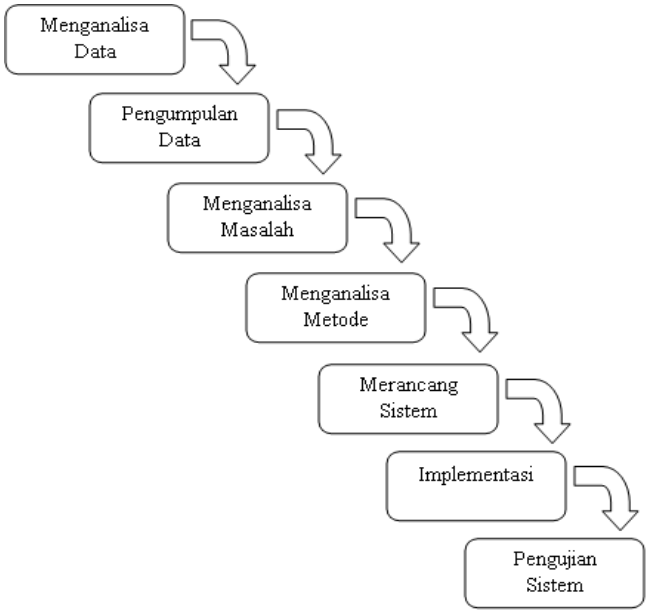
Untuk menyelesaikan masalah ini, maka *user* harus menyimpan *password* yang digunakan di tempat yang aman. Proses pengamanan *password* dapat dilakukan dengan menggunakan metode kriptografi. Kriptografi selama ini merupakan metode yang tepat untuk membantu menyelesaikan masalah. Proses yang dilakukan dalam kriptografi adalah proses enkripsi dan proses dekripsi. Enkripsi digunakan pada saat mengirim informasi dengan cara menyandikan informasi, sedangkan dekripsi digunakan pada saat menerima informasi dengan cara mengubah sandi ke informasi yang aslinya. Akan tetapi proses dekripsi ini hanya dapat digunakan apabila kunci rahasia sudah diketahui oleh pihak yang terkait..

Algoritma DES (*Data Encryption Standart)* merupakan salah satu algoritma kriptografi *cipher block* dengan ukuran bloknya 64 bit serta ukuran kuncinya 56 bit. Algoritma DES (*Data Encryption Standart)* adalah salah satu hasil modifikasi algoritma yang diberi nama Lucifer. Lucifer ini adalah salah satu algoritma *block* yang memiliki blok masukan 64 bit dan ukuran kuncinya 128 bit. Supaya algoritma dapat diimplementasikan, maka harus dilakukan pengurangan jumlah bit kunci pada DES. Algoritma DES merupakan algoritma yang memiliki tingkat keamanan yang cukup walaupun sudah banyak digunakan.

II. Metode Penelitian

Algoritma Triple DES (*Data Encryption Standart)* merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Proses yang dilakukan dalam penyandian datanya, yaitu proses enkripsi dan proses dekripsi. Algoritma triple Des adalah salah satu Algoritma pengembangan dari algoritma Des. Algorima Des hanya memiliki satu kunci. Setelah itu, algoritma Des dikembangkan kembali menjadi algoritma *Double* Des yang memiliki dua kunci. Setelah itu diuji kembali keakuratan dalam menyimpan data masih kurang akurat. Kemudian algoritna *Double Des* dikembangkan kembali menjadi algoritma *Triple* Des. Dimana algoritma ini memiliki tiga kunci yang dianggap lebih aman dalam menyimpa suatu data. Kunci yang digunakan algoritma ini boleh sama antara kunci 1, kunci 2, dank unci 3, dan boleh juga berbeda. Algoritma *Triple Des* memiliki panjang kunci 168 bit, dimana masing-masing kunci terdiri dari 56 bit panjangnya.

A. Kerangka Kerja Penelitian



Gambar 1. Kerangka Kerja Penelitian

III.Hasil Dan Pembahasan

Hasil dan pembahasan merupakan bagian akhir dari suatu penelitian. Dimana penulis telah berhasil meneliti dan menemukan hasil yang cocok dari penelitiannya. Dalam penelitian ini penulis merancang aplikasi dengan

menggunakan Plainteks, kunci, dan visual basic 2012. Adapun hasil pembahasan penelitian ini adalah sebagai berikut :

Proses Enkripsi

Plainteks : MARIASHN

Plainteks adalah pesan asli yang akan disandikan dengan menggunakan proses enkripsi dan dekripsi.

Key 1 : 16012119

Key adalah kunci yang akan digunakan sebagai password untuk dapat masuk kedalam proses enkripsi dan dekripsi.

Langkah pertama mengubah plainteks dan key 1 ke biner:

Tabel 1. Plainteks dirubah ke bentuk biner

M=	0	1	0	0	1	1	0	1
A=	0	1	0	0	0	0	0	1
R=	0	1	0	1	0	0	1	0
I=	0	1	0	0	1	0	0	1
A=	0	1	0	0	0	0	0	1
S=	0	1	0	1	0	0	1	1
H=	0	1	0	0	1	0	0	0
N=	0	1	0	0	1	1	1	0

a. Proses Enkripsi

R16= 0000 0011 0111 0101 1001 1111 1010 1011

L16= 0000 0001 0101 0111 0010 0011 1010 1000

Gabungkan R_{16} dengan L_{16} kemudian dipermutasikan untuk terakhir kali dengan tabel Invers Initial Permutasi(IP^{-1}).

Proses ini dilakukan sampai R memiliki putaran 16 dan L memiliki putaran 16.

Tabel 2. Tabel IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Keterangan:

Tabel IP-1 adalah table rumus yang digunakan oleh Algoritma Triple DES.

Tabel IP-1 digunakan sebagai penentu hasil Plainteks dalam bentuk kode-kode biner, decimal dan heksa.

Sehingga Input :

R16= 0000^{4} 0011^{8} 0111^{12} 0101^{16} 1001^{20} 1111^{24} 1010^{28} 1011^{32}

L16= 0000^{36} 0001^{40} 0101^{44} 0111^{48} 0010^{52} 0011^{56} 1010^{60} 1000^{64}

MenghasilkanOutput:

Cipher dalam biner = 11111101 01101101 00110100 00000111 00110100 00011011 00110000 00000111

Cipher dalam Hex = FD 6D 34 07 34 33 30 07

Cipher dalam Karakter = ÄÇeü)ˆrk«®|4_

X.

b. Proses Dekripsi

A3 = 010011 101000 000010 001110 111000 100101 000010 001011

Hasil ekspansi disubstitusikan kedalam S-Box:

Tabel 3. inisiasi S-Box

S1	0	1	0	0	1	1

S2	1	0	1	0	0	0
S3	0	0	0	0	1	0
S4	0	0	1	1	1	0
S5	1	1	1	0	0	0
S6	1	0	0	1	0	1
S7	0	0	0	0	1	0
S8	0	0	1	0	1	1

B3 = 6 10 0 10 6 2 11 3 diubah ke biner
B3 = 0110^{4} 1010^{8} 0000^{12} 1010^{16} 0110^{20} 0010^{24} 1011^{28} 0011^{32}
Dipermutasikan dengan table P-Box sehingga:

Tabel 4. P-Box

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	3	30	6	22	11	4	25

P3=01000010 01101110 10001110 1100001
P16: 1101000100101001000100111000111 0
Sampai iterasi 16 dan hasilnya:

Tabel 5. Konversi

Hex	4D	41	52	49
Biner	1101	0001	0010	1001
Plaintext	M	A	R	I

41	53	48	4E
0001	0011	1000	1110
A	S	H	N

1. PENUTUP

A. Kesimpulan

Berdasarkan penelitian dan uraian diatas, maka didapatkan kesimpulannya sebagai berikut:

1. *Triple DES memiliki tingkat keamanan yang berlibat dan kuat karena memiliki 3 kunci sekaligus*.
2. *Kunci yang terdapat pada Triple DES memiliki panjang 8 sampai 128 digit.*

B. Saran

Adapun saran-saran yang dapat disampaikan dari hasil penelitian Penyandian Teks Menggunakan Algoritma Triple DES antara lain.

1. Pada penelitian selanjutnya dapat mengembangkan system Enkripsi database dengan algoritma TRIPLE DES.
2. Dapat menerapkan beberapa metode sebagai perbandingan agar lebih akurat lagi.
3. Dapat dilakukan perbandingan metode lain dan kombinasi dengan metode lain.
4. Dapat mengembangkan system untuk penampilan iterasi agar mempermudah proses pembelajaran.

Dafrtar Pustaka

[1] Arief, P & Nurdin, N, 2017. ***"Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition".*** Jurnal Elektronik Sistem Informasi Dan Komputer Sekolah Tinggi Managemen Informasi dan Komputer (STMIK) Bina Mulia.

[2] Akik, H & Deni, S, 2018. ***"Perbandingan Waktu dan Kecepatan Proses Eknnkripsi dan Dekripsi Data Teks. Txt Menggunakan Algoritma Des Dan 3 Des".*** Program Studi Teknik Informatika Departement Ilmu Komputer Fakultas Matematika Dan Ilmu Pengetahuan Alam, Universitas Padjadjaran.

[3] Dermawan Hendrik Gulo, ***"Pengamanan File Mp3 Dengan Menggunakan Metode Triple Dan Encryption Standar (Triple Des)"*** , Jurnal Teknik Informatika Unika St. Thomas (JTIUST), Volume 02 Nomor 02, Desember 2017, ISSN : 2548-1916.

[4] Heru Adya Gunawan, Zainal Arifin, dan Indah Fitria Astuti, ***" Keamanan Login Web Menggunakan Metode 3 Des Berbasis Teknologi Quick Response Code"***, Jurnal Ilmiah Ilmu Komputer, 2018.

[5] Joko Susanto, Ilhamsyah dan Tedy Rismawan, ***"Aplikasi Enkripsi dan Dekripsi Untuk Keamanan Dokument Menggunakan Triple Des Dengan Memanfaatkan Usb Flash Drive"***, Jurnal Coding, Sistem Komuter Utan Volume 04, No.2 (2016).

[6] Mohammad Nafsir, 2017. ***"Pengembangan Protoype Sistem Kriptografi Untuk Enkripsi dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemograman Java".*** Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Merju Buana. Jl. Raya Meruya Selatan, Kembangan, Jakarta, 11650.

[7] Nurmalina Siregar, 2019. ***"Perancangan Aplikasi Keamanan Pesan Teks Dengan Menggunakan Algoritma Triple Des"***. STMIK Budi Darma Jl. Sisingamangaraja No.338 Sp. Limun Medan.

[8] Nurmalina Siregar, 2019. ***"Perancangan Aplikasi Keamanan Pesan Teks Dengan Menggunakan Algoritma Triple Des"***, Jurnal Teknik Informatika Kaputama (JTIK) Vol. 3, No. 2, Juli 2017.

[9] Pama Hadi Rantellinggi dan Eka Saputra, ***"Algoritma Kriptografi Triple Des dan Steganografi LSB Sebagai Metode Gabungan dalam Keamanan Data"***, Jurnal Teknologi Informatika dan Komputer.

[10] Rahmadhana, T, 2015. ***"Perancangan Aplikasi Penyandian Data Teks Menggunakan Metode Symmetric Stream Ipher"***, Mahasiswa Program Studi Teknik Informatika STMIK Budi Darma Medan. Jl. Sisingamangaraja No. 338 Sp. Limun Medan.