Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (Data Encryption Standard)

Novelius Buulolo[1], Anita Sindar[2]
Teknik Informatika STMIK Pelita Nusantara
Jl. Iskandar Muda No. 1 Medan 20154 INDONESIA
[1]novellius801@gmail.com, [2]haito_ita@yahoo.com

INTISARI

Dalam mengirim pesan ataupun pertukaran informasi menggunakan koneksi internet melalui alat komunikasi, data tersebut bisa dibaca oleh orang lain. Untuk mengatasi masalah ini diperlukan keamanan komputer untuk menjaga data dari pihak yang tidak berwenang. Permasalahan yang muncul adanya data atau dokumen yang tidak aman pada software, keamanan data pada software maka perlu diterapkan algoritma kriptografi DES dalam merancang aplikasi untuk menjaga kerahasiaan data. Data dienkrip dalam blok-blok 64 bit menggunakan kunci 56 bit. DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit, dengan tahapan dan kunci yang sama. .

Kata kunci*— Keamanan Data, Algortima DES, Cipherteks, Plainteks*

ABSTRACT

In sending messages or exchanging information using an internet connection via communication tools, the data can be read by other people. To solve this problem, computer security is needed to protect data from unauthorized parties. Problems that arise are data or documents that are not secure in the software, data security in the software, it is necessary to apply the DES cryptographic algorithm in designing applications to maintain data confidentiality. Data is encrypted in 64-bit blocks using a 56-bit key. DES transforms 64-bit input in several encryption steps into 64-bit output with the same stages and keys.

Keywords— *Data Security, DES Algorithm, Ciphertext, Plaintext*

I. PENDAHULUAN

Keamanan data merupakan apek penting untuk menjaga sebuah data maupun informasi supaya aman dan tidak mudah dibaca. Maka dari itu, data tersebut perlu untuk dijaga kerahasiaannya [1]. Data yang telah dibajak menimbulkan resiko bila informasi yang sensitif dan berharga dibaca oleh orang yang tidak bertanggungjawab. Dalam bidang teknologi informasi dan komunikasi terutama pada pertukaran suatu data atau informasi yang dikirim kepada penerima terkadang menjadi pertanyaan apakah informasi yang dikirim benar dari pengirim yang sebenarnya atau tidak, kemudian apakah data yang diterima sesuai dengan isi informasi dari pengirim yang sebenarnya dan tidak ada perubahan informasi yang terkandung didalamnya [2].

Penyimpanan data menggunakan database sudah umum digunakan oleh setiap instansi, namun penyimpanan secara langsung tanpa memberi suatu keamanan akan dapat menyebabkan data dapat dibobol dan dicuri atau dirusak oleh pihak-pihak yang tidak bertanggungjawab, ataupun seseorang yang biasa menyimpan data-data penting ke dalam suatu dokumen dengan karakter yang tidak terkode *(plaintext)*, sangatlah rawan apabila tidak berhati-hati. cryptography menyiratkan sebuah seni uUntuk dapat menjalankan dengan baik pada proses kriptografi haruslah terdapat empat elemen utama didalamnya, yang paling berkaitan satu sama lain [3]. Plain Text merupakan sebagai pesan awal atau pesan asli yang dikirim pada proses komunikasi. Plain Text inilah yang kemudian di enkripsi dan di dekripsi [4]. *Cipher Text* merupakan sebuah pesan yang tersembunyi, yaitu pesan asli *(plain text)* yang telah dienkripsi pada proses kriptografi. *Cipher Text* ini dapat diubah kembali menjadi bentuk aslinya *(plain text)* dengan memanfaatkan *key* yang sudah di sediakan [5]. Proses yang dilakukan untuk mengamankan sebuah data *(plaintext)* menjadi data yang tersembunyi *(ciphertext)* disebut dengan enkripsi *(encryption* [6]. Algoritma DES adalah salah satu metode penyandian dengan sistem *block cipher* [7]. Sistem penyandian yang

pengacakannya dilakukan secara blok demi blok dengan blok input (teks asli) 64-bit dan menghasilkan output (teks sandi) yang juga per blok 64 bit, algoritma yang digunakan adalah kunci simetris dengan panjang kunci 56 bit [8]. Setelah ditetapkan sebagai standar untuk melindungi data dan informasi baik yang ditransmisikan maupun yang disimpan, sistem sandi DES dengan cepat digunakan secara internasional pada semua berbagai aplikasi yang membutuhkan penyandian pada saat operasionalnya.

Penelitian Nuniek Fahriani et all, berjudul Pembangkit *key polyalphabetic cipher* pada kriptografi simetri menggunakan *Java* menjelaskan kriptografi adalah usaha untuk mengirim pesan rahasia ke penerima dengan menggunakan sistem kode untuk membuat pesan tersebut tidak bisa dipahami oleh pihak ketiga [9].

Penelitian Neti Rusri Yanti, Alimah, dan Afrida dengan judul Implementasi Algoritma Data *Encryption Standard* Pada Penyandian *Record Database* menjelaskan bahwa record database umumnya masih sering ditampilkan dalam bentuk teks sebagai informasi bagi pengguna, sehingga dapat mempermudah kriptanalis untuk mengakses serta memberi peluang untuk melakukan pembocoran, mendistribusikan maupun memodifikasi *record database* [10].

Penelitian Sutisna dengan judul Analisa Proteksi Serangan Enkripsi Data Melalui Keamanan Model Kriptografi Komunikasi Jaringan Komputer menjelaskan keamanan dalam menggunakan teknologi sistem informasi semakin berkembang dan perlu dicermati bagaimana suatu System Security dari mekanisme pengiriman data khususnya menggunakan metode enkripsi kriptografi dapat terjalin dengan baik satu sama lain [11].

II. METODOLOGI PENELITIAN

Uraian tahapan penelitian :

a. Perumusan Masalah

Diperlukan keamanan data pada *software (offline)* dengan menerapkan algoritma kriptografi DES dalam penelitian ini rumusan permasalahan yaitu merancang aplikasi untuk menjaga keamanan data.

b. Analisa Data

Data-data yang sudah diperoleh kemudian dianalisis dengan metode analisis deskriptif. Metode analisis deskriptif dilakukan dengan cara mendeskripsikan fakta-fakta yang kemudian disusul dengan analisis, tidak semata-mata menguraikan, melainkan juga memberikan pemahaman dan penjelasan secukupnya.

c. Penerapan metode DES

Langkah-langkah penyelesaian dari sistem kerja pada algoritma DES :

1. Proses Enkripsi

a. Blok plainteks dipermutasi dengan matrik permutasi awal (initial permutation atau IP).
b. Hasil permutasi awal kemudian di-enciphering sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
c. Hasil *enciphering* kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok cipher teks.

2. Proses Dekripsi

a. Proses dekripsi terhadap cipher teks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah K1, K2, …, K16, maka pada proses dekripsi urutan kunci yang digunakan adalah K16, K15, …, K1.
b. Tiap putaran 16, 15, …, 1, keluaran pada setiap putaran deciphering, Li = Ri – 1 ; Ri = Li – 1 ; f(Ri – 1, Ki), yang dalam hal ini, (R16, L16) adalah blok masukan awal untuk deciphering. Blok (R16, L16) diperoleh dengan mempermutasikan cipherteks dengan matriks permutasi IP-1. Pra-keluaran dari deciphering adalah adalah (L0, R0).
c. Tinjau kembali proses pembangkitan kunci internal K16 dihasilkan dari (C16, D16) dengan permutasi PC-2. (C16, D16) tidak dapat diperoleh langsung pada permulaan deciphering. Tetapi karena (C16, D16) = (C0, D0), maka K16 dapat dihasilkan dari (C0, D0) tanpa perlu lagi melakukan pergeseran bit.
d. Selanjutnya, K15 dihasilkan dari (C15, D15) yang mana (C15, D15) diperoleh dengan menggeser C16 (yang sama dengan C0) dan D16 (yang sama dengan C0) satu bit ke kanan. Sisanya, K14 sampai K1 dihasilkan dari (C14, D14) sampai (C1, D1).

III. HASIL DAN PEMBAHASAN

Penyandian pesan menggunakan algoritma DES *(Data Encryption System)* :

Plaintext (x) = COMPUTER

Key (k) = 13 34 57 79 9B BC DF F1

1. Langkah pertama :

Ubahlah plaintext dan key kedalam bentuk biner.

TABEL I.
KONVERSI BINER

Plaintext	Biner	Key	Biner
C	01000011	13	00010011
O	01001111	34	00110100
M	01001101	57	01010111
P	01010000	79	01111001
U	01010101	9B	10011011
T	01010100	BC	10111100
E	01000101	DF	11011111
R	01010010	F1	11110001

2. Langkah kedua :
Initial Permutation (IP) pada bit plaintext menggunakan tabel IP.

TABEL II.
INITIAL PERMUTATION (IP)

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

Urutan bit pada plaintext urutan ke 58 ditaruh diposisi 1, urutan bit pada
plaintext urutan ke 50 ditaruh di posisi 2, urutan bit pada plaintext urutan ke 42
ditaruh di posisi 3, dan seterusnya.

Sehingga hasil outputnya adalah :
IP(x) :11111111 10111000 01110110 01010111 00000000 00000000 00000110 10000011

Pecah bit pada IP(x) menjadi 2 bagian yaitu:
L0 : 11111111 10111000 01110110 01010111
R0 : 00000000 00000000 00000110 10000011

3. Langkah ketiga :
Generate kunci yang akan digunakan untuk mengenkripsi plainteks dengan menggunakan tabel permutasi kompresi PC-1, pada langkah ini terjadi kompresi dengan membuang 1 bit masing-masing blok kunci dari 64 bit menjadi 56 bit.

CD(k) :1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

Pecah CD (k) menjadi dua bagian kiri dan kanan, sehingga menjadi

C0 : 1111000 0110011 0010101 0101111
D0 : 0101010 1011001 1001111 0001111

4. Langkah keempat
Lakukan pergeseran kiri (Left Shift) pada C0 dan D0, sebanyak 1 atau 2 kali berdasarkan kali putaran yang ada pada tabel putaran. Untuk putaran ke 1, dilakukan pegeseran 1 bit ke kiri. Untuk putaran ke 2, dilakukan pergeseran 1 bit kekiri. Untuk putaran ke 3, dilakukan pergeseran 2 bit kekiri, dan seterusnya. Berikut hasil outputnya:

C0 : 1111000 0110011 0010101 0101111
D0 : 0101010 1011001 1001111 0001111

Digeser 1 bit ke kiri
C1 : 1110000 1100110 0101010 1011111
D1 : 1010101 0110011 0011110 0011110

Digeser 2 bit ke kiri
C2 : 1100001 1001100 1010101 0111111
D2 : 0101010 1100110 0111100 0111101

Digeser 2 bit ke kiri
C3 : 0000110 0110010 1010101 1111111
D3 : 0101011 0011001 1110001 1110101

Digeser 2 bit ke kiri
C4 : 0011001 1001010 1010111 1111100
D4 : 0101100 1100111 1000111 1010101

Digeser 2 bit ke kiri
C5 : 1100110 0101010 1011111 1110000
D5 : 0010011 0011110 0011110 1010101

Digeser 2 bit ke kiri
C6 : 0011001 0101010 1111111 1000011
D6: 1001100 1111000 1111010 1010101

Digeser 2 bit ke kiri
C7 : 1100101 0101011 1111110 0001100
D7 : 0110011 1100011 1101010 1010110

Digeser 2 bit ke kiri
C8 : 0010101 0101111 1111000 0110011
D8 : 1001111 0001111 0101010 1011001

Digeser 1 bit ke kiri
C9 : 0101010 1011111 1110000 1100110
D9 : 0011110 0011110 1010101 0110011

Digeser 2 bit ke kiri
C10 : 0101010 1111111 1000011 0011001
D10 : 1111000 1111010 1010101 1001100

Digeser 2 bit ke kiri
C11 : 0101011 1111110 0001100 1100101
D11 : 1100011 1101010 1010110 0110011

Digeser 2 bit ke kiri

C12 : 0101111 1111000 0110011 0010101
D12: 0001111 0101010 1011001 1001111

Digeser 2 bit ke kiri
C13 : 0111111 1100001 1001100 1010101
D13: 0111101 0101010 1100110 0111100

Digeser 2 bit ke kiri
C14 : 1111111 0000110 0110010 1010101
D14 : 1110101 0101011 0011001 1110001

Digeser 2 bit ke kiri
C15 : 1111100 0011001 1001010 1010111
D15 : 1010101 0101100 1100111 1000111

Digeser 1 bit ke kiri
C16 : 1111000 0110011 0010101 0101111
D16 : 0101010 1011001 1001111 0001111

Setiap hasil putaran digabungkan kembali menjadi CiDi dan diinput kedalam tabel Permutation Compression 2 (PC-2) dan terjadi kompresi data CiDi 56 bit menjadi CiDi 48 bit.

TABEL III.
PERMUTATION COMPRESSION 2 (PC-2)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

5. Langkah kelima :
Pada langkah ini, ekspansi data Ri-1 32 bit menjadi Ri 48 bit sebanyak 16 kali putaran dengan nilai perputaran 1<= i <=16 menggunakan Tabel Ekspansi (E).

TABEL IV.
EKSPANSI (E)

32	1	2	3	4	5
4	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

6. Langkah keenam
Setiap Vektor Ai disubstitusikan ke delapan buah S-Box (Substitution Box), dimana blok pertama disubstitusikan dengan S1, blok kedua dengan S2 dan seterusnya dan menghasilkan output vektor Bi 32.

TABEL V.
INITIAL PERMUTATION-1 (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	11	49	17	57	25

Sehingga *Input* :
$R_{16}L_{16}$ = 00011111 10010111 10100101 11100110 01101110 10100010 10101000 10110001.

Menghasilkan *Output*:

Cipher (dalam *biner*) = 01010110 11110001 11010101 11001000 01010010 10101111 10000001 00111111

Cipher (dalam hexa) = **56 f1 d5 c8 52 af**

IV. KESIMPULAN

Kesimpulan penelitian yaitu penyandian pesan menggunakan algoritma DES *(Data Encryption System)* dimulai dengan mengubah *plaintext* dan *key* kedalam bentuk biner. Setiap hasil putaran digabungkan kembali dan diinput kedalam tabel *Permutation Compression 2* (PC-2) dan terjadi kompresi data CiDi 56 bit menjadi CiDi 48 bit.

REFERENSI

[1] D. Darwis et al., "Proses Pengamanan Data Menggunakan Kombinasi Metode Kriptografi Data Encryption Standard dan Steganografi End Of File," no. 978, pp. 228–240, 2017.

[2] E. L. Hakim, Khairil, and F. H. Utami, "Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4 Dengan Menggunakan Bahasa Pemrograman Php," J. Media Infotama, vol. 10, no. 1, pp. 1–7, 2014.

[3] I. Irmawati, "Pengembangan Aplikasi Kriptografi File Dokumen, Audio Dan Gambar Dengan Algoritma Des," J. Ilm. FIFO, vol. 8, no. 2, p. 185, 2016.

[4] N. Laila and A. S. R. Sinaga, "Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra," Sci. Comput. Sci. Informatics J., vol. 1, no. 2, p. 47, 2019.

[5] D. Laoli, B. Sinaga, and A. Sindar, "Penerapan Algoritma Hill Cipher Dan Least Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital," JISka, vol. 4, no. 3, pp. 1–11, 2020.

[6] A. Mukhlishah, "Analisis Perbandingan Kinerja Jaringan Secure Socket Tunneling Protocol (Sstp) Dan Layer Two Tunneling Protocol (L2tp) + Internet Protocol Security

(Ipsec) Menggunakan Metode Quality Of Service (Qos),” vol. XV, pp. 16–25, 2020.

[7] A. S. R. M. Sinaga, Keamanan Komputer, CV. Insan Cendekia Mandiri, vol. 1, no. 1. 2020.

[8] D. Nurnaningsih and A. A. Permana, “Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes),” J. Tek. Inform., vol. 11, no. 2, pp. 177–186, 2018.

[9] N. M. D. Oktafiansyah, F. Agus, and S. Maharani, “Penerapan Kriptografi Dengan Algoritma Data Encryption Standart Pada Text Hasil Konversi Dari Citra,” Semin. Nas. Ilmu Komput. dan Teknol. Inf., vol. 1, no. 1, pp. 85–89, 2016.

[10] A. Siswanto, A. Syukur, and I. Husna, “Perbandingan Metode Data Encryption Standard (Des) Dan Advanced Encryption Standard (Aes) Pada Steganografi File Citra,” Semin. Nas. Teknol. Inf. Dan Komun., no. October, pp. 229–236, 2018.

[11] P. T. S. Top, E. F. Ginting, K. Ibnutama, and M. G. Suryanata, “Implementasi DES (Data Encryption Standard) Untuk Penyandian Data Bill Of Material pada Divisi Produksi,” vol. 18, no. 2, pp. 161–166, 2019.